COMMUTATIVE ALGEBRA

PETE L. CLARK

Contents

Date: March 9, 2015.

Introduction

0.1. **What is Commutative Algebra?**

Commutative algebra is the study of commutative rings and attendant structures, especially ideals and modules.

This is the only possible short answer I can think of, but it is not completely satisfying. We might as well say that *Hamlet, Prince of Denmark* is about a fictional royal family in late medieval Denmark and especially about the title (crown) prince, whose father (i.e., the King) has recently died and whose father's brother has married his mother (i.e., the Queen). Informative, but not the whole story!

0.2. **Why study Commutative Algebra?**

What are the purely mathematical reasons for studying any subject of pure mathematics? I can think of two:

I. Commutative algebra is a necessary and/or useful prerequisite for the study of other fields of mathematics in which we are interested.

II. We find commutative algebra to be intrinsically interesting and we want to learn more. Perhaps we even wish to *discover* new results in this area.

Most beginning students of commutative algebra can relate to the first reason: they need, or are told they need, to learn some commutative algebra for their study of other subjects. Indeed, commutative algebra has come to occupy a remarkably central role in modern pure mathematics, perhaps second only to category theory in its ubiquitousness, but in a different way. Category theory provides a common language and builds bridges between different areas of mathematics: it is something like a circulatory system. Commutative algebra provides core results that other results draw upon in a foundational way: it is something like a skeleton.

The branch of mathematics which most of all draws upon commutative algebra for its structural integrity is *algebraic geometry*, the study of geometric properties of manifolds and singular spaces which arise as the loci of solutions to systems of polynomial equations. In fact there is a hard lesson here: in the 19th century algebraic geometry split off from complex function theory and differential geometry as its own discipline and then burgeoned dramatically at the turn of the century and the years thereafter. But by 1920 or so the practitioners of the subject had found their way into territory in which "purely geometric" reasoning led to serious errors. In particular they had been making arguments about how algebraic varieties behave *generically*, but they lacked the technology to even give a precise meaning to the term. Thus the subject ultimately proved invertebrate and began to collapse under its own weight. Starting around 1930 there began a heroic shoring up process in which the foundations of the subject were recast with commutative algebraic methods at the core. This was done several times over, in different ways, by Zariski, Weil, Serre and Grothendieck, among others. For the last 60 years it

has been impossible to deeply study algebraic geometry without knowing commutative algebra – a lot of commutative algebra. (More than is contained in these notes!)

The other branch of mathematics which draws upon commutative algebra in an absolutely essential way is algebraic number theory. One sees this from the beginning in that the Fundamental Theorem of Arithmetic is the assertion that the ring $\mathbb{Z}$ is a unique factorization domain (UFD), a basic commutative algebraic concept. Moreover number theory was one of the historical sources of the subject. Notably the concept of Dedekind domain came from Richard Dedekind's number-theoretic investigations. Knowledge of commutative algebra is not as indispensable for number theory (at least, not at the beginning) as it is for algebraic geometry, but such knowledge brings a great clarifying effect to the subject.

In fact the interplay among number theory, algebraic geometry and commutative algebra flows in all directions. What Grothendieck did in the 1960s (with important contributions from Chevalley, Serre and others) was to create a single field of mathematics that encompassed commutative algebra, classical algebraic geometry and algebraic number theory: the theory of schemes. As a result, most contemporary number theorists are also partly commutative algebraists and partly algebraic geometers: we call this cosmopolitan take on the subject **arithmetic geometry**.

There are other areas of mathematics that draw upon commutative algebra in important ways. To mention some which will show up in later in these notes:

- Differential topology.
- General topology.
- Invariant theory.
- Order theory.

The task of providing a commutative algebraic foundation for algebraic geometry – or even the single, seminal text of R. Hartshorne – is a daunting one. Happily, this task has been completed by David Eisenbud (a leading contemporary expert on the interface of commutative algebra and algebraic geometry) in his text [Eis]. This work is highly recommended. It is also 797 pages long, so contains enough material for $3-5$ courses in the subject. It would be folly to try to improve upon, or even successfully imitate, Eisenbud's work here, and I certainly have not tried.

I myself am an arithmetic geometer (which, as I tried to explain above, is a sort of uppity kind of number theorist), so it is not surprising that these notes are skewed more towards number theory than most introductory texts on commutative algebra. However for the most part a respectful distance is maintained: we rarely discuss number theory *per se* but rather classes of rings that a number theorist would like: Dedekind domains, valuation rings, Bézout domains, and so forth.

Just much as I have included some material of interest to number theorists I have included material making connections to other branches of mathematics, especially connections which are less traditionally made in commutative algebra texts. In fact at several points I have digressed to discuss topics and theorems which make

connections to other areas of mathematics:

- §2 on Galois connections.
- §5.2 on rings of continuous functions.
- §6 on vector bundles and Swan's Theorem.
- §9 on Boolean rings, Boolean spaces and Stone Duality.
- §13 on the topology of prime spectra, including Hochster's Theorem.
- §14.6 on invariant theory, including the Shephard-Todd-Chevalley Theorem.

But I do find commutative algebra to be of interest unto itself, and I have tried to craft a sustained narrative rather than just a collection of results.

0.3. **Acknowledgments.**

Thanks to Pablo Barenbaum, Max Bender, Martin Brandenburg, John Doyle, Georges Elencwajg, Emil Jerabek, Keenan Kidwell, David Krumm, Allan Lacy, Casey LaRue, Stacy Musgrave, Alon Regev, Jacob Schlather, Jack Schmidt, Mariano Suárez-Álvarez, Peter Tamaroff and Matthé van der Lee for catching errors[1] and making other useful suggestions. Thanks to Hans Parshall for introducing me to the Stone-Tukey Theorem.

1. Commutative rings

1.1. **Fixing terminology.**

We are interested in studying properties of **commutative rings with unity**.

By a **general algebra** R, we mean a triple $(R, +, \cdot)$ where R is a set endowed with a binary operation $+ : R \times R \to R$ – called **addition** – and a binary operation $\cdot : R \times R \to R$ – called **multiplication** – satisfying the following:

(CG) $(R, +)$ is a commutative group,

(D) For all $a, b, c \in R$, $(a + b) \cdot c = a \cdot c + b \cdot c$, $a \cdot (b + c) = a \cdot b + a \cdot c$.

For at least fifty years, there has been agreement that in order for an algebra to be a **ring**, it must satisfy the additional axiom of associativity of multiplication:

(AM) For all $a, b, c \in R$, $a \cdot (b \cdot c) = (a \cdot b) \cdot c$.

A general algebra which satisfies (AM) will be called simply an **algebra**. A similar convention that is prevalent in the literature is the use of the term **nonassociative algebra** to mean what we have called a general algebra: i.e., a not *necessarily* associative algebra.

A ring R is said to be **with unity** if there exists a multiplicative identity, i.e., an element e of R such that for all $a \in R$ we have $e \cdot a = a \cdot e = a$. If e and e' are two such elements, then $e = e \cdot e' = e'$. In other words, if a unity exists, it is

[1] Of which many, many remain: your name could go here!

unique, and we will denote it by 1.

A ring R is **commutative** if for all $x,\ y \in R, x \cdot y = y \cdot x$.

In these notes we will be (almost) always working in the category of commutative rings with unity. In a sense which will shortly be made precise, this means that the identity 1 is regarded as part of the structure of a ring and must therefore be *preserved* by all homomorphisms.

Probably it would be more natural to study the class of possibly non-commutative rings with unity, since, as we will see, many of the fundamental constructions of rings give rise, in general, to non-commutative rings. But if the restriction to commutative rings (with unity!) is an artifice, it is a very useful one, since two of the most fundamental notions in the theory, that of ideal and module, become significantly different and more complicated in the non-commutative case. It is nevertheless true that many individual results have simple analogues in the non-commutative case. But it does not seem necessary to carry along the extra generality of non-commutative rings; rather, when one is interested in the non-commutative case, one can simply remark "Proposition X.Y holds for (left) R-modules over a noncommutative ring R."

Notation: Generally we shall abbreviate $x \cdot y$ to xy. Moreover, we usually do not use different symbols to denote the operations of addition and multiplication in different rings: it will be seen that this leads to simplicity rather than confusion.

Group of units: Let R be a ring with unity. An element $x \in R$ is said to be a **unit** if there exists an element y such that $xy = yx = 1$.

CONVENTION ON EXERCISES: Throughout the exercises, a "ring" means a commutative ring unless explicit mention is made to the contrary. Some but not all of the results in the exercises still hold for non-commutative rings, and it is left to the interested reader to explore this.

Exercise 1.1:
a) Show that if x is a unit, the element y with $xy = yx = 1$ is unique, denoted x^{-1}.
b) Show that if x is a unit, so is x^{-1}.
c) Show that, for all $x, y \in R$, xy is a unit $\iff$ x and y are both units.
d) Deduce that the units form a commutative group, denoted $R^\times$, under multiplication.

Remark 1. *For elements x, y in a non-commutative ring R, if x and y are units so is xy, but the converse need not hold. (Thus Exercise 1.1c) is an instance of a result in which commutativity is essential.) Nevertheless this is enough to deduce that in any ring the units $R^\times$ form a group...which is not necessarily commutative.*

Example (Zero ring): Our rings come with two distinguished elements, the additive identity 0 and the multiplicative identity 1. Suppose that $0 = 1$. Then for $x \in R$, $x = 1 \cdot x = 0 \cdot x$, whereas in any rin g $0 \cdot x = (0 + 0) \cdot x = 0 \cdot x + 0 \cdot x$, so $0 \cdot x = 0$. In other words, if $0 = 1$, then this is the only element in the ring. It is clear that for any one element set $R = \{0\}$, $0 + 0 = 0 \cdot 0 = 0$ endows R with the structure of

a ring. We call this ring the **zero ring**.

The zero ring exhibits some strange behavior, such that it must be explicitly excluded in many results. For instance, the zero element is a unit in the zero ring, which is obviously not the case in any nonzero ring. A nonzero ring in which every nonzero element is a unit is called a **division ring**. A commutative division ring is called a **field**.

Let R and S be rings (with unity). A **homomorphism** $f : R \to S$ is a map of sets which satisfies

(HOM1) For all $x, y \in R$, $f(x + y) = f(x) + f(y)$.
(HOM2) For all $x, y \in R$, $f(xy) = f(x)f(y)$.
(HOM3) $f(1) = 1$.

Note that (HOM1) implies $f(0) = f(0 + 0) = f(0) + f(0)$, so $f(0) = 0$. Thus we do not need to explcitly include $f(0) = 0$ in the definition of a group homomorphism. For the multiplicative identity however, this argument only shows that if $f(1)$ is a unit, then $f(1) = 1$. Therefore, if we did not require (HOM3), then for instance the map $f : R \to R$, $f(x) = 0$ for all x, would be a homomorphism, and we do not want this.

Exercise 1.2: Suppose R and S are rings, and let $f : R \to S$ be a map satisfying (HOM1) and (HOM2). Show that f is a homomorphism of rings (i.e., satisfies also $f(1) = 1$) iff $f(1) \in S^\times$.

A homomorphism $f : R \to S$ is an **isomorphism** if there exists a homomorphism $g : S \to R$ such that: for all $x \in R$, $g(f(x)) = x$; and for all $y \in S$, $f(g(y)) = y$.

Exercise 1.3: Let $f : R \to S$ be a homomorphism of rings. Show TFAE:
(i) f is a bijection.
(ii) f is an isomorphism.

Remark: In many algebra texts, an isomorphism of rings (or groups, etc.) is *defined* to be a bijective homomorphism, but this gives the wrong idea of what an isomorphism should be in other mathematical contexts (e.g. for topological spaces). Rather, having defined the notion of a morphism of any kind, one defines isomorphism in the way we have above.

Exercise 1.4: a) Suppose R and S are both rings on a set containing exactly one element. Show that there is a unique ring isomorphism from R to S. (This is a triviality, but explains why are we able to speak of **the zero ring**, rather than simply the zero ring associated to one element set. We will therefore denote the zero ring just by 0.)
b) Show that any ring R admits a unique homomorphism to the zero ring. One says that the zero ring is **the final object** in the category of rings.

Exercise 1.5: Show that for a not-necessarily-commutative-ring S there exists a

unique homomorphism from the ring $\mathbb{Z}$ of integers to S. (Thus $\mathbb{Z}$ is the **initial object** in the category of not-necessarily-commutative-rings. It follows immediately that it is also the initial object in the category of rings.)

A **subring** R of a ring S is a subset R of S such that

(SR1) $1 \in R$.
(SR2) For all $r, s \in R$, $r + s \in R$, $r - s \in R$, and $rs \in R$.

Here (SR2) expresses that the subset R is an algebra under the operations of addition and multiplication defined on S. Working, as we are, with rings with unity, we have to be a bit more careful: in the presence of (SR2) but not (SR1) it is possible that R *either* does not have a multiplicative identity or, more subtly, that it has a multiplicative identity which is not the element $1 \in S$.

An example of the first phenomenon is $S = \mathbb{Z}$, $R = 2\mathbb{Z}$. An example of the second is $S = \mathbb{Z}$, $R = 0$. A more interesting example is $S = \mathbb{Z} \times \mathbb{Z}$ – i.e., the set of all ordered pairs (x, y), $x, y \in \mathbb{Z}$ with $(x_1, y_1) + (x_2, y_2) = (x_1 + x_2, y_1 + y_2)$, $(x_1, y_1) \cdot (x_2, y_2) = (x_1 x_2, y_1 y_2)$ – and $R = \{(0, y) \mid y \in \mathbb{Z}\}$. Then with the induced addition and multiplication from S, R is isomorphic to the ring $\mathbb{Z}$ and the element $(0, 1)$ serves as a multiplicative identity on R which is different from the (always unique) multiplicative identity $1_S = (1, 1)$, so according to our conventions R is not a subring of S.

Notice that if R is a subring of S, the inclusion map $R \hookrightarrow S$ is an injective homomorphism of rings. Conversely, if $\iota : R \hookrightarrow S$ is an injective ring homomorphism, then $R \cong \iota(R)$ and $\iota(R)$ is a subring of S, so essentially we may use ι to view R as a subring of S. The only proviso here is that this certainly depends on ι: in general there may be other injective homomorphisms $\iota : R \hookrightarrow S$ which realize R as a different subset of S, hence a different subring.

1.2. **Adjoining elements.**

Let $\iota : R \hookrightarrow S$ be an injective ring homomorphism. As above, let us use ι to view R as a subring of S; we also say that S is an **extension ring** of R and write S/R for this (note: this has nothing to do with cosets or quotients!) We wish now to consider rings T such that $R \subset T \subset S$; such a ring T might be called a **subextension** of S/R or an **intermediate ring**.

Let $X = \{x_i\}$ be a subset of S. Then the partially ordered set of all subrings of T containing R and X contains a bottom element, given (as usual!) by taking the intersection of all of its elements. (This partially ordered set is nonempty, since S is in it.) We call this the ring obtained by **adjoining** the elements of X to R. In the commutative case, we denote this ring by $R[\{x_i\}]$, for reasons that will become more clear when we discuss polynomial rings in §5.4.

Example: Take $R = \mathbb{Z}$, $S = \mathbb{C}$. Then $\mathbb{Z}[i] = \mathbb{Z}[\sqrt{-1}]$ is the smallest subring of $\mathbb{C}$ containing ($\mathbb{Z}$ and) $\sqrt{-1}$.

Example: Take $R = \mathbb{Z}$, $S = \mathbb{Q}$, let $\mathcal{P}$ be any set of prime numbers, and put $X = \{\frac{1}{p}\}_{p\in\mathcal{P}}$. Then there is a subring $\mathbb{Z}_{\mathcal{P}} := \mathbb{Z}[\{\frac{1}{p}\}_{p\in\mathcal{P}}]$ of $\mathbb{Q}$.

Exercise 1.6: Let $\mathcal{P}$, $\mathcal{Q}$ be two sets of prime numbers. Show TFAE:
(i) $\mathbb{Z}_{\mathcal{P}} \cong \mathbb{Z}_{\mathcal{Q}}$.
(ii) $\mathbb{Z}_{\mathcal{P}} = \mathbb{Z}_{\mathcal{Q}}$.
(iii) $\mathcal{P} = \mathcal{Q}$.

Exercise 1.7: Show that every subring of $\mathbb{Q}$ is of the form $\mathbb{Z}_{\mathcal{P}}$ for some $\mathcal{P}$.

The adjunction process $R \mapsto R[X]$ is defined only relative to some extension ring S of R, although the notation hides this. In fact, one of the recurrent themes of the subject is the expression of the adjunction process in a way which depends only on R itself. In the first example, this is achieved by identifying $\sqrt{-1}$ with its minimal polynomial $t^2 + 1$ and replacing $\mathbb{Z}[\sqrt{-1}]$ with the quotient ring $\mathbb{Z}[t]/(t^2 + 1)$. The second example will eventually be turned around: we will be able to give an independent definition of $\mathbb{Z}_{\mathcal{P}}$ as a certain "ring of fractions" formed from $\mathbb{Z}$ and then $\mathbb{Q}$ will be the ring of fractions obtained by taking $\mathcal{P}$ to be the set of all prime numbers.

Nevertheless, the existence of such turnabouts should not cause us to forget that adjunction is relative to an extension; indeed forgetting this can lead to serious trouble. For instance, if $\sqrt[3]{2}$ is the unique real cube root of 2 and ζ_3 is a primitive cube root of unity, then the three complex numbers with cube 2 are $z_1 = \sqrt[3]{2}$, $z_2 = \sqrt[3]{2}\zeta_3$ and $z_3 = \sqrt[3]{2}\zeta_3^2$. Each of the rings $\mathbb{Q}[z_1]$, $\mathbb{Q}[z_2]$, $\mathbb{Q}[z_3]$ is isomorphic to the ring $\mathbb{Q}[t]/(t^3 - 2)$, so all three are isomorphic to each other. But they are not *the same* ring: on the one hand $\mathbb{Q}[z_1]$ is contained in $\mathbb{R}$ and the other two are not. More seriously $\mathbb{Q}[z_1, z_2, z_3] = \mathbb{Q}[\sqrt[3]{2}, \zeta_3]$, which strictly contains any one of $\mathbb{Q}[z_1]$, $\mathbb{Q}[z_2]$ and $\mathbb{Q}[z_3]$.

1.3. **Ideals and quotient rings.**

Let $f : R \to S$ be a homomorphism of rings, and put

$$I = f^{-1}(0) = \{x \in R \mid f(x) = 0\}.$$

Then, since f is in particular a homomorphism of commutative groups $(R, +) \to (S, +)$, I is a subgroup of $(R, +)$. Moreover, it enjoys both of the following properties:

(LI) For all $i \in I$ and $y \in R$, $iy \in I$.
(RI) For all $j \in I$ and $x \in R$, $xj \in I$.

Indeed,

$$f(xj) = f(x)f(j) = f(x) \cdot 0 = 0 = 0 \cdot f(y) = f(i)f(y) = f(iy).$$

In general, let R be a ring. An **ideal** is a subset $I \subset R$ which is a subgroup of $(R, +)$ (in particular, $0 \in I$) and which satisfies (LI) and (RI).

Theorem 1.1. *Let R be a ring, and let I be a subgroup of $(R, +)$. TFAE:*
(i) I is an ideal of R.
(ii) There exists a ring structure on the quotient group R/I making the additive

homomorphism $R \to R/I$ into a homomorphism of rings.
When these conditions hold, the ring structure on R/I in (ii) is unique, and R/I is called the quotient of R by the ideal I.

Proof. Consider the group homomorphism $q : R \to R/I$. If we wish R/I to be a ring in such a way so that q is a ring homomorphism, we need

$$(x + I)(y + I) = q(x)q(y) = q(xy) = (xy + I).$$

This shows that there is only one possible ring structure, and the only question is whether it is well-defined. For this we need that for all $i, j \in I$, $(x+i)(y+j)-xy = xj+iy+ij \in I$. Evidently this holds for all x, y, i, j iff (LI) and (RI) both hold. □

Remark: If R is commutative, then of course there is no difference between (LI) and (RI). For a non-commutative ring R, an additive subgroup I satisfying condition (LI) but not necessarily (RI) (resp. (RI) but not necessarily (LI)) is called a **left ideal** (resp. a **right ideal**). Often one says **two-sided ideal** to emphasize that (LI) and (RI) both hold. Much of the additional complexity of the non-commutative theory comes from the need to distinguish between left, right and two-sided ideals.

We do not wish to discuss such complexities here, so henceforth in this section we assume (except in exercises, when indicated) that our rings are commutative.

Example: In $R = \mathbb{Z}$, for any integer n, consider the subset $(n) = n\mathbb{Z} = \{nx \mid x \in \mathbb{Z}\}$ of all multiples of n. This is easily seen to be an ideal.[2] The quotient $\mathbb{Z}/n\mathbb{Z}$ is the ring of integers modulo n.

An ideal $I \subsetneq R$ is called **proper**.

Exercise 1.8: Let R be a ring and I an ideal of R. Show that TFAE:
(i) $I \cap R^\times \neq \emptyset$.
(ii) $I = R$.

Exercise 1.9: a) Let R be a commutative ring. Show that R is a field iff R has exactly two ideals, 0 and R.
b) Let R be a not necessarily commutative ring. Show that TFAE: (i) The only one-sided ideals of R are 0 and R. (ii) R is a division ring.
c) For a field k and an integer $n > 1$, show that the matrix ring $M_n(k)$ has no two-sided ideals but is not a division ring.

Exercise 1.10: Some contemporary undergraduate algebra texts define the finite ring $\mathbb{Z}/n\mathbb{Z}$ in a different and apparently simpler way: put $Z_n = \{0, 1, \ldots, n-1\}$. For any integer x, there is a unique integer k such that $x - kn \in Z_n$. Define a function $\mod n : \mathbb{Z} \to Z_n$ by $\mod n(x) := x - kn$. We then define $+$ and $\cdot$ on Z_n by $x + y := \mod n(x+y)$, $xy = \mod n(xy)$. Thus we have avoided any mention of ideals, equivalence classes, quotients, etc. Is this actually simpler? (Hint: how do we know that Z_n satisfies the ring axioms?)

For any commutative ring R and any element $y \in R$, the subset $(y) = yR =$

[2] If this is not known and/or obvious to the reader, these notes will probably be too brisk.

$\{xy \mid x \in R\}$ is an ideal of R. Such ideals are called **principal**. A **principal ideal ring** is a commutative ring in which each ideal is principal.

Exercise 1.11: a) The intersection of any family of (left, right or two-sided) ideals in a not-necessarily-commutative-ring is a (left, right or two-sided) ideal.
b) Let $\{I_i\}$ be a set of ideals in the commutative ring R. Show that $\bigcap_i I_i$ has the following property: for any ideal J of R such that $J \subset I_i$ for all i, $J \subset \bigcap_i I$.

Let R be a ring and S a subset of R. There is then a smallest ideal of R containing S, namely $\bigcap I_i$, where I_i are all the ideals of R containing S. We call this the ideal **generated** by S. This is a "top-down" description; as usual, there is a complementary "bottom-up" description which is not quite as clean but often more useful. Namely, put

$$\langle S \rangle := \{\sum r_i s_i \mid r_i \in R, s_i \in S\}$$

i.e., the set of all finite sums of an element of R times an element of S.

Proposition 1.2. *For a subset S of a commutative ring R, $\langle S \rangle$ is an ideal, the intersection of all ideals containing S.*

Exercise 1.12: Prove Proposition 1.2.

When S is a subset of R such that $I = \langle S \rangle$, we say S is a **set of generators** for I. In general the same ideal will have many (most often infinitely many) sets of generators.

An ideal I is **principal** if it can be generated by a single element. In any ring, the zero ideal $0 = \langle 0 \rangle$ and the entire ring $R = \langle 1 \rangle$ are principal. For $x \in \mathbb{R}$, we tend to denote the principal ideal generated by x as either Rx or (x) rather than $\langle x \rangle$.

An ideal I is **finitely generated** if...it admits a finite set of generators.[3]

Stop and think for a moment: do you know an example of an ideal which is *not* finitely generated? You may well find that you do not. It turns out that there is a very large class of rings – including most or all of the rings you are likely to meet in undergraduate algebra – for which every ideal is finitely generated. A ring R in which every ideal is finitely generated is called **Noetherian**. This is probably the single most important class of rings, as we will come to appreciate slowly but surely over the course of these notes.

Exercise 1.13: Let R be a ring.
a) For ideals I and J of R, define $I + J = \{i + j \mid i \in I,\ j \in J\}$. Show that $I + J = \langle I \cup J \rangle$ is the smallest ideal containing both I and J.
b) Extend part a) to any finite number of ideals $I_1, \ldots, I_n$.
c) Suppose $\{I_i\}$ is a set of ideals of I. Give an explicit description of the ideal $\langle I_i \rangle$.

Remark: The preceding considerations show that the collection of all ideals of a commutative ring R, partially ordered by inclusion, form a **complete lattice**.

[3]Well, obviously. Nevertheless this definition is so critically important that it would have been a disservice to omit it.

If I is an ideal in the ring R, then there is a correspondence between ideals J of R containing I and ideals of the quotient ring R/I, exactly as in the case of a normal subgroup of a group:

Theorem 1.3. *(Correspondence theorem) Let I be an ideal of a ring R, and denote the quotient map $R \to R/I$ by q. Let $\mathcal{I}(R)$ be the lattice of ideals of R, $\mathcal{I}_I(R)$ be the sublattice of ideals containing I and $\mathcal{I}(R/I)$ the lattice of ideals of the quotient ring R/I. Define maps*

$$\Phi : \mathcal{I}(R) \to \mathcal{I}(R/I),\ J \mapsto (I+J)/I,$$

$$\Psi : \mathcal{I}(R/I) \to \mathcal{I}(R),\ J \mapsto q^{-1}(J).$$

Then $\Psi \circ \Phi(J) = I + J$ and $\Phi \circ \Psi(J) = J$. In particular Ψ induces an isomorphism of lattices from $\mathcal{I}(R/I)$ to $\mathcal{I}_I(R)$.

Proof. For all the abstraction, the proof is almost trivial. For $J \in \mathcal{I}(R)$, we check that $\Psi(\Phi(J)) = \Psi(J + I \pmod I) = \{x \in R \mid x + I \in J + I\} = J + I \in \mathcal{I}_I(R)$. Similarly, for $J \in \mathcal{I}(R/I)$, we have $\Phi(\Psi(J)) = J$. □

Remark: In fancier language, the pair (Φ, Ψ) give an **isotone Galois connection** between the partially ordered sets $\mathcal{I}(R)$ and $\mathcal{I}(R/I)$. The associated closure operator $\Phi \circ \Psi$ on $\mathcal{I}(R/I)$ is the identity, whereas the closure operator $\Psi \circ \Phi$ on $\mathcal{I}(R)$ carries each ideal J to the smallest ideal containing both J and I.[4]

The Correspondence Theorem will be our constant companion. As is common, we will often use the map Ψ to identify the sets $\mathcal{I}(R/I)$ and $\mathcal{I}_I(R)$.

Exercise 1.14: Let I be an ideal of R and $\{J_i\}$ be a set of ideals of R. Show that Φ preserves suprema and Ψ preserves infima:

$$\Phi(\langle J_i \rangle) = \langle \Phi(J_i) \rangle$$

and

$$\Psi(\bigcap J_i) = \bigcap \Psi(J_i).$$

1.4. **The monoid of ideals of R.**

Let I and J be ideals of the ring R. The **product ideal** IJ is the least ideal containing all elements of the form xy for $x \in I$ and $y \in J$. (It is easy to see that $IJ = \{\sum x_i y_i \mid x_i \in I,\ y_i \in J\}$ is precisely the set of all finite sums of such products.) Recall that we have written $\mathcal{I}(R)$ for the lattice of all ideals of R. Then $(I, J) \mapsto IJ$ gives a binary operation on $\mathcal{I}(R)$, the **ideal product**.

Exercise 1.15: Show that $\mathcal{I}(R)$ under the ideal product is a commutative monoid, with identity element R and absorbing element the (0) ideal of R.[5]

If you are given a commutative monoid M, then invariably the property you are hoping it has is **cancellation**: for all $x, y, z \in M$, $xz = yz \implies x = y$.[6] For

[4] This point of view will be explored in more detail in §2.

[5] An element z of a monoid M is called **absorbing** if for all $x \in M$, $zx = xz = z$.

[6] Well, obviously this is an exaggeration, but you would be surprised how often it is true.

example, if R is a ring, then the set $R^\bullet$ of nonzero elements of R is cancellative iff R is a domain. Note that 0 is an absorbing element of $(R, \cdot)$, which we have removed in order to have any chance at cancellativity.

Exercise 1.16:
a) Let M be a cancellative monoid of cardinality greater than one. Show that M does not have any absorbing elements.
b) Let R be a ring which is not the zero ring. Show that the monoid $\mathcal{I}(R)$ is not cancellative.

In light of the previous exercise, for a domain R we define $\mathcal{I}^\bullet(R)$ to be the monoid of *nonzero ideals* of R under multiplication.

Warning: Just because R is a domain, $\mathcal{I}^\bullet(R)$ need not be cancellative!

Exercise 1.17: Let $R = \mathbb{Z}[\sqrt{-3}]$, and let $\mathfrak{p}_2 = \langle 1 + \sqrt{-3}, 1 - \sqrt{-3} \rangle$ (i.e., the ideal generated by these two elements.
a) Show that $\#R/(2) = 4$ and $R/\mathfrak{p}_2 \cong \mathbb{Z}/2\mathbb{Z}$.
b) Show that $\mathfrak{p}_2^2 = \mathfrak{p}_2 \cdot (2)$.
c) Conclude that $\mathcal{I}^\bullet(R)$ is *not* cancellative.

Exercise 1.18: Let R be a PID. Show that $\mathcal{I}^\bullet(R)$ is cancellative.

Exercise 1.19: Show that for a commutative monoid M, TFAE:
(i) M is cancellative.
(ii) There exists a commutative group G and an injective monoid homomorphism $\iota : M \hookrightarrow G$.

Exercise 1.20: Let M be a commutative monoid. A **group completion** of M consists of a commutative group $G(M)$ and a monoid homomorphism $F : M \to G(M)$ which is *universal* for monoid homomorphisms into a commutative group. That is, for any commutative group G and monoid homomorphism $f : M \to G$, there exists a unique homomorphism of groups $q : G \to G(M)$ such that $F = q \circ f$.
a) Show that any two group completions are isomorphic.
b) Show that any commutative monoid has a group completion.
c) Show that a commutative monoid injects into its group completion iff it is cancellative.

1.5. **Pushing and pulling ideals.**

Let $f : R \to S$ be a homomorphism of commutative rings. We can use f to transport ideals from R to S and also to transport ideals from S to R.

More precisely, for I an ideal of R, consider $f(I)$ as a subset of S.

Exercise 1.21: Give an example to show that $f(I)$ need not be an ideal of S.

Nevertheless we can consider the ideal it generates: we define

$$f_*(I) = \langle f(I) \rangle,$$

and we call $f_*(I)$ the **pushforward of I to S**.

Similarly, let J be an ideal of S, and consider its complete preimage in R, i.e., $f^{-1}(J) = \{x \in R \mid f(x) \in J\}$. As you are probably already aware, preimages have much nicer algebraic properties than direct images, and indeed $f^{-1}(J)$ is necessarily an ideal of R. We denote it by $f^*(J)$ and call it the **pullback of J to R**.

Example: Suppose that I is an ideal of R, $S = R/I$ and $f : R \to R/I$ is the quotient map. In this case, pushforwards and pullbacks were studied in detail in Theorem 1.3. In this case $f^* : \mathcal{I}(S) \hookrightarrow \mathcal{I}(R)$ is an injection, which allows us to view the lattice of ideals of S as a sublattice of the lattice of ideals of R. Moreover we have a **push-pull formula**: for all ideals J of R,

$$f^* f_* J = J + I$$

and also a **pull-push formula**: for all ideals J of R/I,

$$f_* f^* J = J.$$

These formulas are extremely useful at all points in the study of ring theory. More generally, whenever one meets a homomorphism $f : R \to S$ of rings (or better, a certain class of homomorphisms), it is fruitful to ask about properties of f_* and f^*: in particular, is f^* necessarily injective, or surjective? Can we identify the composite maps $f^* f_*$ and/or $f_* f^*$?

In these notes, the most satisfying and important answers will come for **localizations** and **integral extensions**.

1.6. **Maximal and prime ideals.**

An ideal $\mathfrak{m}$ of R is **maximal** if it is proper and there is no proper ideal of R strictly containing $\mathfrak{m}$. An ideal $\mathfrak{p}$ of R is **prime** if for all $x, y \in R$, $xy \in \mathfrak{p}$ implies $x \in \mathfrak{p}$ or $y \in \mathfrak{p}$ or both.

Exercise 1.22: For an ideal I in a ring R, show that TFAE:
(i) I is maximal.
(ii) R/I is a field.

Exercise 1.23: For an ideal I in a ring R, show that TFAE:
(i) I is prime.
(ii) $R/\mathfrak{p}$ is an integral domain.

Exercise 1.24: Show that any maximal ideal is prime.

Exercise 1.25: Let $f : R \to S$ be a homomorphism of rings.
a) Let I be a prime ideal of R. Show that $f_* I$ need *not* be a prime ideal of S.
b) Let J be a prime ideal of S. Show that $f^* J$ is a prime ideal of R.
c) Let J be a maximal ideal of S. Show that $f^* J$ need *not* be maximal in R.

If I and J are ideals of a ring R, we define the **colon ideal**[7]

$$(I : J) = \{x \in R \mid xJ \subset I\}.$$

Exercise 1.26: Show that $(I : J)$ is indeed an ideal of R.

1.7. **Products of rings.**

Let R_1 and R_2 be rings. The Cartesian product $R_1 \times R_2$ has the structure of a ring with "componentwise" addition and multiplication:

$$(r_1, r_2) + (s_1, s_2) := (r_1 + s_1, r_2 + s_2).$$
$$(r_1, r_2) \cdot (s_1, s_2) := (r_1 s_1, r_2 s_2).$$

Exercise 1.27:
a) Show that $R_1 \times R_2$ is commutative iff both R_1 and R_2 are commutative.
b) $R_1 \times R_2$ has an identity iff both R_1 and R_2 do, in which case $e := (e_1, e_2)$ is the identity of $R_1 \times R_2$.

As for any Cartesian product, $R_1 \times R_2$ comes equipped with its projections

$$\pi_1 : R_1 \times R_2 \to R_1, \mid (r_1, r_2) \mapsto r_1$$
$$\pi_2 : R_1 \times R_2 \to R_2, \mid (r_1, r_2) \mapsto r_2.$$

The Cartesian product $X_1 \times X_2$ of sets X_1 and X_2 satisfies the following universal property: for any set Z and any maps $f_1 : Z \to X_1$, $f_2 : Z \to X_2$, there exists a unique map $f : Z \to X_1 \times X_2$ such that $f_1 = \pi_1 \circ f$, $f_2 = \pi_2 \circ f$. The Cartesian product $R_1 \times R_2$ satisfies the analogous universal property in the category of rings:

Exercise 1.28: For rings R_1, R_2, S and ring homomorphisms $f_i : S \to R_i$, there exists a unique homomorphism of rings $f : S \to R_1 \times R_2$ such that $f_i = \pi_i \circ f$.

So the Cartesian product of R_1 and R_2 is also the product in the categorical sense.

As with sets, we can equally well take the Cartesian product over an arbitrary indexed family of rings: if $\{R_i\}_{i \in I}$ is a family of rings, their Cartesian product $\prod_{i \in I} R_i$ becomes a ring under coordinatewise addition and multiplication, and satisfies the universal property of the product. Details are left to the reader.

It is natural to ask whether the category of rings has a direct sum as well. In other words, given rings R_1 and R_2 we are looking for a ring R together with ring homomorphisms $\iota_i : R_i \to R$ such that for any ring S and homomorphisms $f_i : R_i \to S$, there exists a unique homomorphism $f : R \to S$ such that $f_i = f \circ \iota_i$. We recall that in the category of abelian groups, the Cartesian product group $G_1 \times G_2$ also the categorical direct sum, with $\iota_1 : g \mapsto (g, 0)$ and $\iota_2 : g \mapsto (0, g)$. Since each ring has in particular the structure of an abelian group, it is natural to wonder whether the same might hold true for rings. However, the map $\iota_1 : R_1 \to R_1 \times R_2$ does not

[7]The terminology is unpleasant and is generally avoided as much as possible. One should think of $(I : J)$ as being something like the "ideal quotient" I/J (which of course has no formal meaning). Its uses will gradually become clear.

preserve the multiplicative identity (unless $R_2 = 0$), so is not a homomorphism of rings when identities are present. Moreover, even in the category of algebras, in order to satisfy the universal property on the underlying additive subgroups, the homomorphism f is uniquely determined to be $(r_1, r_2) \mapsto f_1(r_1) + f_2(r_2)$, and it is easily checked that this generally does not preserve the product.

We will see later that the category of rings *does* have direct sums in the categorical sense: the categorical direct sum of R_1 and R_2 is given by the tensor product $R_1 \otimes_{\mathbb{Z}} R_2$.

Now returning to the case of commutative rings, let us consider the ideal structure of the product $R = R_1 \times R_2$. If I_1 is an ideal of R_1, then $I_1 \times \{0\} = \{(i, 0) \mid i \in I\}$ is an ideal of the product; moreover the quotient R/I_1 is isomorphic to $R_1/I_1 \times R_2$. Similarly, if I_2 is an ideal, $\{0\} \times I_2$ is an ideal of R_2. Finally, if I_1 is an ideal of R_1 and I_2 is an ideal of R_2, then

$$I_1 \times I_2 := \{(i_1, i_2) \mid i_1 \in I_1,\ i_2 \in I_2\}$$

is an ideal of R. In fact we have already found all the ideals of the product ring:

Proposition 1.4. *Let R_1 and R_2 be commutative rings, and let I be an ideal of $R := R_1 \times R_2$. Put*

$$I_1 := \{r_1 \in R_1 \mid \exists r_2 \in R_2 \mid (r_1, r_2) \in I\},$$
$$I_2 := \{r_2 \in R_2 \mid \exists r_1 \in R_1 \mid (r_1, r_2) \in I\}.$$

Then $I = I_1 \times I_2 = \{(i_1, i_2) \mid i_1 \in I_1,\ i_2 \in I_2\}$.

Proof. Observe first that $I_1 \times \{0\}$ and $\{0\} \times I_2$ are ideals of R contained in I. Indeed, if $i_1 \in I_1$, then $(i_1, r_2) \in I$ for some r_2 and then $(i_1, 0) = (i_1, r_2) \cdot (1, 0)$, and similarly for I_2. Therefore

$$I_1 \times I_2 = (I_1 \times \{0\}) + (\{0\} \times I_2) \subset I.$$

Conversely, if $(x, y) \in I$, then

$$(x, y) = (x, 0)(1, 0) + (0, y)(0, 1) \in I_1 \times I_2.$$

□

Remark: Another way to express the result is that, corresponding to a decomposition $R = R_1 \times R_2$, we get a decomposition $\mathcal{I}(R) = \mathcal{I}(R_1) \times \mathcal{I}(R_2)$.

Let us call a commutative ring R **disconnected** if there exists nonzero rings R_1, R_2 such that $R \cong R_1 \times R_2$, and **connected** otherwise.[8] If R is disconnected, then choosing such an isomorphism φ, we may put $I_1 = \varphi^{-1}(R_1 \times \{0\})$ and $I_2 = \varphi^{-1}(\{0\} \times R_2)$. Evidently I_1 and I_2 are ideals of R such that $I_1 \cap I_2 = \{0\}$ and $I_1 \times I_2 = R$. Conversely, if in a ring R we can find a pair of ideals I_1, I_2 with these properties then it will follow from the Chinese Remainder Theorem (Theorem 4.18) that the natural map $\Phi : R \to R/I_2 \times R/I_1$, $r \mapsto (r + I_2, r + I_1)$ is an isomorphism.

Now Φ restricted to I_1 induces an isomorphism of groups onto R/I_2 (and similarly

[8]We will see later that there is a topological space $\operatorname{Spec} R$ associated to every ring, such that $\operatorname{Spec} R$ is disconnected in the usual topological sense iff R can be written as a nontrivial product of rings

with the roles of I_1 and I_2 reversed). We therefore have a distinguished element of I_1, $e_1 := \Phi^{-1}(1)$. This element e_1 is an identity for the multiplication on R restricted to I_1; in particular $e_1^2 = e_1$; such an element is called an **idempotent**. In any ring the elements 0 and 1 are idempotents, called trivial; since $e_1 = \Phi^{-1}(1,0)$ – and not the preimage of $(0,0)$ or of $(1,1)$ – e_1 is a **nontrivial idempotent**. Thus a nontrivial decomposition of a ring implies the presence of nontrivial idempotents.

The converse is also true:

Proposition 1.5. *Suppose R is a ring and e is a nontrivial idempotent element of R: $e^2 = e$ but $e \neq 0, 1$. Put $I_1 = Re$ and $I_2 = R(1-e)$. Then I_1 and I_2 are ideals of R such that $I_1 \cap I_2 = 0$ and $R = I_1 + I_2$, and therefore $R \cong R/I_1 \times R/I_2$ is a nontrivial decomposition of R.*

Exercise 1.29: Prove Proposition 1.5.

Exercise 1.30: Generalize the preceding discussion to decompositions into a finite number of factors: $R = R_1 \times \cdots \times R_n$.

1.8. **A cheatsheet.**

Let R be a commutative ring. Here are some terms that we will analyze in loving detail later, but would like to be able to mention in passing whenever necessary.

R is an **integral domain** if $xy = 0 \implies x = 0$ or $y = 0$.

An ideal $\mathfrak{p}$ of R is **prime** if the quotient ring $R/\mathfrak{p}$ is an integral domain. Equivalently, $\mathfrak{p}$ is an ideal such that $xy \in \mathfrak{p} \implies x \in \mathfrak{p}$ or $y \in \mathfrak{p}$.

An ideal $\mathfrak{m}$ of R is **maximal** if it is proper – i.e., not R itself – and not strictly contained in any larger proper ideal. Equivalently, $\mathfrak{m}$ is an ideal such that the quotient ring $R/\mathfrak{m}$ is a field.

R is **Noetherian** if it satisfies any of the following equivalent conditions:[9]
(i) For any nonempty set S of ideals of R, there exists $I \in S$ which is not properly contained in any $J \in S$.
(ii) There is no infinite sequence of ideals $I_1 \subsetneq I_2 \subsetneq \dots$ in R.
(iii) Every ideal of R is finitely generated.

R is **Artinian** (or sometimes, an **Artin ring**) if the partially ordered set of ideals of R satisfies the descending chain condition: there is no infinite sequence of ideals $I_1 \supsetneq I_2 \supsetneq \dots$.

If I and J are ideals of a ring R, we define the **colon ideal**[10]

$$(I : J) = \{x \in R \mid xJ \subset I\}.$$

[9]See Theorem 8.22 for a proof of their equivalence.

[10]The terminology is unpleasant and is generally avoided as much as possible. One should think of $(I : J)$ as being something like the "ideal quotient" I/J (which of course has no formal meaning). Its uses will gradually become clear.

$(I : J)$ is also an ideal.

Let $R \subset S$ be an inclusion of rings. We say that $s \in S$ is **integral over R** if there are $a_0, \ldots, a_{n-1} \in R$ such that

$$s^n + a_{n-1}s^{n-1} + \ldots + a_1 s + a_0 = 0.$$

We say that **S is integral over R** if every element of S is integral over R. This is the appropriate generalization to rings of the notion of an algebraic field extension. We will study integral elements and extensions, um, extensively in § 14, but there is one easy result that we will need earlier, so we give it now.

Proposition 1.6. *Let $R \subset S$ be an integral extension of integral domains. If S is a field then R is a field.*

Proof. Let $\alpha \in R^\bullet$. Then $\alpha^{-1} \in S$ is integral over R: there exist $a_i \in R$ such that

$$\alpha^{-n} = a_{n-1}\alpha^{-n+1} + \ldots + a_1\alpha^{-1} + a_0.$$

Multiplying through by α^{n-1} gives

$$\alpha^{-1} = a_{n-1} + a_{n-2}\alpha + \ldots + a_1\alpha^{n-2} + a_0\alpha^{n-1} \in R.$$

□

2. Galois Connections

2.1. **The basic formalism.**

Let $(X, \leq)$ and $(Y, \leq)$ be partially ordered sets. A map $f : X \to Y$ is **isotone** (or **order-preserving**) if for all $x_1, x_2 \in X$, $x_1 \leq x_2 \implies f(x_1) \leq f(x_2)$. A map $f : X \to Y$ is **antitone** (or **order-reversing**) if for all $x_1, x_2 \in X$, $x_1 \leq x_2 \implies f(x_1) \geq f(x_2)$.

Exercise 2.1: Let X, Y, Z be partially ordered sets, and let $f : X \to Y$, $g : Y \to Z$ be functions. Show:
a) If f and g are isotone, then $g \circ f$ is isotone.
b) If f and g are antitone, then $g \circ f$ is isotone.
c) If one of f and g is isotone and the other is antitone, then $g \circ f$ is antitone.

Let $(X, \leq)$ and $(Y, \leq)$ be partially ordered sets. An **antitone Galois connection between X and Y** is a pair of maps $\Phi : X \to Y$ and $\Psi : Y \to X$ such that:

(GC1) Φ and Ψ are both antitone maps, and
(GC2) For all $x \in X$ and all $y \in Y$, $x \leq \Psi(y) \iff y \leq \Phi(x)$.

There is a pleasant symmetry in the definition: if (Φ, Ψ) is a Galois connection between X and Y, then (Ψ, Φ) is a Galois connection between Y and X.

If $(X, \leq)$ is a partially ordered set, then a mapping $f : X \to X$ is called a **closure operator** if it satisfies all of the following properties:

(C1) For all $x \in X$, $x \leq f(x)$.

(C2) For all $x_1, x_2 \in X$, $x_1 \leq x_2 \implies f(x_1) \leq f(x_2)$.
(C3) For all $x \in X$, $f(f(x)) = f(x)$.

Proposition 2.1. *The mapping $\Psi \circ \Phi$ is a closure operator on $(X, \leq)$ and the mapping $\Phi \circ \Psi$ is a closure operator on $(Y, \leq)$.*

Proof. By symmetry, it is enough to consider the mapping $x \mapsto \Psi(\Phi(x))$ on X.

If $x_1 \leq x_2$, then since both Φ and Ψ are antitone, we have $\Phi(x_1) \geq \Phi(x_2)$ and thus $\Psi(\Phi(x_1)) \leq \Psi(\Phi(x_1))$: (C2).

For $x \in X$, $\Phi(x) \geq \Phi(x)$, and by (GC2) this implies $x \leq \Psi(\Phi(x))$: (C1).

Finally, for $x \in X$, applying (C1) to the element $\Psi(\Phi(x))$ of X gives

$$\Psi(\Phi(x)) \leq \Psi(\Phi(\Psi(\Phi(x)))).$$

Conversely, we have

$$\Psi(\Phi(x)) \leq \Psi(\Phi(x)),$$

so by (GC2)

$$\Phi(\Psi(\Phi(x)) \geq \Phi(x),$$

and applying the order-reversing map Ψ gives

$$\Psi(\Phi(\Psi(\Phi(x)))) \leq \Psi(\Phi(x)).$$

Thus

$$\Psi(\Phi(x)) = \Psi(\Phi(\Psi(\Phi(x))).$$

□

Corollary 2.2. *The following **tridempotence** properties are satisfied by Φ and Ψ:*
a) For all $x \in X$, $\Phi\Psi\Phi x = \Phi x$.
b) For all $y \in X$, $\Psi\Phi\Psi y = \Psi y$.

Proof. By symmetry, it suffices to prove a). Since $\Phi \circ \Psi$ is a closure operator, $\Phi\Psi\Phi x \geq \Phi x$. Moreover, since $\Psi \circ \Phi$ is a closure operator, $\Psi\Phi x \geq x$, and since Φ is antitone, $\Phi\Psi\Phi x \leq \Phi x$. So $\Phi\Psi\Phi x = \Phi x$. □

Proposition 2.3. *Let (Φ, Ψ) be a Galois connection between partially ordered sets X and Y. Let $\overline{X} = \Psi(\Phi(X))$ and $\overline{Y} = \Psi(\Phi(Y))$.*
a) $\overline{X}$ and $\overline{Y}$ are precisely the subsets of closed elements of X and Y respectively.
b) We have $\Phi(X) \subset \overline{Y}$ and $\Psi(Y) \subset \overline{X}$.
c) $\Phi : \overline{X} \to \overline{Y}$ and $\Psi : \overline{Y} \to \overline{X}$ are mutually inverse bijections.

Proof. a) If $x = \Psi(\Phi(x))$ then $x \in \overline{X}$. Conversely, if $x \in \overline{X}$, then $x = \Psi(\Phi(x'))$ for some $x' \in X$, so $\Psi(\Phi(x))) = \Psi(\Phi(\Psi(\Phi(x')))) = \Psi(\Phi(x')) = x$, so X is closed.
b) This is just a reformulation of Corollary 2.2.
c) If $x \in \overline{X}$ and $y \in \overline{Y}$, then $\Psi(\Phi(x)) = x$ and $\Psi(\Phi(y)) = y$. □

We speak of the mutually inverse antitone bijections $\Phi : \overline{X} \to \overline{Y}$ and $\Psi : \overline{Y} \to \overline{X}$ as the **Galois correspondence** induced by the Galois connection (Φ, Ψ).

Example: Let K/F be a field extension, and G a subgroup of $\mathrm{Aut}(K/F)$. Then there is a Galois connection between the set of subextensions of K/F and the set of subgroups of G, given by

$$\Phi : L \to G_L = \{\sigma \in G \mid \sigma x = x \ \forall x \in L\},$$
$$\Psi : H \to K^H = \{x \in K \mid \sigma x = x \ \forall \sigma \in H\}.$$

Having established the basic results, we will now generally abbreviate the closure operators $\Psi \circ \Phi$ and $\Phi \circ \Psi$ to $x \mapsto \overline{x}$ and $y \mapsto \overline{y}$.

2.2. **Lattice Properties.**

Recall that a partially ordered set X is a **lattice** if for all $x_1, x_2 \in X$, there is a greatest lower bound $x_1 \wedge x_2$ and a least upper bound $x_1 \vee x_2$. A partially ordered set is a **complete lattice** if for every subset A of X, the greatest lower bound $\bigwedge A$ and the least upper bound $\bigvee A$ both exist.

Lemma 2.4. *Let (X, Y, Φ, Ψ) be a Galois connection.*
a) If X and Y are both lattices, then for all $x_1, x_2 \in X$,

$$\Phi(x_1 \wedge x_2) = \Phi(x_1) \vee \Phi(x_2),$$

$$\Phi(x_2 \vee x_2) = \Phi(x_1) \wedge \Phi(x_2).$$

b) If X and Y are both complete lattices, then for all subsets $A \subset X$,

$$\Phi(\bigwedge A) = \bigvee \Phi(A),$$

$$\Phi(\bigvee A) = \bigwedge \Phi(A).$$

Exercise 2.2: Prove Lemma 2.4.

Complete lattices also intervene in this subject in the following way.

Proposition 2.5. *Let A be a set and let $X = (2^A, \subset)$ be the power set of A, partially ordered by inclusion. Let $c : X \to X$ be a closure operator. Then the collection $c(X)$ of closed subsets of A forms a complete lattice, with $\bigwedge S = \bigcap_{B \in S} B$ and $\bigvee S = c(\bigcup_{B \in S} B)$.*

Exercise 2.3: Prove Proposition 2.5.

2.3. **Examples of Antitone Galois Connections.**

Example (Indiscretion): Let $(X, \leq)$ and $(Y, \leq)$ be posets with top elements T_X and T_Y respectively. Define $\Phi : X \to Y$, $x \mapsto T_Y$ and $\Psi : Y \to X$, $y \mapsto T_X$. Then (X, Y, Φ, Ψ) is a Galois connection. The induced closure operators are "indiscrete": they send every element of X (resp. Y) to the top element T_X (resp. T_Y).

Example (Perfection): Let $(X, \leq)$ and $(Y, \leq)$ be **anti-isomorphic posets**, i.e., suppose that there exists a bijection $\Phi : X \to Y$ with $x_1 \leq x_2 \iff \Phi(x_2) \leq \Phi(x_1)$. Then the inverse map $\Psi : Y \to X$ satisfies $y_1 \leq y_2 \iff \Psi(y_2) \leq \Psi(y_1)$. Moreover, for $x \in X$, $y \in Y$, $x \leq \Psi(y) \iff y = \Psi(\Phi(y)) \leq \Phi(x)$, so (X, Y, Φ, Ψ) is a Galois connection. Then $\overline{X} = X$ and $\overline{Y} = Y$. As we saw above, the converse also holds: if $\overline{X} = X$ and $\overline{Y} = Y$ then Φ and Ψ are mutually inverse bijections. Such a Galois connection is called **perfect**.[11]

[11]There is a small paradox here: in purely order-theoretic terms this example is not any more interesting than the previous one. But in practice given two posets it is infinitely more useful to have a pair of mutually inverse antitone maps running between them than the trivial operators of the previous example: Galois theory is a shining example! The paradox already shows up in the distinction between indiscrete spaces and discrete spaces: although neither topology looks more

The remaining examples of this section make use of some important ring-theoretic concepts which will be treated in detail later.

Example: Let R be a commutative ring. Let X be the set of all ideals of R and $Y = 2^{\operatorname{Spec} R}$ the power set of the set of prime ideals of R. For $I \in X$, put

$$\Phi(I) = V(I) = \{\mathfrak{p} \in \operatorname{Spec} R \mid I \subset \mathfrak{p}\}.$$

For $V \in Y$, put

$$\Psi(V) = \bigcap_{\mathfrak{p} \in V} \mathfrak{p}.$$

The maps Φ and Ψ are antitone, and for $I \in \mathcal{X}$, $V \in \mathcal{Y}$,

$$I \subset \Psi(V) \iff I \subset \bigcap_{\mathfrak{p} \in V} \mathfrak{p} \iff \forall \mathfrak{p} \in V, I \subset \mathfrak{p} \iff V \subset \Phi(I), \tag{1}$$

so (Φ, Ψ) is a Galois connection. Then $\overline{X}$ consists of all ideals which can be written as the intersection of a family of prime ideals. For all $I \in X$,

$$\overline{I} = \bigcap_{\mathfrak{p} \supset I} \mathfrak{p} = \operatorname{rad} I = \{x \in R \mid \exists n \in \mathbb{Z}^+ \ x^n \in I\};$$

that is, the induced closure operation on X takes any ideal to its **radical** $r(I)$. In particular $\overline{X}$ consists precisely of the radical ideals.

It is not so easy to describe the closure operator on Y or even the subset $\overline{Y}$ explicitly, but there is still something nice to say. Since:

$$V((0)) = \operatorname{Spec} R, \ V(R) = \varnothing, \tag{2}$$

$$V(I_1) \cup V(I_2) = V(I_1 I_2), \tag{3}$$

$$\bigcap_{\alpha \in A} V(I_\alpha) = V(\sum_{\alpha \in A} I_\alpha), \tag{4}$$

the elements of $\overline{Y}$ are the closed subsets for a topology, the **Zariski topology**.

Example: Take R and X as above, but now let S be any set of ideals of R and put $Y = 2^S$. For $I \in X$, put

$$\Phi(I) = V(I) = \{\mathfrak{s} \in S \mid I \subset \mathfrak{s}\}$$

and for $V \in \mathcal{Y}$, put

$$\Psi(V) = \bigcap_{\mathfrak{s} \in V} \mathfrak{s}.$$

Once again Φ and Ψ are antitone maps and (1) holds, so we get a Galois connection. The associated closure operation on X is

$$I \mapsto \overline{I} = \bigcap_{\mathfrak{s} \in S} \mathfrak{s}.$$

The relation (4) holds for any S, and the relation (2) holds so long as $R \notin S$. The verification of (2) for $R = \operatorname{Spec} R$ uses the fact that a prime ideal $\mathfrak{p}$ contains $I_1 I_2$ iff it contains I_1 or I_2, so as long as $S \subset \operatorname{Spec} S$, $\overline{Y} = \{V(I) \mid I \in X\}$ are the closed

interesting than the other, the discrete topology is natural and useful (as we shall see...) whereas the indiscrete topology entirely deserves its alternate name "trivial".

subsets for a topology on S. This is indeed the topology S inherits as a subspace of $\operatorname{Spec} R$, so we call it the **(relative) Zariski topology**.

Various particular choices of $S \subset \operatorname{Spec} R$ have been considered. Of these the most important is certainly $S = \operatorname{MaxSpec} R$, the set of all maximal ideals of R. In this case, $\overline{X}$ consists of all ideals which can be written as the intersection of some family of maximal ideals. Such ideals are necessarily radical, but in a general ring not all radical ideals are obtained in this way. Observe that in a general ring every radical ideal is the intersection of the maximal ideals containing it iff every prime ideal is the intersection of maximal ideals containing it; a ring satisfying these equivalent conditions is called a **Jacobson ring**.

Example: Let k be a field and put $R = k[t_1, \ldots, t_n]$. Then R is a Jacobson ring. To prove this one needs as prerequisite knowledge **Zariski's Lemma** – for every $\mathfrak{m} \in \operatorname{MaxSpec} R$, the field extension $R/\mathfrak{m}/k$ is finite – and the proof uses a short but clever argument: the **Rabinowitsch trick**.

Suppose that k is algebraically closed. Then Zariski's Lemma assumes a stronger form: for all $\mathfrak{m} \in \operatorname{MaxSpec} R$, the k-algebra $R/\mathfrak{m}$ is equal to k. Let $q : R \to R/\mathfrak{m} = k$ be the quotient map, and for $1 \leq i \leq n$, put $x_i = q(t_i)$ and $x = (x_1, \ldots, x_n)$. It follows that $\mathfrak{m}$ contains the ideal $\mathfrak{m}_x = \langle t_1 - x_1, \ldots, t_n - x_n \rangle$, and since $\mathfrak{m}_x$ is maximal, $\mathfrak{m} = \mathfrak{m}_x$. This gives the following description of the Galois connection between the set X of ideals of R and $Y = 2^{\operatorname{MaxSpec} R}$, **Hilbert's Nullstellensatz**:
(i) Maximal ideals of R are canonically in bijection with n-tuples of points of k, i.e., with points of **affine n-space** $\mathbb{A}^n_{/k}$.
(ii) The closure operation on ideals takes I to its radical ideal $\operatorname{rad} I$.
(iii) The closure operation on subsets of $\mathbb{A}^n$ coincides with topological closure with respect to the Zariski topology, i.e., the topology on $\mathbb{A}^n$ for which the closed subsets are the intersections of the zero sets of polynomial functions.

Example: Let K be a field, let $X = 2^K$, let $\operatorname{RSpec} K$ be the set of orderings on K, and let $Y = 2^{\operatorname{RSpec} K}$. Let $H : X \to Y$ by

$$S \mapsto H(S) = \{P \in \operatorname{RSpec} K \mid \forall x \in S \ x >_P 0\}.$$

Let $\Psi : Y \to X$ by

$$T \mapsto \Psi(T) = \{x \in \operatorname{RSpec} K \mid \forall P \in T \ x >_P 0\}.$$

Then (X, Y, H, Ψ) is a Galois connection.

The set $\operatorname{RSpec} K$ carries a natural topology. Namely, we may view any ordering P as an element of $\{\pm 1\}^{K^\times}$: $P : x \in K^\times \mapsto +1$ if $P(x) > 0$ and -1 is $P(x) < 0$. Giving $\{\pm 1\}$ the discrete topology and $\{\pm 1\}^{K^\times}$, it is a compact (by Tychonoff's Theorem) zero-dimensional space. It is easy to see that $\operatorname{RSpec} K$ embeds in $\{\pm 1\}^{K^\times}$ as a closed subspace, and therefore $\operatorname{RSpec} K$ is itself compact and zero-dimensional.

Example: Let $\mathcal{L}$ be a language, let X be the set of $\mathcal{L}$-theories, and let Y be the class of all classes $\mathcal{C}$ of $\mathcal{L}$-structures, partially ordered by inclusion.[12] For a theory $\mathcal{T}$, let $\Phi(\mathcal{T}) = \mathcal{C}_\mathcal{T}$ be the class of all models of $\mathcal{T}$, whereas for a class $\mathcal{C}$, we define $\Psi(\mathcal{C})$ to be the collection of all sentences φ such that for all $X \in \mathcal{C}$, $X \models \varphi$.

[12]Here we are cheating a bit by taking instead of a partially ordered set, a *partially ordered class*. We leave it to the interested reader to devise a remedy.

2.4. **Antitone Galois Connections Decorticated: Relations.**

Example: Let S and T be sets, and let $R \subset S \times T$ be a **relation** between S and T. As is traditional, we use the notation xRy for $(x, y) \in R$. For $A \subset S$ and $y \in T$, we let us write ARy if xRy for all $x \in A$; and dually, for $x \in S$ and $B \subset T$, let us write xRB if xRy for all $y \in B$. Finally, for $A \subset S,\ B \subset T$, let us write ARB if xRy for all $x \in A$ and all $y \in B$.

Let $X = (2^S, \subset)$, $Y = (2^T, \subset)$. For $A \subset S$ and $B \subset T$, we put

$$\Phi_R(A) = \{y \in T \mid ARy\},$$

$$\Psi_R(B) = \{x \in S \mid xRB\}.$$

We claim that $\mathcal{G}_R = (X, Y, \Phi_R, \Psi_R)$ is a Galois connection. Indeed, it is immediate that Φ_R and Ψ_R are both antitone maps; moreover, for all $A \subset S,\ B \subset T$ we have

$$A \subset \Psi_R(B) \iff ARB \iff B \subset \Phi_R(A).$$

Remarkably, this example includes most of the Galois connections above. Indeed:

• In Example 2.2, take X to be 2^K and $Y = 2^{\mathrm{Aut}(K/F)}$. The induced Galois connection is the one associated to the relation $gx = x$ on $K \times \mathrm{Aut}(K/F)$.
• In Example 2.5, take X to be 2^R. The induced Galois connection is the one associated to the relation $x \in \mathfrak{p}$ on $R \times \operatorname{Spec} R$. Similarly for Examples 2.7 and 2.8.
• The Galois connection of Example 2.8 is the one associated to the relation $x \in P$ on $K \times \operatorname{RSpec} K$.
• The Galois connection of Example 2.9 is the one associated to the relation $X \models \varphi$.

Theorem 2.6. *Let S and T be sets, let $X = (2^S, \subset)$, $Y = (2^S, \subset)$, and let $\mathcal{G} = (X, Y, \Phi, \Psi)$ be any Galois connection. Define a relation $R \subset S \times T$ by xRy if $y \in \Phi(\{x\})$. Then $\mathcal{G} = \mathcal{G}_R$.*

Proof. Note first that X and Y are complete lattices, so Lemma 2.4b) applies. Indeed, for $A \subset S$, $A = \bigcup_{x \in A} \{x\} = \bigvee_{x \in A} \{x\}$, so

$$\Phi(A) = \bigcap_{x \in A} \Phi(\{x\}) = \bigcap_{x \in A} \{y \in T \mid xRy\} = \{y \in T \mid ARy\} = \Phi_R(A).$$

Moreover, since $\mathcal{G}$ is a Galois connection we have $\{x\} \subset \Psi(\{y\}) \iff \{y\} \subset \Phi(\{x\}) \iff xRy$. Thus for $B \subset T$, $B = \bigcup_{y \in B} \{y\} = \bigvee_{y \in B} \{y\}$, so

$$\Psi(B) = \bigcap_{y \in B} \Psi(\{y\}) = \bigcap_{y \in A} \{x \in S \mid xRy\} = \{x \in S \mid xRB\} = \Psi_R(B).$$

□

For any partially ordered set $(X, \leq)$, a **downset** is a subset $Y \subset X$ such that for all $x_1, x_2 \in X$, if $x_2 \in Y$ and $x_1 \leq x_2$ then $x_1 \in Y$. Let $D(X)$ be the collection of all downsets of X, viewed as a subset of $(2^X, \subset)$. To each $x \in X$ we may associate the **principal downset** $d(x) = \{y \in X \mid y \leq x\}$. The map $d : X \to D(X)$ is an order embedding; composing this with the inclusion $D(X) \subset 2^X$ we see that every partially ordered set embeds into a power set lattice.

Let $\mathcal{G} = (X, Y, \Phi, \Psi)$ be a Galois connection with X and Y complete lattices. Then we may extend $\mathcal{G}$ to a Galois conection between 2^X and 2^Y as follows: for $A \subset X$, put $\Phi(A) = \bigwedge \{\Phi(x)\}_{x \in A}$, and simialrly for $B \subset Y$, put $\Psi(B) = \bigwedge \{\Psi(y)\}_{y \in B}$.

Thus every Galois connection between complete lattices may be viewed as the Galois connection induced by a relation between sets.

2.5. **Isotone Galois Connections.**

Let $(X, \leq)$ and $(Y, \leq)$ be partially ordered sets. An **isotone Galois connection between X and Y** is a pair of maps $\Phi : X \to Y$ and $\Psi : Y \to X$ such that:

(IGC1) Φ and Ψ are both isotone maps, and
(IGC2) For all $x \in X$ and all $y \in Y$, $\Phi(x) \leq y \iff x \leq \Psi(y)$.

Note that in contrast to the antitone case, this time there is an *asymmetry* between Φ and Ψ. We call Φ the **lower adjoint** and Ψ the **upper adjoint**.

Every isotone Galois connection comes from an antitone Galois connection:

Exercise 2.4:
Let X, Y be partially ordered sets, and let $\Phi : X \to Y$, $\Psi : Y \to X$ be functions.
a) Show that (Φ, Ψ) is an antitone Galois connection between X and Y iff (Φ, Ψ) is an isotone Galois connection between $X^\vee$ and Y.
b) Show that (Φ, Ψ) is an antitone Galois connection between X and Y iff (Ψ, Φ) is an isotone Galois connection between $Y^\vee$ and X.

If $(X, \leq)$ is a partially ordered set, then a mapping $f : X \to X$ is called an **interior operator** if it satisfies all of the following properties:

(I1) For all $x \in X$, $x \geq f(x)$.
(C2) For all $x_1, x_2 \in X$, $x_1 \leq x_2 \implies f(x_1) \leq f(x_2)$.
(C3) For all $x \in X$, $f(f(x)) = f(x)$.

Exercise 2.5: Let $(X, \leq)$ be a partially ordered set, and let $f : X \to X$ be a function. Show that f is a closure operator iff $f : X^\vee \to X^\vee$ is an interior operator.

Proposition 2.7. *Let (Φ, Ψ) be an isotone Galois connection. Then $\Psi \circ \Phi$ is an interior operator on $(X, \leq)$, and $\Phi \circ \Psi$ is a closure operator on $(Y, \leq)$.*

Proof. By Exercise 2.4, (Φ, Ψ) is an antitone Galois connection between $X^\vee$ and Y, so by Proposition 2.1, $\Phi \circ \Psi$ is a closure operator on Y and $\Psi \circ \Phi$ is a closure operator on $X^\vee$ and thus, by Exercise 2.5, an interior operator on X. □

2.6. **Examples of Isotone Galois Connections.**

Example (Galois connection of a function): Let $f : S \to T$ be a function. Let $X = (2^S, \subset)$ and $Y = (2^T, \subset)$. For $A \subset S$ and $B \subset T$, put

$$f_*(S) = f(S) = \{f(s) \mid s \in S\}, \ f^*(T) = f^{-1}(B) = \{s \in S \mid f(s) \in B\}.$$

Exercise 2.6: a) Show: (f^*, f_*) is an isotone Galois connection between 2^T and 2^S.
b) Show that the interior operator $f_* \circ f^* : B \subset T \mapsto B \cap f(S)$. In particular the Galois connection is **left perfect** iff f is surjective.
c) Show that the Galois connection is **right perfect** – i.e., $f^* f_* A = A$ for all $A \subset S$

– iff f is injective.
d) Interpret this isotone Galois connection in terms of the "universal" antitone Galois connection of §2.4.

Example (Galois Connection of a Ring Homomorphism): Let $f : R \to S$ be a homomorphism of rings, and let $\mathcal{I}(R)$ and $\mathcal{I}(S)$ be the lattices of ideals of R and S. In §1.5 we defined a pushforward map

$$f_* : \mathcal{I}(R) \to \mathcal{I}(S),\ f_*(I) = \langle f(I) \rangle$$

and a pullback map

$$f^* : \mathcal{I}(S) \to \mathcal{I}(R),\ f^*(J) = f^{-1}(J).$$

Proposition 2.8. *The maps (f^*, f_*) give an isotone Galois connection between $\mathcal{I}(S)$ and $\mathcal{I}(T)$.*

Exercise 2.7: Prove Proposition 2.8.

3. Modules

3.1. **Basic definitions.**

Suppose $(M, +)$ is an abelian group. For any $m \in M$ and any integer n, one can make sense of $n \bullet m$. If n is a positive integer, this means $m + \cdots + m$ (n times); if $n = 0$ it means 0, and if n is negative, then $n \bullet m = -(-n) \bullet m$. Thus we have defined a function $\bullet : \mathbb{Z} \times M \to M$ which enjoys the following properties: for all $n,\ n_1,\ n_2 \in \mathbb{Z},\ m,\ m_1,\ m_2 \in M$, we have

(ZMOD1) $1 \bullet m = m$.
(ZMOD2) $n \bullet (m_1 + m_2) = n \bullet m_1 + n \bullet m_2$.
(ZMOD3) $(n_1 + n_2) \bullet m = n_1 \bullet m + n_2 \bullet m$.
(ZMOD4) $(n_1 n_2) \bullet m = n_1 \bullet (n_2 \bullet m)$

It should be clear that this is some kind of ring-theoretic analogue of a group action on a set. In fact, consider the slightly more general construction of a monoid $(M, \cdot)$ acting on a set S: that is, for all $n_1,\ n_2 \in M$ and $s \in S$, we require $1 \bullet s = s$ and $(n_1 n_2) \bullet s = n_1 \bullet (n_2 \bullet s)$.

For a group action G on S, each function $g\bullet : S \to S$ is a bijection. For monoidal actions, this need not hold for all elements: e.g. taking the natural multiplication action of $M = (\mathbb{Z}, \cdot)$ on $S = \mathbb{Z}$, we find that $0\bullet : \mathbb{Z} \to \{0\}$ is neither injective nor surjective, $\pm 1\bullet : \mathbb{Z} \to \mathbb{Z}$ is bijective, and for $|n| > 1$, $n\bullet : \mathbb{Z} \to \mathbb{Z}$ is injective but not surjective.

Exercise 3.1: Let $\bullet : M \times S \to S$ be a monoidal action on a set. Show that for each unit $m \in M$ – i.e., an element for which there exists m' with $mm' = m'm = 1$ – $m\bullet : S \to S$ is a bijection.

Then the above "action" of $\mathbb{Z}$ on an abelian group M is in particular a monoidal action of $(\mathbb{Z}, \cdot)$ on the set M. But it is more: M has an additive structure, and

(ZMOD2) asserts that for each $n \in \mathbb{Z}$, $n\bullet$ respects this structure – i.e., is a homomorphism of groups; also (ZMOD3) is a compatibility between the additive structure on $\mathbb{Z}$ and the additive structure on M.

These axioms can be restated in a much more compact form. For an abelian group M, an **endomorphism** of M is just a group homomorphism from M to itself: $f : M \to M$. We write $\mathrm{End}(M)$ for the set of all endomorphisms of M. But $\mathrm{End}(M)$ has lots of additional structure: for $f, g \in \mathrm{End}(M)$ we define $f + g \in \mathrm{End}(M)$ by

$$(f + g)(m) := f(m) + g(m),$$

i.e., pointwise addition. We can also define $f \cdot g \in \mathrm{End}(M)$ by composition:

$$(f \cdot g)(m) := f(g(m)).$$

Proposition 3.1. *For any abelian group M, the set $\mathrm{End}(M)$ of group endomorphisms of M, endowed with pointwise addition and multiplication by composition, has the structure of a ring.*

Exercise 3.2: Prove Proposition 3.1.

Exercise 3.3: Show that $\mathrm{End}(\mathbb{Z}) = \mathbb{Z}$, and for any $n \in \mathbb{Z}$, $\mathrm{End}(\mathbb{Z}/n\mathbb{Z}) = \mathbb{Z}/n\mathbb{Z}$. (More precisely, find canonical isomorphisms.)

These simple examples are potentially misleading: we did not say that the multiplication was commutative, and of course there is no reason to expect composition of functions to be commutative.

Exercise 3.4: a) Show that $\mathrm{End}(\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}) = M_2(\mathbb{Z}/2\mathbb{Z})$, the (noncommutative!) ring of 2×2 matrices with $\mathbb{Z}/2\mathbb{Z}$-coefficients.
b) If M is an abelian group and $n \in \mathbb{Z}^+$, show $\mathrm{End}(M^n) = M_n(\mathrm{End}(M))$.

Now observe that the statement that the action of $\mathbb{Z}$ on M satisfes (ZMOD1) through (ZMOD4) is equivalent to the following much more succinct statement:

For any abelian group M, the map $n \in \mathbb{Z} \mapsto (n\bullet) : M \to M$ is a homomorphism of rings $\mathbb{Z} \to \mathrm{End}(M)$.

This generalizes very cleanly: if R is any ring (not necessarily commuative) and M is an abelian group, a homomorphism $\bullet : R \to \mathrm{End}(M)$ will satisfy: for all $r \in R,\ m, m_1, m_2 \in M$:

(LRMOD1) $1 \bullet m = m$.
(LRMOD2) $r \bullet (m_1 + m_2) = r \bullet m_1 + r \bullet m_2$.
(LRMOD3) $(r_1 + r_2) \bullet m = r_1 \bullet m + r_2 \bullet m$.
(LRMOD4) $(r_1 r_2) \bullet m = r_1 \bullet (r_2 \bullet m)$.

The terminology here is that such a homomorphism $r \mapsto (r\bullet)$ is a **left R-module structure** on the abelian group M.

What then is a **right R-module structure** on M? The pithy version is that

it is a ring homomorphism from R^{op}, the opposite ring of R to $\mathrm{End}(M)$. This definition makes clear (only?) that if R is commutative, there is no difference between left and right R-module structures. Since our interest is in the commutative case, we may therefore not worry too much. But for the record:

Exercise 3.5: Show that a homomorphism $R^{\mathrm{op}} \to \mathrm{End}(M)$ is equivalent to a mapping $\bullet : M \times R \to M$ satisfying

$$m \bullet 1 = m,$$
$$(m_1 + m_2) \bullet r = m_1 \bullet r + m_2 \bullet r,$$
$$m \bullet (r_1 + r_2) = m \bullet r_1 + m \bullet r_2,$$
$$m \bullet (r_1 r_2) = (m \bullet r_1) \bullet r_2.$$

As usual for multiplicative notation, we will generally suppress the bullet, writing rm for left R-modules and mr for right R-modules.

The calculus of left and right actions is at the same time confusing and somewhat miraculous: it is a somewhat disturbing example of a purely lexicographical convention that has – or looks like it has – actual mathematical content. Especially, suppose we have an abelian group M and two rings R and S, such that M simultaneously has the structure of a left R-module and a right S-module. Thus we wish to entertain expressions such as rms for $m \in M$, $r \in R$, $s \in S$. But as stands this expression is ambiguous: it could mean either

$$(r \bullet m) \bullet s$$

or

$$r \bullet (m \bullet s).$$

We say that M is an **R-S bimodule** if both of these expressions agree. Here is what is strange about this: lexicographically, it is an associativity condition. But "really" it is a commutativity condition: it expresses the fact that for all $r \in R$, $s \in S$, $(r\bullet) \circ (\bullet s) = (\bullet s) \circ (r\bullet)$: every endomorphism coming from an element of R commutes with every endomorphism coming from an element of S. Thus for instance:

Exercise 3.6: Show that any ring R is naturally a left R-module and a right R-module.

We will not deal with bimodules further in these notes. In fact, when we say R-module at all, it will be understood to mean a left R-module, and again, since we shall only be talking about commutative rings soon enough, the distinction between left and right need not be made at all.

Definition: For M a left R-module, we define its **annihilator**

$$\mathrm{ann}(M) = \{r \in R \mid \forall m \in M, rm = 0\}.$$

Equivalently, $\mathrm{ann}(M)$ is the set of all r such that $r\cdot = 0 \in \mathrm{End}(M)$, so that it is precisely the kernel of the associated ring homomorphism $R \to \mathrm{End}(M)$. It follows that $\mathrm{ann}(M)$ is an ideal of R (note: two-sided, in the noncommutative case).

Definition: A left R-module M is **faithful** if $\operatorname{ann}(M) = 0$. Explicitly, this means that for all $0 \neq r \in R$, there exists $m \in M$ such that $rm \neq 0$.

Exercise 3.7: Let M be an R-module. Show that M has the natural structure of a faithful $R/\operatorname{ann}(M)$-module.

Definition: Let M be a left R-module. A **submodule** of M is a subgroup N of $(M, +)$ such that $RN \subset N$. The following result is extremely easy and all-important:

Theorem 3.2. *Let R be a ring. The left R-submodules of R are precisely the left ideals of R.*

Exercise 3.8: Prove Theorem 3.2.

Definition: Let M and N be left R-modules. A **homomorphism** of R-modules is a homomorphism of abelian groups $f : M \to N$ such that for all $r \in R,\ m \in M,\ n \in N,\ f(rm) = rf(m)$.

Exercise 3.9: a) Define an isomorphism of R-modules in the correct way, i.e., *not* as a bijective homomorphism of R-modules.
b) Show that a homomorphism of R-modules is an isomorphism iff it is bijective.

If N is a submodule of a left R-module M, then the quotient group M/N has a natural R-module structure. More precisely, there is a unique left R-module structure on M/N such that the quotient map $M \to M/N$ is a homomorphism of R-modules. (Exercise!)

Exercise 3.10: Let I be a two-sided ideal of the ring R, so that the quotient ring R/I has the structure of a left R-module. Show that

$$\operatorname{ann}(R/I) = I.$$

In particular, every two-sided ideal of R occurs as the annihilator of a left R-module.

Exercise 3.11: a) Let R be a ring and $\{M_i\}_{i \in I}$ a family of R-modules. Consider the abelian group $M = \bigoplus_{i \in I} M_i$. Show that putting $r(m_i) = (rm_i)$ makes R into an R-module. Show that the usual inclusion map $\iota_i : M_i \to M$ is a homomorphism of R-modules.
b) Show that for any R-module N and R-module maps $f_i : M_i \to N$, there exists a unique R-module map $f : M \to N$ such that $f_i = f \circ \iota_i$ for all $i \in I$. Thus M satisfies the universal mapping property of the direct sum.

As a matter of notation, for $n \in \mathbb{Z}^+$, $R^n := \bigoplus_{i=1}^n R$, $R^0 = 0$.

Exercise 3.12: Work out the analogue of Exercise 3.12 for direct products.

Exercise 3.13: a) Suppose that M is an R-module and S is a subset of M. Show that the intersection of all R-submodules of M containing S is an R-submodule, and is contained in every R-submodule that contains S. We call it the R-submodule **generated** by S.

b) If $S = \{s_i\}_{i \in I}$, show that the R-module generated by S is the set of all sums $\sum_{i \in J} r_i s_i$, where J is a finite subset of S.

Exercise 3.14: Suppose that k is a field. Show that the terms "k-module" and "vector space over k" are synonymous.

One can therefore view the theory of R-modules as a generalization of vector spaces to arbitrary rings. But really this is something like a zeroth order approximation of the truth: for a general ring R, the theory of R-modules is incomparably richer than the theory of vector spaces over a field. There are two explanations for this. First, even when working with very simple R-modules such as R^n, the usual linear algebra notions of linear independence, span and basis remain meaningful, but behave in unfamiliar ways:

Call a subset S of an R-module M **linearly independent** if for every finite subset $m_1, \ldots, m_n$ of S and any $r_1, \ldots, r_n \in R$, $r_1 m_1 + \ldots + r_n m_n = 0$ implies $r_1 = \ldots = r_n = 0$. Say that S **spans** R if the R-submodule generated by S is R, and finally a **basis** for an R-module is a subset which is both linearly independent and spanning. For example, for any set I, the R-module $\bigoplus_i R$ has a basis e_i.

In linear algebra – i.e., when R is a field – every R-module has a basis.[13] However the situation is quite different over a general ring:

Theorem 3.3. *a) Let M be an R-module. Suppose that $S \subset R$ is a basis. Then M is isomorphic as an R-module to $\bigoplus_{s \in S} R$.*
b) Let S be any set, and consider the R-module $R_S := \bigoplus_{s \in S} R$. For each $s \in S$, let $e_s \in \bigoplus_{s \in S} R$ be the element whose s-coordinate is 1 and all of whose other coordinates are 0. Then set $\{e_s\}_{s \in S}$ is a basis for R_S.

Exercise 3.15: Prove Theorem 3.3.

A module which has a basis – so, by the theorem, admits an isomorphism to $\bigoplus_{s \in S} R$ for some index set S – is called **free**.

Exercise 3.16: Show that a nonzero free R-module is faithful.

Let us examine the case of modules over $R = \mathbb{Z}$, i.e., of abelian groups. Here the term **free abelian group** is synonymous with "free $\mathbb{Z}$-module". It is (of course?) not the case that all abelian groups are free: for any integer $n > 1$, $\mathbb{Z}/n\mathbb{Z}$ is not free, since it has nonzero annihilator $n\mathbb{Z}$. Thus $\mathbb{Z}/n\mathbb{Z}$ does not have a basis as a $\mathbb{Z}$-module, and indeed has no nonempty linearly independent subsets!

Proposition 3.4. *For a commutative ring R, TFAE:*
(i) Every R-module is free.
(ii) R is a field.

Proof. As discussed above, (ii) $\implies$ (i) is a fundamental theorem of linear algebra, so we need only concern ourselves with the converse. But if R is not a field, then

[13] This uses, and is in fact equivalent to, the Axiom of Choice, but the special case that any vector space with a finite spanning set has a basis does not.

there exists a nonzero proper ideal I, and then R/I is a nontrivial R-module with $0 \neq I = \operatorname{ann}(R/I)$, so by Exercise 3.16 R/I is not free. □

Remark: If R is a not-necessarily-commutative ring such that every left R-module is free, then the above argument shows R has no nonzero proper twosided ideals, so is what is called a **simple ring**. But a noncommutative simple ring may still admit a nonfree module. For instance, let k be a field and take $R = M_2(k)$, the 2×2 matrix ring over k. Then $k \oplus k$ is a left R-module which is not free. However, suppose R is a ring with no proper nontrivial one-sided ideals. Then R is a division ring – i.e., every nonzero element of R is a unit – and every R-module is free.

In linear algebra – i.e., when R is a field – every linearly independent subset of an R-module can be extended to a basis. Over a general ring this does not hold even for free R-modules. For instance, take $R = M = \mathbb{Z}$. A moment's thought reveals that the only two bases are $\{1\}$ and $\{-1\}$, whereas the linearly independent sets are precisely the singleton sets $\{n\}$ as n ranges over the nonzero integers.

Note well the form of Proposition 3.4: we assume that R is a commutative ring for which R-modules satisfy some nice property, and we deduce a result on the structure of R. Such "inverse problems" have a broad appeal throughout mathematics and provide one of the major motivations for studying modules above and beyond their linear algebraic origins. We will see other such characterizations later on.

3.2. **Finitely presented modules.**

One of the major differences between abelian groups and nonabelian groups is that a subgroup N of a finitely generated abelian group M remains finitely generated, and indeed, the minimal number of generators of the subgroup N cannot exceed the minimal number of generators of M, whereas this is not true for nonabelian groups: e.g. the free group of rank 2 has as subgroups free groups of every rank $0 \leq r \leq \aleph_0$. (For instance, the commutator subgroup is not finitely generated.)

Since an abelian group is a $\mathbb{Z}$-module and every R-module has an underlying abelian group structure, one might well expect the situation for R-modules to be similar to that of abelian groups. We will see later that this is true in many but not all cases: an R-module is called **Noetherian** if all of its submodules are finitely generated. Certainly a Noetherian module is itself finitely generated. The basic fact here – which we will prove in §8.7 – is a partial converse: if the ring R is Noetherian, any finitely generated R-module is Noetherian. Note that we can already see that the Noetherianity of R is necessary: if R is not Noetherian, then by definition there exists an ideal I of R which is not finitely generated, and this is nothing else than a non-finitely generated R-submodule of R (which is itself generated by the single element 1.) Thus the aforementioned fact about subgroups of finitely generated abelian groups being finitely generated holds because $\mathbb{Z}$ is a Noetherian ring.

When R is not Noetherian, it becomes necessary to impose stronger conditions than finite generation on modules. One such condition indeed comes from group

theory: recall that a group G is **finitely presented** if it is isomorphic to the quotient of a finitely generated free group F by the least normal subgroup N generated by a finite subset $x_1, \ldots, x_m$ of F.

Proposition 3.5. *For a finitely generated R-module M, TFAE:*
(i) There exist non-negative integers m, n and an exact sequence

$$R^m \to R^n \to M \to 0.$$

(ii) M is the quotient of an f.g. free R-module R^n by some f.g. submodule N.
*A module M satisfying these equivalent conditions is said to be **finitely presented**.*

Proof. That (i) implies (ii) is immediate. Conversely, let $M = R^n/N$ where N is finitely generated. Then there exists a surjection $R^m \to N$ and thus the sequence

$$R^m \to R^n \to M \to 0$$

is exact. □

Proposition 3.6. *Let*

$$0 \to K \xrightarrow{\psi} N \xrightarrow{\phi} M \to 0$$

be a short exact sequence of R-modules, with M finitely presented and N finitely generated. Then K is finitely generated.

Proof. (Matsumura) By definition of finitely presented, we can place M in an exact sequence

$$R^m \to R^n M \xrightarrow{f} 0 \tag{5}$$

for some $m, n \in \mathbb{N}$. For $1 \leq i \leq n$, let e_i be the ith standard basis element of M, let $m_i = f(e_i)$ be the image in M, and choose $n_i \in N$ any element in $\phi^{-1}(m_i)$. Then there is a unique R-module homomorphism $\alpha : R^n \to N$ given by $\alpha(e_i) = n_i$, which restricts to an R-module homomorphism $\beta : B^m \to K$. Altogether we get a commutative diagram

$$\begin{array}{ccccccc} R^m & \longrightarrow & R^n & \xrightarrow{f} & M & \longrightarrow & 0 \\ 0 & \longrightarrow & K & \xrightarrow{\psi} & N & \xrightarrow{\phi} & M. \end{array}$$

The rest of the proof is essentially a diagram chase. Suppose $N = \langle \xi_1, \ldots, \xi_k \rangle_R$, and choose $v_1, \ldots, v_k \in R^n$ such that $\phi(\xi_i) = f(v_i)$. Put

$$\xi_i' = \xi_i - \alpha(v_i).$$

Then $\varphi(\xi_i') = 0$, so there exist unique $\eta_i \in K$ such that

$$\xi_i' = \psi(\eta_i).$$

We CLAIM that K is generated as an R-module by $\beta(R^m)$ and $\eta_1, \ldots, \eta_k$ and thus is finitely generated. Indeed, for $\eta \in K$, there are $r_1, \ldots, r_k \in R$ such that

$$\psi(\eta) = \sum_i r_i \xi_i.$$

Then

$$\psi(\eta - \sum_i r_i \eta_i) = \sum_i r_i(\xi_i - \xi_i') = \alpha(\sum_i r_i v_i).$$

Since

$$0 = \phi(\alpha(\sum_i r_i v_i)) = f(\sum_i r_i v_i),$$

we may write $\sum_i r_i v_i = g(u)$ with $u \in R^m$. Then

$$\psi(\beta(u)) = \alpha(g(u)) = \alpha(\sum_i r_i v_i) = \psi(\eta - \sum_i r_i \eta_i).$$

Since ψ is injective, we conclude

$$\eta = \beta(u) + \sum_i r_i \eta_i.$$

□

Exercise 3.17:
Let $0 \to M' \to M \to M'' \to 0$ be a short exact sequence of R-modules.
a) Show that if M' and M'' are both finitely presented, so is M.
b) Show that if M is finitely presented and M' is finitely generated, then M'' is finitely presented.

A stronger condition yet is the following: an R-module M is **coherent** if it is finitely generated and every finitely generated submodule is finitely presented. Evidently coherent implies finitely presented implies finitely generated, and all three coincide over a Noetherian ring. The significance of coherence lies in the following:

Theorem 3.7. *Let R be a ring (not necessarily commutative, but with unity).*
a) The category of all left R-modules is an abelian category.
b) The category of all coherent left R-modules is an abelian category.
c) In particular, if R is left Noetherian, the category of all finitely generated left R-modules is an abelian category.
*d) There exists a commutative ring R for which the category of all finitely generated (left) R-modules is **not** abelian.*

The proof of this result – and even an explanation of the term "abelian category" is beyond the scope of these notes, so this is definitely an ancillary remark. Nevertheless we hope that it will be of some use to students of algebraic geometry: for instance, it explains the fact that Hartshorne only defines coherent sheaves of modules on a scheme X in the case that the scheme is Noetherian and suggests the correct (and more subtle) definition in the non-Noetherian case.

3.3. **Torsion and torsionfree modules.**

Let R be a domain, and let M be an R-module. An element $x \in M$ is said to be **torsion** if there exists $0 \neq a \in R$ such that $ax = 0$. Equivalently, the annihilator $\text{ann}(x) = \{a \in R \mid ax = 0\}$ is a nonzero ideal of R. We define $M[\text{tors}]$ to be the set of all torsion elements of M. It is immediate to see that $M[\text{tors}]$ is a submodule of M. We say that M is a **torsion** R-module if $M = M[\text{tors}]$ and that M is **torsionfree** if $M[\text{tors}] = 0$.

Exercise 3.18: Let $0 \to M_1 \to M \to M_2 \to 0$ be an exact sequence.
a) Show that if M is torsion, so are M_1 and M_2.
b) If M_1 and M_2 are torsion modules, must M be torsion?
c) Show that if M is torsionfree, show that so is M_1, but M_2 need not be.
d) If M_1 and M_2 are torsionfree, must M be torsionfree?

Proposition 3.8. *Let R be an integral domain and M an R-module.*
a) The quotient $M/M[\text{tors}]$ is torsionfree.
b) If M is finitely generated, the following are equivalent:
(i) M embeds in a finitely generated free R-module.
(ii) M is torsionfree.

Proof. a) Put $N = M/M[\text{tors}]$, and let $\overline{x} \in N$ be such that there exists $0 \neq a \in R$ with $a\overline{x} = 0$. Let x be any lift of $\overline{x}$ to M; then there exists $t \in M[\text{tors}]$ such that $ax = t$. By definition of torsion, there exists $a' \in R$ such that $a't = 0$, so $a'ax = a't = 0$. Since R is a domain, $a'a$ is nonzero, so $x \in M[\text{tors}]$ and $\overline{x} = 0$.
b) (i) $\implies$ (ii) is very easy: free modules are torsionfree and submodules of torsionfree modules are torsionfree.
(ii) $\implies$ (i): We may assume $M \neq 0$. Let $M = \langle x_1, \ldots, x_r \rangle$ with $r \geq 1$ and all the x_i are nonzero. Further, after reordering the x_i's if necessary, there exists a unique s, $1 \leq s \leq r$, such that $\{x_1, \ldots, x_s\}$ is linearly independent over R but for all i with $s < i \leq r$, $\{x_1, \ldots x_s, x_i\}$ is linearly dependent over R. Then $F = \langle x_1, \ldots, x_s \rangle \cong R^s$, so we are done if $s = r$. If $s < r$, then for each $i > s$ there exists $0 \neq a_i \in R$ such that $a_i x_i \in F$. Put $a = \prod_{s<i\leq r} a_i$: then $aM \subset F$. Let $[a] : M \to M$ denote multiplication by a. Since M is torsionfree, $[a]$ is injective hence gives an R-module isomorphism from M to a submodule of the finitely generated free module F. □

Exercise 3.19: Show that the torsionfree $\mathbb{Z}$-module $(\mathbb{Q}, +)$ is not isomorphic to a submodule of any finitely generated free $\mathbb{Z}$-module. Thus – even for very nice rings! – the hypothesis of finite generation is necessary in Proposition 3.8.

3.4. **Tensor and Hom.**

3.4.1. *Tensor products.*

We assume that the reader has some prior familiarity with tensor products, say of vector spaces and/or of abelian groups. The first is an instance of tensor products of k-modules, for some field k, and the second is an instance of tensor products of $\mathbb{Z}$-modules. We want to give a general definition of $M \otimes_R N$, where M and N are two R-modules.

There are two ways to view the tensor product construction: as a solution to a universal mapping problem, and as a generators and relations construction. They are quite complementary, so it is a matter of taste as to which one takes as "the" definition. So we will follow our taste by introducing the mapping problem first:

Suppose M, N, P are R-modules. By an R-**bilinear** map $f : M \times N \to P$ we mean a function which is separately R-linear in each variable: for all $m \in M$, the mapping $n \mapsto f(m, n)$ is R-linear, and for each $n \in N$, the mapping $m \mapsto f(m, n)$ is R-linear. Now consider all pairs (T, ι), where T is an R-module and $\iota : M \times N \to T$ is an R-bilinear map. A morphism from (T, ι) to (T', ι') will be an R-module homomorphism $h : T \to T'$ such that $\iota' = h \circ \iota$. By definition, a tensor product $M \otimes_R N$ is an initial object in this category: i.e., it comes equipped with an R-bilinear map $M \times NraM \otimes_R N$ such that any R-bilinear map $f : M \times N \to P$ factors through it. As usual, the initial object of a category is unique up to unique isomorphism provided it exists.

As for the existence, we fall back on the generators and relations construction. Namely, we begin with the free R-module F whose basis is $M \times N$, and we write the basis elements (purely formally) as $m \otimes n$. We then take the quotient by the submodule generated by the following relations R:

$$(x + x') \otimes y - x \otimes y - x' \otimes y,$$

$$x \otimes (y + y') - x \otimes y - x \otimes y',$$

$$(ax) \otimes y - a(x \otimes y),$$

$$x \otimes (ay) - a(x \otimes y).$$

It is then easy to see that the quotient map $M \times N \to F/N$ satisfies all the properties of a tensor product (details left to the reader).

Note that the general element of $M \otimes_R N$ is not a single element of the form $x \otimes y$ but rather a finite sum of such elements. (Indeed, from the free R-module, every element can be represented by a finite R-linear combination of elements of the form $x \otimes y$, but the last two defining relations in the tensor product allow us to change $r_i(x \otimes y)$ to either $(r_i x) \otimes y$ or $x \otimes (r_i y)$.) Of course, this representation of an element of the tensor product need not be (and will never be, except in trivial cases) unique.

One can also take the tensor product of R-algebras: if R is a (commutative!) ring and A and B are commutative R-algebras, then on the tensor product $A \otimes_R B$ we have a naturally defined product, induced by $(a_1 \otimes b_1) \cdot (a_2 \otimes b_2) := (a_1 a_2 \otimes b_1 b_2)$. We have to check that this is well-defined, a task which we leave to the reader (or see [AM, pp. 30-31])). The tensor product of algebras is a powerful tool – e.g. in the structure theory of finite-dimensional algebras over a field, or in the theory of linear disjointness of field extensions – and is given misleadingly short shrift in most elementary treatments.

Base change: Suppose that M is an R-module and $f : R \to S$ is a ring homomorphism. Then S is in particular an R-module, so that we can form the tensor product $S \otimes_R M$. This is still an R-module, but it is also an S-module in an evident way: $s \bullet (\sum_i s_i \otimes m_i) := \sum_i s s_i \otimes m_i$. This is process is variously called **scalar extension**, **base extension** or **base change**. Note that this process is functorial, in the following sense: if $f : M \to M'$ is an R-algebra homomorphism, then there exists an induced S-algebra homomorphism $S \otimes_R M \to S \otimes_R M'$, given by $s \otimes m \mapsto s \otimes f(m)$.

Exercise 3.20: If M is a finitely generated R-module and $f : R \to S$ is a ring homomorphism, then $S \otimes_R M$ is a finitely generated S-module.

Exercise 3.21: Let A and B be rings, M an A-module, P a B-module, and N an (A, B)-bimodule. Then $M \otimes_A N$ is naturally a B-module, $N \otimes_B P$ is naturally an A-module, and

$$(M \otimes_A N) \otimes_B P \cong M \otimes_A (N \otimes_B P).$$

Exercise 3.22: Let R be a commutative ring, I an ideal of R and M an R-module.

a) Show that there is a well-defined R-bilinear map $R/I \times M \to M/IM$ given by $(r+I, m) \mapsto rm + I$. Thus there is an induced homomorphism of R-modules

$$\varphi : R/I \otimes_R M \to M/IM.$$

b) Show that φ is an isomorphism of R-modules.

Proposition 3.9. *Let R be a commutative ring, M an R-module and $\{N_i\}_{i\in I}$ a directed system of R-modules. Then the R-modules $\varinjlim(M \otimes N_i)$ and $M \otimes (\varinjlim N_i)$ are canonically isomorphic.*

Exercise 3.23: Prove Proposition 3.9.

3.5. **Projective modules.**

3.5.1. *Basic equivalences.*

Proposition 3.10. *For an R-module P, TFAE:*
(i) There exists an R-module Q such that $P \oplus Q$ is a free R-module.
(ii) If $\pi : M \to N$ is a surjective R-module homomorphism and $\varphi : P \to N$ is a homomorphism, then there exists at least one R-module homomorphism $\Phi : P \to M$ such that $\varphi = \pi \circ \Phi$.
(iii) If $\pi : M \to N$ is a surjection, then the natural map $\mathrm{Hom}(P, M) \to \mathrm{Hom}(P, N)$ given by $\Phi \mapsto \pi \circ \Phi$ is surjective.
(iv) The functor $\mathrm{Hom}(P, \ )$ is exact.
(v) Any short exact sequence of R-modules

$$0 \to N \to M \xrightarrow{q} P \to 0$$

splits: there exists an R-module map $\sigma : P \to M$ such that $q \circ \sigma = 1_P$ and thus an internal direct sum decomposition $M = N \oplus \sigma(P)$.
A module satisfying these equivalent conditions is called ***projective****.*

Proof. (i) $\implies$ (ii): Let $F \cong P \oplus Q$ be a free module. Let $\{f_i\}$ be a free basis for F and let $\{p_i\}$ be the corresponding generating set for P, where p_i is the image of f_i under the natural projection $P \oplus Q \to P$. Put $n_i = \varphi(p_i)$. By surjectivity of π, let $m_i \in \pi^{-1}(n_i)$. By the freeness of F, there is a unique R-module homomorphism $h : F \to M$ carrying each f_i to m_i. Pull h back to P via the natural inclusion $P \hookrightarrow F$. Then $h : P \to M$ is such that $\pi \circ f = \varphi$.
(ii) $\implies$ (i): As for any R-module, there exists a free R-module F and a surjection $\pi : F \to P$. Applying (ii) with $N = p$ and $\varphi : P \to N$ the identity map, we get a homomorphism $\Phi : P \to F$ such that $\pi \circ \varphi = 1_P$. It follows that $F = \Phi(P) \oplus \ker(\pi)$ is an internal direct sum decomposition.
(ii) $\iff$ (iii): (iii) is nothing more than a restatement of (ii), as we leave it to the reader to check.
(iii) $\iff$ (iv): To spell out (iv), it says: if

$$0 \to M' \to M \to M'' \to 0$$

is a short exact sequence of R-modules, then the corresponding sequence

$$0 \to \mathrm{Hom}(P, M') \to \mathrm{Hom}(P, M) \to \mathrm{Hom}(P, M'') \to 0$$

is exact. Now for any R-module P, the sequence

$$0 \to \mathrm{Hom}(P, M') \to \mathrm{Hom}(P, M) \to \mathrm{Hom}(P, M'')$$

is exact – i.e., $\mathrm{Hom}(P, \ )$ is left exact – so (iv) amounts to: for any surjection $M \to M''$, the corresponding map $\mathrm{Hom}(P, M) \to \mathrm{Hom}(P, M'')$ is surjective, and this is condition (iii).
(ii) $\implies$ (v): Given

$$0 \to N \to M \to P \xrightarrow{q} 0,$$

we apply (ii) to the identity map $1_P : P \to P$ and the surjection $q : M \to P$, getting a map $\sigma : P \to M$ such that $q \circ \sigma = 1_P$, so σ is a section as required.
(v) $\implies$ (i): Choosing a set of generators for P gives rise to a surjective homomorphism $q : F \to P$ from a free R-module F to P and thus a short exact sequence

$$0 \to \mathrm{Ker}\, q \to F \xrightarrow{q} P \to 0.$$

By hypothesis, there exists a section $\sigma : P \to F$ and thus an internal direct sum decomposition $F \cong \mathrm{Ker}(q) \oplus \sigma(P) \cong \mathrm{Ker}(q) \oplus P$. □

Exercise 3.24: Give a direct proof that (v) $\implies$ (ii) in Proposition 3.10. (Suggestion: Given the surjection $q : M \to N$ and the map $\pi : P \to N$, form the short exact sequence $0 \to K \to M \to N \to 0$ and show that it is mapped to by a short exact sequence $0 \to K \to M \times_N P \to P \to 0$, where

$$M \times_N P = \{(x, y) \in M \times P \mid q(x) = \pi(y)\}$$

is the **fiber product** of M and P over N.)

Exercise 3.25: Use Proposition 3.10 to show, several times over, that a free R-module is projective.

Exercise 3.26: Let $\{M_i\}_{i \in I}$ be an index family of R-modules. Show that the direct sum $M = \bigoplus_{i \in I} M_i$ is projective iff each M_i is projective.

Exercise 3.27:
a) Show that the tensor product of two free R-modules is free.
b) Show that the tensor product of two projective R-modules is projective.

Exercise 3.28: Show that a finitely generated projective module is finitely presented. (Hint: the problem is that over a not-necessarily-Noetherian ring, a submodule of a finitely generated module need not be finitely generated. However, a *direct summand* of a finitely generated module is always finitely generated: why?)

3.5.2. *Linear algebraic characterization of projective modules.*

Let R be a commutative ring, $n \in \mathbb{Z}^+$, and let P be an element of the (non-commutative!) ring $M_n(R)$ of $n \times n$ matrices with entries in R such that $P^2 = P$. There are several names for such a matrix. The pure algebraist would call such a matrix **idempotent**, for that is the name of an element in any ring which is equal to its square. A geometrically minded algebraist however may call such a matrix a **projection**, the idea being that the corresponding R-module endomorphism of R^n "projects" R^n onto the submodule $P(R^n)$.

Proposition 3.11. *An R-module M is finitely generated and projective iff it is, up to isomorphism, the image of a projection: i.e., iff there exists $n \in \mathbb{Z}^+$ and a matrix $P \in M_n(R)$ with $P = P^2$ such that $M \cong P(R^n)$.*

Proof. Suppose first that M is a finitely generated projective R-module. Since M is finitely generated,, there exists $n \in \mathbb{Z}^+$ and a surjective R-module homorphism $\pi : R^n \to M$. Since M is projective, this homomorphism has a section $\sigma : M \to R^n$, and we may thus write $R^n = \sigma(M) \oplus M'$. Put $P = \sigma \circ \pi \in \mathrm{End}_R(R^n)$. Then $P(R^n) = \sigma(\pi(R^n)) = \sigma(M) \cong M$ and

$$P^2 = \sigma \circ (\pi \circ \sigma) \circ \pi = \sigma \circ 1_M \circ \pi = \sigma \circ \pi = P.$$

Conversely, suppose that there exists $P \in \mathrm{End}_R(R^n)$ with $P^2 = P$ and let $M \cong P(R^n)$. Then – since $P(1-P) = 0$ – $R^n = P(R^n) \oplus (1-P)(R^n)$, exhibiting $P(R^n)$ as a direct summand of a free module.[14] □

3.5.3. *The Dual Basis Lemma.*

Proposition 3.12. *(Dual Basis Lemma) For an R-module M, TFAE:*
(i) There exists an index set I, elements $\{a_i\}_{i\in I}$ of M and homomorphisms $\{f_i : M \to R\}_{i\in I}$ such that for each $a \in M$, $\{i \in I \mid f_i(a) \neq 0\}$ is finite, and

$$a = \sum_{i\in I} f_i(a)a_i.$$

(ii) M is projective.

Proof. (i) $\implies$ (ii): Let F be the free R-module with basis elements $\{e_i\}_{i\in I}$, and define $f : F \to M$ by $f(e_i) = a_i$. Then the map $\iota : M \to F$ given by $\iota(a) = \sum_{i\in I} f_i(a)e_i$ is a section of f, so M is a direct summand of F.
(ii) $\implies$ (i): Let $f : F = \bigoplus_{i\in I} R \to M$ be an epimorphism from a free R-module onto M. Since M is projective, there exists a section $\iota : M \hookrightarrow F$. If $\{e_i\}_{i\in I}$ is the standard basis of F, then for all $a \in M$, the expression

$$\iota(a) = \sum_{i\in I} f_i(a)e_i$$

defines the necessary family of functions $f_i : M \to R$. □

Exercise 3.29: Let P be a projective R-module. Show that one can can find a *finite* index set I satisfying condition (i) of the Dual Basis Lemma iff P is finitely generated.

3.5.4. *Projective versus free.*

Having established some basic facts about projective modules, we should now seek examples in nature: which modules are projective? Note that by Exercise 3.25 any free module is projective. But this surely counts as a not very interesting example! Indeed the following turns out to be one of the deepest questions of the subject.

Question 1. *When is a projective module free?*

We want to give examples to show that the answer to Question 1 is *not* "always". But even by giving examples one wades into somewhat deep waters. The following is the one truly "easy" example of a non-free projective module I know.

Example: Suppose R_1 and R_2 are nontrivial rings. Then the product $R = R_1 \times R_2$ admits nonfree projective modules. Indeed, let P be the ideal $R_1 \times \{0\}$ and Q the

[14]Note that this part of the proof redeems the pure algebraist: this the decomposition afforded by the pair of orthogonal idempotents $P, 1-P$.

ideal $\{0\} \times R_2$. Since $R = P \oplus Q$, P and Q are projective. On the other hand P cannot be free because taking $e := (0,1) \in R$, we have $eP = 0$, whereas $eF \neq 0$ for any nonzero free R-module F (and of course, Q is not free either for similar reasons).

One way to construe Question 1 is to ask for the class of rings over which every projective module is free, or over which every finitely generated projective module is free. I actually do not myself know a complete answer to this question, but there are many interesting and important special cases.

Recall the following result from undergraduate algebra.

Theorem 3.13. *A finitely generated module over a PID is free iff it is torsionfree.*

Of course submodules of torsionfree modules are torsionfree, so projective implies torsionfree. We deduce:

Corollary 3.14. *A finitely generated projective module over a PID is free.*

Theorem 3.13 does not extend to all torsionfree modules: for instance, the $\mathbb{Z}$-module $\mathbb{Q}$ is torsionfree but not free. However Corollary 3.14 *does* extend to all modules over a PID. The proof requires transfinite methods and is given in §3.10.

Recall that a ring R is local if it has a unique maximal ideal. It is convenient to reserve the notation $\mathfrak{m}$ for the unique maximal ideal of a local ring and speak of "the local ring $(R, \mathfrak{m})$". We want to show that every finitely generated projective module over a local ring is free. First a few preliminaries.

Let $f : R \to S$ be a homomorphism of rings. Then necessarily f induces a homomorphism $f^\times : R^\times \to S^\times$ on unit groups: if $xy = 1$, then $f(x)f(y) = f(1) = 1$, so units get mapped to units. But what about the converse: if $x \in R$ is such that $f(x)$ is a unit in S, must x be a unit in R?

It's a nice idea, but it's easy to see that this need not be the case. For instance, let $a > 1$ be any positive integer. Then a is not a unit of $\mathbb{Z}$, but for each prime $p > a$, the image of a in the quotient ring $\mathbb{Z}/p\mathbb{Z}$ is a unit. Too bad! Let us not give up so soon: a conjecture may fail, but a definition cannot: say a homomorphism $f : R \to S$ of rings is **unit-faithful** if for all $x \in R$, $f(x) \in S^\times \implies x \in R^\times$.

Lemma 3.15. *If $(R, \mathfrak{m})$ is a local ring, the quotient map $q : R \to R/\mathfrak{m}$ is unit-faithful.*

Proof. An element of any ring is a unit iff it is contained in no maximal ideal, so in a local ring we have $R^\times = R \setminus \mathfrak{m}$. Moreover, since $\mathfrak{m}$ is maximal, $R/\mathfrak{m}$ is a field. Thus, for $x \in R$,

$$q(x) \in (R/\mathfrak{m})^\times \iff x \notin \mathfrak{m} \iff x \in R^\times.$$

□

Later we will see a generalization: if J is any ideal contained the *Jacobson radical* of R, then $q : R \to R/J$ is unit-faithful.

Theorem 3.16. *A finitely generated projective module over a local ring is free.*

Proof. Let P be a finitely generated projective module over the local ring $(R, \mathfrak{m})$. We may find Q and $n \in \mathbb{Z}^+$ such that $P \oplus Q = R^n$. Now tensor with $R/\mathfrak{m}$: we get a direct sum decomposition $P/\mathfrak{m}P \oplus Q/\mathfrak{m}Q = (R/\mathfrak{m})^n$. Since $R/\mathfrak{m}$ is a field, all $R/\mathfrak{m}$-modules are free. Choose bases $\{\overline{p_i}\}$ for $P/\mathfrak{m}P$ and $\{\overline{q_j}\}$ for $Q/\mathfrak{m}Q$, and for all i, j, lift each $\overline{p_i}$ to an element p_i of P and each $\overline{q_j}$ to an element q_j of Q. Consider the $n \times n$ matrix A with coefficients in R whose columns are $p_1, \ldots, p_a, q_1, \ldots, q_b$. The reduction modulo $\mathfrak{m}$ of A is a matrix over the field $R/\mathfrak{m}$ whose columns form a basis for $(R/\mathfrak{m})^n$, so its determinant is a unit in $(R/\mathfrak{m})^\times$. Since $\det(M \pmod{\mathfrak{m}}) = \det(M) \pmod{\mathfrak{m}}$, Lemma 3.15 implies that $\det(M) \in R^\times$, i.e., M is invertible. But this means that its columns are linearly independent, so $p_1, \ldots, p_a$, *a priori* only a generating set for the R-module P, is in fact a basis. □

Once again, in Section 3.9 this result wll be improved upon: it is a celebrated theorem of Kaplansky that *any* projective module over a local ring is free.

Much more interesting is an example of a finitely generated projective, nonfree module over an integral domain. Probably the first such examples come from non-principal ideals in rings of integers of number fields with class number greater than 1. To give such an example with proof of its projectivity this early in the day, we require a little preparation.[15]

Two ideals I and J in a ring R are **comaximal** if $I + J = R$. More generally, a family $\{I_i\}$ of ideals in a ring is **pairwise comaximal** if for all $i \neq j$, $I + J = R$.

Lemma 3.17. *Let I, J, $K_1, \ldots, K_n$ be ideals in the ring R.*
a) We have $(I + J)(I \cap J) \subset IJ$.
b) If I and J are comaximal, $IJ = I \cap J$.
c) If $I + K_i = R$ for all $1 \leq i \leq n$, then $I + K_1 \cdots K_n = R$.

Proof. a) $(I + J)(I \cap J) = I(I \cap J) + J(I \cap J) \subset IJ + IJ = IJ$.
b) If $I + J = R$, the identity of part a) becomes $I \cap J \subset IJ$. Since the converse inclusion is valid for all I and J, the conclusion follows. c) We go by induction on n, the case $n = 1$ being trivial. If $n = 2$, then for $i = 1, 2$, let $a_i \in I$ and $b_i \in K_i$ be such that $1 = a_i + b_i$. Then

$$1 = a_1 + a_2 - a_1 a_2 + b_1 b_2 \in I + K_1 K_2.$$

Now assume that $n \geq 3$ and that the result holds for $n - 1$. By induction, $I + K_1 \cdots K_{n-1} = R$ and by hypothesis $I + K_n = R$, so by the $n = 2$ case $I + K_1 \cdots K_n = R$. □

Proposition 3.18. *Let I and J be comaximal ideals in a domain R, and consider the R-module map $q : I \oplus J \to R$ given by $(x, y) \mapsto x + y$. Then:*
a) The map q is surjective.
b) $\mathrm{Ker}(q) = \{(x, -x) \mid x \in I \cap J\}$, hence is isomorphic as an R-module to $I \cap J$.
c) We have an isomorphism of R-modules

$$I \oplus J \cong IJ \oplus R.$$

d) Thus if IJ is a principal ideal, I and J are projective modules.

[15]Here we wish to acknowledge our indebtedness to K. Conrad: we took our inspiration for Proposition 3.18 and the following Exercise from Example 3.1 of http://www.math.uconn.edu/∼kconrad/blurbs/linmultialg/splittingmodules.pdf.

Proof. It is clear that for any ideals I and J, the image of the map q is the ideal $I + J$, and we are assuming $I + J = R$, whence part a).
Part b) is essentially immediate: details are left to the reader.
Combining parts a) and b) we get a short exact sequence

$$0 \to I \cap J \to I \oplus J \to R \to 0.$$

But R is free, hence projective, and thus the sequence splits, giving part c). Finally, a nonzero principal ideal (x) in a domain R is isomorphic as an R-module to R itself: indeed, multiplication by x gives the isomorphism $R \to (x)$. So if IJ is principal, $I \oplus J \cong R^2$ and I and J are both direct summands of a free module. □

In particular, if we can find in a domain R two comaximal nonprincipal ideals I and J with IJ principal, then I and J are finitely generated projective nonfree R-modules. The following exercise asks you to work through an explicit example.

Exercise 3.30: Let $R = \mathbb{Z}[\sqrt{-5}]$, and put

$$\mathfrak{p}_1 = \langle 3, 1 + \sqrt{-5} \rangle, \ \mathfrak{p}_2 = \langle 3, 1 - \sqrt{-5} \rangle.$$

a) Show that $R/\mathfrak{p}_1 \cong R/\mathfrak{p}_2 \cong \mathbb{Z}/3\mathbb{Z}$, so $\mathfrak{p}_1$ and $\mathfrak{p}_2$ are maximal ideals of R.
b) Show that $\mathfrak{p}_1 + \mathfrak{p}_2 = R$ (or equivalently, that $\mathfrak{p}_1 \neq \mathfrak{p}_2$).
c) Show that $\mathfrak{p}_1\mathfrak{p}_2 = (3)$.
d) Show that neither $\mathfrak{p}_1$ nor $\mathfrak{p}_2$ is principal.
(Suggestion: show that if $\mathfrak{p}_1 = (x + \sqrt{-5}y)$ then $\mathfrak{p}_2 = (x - \sqrt{-5}y)$ and thus there are integers x, y such that $x^2 + 5y^2 = \pm 3$.)
e) Conclude that $\mathfrak{p}_1$ and $\mathfrak{p}_2$ are (in fact isomorphic) nonfree finitely generated projective modules over the domain R.
f) Show that $\mathfrak{p}^2$ is principal, and thus that the class of $\mathfrak{p}$ in $\widetilde{K_0(R)}$ is 2-torsion.

This construction looks very specific, and the number-theoretically inclined reader is warmly invited to play around with other quadratic rings and more general rings of integers of number fields to try to figure out what is really going on. From our perspective, we will (much later on) gain a deeper understanding of this in terms of the concepts of invertible ideals, the Picard group and Dedekind domains.

Example: Let X be a compact space, and let $C(X)$ be the ring of continuous real-valued functions on X. The basic structure of these rings is studied in §5.2. Let $E \to X$ be a real topological vector bundle over X. Then the group $\Gamma(E)$ of global sections is naturally a module over $C(X)$. In fact it is a finitely generated projective module, and all finitely generated projective $C(X)$-modules arise faithfully in this way: the global section functor gives a categorical equivalence between vector bundles on X and finitely generated projective modules over $C(X)$. This is a celebrated theorem of R.G. Swan, and Section X is devoted to giving a self-contained discussion of it, starting from the definition of a vector bundle. In particular, via Swan's Theorem basic results on the tangent bundles of compact manifolds translate into examples of finitely generated projective modules: for instance, an Euler characteristic argument shows that the tangent bundle of any even-dimensional sphere S^{2k} is nontrivial, and thus $\Gamma(TS^{2k})$ is a finitely generated nonfree $C(S^{2k})$-module! Following Swan, we will show that examples of nonfree projective modules over more traditional rings like finitely generated $\mathbb{R}$-algebras

follow from examples like these.

Example: Let k be a field and $R = k[t_1, \ldots, t_n]$ be the polynomial ring over k in n indeterminates. When $n = 1$, R is a PID, so indeed every finitely generated R-module is projective. For $n > 1$, the situation is much less clear, but the problem of freeness of finitely generated projective R-modules can be stated geometrically as follows: is any algebraic vector bundle on affine n-space $\mathbb{A}^n_{/k}$ algebraically trivial? When $k = \mathbb{C}$, the space $\mathbb{A}^n_{/\mathbb{C}} = \mathbb{C}^n$ in its usual, Euclidean topology is contractible, which by basic topology implies that any continuous $\mathbb{C}$-vector bundle on $\mathbb{A}^n$ is (continuously) trivial. Moreover, relatively classical complex variable theory shows that any *holomorphic* vector bundle on $\mathbb{A}^n$ is (holomorphically) trivial. But asking the transition functions and the trivialization to be algebraic – i.e., polynomial functions – is a much more stringent problem. In his landmark 1955 paper FAC, J.-P. Serre noted that this natural problem remained open for algebraic vector bundles: he was able to prove only the weaker result that a finitely generated projective R-module M is **stably free** – i.e., there exists a finitely generated free module M such that $M \oplus F$ is free. This became known as **Serre's Conjecture** (to his dismay) and was finally resolved independently in 1976 by D. Quillen [Qui76] and A. Suslin [Su76]: indeed, every finitely generated projective R-module is free. Quillen received the Fields Medal in 1978. Fields Medals are not awarded for the solution of any single problem, but the prize committee writes an official document describing the work of each winner that they found particularly meritorious. In this case, it was made clear that Quillen's resolution of Serre's Conjecture was one of the reasons he received the prize. All this for modules over a polynomial ring!

For more information on Serre's Conjecture, the reader could do no better than to consult a recent book of T.Y. Lam [Lam06].

Exercise 3.31 ($K_0(R)$): From a commutative ring R, we will construct another commutative ring $K_0(R)$ whose elements correspond to formal differences of finite rank projective modules. More precisely:
a) Let $M_0(R)$ denote the set of all isomorphism classes of finitely generated projective modules. For finitely generated projective modules P and Q we define

$$[P] + [Q] = [P \oplus Q],$$
$$[P] \cdot [Q] = [P \otimes Q].$$

Check that this construction is well-defined on isomorphism classes and endows $M_0(R)$ with the structure of a commutative semiring with unity. What are the additive and mulitplicative identity elements?
b) Define $K_0(R)$ as the Grothendieck group of $M_0(R)$, i.e., as the group completion of the commutative monoid $M_0(R)$. Convince yourself that $K_0(R)$ has the structure of a semiring. The elements are of the form $[P] - [Q]$, and we have $[P_1] - [Q_1] = [P_2] - [Q_2] \iff$ there exists a finitely generated projective R-module M with

$$P_1 \oplus Q_2 \oplus M \cong P_2 \oplus Q_1 \oplus M.$$

In particular, if P and Q are projective modules, then $[P] = [Q]$ in $K_0(R)$ iff $[P]$ and $[Q]$ are **stably isomorphic**, i.e., iff they become isomorphic after taking the direct sum with some other finitely generated projective module M. c) Show that we also have $[P] = [Q]$ iff there exists a finitely generated *free* module R^n such that

$P \oplus R^n \cong Q \oplus R^n$. In particular, $[P] = [0] = 0$ iff P is **stably free**: there exists a finitely generated free module F such that $P \oplus F$ is free.
d) Show that $M_0(R)$ is cancellative iff every stably free finitely generated projective module is free.
e)* Find a ring R admitting a finitely generated projectve module which is stably free but not free.
f) Show that the mapping $R^n \mapsto [R^n]$ induces an injective homomorphism of rings $\mathbb{Z} \to K_0(R)$. Define $\tilde{K}_0(R)$ to be the quotient $K_0(R)/\mathbb{Z}$. Show that if R is a PID then $\tilde{K}_0(R) = 0$.

3.6. **Injective modules.**

3.6.1. *Basic equivalences.*

Although we will have no use for them in the sequel of these notes, in both commutative and (especially) homological algebra there is an important class of modules "dual" to the projective modules. They are characterized as follows.

Proposition 3.19. *For a module E over a ring R, the following are equivalent:*
(ii) If $\iota : M \to N$ is an injective R-module homomorphism and $\varphi : M \to E$ is any homomorphism, there exists at least one extension of φ to a homomorphism $\Phi : N \to E$.
(iii) If $M \hookrightarrow N$, the natural map $\mathrm{Hom}(N, E) \to \mathrm{Hom}(M, E)$ is surjective.
(iv) The (contravariant) functor $\mathrm{Hom}(\ , E)$ is exact.
(v) Any short exact sequence of R-modules

$$0 \to E \xrightarrow{\iota} M \to N \to 0$$

splits: there exists an R-module map $\pi : M \to E$ such that $\pi \circ \iota = 1_E$ and thus an internal direct sum decomposition $M = \iota(E) \oplus \ker(\pi) \cong E \oplus N$.
*A module satisfying these equivalent conditions is called **injective**.*

Exercise 3.33: Prove Proposition 3.19.

Exercise 3.34: Show that an R-module E is injective iff whenever E is a submodule of a module M, E is a direct summand of M.

Remark: Note that the set of equivalent conditions starts with (ii)! This is to facilitate direct comparison to Proposition 3.10 on projective modules. Indeed, one should check that each of the properties (ii) through (v) are *duals* of the corresponding properties for projective modules: i.e., they are obtained by reversing all arrows. The difficulty here with property (i) is that if one literally reverses the arrows in the definition of free R-module to arrive at a "cofree" R-module, one gets a definition which is unhelpfully strong: the "cofree R-module on a set X" does not exist when $\#X > 1$! This can be remedied by giving a more refined definition of *cofree* module. For the sake of curiosity, we will give it later on in the exercises, but to the best of my knowledge, cofree R-modules by any definition do not play the fundamental role that free R-modules do.

Exercise 3.35: Show that every module over a field is injective.

Exercise 3.36: Show that $\mathbb{Z}$ is *not* an injective $\mathbb{Z}$-module. (Thus injectivity is

the first important property of modules that is not satisfied by free modules.)

Exercise 3.37: Let $\{M_i\}_{i \in I}$ be any family of R-modules and put $M = \prod_{i \in I} M_i$. Show that M is injective iff M_i is injective for all $i \in I$.

Exercise 3.38: For a ring R, show TFAE:
(i) R is **absolutely projective**: every R-module is projective.
(ii) R is **absolutely injective**: every R-module is injective.

3.6.2. *Baer's Criterion.*

Theorem 3.20. *(Baer's Criterion* [Bae40]*) For a module E over a ring R, TFAE:*
(i) E is injective.
(ii) For every ideal nonzero I of R, every R-module map $\varphi : I \to E$ extends to an R-module map $\Phi : R \to E$.

Proof. (i) $\implies$ (ii): this is a special case of condition (ii) of Proposition 3.19: take $M = I$, $N = R$.
(ii) $\implies$ (i): Let M be an R-submodule of N and $\varphi : M \to E$ an R-module map. We need to show that φ may be extended to N. Now the set $\mathcal{P}$ of pairs (N', φ') with $M \subset N' \subset N$ and $\varphi : N' \to E$ a map extending φ is nonempty and has an evident partial ordering, with respect to which the union of any chain of elements in $\mathcal{P}$ is again an element of $\mathcal{P}$. So by Zorn's Lemma, there is a maximal element $\varphi' : N' \to E$. Our task is to show that $N' = N$.

Assume not, and choose $x \in N \setminus N'$. Put

$$I = (N' : x) = \{r \in R \mid rx \subset N'\};$$

one checks immediately that I is an ideal of R (a generalization to modules of the *colon ideal* we have encountered before). Consider the composite map

$$I \stackrel{\cdot x}{\to} N' \stackrel{\varphi}{\to} E;$$

by our hypothesis, this extends to a map $\psi : R \to E$. Now put $N'' = \langle N', x \rangle$ and define[16] $\varphi'' : N'' \to E$ by

$$\varphi''(x' + rx) = \varphi'(x') + \psi(r).$$

Thus φ'' is an extension of φ' to a strictly larger submodule of N than N', contradicting maximality. □

Exercise 3.39: Verify that the map φ'' is well-defined.

3.6.3. *Divisible modules.*

Recall that a module M over a domain R is **divisible** if for all $r \in R^\bullet$ the endomorphism $r\bullet : M \to M, x \mapsto rx$, is surjective. Further, we define M to be **uniquely divisible** if for all $r \in R^\bullet$, the endomorphism $r\bullet : M \to M$ is a bijection.

Example: The $\mathbb{Z}$-modules $\mathbb{Q}$ and $\mathbb{Q}/\mathbb{Z}$ are divisible. $\mathbb{Q}$ is moreover uniquely divisible but $\mathbb{Q}/\mathbb{Z}$ is not.

[16]Since N'' need not be the direct sum of N' and $\langle x \rangle$, one does need to check that φ'' is well-defined; we ask the reader to do so in an exercise following the proof.

Exercise 3.40: Show that a divisible module is uniquely divisible iff it is torsionfree.

Exercise 3.41: a) Show that a quotient of a divisible module is divisible.
b) Show that arbitrary direct sums and direct products of divisible modules are divisible.

Exercise 3.42: Let R be a domain with fraction field K.
a) Show that K is a uniquely divisible R-module.
b) Let M be any R-module. Show that the natural map $M \to M \otimes_R K$ is injective iff M is torsionfree.
c) Show that for any R-module M, $M \otimes_R K$ is uniquely divisible.
d) Show that K/R is divisible but not uniquely divisible.

Exercise 3.43:
a) Show that a $\mathbb{Z}$-module is uniquely divisible iff it can be endowed with the (compatible) structure of a $\mathbb{Q}$-module, and if so this $\mathbb{Q}$-module structure is unique.
b) Show that a $\mathbb{Z}$-module M is a subgroup of a uniquely divisible divisible $\mathbb{Z}$-module iff it is torsionfree.

Proposition 3.21. *Let R be a domain and E an R-module.*
a) If E is injective, it is divisible.
b) If E is torsionfree and divisible, it is injective.
c) If R is a PID and E is divisible, it is injective.

Proof. a) Let $r \in R^\bullet$. For $x \in E$, consider the R-module homomorphism $\varphi : rR \to E$ given by $r \mapsto x$. Since E is injective, this extends to an R-module map $\varphi : R \to E$. Then $r\varphi(1) = \varphi(r \cdot 1) = \varphi(r) = x$, so $r\bullet$ is surjective on E.
b) Let I be a nonzero ideal of R and $\varphi : I \to E$ be an R-module map. For each $a \in I^\bullet$, there is a unique $e_a \in E$ such that $\varphi(a) = ae_a$. For $b \in I^\bullet$, we have

$$bae_a = b\varphi(a) = \varphi(ba) = a\varphi(b) = abe_b;$$

since E is torsionfree we conclude $e_a = e_b = e$, say. Thus we may extend φ to a map $\Phi : R \to E$ by $\Phi(r) = re$. Thus E is injective by Baer's Criterion.
c) As above it is enough to show that given a nonzero ideal I of R, every homomorphism $\varphi : I \to E$ extends to a homomorphism $R \to E$. Since R is a PID, we may write $I = xR$ for $x \in R^\bullet$. Then, as in part a), one checks that φ extends to Φ iff multiplication by x is surjective on M, which it is since M is divisible. □

By combining Proposition 3.21 with Exercise 3.42, we are able to show an important special case of the desired fact that every R-module can be realized as a submodule of an injective module. Namely, if M is a torsionfree module over a domain R, then M is a submodule of the uniquely divisible – hence injective – module $M \otimes_R K$.

Exercise 3.44: Let $n \in \mathbb{Z}^+$.
a) Show that as a $\mathbb{Z}$-module $\mathbb{Z}/n\mathbb{Z}$ is not divisible hence not injective.
b) Show that as a $\mathbb{Z}/n\mathbb{Z}$ module $\mathbb{Z}/n\mathbb{Z}$ is divisible iff n is a prime number.
c) Show that $\mathbb{Z}/n\mathbb{Z}$ is always injective as a $\mathbb{Z}/n\mathbb{Z}$-module.

Exercise 3.45: Let $R = \mathbb{Z}[t]$ and let K be its fraction field. Show that the R-module K/R is divisible but not injective.

Exercise 3.46: Let R be a domain with fraction field K.
a) If $R = K$, (of course) all R-modules are both injective and projective.
b) If $R \neq K$, the only R-module which is both projective and injective is 0.

3.6.4. *Enough injectives.*

The idea of this section is to pursue the dual version of the statement "Every R-module is a quotient of a projective module": namely we wish to show that every R-module is a *submodule* of an injective module. This is a good example of a statement which remains true upon dualization but becomes more elaborate to show. The projective version is almost obvious: indeed, we have the stronger result that every module is a quotient of a *free* module, and – as we have seen – to realize M as a quotent of a free R-module is equivalent to simply choosing a set of generators for M. (But again, if we choose the most obvious definition of "cofree", then this statement will be false.)

Let k be a ring, R a k-algebra, M an R-module and N a k-module. Consider the commutative group $\mathrm{Hom}_k(M, N)$. We may endow it with the structure of an R-module as follows: for $r \in R$ and $f \in \mathrm{Hom}_{\mathbb{Z}}(M, N)$, $(rf)(x) := f(rx)$.

Consider the special case $k = \mathbb{Z}$ and $N = \mathbb{Q}/\mathbb{Z}$ of the above construction. It gives $\mathrm{Hom}_{\mathbb{Z}}(M, \mathbb{Q}/\mathbb{Z})$ the structure of an R-module, which we denote by M^* and call the **Pontrjagin dual** of M.[17] Because $\mathbb{Q}/\mathbb{Z}$ is an injective $\mathbb{Z}$-module, the (contravariant) functor $M \mapsto M^*$ – or in other words $\mathrm{Hom}_{\mathbb{Z}}(\ , \mathbb{Q}/\mathbb{Z})$ – is exact.[18] In particular, if $f : M \to N$ is an R-module map, then f injective implies f^* surjective and f surjective implies f^* injective.

As is often the case for "duals", we have a natural map $M \to M^{**}$: namely $x \mapsto (f \mapsto f(x))$.

Lemma 3.22. *For any R-module M, the natural map $\Psi_M : M \to M^{**}$ is injective.*

Proof. Seeking a contradiction, let $x \in M^\bullet$ be such that $\Psi(x) = 0$. Unpacking the definition, this means that for all $f \in \mathrm{Hom}_{\mathbb{Z}}(M, \mathbb{Q}/\mathbb{Z})$, $f(x) = 0$. But since $\mathbb{Q}/\mathbb{Z}$ is an injective $\mathbb{Z}$-module, it suffices to find a nontrivial homomorphism $\mathbb{Z}x \to \mathbb{Q}/\mathbb{Z}$, and this is easy: if x has finite order $n > 1$, we may map x to $\frac{1}{n}$, whereas if x has infinite order we may map it to any nonzero element of $\mathbb{Q}/\mathbb{Z}$. □

Lemma 3.23. *Every $\mathbb{Z}$-module M can be embedded into an injective $\mathbb{Z}$-module.*

Proof. Let $I \subset M$ be a generating set and let $\bigoplus_{i \in I} \mathbb{Z} \to M$ be the corresponding surjection, with kernel K, so $M \cong (\bigoplus_{i \in I} \mathbb{Z})/K$. The natural map $\bigoplus_{i \in I} \mathbb{Z} \hookrightarrow \bigoplus_{i \in I} \mathbb{Q}$ induces an injection $M \hookrightarrow (\bigoplus_{i \in I} \mathbb{Q})/K$, and the latter $\mathbb{Z}$-module is divisible, hence injective since $\mathbb{Z}$ is a PID. □

Lemma 3.24. *(Injective Production Lemma) Let R be a k-algebra, E an injective k-module and F a free R-module. Then $\mathrm{Hom}_k(F, E)$ is an injective R-module.*

[17] Recall that the notation $M^\vee$ has already been taken: this is the *linear dual* $\mathrm{Hom}_R(M, R)$.

[18] Here we are using the (obvious) fact that a sequence of R-modules is exact iff it is exact when viewed merely as a sequence of $\mathbb{Z}$-modules.

Proof. We will show that the functor $\mathrm{Hom}_R(\ , \mathrm{Hom}_k(F,E))$ is exact. For any R-module M, the adjointness of $\otimes$ and Hom gives

$$\mathrm{Hom}_R(M, \mathrm{Hom}_k(F,E)) = \mathrm{Hom}_k(F \otimes_R M, E)$$

so we may look at the functor $M \mapsto \mathrm{Hom}_k(F \otimes_R M, E)$ instead. This is the composition of the functor $M \mapsto F \otimes_R M$ with the functor $N \mapsto \mathrm{Hom}_k(N,E)$. But both functors are exact – in the former case a moment's thought shows this to be true, and the latter case is one of our defining properties of injective modules. □

Remark: Soon enough we will define a *flat* R-module to be an R-module N such that the functor $M \mapsto M \otimes_R N$ is exact. Then Lemma 3.24 can be rephrased with the hypothesis that F is a flat R-module, and (since as we have just seen, free R-modules are flat) this gives a somewhat more general result.

Theorem 3.25. *Every R-module can be embedded into an injective R-module.*

Proof. Let M be an R-module. Viewing M as a $\mathbb{Z}$-module, by Lemma 3.23 there is an injective $\mathbb{Z}$-module E_1 and a $\mathbb{Z}$-module map $\varphi_1 : M \hookrightarrow E_1$. Further, by Lemma 3.24, $\mathrm{Hom}_{\mathbb{Z}}(R, E_1)$ is an injective R-module. Now consider the R-module map

$$\varphi : M \to \mathrm{Hom}_{\mathbb{Z}}(R, E_1),\ x \mapsto (r \mapsto \varphi_1(rx)).$$

We claim that φ is a monomorphism into the injective R-module $\mathrm{Hom}_{\mathbb{Z}}(R, E_1)$. Indeed, if $\varphi(x) = 0$ then for all $r \in R$, $\varphi_1(rx) = 0$. In particular $\varphi_1(x) = 0$, so since φ_1 is a monomorphism, we conclude $x = 0$. □

Exercise 3.47: Let us say that a $\mathbb{Z}$-module is **cofree** if it is of the form F^* for a free $\mathbb{Z}$-module F. Then the proof of Lemma 3.23 gives the stronger statement that every $\mathbb{Z}$-module can be embedded into a cofree $\mathbb{Z}$-module. Formulate a definition of **cofree R-module** so that the proof of Theorem 3.25 gives the stronger statement that every R-module can be embedded into a cofree R-module. (Hint: remember to pay attention to the difference between direct sums and direct products.)

3.6.5. *Essential extensions and injective envelopes.*

The results of this section are all due to B. Eckmann and A. Schopf [ES53].

Proposition 3.26. *Let M be an R-module and $M \subset_R N$ an R-submodule. TFAE:*
(i) If X is any nonzero R-submodule of N, then $X \cap M$ is nonzero.
(ii) If $x \in N^\bullet$, there exists $r \in R$ such that $rx \in M^\bullet$.
(iii) If $\varphi : N \to Y$ is an R-module map, then φ is injective iff $\varphi|_M$ is injective.
An extension $M \subset N$ satisfying these equivalent conditions is called ***essential****.*

Proof. (i) $\implies$ (ii): Apply (i) with $X = \langle x \rangle$.
(ii) $\implies$ (iii): Assuming (ii), let $\varphi : N \to Y$ be a homomorphism with $\varphi|_M$ is injective. It is enough to show that φ is injective. Seeking a contradiction, let $x \in N^\bullet$ be such that $\varphi(x) = 0$. By (ii), there exists $r \in R$ such that $rx \in M^\bullet$. But then by assumption $r\varphi(x) = \varphi(rx) \neq 0$, so $\varphi(x) \neq 0$, contradiction.
(iii) $\implies$ (i): We go by contraposition. Suppose there exists a nonzero submodule X of N such that $X \cap M = 0$. Then the map $\varphi : N \to N/X$ is not an injection but its restriction to M is an injection. □

Proposition 3.27. *(Tower Property of Essential Extensions) Let $L \subset M \subset N$ be R-modules. Then $L \subset N$ is an essential extension iff $L \subset M$ and $M \subset N$ are both essential extensions.*

Proof. Suppose first that $L \subset N$ is an essential extension. Then for any nonzero submodule X of N, $X \cap L \neq 0$. In particular this holds for $X \subset M$, so $L \subset M$ is essential. Moreover, since $L \subset M$, $X \cap L \neq 0$ implies $X \cap M \neq 0$, so $M \subset N$ is essential. Conversely, suppose $L \subset M$ and $M \subset N$ are both essential, and let X be a nonzero submodule of N. Then $X \cap M$ is a nonzero submodule of M and thus $(X \cap M) \cap L = X \cap L$ is a nonzero submodule of L. So $L \subset N$ is essential. □

So why are we talking about essential extensions when we are supposed to be talking about injective modules? The following result explains the connection.

Theorem 3.28. *For an R-module M, TFAE:*
(i) M is injective.
(ii) M has no proper essential extensions: i.e., if $M \subset N$ is an essential extension, then $M = N$.

Proof. (i) $\implies$ (ii): Let M be injective and $M \subsetneq N$. Then M is a direct summand of N: there exists M' such that $M \oplus M' = N$. Thus M has zero intersection with M', and by criterion (ii) of Proposition 3.26, we must have $M' = 0$ and thus $M = N$.
(ii) $\implies$ (i): It suffices to show: if N is an R-module and $M \subset N$, then M is a direct summand of N. Now consider the family of submodules M' of N with the property that $M \cap M' = 0$. This family is partially ordered by inclusion, nonempty, and closed under unions of chains, so by Zorn's Lemma there exists a maximal such element M'. Now consider the extension $M \hookrightarrow N/M'$: we claim it is essential. Indeed, if not, there exists $x \in N \setminus M'$ such that $\langle M', x \rangle \cap M = 0$, contradicting maximality of M'. But by hypothesis, M has no proper essential extensions: thus $M = N/M'$, i.e., $M \oplus M' = N$ and M is a direct summand of N. □

We say that an extension $M \subset N$ is **maximal essential** if it is essential and there is no proper extension N' of N such that $M \subset N'$ is essential. Combining Proposition 3.27 and Theorem 3.28 yields the following important result.

Theorem 3.29. *For an essential extension $M \subset N$ of R-modules, TFAE:*
(i) $M \subset N$ is maximal essential.
(ii) N is injective.

Exercise 3.48: To be sure you're following along, prove Theorem 3.29.

Once again we have a purpose in life – or at least, this subsubsection of it – we would like to show that every R-module admits a maximal essential extension and that such extensions are unique up to isomorphism over M. Moreover, a plausible strategy of proof is the following: let M be an R-module. By Theorem 3.25 there exists an extension $M \subset E$ with E injective. Certainly this extension need not be essential, but we may seek to construct within it a maximal essential subextension N and then hope to show that $M \subset E'$ is injective.

Theorem 3.30. *Let M be an R-module and $M \subset E$ an extension with E injective. Let $\mathcal{P}$ be the set of all essential subextensions N of $M \subset E$. Then:*
a) $\mathcal{P}$ contains at least one maximal element.
b) Every maximal element E' of $\mathcal{P}$ is injective.

Proof. The proof of part a) is the usual Zorn's Lemma argument: what we need to check is that the union N of any chain $\{N_i\}$ of essential subextensions is again

an essential subextension. Suppose for a contradiction that there exists a nonzero submodule X of N such that $X \cap M = 0$. Choose $x \in X^\bullet$ and put $X' = \langle x \rangle$. Then $X' \subset N_i$ for some i and $X' \cap M \subset X \cap M = 0$, contradicting the essentialness (?!) of the extension $M \subset N_i$.
Now let E' be a maximal essential *subextension* of $M \subset E$. We need to show that $M \subset E'$ is actually a maximal essential extension: so suppose there is an essential extension $E' \subset N$. Let $\iota : M \subset E' \subset N$ be the composite map. It is a monomorphism, so by the injectivity of E the injection $M \subset E$ extends to a homomorphism $\varphi : N \to E$. But $\varphi|_M$ is an injection and $M \subset N$ is an essential extension, so by condition (iii) of Proposition 3.26 this implies that φ itself is an injection. By maximality of E' among essential subextensions of $M \subset E$ we must have $E' = N$. □

For an R-module M, we say that an extension $M \subset E$ is an **injective envelope** (other common name: **injective hull**) of M if $M \subset E$ is a maximal essential extension; equivalently, an essential extension with E injective. Thus Theorem 3.30 shows that any R-module admits an injective envelope.

Proposition 3.31. *Let R be an integral domain with fraction field K. Then $R \subset K$ is an injective envelope of R.*

Exercise 3.49: Prove Proposition 3.31. (Suggestion: use the relationship between injective modules and divisible modules.)

Exercise 3.50: More generally, let M be a torsionfree module over a domain R. Show that $M \subset M \otimes_R K$ is an injective envelope of M.

Let us touch up our characterization of injective envelopes a bit.

Proposition 3.32. *(Equivalent Properties of an Injective Envelope) For an extension $M \subset E$ of R-modules, TFAE:*
(i) $M \subset E$ is a maximal essential extension.
(ii) $M \subset E$ is essential and E is injective.
(iii) E is minimal injective over M: there does not exist any proper subextension $M \subset E' \subset E$ with E' injective.

Proof. We have already seen that (i) $\iff$ (ii).
(ii) $\implies$ (iii): Assume that E is injective and E' is an injective subextension of $M \subset E$. Since E' is injective, there exists $N \subset E$ such that $E' \oplus N = E$. Moreover, $M \cap N \subset E' \cap N = 0$, so $M \cap N = 0$. Since $M \subset E$ is essential, we must have $N = 0$, i.e., $E' = E$.
(iii) $\implies$ (ii): Suppose that $M \subset E$ is minimal injective. The proof of Theorem 3.30 gives us a subextension E' of $M \subset E$ such that E' is injective and $M \subset E'$ is essential. Thus by minimality $E = E'$, i.e., $M \subset E$ is essential. □

Theorem 3.33. *(Uniqueness of Injective Envelopes) Let M be an R-module and let $\iota_1 : M \subset E_1$, $\iota_2 : M \subset E_2$ be two injective envelopes of M. Then E_1 and E_2 are isomorphic as R-module extensions of M: i.e., there exists an R-module isomorphism $\Phi : E_1 \to E_2$ such that $\Phi \circ \iota_1 = \iota_2$.*

Proof. Since $\iota_1 : M \to E_1$ is a monomorphism and E_2 is injective, the map $\iota_2 : M \to E_2$ extends to a map $\Phi : E_1 \to E_2$ such that $\Phi \circ \iota_1 = \iota_2$. Since the restriction

of Φ to the essential submodule M is a monomorphism, so is Φ. The image $\Phi(E_1)$ is an essential subextension of $M \subset E_2$, so by condition (iii) of Proposition 3.32 we must have $E_2 = \Phi(E_1)$. Thus $\Phi : E_1 \to E_2$ is an isomorphism. □

In view of Theorem 3.33, it is reasonable to speak of "the" injective envelope of M and denote it by $M \to E(M)$. Reasonable, that is, but not ideal: it is not true that any two injective envelopes are canonically isomorphic.[19] Otherwise put, formation of the injective envelope is not functorial. For more on this in a more general category-theoretic context, see [AHRT].

Exercise 3.51: Let M be a submodule of an injective module E. Show that E contains an isomorphic copy of the injective envelope $E(M)$.

Exercise 3.52: If $M \subset N$ is an essential extension of modules, then $E(M) = E(N)$.

3.7. **Flat modules.**

Suppose we have a short exact sequence

$$0 \to M' \to M \to M'' \to 0$$

of R-modules. If N is any R-module, we can tensor each element of the sequence with N, getting by functoriality maps

$$0 \to M' \otimes N \to M \otimes N \to M''\otimes \to 0.$$

Unfortunately this new sequence need not be exact. It is easy to see that it is **right exact**: that is, the piece of the sequence

$$M' \otimes N \to M \otimes N \to M'' \otimes N \to 0$$

remains exact. This follows because of the canonical "adjunction" isomorphism

$$\mathrm{Hom}(M \otimes N, P) = \mathrm{Hom}(M, \mathrm{Hom}(N, P))$$

and the left-exactness of the sequence $\mathrm{Hom}(\ , Y)$ for all R-modules Y. However, tensoring an injection need not give an injection. Indeed, consider the exact sequence

$$0 \to \mathbb{Z} \stackrel{[2]}{\to} \mathbb{Z}.$$

If we tensor this with $\mathbb{Z}/2\mathbb{Z}$, we get a sequence

$$0 \to \mathbb{Z}/2\mathbb{Z} \stackrel{[2]}{\to} \mathbb{Z}/2\mathbb{Z},$$

but now the map $\mathbb{Z} \otimes Z/2\mathbb{Z} \to \mathbb{Z} \otimes \mathbb{Z}/2\mathbb{Z}$ takes $n \otimes i \to (2n \otimes i) = n \otimes 2i = 0$, so is not injective.

Definition: A module M over a ring R is **flat** if the functor $N \mapsto N \otimes_R M$ is exact. This means, equivalently, that if $M \hookrightarrow M'$ then $M \otimes N \hookrightarrow M' \otimes N$, or also that tensoring a short exact sequence with M gives a short exact sequence.

It will probably seem unlikely at first, but in fact this is one of the most important and useful properties of an R-module.

[19] The situation here is the same as for "the" splitting field of an algebraic field extension or "the" algebraic closure of a field.

So, which R-modules are flat?

Proposition 3.34. *Let $\{M_i\}_{i \in I}$ be a family of R-modules. TFAE:*
(i) For all i, M_i is flat.
(ii) The direct sum $M = \bigoplus_i M_i$ is flat.

Exercise 3.53: Prove Proposition 3.34.

Proposition 3.35. *Let R be a domain. Then flat R-modules are torsionfree.*

Proof. We will prove the contrapositive. Suppose that $0 \neq m \in R[\text{tors}]$, and let $0 \neq r \in R$ be such that $rm = 0$ Since R is a domain, we have a short exact sequence

$$0 \to R \stackrel{[r]}{\to} R \to R/rR \to 0$$

and tensoring it with M gives

$$0 \to M \stackrel{[r]}{\to} M \to M/rM \to 0,$$

but since $rm = 0$ the first map is not injective. □

Proposition 3.36. *Projective R-modules are flat.*

Proof. A projective R-module is a module P such that there exists P' with $P \oplus P' \cong F$ a free module. Therefore, by Proposition 3.34, it is enough to show that free modules are flat. By abuse of notation, we will abbreviate the infinite direct sum of d copies of R as R^d. Since for any R-module M we have $M \otimes_R R^d = M^d$, it follows that tensoring a short exact sequence

$$0 \to M' \to M \to M'' \to 0$$

with $F = R^d$ just yields

$$0 \to (M')^d \to (M)^d \to (M'')^d \to 0.$$

This is still exact. □

3.8. **Nakayama's Lemma.**

3.8.1. *Nakayama's Lemma.*

Proposition 3.37. *Let M be a finitely generated R-module, I an ideal of R, and φ be an R-endomorphism of M such that $\varphi(M) \subset IM$. Then φ satisfies an equation of the form*

$$\varphi^n + a_{n-1}\varphi^{n-1} + \ldots + a_1\varphi + a_0 = 0,$$

with $a_i \in I$.

Proof. Let $x_1, \ldots, x_n$ be a set of generators for M as an R-module. Since each $\varphi(x_i) \in IM$, we may write $\varphi(x_i) = \sum_j a_{ij}x_j$, with $a_{ij} \in I$. Equivalently, for all i,

$$\sum_{j=1}^{n} (\delta_{ij}\varphi - a_{ij})x_j = 0.$$

By multiplying on the left by the adjoint of the matrix $M = (\delta_{ij}\varphi - a_{ij})$, we get that $\det(\delta_{ij}\varphi - a_{ij})$ kills each x_i, hence is the zero endomorphism of M. Expanding out the determinant gives the desired polynomial relation satisfied by φ. □

Exercise 3.54: Some refer to Prop. 3.37 as the Cayley-Hamilton Theorem. Discuss.

Theorem 3.38. *(Nakayama's Lemma) Let R be a ring, J an ideal of R, and M a finitely generated R-module such that $JM = M$.*
a) There exists $x \in R$ with $x \equiv 1 \pmod{J}$ such that $xM = 0$.
b) Suppose moreover that J is contained in every maximal ideal of R. Then $M = 0$.

Proof. Applying Proposition 3.37 to the identity endomorphism φ: gives $a_1, \ldots, a_n \in J$ such that for $x := 1 + a_1 + \ldots + a_n$, $xM = 0$ and $x \equiv 1 \pmod{J}$, proving part a). If moreover J lies in every maximal ideal $\mathfrak{m}$ of R, then $x \equiv 1 \pmod{)m}$ for all maximal ideals $\mathfrak{m}$, hence x lies in no maximal ideal of R. Therefore x is a unit and $xM = 0$ implies $M = 0$. □

Corollary 3.39. *Let R be a ring, J an ideal of R which is contained in every maximal ideal of R, M a finitely generated R-module and N a submodule of M such that $JM + N = M$. Then $M = N$.*

Proof. We have $J(M/N) = (JM + N)/N = M/N$. Applying Nakayama's Lemma to the finitely generated module M/N, we conclude $M/N = 0$, i.e., $N = M$. □

Corollary 3.40. *Let R be a ring, J an ideal of R which is contained in every maximal ideal of R, and M a finitely generated R-module. Let $x_1, \ldots, x_n \in M$ be such that their images in M/JM span M/JM as an R/J-module. Then the x_i's span M.*

Proof. Let $N = \langle x_1, \ldots, x_n \rangle_R$, and apply Corollary 3.39. □

Corollary 3.41. *Let R be a ring and J an ideal which is contained in every maximal ideal of R. Let M and N be R-modules, with N finitely generated, and let $u : M \to N$ be an R-module map. Suppose that the map $u_J : M/JM \to N/JN$ is surjective. Then u is surjective.*

Proof. Apply Nakayama's Lemma to J and N/M. □

Recall that an element x in a ring R such that $x^2 = x$ is called **idempotent**. Similarly, an ideal I of R such that $I^2 = I$ is called **idempotent**.

Exercise 3.55: Let R be a ring and I an ideal of R.
a) Suppose $I = (e)$ for an idempotent element e. Show that I is idempotent.
b) Give an example of a nonidempotent x such that (x) is idempotent.
c) Is every idempotent ideal generated by some idempotent element?

The last part of the preceding exercise is rather difficult. It turns out that the answer is negative in general: we will see later that counterexamples exist in any infinite *Boolean ring*. However under a relatively mild additional hypothesis the answer is affirmative.

Corollary 3.42. *Let R be any ring and I a* finitely generated *idempotent ideal of R. Then there exists an idempotent $e \in R$ such that $I = (e)$. In particular, in a Noetherian ring every idempotent ideal is generated by a single idempotent element.*

Exercise 3.56: Prove Corollary 3.42. (Hint: apply Theorem 3.38!)

3.8.2. *Hopfian modules.*

A group G is **Hopfian** if every surjective group homomorphism $f : G \to G$ is an isomorphism – equivalently, G is not isomorphic to any of its proper quotients.

This concept has some currency in combinatorial and geometric group theory. Some basic examples: any finite group is certainly Hopfian. A free group is Hopfian iff it is finitely generated, and more generally a finitely generated residually finite group is Hopfian. An obvious example of a non-Hopfian group is $\prod_{i=1}^{\infty} G$ for any nontrivial group G. A more interesting example is the **Baumslag-Solitar group**

$$B(2,3) = \langle x, y \mid yx^2y^{-1} = x^3 \rangle.$$

More generally, let $\mathcal{C}$ be a concrete category: that is, $\mathrm{Ob}\,\mathcal{C}$ is a class of sets and for all $X, Y \in \mathrm{Ob}\,\mathcal{C}$, $\mathrm{Hom}_{\mathcal{C}}(X,Y) \subset \mathrm{Hom}_{\mathrm{Set}}(X,Y)$, i.e., the morphisms between X and Y are certain functions from X to Y. We may define an object X in $\mathcal{C}$ to be **Hopfian** if every surjective endomorphism of X is an isomorphism.

Exercise 3.57:
a) (C. LaRue) Show that any finite object in a concrete category is Hopfian.
b) In the category of Sets, the Hopfian objects are precisely the finite sets.

Remark: Our discussion of "Hopfian objects" in categories more general than R-Mod is not particularly serious or well thought out. So far as I know there is not a completely agreed upon definition of a Hopfian object, but Martin Brandenburg has suggested (instead) the following: $X \in \mathcal{C}$ is Hopfian if every **extremal epimorphism** $X \to X$ is an isomorphism.

Theorem 3.43. *Let R be a ring and M a finitely generated R-module. Then M is a Hopfian object in the category of R-modules.*

Proof. ([M, p. 9]) Let $f : M \to M$ be a surjective R-map. We show f is injective.

There is a unique $R[t]$-module structure on M extending the given R-module structure and such that for all $m \in$M, $tm = f(m)$. Let $I = tR[t]$. By hypothesis $IM = M$, so by Nakayama's Lemma there exists $P(t) \in R[t]$ such that $(1 + P(t)t)M = 0$. Let $y \in \ker f$. Then

$$0 = (1 + P(t)t)y = y + P(t)f(y) = y + P(t)0 = y.$$

So f is injective. □

Exercise 3.58: Show that $(\mathbb{Q}, +)$ is a Hopfian $\mathbb{Z}$-module which is not finitely generated.

Exercise 3.59*: Do there exist Hopfian $\mathbb{Z}$-modules of all cardinalities? (An affirmative answer was claim in [Bau62], but it was announced in [Bau63] that the construction is not valid. So far as I know the problem remains open lo these many years later.)

3.8.3. *A variant.*

The results of this section are taken from [DM71, §I.1].

Proposition 3.44. *(Generalized Nakayama's Lemma) Let R be a ring, J an ideal of R and M a finitely generated R-module. TFAE:*

(i) $J + \operatorname{ann} M = R$.
(ii) $JM = M$.

Proof. (i) $\implies$ (ii): If $J + \operatorname{ann} M = R$, we may write $1 = x + y$ with $x \in J$, $y \in \operatorname{ann} M$, so that for all $m \in M$, $m = 1m = xm + ym = xm$. Thus $JM = M$.
(ii) $\implies$ (i): Conversely, suppose $M = \langle m_1, \ldots, m_n \rangle$. For $1 \leq i \leq n$, put $M_i = \langle m_i, \ldots, m_n \rangle$ and $M_{n+1} = 0$. We claim that for all $1 \leq i \leq n+1$ there exists $a_i \in J$ with $(1 - a_i)M \subset M_i$, and we will prove this by induction on n. We may take $a_1 = 0$. Having chosen $a_1, \ldots, a_i$, we have

$$(1 - a_i)M = (1 - a_i)JM = J(1 - a_i)M \subset M_i,$$

so there exist $a_{ij} \in J$ such that

$$(1 - a_i)m_j = \sum_{j=i}^{n} a_{ij} m_j,$$

or

$$(1 - a_i - a_{ii})m_i \in M_{i+1}.$$

Thus

$$\left(1 - (2a_i + a_{ii} - a_i^2 - a_i a_i i)\right) M = (1-a_i)(1-a_i-a_{ii})M \subset (1-a_i-a_{ii})M_i \subset M_{i+1},$$

and we may take

$$a_{i+1} = 2a_i + a_{ii} - a_i^2 - a_i a_i i.$$

So there is $a_n \in J$ such that $1 - a_n \in \operatorname{ann} M$, and thus $1 \in J + \operatorname{ann} M$. □

Exercise 3.60: Deduce part b) of Nakayama's Lemma from Proposition 3.44.

Corollary 3.45. *Let M be a finitely generated R-module such that $\mathfrak{m}M = M$ for all maximal ideals of R. Then $M = 0$.*

Exercise 3.61: Prove Corollary 3.45.

For an R-module M, we define its **trace ideal** to be the ideal $\mathcal{T}(M)$ of R generated by all the images $f(M)$ of R-module maps $f \in R^\vee = \operatorname{Hom}_R(M, R)$.

Theorem 3.46. *Let P be a finitely generated projective R-module. Then R splits as a direct product of rings:*

$$R = \mathcal{T}(P) \oplus \operatorname{ann} P.$$

Proof. Step 1: We show that $\mathcal{T}(P)$ and $\operatorname{ann} P$ are comaximal ideals of R, i.e., $\mathcal{T}(P) + \operatorname{ann} P = R$. By the Dual Basis Lemma (Proposition 3.12) and the following exercise, there exist $x_1, \ldots, x_n \in P$ and $f_1, \ldots, f_n \in P^\vee = \operatorname{Hom}_R(P, R)$ forming a dual basis: for all $x \in P$, $x = \sum_{i=1}^n f_i(x)x_i$. By its very definition we have $f_i(x) \in \mathcal{T}(P)$ for all i and x, hence $\mathcal{T}(P)P = P$. By the Generalized Nakayama's Lemma (Lemma 3.44) we have $\mathcal{T}(P) + \operatorname{ann} P = R$.

For any $a \in \operatorname{ann} P$, $f \in P^\vee$ and $x \in P$ we have $af(x) = f(ax) = f(0) = 0$: thus $\mathcal{T}(P) \cap \operatorname{ann} P = 0$. By comaximality, $\mathcal{T}(P) \cap \operatorname{ann} P = 0$ and the sum is direct. □

Corollary 3.47. *A nonzero finitely generated projective module over a connected ring R (i.e., without idempotents other than 0 and 1) is faithful.*

Exercise 3.62: Prove Corollary 3.47.

3.8.4. *Applications to modules over local rings.*

Lemma 3.48. *Let R be a ring and J an ideal which is contained in every maximal ideal of R, and let M be a finitely presented R-module. Suppose that:*
(i) M/JM is a free R/J-module, and
(ii) The canonical map $J \otimes_R M \to JM$ is injective.
Then M is a free R-module.

Proof. We may choose a family $\{x_i\}_{i \in I}$ of elements of M such that the images in M/JM give a R/J-basis. (Since M is finitely generated over R, M/JM is finitely generated over R/J, so the index set I is necessarily finite.) Consider the finitely generated free R-module $L = \bigoplus_{i \in I} R$, with canonical basis $\{e_i\}$. Let $u : L \to M$ be the unique R-linear mapping each e_i to x_i, and let $K = \ker(u)$. Since M is finitely *presented*, by Proposition 3.6 K is finitely generated. We have a commutative diagram with exact rows:

$$J \otimes K \to J \otimes L \to J \otimes M \to 0$$
$$0 \to K \to L \to M \to 0,$$

where each vertical map – $a : J \otimes K \to K$, $b : J \otimes L \to L$, $c : J \otimes M \to M$ – is the natural multiplication map. Our hypothesis is that the the map $J \otimes_R M \to JM$ is injective, so by the Snake Lemma we get an exact sequence

$$0 \to \operatorname{coker}(a) \to \operatorname{coker}(b) \xrightarrow{\overline{u}} \operatorname{coker}(c).$$

Now observe that $\operatorname{coker}(b) = (R/J) \otimes_R L$ and $\operatorname{coker}(c) = (R/J) \otimes_R M$, and by definition the mapping $u : L \to M$ gives, upon passage to the quotient modulo J, a mapping from one R/J-module basis to another. So $\overline{u}$ is an isomorphism and thus $\operatorname{coker}(a) = 0$, i.e., $K/JK = 0$. By Nakayama's Lemma we conclude $K = 0$, i.e., u gives an isomorphism from the free module L to M, so M is free. □

We can now prove the following result, which is one that we will build upon in our future studies of modules over commutative rings.

Theorem 3.49. *Let R be a ring with a unique maximal ideal $\mathfrak{m}$ – i.e., a* local ring. *For a* finitely presented *R-module M, TFAE:*
(i) M is free.
(ii) M is projective.
(iii) $M$is flat.
(iv) The natural map $\mathfrak{m} \otimes_R M \to \mathfrak{m}M$ is an injection.

Proof. Each of the implications (i) $\implies$ (ii) $\implies$ (iii) $\implies$ (iv) is immediate. Assume (iv). Then, since $\mathfrak{m}$ is maximal, $R/\mathfrak{m}$ is a field, so every $R/\mathfrak{m}$-module is free. Therefore Lemma 3.48 applies to complete the proof. □

3.9. **Ordinal Filtrations and Applications.**

3.9.1. *The Transfinite Dévissage Lemma.*

Let M be an R-module. By an **ordinal filtration** on M we mean an ordinal number α and for each $i \leq \alpha$ a submodule M_i of M satisfying all of the following:
(OF1) $M_0 = 0$, $M_\alpha = M$.
(OF2) For all $i, j \in \alpha + 1$, $i \leq j \implies M_i \subset M_j$.
(OF3) For all limit ordinals $i \leq \alpha$, $M_i = \bigcup_{j<i} M_j$.

So for instance, taking $\alpha = \omega = \{1, 2, 3, \ldots\}$ the first infinite ordinal, we recover the usual notion of an exhaustive filtration by submodules M_n, with the additional convention that $M_\omega = \bigcup_{n\in\omega} M_n$.

For $i < \alpha$, we call M_{i+1}/M_i the **ith successive quotient**. If for a class $\mathcal{C}$ of R-modules each successive quotient lies in $\mathcal{C}$, we say the filtration is of **class** $\mathcal{C}$.

Define the **associated graded module** $\mathrm{Gr}(M) = \bigoplus_{i<\alpha} M_{i+1}/M_i$.

Lemma 3.50. *(Transfinite Dévissage Lemma) Let M be an R-module and $\{M_i\}_{i\leq\alpha}$ an ordinal filtration of M.*
a) Suppose we make the following hypothesis:
(DS) For all $i < \alpha$ the submodule M_i is a direct summand of M_{i+1}. Then

$$M \cong \mathrm{Gr}(M) = \bigoplus_{i<\alpha} M_{i+1}/M_i.$$

b) Hypothesis (DS) holds if each successive quotient M_{i+1}/M_i is projective.
c) Hypothesis (DS) holds if each M_i is injective.

Exercise 3.63: Prove Lemma 3.50. (Hint: transfinite induction.)

Corollary 3.51. *For an R-module M, TFAE:*
(i) M is free.
(ii) M admits an ordinal filtration with successive quotients isomorphic to R.
(iii) M admits an ordinal filtration with free successive quotients.

Proof. (i) $\implies$ (ii): If M is free, then $M \cong \bigoplus_{i\in I} R$. By the Well-Ordering Principle[20], I is in bijection with an ordinal α, so we may write $M \cong \bigoplus_{i<\alpha} R$, and put $M_i = \bigoplus_{j<i} R$.
(ii) $\implies$ (iii) is immediate.
(iii) $\implies$ (i) follows from Lemma 3.50 since free modules are projective. □

3.9.2. *Hereditary and semihereditary rings.*

An R-module is **hereditary** if every submodule is projective. (In particular a hereditary module is projective, and thus the property of being projective is "inherited" by its submodules.) We say that a ring R is **hereditary** if R is a hereditary R-module, or equivalently every ideal of R is projective as an R-module.

Exercise 3.64:
a) Show that every submodule of a hereditary module is hereditary.
b) Show that the zero module is hereditary.
c) Show that there are nonzero rings R for which the only hereditary R-module is the zero module.

Example: A PID is a hereditary ring. Indeed, any nonzero ideal of a PID R is isomorphic as an R-module to R.

[20]This set-theoretic axiom is equivalent to the Axiom of Choice and also to Zorn's Lemma. Our running convention in these notes is to freely use these axioms when necessary.

Theorem 3.52. *a) Let $\{M_i\}_{i \in I}$ a family of hereditary R-modules, put $M = \bigoplus_{i \in I} M_i$, and let $\pi_i : M \to M_i$ be projection onto the ith factor. Then, for any submodule N of M, $N \cong \bigoplus_{i \in I} \pi_i(N)$.*
b) Let R be a hereditary ring, and let M be an R-module. TFAE:
(i) M is isomorphic to to a direct sum of ideals of R.
(ii) M can be embedded in a free R-module.

Proof. a) By the Well-Ordering Principle there is a bijection from I to some ordinal α, and without loss of generality we may assume $M = \bigoplus_{i \in \alpha} M_i$. For $j \in \alpha^+$, put $P_j = \bigoplus_{i < j^+} M_i$, so that $\{M_j\}$ is an ordinal-indexed chain of R-submodules of M with final element $P_\alpha = M$. For each $j \in \alpha^+$, put

$$N_j = N \cap P_j,$$

so $\{N_j\}$ is an ordinal filtration on N with $N_\alpha = N$. Moreover, for all $i \in \alpha$ we have $N_i = N_{i+1} \cap P_i$ and thus

$$N_{i+1}/N_i = N_i/(N_{i+1} \cap P_i) \cong (N_{i+1} + P_i)/P_i.$$

Thus N_{i+1}/N_i is isomorphic to a submodule of $P_{i+1}/P_i \cong M_i$. Since each M_i is hereditary, each successive quotient N_{i+1}/N_i is projective, and the Transfinite Dévissage Lemma (Lemma 3.50) applies to show that

$$N \cong \operatorname{Gr} N = \bigoplus_{j < \alpha^+} N_{j+1}/N_j$$

$$= \bigoplus_{j < \alpha^+} \left((N \cap \bigoplus_{i < j^{++}} M_j)/(N \cap \bigoplus_{i < j^+} M_j) \right) \cong \bigoplus_{j < \alpha^+} \pi_j(N).$$

b) (i) $\implies$ (ii) holds over any ring. (ii) $\implies$ (i) follows from part a). □

Corollary 3.53. *Let $\{M_i\}_{i \in I}$ be a family of R-modules. Then $M = \bigoplus_{i \in I} M_i$ is hereditary iff M_i is hereditary for all i.*

Proof. Suppose each M_i is hereditary, and let N be a submodule of M. By Theorem 3.52, $N \cong \bigoplus_{i \in I} \pi_i(N)$. For all i, $\pi_i(N)$ is a submodule of the hereditary module M_i hence is projective. Thus N is a direct sum of projective modules, hence projective. Conversely, if M is hereditary, so are all of its submodules M_i. □

Lemma 3.54. *a) (Checking Projectivity With Injectives) Let P be an R-module such that: for every injective module I, surjection $q : I \to Q$ and module map $f : P \to Q$, there is $F : P \to I$ such that $q \circ F = f$. Then P is projective.*
b) (Checking Injectivity With Projectives) Let I be an R-module such that: for every projective R-module P, injection $\iota : S \to P$ and module map $f : S \to I$, there is $F : P \to I$ such that $F \circ \iota = f$. Then I is injective.

Proof. a) Let $0 \to A' \xrightarrow{\iota} A \xrightarrow{\tau} A'' \to 0$ be a short exact sequence of R-modules, and let $f : P \to A''$ be a module map. Let $\sigma : A \to I$ be an embedding into an injective module, and consider the following commutative diagram with exact rows:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & A' & \xrightarrow{\iota} & A & \xrightarrow{\tau} & A'' & \longrightarrow & 0 \\ & & \| & & \downarrow{\scriptstyle \sigma} & & & & \\ 0 & \longrightarrow & A' & \xrightarrow{\sigma \circ \iota} & I & \xrightarrow{q} & Q & \longrightarrow & 0 \end{array}$$

Step 1: We claim there is $\rho : A'' \to Q$ making the diagram commute.
Proof: This is a routine diagram chase: choose $y \in A''$, lift to x in A, and put $\rho(y) = (q \circ \sigma)(x)$. Let us check that this is well-defined: if we chose a different lift x' in A, then $x - x' \in A'$, so $(q \circ \sigma)(x - x') = 0$.
Step 2: By hypothesis, the map $\rho \circ f : P \to Q$ can be lifted to $G : P \to I$. To complete the proof it suffices to show $G(P) \subset \sigma(A)$. To see this, let $x \in P$ and choose $a \in A$ such that $\tau(a) = f(x)$. Then

$$q(G(x)) = \rho(f(x)) = \rho(\tau(a)) = q(\sigma(a)),$$

so $G(x) - \sigma(a) \in \operatorname{Ker} q = \operatorname{Im}(\sigma \circ q)$. That is, there is $a' \in A'$ such that $\sigma(\iota(a')) = G(x) - \sigma(a)$, so

$$G(x) = \sigma(\iota(a') + a) \in \sigma(A).$$

b) This is the dual version of part a), i.e., obtained by reversing all the arrows. The above proof also dualizes, as we leave it to the reader to check. □

Corollary 3.55. *(Cartan-Eilenberg) For a ring R, the following are equivalent:*
(i) R is hereditary.
(ii) Every free R-module is hereditary.
(iii) Every projective R-module is hereditary.
(iv) Every quotient of an injective R-module is injective.

Proof. (i) $\implies$ (ii) is immediate from Corollary 3.53.
(ii) $\implies$ (iii): Suppose that every free R-module is hereditary. Then if P is a projective R-module, P is a submodule of a free module, hence a submodule of a hereditary module, hence itself hereditary.
(iii) $\implies$ (i): R is a projective R-module.
(iv) $\iff$ (iii): Let P' be a submodule of a projective R-module P; call the inclusion j. We will use Lemma 3.54a) : let I be an injective module, $q : I \to I'$ a surjection, and $f : P' \to I'$ a module map. By assumption I' is injective, so there is $h : P \to I'$ such that $h \circ j = f$. Since P is projective, there is $k : P \to I$ such that $q \circ k = h$. Then $F = k \circ j : P' \to I$ lifts f: $q \circ F = q \circ k \circ j = h \circ j = f$.
(iii) $\implies$ (iv): Using Lemma 3.54b) we may dualize the proof of (iv) $\implies$ (iii). □

Theorem 3.56. *Let R be a a PID and $F = \bigoplus_{i \in I} R$ a free R-module. Then any submodule M of F is again free, of rank less than or equal to the rank of F.*

Proof. Let N be a submodule of F. By Theorem 3.52, $N \cong \bigoplus_{i \in I} \sigma_i(N)$, where each $\sigma_i(N)$ is an R-submodule of R, i.e., an ideal of R. Since R is a PID, either $\sigma_i(N)$ is the zero module or is isomorphic as an R-module to R. □

Corollary 3.57. *A projective module over a PID is free.*

We expect that the following result is familiar to the reader as a special case of the classification of (all) finitely generated modules over a PID, but while we are here we may as well give a commutative algebraic proof.

Proposition 3.58. *A finitely generated torsionfree module over a PID is free.*

Proof. Let M be finitely generated and torsionfree. Certainly we may assume that M is nonzero. Let X be a finite generating set for M with $0 \notin X$. Let $S \subset X$ be a maximal R-linearly independent subset. Since M is torsionfree, S is not empty. Let $N = \langle S \rangle_R$ be the R-module spanned by S. Clearly N is free with basis S, and we will be done if we can show $N = M$.

There is an annoying technicality here: we must check that S is finite. In fact, let $n = \#X$, and let S be any finite R-linearly independent subset and let $s = \#S$. We claim that $s \leq n$. To see this, we tensor with the fraction field K of R, getting $K^s \cong S \otimes_R K \stackrel{\iota_K}{\to} M \otimes_R K \cong K^m$ with $m \leq n$. We may conclude that $s \leq m \leq n$ provided we know that ι_K is injective. And this holds because K is a flat R-module, which we will prove later on as a special case of the flatness of localization maps. Until then, the reader must take this part of the proof on faith.
Say $S = \{x_1, \ldots, x_k\}$. Of course we are done already if $S = X$, so assume that $X \setminus S$ is nonempty. For each $y \in X \setminus S$ there exist $r_y, r_1, \ldots, r_k \in R$, not all zero, such that $r_y y = r_1 x_1 + \ldots + r_k x_k$. Then $r_y \neq 0$, since otherwise by the linear independence of S all the r_i would be zero. In other words, we have shown that for each $y \in X \setminus S$ there exists $r_y \in R^\bullet$ such that $r_y y \in N$. Put $r := \prod_{y \in X \setminus S} r_y$. Then $rX \subset N$ and thus $rM \subset N$. Now consider the R-module homomorphism $L : M \to M$ given by multiplication by r: $x \mapsto rx$. We have just established that $L(M) \subset N$, so we may regard L as a homomorphism $M \to N$. Moreover, since M is torsionfree, L is injective, and therefore L realizes M as a submodule of the free R-module N. By Theorem 3.56 we conclude that M is free. □

Exercise 3.65: Let R be a ring with the following property: every submodule of a finitely generated free R-module is free. Show that R is a principal ring (i.e., every ideal of R is principal).

An R-module M is **semihereditary** if every finitely generated submodule is projective. Thus a Noetherian semihereditary module is hereditary. A ring R is **semihereditary** if R is a semihereditary R-module, or equivalently every finitely generated ideal of R is projective as an R-module.

Example: A domain R is semihereditary if every finitely generated ideal is principal. Such domains are called **Bézout domains** and will be studied later on.

Theorem 3.59. *Let $\{M_i\}_{i \in I}$ a family of semihereditary R-modules, put $M = \bigoplus_{i \in I} M_i$, and let $\pi_i : M \to M_i$ be projection onto the ith factor. Then, for any finitely generated submodule N of M, $N \cong \bigoplus_{i \in I} \pi_i(N)$.*

Proof. The proof of Theorem 3.52 goes through verbatim. □

Theorem 3.60. *Let R be a domain in which every finitely generated ideal is principal, and let F be a free R-module. Then any finitely generated submodule N of F is free, of rank less than or equal to the rank of F.*

Proof. One can adapt the proof of Theorem 3.57, using Theorem 3.59 in place of Theorem 3.52. □

Theorem 3.61. *Let R be a domain in which every finitely generated ideal is principal. Then every finitely generated torsionfree R-module is principal.*

Proof. The argument is the same as that of Proposition 3.58 (a special case), using Theorem 3.60 in place of Theorem 3.56. □

Theorem 3.62. *(F. Albrecht) Let R be a semihereditary ring, F a free R-module, and P a finitely generated submodule of F.*
a) P is isomorphic to a finite direct sum of finitely generated ideals of R.

b) In particular, P is a finitely generated projective module.
c) If R is a domain with fraction field K and F is free of finite rank n, then the rank of P – i.e., $\dim_K P \otimes_R K$ – is at most n.

Exercise 3.66: Use Theorem 3.59 to prove Theorem 3.62.

3.9.3. *Big modules.*

Lemma 3.63. *(Kaplansky) Let R be a ring, and let F be an R-module which is a direct sum of countably generated submodules: say $F = \bigoplus_{\lambda \in \Lambda} E_\lambda$. Then every direct summand of F is again a direct sum of countably generated submodules.*

Proof. We CLAIM that there is an ordinal filtration $\{F_i\}_{i \leq \alpha}$ on F satisfying all of the following properties. (i) For all $i < \alpha$, F_{i+1}/F_i is countably generated.
(ii) If $M_i = F_i \cap M$, $N_i = F_i \cap N$, then $F_i = M_i \oplus N_i$.
(iii) For each i there is a subset Λ_i of Λ such that $F_i = \bigoplus_{\lambda \in \Lambda_i} \Lambda_i$.
SUFFICIENCY OF CLAIM: If so, $\{M_i\}_{i \leq \alpha}$ is an ordinal filtration on M. Moreover, since $M_i \subset M_{i+1}$ are both direct summands of F, M_i is a direct summand of M_{i+1}. The Transfinite Dévissage Lemma (Lemma 3.50) applies to give

$$M \cong \mathrm{Gr}(M) = \bigoplus_{i < \alpha} M_{i+1}/M_i.$$

Moreover, for all $i < \alpha$ we have

$$F_{i+1}/F_i = (M_{i+1} \oplus N_{i+1})/(M_i \oplus N_i) \cong M_{i+1}/M_i \oplus N_{i+1}/N_i,$$

which shows that each successive quotient M_{i+1}/M_i is countably generated. Therefore M is a direct sum of countably generated submodules.
PROOF OF CLAIM: We will construct the filtration by transfinite induction. The base case and the limit ordinal induction step are forced upon us by the definition of ordinal filtration: we must have $F_0 = \{0\}$, and for any limit ordinal $\beta \leq \alpha$, assuming we have defined F_i for all $i < \beta$ we must have $F_\beta = \bigcup_{i < \beta} F_i$.

So consider the case of a successor ordinal $\beta = \beta' + 1$. Let Q_1 be any E_λ which is not contained in $F_{\beta'}$. (Otherwise we have $F_{\beta'} = F$ and we may just define $F_i = F$ for all $\beta \leq i \leq \alpha$.) Let $x_{11}, x_{12}, \ldots$ be a sequence of generators of Q_1, and decompose x_{11} into its M- and N-components. Let Q_2 be the direct sum of the finitely many E_λ which are necessary to write both of these components, and let $x_{21}, x_{22}, \ldots$ be a sequence of generators for Q_2. Similarly decompose x_{12} into M and N components, and let Q_3 be the direct sum of the finitely many E_λ needed to write out these components, and let $x_{31}, x_{32}, \ldots$ be a sequence of generators of Q_3. We continue to carry out this procedure for all x_{ij}, proceeding according to a diagonal enumeration of $\mathbb{Z}^+ \times \mathbb{Z}^+$: i.e., $x_{11}, x_{12}, x_{21}, x_{13}, x_{22}, x_{31}, \ldots$. Put $F_\beta = \langle F_{\beta'}, \{x_{ij}\}_{i,j \in \mathbb{Z}^+} \rangle_R$. This works! □

For a cardinal number κ, we say that a module is **κ-generated** if it admits a generating set of cardinality at most κ.

Exercise 3.67 (Warfield): Let κ be an infinite cardinal. Formulate and prove a version of Lemma 3.63 in which "countably generated" is replaced by "κ-generated".

Theorem 3.64. *(Kaplansky) For a ring R, let $\mathcal{P}_c$ be the class of countably generated projective R-modules. For an R-module M, TFAE:*
(i) M admits an ordinal filtration of class $\mathcal{P}_c$.

(ii) M is a direct sum of countably generated projective submodules.
(iii) M is projective.

Proof. (i) $\iff$ (ii) follows immediately from Lemma 3.50.
(ii) $\implies$ (iii): any direct sum of projective modules is projective.
(iii) $\implies$ (ii): If M is projective, let F be a free R-module with $F = M \oplus N$. Certainly F is a direct sum of countably generated submodules (indeed, of singly generated submodules!), so by Lemma 3.63 M is a direct sum of a family of countably generated submodules, each of which must be projective. □

While pondering the significance of this result, one naturally inquires:

Question 2. *Is there a ring R and an R-module M which is* not *a direct sum of countably generated submodules?*

Theorem 3.65. *(Cohen-Kaplansky* [CK51]*, Griffith) For a ring R, TFAE:*
(i) Every R-module is a direct sum of cyclic (i.e., singly generated) R-modules.
(ii) Every R-module is a direct sum of finitely generated submodules.
(iii) R is an Artinian principal ideal ring.

Building on these results as well as work of Faith and Walker [FW67], R.B. Warfield Jr. proved the following striking results.

Theorem 3.66. *(Warfield* [Wa]*) Let R be a Noetherian ring which is not a principal Artinian ring. Then for any cardinal κ, there exists a module M with the following properties:*
(i) M is not κ-generated, and
(ii) Any decomposition of M into the direct sum of nonzero submodules has only finitely many direct summands.

The hypotheses of Theorem 3.66 apply for instance to the ring $\mathbb{Z}$ of integers and yields, in particular, for any infinite cardinal κ a commutative group M which is not a direct sum of κ-generated submodules.

Theorem 3.67. *(Warfield* [Wa]*) For a ring R, TFAE:*
(i) Every R-module is a direct sum of cyclic submodules.
(ii) There exists a cardinal number κ such that every R-module is a direct sum of κ-generated submodules.
(iii) R is a principal Artinian ring.

It is natural to wonder whether Theorem 3.66 can be strengthened in the following way: an R-module M is **indecomposable** if it cannot be expressed as a direct sum of two nonzero submodules.

Question 3. *For which rings R do there exist indecomposable R-modules of all infinite cardinalities?*

However, Question 3 has turned out to be bound up with sophisticated set-theoretic considerations. Namely, in a 1959 paper [Fu59], L. Fuchs claimed that there exist indecomposable commutative groups of all infinite cardinalties, thus giving an affirmative answer to Question 3 for the ring $R = \mathbb{Z}$. However, it was later observed (by A.L.S. Corner) that Fuchs' argument is valid only for cardinals κ less than the first **inaccessible cardinal**. Exactly what an inaccessible cardinal is we do not wish to say, but we mention that the nonexistence of inaccessible cardinals is equiconsistent

with the standard ZFC axioms of set theory (in other words, if the ZFC axioms are themselves consistent, then ZFC plus the additional axiom that there are no inaccessible cardinals remains consistent) but that nevertheless set theorists have reasons to believe in them. See also [Fu74] in which these issues are addressed and he proves that there is an indecomposable commutative group of any infinite **nonmeasurable** cardinality (note: accessible implies nonmeasurable).

Question 4. *Is there a ring R and a projective R-module M which is* not *a direct sum of finitely generated submodules?*

Again the answer is *yes*. A very elegant example was given by Kaplansky (unpublished, apparently).[21] Namely that R be the ring of all real-valued continuous functions on the unit interval $[0,1]$, and let I be the ideal of functions $f : [0,1] \to \mathbb{R}$ which vanish near zero: i.e., for which there exists $\epsilon = \epsilon(f) > 0$ such that $f|_{[0,\epsilon(f)]} = 0$.

Exercise 3.68: Show the ideal I defined above gives a projective R-module which is not the direct sum of finitely generated submodules. (Suggestions: (i) to show that I is projective, use the Dual Basis Lemma. (ii) A slick proof of the fact that I is not a direct sum of finitely generated submodules can be given by Swan's Theorem using the contractibility of the unit interval.)

Lemma 3.68. *Let M be a projective module over the local ring R, and let $x \in M$. There is a direct summand M' of M such that M' contains F and M' is free.*

Proof. Let F be a free module with $F = M \oplus N$. Choose a basis $B = \{u_i\}_{i \in I}$ of F with respect to which the element x of M has the minimal possible number of nonzero coordinates. Write

$$x = r_1 u_1 + \ldots + r_n u_n, \ r_i \in R^\bullet.$$

Then for all $1 \leq i \leq n$, $r_i \notin \sum_{j \neq i} R r_j$. Indeed, if say $r_n = \sum_{i=1}^{n-1} s_i r_i$, then $x = \sum_{i=1}^{n-1} r_i(u_i + s_i u_n)$, contradicting the minimality of the chosen basis.
Now write $u_i = y_i + z_i$ with $y_i \in M, \ z_i \in N$, so

$$x = \sum_i r_i u_i = \sum_i r_i y_i. \tag{6}$$

We may write

$$y_i = \sum_{j=1}^{n} c_{ij} u_j + t_i, \tag{7}$$

with t_i a linear combination of elements of $B \setminus \{u_1, \ldots, u_n\}$. Substituting (7) into (6) and projecting onto M gives the relations

$$r_i = \sum_{j=1}^{n} c_{ji} r_j,$$

or equivalently, for all i,

$$(1 - c_{ii}) r_i = \sum_{j \neq i} c_{ji} r_j.$$

If for any i and j, then one of the coefficients of r_j in the above equation is a unit of R, then dividing through by it expresses r_j as an R-linear combination of the

[21] Warm thanks to Gjergji Zaimi for bringing this important example to my attention.

other r_i's, which as above is impossible. Therefore, since R is local, each coefficient must lie in the maximal ideal of R:

$$\forall i,\ 1 - c_{ii} \in \mathfrak{m},\ \ \forall i \neq j,\ c_{ij} \in \mathfrak{m}.$$

It follows that the determinant of the matrix $C = (c_{ij})$ is congruent to 1 modulo $\mathfrak{m}$, hence invertible: if $x \in \mathfrak{m}$ and $1 + x$ is not invertible, then $1 + x = y$ for $y \in \mathfrak{m}$, so $1 = y - x \in \mathfrak{m}$, contradiction. Therefore replacing $u_1, \ldots, u_n$ in B with $y_1, \ldots, y_n$ still yields a basis of F. It follows that $M' = \langle y_1, \ldots, y_n \rangle_R$ is a direct summand of F hence also of M which is a free module containing x. □

Theorem 3.69. *(Kaplansky) Let $(R, \mathfrak{m})$ be a local ring, and let P be any projective R-module. Then P is free.*

Proof. Step 1: Since by Theorem 3.64 P is a direct sum of countably generated projective submodules, we may as well assume that P itself is countably generated. Step 2: Suppose $M = \langle \{x_n\}_{n=1}^{\infty} \rangle_R$ is a countably generated projective module over the local ring R. By Lemma 3.68, $M = F_1 \oplus M_1$ with F_1 free containing x_1. Note that M_1 is again projective and is generated by the images $\{x_n'\}_{n=2}^{\infty}$ of the elements x_n under the natural projection map $M \to M_1$. So reasoning as above, we may write $M_2 = F_2 \oplus M_2$ with F_2 free containing x_2'. Continuing in this manner, we get

$$M = \bigoplus_{n=1}^{\infty} F_n,$$

so M is free. □

Exercise 3.69: Give an example of a (necessarily infinitely generated) module over a local PID which is flat but not free.

3.10. **Tor and Ext.**

3.10.1. *Co/chain complexes.*

Let R be a ring. A **chain complex** $C_\bullet$ of R-modules is a family $\{C_n\}_{n \in \mathbb{Z}}$ of R-modules together with for all $n \in \mathbb{Z}$, an R-module map $d_n : C_n \to C_{n-1}$ such that for all n, $d_{n-1} \circ d_n = 0$. (It is often the case that $C_n = 0$ for all $n < 0$, but this is not a required part of the definition.)

An example of a chain complex of R-modules is any long exact sequence. However, from the perspective of homology theory this is a trivial example in the following precise sense: for any chain complex we may define its **homology modules**: for all $n \in \mathbb{Z}$, we put

$$H_n(C) = \operatorname{Ker}(d_n)/\operatorname{Im}(d_{n+1}).$$

Example: Let X be any topological space. For any ring R, we have the **singular chain complex** $S(X)_\bullet$: $S(X)_n = 0$ for $n < 0$, and for $n \geq 0$, $S(X)_n$ is the free R-module with basis the set of all continuous maps $\Delta_n \to X$, where Δ_n is the standard n-dimensional simplex. A certain carefully defined alternating sum of restrictions to faces of Δ_n gives rise to a boundary map $d_n : S(X)_n \to S(X)_{n-1}$, and the indeed the homology groups of this complex are nothing else than the singular homology groups $H_n(X, R)$ with coefficients in R.

If $C_\bullet$ and $D_\bullet$ are two chain complexes of R-modules, a **homomorphism** $\eta : C_\bullet \to$

$D_\bullet$ is given by maps $\eta_n : C_n \to D_n$ for all n rendering the following infinite ladder commutative:

INSERT ME!.

In this way one has evident notions of a **monomorphism** and **epimorphisms** of chain complexes. In fact the chain complexes of R-modules form an abelian category and thus these notions have a general categorical meaning, but it turns out they are equivalent to the much more concrete naive conditions: η is a monomorphism iff each η_n is injective and is an epiomorphism iff each η_n is surjective.

In particular it makes sense to consider a short exact sequence of chain complexes:

$$0 \longrightarrow A_\bullet \longrightarrow B_\bullet \longrightarrow C_\bullet.$$

Here is the first basic theorem of homological algebra.

Theorem 3.70. *Let*

$$0 \longrightarrow A_\bullet \xrightarrow{f} B_\bullet \xrightarrow{g} C_\bullet \longrightarrow 0$$

*be a short exact sequence of chain complexes of R-modules. Then for all $n \in \mathbb{Z}$ there is a natural **connecting homomorphism** $\partial : H_n(C) \to H_{n-1}(A)$ such that*

$$\ldots \xrightarrow{g} H_{n+1}(C) \xrightarrow{\partial} H_n(A) \xrightarrow{f} H_n(B) \xrightarrow{g} H_n(C) \xrightarrow{\partial} H_{n-1}(A) \xrightarrow{f} \ldots$$

is exact.

Proof. No way. See [W, Thm. 1.3.1]. □

Moreover, the homology modules H_n are functors: if $f : C_\bullet \to D_\bullet$ is a morphism of chain complexes, there are induced maps on the homology groups

$$H_n(f) : H_n(C) \to H_n(D).$$

Example: Let $f : X \to Y$ be a continuous map of topological spaces. Then for any basic n-chain $\Delta_n \to X$ in $S(X)_n$, composition with f gives a basic n-chain $\Delta_n \to Y$ in $S(Y)_n$ and thus a homomorphism of chain complexes $S(f) : S(X)_\bullet \to S(Y)_\bullet$. There are induced maps on homology, namely the usual maps

$$H_n(f) : H_n(X, R) \to H_n(Y, R).$$

There is an entirely parallel story for **cochain complexes** of R-modules, which are exactly the same as chain complexes but with a different indexing convention: a cochain complex $C^\bullet$ consists of for each $n \in \mathbb{Z}^+$ an R-module C^n and a "coboundary map" $d^n : C^n \to C^{n+1}$. To any cochain complex we get **cohomology modules**: for all $n \in \mathbb{Z}$, put

$$H^n(C) = \operatorname{Ker}(d^n)/\operatorname{Im}(d^{n-1}).$$

The rest of the discussion proceeds in parallel to that of chain complexes (including the realization of singular cohomology as a special case of this construction).

3.10.2. *Chain homotopies.*

Let $C_\bullet, D_\bullet$ be two chain complexes, and let $f, g : C_\bullet \to D_\bullet$ be two homomorphisms between them. We say that f and g are **chain homotopic** if there exist for all $n \in \mathbb{Z}^+$ R-module maps $s_n : C_n \to D_{n+1}$ such that

$$f_n - g_n = d_{n+1}s_n + s_{n-1}d_n.$$

The sequence $\{s_n\}$ is called a **chain homotopy** from f to g.

Exercise 3.70: Show that chain homotopy is an equivalence relation on morphisms from $C_\bullet$ to $D_\bullet$.

What on earth is going on here? Again topology is a good motivating example: we say that two maps $f, g : X \to Y$ are **homotopic** if there exists a continuous map $F : X \times [0,1] \to Y$ such that for all $x \in X$, $F(x,0) = f(x)$ and $F(x,1) = g(x)$. This is an equivalence relation and is generally denoted by $f \sim g$. We then define two topological spaces to be **homotopy equivalent** if there exist maps $\varphi : X \to Y$ and $\psi : Y \to X$ such that

$$\psi \circ \varphi \sim 1_X, \ \varphi \circ \psi \sim 1_Y.$$

(We say that $\varphi : X \to Y$ is a **homotopy equivalence** if there exists a map ψ as above.) E.g. a space is **contractible** if it is homotopy equivalent to a single point.

One of the basic tenets of algebraic topology is that it aspires to study topological spaces only up to homotopy equivalence. That is, all of the fundamental invariants of spaces should be the same on homotopy equivalent spaces and homomorphisms between these invariants induced by homotopic maps should be identical. Especially, if $f : X \to Y$ is a homotopy equivalence, the induced maps $H_n(f) : H_n(X) \to H_n(Y)$ should be isomorphisms. In fact, if $f, g : X \to Y$ are homotopic, the induced morphisms $S(f), S(g) : S(X)_\bullet \to S(Y)_\bullet$ are chain homotopic. So the following result ensures that the induced maps on homology are equal.

Proposition 3.71. *If $f, g : C_\bullet \to D_\bullet$ are chain homotopic, then for all $n \in \mathbb{Z}$, $H_n(f) = H_n(g)$.*

Proof. Replacing f and g by $f - g$ and 0, it is enough to assume that there exists a chain homotopy s from f to the zero map – i.e., for all n $f_n = d_{n+1}s_n + s_{n-1}d_n$ – and show that f induces the zero map on homology. So take $x \in H_n(C)$. Then x is represented by an element of C_n lying in the kernel of d_n, so

$$f_n(x) = d_{n+1}s_n x + s_{n-1}d_n x = d_{n+1}s_n x + 0 = d_{n+1}s_n x.$$

Thus $f_n(x)$ lies in the image of $d_{n+1}D_{n+1} \to D_n$ so represents $0 \in H_n(D)$. □

3.10.3. *Resolutions.*

Let M be an R-module. A **left resolution** of M is an infinite sequence $\{A_i\}_{i=0}^\infty$ of R-modules, for all $n \in \mathbb{N}$ an R-module map $A_{n+1} \to A_n$ and an R-module map $A_0 \to M$ such that the sequence

$$\ldots \longrightarrow A_{n+1} \to A_n \longrightarrow \ldots \longrightarrow A_1 \longrightarrow A_0 \longrightarrow M \longrightarrow 0$$

is exact. By abuse of notation, we often speak of "the resolution $A_\bullet$. Dually, a **right resolution** of M is an infinite sequence $\{B^i\}_{i=0}^\infty$ of R-modules, for all $n \in \mathbb{N}$ an R-module map $B^n \to B^{n+1}$ and an R-module map $M \to B^0$ such that the sequence

$$0 \longrightarrow M \longrightarrow B^0 \longrightarrow B^1 \longrightarrow \ldots \longrightarrow B^n \longrightarrow B^{n1} \ldots$$

is exact. We speak of "the resolution $B^\bullet$".

A **projective resolution** of M is a left resolution $A_\bullet$ such that each A_n is projective. A **injective resolution** of M is a right resolution $B^\bullet$ such that each B^n is injective. (Exactly why we are not interested in left injective resolutions and right projective resolutions will shortly become clear.)

Theorem 3.72. *(Existence of resolutions) Let M be an R-module.*
a) Since every R-module is the quotient of a projective (indeed, of a free) module, M admits a projective resolution.
b) Since every R-module can be embedded in an injective module, M admits an injective resolution.

Proof. a) Choose a projective module P_0, a surjection $\epsilon_0 : P_0 \to M$, and put $M_0 = \ker(\epsilon_0)$. Inductively, given M_{n-1}, we choose a projective module P_n, a surjection $\epsilon_n : P_n \to M_{n-1}$, and put $M_n = \ker(\epsilon_0)$. As our map $d_n : P_n \to P_{n-1}$ we take the composite

$$P_n \xrightarrow{\epsilon_n} M_{n-1} \xrightarrow{\ker(\epsilon_{n-1})} P_{n-1}.$$

We claim that the resulting sequence

$$\ldots \longrightarrow P_{n+1} \to P_n \longrightarrow \ldots \longrightarrow P_1 \longrightarrow P_0 \longrightarrow M \longrightarrow 0$$

is exact. It is certainly exact at M. If $x \in P_0$ and $\epsilon_0(x) = 0$, then $x_0 \in M_0$. Lifting x_0 via the surjection ϵ_1 to $x_1 \in P_1$, we find $d_1(x_1) = \epsilon_1(x_1) = x_0$, so $\ker(\epsilon_0) \subset \mathrm{Im}(d_1)$. Conversely, since d_1 factors through $\ker(\epsilon_0)$, it is clear that $\mathrm{Im}(d_1) \subset \ker(\epsilon_0)$. Exactly the same argument verifies exactness at P_n for each $n > 0$, so $P_\bullet$ is a projective resolution of M.
b) We leave the proof of this part to the reader as an exercise, with the following comforting remark: the notion of an injective module is obtained from the notion of a projective module by "reversing all the arrows", which is the same relationship that a left resolution bears to a right resolution. Therefore it should be possible to prove part b) simply by holding up the proof of part a) to a mirror. (And it is.) □

Theorem 3.73. *(Comparison theorem for resolutions)*
a) Let $P_\bullet$ be a projective resolution of the R-module M. Let N be another R-module and $f_{-1} : M \to N$ be an R-module map. Then for every left resolution $A_\bullet$ of N there exists a homomorphism η from the chain complex $P_\bullet \to M \to 0$ to the chain complex $A_\bullet \to N \to 0$. Moreover η is unique up to chain homotopy.
b) Let $E^\bullet$ be an injective resolution of the R-module N. Let M be another R-module and $f' : M \to N$ be an R-module map. Then for every right resolution $A^\bullet$ of M there exists a homomorphism η from the chain complex $0 \to M \to A^\bullet$ to the chain complex $0 \to N \to E^\bullet$. Moreover η is unique up to chain homotopy.

Proof. No way. See [W, Thms. 2.2.6 and 2.3.7]. □

Exercise 3.71: Let F be a covariant additive functor on the category of R-modules. Let $C_\bullet$ and $D_\bullet$ be two chain complexes of R-modueles and $f, g : C_\bullet \to D_\bullet$ be two homomorphisms between them.
a) Show that $FC_\bullet$ and $FD_\bullet$ are chain complexes and there are induced chain homomorphisms $Ff,\ Fg : FC_\bullet \to FD_\bullet$.
b) Show that if f and g are chain homotopic, so are Ff and Fg. (Suggestion: Show that it makes sense to apply F to a chain homotopy s.)

3.10.4. *Derived functors.*

Let us consider covariant, additive functors F from the category of R-modules to itself. (Recall that additive means that for any M, N, the induced map $\mathrm{Hom}(M, N) \to \mathrm{Hom}(F(M), F(N))$ is a homomorphism of commutative groups.)

Exercise 3.72: For any additive functor F and any chain complex $C_\bullet$ of R-modules, $FC_\bullet$ is again a chain complex. (Hint: the point here is that an additive functor takes the zero homomorphism to the zero homomorphism.)

Thus if

$$0 \longrightarrow M_1 \longrightarrow M_2 \longrightarrow M_3 \longrightarrow 0$$

is a short exact sequence of R-modules, then

$$0 \longrightarrow F(M_1) \longrightarrow F(M_2) \longrightarrow F(M_3) \longrightarrow 0$$

is necessarily a *complex* of modules but not necessarily exact: it may have nonzero homology.

Example: For any ring R, the functor $F(M) = M \oplus M$ is exact. For $R = \mathbb{Z}$ the functor $F(M) = M \otimes \mathbb{Z}/2\mathbb{Z}$ is not exact: for instance it takes the short exact sequence

$$0 \longrightarrow \mathbb{Z} \xrightarrow{\cdot 2} \mathbb{Z} \longrightarrow \mathbb{Z}/2\mathbb{Z} \longrightarrow 0$$

to the complex

$$0 \longrightarrow \mathbb{Z}/2\mathbb{Z} \xrightarrow{\cdot 2} \mathbb{Z}/2\mathbb{Z} \to \mathbb{Z}/2\mathbb{Z} \longrightarrow 0,$$

but multiplication by 2 on $\mathbb{Z}/2\mathbb{Z}$ is not an injection.

Although an exact functor is a thing of beauty and usefulness to all, it turns out that from a homological algebraic point of view, it is the functors which are "half exact" which are more interesting: they give rise to co/homology theories.

An additive functor F is **right exact** if for any exact sequence of the form

$$M_1 \longrightarrow M_2 \longrightarrow M_3 \longrightarrow 0,$$

the induced sequence

$$FM_1 \longrightarrow FM_2 \longrightarrow FM_3 \longrightarrow 0$$

is again exact. Note that this much was true for the functor $F(M) = M \otimes \mathbb{Z}/2\mathbb{Z}$, at least for the sequence we chose above. In fact this holds for all tensor products.

Proposition 3.74. *For any ring R and any R-module N, the functor $F(M) = M \otimes_R N$ is right exact.*

Exercise 3.73: Prove Proposition 3.74.

We have also the dual notion of an additive functor F being **left exact**: for any exact sequence of the form

$$0 \to M_1 \to M_2 \to M_3,$$

the induced sequence

$$0 \to FM_1 \to FM_2 \to FM_3$$

is again exact.

We now wish to press our luck a bit by extending this definition to contravariant functors. Here a little abstraction actually makes me less confused, so I will pass it along to you: we say that a contravariant functor F from the abelian category $\mathcal{C}$ to the abelian category $\mathcal{D}$ is left exact (resp. right exact) if the associated

covariant functor $F^{\mathrm{opp}} : \mathcal{C}^{\mathrm{opp}} \to \mathcal{D}$ is left exact (resp. right exact). Concretely, a contravariant functor F from R-modules to R-modules is **left exact** if every exact sequence of the form

$$M_1 \to M_2 \to M_3 \to 0$$

is transformed to an exact sequence

$$0 \to FM_3 \to FM_2 \to FM_1.$$

(And similarly for right exact contravariant functors.)

Proposition 3.75. *Let R be a ring and X be an R-module.*
a) The functor $M \mapsto \mathrm{Hom}(X, M)$ is covariant and left exact.
(Recall that it is exact iff X if projective.)
b) The functor $M \mapsto \mathrm{Hom}(M, X)$ is contravariant and left exact.
(Recall that it is exact iff X is injective.)

Exercise 3.74: Prove Proposition 3.75.

Let F be a right exact additive functor on the category of R-modules. We will define a sequence $\{L_nF\}_{n\in\mathbb{N}}$ of functors, with $L_0F = F$, called the **left derived functors** of F. The idea here is that the left-derived functors quantify the failure of F to be exact.

Let M be an R-module. We define all the functors L^nM at once, as follows: first we choose any projective resolution $P_\bullet \to M \to 0$ of M. Second we take away the M, getting a complex $P_\bullet$ which is exact except at P_0, i.e.,

$$H_0(P) = P_0/\operatorname{Im}(P_1 \to P_0) = P_0/\operatorname{Ker}(P_0 \to M) = M,$$

$$\forall n > 0, H_n(P) = 0.$$

Third we apply the functor F getting a new complex $FP_\bullet$. And finally, we take homology of this new complex, defining

$$(L_nF)(M) := H_n(FP_\bullet).$$

Now there is (exactly?) one thing which is relatively clear at this point.

Proposition 3.76. *We have $(L_0F)(M) = FM$.*

Proof. Since $P_1 \to P_0 \to M \to 0$ is exact and F is right exact, $FP_1 \to FP_0 \to FM \to 0$ is exact, hence

$$\operatorname{Im}(FP_1 \to FP_0) = \operatorname{Ker}(FP_0 \to FM).$$

Thus

$$\begin{aligned}(L_0F)(M) = H_0(FP_\bullet) &= \operatorname{Ker}(FP_0 \to 0)/\operatorname{Im}(FP_1 \to FP_0)\\ &= FP_0/\operatorname{Ker}(FP_0 \to FM) = FM.\end{aligned}$$

□

Before saying anything else about the left derived functors L_nF, there is an obvious point to be addressed: how do we know they are well-defined? On the face of it, they seem to depend upon the chosen projective resolution $P_\bullet$ of M, which is very far from being unique. To address this point we need to bring in the Comparison Theorem for Resolutions (Theorem 3.73). Namely, let $P'_\bullet \to M \to 0$ be any other projective resolution of M. By Theorem 3.73, there exists a homomorphism of

chain complexes $\eta : P_\bullet \to P'_\bullet$ which is unique up to chain homotopy. Interchanging the roles of $P'_\bullet$ and $P_\bullet$, we get a homomorphism $\eta' : P'_\bullet \to P_\bullet$. Moreover, the composition $\eta' \circ \eta$ is a homomorphism from $P_\bullet$ to itself, so by the uniqueness $\eta' \circ \eta$ is chain homotopic to the identity map on $P_\bullet$. Similarly $\eta \circ \eta'$ is chain homotopic to the identity map on $P'_\bullet$, so that η is a chain homotopy equivalence. By Exercise 3.71, $F\eta : FP_\bullet \to FP'_\bullet$ is a chain homotopy equivalence, and therefore the induced maps on homology $H_n(F\eta) : H_n(FP_\bullet) \to H_n(FP'_\bullet)$ are isomorphisms. Thus we have shown that two different choices of projective resolutions for M lead to *canonically* isomorphic modules $(L_nF)(M)$.

Exercise 3.75: Suppose M is projective. Show that for any right exact functor F and all $n > 0$, $(L_nF)(M) = 0$.

The next important result shows that a short exact sequence of R-modules induces a long exact sequence involving the left-derived functors and certain connecting homomorphisms (which we have not defined and will not define here).

Theorem 3.77. *Let*

$$0 \longrightarrow M_1 \longrightarrow M_2 \longrightarrow M_3 \longrightarrow 0 \tag{8}$$

be a short exact sequence of R-modules, and let F be any left exact functor on the category of R-modules. Then:
a) There is a long exact sequence
(9)
$$\ldots \to (L_2F)(M_3) \xrightarrow{\partial} (L_1F)(M_1) \to (L_1F)(M_2) \to (L_1F)(M_3) \xrightarrow{\partial} FM_1 \to FM_2 \to FM_3 \to 0.$$

b) The above construction is functorial in the following sense: if $0 \longrightarrow N_1 \longrightarrow N_2 \longrightarrow N_3 \longrightarrow 0$ is another short exact sequence of R-modules and we have maps $M_i \to N_i$ making a "short commutative ladder", then there is an induced "long commutative latter" with top row the long exact sequence associated to the first short exact sequence and the bottom row the long exact sequence associated to the second short exact sequence.

Proof. No way. See [W, Thm. 2.4.6]. □

Remark: One says that (9) is the **long exact homology sequence** associated to the short exact sequence (8).

Now, dually, if F is a right exact functor on the category of R-modules, we may define **right derived functors** R^nF. Namely, for an R-module M, first choose an injective resolution $0 \to M \to E^\bullet$, then take M away to get a cochain complex $E^\bullet$, then apply F to get a cochain complex $FE^\bullet$, and then finally define $(R^nF)(M) = H^n(FE^\bullet)$. In this case, a short exact sequence of modules (8) induces a **long exact cohomology sequence**
(10)
$$0 \to FM_1 \to FM_2 \to FM_3 \xrightarrow{\partial} (R^1F)(M_1) \to (R^1F)(M_2) \to (R^1F)(M_3) \xrightarrow{\partial} (R^2F)(M_1) \ldots$$

Exercise 3.76: Suppose M is injective. Show that for any left exact functor F and all $n > 0$, $(R^nF)(M) = 0$.

3.10.5. *Tor.*

Let M, N be R-modules, and let $F : N \to M \otimes_R N$ be the functor "tensor with M". By X.X F is right exact so has left derived functors (L_nF). By definition, for all $n \in \mathbb{N}$,

$$\mathrm{Tor}_n(M, N) := (L_nF)(N).$$

Now un/fortunately the situation is even a little richer than the general case of left-derived functors discussed above. Namely, the tensor product is really a **bifunctor**: i.e., a functor in M as well as in N, additive and covariant in each variable separately. So suppose we took the right-derived functors of $M \mapsto M \otimes_R N$ and applied them to M: this would give us $\mathrm{Tor}_n(N, M)$. So it is natural to ask: how does $\mathrm{Tor}_n(M, N)$ compare to $\mathrm{Tor}_n(N, M)$? Since for $n = 0$ we have that $M \otimes_R N$ is canonically isomorphic to $N \otimes_R M$, it is natural to hope that the Tor functors are symmetric. And indeed this turns out to be the case.

Theorem 3.78. *(Balancing Tor) For any R-modules M and N and all $n \geq 0$, there are natural isomorphisms $\mathrm{Tor}_n(M, N) = \mathrm{Tor}_n(N, M)$.*

Proof. No way. See [W, Thm. 2.7.2]. □

Exercise 3.77: In order to use the Universal Coefficient Theorem (for homology) in algebraic topology, it is necessary to know the values of $\mathrm{Tor}_1(M, N)$ for any two finitely generated $\mathbb{Z}$-modules M and N.
a) Show that for any $m, n \in \mathbb{Z}^+$, $\mathrm{Tor}_1(\mathbb{Z}/m\mathbb{Z}, \mathbb{Z}/n\mathbb{Z}) \cong \mathbb{Z}/\gcd(m, n)\mathbb{Z}$.
b) Show that for all $\mathbb{Z}$-modules N, $\mathrm{Tor}_1(\mathbb{Z}, N) = 0$.
c) Explain how the structure theorem for finitely generated $\mathbb{Z}$-modules reduces the problem of computation of $\mathrm{Tor}_1(M, N)$ for any finitely generated M and N to the two special cases done in parts a) and b).

Exercise 3.78: Show that the tor functors commute with direct limits: for all $n \in \mathbb{N}$, any directed system $\{M_i\}_{i \in I}$ of R-modules M and any R-module N we have a canonical isomorphism

$$\mathrm{Tor}_n(\varinjlim_i M_i, N) \to \varinjlim_i \mathrm{Tor}_n(M_i, N).$$

(Suggestion: the case $n = 0$ is Proposition 3.9. Use this to show the general case by brute force: i.e., take a projective resolution of N and track these isomorphisms through the definition of Tor_n.)

3.10.6. *Ext.*

Nota Bene: At the present time, we do not use the Ext functors *for anything* in these notes. However they certainly do appear in commutative algebra and elsewhere. Moreover, having taken the trouble (and it was some trouble!) to set up enough machinery to define the Tor functors, we might as well follow it up with the parallel disucssion of the Ext functors.

Let M, N be R-modules, and let $F : N \to \mathrm{Hom}(M, N)$. By Proposition X.X, F is covariant and left exact. By definition, for all $n \in \mathbb{N}$,

$$\mathrm{Ext}^n(M, N) = (R^nF)(N).$$

But again, we have an embarrassment of riches: why didn't we define the Ext functors as the right-derived functors of the contravariant left exact functor $G : N \to \mathrm{Hom}(N, M)$? Again, we can do this.

Theorem 3.79. *(Balancing Ext) Let M and N be R-modules. Define functors $F_M : N \to \mathrm{Hom}(M, N)$ and $G_N : M \to \mathrm{Hom}(M, N)$. Then for all $n \geq 0$,*

$$(R^n F_M)(N) = (R^n G_N)(M).$$

Proof. No way. See [W, Thm. 2.7.6]. □

Exercise 3.79: In order to use the Universal Coefficient Theorem (for cohomology) in algebraic topology, it is necessary to know the values of $\mathrm{Ext}_1(M, N)$ for any two finitely generated $\mathbb{Z}$-modules M and N. Compute them. (Hint: as for the analgous problem with Tor, one reduces immediately to the case in which M and N are cyclic.)

Theorem 3.80. *a) For an R-module P, the following are equivalent:*
(i) P is projective.
(ii) $\mathrm{Ext}^1_R(P, B) = 0$ for all R-modules B.
b) For an R-module E, the following are equivalent:
(i) E is injective.
(ii) $\mathrm{Ext}^1_R(A, E) = 0$ for all R-modules A.

Theorem 3.81. *a) For a ring R, the following are equivalent:*
(i) R is hereditary.
(ii) Every R-module M admits a projective resolution of the form $0 \to P_1 \to P_0 \to M \to 0$.
(iii) For all R-modules M and N and all $n \geq 2$, $\mathrm{Ext}^n_R(M, N) = 0$.
b) The conditions of part a) imply:
(iv) For all R-modules M and N and all $n \geq 2$, $\mathrm{Tor}^n_R(M, N) = 0$.
c) If R is Noetherian, then (iv) $\implies$ (i) and thus all are equivalent.

Proof. CITE. □

Exercise: Use Corollary 3.56 to show (i) $\implies$ (ii) $\implies$ (iii).

Theorem 3.82. *For R-modules A and C, the following are equivalent:*
(i) Every short exact sequence $0 \to A \to B \twoheadrightarrow C \to 0$ splits.
(ii) $\mathrm{Ext}^1_R(C, A) = 0$.

Proof. See e.g. [Rot, Thm. 7.31]. □

3.11. **More on flat modules.**

Theorem 3.83. *(Tensorial Criterion for Flatness) For an R-module M, TFAE:*
(i) M is flat.
(ii) For every finitely generated ideal I of R the canonical map $I \otimes_R M \to IM$ is an isomorphism.

Proof. Fist note that the canonical map $I \otimes_R M \to IM$ is always a surjection.
(i) $\implies$ (ii): if M is flat, then since $I \hookrightarrow R$, $I \otimes_R M \hookrightarrow R \otimes_R M = M$, so $I \otimes_R M \xrightarrow{\sim} IM$.
(ii) $\implies$ (i): Every ideal of R is the direct limit of its finitely generated subideals, so it follows from Proposition 3.9 and the exactness of direct limits that $I \otimes M \to M$

is injective for *all* ideals I. Moreover, if N is an R-module and $N' \subset N$ is an R-submodule, then since N is the direct limit of submodule $N' + F$ with F finitely generated, to show that $N' \otimes M \to N \otimes M$ is injective we may assume

$$N = N' + \langle \omega_1, \ldots, \omega_n \rangle_R.$$

We now proceed by dévissage: putting $N_i = N' + \langle \omega_1, \ldots, \omega_i \rangle_R$, it is enough to show injectivity at each step of the chain

$$N' \otimes M \to N_1 \otimes M \to \ldots \to N \otimes M,$$

and further simplifying, it is enough to show that if $N = N' + R\omega$, then $N' \otimes M \hookrightarrow N \otimes M$. Let I be the "conductor ideal of N/N'", i.e., $I = \{x \in R \mid x\omega \in N'\}$, so that we get a short exact sequence of R-modules

$$0 \to N' \to N \to R/I \to 0$$

which gives rise to a long exact homology sequence

$$\ldots \to \mathrm{Tor}_1^R(M, R/I) \to N' \otimes M \to N \otimes M \to M/IM \to 0.$$

Thus it suffices to prove $\mathrm{Tor}_1^R(M, R/I) = 0$. For this we consider the homology sequence associated to

$$0 \to I \to R \to R/I \to 0,$$

namely

$$\ldots \to \mathrm{Tor}_1^R(M, R) = 0 \to \mathrm{Tor}_1^R(M/R/I) \to I \otimes M \to M \to \ldots,$$

and from the injectivity of $I \otimes M \to M$ we deduce $\mathrm{Tor}_1^R(M, R/I) = 0$. □

Theorem 3.84. *(Homological Criterion for Flatness) For an R-module M, TFAE:*
(i) M is flat.
(ii) For every R-module N all $i > 0$, $\mathrm{Tor}_i^R(M, N) = 0$.
(ii′) For every R-module N, $\mathrm{Tor}_1^R(M, N) = 0$.
(iii) For every finitely generated ideal I of R, $\mathrm{Tor}_1^R(M, R/I) = 0$.

Proof. (i) $\implies$ (ii): This is a statement about projective resolutions, but given that it is just about the most basic possible one. Namely, let $L_\bullet \to N \to 0$ be a projective resolution of N. Then

$$\ldots \to L_n \otimes M \to L_{n-1} \otimes M \to \ldots \to L_0 \otimes M$$

is exact, so $\mathrm{Tor}_i^R(M, N) = 0$ for all $i > 0$.
(ii) $\implies$ (ii′) and (ii′) $\implies$ (iii) are both immediate.
(iii) $\implies$ (i): For each finitely generated ideal I of R, the short exat sequence

$$0 \to I \to R \to R/I \to 0$$

of R-modules induces a long exact sequence in homology, which ends

$$\ldots \to \mathrm{Tor}_1^R(M, R/I) = 0 \to I \otimes M \to M \to M/IM \to 0,$$

i.e., the map $I \otimes M \to M$ is injective and thus induces an isomorphism $I \otimes M \xrightarrow{\sim} IM$. Using the Tensorial Criterion for Flatness (Theorem 3.83), we conclude M is flat. □

Corollary 3.85. *(Direct limits preserve flatness) Let R be a ring and $\{M_i\}_{i \in I}$ a directed system of flat R-modules. Then $M = \varinjlim M_i$ is a flat R-module.*

Proof. For every R-module N, we have

$$\mathrm{Tor}_1^R(\varinjlim M_i, N) \cong \mathrm{Tor}_1^R(N, \varinjlim M_i) = \varinjlim \mathrm{Tor}_1^R(N, M_i) \cong \varinjlim \mathrm{Tor}_1^R(M_i, N) = \varinjlim 0 = 0.$$

Now apply the Homological Criterion for Flatness. □

Corollary 3.86. *For a domain R, TFAE:*
(i) Every finitely generated torsionfree R-module is flat.
(ii) Every torsionfree R-module is flat.

Proof. Every submodule of a torsionfree R-module is torsionfree, and every R-module is the direct limit of its finitely generated submodules. So the result follows immediately from Proposition 3.85. □

Corollary 3.87. *Let $0 \to M' \to M \to M'' \to 0$ be a short exact sequence of R-modules, with M'' flat. Then M' is flat iff M is flat.*

Exercise 3.80: Use the Homological Criterion of Flatness to prove Corollary 3.87.

Exercise 3.81: In a short exact sequence of R-modules as in Corollary 3.87, if M' and M are flat, must M'' be flat?

Now recall that a finitely generated torsion free module over a PID is free (Proposition 3.58). From this we deduce:

Corollary 3.88. *A module over a PID is flat iff it is torsionfree.*

Exercise 3.82: Let R be a domain and M a torsion R-module. Show that for all R-modules N and all $n \geq 0$, $\mathrm{Tor}_n(M, N)$ is a torsion R-module.

Theorem 3.89. *Let R be a PID and let M, N be R-modules.*
a) For all $n \geq 2$, $\mathrm{Tor}_n(M, N) = 0$.
b) $\mathrm{Tor}_1(M, N)$ is a torsion R-module.

Proof. a) Choose a free module F_0 and a surjection $d_0 : F_0 \to N$. By X.X, $F_1 = \mathrm{Ker}(d_0)$ is free, so we get a **finite free resolution of N**:

$$0 \to F_1 \to F_0 \to N \to 0.$$

Therefore we certainly have $\mathrm{Tor}_n(M, N)$ for all M and all $n \geq 2$.
b) Let $\{M_i\}_{i \in I}$ be the direct system of all finitely generated submodules of M. As above, we have $M = \varinjlim M_i$, so

$$\mathrm{Tor}_1(M, N) = \mathrm{Tor}_1(\varinjlim M_i, N)) = \varinjlim \mathrm{Tor}_1(M_i, N).$$

By Corollary 3.88, each M_i which is torsionfree is flat, hence $\mathrm{Tor}_1(M_i, N) = 0$. Thus the only possible contribution to $\varinjlim \mathrm{Tor}_1(M_i, N)$ comes from torsion modules M_i, and by Exercise X.X, M_i torsion implies $\mathrm{Tor}_1(M_i, N)$ torsion. Thus $\mathrm{Tor}_1(M, N)$ is a direct limit of torsion modules, hence itself a torsion module. □

Theorem 3.90. *(Equational Criterion for Flatness) Let M be an R-module.*
a) Suppose M is flat, and that we are given $r, n \in \mathbb{Z}^+$, a matrix $A = (a_{ij}) \in M_{r \times n}(R)$ and elements $x_1, ldots, x_n \in M$ such that

$$\forall 1 \leq i \leq r, \ \sum_j a_{ij} x_j = 0.$$

Then there exists $s \in \mathbb{Z}^+$, $b_{jk} \in R$ and $y_k \in M$ (for $1 \leq j \leq n$ and $1 \leq k \leq s$) such that

$$\forall i, k, \ \sum_j a_{ij} b_j = 0$$

and

$$\forall j, \ x_j = \sum_j b_{jk} y_k = 0.$$

Thus the solutions in a flat module of a system of linear equations with R-coefficients can be expressed as a linear combination of solutions of the system in R.
b) Conversely, if the above conditions hold for a single equation (i.e., with $r = 1$), then M is a flat R-module.

Proof. a) Let $\varphi : R^n \to R^r$ be the linear map corresponding to multiplication by the matrix A and let $\varphi_M : M^n \to M^r$ be the same for M, so that $\varphi_M = \varphi \otimes 1_M$. Let $K = \operatorname{Ker} \varphi$. Since M is flat, tensoring with M preserves exact sequences, thus the sequence

$$K \otimes_R M \overset{\iota \otimes 1}{\to} M^n \overset{\varphi}{\to} M^r$$

is exact. By our hypothesis we have $\varphi_M(x_1, \ldots, x_n) = 0$, so that we may write

$$(x_1, \ldots, x_n) = (\iota \otimes 1) \left(\sum_{k=1}^{s} \beta_k \otimes y_k \right)$$

with $\beta_k \in K$ and $y_k \in M$. Writing out each β_k as an element $(b_{1k}, \ldots, b_{nk}) \in R^n$ gives the desired conclusion.
b) We will use the Tensorial Criterion for Flatness to show that M is flat. Let $I = \langle a_1, \ldots, a_n \rangle$ be a finitely generated ideal of R. We may write an arbitrary element z of $I \otimes M$ as $\sum_{i=1}^n a_i \otimes m_i$ with $m_i \in M$. Let $\overline{z} = \sum_{i=1}^n a_i m_i$ denote the image of z in $IM \subset M$. We want to show that $\overline{z} = 0$ implies $z = 0$, so suppose that $\sum_i a_i m_i = 0$. By hypothesis, there exist $b_{ij} \in R$ and $y_j \in M$ such that for all j, $\sum_i a_i b_{ij} = 0$ and for all i, $m_i = \sum_j b_{ij} y_j$. Thus

$$z = \sum_i a_i \otimes m_i = \sum_i \sum_j a_i b_{ij} \otimes y_j = \sum_j \left(\sum_i a_i b_{ij} \right) \otimes y_j = \sum_j 0 \otimes y_j = 0.$$

□

As an application, we can now improve Theorem 3.49 by weakening the hypothesis of "finite presentation" to the simpler one of "finite generation".

Theorem 3.91. *Let M be a* finitely generated *flat module over the local ring $(R, \mathfrak{m})$. Then for all $n \in \mathbb{Z}^+$, $x_1, \ldots, x_n$ are elements of M such that the images in $R/\mathfrak{m}$ are $R/\mathfrak{m}$-linearly independent, then $x_1, \ldots, x_n$ are R-linearly independent.*

Proof. We go by induction on n. Suppose first that $n = 1$, in which case it is sufficient to show that $a_1 \in R$, $a_1 x_1 \neq 0$ implies $a_1 = 0$. By the Equational Criterion for Flatness, there exist $b_1, \ldots, b_s \in R$ such that $ab_i = 0$ for all i and $x_1 \in \sum_i b_i M$. By assumption, x_1 does not lie in $\mathfrak{m}M$, so that for some i we must have $b_i \in R^\times$, and then $ab_i = 0$ implies $a = 0$.

Now suppose $n > 1$, and let $a_1, \ldots, a_n \in R$ are such that $a_1 x_1 + \ldots + a_n x_n = 0$. Again using the Equational Criterion for Flatness, there are $b_{ij} \in R$ and $y_1, \ldots, y_s \in M$ such that for all j, $\sum a_i b_{ij} = 0$ and $x_i = \sum b_{ij} y_j$. Since the set of generators

is minimal, by Nakayama's Lemma their images in $M/\mathfrak{m}M$ must be $R/\mathfrak{m}$-linearly independent. In particular $x_n \notin \mathfrak{m}M$, so that at least one b_{nj} is a unit. It follows that there exist $c_1, \ldots, c_{n-1} \in R$ such that $a_n = \sum_{i=1}^{n-1} a_i c_i$. Therefore

$$a_1(x_1 + c_1 x_n) + \ldots + a_{n-1}(x_{n-1} + c_{n-1} x_n) = 0.$$

The images in $M/\mathfrak{m}M$ of the $n-1$ elements $x_1 + c_1 x_n, \ldots, x_{n-1} + c_{n-1} x_n$ are $R/\mathfrak{m}$-linearly independent, so by induction $a_1 = \ldots = a_{n-1} = 0$. Thus $a_n = 0$. □

Theorem 3.92. *For a finitely generated module M over a local ring R, TFAE:*
(i) M is free.
(ii) M is projective.
(iii) M is flat.

Proof. For any module over any ring we have (i) $\implies$ (ii) $\implies$ (iii). So suppose that M is a finitely generated flat module over the local ring $(R, \mathfrak{m})$. Let $(x_1, \ldots, x_n)$ be a set of R-module generators for M of minimal cardinality. By Nakayama's Lemma the images of $x_1, \ldots, x_n$ in $R/\mathfrak{m}$ are $R/\mathfrak{m}$-linearly independent, and then Theorem 3.91 implies that $x_1, \ldots, x_n$ is a basis for M as an R-module. □

A ring R is called **absolutely flat** if every R-module is flat.

Exercise 3.83: Show that any quotient of an absolutely flat ring is absolutely flat.

Proposition 3.93. *For a ring R, TFAE:*
(i) R is absolutely flat.
(ii) For every principal ideal I of R, $I^2 = I$.
(iii) Every finitely generated ideal of R is a direct summand of R.

Proof. (i) $\implies$ (ii): Assume R is absolutely flat, and let $I = (x)$ be a principal ideal. Tensoring the natural inclusion $(x) \to R$ with $R/(x)$, we get a an injection $(x) \otimes_R R/(x) \to R/(x)$. But this map sends $x \otimes r \mapsto xr + (x) = (x)$, so it is identically zero. Therefore its injectivity implies that $0 = (x) \otimes_R R/(x) \cong (x)/(x^2)$, so $(x) = (x^2)$.

(ii) $\implies$ (iii): Let $x \in R$. Then $x = ax^2$ for some $a \in R$, so putting $e = ax$ we have $e^2 = a^2x^2 = a(ax^2) = ax = e$, so e is idempotent, and $(e) = (x)$. In general, for any two idempotents e, f, we have $\langle e, f \rangle = (e + f - ef)$. Hence every finitely generated ideal is principal, generated by an idempotent element, and thus a direct summand.

(iii) $\implies$ (i): Let M be an R-module, and let I be any finitely generated ideal of R. By assumption, we may choose J such that $R = I \oplus J$. Therefore J is projective, so $\mathrm{Tor}_1(R/I, M) = \mathrm{Tor}_1(J, M) = 0$. By the Homological Criterion for Flatness, M is flat. □

Exercise 3.84: Show that any (finite or infinite) product of absolutely flat rings is absolutely flat.

The following striking result came relatively late in the game: it is due independently to Govorov [Gov65] and Lazard [Laz64].

Theorem 3.94. *(Govorov-Lazard) For a module M over a ring R, TFAE:*
(i) M is flat.
(ii) There exists a directed family $\{F_i\}_{i \in I}$ of finitely generated free submodules of M such that $M = \varinjlim F_i$.

Proof. (i) $\implies$ (ii): Suppose $M = \varinjlim F_i$ is a direct limit of free modules. Then in particular M is a direct limit of flat modules, so by Corollary 3.85 M is flat.
(ii) $\implies$ (i): see [Eis, Thm. A6.6]. □

3.11.1. *Flat Base Change.*

Proposition 3.95. *(Stability of flatness under base change) Let M be a flat R-module, and $f : R \to S$ a ring homomorphism. Then $S \otimes_R M$ is a flat S-module.*

Exercise 3.85: Prove Proposition 3.95.

Exercise 3.86: Show that the tensor product of flat R-modules is a flat R-module.

Exercise 3.87: Let R be a nonzero commutative ring, and $n, m \in \mathbb{N}$.
a) Show that $R^m \cong R^n$ iff $m = n$.
b) Suppose that $\varphi : R^m \to R^n$ is a surjective R-module map. Show that $m \geq n$.
c)[22] Suppose that $\varphi : R^m \to R^n$ is an injective R-module map. Show that $m \leq n$.
d) Find a noncommutative ring R for which part a) fails.

Theorem 3.96. *(Hom commutes with flat base change) Let S be a flat R-algebra and M, N R-modules with M finitely presented. Then the canonical map*

$$\Phi_M : S \otimes_R \mathrm{Hom}_R(M, N) \to \mathrm{Hom}_S(M \otimes_R S, N \otimes_R S)$$

induced by $(s, f) \mapsto (m \otimes t) \mapsto f(m) \otimes st$ is an isomorphism.

Proof. (Hochster) It is immediate that Φ_R is an isomorphism and that $\Phi_{M_1 \oplus M_2} = \Phi_{M_1} \oplus \Phi_{M_2}$, and thus Φ_M is an isomorphism when M is finitely generated free. For finitely presented M, there is an exact sequence

$$H \to G \to M \to 0$$

with H and G finitely generated free modules. Now we have the following commutative diagram:

$$0 \longrightarrow 0$$

$$S \otimes_R \mathrm{Hom}_R(M, N) \xrightarrow{\theta_M} \mathrm{Hom}_S(M \otimes_R S, N \otimes_R S)$$

$$S \otimes_R \mathrm{Hom}_R(G, N) \xrightarrow{\theta_G} \mathrm{Hom}_S(G \otimes_R S, N \otimes_R S)$$

$$S \otimes_R \mathrm{Hom}_R(H, N) \xrightarrow{\theta_H} \mathrm{Hom}_S(H \otimes_R S, N \otimes_R S).$$

Note that the right column is obtained by first applying the exact functor $A \mapsto A \otimes_R S$ and then applying the right exact cofunctor $U \mapsto \mathrm{Hom}_S(U, N \otimes_R S)$, so it is exact. Similarly, the left column is obtained by first applying the right exact cofunctor $A \mapsto \mathrm{Hom}_R(A, N)$ and then applying the exact (since R is flat) functor $A \mapsto A \otimes_R S$, so is exact. Since G and H are finitely generated free, θ_G and θ_H are isomorphisms, and a diagram chase shows that θ_M is an isomorphism. □

[22]This is actually quite challenging.

3.12. **Faithful flatness.**

Proposition 3.97. *For an R-module M, TFAE:*
(i) For a sequence

$$N_1 \xrightarrow{\alpha} N_2 \xrightarrow{\beta} N_3 \tag{11}$$

of left R-modules to be exact it is necessary and sufficient that

$$M \otimes_R N_1 \xrightarrow{A} M \otimes_R N_2 \xrightarrow{B} M \otimes_R N_3 \tag{12}$$

be exact.
(ii) M is flat and for all nonzero R-modules N, $M \otimes_R N \neq 0$.
(iii) M is flat and for all nonzero R-module maps $u : N \to N'$,

$$1_M \otimes u : M \otimes_R N \to M \otimes_R N' \text{ is not zero .}$$

(iv) M is flat and for every $\mathfrak{m} \in \operatorname{MaxSpec} R$, $\mathfrak{m}M \subsetneq M$.
(v) M is flat and for every $\mathfrak{p} \in \operatorname{Spec} R$, $\mathfrak{p}M \subsetneq M$.
A module satisfying these equivalent conditions is ***faithfully flat****.*

Proof. (i) $\implies$ (ii): Certainly (i) implies that M is flat. Moreover, if N is a nonzero R-module such that $M \otimes N = 0$, then $0 \to N \to 0$ is not exact but its tensor product with M is exact, contradicting (i).
(ii) $\implies$ (iii): Let $I = \operatorname{Im}(u)$; then $M \otimes I = \operatorname{Im}(1_M \otimes u)$. So assuming (ii) and that $I \neq 0$, we conclude $\operatorname{Im}(1_M \otimes u) \neq 0$.
(iii) $\implies$ (i): Assume (iii). Then, since M is flat, if (11) is exact, so is (12). Conversely, suppose (12) is exact, and put $I = \operatorname{Im}(\alpha)$, $K = \ker(\beta)$. Then $B \circ A = 1_M \otimes (\beta \circ \alpha) = 0$, so $\beta \circ \alpha = 0$, or in other words, $I \subset K$. We may therefore form the exact sequence

$$0 \to I \to K \to K/I \to 0,$$

and tensoring with the flat module M gives an exact sequence

$$0 \to M \otimes I \to M \otimes K \to M \otimes K/I \to 0.$$

But $M \otimes K = M \otimes I$ by hypothesis, so $K/I = 0$ and $I = K$.
(ii) $\implies$ (iv): Let $\mathfrak{m} \in \operatorname{MaxSpec} R$. Then $R/\mathfrak{m}$ is a nonzero R-module, so by (ii) so is $M \otimes R/\mathfrak{m} = M/\mathfrak{m}M$, i.e., $\mathfrak{m}M \subsetneq M$.
(iv) $\implies$ (ii): Assume (iv) holds. Then, since every proper ideal is contained in a maximal ideal, we have moreover that for all proper ideals I of R, $IM \subsetneq M$, or equivalently $M \otimes (R/I) \neq 0$. But the modules of the form R/I as I ranges over all proper ideals of R are precisely all the *cyclic* (a.k.a. monogenic) R-modules, up to isomorphism. Now if N is any nonzero R-module, choose $0 \neq x \in M$ and let $N' = \langle x \rangle$ by the cyclic submodule spanned by x. It follows that $M \otimes N' \neq 0$. Since M is flat, $N' \hookrightarrow N$ implies $M \otimes N' \hookrightarrow M \otimes N$, so $M \otimes N \neq 0$.
(iv) $\iff$ (v): this follows immediately from the proofs of the last two implications, as we leave it to the reader to check. □

Exercise 3.88: Show that (iv) $\iff$ (v) in Proposition 3.97.

Corollary 3.98. *Let M be a faithfully flat and $u : N \to N'$ an R-module map. Then:*
a) u is injective iff $1_M \otimes u : M \otimes N \to M' \otimes N$ is injective.
b) u is surjective iff $1_M \otimes u$ is surjective.
c) u is an isomorphism iff $1_M \otimes u$ is an isomorphism.

Exercise 3.89: Deduce Corollary 3.98 from Proposition 3.97.

Exercise 3.90: Use each of the criteria of Proposition 3.97 to show that the (flat) $\mathbb{Z}$-module $\mathbb{Q}$ is not faithfully flat.

Exercise 3.91: Show that a faithfully flat module is faithful and flat, and that – unfortunately! – a flat, faithful module need not be faithfully flat.

Exercise 3.92: Show that a nonzero free module is faithfully flat but that a nonzero (even finitely generated) projective module need not be.

Exercise 3.93: Let $\{M_i\}_{i \in I}$ be a family of flat R-modules, and put $M = \bigoplus_{i \in I} M_i$.
a) Suppose that for some i, M_i is faithfully flat. Show that M is faithfully flat.
b) Give an example where no M_i is faithfully flat yet M is faithfully flat.

Proposition 3.99. *Let $0 \to M' \to M \to M'' \to 0$ be a short exact sequence of R-modules. Suppose M' and M'' are flat and that at least one is faithfully flat. Then M is faithfully flat.*

Proof. By Proposition 3.87, M is flat. Now let N be any R-module. Since M'' is flat, $\mathrm{Tor}_1(M'', N) = 0$ so

$$0 \to M' \otimes N \to M \otimes N \to M'' \otimes N \to 0$$

is exact. Thus if $M \otimes N = 0$ then $M' \otimes N = M'' \otimes N = 0$. Since one of M', M'' is faithfully flat, by criterion (ii) of Proposition 3.97 we have $N = 0$, and then that same criterion shows that M is faithfully flat. □

By a **faithfully flat R-algebra**, we mean a ring S equipped with a ring homomorphism $R \to S$ making S into a faithfully flat R-module.

Proposition 3.100. *Let $f : R \to S$ be a ring map and M an R-module. Then: M is faithfully flat iff $M \otimes_R S$ is faithfully flat.*

Proof. The key fact is that for any S-module N, we have

$$(M \otimes_R S) \otimes_S N \cong_R M \otimes_R N.$$

With this, the proof becomes straightforward and is left to the reader. □

Exercise 3.94: Complete the proof of Proposition 3.100.

Theorem 3.101. *For a flat algebra $f : R \to S$, TFAE:*
(i) S is faithfully flat over R.
(ii) $f^* : \mathrm{MaxSpec}\, S \to \mathrm{MaxSpec}\, R$ is surjective.
(iii) $f^* : \mathrm{Spec}\, S \to \mathrm{Spec}\, R$ is surjective.

Proof. (i) $\iff$ (ii): Let $\mathfrak{m}$ be any maximal ideal of R. Then $\mathfrak{m}S \subsetneq S$ holds iff there is a maximal ideal $\mathcal{M}$ of S containing $\mathfrak{m}S$ iff $f^*(\mathcal{M}) = \mathfrak{m}$. The equivalence now follows from criterion (iv) of Proposition 3.97.
(i) $\implies$ (iii): Let $\mathfrak{p} \in \mathrm{Spec}\, R$, and let $k(\mathfrak{p})$ be the fraction field of the domain $R/\mathfrak{p}$. By faithful flatness, $S \otimes_R k(\mathfrak{p})$ is a nonzero $k(\mathfrak{p})$-algebra so has a prime ideal $\mathcal{P}$. Consider the composite map $h : R \xrightarrow{f} S \xrightarrow{g} S \otimes_R k(\mathfrak{p})$. We CLAIM that $g^* : \mathrm{Spec}(S \otimes_R k(\mathfrak{p})) \to \mathrm{Spec}\, R$ has image precisely $\{\mathfrak{p}\}$. The proof of this result, a spectral description of the **fiber of the morphism** $f : R \to S$ over $\mathfrak{p}$, will have to

wait until we have developed the theory of localization in §7.3. Assuming it for now, we get that $g^*(\mathcal{P})$ is a prime ideal of $\operatorname{Spec} S$ such that $f^*g^*(\mathcal{P}) = (g \circ f)^*(\mathcal{P}) = \mathfrak{p}$, so $f^* : \operatorname{Spec} S \to \operatorname{Spec} R$ is surjective.
(iii) $\implies$ (ii): Let $\mathfrak{m} \in \operatorname{MaxSpec} R \subset \operatorname{Spec} R$. By assumption, the set of prime ideals $\mathcal{P}$ of S such that $f^*\mathcal{P} = \mathfrak{m}$ is nonempty. Moreover the union of any chain of prime ideals pulling back to $\mathfrak{m}$ is again a prime ideal pulling back to $\mathfrak{p}$, so by Zorn's Lemma there exists an ideal $\mathcal{M}$ which is maximal with respect to the property that $f^*\mathcal{M} = \mathfrak{m}$. Suppose $\mathcal{M}$ is not maximal and let $\mathcal{M}'$ be a maximal ideal properly containing $\mathcal{M}$. Then by construction $f^*(\mathcal{M}')$ properly contains the maximal ideal $\mathfrak{m}$ of R, i.e., $f^*(\mathcal{M})') = R$, contradicting the fact that prime ideals pull back to prime ideals. So $\mathcal{M}$ is indeed maximal in S. □

Proposition 3.102. *Let $f : R \hookrightarrow S$ be a ring extension such that S is a faithfully flat R-module, and let M be an R-module. Then:*
a) M is finitely generated iff $M \otimes_R S$ is finitely generated.
b) M is finitely presented iff $M \otimes_R S$ is finitely presented.

Proof. Note first that the properties of finite generation and finite presentation are preserved by arbitrary base change $f : R \to S$. So it suffices to prove that if $M \otimes_R S$ is finitely generated (resp. finitely presented), then M is finitely generated (resp. finitely presented).
a) Since $M \otimes_R S$ is finitely generated over S, it has a finite set of S-module generators of the form $x_i \otimes 1$. Let $N = \langle x_1, \ldots, x_n \rangle_R$ and $\iota : N \hookrightarrow M$ the canonical injection. Then $\iota_S : N \otimes_R S \to M \otimes_R S$ is an isomorphism, so by faithful flatness ι was itself an isomorphism and thus $M = \langle x_1, \ldots, x_n \rangle$ is finitely generated.
b) By part a), M is finitely generated over R, so let $u : R^n \to M$ be a surjection. Since $M \otimes_R S$ is finitely presented, the kernel of $u_S : S^n \to M \otimes_R S$ is finitely generated over S. Since by flatness $\ker u_S = (\ker u)_S$, part a) shows that $\ker u$ is finitely generated and thus that M is finitely presented. □

Lemma 3.103. *Let $f : R \to S$ be a ring map, and let M, N be R-modules.*
a) There is a canonical S-module map

$$\omega : \operatorname{Hom}_R(M, N) \otimes_R S \to \operatorname{Hom}_S(M \otimes_R S, N \otimes_R S)$$

such that for all $u \in \operatorname{Hom}_R(M, N)$, $\omega(u \otimes 1) = u \otimes 1_B$.
b) If S is flat over R and M is finitely generated, then ω is injective.
c) If S is flat over R and M is finitely presented, then ω is an isomorphism.

Exercise 3.95: Prove Lemma 3.103. (It is not difficult, really, but it is somewhat technical. Feel free to consult [B, p. 23] for the details.)

Theorem 3.104. *(Faithfully flat descent for projective modules) Let $f : R \hookrightarrow S$ be a faithfully flat ring extension, and let P be an R-module. Then P is finitely generated and projective iff $P \otimes_R S$ is finitely generated and projective.*

Proof. Begin, once again the implication P finitely generated projective implies $P \otimes_R S$ is finitely generated projective holds for any base change. So suppose $P \otimes_R S$ is finitely generated projective. Then $P \otimes_R S$ is finitely presented, so by Proposition 3.102, M is finitely presented. It remains to show that M is projective.

Let $v : M \to N$ be a surjection of R-modules. We wish to show that the natural map $\operatorname{Hom}_R(P, M) \to \operatorname{Hom}_R(P, N)$ is surjective. Because of the faithful flatness

of S/R, it is sufficient to show that $\mathrm{Hom}_R(P,M) \otimes_R S \to \mathrm{Hom}_R(P,N) \otimes_R S$ is surjective, and by Lemma 3.103 this holds iff

$$\mathrm{Hom}_S(P \otimes_R S, M \otimes_R S) \to \mathrm{Hom}_S(P \otimes_R S, N \otimes_R S)$$

is surjective. But this latter map is surjective because $M \otimes_R S \to N \otimes_R S$ is surjective and the S-module $P \otimes_R S$ is projective by assumption. □

4. First Properties of Ideals in a Commutative Ring

4.1. **Introducing maximal and prime ideals.**

Consider again the set $\mathcal{I}(R)$ of all ideals of R, partially ordered by inclusion. The maximal element is the ideal R itself, and the minimal element is the ideal (0).

In general our attitude to the ideal R of R is as follows: although we must grudgingly admit its existence – otherwise, given a subset S of R it would be in general a difficult question to tell whether the ideal $\langle S \rangle$ generated by S "exists" (i.e., is proper) or not – nevertheless we regard it as exceptional and try to ignore it as much as possible. Because of this we define an ideal I of R to be **maximal** if it is maximal among all *proper* ideals of R, i.e., $I \subsetneq R$ and there does not exist J such that $I \subsetneq J \subsetneq R$. That this is a more interesting concept than the literally maximal ideal R of R is indicated by the following result.

Proposition 4.1. *For an ideal I of R, TFAE:*
(i) I is maximal.
(ii) R/I is a field.

Proof. Indeed, R/I is a field iff it has precisely two ideals, I and R, which by the Correspondence Theorem says precisely that there is no proper ideal strictly containing I. □

Example: In $R = \mathbb{Z}$, the maximal ideals are those of the form (p) for p a prime number. The quotient $\mathbb{Z}/p\mathbb{Z}$ is the finite field of order p.

Does every ring have a maximal ideal? With a single (trivial) exception, the answer is yes, assuming – as we must, in order to develop the theory as it is used in other branches of mathematics – suitable transfinite tools.

Proposition 4.2. *Let R be a nonzero ring and I a proper ideal of R. Then there exists a maximal ideal of R containing I.*

Proof. Consider the set S of all proper ideals of R containing I, partially ordered by inclusion. Since $I \in S$, S is nonempty. Moreover the union of a chain of ideals is an ideal, and the union of a chain of proper ideals is proper (for if 1 were in the union, it would have to lie in one of the ideals of the chain). Therefore by Zorn's Lemma we are entitled to a maximal element of S, which is indeed a maximal ideal of R that contains I. □

Corollary 4.3. *A nonzero ring R contains at least one maximal ideal.*

Proof. Apply Proposition 4.2 with $I = (0)$. □

Remark: The zero ring has the disquieting property of having no maximal ideals.

Remark: The appeal to Zorn's Lemma cannot be avoided, in the sense that Corollary 4.3 implies the Axiom of Choice (AC). In fact, W. Hodges has shown that the axioms of ZF set theory together with the statement that every UFD (see §15) has a maximal ideal already implies AC [Ho79].

A proper ideal I of a ring R is **prime** if $xy \in I$ implies $x \in I$ or $y \in I$.

Exercise 4.1: Let $\mathfrak{p}$ be a prime ideal of R.
a) Suppose $x_1, \ldots, x_n$ are elements of R such that $x_1 \cdots x_n \in \mathfrak{p}$. Then $x_i \in \mathfrak{p}$ for some at least one i.
b) In particular, for $x \in R$ and $n \in \mathbb{Z}^+$ we have $x^n \in \mathfrak{p}$, then $x \in \mathfrak{p}$.

Proposition 4.4. *Let $f : R \to S$ be a homomorphism of rings, and let J be an ideal of S.*
a) Put $f^*(J) := f^{-1}(J) = \{x \in R \mid f(x) \in J\}$. Then $f^*(J)$ is an ideal of R.
b) If J is a prime ideal, so is $f^*(J)$.

Exercise 4.2: Prove Proposition 4.4.

Proposition 4.5. *For a commutative ring R, TFAE:*
(i) If $x, y \in R$ are such that $xy = 0$, then $x = 0$ or $y = 0$.
(ii) If $0 \neq x \in R$ and $y, z \in R$ are such that $xy = xz$, then $y = z$.
*A ring satisfying either of these two properties is called an **integral domain**.*

Proof. Assume (i), and consider $xy = xz$ with $x \neq 0$. We have $x(y - z) = 0$, and since $x \neq 0$, (i) implies $y - z = 0$, i.e., $y = z$. Assuming (ii) suppose $xy = 0$ with $x \neq 0$. Then $xy = 0 = x \cdot 0$, so applying cancellation we get $y = 0$. □

A **zero divisor** in a ring R is an element x such that there exists $0 \neq y \in R$ with $xy = 0$. (In particular 0 *is* a zero divisor, albeit not a very interesting one.) So property (i) expresses that there are no zero divisors other than 0 itself. Property (ii) makes sense in any commutative monoid and is called **cancellation**.

Remark: The terminology "integral domain" is motivated by the fact the integers $\mathbb{Z}$ satisfy (i) and (ii) of Proposition 4.5, so any ring which satisfies these properties can be viewed as a sort of ring of "generalized integers." The analogy is apt – in particular, later on we shall build from any integral domain a field of fractions in exactly the same way that the rational numbers are constructed from the integers – but the terminology is quite awkward, as the reader will come to appreciate. First of all the word "integral" is logically superfluous – we do not have any other definition of a domain, and indeed often we will use **domain** as a more succinct synonym for "integral domain". So why not just "domain"? One problem is that, being a property of an object and not an object itself, we would prefer an English word which is an adjective rather than a noun. So why not just "integral"? The problem is that the word "integral" will be used later for something else (not a property of a single ring but a property of an extension ring S of R). It would certainly be confusing to use the term integral for these two different concepts. Ideal would probably be to reserve the term "integral" for a ring without zero divisors, give some other name to integral extensions (**integrally algebraic**?), and eliminate the use of "domain" from terms like "principal ideal domain." (This would be

consistent with geometric terminology: an affine scheme $\operatorname{Spec} R$ is called integral iff R is an integral domain.) However, the terminology is too entrenched for this to be a feasible solution.

Proposition 4.6. *For an ideal I in a ring R, TFAE:*
(i) I is prime.
(ii) R/I is an integral domain.

Exercise 4.3: Prove Proposition 4.6.

Corollary 4.7. *A maximal ideal is prime.*

Proof. If I is maximal, R/I is a field, hence an integral domain, so I is prime. □

Corollary 4.7 is the first instance of a somewhat mysterious meta-principle in ideal theory: for some property P of ideals in a ring, it is very often the case that an ideal which is maximal with respect to the satisfaction of property P (i.e., is not strictly contained in any other ideal satisfying P) must be prime. In the above, we saw this with P = "proper". Here is another instance:

Proposition 4.8. *(Multiplicative Avoidance) Let R be a ring and $S \subset R$. Suppose: 1 is in S; 0 is not in S; and S is closed under multiplication: $S \cdot S \subset S$.*
Let $\mathcal{I}_S$ be the set of ideals of R which are disjoint from S. Then:
a) $\mathcal{I}_S$ is nonempty;.
b) Every element of $\mathcal{I}_S$ is contained in a maximal element of $\mathcal{I}_S$.
c) Every maximal element of $\mathcal{I}_S$ is prime.

Proof. a) $(0) \in \mathcal{I}_S$. b) Let $I \in \mathcal{I}_S$. Consider the subposet P_I of $\mathcal{I}_S$ consisting of ideals which contain I. Since $I \in P_I$, P_I is nonempty; moreover, any chain in P_I has an upper bound, namely the union of all of its elements. Therefore by Zorn's Lemma, P_I has a maximal element, which is clearly also a maximal element of $\mathcal{I}_S$. c) Let I be a maximal element of $\mathcal{I}_S$; suppose that $x, y \in R$ are such that $xy \in I$. If x is not in I, then $\langle I, x\rangle \supsetneq I$ and therefore contains an element s_1 of S, say

$$s_1 = i_1 + ax.$$

Similarly, if y is not in I, then we get an element s_2 of S of the form

$$s_2 = i_2 + by.$$

But then

$$s_1 s_2 = i_1 i_2 + (by) i_1 + (ax) i_2 + (ab) xy \in I \cap S,$$

a contradiction. □

In fact Corollary 4.7 is precisely the special case $S = \{1\}$ of Proposition 4.8.

If I and J are ideals of R, we define the **product** IJ to be the ideal generated by all elements of the form xy with $x \in I, y \in J$. Every element of IJ is of the form $\sum_{i=1}^n x_i y_i$ with $x_1, \ldots, x_n \in I,\ y_1, \ldots, y_n \in J$.

The following simple result will be used many times in the sequel.

Proposition 4.9. *Let $\mathfrak{p}$ be a prime ideal and $I_1, \ldots, I_n$ be ideals of a ring R. If $\mathfrak{p} \supset I_1 \cdots I_n$, then $\mathfrak{p} \supset I_i$ for at least one i.*

Proof. An easy induction argument reduces us to the case of $n = 2$. So suppose for a contradiction that $\mathfrak{p} \supset I_1 I_2$ but there exists $x \in I_1 \setminus \mathfrak{p}$ and $y \in I_2 \setminus \mathfrak{p}$. Then $xy \in I_1 I_2 \subset \mathfrak{p}$; since $\mathfrak{p}$ is prime we must have $x \in \mathfrak{p}$ or $y \in \mathfrak{p}$, contradiction. □

Exercise 4.4: Show that Proposition 4.9 characterizes prime ideals, in the sense that if $\mathfrak{p}$ is any ideal such that for all ideals I, J of R, $\mathfrak{p} \subset IJ$ implies $\mathfrak{p} \subset I$ or $\mathfrak{p} \subset JJ$, then $\mathfrak{p}$ is a prime ideal.

For an ideal I and $n \in \mathbb{Z}^+$, we denote the n-fold product of I with itself by I^n.

Corollary 4.10. *If $\mathfrak{p}$ is a prime ideal and I is any ideal, then $\mathfrak{p} \supset I^n \implies \mathfrak{p} \supset I$.*

4.2. **Radicals.**

An element x of a ring R is **nilpotent** if $x^n = 0$ for some $n \in \mathbb{Z}^+$. Obviously 0 is a nilpotent element; a ring in which 0 is the only nilpotent element is called **reduced**. An ideal I of R is **nil** if every element of I is nilpotent. An ideal I is **nilpotent** if there exists $n \in \mathbb{Z}^+$ such that $I^n = (0)$.

Proposition 4.11. *Let I be an ideal of a ring R.*
a) If I is nilpotent, then I is a nil ideal.
b) If I is finitely generated and nil, then I is nilpotent.

Proof. Part a) is immediate from the definition, as we invite the reader to check.

Suppose $I = \langle a_1, \ldots, a_n \rangle_R$. Since I is nil, for each i, $1 \leq i \leq r$, there exists n_i such that $a_i^{n_i} = 0$. Let $N = n_1 + \ldots + n_r$. We claim $I^N = 0$. Indeed, an arbirary element of I is of the form $x_1 a_1 + \ldots + x_n a_n$. Raising this element to the nth power yields a sum of monomials of the form $x_1^{j_1} \cdots x_r^{j_r} a_1^{j_1} \cdots a_r^{j_r}$, where $\sum_{i=1}^r j_i = N$. If we had for all i that $j_i < n_i$, then certainly $j_1 + \ldots + j_r < N$. So for at least one i we have $j_i \geq n_i$ and thus $x_i^{j_i} = 0$; so every monomial term equals zero. □

Exercise 4.5: Find a ring R and an ideal I of R which is nil but not nilpotent.

The **nilradical** $\mathcal{N}$ of R is the set of all nilpotent elements of R.

Proposition 4.12. *Let R be a ring.*
a) The nilradical $\mathcal{N}$ is a nil ideal of R.
b) The quotient $R/\mathcal{N}$ is reduced.
c) The map $q : R \to R/\mathcal{N}$ is universal *for maps from R into a reduced ring.*
d) The nilradical is the intersection of all prime ideals of R.

Proof. a) In establishing that $\mathcal{N}$ is an ideal, the only property which is not absolutely immediate is its closure under addition. Suppose $x^m = 0 = y^n$. Then every term in the binomial expansion of $(x + y)^{m+n-1}$ is an integer times $x^i y^{m+n-1-i}$ for $0 \leq i \leq m + n$. Here either $i \geq m$ so $x^i y^{m+n-1-i} = 0 \cdot y^{m+n-i} = 0$, or $m + n - 1 - i \geq n$, so $x^i y^{m+n-i-i} = x^i \cdot 0 = 0$, so $x + y$ is nilpotent and $\mathcal{N}$ is an ideal, and by definintion a nil ideal.
b) Let $r + \mathcal{N}$ be a nilpotent element of $R/\mathcal{N}$, so there exists $n \in \mathbb{Z}^+$ such that $r^n \in \mathcal{N}$. But this means there exists $m \in \mathbb{Z}^+$ such that $0 = (r^n)^m = r^{nm}$, and thus r itself is a nilpotent element.
c) In plainer terms: if S is a reduced ring and $f : R \to S$ is a ring homomorphism, then there exists a unique homomorphism $\overline{f} : R/\mathcal{N} \to S$ such that $f = \overline{f} \circ q$. Given this, the proof is straightforward, and we leave it to the reader.

d) Suppose x is a nilpotent element of R, i.e., $\exists n \in \mathbb{Z}^+$ such that $x^n = 0$. If $\mathfrak{p}$ is a prime ideal, then since $0 = x \cdots x \in \mathfrak{p}$, we conclude $x \in \mathfrak{p}$: this shows $\mathcal{N} \subset \bigcap \mathfrak{p}$. Conversely, suppose x is not nilpotent. Then the set $S_x := \{x^n \mid n \in \mathbb{N}\}$ satisfies (i) and (ii) of Proposition 4.8, so we may apply that result to get a prime ideal $\mathfrak{p}$ which is disjoint from S_x, hence not containing x. □

Exercise 4.6: Prove Proposition 4.12c).

An ideal I of a ring R is **radical** if for all $x \in R$, $n \in \mathbb{Z}^+$, $x^n \in I$ implies $x \in I$.

Exercise 4.7: a) Show that a prime ideal is radical.
b) Exhibit a radical ideal which is not prime.
c) Find all radical ideals in $R = \mathbb{Z}$.
d) Show that R is reduced iff (0) is a radical ideal.
e) Let $\{I_i\}$ be a set of radical ideals in a ring R. Show $I = \bigcap_i I_i$ is a radical ideal.

For any ideal I of R, we define the **radical** of I:

$$r(I) = \{x \in R \mid \exists n \in \mathbb{Z}^+ \ x^n \in I\}.$$

Proposition 4.13. *Let R be a commutative ring and I, J ideals of R.*
a) $r(I)$ is the intersection of all prime ideals containing I, and is a radical ideal.
b) (i) $I \subset r(I)$, (ii) $r(r(I)) = r(I)$; (iii) $I \subset J \implies r(I) \subset r(J)$.
c) $r(IJ) = r(I \cap J) = r(I) \cap r(J)$.
d) $r(I + J) = r(r(I) + r(J))$.
e) $r(I) = R \iff I = R$.
f) For all $n \in \mathbb{Z}^+$, $r(I^n) = r(I)$.
g) If R is Noetherian and $r(I) \supset J$, then there is $n \in \mathbb{Z}^+$ such that $I \supset J^n$.

Proof. First we make the following observation: under the canonical homomorphism $q : R \to R/I$, $r(I) = q^{-1}(\mathcal{N}(R/I))$. By Proposition 4.4a), $r(I)$ is an ideal.
a) Since $\mathcal{N}$ is the intersection of all prime ideals of R/I, $r(I)$ is the intersection of all prime ideals containing I, which is, by Exericse X.Xe), a radical ideal.
b) (i) is immediate from the definition, and (ii) and (iii) follow from the characterization of $r(I)$ as the intersection of all radical ideals containing I.
c) Since $IJ \subset I \cap J$, $r(IJ) \subset r(I \cap J)$. If $x^n \in I \cap J$, then $x^{2n} = x^n x^n \in IJ$, so $x \in r(IJ)$; therefore $r(IJ) = r(I \cap J)$. Since $I \cap J$ is a subset of both I and J, $r(I \cap J) \subset r(I) \cap r(J)$. Conversely, if $x \in r(I) \cap r(J)$, then there exist m and n such that $x^m \in I$ and $x^n \in J$, so $x^{mn} \in I \cap J$ and $x \in r(I \cap J)$.
d) Since $I + J \subset r(I) + r(J)$, $r(I + J) \subset r(r(I) + r(J))$. A general element of $r(I)+r(J)$ is of the form $x+y$, where $x^m \in I$ and $y^n \in J$. Then $(x+y)^{m+n} \in I+J$, so $x + y \in r(I + J)$.
e) Evidently $r(R) = R$. Conversely, if $r(I) = R$, then there exists $n \in \mathbb{Z}^+$ such that $1 = 1^n \in I$.
f) By part a), $r(I^n)$ is the intersection of all prime ideals $\mathfrak{p} \supset I^n$. But by Corollary 4.10, a prime contains I^n iff it contains I, so $r(I^n) = r(I)$.
g) Replacing R with R/I we may assume $I = 0$. Then J is a nil ideal in a Noetherian ring, so it is nilpotent. □

Remark: Proposition 4.13b) asserts that the mapping $I \mapsto r(I)$ is a **closure operator** on the lattice $\mathcal{I}(R)$ of ideals of R.

Exercise 4.8: Let I be an ideal in the ring R. Show that $r(I)$ is the intersection of all prime ideals containing I. (Hint: reduce to the case $I = 0$.)

An ideal $\mathfrak{p}$ of a ring R is **primary** if every zero divisor of $R/\mathfrak{p}$ is nilpotent. Equivalently, $xy \in \mathfrak{p}$, $x \notin \mathfrak{p} \implies y^n \in \mathfrak{p}$ for some $n \in \mathbb{Z}^+$. More on primary ideals in §X.X.

We also define the **Jacobson radical** $J(R)$ as the intersection of all maximal ideals of R. Evidently we have $\mathcal{N} \subset J(R)$.

Proposition 4.14. *Let R be a ring. An element x of R lies in the Jacobson radical $J(R)$ iff $1 - xy \in R^\times$ for all $y \in R$.*

Proof. Suppose x lies in every maximal ideal of R. If there exists y such that $1-xy$ is not a unit of R, then $1-xy$ lies in some maximal ideal $\mathfrak{m}$, and then $x \in \mathfrak{m}$ implies $xy \in \mathfrak{m}$ and then $1 = (1 - xy) + xy \in \mathfrak{m}$, a contradiction. Conversely, suppose that there is a maximal ideal $\mathfrak{m}$ of R which does not contain x. Then $\langle \mathfrak{m}, x \rangle = R$, so $1 = m + xy$ for some $m \in \mathfrak{m}$ and $y \in R$, and thus $1 - xy$ is not a unit. □

Proposition 4.15. *Let J be an ideal of R contained in the Jacobson radical, and let $\varphi : R \to R/J$ be the natural map.*
*a) For all $x \in R$, $x \in R^\times \iff \varphi(x) \in (R/J)^\times$: φ is **unit-faithful**.*
b) The map $\varphi^\times : R^\times \to (R/J)^\times$ is surjective.

Proof. a) For any homomorphism of rings $\varphi : R \to S$, if $x \in R^\times$ then there is $y \in R$ with $xy = 1$, so $1 = \varphi(1) = \varphi(xy) = \varphi(x)\varphi(y)$, and thus $\varphi(x) \in S^\times$. For the converse we assume $S = R/J$ and let $x \in R$ be such that $\varphi(x) \in (R/J)^\times$. Then there is $y \in R$ such that $xy-1 \in J$. Thus for each maximal ideal $\mathfrak{m}$ of R, $xy-1 \in \mathfrak{m}$. It follows that $x \notin \mathfrak{m}$, for otherwise $xy \in \mathfrak{m}$ and thus $1 = xy - (xy - 1) \in \mathfrak{m}$. So x is not contained in any maximal ideal and thus $x \in R^\times$.
b) This is immediate from part a): in fact we've shown that *every* preimage under φ of a unit in R/J is a unit in R. □

Remark: It is not yet clear why we have defined these two different notions of "radical." Neither is it so easy to explain in advance, but nevertheless let us make a few remarks. First, the Jacobson radical plays a very important role in the theory of noncommutative rings, especially that of finite dimensional algebras over a field. (Indeed, a finite dimensional k-algebra is semisimple – i.e., a direct product of algebras without nontrivial two-sided ideals – iff its Jacobson radical is zero. In the special case of commutative algebras this comes down to the simpler result that a finite dimensional commutative k-algebra is reduced iff it is a product of fields.) Note that one important place in commutative algebra in which the Jacobson radical $J(R)$ appears – albeit not by name, because of the necessity of putting the results in a fixed linear order – is in the statement of Nakayama's Lemma. In general, the defining condition of $\mathrm{nil}(R)$ – i.e., as the intersection of all prime ideals of R – together with the fact that the radical of an arbitrary ideal I corresponds to the nilradical of R/I, makes the nilradical more widely useful in commutative algebra (or so it seems to the author of these notes). It is also important to consider when the nil and Jacobson radicals of a ring coincide. A ring R for which every homomorphic image S has $\mathrm{nil}(S) = J(S)$ is called a **Jacobson ring**; such rings will be studied in detail in §12.

4.3. **Comaximal ideals.**

Recall that two ideals I and J in a ring R are **comaximal** if $I + J = R$. A family of ideals in R is **pairwise comaximal** if any two members of the family are comaximal.

Exercise 4.9: Let $I_1, \ldots, I_n$ be pairwise comaximal. Show: $\sum_{j=1}^n \prod_{i \neq j} I_i = R$.

Proposition 4.16. *Let I and J be ideals in R. If $r(I)$ and $r(J)$ are comaximal, so are I and J.*

Proof. Apply Proposition 4.13d) and then Proposition 4.13e) to $r(I) + r(J) = R$:

$$R = r(r(I) + r(J)) = r(I + J) = I + J.$$

□

Recall that a set $\{I_i\}$ of ideals of R is **pairwise comaximal** if for each $i \neq j$, $I_i + I_j = R$. An immediate corollary of Proposition 4.16 is that if $\{I_i\}$ are pairwise comaximal and $\{n_i\}$ are any positive integers, then $\{I_i^{n_i}\}$ are pairwise comaximal.

Lemma 4.17. *Let $K_1, \ldots, K_n$ be pairwise comaximal ideals in the ring R. Then $K_1 \cdots K_n = \bigcap_{i=1}^n K_i$.*

Proof. We go by induction on n: $n = 1$ is trivial and $n = 2$ is Lemma 3.17b). Suppose the theorem is true for any family of $n-1$ pairwise comaximal ideals. Let $K' = \bigcap_{i=2}^n$; by induction, $K' = K_2 \cdots K_n$. By Lemma 3.17c), $K_1 + K' = R$, so by the $n = 2$ case $\bigcap_{i=1}^n K_i = K_1 \cap K' = K_1 K' = K_1 \cdots K_n$. □

Theorem 4.18. *(Chinese Remainder Theorem, or "CRT") Let R be a ring and $I_1, \ldots, I_n$ a finite set of pairwise comaximal ideals. Consider the natural map*

$$\Phi : R \to \prod_{i=1}^n R/I_i,$$

$x \mapsto (x + I_i)_{i=1}^n$. Then Φ is surjective with kernel $I_1 \cdots I_n$, so that there is an induced isomorphism

$$\Phi : R/(I_1 \cdots I_n) \xrightarrow{\sim} \prod_{i=1}^n R/I_i. \tag{13}$$

Proof. The map Φ is well-defined and has kernel $\bigcap_{i=1}^n I_i$. Since the I_i's are pairwise comaximal, Lemma 4.17 gives $\bigcap_{i=1}^n I_i = I_1 \cdots I_n$. So it remains to show that Φ is surjective. We prove this by induction on n, the case $n = 1$ being trivial. So we may assume that the natural map $\Phi' : R \to R' := \prod_{i=1}^{n-1} R/I_i$ is surjective, with kernel $I' := I_1 \cdots I_{n-1}$. Let $(r', \overline{s})$ be any element of $R' \times R/I_n$. By assumption, there exists $r \in R$ such that $\Phi'(r + I') = r'$. Let s be any element of R mapping to $\overline{s} \in R/I_n$. By Lemma 3.15, $I' + I_n = R$, so there exist $x \in I'$, $y \in I_n$ such that $s - r = x + y$. Then $\Phi'(r + x) = r'$, and $r + x \equiv r + x + y \equiv s \pmod{I_n}$, so $\Phi(r + x) = (r', \overline{s})$ and Φ is surjective. □

Remark: In the classical case $R = \mathbb{Z}$, we can write $I_i = (n_i)$ and then we are trying to prove – under the assumption that the n_i's are coprime in pairs in the sense of elementary number theory – that the injective ring homomorphism $\mathbb{Z}/(n_1 \cdots n_n) \to \mathbb{Z}/n_1 \times \cdots \times \mathbb{Z}/n_n$ is an isomorphism. But both sides are finite

rings of order $n_1 \cdots n_n$, so since the map is an injection it must be an isomorphism! Nevertheless the usual proof of CRT in elementary number theory is much closer to the one we gave in the general case: in particular, it is constructive.

The following *modulization* of CRT is sometimes useful.

Theorem 4.19. *(Module-theoretic CRT) Let R be a ring, $I_1, \ldots, I_n$ a finite set of pairwise comaximal ideals, and let M be an R-module. Then $(I_1 \cdots I_n)M = \bigcap_{i=1}^r I_i M$, and there is an induced R-moduleisomorphism*

$$\Phi_M : M/(I_1 \cdots I_r)M \to \prod_{i=1}^n M/I_i M. \tag{14}$$

Proof. Indeed $\Phi_M = \Phi \otimes_R M$, so it is an isomorphism. Thus

$$\bigcap_{i=1}^r I_i M = \ker \left(M \to \prod_{i=1}^n M/I_i M \right) = (I_1 \cdots I_r)M.$$

□

Exercise 4.10: Let R be a ring and $I_1, \ldots, I_n$ any finite sequence of ideals. Consider the map $\Phi : R \to \prod_{i=1}^n R/I_i$ as in CRT.
a) Show that Φ is surjective only if the $\{I_i\}$ are pairwise comaximal.
b) Show that Φ is injective iff $\bigcap_{i=1}^n I_i = (0)$.

Exercise 4.11:
a) Let G be a finite commutative group with exactly one element z of order 2. Show that $\sum_{x \in G} x = z$.
b) Let G be a finite commutative group which does not have exactly one element of order 2. Show that $\sum_{x \in G} x = 0$.
c) Prove the following result of Gauss (a generalization of **Wilson's Theorem**): let $N \in \mathbb{Z}^+$, and put

$$P(N) = \prod_{x \in (\mathbb{Z}/N\mathbb{Z})^\times} x.$$

Then: $P(N) = \pm 1$, and the minus sign holds iff $N = 4$ or is of the form p^m or $2p^m$ for an odd prime p and $m \in \mathbb{Z}^+$.
d) For a generalization to the case of $(\mathbb{Z}_K/A)^\times$, where A is an ideal in the ring $\mathbb{Z}_K$ of integers of a number field K, see [Da09]. Can you extend Dalawat's results to the function field case?

Exercise 4.12: Let K be any field, and put $R = K[t]$.
a) Let $n_1, \ldots, n_k$ be a sequence of non-negative integers and $\{x_1, \ldots, x_k\}$ a k-element subset of K. For $1 \leq i \leq k$, let $c_{i0}, \ldots, c_{in_i}$ be a finite sequence of $n_i + 1$ elements of k (not necessarily distinct). By applying the Chinese Remainder Theorem, show that there is a polynomial $P(t)$ such that for $1 \leq i \leq k$ and $0 \leq j \leq n_i$ we have $P^{(j)}(x_i) = c_{ij}$, where $P^{(j)}(x_i)$ denotes the jth "formal" derivative of P evaluated at x_i. Indeed, find all such polynomials; what can be said about the least degree of such a polynomial?
b) Use the proof of the Chinese Remainder Theorem to give an explicit formula for such a polynomial P.

Exercise 4.13: Let $(M, \cdot)$ be a monoid and k a field. A **character** on M with values in k is a homomorphism of monoids from M to the multiplicative group $k^\times$ of k. Each character lies in the k-vector space k^M of all functions from M to k.
a) (Dedekind) Show that any finite set of characters is k-linearly independent.
b) Give an example of an infinite set of characters which is k-linearly dependent.

Exercise 4.14: Show that for a ring R, TFAE:
(i) R has finitely many maximal ideals.[23]
(ii) The quotient of R by its Jacobson radical $J(R)$ is a finite product of fields.

We now give a commutative algebraic version of Euclid's proof of the infinitude of prime numbers. A special case for domains appears in [K, § 1.1, Exc. 8]. The case in which R is infinite and $R^\times$ is finite has appeared on an algebra qualifying exam at UGA; the appearance of this unusually interesting and challenging problem on a qual was remarked to me by both D. Lorenzini and B. Cook. I learned the slightly stronger version presented here from W.G. Dubuque.

Theorem 4.20. *If R is infinite and $\#R > \#R^\times$, then* $\operatorname{MaxSpec} R$ *is infinite.*

Proof. Since R is not the zero ring, it has at least one maximal ideal $\mathfrak{m}_1$. We proceed by induction: given maximal ideals $\mathfrak{m}_1, \ldots, \mathfrak{m}_n$, we construct another maximal ideal.
Step 1: Suppose $J + 1 \subset R^\times$. Then

$$\#J = \#(J+1) \leq \#R^\times < \#R.$$

Moreover, by Proposition 4.14, J is contained in the Jacobson radical of R and thus by Proposition 4.15, $R^\times \to (R/J)^\times$ is surjective. It follows that $\#(R/J)^\times \leq \#R^\times < \#R$: by the Chinese remainder Theorem, $R/J \cong \prod_{i=1}^n R/\mathfrak{m}_i$, hence there is an injection $(R/\mathfrak{m}_i)^\times \to (R/J)^\times$. Putting the last two sentences together we conclude $\#(R/\mathfrak{m}_i)^\times < \#R$, and thus, since $R/\mathfrak{m}_i$ is a field and R is infinite, $\#R/\mathfrak{m}_i = \#R/\mathfrak{m}_i + 1 < \#R$. Finally this gives

$$\#R = \#J \cdot \#R/J = \#J \cdot \prod_{i=1}^n \#R/\mathfrak{m}_i < (\#R)^{n+1} = \#R,$$

a contradiction.
Step 2: So $J+1 \not\subset R^\times$. Let $x \in J+1 \setminus R^\times$, and let $\mathfrak{m}$ be a maximal ideal containing x. Then for all $1 \leq i \leq n$, $x - 1 \in J \subset \mathfrak{m}_i$, so $1 = x + (1 - x) \in \mathfrak{m} + \mathfrak{m}_i$. It follows that $\mathfrak{m} \not\subseteq \mathfrak{m}_i$, so it's a new maximal ideal.

□

4.4. **Local rings.**

Proposition 4.21. *For a ring R, TFAE:*
(i) There is exactly one maximal ideal $\mathfrak{m}$.
(ii) The set $R \setminus R^\times$ of nonunits forms a subgroup of $(R, +)$.
(iii) The set $R \setminus R^\times$ is a maximal ideal.
A ring satisfying these equivalent conditions is called a ***local ring****.*

[23]Such rings are typically called **semilocal**. I am not a fan of the terminology – it seems to either suggest that R has one half a maximal ideal (whatever that could mean) or two maximal ideals. But it is well entrenched, and I will not campaign to change it.

Proof. Since $R^\times = R \setminus \bigcup_{\mathfrak{m}} \mathfrak{m}$, the union extending over all maximal ideals of R, it follows that if there is only one maximal ideal $\mathfrak{m}$ then $\mathfrak{m} = R \setminus R^\times$. This shows (i) $\implies$ (iii) and certainly (iii) $\implies$ (ii). Conversely, since the set of nonunits of a ring is a union of ideals, it is closed under multiplication by all elements of the ring. Thus it is itself an ideal iff it is an additive subgroup: (ii) $\implies$ (iii). The implication (iii) implies (i) is very similar and left to the reader. □

Warning: In many older texts, a ring with a unique maximal ideal is called "quasi-local" and a local ring is a Noetherian quasi-local ring. This is not our convention.

Local rings (especially Noetherian local rings) play a vital role in commutative algebra: the property of having a single maximal ideal simplifies many ideal-theoretic considerations, and many ring theoretic considerations can be reduced to the study of local rings (via a process called, logically enough, *localization*: see §X).

A field is certainly a local ring. The following simple result builds on this trivial observation to give some further examples of local rings:

Proposition 4.22. *Let I be an ideal in the ring R.*
a) If $\mathrm{rad}(I)$ *is maximal, then R/I is a local ring.*
b) In particular, if $\mathfrak{m}$ is a maximal ideal and $n \in \mathbb{Z}^+$ then $R/\mathfrak{m}^n$ is a local ring.

Proof. a) We know that $\mathrm{rad}(I) = \bigcap_{\mathfrak{p} \supset I} \mathfrak{p}$, so if $\mathrm{rad}(I) = \mathfrak{m}$ is maximal it must be the *only* prime ideal containing I. Therefore, by correspondence R/I is a local ring. (In fact it is a ring with a unique prime ideal.)

b) By Proposition 4.13f), $r(\mathfrak{m}^n) = r(\mathfrak{m}) = \mathfrak{m}$, so part a) applies. □

So, for instance, for any prime number p, $\mathbb{Z}/(p^k)$ is a local ring, whose maximal ideal is generated by p. It is easy to see (using, e.g. the Chinese Remainder Theorem) that conversely, if $\mathbb{Z}/(n)$ is a local ring then n is a prime power.

Example: The ring $\mathbb{Z}_p$ of p-adic integers is a local ring. For any field k, the ring $k[[t]]$ of formal power series with coefficients in k is a local ring. Both of these rings are also PIDs. A ring which is a local PID is called a **discrete valuation ring**; these especially simple and important rings will be studied in detail later.

Exercise 4.16: Show that a local ring is connected, i.e., $e^2 = e \implies e \in \{0, 1\}$.

4.5. **The Prime Ideal Principle of Lam and Reyes.**

A recurrent meta-principle in commutative algebra is that if $\mathcal{F}$ is a naturally given family of ideals in commutative ring R, then it is often the case that every maximal element of $\mathcal{F}$ is prime. In this section we review some known examples, give some further classical ones, and then discuss a beautiful theorem of T.-Y. Lam and M. Reyes which gives a general criterion for this phemenon to occur.

Recall that for a ring R, $\mathcal{I}(R)$ is the monoid of ideals of R under multiplication. For any $\mathcal{F} \subset \mathcal{I}(R)$, let $\mathrm{Max}\,\mathcal{F}$ denote the maximal elements of $\mathcal{F}$ (to be sure, this means the elements of $\mathcal{F}$ which are not properly contained in any other element of $\mathcal{F}$, not the elements of $\mathcal{F}$ which are not contained in any other proper ideal!). We say that $\mathcal{F}$ is an **MP family** if $\mathrm{Max}\,\mathcal{F} \subset \mathrm{Spec}\,R$.

We have already seen two instances of this principle.

First, by Exercise 1.24 / Corollary 4.7, the set $\mathcal{F}$ of all proper ideals of R is an MP family: in other words, maximal ideals are prime.

Second, if $S \subset R$ is multiplicatively closed subset containing 1 but not 0, then the set of all ideals which are disjoint from S is an MP family (Multiplicative Avoidance).[24]

Later we will naturally encounter the following further instances of MP families:

Third, the set of of all ideals which are *not* principal is an MP family. (Thus if in a ring every prime ideal is principal, every ideal is principal.)

Fourth, the set of all ideals which are *not* finitely generated is an MP family. (Thus if in a ring every prime ideal is finitely generated, every ideal is finitely generated.)

The challenge is to come up with a common explanation and proof for all of these examples. One first observation is that there is a complementation phenomenon in play here: for $\mathcal{F} \subset \mathcal{I}(R)$, put $\mathcal{F}' = \mathcal{I}(R) \setminus \mathcal{F}$. Then in each of the last three cases it is most natural to view the MP family as $\mathcal{F}'$ for a suitable $\mathcal{F}$: in the second case, $\mathcal{F}$ is the set of ideals meeting S; in the third case, $\mathcal{F}$ is the set of all principal ideals; in the fourth case $\mathcal{F}$ is the set of all finitely generated ideals.

Let us also recall that for $I, J \in \mathcal{I}(R)$,

$$(I : J) = \{x \in R \mid xJ \subset I\}.$$

For $a, b \in R$, we write $(I : b)$ for $(I : Rb)$ and $(a : J)$ for $(aR : J)$.

Exercise 4.17: For ideals I, J in R, show that

$$(I : J)\langle I, J\rangle \subseteq I. \tag{15}$$

Exercise 4.18: Let R be a PID, and let $a, b \in R^\bullet$. We will use the fact that a and b can be uniquely (up to units) factored into products of principal prime ideals, say

$$a = \pi_1^{a_1} \cdots \pi_r^{a_r}, b = \pi_1^{b_1} \cdots \pi_r^{b_r},\ a_i, b_i \in \mathbb{N}.$$

a) Show $\langle a, b\rangle = \langle \pi_1^{\min(a_1,b_1)} \cdots \pi_r^{\min(a_r,b_r)}\rangle$.
b) Show $(a : b) = \langle \pi_1^{\max(a_1-b_1,0)} \cdots \pi_r^{\max(a_r-b_r,0)}\rangle$.
c) Show $\langle a\rangle \subset (a : b)$ and (of course!) $\langle a\rangle \subset \langle a, b\rangle$.
d) Show that $(a : b)\langle a, b\rangle = \langle a\rangle$.
e) Suppose that R has at least two nonzero prime ideals. Find $a, b \in R^\bullet$ such that:
(i) $(a : b) \subset \langle a, b\rangle$.
(ii) $\langle a, b\rangle \subset (a : b)$.
(iii) Neither of $(a : b)$, $\langle a, b\rangle$ contains the other.

[24]Recall that this is direct genealization of the first example: take $S = \{1\}$.

Here is the key definition: $\mathcal{F} \subset \mathcal{I}(R)$ is an **Oka family** if for all $x \in R$ and $I \in \mathcal{I}(R)$, if $\langle I, x\rangle, (I : x) \in \mathcal{F}$, then $I \in \mathcal{F}$.

Proposition 4.23. *For a ring R, each of the following families $\mathcal{F} \subset \mathcal{I}(R)$ is Oka:*
(i) The set of all ideals meeting a multiplicatively closed subset $S \subset R$.
(ii) The set of all principal ideals.
(iii) The set of all finitely generated ideals.

Proof. (i) Let $x \in R$, $I \in \mathcal{I}(R)$ be such that $\langle I, x\rangle, (I : x) \in \mathcal{F}$. Then there are $s_1, s_2 \in S$, $i_1, i_2 \in I$ and $a, b \in R$ such that

$$s_1 = ai_1 + bx,\ s_2x = i_2.$$

Then

$$s_2s_2 = as_2i_1 + bs_2x = as_2i_1 + bi_2 \in S \cap I.$$

(ii) Suppose $(I : x) = \langle a\rangle$ and $\langle I, x\rangle = \langle b\rangle$. Exercise 4.18d) gives us a useful hint: we will show $I = \langle ab\rangle$. Let $i \in I$; since $I \subset \langle I, x\rangle$, $i = \alpha b$ for some $\alpha \in R$. Thus $\alpha\langle b\rangle \subset= \alpha\langle I, c\rangle \subset I$, so $\alpha x \in I$ and thus $\alpha \in (I : x) = \langle a\rangle$ and we may write $\alpha = \beta a$. It follows that $i = \alpha b = \beta ab \in \langle ab\rangle$, so $I \subset \langle ab\rangle$. The containment $(I : x)\langle I, x\rangle \subset I$ is a special case of (15).
(iii) Suppose $(I : x) = \langle a_1, \ldots, a_m\rangle$ and $\langle I, x\rangle = \langle i_1 + \alpha_1 x, \ldots, i_n + \alpha_n x\rangle$. Let $J = \langle i_1, \ldots, i_n, xa_1, \ldots, xa_m\rangle$. We will show $I = J$, hence I is finitely generated. It is immediate that $J \subset I$. Conversely $z \in I$; since $I \subset \langle I, x\rangle$, we may write

$$z = \beta_1(i_1 + \alpha_1 x) + \ldots + \beta_n(i_1 + \alpha_n x) = (\beta_1 i_1 + \ldots + \beta_n i_n) + (\alpha_1\beta_1 + \ldots + \alpha_n\beta_n)x.$$

Since z and $\beta_1 i_1 + \ldots + \beta_n i_n \in I$, so is $(\alpha_1\beta_1 + \ldots + \alpha_n\beta_n)x$, i.e., $\alpha_1\beta_1 + \ldots + \alpha_n\beta_n \in (I : x) = \langle a_1, \ldots, a_m\rangle$, so $(\alpha_1\beta_1 + \ldots + \alpha_n\beta_n)x \in \langle xa_1, \ldots, xa_m\rangle$ and thus $z \in J$. □

Exercise 4.19: a) Let κ be any infinite cardinal. Show that in any ring R, the family of ideals which can be generated by a set of cardinality less than κ is Oka.
b) Proposition 4.23(ii) is equivalent to the statement that in any ring R, the family of ideals which can be generated by a set of cardinality less than 2 is Oka. The case of $\kappa = 1$ is a triviality. What if $2 < \kappa < \aleph_0$: must it be the case that the family of ideals generated by a set of cardinality κ is Oka?

Theorem 4.24. *(Prime Ideal Principle* [LR08, 2.4]*) Let R be a ring and $\mathcal{F} \subset \mathcal{I}(R)$. If $\mathcal{F}$ is an Oka family, then $\mathcal{F}'$ is an MP family.*

Proof. By contraposition: let $I \in \operatorname{Max} \mathcal{F}'$ be an ideal which is not prime, so there are $a, b \in R \setminus I$ with $ab \in I$. Since $b \in (I : a)$, the ideals $\langle I, a\rangle, (I : a)$ each properly contain I, so by maximality $\langle I, a\rangle, (I : a) \in \mathcal{F}$. Since $I \notin \mathcal{F}$, $\mathcal{F}$ is not Oka. □

Combining Proposition 4.23 and Theorem 4.24 we deduce a new proof of Multiplicative Avoidance as well as the following results.

Theorem 4.25. *If every prime ideal of R is principal, every ideal of R is principal.*

Proof. Let $\mathcal{F} \subset \mathcal{I}(R)$ be the family of principal ideals. By Proposition 4.23 and Theorem 4.24, every maximal element of $\mathcal{F}'$ is prime. It remains to show that if $\mathcal{F}'$ is nonempty, it has maximal elements, but this is an easy Zorn's Lemma argument: let $\{I_i\}$ be a chain of nonprincipal ideals, and put $I = \bigcup I_i$. If $I = \langle x\rangle$, then for some i we must have $x \in I_i \subset I = \langle x\rangle$, so $I_i = \langle x\rangle$, contradiction. □

Theorem 4.26. *(Cohen* [Coh50]*) If every prime ideal of R is finitely generated, then every ideal of R is finitely generated.*

Proof. Let $\mathcal{F} \subset \mathcal{I}(R)$ be the family of ideals which can be generated by finitely many elements. By Exercise X.X and Theorem 4.24, every maximal element of $\mathcal{F}'$ is prime. Again we must show that if $\mathcal{F}'$ is nonempty, it has maximal elements, and again this is an easy Zorn's Lemma argument:[25] $\{I_i\}_{i \in I}$ be a chain of non-finitely generated ideals, and put $I = \bigcup I_i$. If $I = \langle x_1, \ldots, x_n \rangle$, then for $1 \leq j \leq n$, there exists an index i_j such that $x_j \in I_{i_j}$, and thus if $i_\bullet = \max_{1 \leq j \leq n} i_j$, $\langle x_1, \ldots, x_n \rangle \subset I_{i_\bullet} \subset I = \langle x_1, \ldots, x_n \rangle$, so $I_{i_\bullet}$ is finitely generated, contradiction. □

Exercise 4.20: By Exercise 4.19, for any infinite cardinal κ and any ring R, the family $\mathcal{I}_\kappa$ of ideals of R with fewer than κ generators is an Oka family. So it's tempting to generalize Theorem 4.26 to: for any infinite cardinal κ, if every prime ideal of a ring R can be generated by fewer than κ elements then every ideal of R can be generated by fewer than κ elements. Is this generalization true?

4.6. **Minimal Primes.**

Let R be a ring. A **minimal prime** $\mathfrak{p}$ of R is just what it sounds like: a minimal element of the set $\operatorname{Spec} R$ of prime ideals of R, partially ordered by inclusion.

The mind of the novitiate algebraist tends to balk a bit at this definition, since until we are trained otherwise we naturally think first of domains, and in a domain the uniqu minimal prime is zero. (In particular, minimal prime *does not* mean "minimal nonzero prime"!) However the minimal primes play an important (and easy to grasp) role in understanding the basic structure of a general ring.

Of course the zero ring contains no primes, hence no minimal primes. It is not completely obvious that a nonzero ring necessarily has at least one minimal prime, but this, and a bit more, is true.

Exercise: Let $\mathcal{C}$ be a chain of prime ideals in a ring R. Show that $\bigcap_{\mathfrak{p} \in \mathcal{C}} \mathfrak{p}$ is a prime ideal.

Proposition 4.27. *Let $I \subset \mathcal{P}$ be ideals of R, with $\mathcal{P}$ prime. Then the set $\mathcal{S}$ of all prime ideals $\mathfrak{p}$ of R with $I \subset \mathfrak{p} \subset \mathcal{P}$ has a minimal element.*

Proof. We partially order $\mathcal{S}$ by reverse inclusion i.e., $\mathfrak{p}_1 \leq \mathfrak{p}_2 \iff \mathfrak{p}_1 \supset \mathfrak{p}_2$. Let C be any chain in $\mathcal{S}$. By Exercise X.X, $\bigcap_{\mathfrak{p} \in \mathcal{C}} \mathfrak{p}$ is a prime ideal and thus it is an upper bound for $\mathcal{C}$ in $\mathcal{S}$. By Zorn's Lemma, $\mathcal{S}$ contains a maximal element, i.e., a minimal element under ordinary containment. □

Corollary 4.28. *Every nonzero ring has at least one minimal prime.*

Exercise: Prove Corollary X.X.

We write $\operatorname{MinSpec} R$ for the set of all minimal primes of R and $\operatorname{ZD}(R)$ for the set of all zerodivisors in R.

Exercise: Show that in any ring R,

$$r(R) = \bigcap_{\mathfrak{p} \in \operatorname{MinSpec} R} \mathfrak{p}.$$

[25] But we have our reasons for spelling it out in detail: see the following exercise!

In order to prove the next result, it is convenient (though not strictly necessary) to use the theory of localization, which we will (unfortunately) not develop until § 7. Nevertheless we have decided to put the complete proof here, as it fits logically with the other results of the section (and the reader can verify that there is no logical circularity).

Theorem 4.29. *Let R be a ring.*
a) We have $\bigcup_{\mathfrak{p} \in \operatorname{MinSpec} R} \mathfrak{p} \subset \operatorname{ZD}(R)$.
b) If R is reduced, then equality holds:

$$\bigcup_{\mathfrak{p} \in \operatorname{MinSpec} R} \mathfrak{p} = \operatorname{ZD}(R). \tag{16}$$

Proof. a) Let $\mathfrak{p} \in \operatorname{MinSpec} R$ and let $x \in \mathfrak{p}$. Then $\mathfrak{p}R_{\mathfrak{p}}$ is the unique prime ideal of $R_{\mathfrak{p}}$, so $x \in r(\mathfrak{p}A_{\mathfrak{p}})$ is nilpotent. By Exercise 7.4, this implies that there is $y \in R \setminus \mathfrak{p}$ such that $yx^n = 0$. Since $y \neq 0$, x^n – and thus also x – is a zero-divisor.
b) Suppose $a \in \operatorname{ZD}(R)$, so there is $b \in R^\bullet$ with $ab = 0$. Since $b \neq 0$ and R is reduced, by Exercise X.X,

$$b \notin \bigcap_{\mathfrak{p} \in \operatorname{MinSpec} R} \mathfrak{p},$$

so there is a minimal prime $\mathfrak{p}$ not containing b. Since $0 = ab \in \mathfrak{p}$ and $\mathfrak{p}$ is prime, $a \in \mathfrak{p}$. □

5. Examples of Rings

5.1. **Rings of numbers.**

The most familiar examples of rings are probably rings of numbers, e.g.

$$\mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}.$$

These are, respectively, the integers, the rational numbers, the real numbers and the complex numbers. For any positive integer N the ring integers modulo N, denoted $\mathbb{Z}/N\mathbb{Z}$. We assume that the reader has seen all these rings before.

Historically, the concept of a ring as an abstract structure seems to have arisen as an attempt formalize common algebraic properties of number rings of various sorts. It is my understanding that the term "ring" comes from Hilbert's *Zahlring* ("Zahl" means "number" in German). Indeed, various sorts of extension rings of $\mathbb{C}$ – most famously Hamilton's quaternions $\mathbb{H}$ – have been referred to as systems of **hypercomplex numbers**. This terminology seems no longer to be widely used.

The adjunction process gives rise to many rings and fields of numbers, as already seen in §2.2. For instance, for any nonsquare integer D, let $\sqrt{D}$ be a complex number whose square is D: then $\mathbb{Z}[\sqrt{D}]$ is an interesting ring.

Exercise 5.1: Show that $\mathbb{Z}[\sqrt{D}] = \{a + b\sqrt{D} \mid a, b \in \mathbb{Z}\}$.

In particular, $(\mathbb{Z}[\sqrt{D}], +) \cong (\mathbb{Z}^2, +)$ as abelian groups, although not as rings, since $\mathbb{Z}[\sqrt{D}]$ is an integral domain and $\mathbb{Z}^2$ has nontrivial idempotents.

More generally, let K be any number field (a finite degree field extension of $\mathbb{Q}$),

and let $\mathbb{Z}_K$ be the set of elements $x \in K$ which satisfy a monic polynomial with $\mathbb{Z}$-coefficients. It turns out that $\mathbb{Z}_K$ is a ring, the **ring of algebraic integers in K**. This is a special case of the theory of integral closure: see §14.

Algebraic number theory proper begins with the observation that in general the rings $\mathbb{Z}_K$ need not be UFDs but are otherwise as nice as possible from a commutative algebraic standpoint. That is, every ring $\mathbb{Z}_K$ is a **Dedekind domain**, which among many other characterizations, means that every nonzero ideal factors into a product of prime ideals. That the rings $\mathbb{Z}_K$ are Dedekind domains is an example of a *normalization theorem*, more specifically a very special case of the **Krull-Akizuki Theorem** of §18.

Let $\overline{\mathbb{Q}}$ be an algebraic closure of $\mathbb{Q}$. (This is *not* a number field, being an infinite degree algebraic extension of $\mathbb{Q}$.) We may define $\overline{\mathbb{Z}}$ to be the set of all elements of $\overline{\mathbb{Q}}$ which satsify a monic polynomial with integer coefficients: this is **the ring of all algebraic integers**. In particular,

$$\overline{\mathbb{Z}} = \varinjlim \mathbb{Z}_K$$

is the direct limit of all rings of integers in fixed number fields.

Exercise 5.2: Let $\overline{\mathbb{Z}}$ be the set of all algebraic integers.
a) Taking as given that for any fixed number field K, the algebraic integers in K form a subring of K, show that $\overline{\mathbb{Z}}$ is a subring of $\overline{\mathbb{Q}}$.
b) Show that $\overline{\mathbb{Z}}$ is an integral domain which is *not* Noetherian. Hint: use the fact that the nth root of an algebraic integer is an algebraic integer to construct an infinite strictly ascending chain of principal ideals in $\overline{\mathbb{Z}}$.

Theorem 5.1. *Every finitely generated ideal in the ring $\overline{\mathbb{Z}}$ is principal.*

Thus, if only $\overline{\mathbb{Z}}$ were Noetherian, it would be a principal ideal domain! Later on we will prove a more general theorem, due to Kaplansky, in the context of limits of Dedekind domains with torsion Picard groups.

5.2. **Rings of continuous functions.**

5.2.1. *The ring of real-valued functions.*

Let R be a ring, X a set, and consider the set R^X of all functions $f : X \to R$. We may endow R^X with the structure of a ring by defining addition and multiplication "pointwise", i.e.,

$$(f + g) : x \mapsto f(x) + g(x),$$
$$(fg) : x \mapsto f(x)g(x).$$

Exercise 5.3: Show that this makes R^X into a ring with additive identity the constant function 0 and multiplicative identity the constant function 1.

However, this is not really a "new" example of a ring.

Exercise 5.4: Show that R^X is isomorphic as a ring, to $\prod_{x \in X} R$.

Later on we will see this construction in the special case $R = \mathbb{F}_2$, in which case

we get an important subclass of **Boolean rings**. However, in general R^X is quite a roomy ring. It contains many interesting subrings, some of which can be nicely consructed and analyzed using topological, geometric and analytic considerations.

5.2.2. *Separation axioms and $C(X)$.*

Suppose instead that we specialize to the following situation: $R = \mathbb{R}$ (the real numbers!), X is a topological space, and instead of the ring $\mathbb{R}^X$ of all functions $f : X \to \mathbb{R}$ we look at the subring $C(X)$ of *continuous* functions.

Exercise 5.5: Show that for a topological space X, TFAE:
(i) For every $x, y \in X$ with $x \neq y$, there exists $f \in C(X)$ with $f(x) \neq f(y)$.
(ii) For every $x, y \in X$ with $x \neq y$ and every $\alpha, \beta \in \mathbb{R}$, there exists $f \in C(X)$ with $f(x) = \alpha,\ f(y) = \beta$.
(iii) For every finite subset S of X and any function $g : S \to \mathbb{R}$, there exists $f \in C(X)$ such that $f|_S = g$.
A space which satisfies these equivalent conditions is called **C-separated**.[26]

Recall the following chains of implications from general topology:

Lemma 5.2. *For any topological space, the following implications hold (and none of the arrows may be reversed)):*
a) X compact $\implies$ X normal $\implies$ X Tychonoff $\implies$ X regular $\implies$ X Hausdorff $\implies$ X separated $\implies$ X Kolmogorov.
b) X locally compact $\implies$ X Tychonoff.

Exercise 5.6: a) Show that a Tychonoff space is C-separated.
b) Show that a C-separated space is Hausdorff.
c)* Show that a regular space need not be C-separated. (Suggestion: see [Ga71].)

For a topological space X, a **zero set** is a set of the form $f^{-1}(0)$ for some continuous function $f : X \to \mathbb{R}$. A **cozero set** is a complement of a zero set. The cozero sets in fact form a base for a topology on X, called (by us, at least) the **Z-topology**. Let us write X_Z for X endowed with the Z-topology. Since every cozero set is an open set in the given topology on X, X_Z is a coarser topology than the given topology on X: of course by this we allow the possibility that the two topologies coincide: i.e., every closed set is an intersection of zero sets of continuous $\mathbb{R}$-valued functions. The following basic (but not so widely known) result gives a condition for this.

Theorem 5.3. *a) For a Hausdorff topological space X, TFAE:*
(i) $X_Z = X$: every closed set is an intersection of zero sets of continuous functions.
(ii) X is Tychonoff, i.e., if Y is a closed subset of X and $x \in X \setminus Y$, then there exists a continuous function $f : X \to [0, 1]$ with $f(x) = 0$, $f|_Y \equiv 1$.
b) For any topological space X, the space X_Z is completely regular, and is the finest completely regular topology on the underlying set of X which is coarser than X.

Proof. [GJ76, p. 38]. □

[26]More standard terminology: "the continuous functions on X separate points".

Let X be a topological space, and let $x \in X$ be any point. Consider the set

$$\mathfrak{m}_x = \{f \in C(X) \mid f(x) = 0\}.$$

Evidently $\mathfrak{m}_x$ is an ideal of $C(X)$. But more is true.

Proposition 5.4. *Evaluation at x gives a canonical isomorphism $C(X)/\mathfrak{m}_x \xrightarrow{\sim} \mathbb{R}$. In particular, $\mathfrak{m}_x$ is a* maximal *ideal of $C(X)$.*

Exercise 5.7: Prove Proposition 5.4.

Thus $x \mapsto \mathfrak{m}_x$ gives a map of sets $\mathcal{M} : X \to M(X)$.

Proposition 5.5. *The map $\mathcal{M} : X \to M(X)$ is injective iff X is C-separated.*

Proof. This is left to the reader as a routine check on parsing the definitions. □

5.2.3. *Quasi-compactness and $C(X)$.*

Proposition 5.6. *If X is quasi-compact, then $\mathcal{M}$ is surjective, i.e., every maximal ideal of $C(X)$ is of the form $\mathfrak{m}_x$ for at least one point $x \in X$.*

Proof. It suffices to show: let I be an ideal of $C(X)$ such that for no $x \in X$ do we have $I \subset \mathfrak{m}_x$. Then $I = C(X)$.

By hypothesis, for every $x \in X$ there exists $f_x \in I$ such that $f_x(x) \neq 0$. Since f_x is continuous, there exists an open neighborhood U_x of x such f_x is nowhere vanishing on U_x. By quasi-compactness of X, there exists a finite set $x_1, \ldots, x_N$ such $X = \bigcup_{i=1}^N U_{x_i}$. Then the function $f = f_{x_1}^2 + \ldots + f_{x_n}^2$ is an element of $\mathfrak{m}$ which is strictly positive at every $x \in X$. But then $\frac{1}{f}$ is also a continuous function on X, i.e., $f \in C(X)^\times$, so $I = R$. □

A compact space is quasi-compact and C-separated. Thus previous results yield:

Theorem 5.7. *If X is compact, then $\mathcal{M} : X \to M(X)$ is a bijection: every maximal ideal of $C(X)$ is of the form $\mathfrak{m}_x$ for a unique $x \in X$.*

In fact more is true. There is a natural topology on $M(X)$, the **initial topology**: namely, each $f \in C(X)$ induces a function $M_f : M(X) \to \mathbb{R}$, namely M_f maps $\mathfrak{m}$ to the image of f in $C(X)/\mathfrak{m} = \mathbb{R}$. Now we endow $M(X)$ with the coarsest topology which makes each of the functions M_f continuous.

Lemma 5.8. *For a compact space X, the initial topology on $M(X)$ is Hausdorff.*

Proof. For distinct $x, x' \in X$, consider the maximal ideals $\mathfrak{m}_x, \mathfrak{m}_{x'}$. By C-separatedness, there exists $f \in C(X)$ with $f(x) = 0$, $f(x') \neq 0$. Thus choose disjoint neighborhoods V, V' of $f(x), f(x') \in \mathbb{R}$. The sets

$$U_{f,V} = \{x \in X \mid f(x) \in V\},\ U_{f,V'} = \{x \in X \mid f(x) \in V'\}$$

are disjoint open neighborhoods of x and x'. □

Theorem 5.9. *For a compact space X, let $M(X)$ be the set of maximal ideals of $C(X)$ endowed with the initial topology. Then $\mathcal{M} : X \to M(X)$, $x \mapsto \mathfrak{m}_x$ is a homeomorphism.*

Proof. Step 1: We claim that $\mathcal{M}$ is continuous. But indeed, by the universal property of the initial topology, it is continuous iff for all $f \in C(X)$, the composite function $x \mapsto \mathfrak{m}_x \mapsto f(\mathfrak{m}_x)$ is continuous. But this is nothing else than the function $x \mapsto f(x)$, i.e., the continuous function f! So that was easy.
Step 2: We now know that $\mathcal{M}$ is a continuous bijection from a compact space to a Hausdorff space. Therefore it is a closed map: if Y is closed in X, then Y is compact, so $\mathcal{M}(Y)$ is compact, so $\mathcal{M}(Y)$ is closed. Therefore $\mathcal{M}^{-1}$ is continuous and thus $\mathcal{M}$ is a homeomorphism. □

5.2.4. *The Zariski topology on $C(X)$.*

For any commutative ring R, we define $\operatorname{MaxSpec}(R)$ to be the maximal ideals and put a topology on it: for any ideal I of R, we define

$$V(I) = \{\mathfrak{m} \in \operatorname{MaxSpec} R \mid I \subset \mathfrak{m}\}$$

The sets $V(I)$ are the closed sets for a unique topology on $\operatorname{MaxSpec} R$, the **Zariski topology**. Another way to say it is that the closed sets in the Zariski topology are precisely all sets obtained by intersecting sets of the form

$$V(f) = \{\mathfrak{m} \in \operatorname{MaxSpec} R \mid f \in \mathfrak{m}\}.$$

To see this, note first that for any ideal I of R,

$$V(I) = \bigcap_{f \in I} V(f)$$

and for any subset S of R,

$$\bigcap_{f \in S} V(f) = \bigcap_{f \in \langle S \rangle_R} V(f).$$

Thus, from the perspective of the rest of these notes, it is natural to consider $M(X) = \operatorname{MaxSpec} C(X)$ as being endowed with the Zariski topology rather than the initial topology (note that the latter is defined only in the quasi-compact case).

Proposition 5.10. *Let X be any topological space. Then the map $\mathcal{M} : X \to \operatorname{MaxSpec} C(X)$ is continuous when $\operatorname{MaxSpec} X$ is given the Zariski topology.*

Proof. As above, it is enough to show that for all $f \in C(X)$, the preimage $\mathcal{M}^{-1}(V(f))$ is closed in X. Unpacking the definitions, we find

$$\mathcal{M}^{-1}(V(f)) = f^{-1}(0),$$

thus the preimage is the zero set of the continuous function f, hence closed. □

Corollary 5.11. *For a compact space X, the Zariski topology on $M(X) = \operatorname{MaxSpec} C(X)$ coincides with the initial topology.*

Proof. By Theorem 5.9, we may compare the *Zariski topology on X* – the topology obtained by pulling back the Zariski topology on $\operatorname{MaxSpec} C(X)$ via $\mathcal{M}$ – with the given topology on X. But the proof of Proposition 5.10 shows that the Zariski topology on X is precisely the Z-topology, i.e., the one in which the closed subsets are the intersections of zero sets. But X is compact hence quasi-Tychonoff, so by Theorem 5.3 the Z-topology on X coincides with the given topology on X. □

Now let $\pi : X \to Y$ be a continuous map between compact spaces. There is an induced map $C(\pi) : C(Y) \to C(X)$: given $g : Y \to \mathbb{R}$, we pullback by π to get $g \circ \pi : X \to \mathbb{R}$. It is no problem to see that $C(\pi)$ is a homomorphism of rings. Now let $\mathfrak{m}_x \in \operatorname{MaxSpec} C(X)$ be a maximal ideal and consider its pullback $C(\pi)^*(\mathfrak{m}_x)$ to an ideal of $C(Y)$: we find

$$C(\pi)^*(\mathfrak{m}_x) = \{g : Y \to \mathbb{R} \mid g(\pi(x)) = 0\} = \mathfrak{m}_{\pi(x)}.$$

Thus the pullback map carries maximal ideals to maximal ideals (recall this is certainly not true for all homomorphisms of rings!) and thus induces a map from X to Y which is indeed nothing else than the given map π.

All in all we see that the functors C and MaxSpec give a duality between the categories of compact spaces and rings of continuous $\mathbb{R}$-valued functions on compact spaces. In functional analysis this the first step in an important circle of ideas leading up to **Gelfand duality** for commutative Banach algebras.

5.2.5. *Further results when X is not compact.*

What about the case of noncompact spaces X?

Example: Let X be an infinite discrete space, so $C(X) = \mathbb{R}^X$ is the ring of *all* functions from X to $\mathbb{R}$. Thus X is a noncompact Tychonoff space. So it follows from our work so far that $\mathcal{M}$ gives a continuous injection from $\mathcal{M}$ to the quasi-compact space $\operatorname{MaxSpec} C(X)$. In fact $\mathcal{M}$ is an embedding: for any subset $Y \subset X$, let I_Y be the ideal of functions vanishing identically on Y. Then the restriction of the closed subset $V(I)$ of $\operatorname{MaxSpec} C(X)$ to $\mathcal{M}(X)$ is precisely $\mathcal{M}(Y)$, so $\mathcal{M}(Y)$ is closed in $\operatorname{MaxSpec} C(X)$. Thus $\mathcal{M}(X)$ is discrete as a subspace of $\operatorname{MaxSpec} C(X)$, and this implies that $\mathcal{M}$ is *not* surjective.

Theorem 5.12. *For any topological space X, $\operatorname{MaxSpec} C(X)$ endowed with the Zariski topology is compact.*

Theorem 5.13. *Let X be any topological space, let $\mathcal{M} : X \to \operatorname{MaxSpec} C(X)$, and let $X_T = \mathcal{M}(X)$, viewed as a subspace of $\operatorname{MaxSpec} C(X)$.*
a) X_T is a Tychonoff space.
b) The map $\mathcal{M} : X \to X_T$ is the Tychonoff completion of X: i.e., it is universal for continuous maps from X to a Tychonoff space.
c) The induced map $C(\mathcal{M}) : C(X_T) \to C(X)$ is an isomorphism of rings.

Proof. See [GJ76, §3.9]. □

Thus the ring of continuous functions on an arbitrary space X "sees" precisely its Tychonoff completion X_T. Henceforth we restrict to Tychonoff spaces.

Theorem 5.14. *Let X be a Tychonoff space. Then the map $\mathcal{M} : X \to C(X)$ is nothing else than the Stone-Cech compactification.*

Proof. See [GJ76, §7.10]. □

Exercise 5.8: a) Show that $C(X)$ is an $\mathbb{R}$-subalgebra of $\mathbb{R}^X$.
b) Show that $C(X)$ is reduced: it contains no nonzero nilpotent elements.
c) (T. Rzepecki) Show that for a topological space, the following are equivalent:
(i) The Tychonoff completion X_T of X is a one-point space.
(ii) $C(X) = \mathbb{R}$.

(iii) $C(X)$ is a domain.
(Suggestion: (ii) $\iff$ (i) $\implies$ (iii) are straightforward. For (iii) $\implies$ (ii), let $f \in C(X)$ be nonconstant, so $f(x) \neq f(y)$ for some $x, y \in X$. Show that for suitable real numbers C_1 and C_2 the functions $g_1 = \max(0, f_1 + C_1)$ and $g_2 = \max(0, -f_1 + C_2)$ give nonzero elements of $C(X)$ with $g_1 g_2 = 0$.)

Exercise 5.9: Show that $C(X)$ is connected in the algebraic sense – i.e., there are no idempotents other than 0 and 1 – iff the topological space X is connected.

Exercise 5.10: Show that there is an antitone Galois connection between 2^X and the set of ideals of $C(X)$, as follows:
$S \subset X \mapsto I_S = \{f \in C(X) \mid f|_S \equiv_0\}$ and
$I \mapsto V_I = \{x \in X \mid \forall f \in I, f(x) = 0\}$.

Exercise 5.11: Let X be a compact space.
a) Let $\mathfrak{p}$ be a prime ideal of $C(X)$. Show that $V(\mathfrak{p})$ consists of a single point.
b) Deduce that a prime ideal $\mathfrak{p}$ of $C(X)$ is closed in the sense of the Galois connection – i.e., $\mathfrak{p} = I_{V_\mathfrak{p}}$ iff $\mathfrak{p}$ is maximal.
c) Deduce that each prime ideal $\mathfrak{p}$ of $C(X)$ is contained in a *unique* maximal ideal.

Exercise 5.12: Let $X = [0, 1]$ with the standard Euclidean topology. Let $\mathfrak{r}_0$ be the ideal of all functions $f \in C(X)$ such that for all $k \in \mathbb{N}$, $\lim_{x \to 0^+} \frac{f(x)}{x^k} = 0$. Equivalently $\mathfrak{r}_0$ is the ideal of all functions which are infinitely differentiable at 0 and have identically zero Taylor series at zero.
a) Show that $\mathfrak{r}_0$ is a radical ideal but not a prime ideal.
b) Show that the only maximal ideal containing $\mathfrak{r}_0$ is $\mathfrak{m}_0$, the set of all functions vanishing at 0.
c) Deduce that there exist ideals of $C(X)$ which are prime but not maximal.

Exercise 5.13: Let X be a C-separated topological space.
a) Let $S \subset X$ with $\#S > 1$. Show that I_S is not maximal.
b) Suppose X is Tychonoff and $S, T \subset X$. Show that $I_S \subset I_T \iff \overline{T} \subset \overline{S}$.
c) In particular if X is Tychonoff, then for closed subsets S and T of X, $I_S = I_T \iff S = T$.

Exercise 5.14: Let $\varphi : X \to Y$ be a continuous function between topological spaces.
a) Show that φ induces a ring homomorphism $C(\varphi) : C(Y) \to C(X)$ by $g \in C(Y) \mapsto \varphi^* g = g \circ \varphi$.
b) Suppose Y is normal, X is a closed subspace of X and $\varphi : X \to Y$ is the inclusion map. Show that $C(\varphi)$ is surjective.

Exercise 5.15: Let X be a normal topological space. Show that the closure operator on subsets of X given by the Galois connection coincides with the topological closure operator on X.

Exercise 5.16: Let X be the subspace $\{\frac{1}{n}\}_{n \in \mathbb{Z}^+} \cup \{0\}$ of $\mathbb{R}$, and let $\mathfrak{m}$ be the maximal ideal of all functions vanishing at 0. Fill in the details of the following outline of

a proof that $\mathfrak{m}$ is *not* finitely generated.[27] Assume otherwise: $\mathfrak{m} = \langle a_1, \ldots, a_n \rangle$. Then for every element $g \in \mathfrak{m}$, $\lim_{x \to 0} \frac{g^2(x)}{|a_1(x)| + \ldots + |a_n(x)|} = 0$. (In particular, there exists $\delta > 0$ such that the denominator is strictly positive on $(0, \delta)$.) Now choose $g \in \mathfrak{m}$ so as to get a contradiction.

Exercise 5.17: Let X be a normal space, and let $x \in X$.
a) Show that the following are equivalent:
(i) The ideal I_x is finitely generated.
(ii) The ideal I_x is principal.
(iii) The point x is isolated in X (i.e., $\{x\}$ is open).
b) Suppose X is compact. Show that the following are equivalent:
(i) $C(X)$ is a Noetherian ring.
(ii) $C(X)$ is finite-dimensional as an $\mathbb{R}$-vector space.
(iii) X is finite.

Exercise 5.18: Show that if we worked throughout with rings $C(X, \mathbb{C})$ of continuous $\mathbb{C}$-valued functions, then all of the above results continue to hold.

Exercise 5.19: Suppose that we looked at rings of continuous functions from a topological space X to $\mathbb{Q}_p$. To what extent to the results of the section continue to hold?

Exercise 5.20: Let X be a compact smooth manifold and consider the ring $C_\infty(X)$ of smooth functions $f : X \to \mathbb{R}$.
a)* Show that for $x \in X$, the ideal $\mathfrak{m}_x$ of all functions vanishing at x is maximal and *finitely generated*.
b) Note that the phenomenon of part a) is in contrast to the case of maximal ideals in the ring $C([0,1])$, say. However, I believe that with this sole exception, all of the results of this section hold for the rings $C_\infty(X)$ just as for the rings $C(X)$. Try it and see.

5.2.6. *A theorem of B. Sury.*

The recent note [Su11] gives the following striking generalization of Exercise 5.16.

Theorem 5.15. *(Sury) Let $c \in [0,1]$, and let $\mathfrak{m}_c = \{f \in C[0,1] \mid f(c) = 0\}$. Then $\mathfrak{m}_c$ admits no* countable *generating set.*

Proof. Let $\{f_n\}_{n=1}^\infty$ be a countably infinite subset of $\mathfrak{m}_c$, and let $J = \langle \{f_n\}_{n=1}^\infty \rangle$. It suffices to exhibit $f \in \mathfrak{m}_c \setminus J$.

By rescaling, we may assume $||f_n|| \leq 1$ for all n. Moreover, we may assume that $\bigcap_{n=1}^\infty f_n^{-1}(0) = \{c\}$, for otherwise $x \mapsto |x - c|$ lies in $\mathfrak{m}_c \setminus J$. Consider

$$f(x) = \sum_{n=1}^\infty \sqrt{\frac{|f_n(x)|}{2^n}}.$$

The series is uniformly convergent (by "Weierstrass's M-Test") and thus f, being the uniform limit of continuous functions, is itself continuous. Moreover $f^{-1}(0) =$

[27] Or, if you like, give your own proof that $\mathfrak{m}$ is not finitely generated!

$\{c\}$, and in particular $f \in \mathfrak{m}_c$. Seeking a contradiction, we suppose $f \in J$: then there is $r \in \mathbb{Z}^+$ and $g_1, \ldots, g_r \in C([0,1])$ such that

$$f = \sum_{n=1}^{r} g_n f_n.$$

Let $M = \max_{1 \le n \le r} ||g_n||$, so $||f|| \le M \sum_{n=1}^{r} ||f_n||$. Let U be a neighborhood of c such that $||\sqrt{f_n}||_U < \frac{1}{2^n M}$ for $1 \le n \le r$. Since $f = \sum_{n=1}^{r} g_n f_n$ vanishes only at c, for each $x \in U \setminus \{c\}$, there exists $1 \le N \le r$ such that $f_N(x) \neq 0$ and thus

$$|f_N(x)| < \frac{\sqrt{|f_N(x)|}}{2^N M}.$$

Hence

$$|f(x)| \le M \sum_{n=1}^{r} |f_n(x)| < \sum_{n=1}^{r} \frac{\sqrt{|f_n(x)|}}{2^n} \le |f(x)|,$$

a contradiction. □

5.3. **Rings of holomorphic functions.**

As we saw in the previous section, one of the characteristic properties of the ring of continuous functions on a normal space (or even smooth functions on a manifold) is that it is typically very far from being an integral domain. A remedy for this is to consider more "rigid" collections of functions.

Let U be an open subset of the complex plane $\mathbb{C}$, and let $\mathrm{Hol}(U)$ be the set of holomorphic functions $f : U \to \mathbb{C}$. (Recall that a holomorphic function on U is one for which the complex derivative $f'(z)$ exists for each $z \in U$. Equivalently, for each $z \in U$ f admits a power series development with positive radius of convergence.) It is immediate that $\mathrm{Hol}(U)$ is a subring of the ring $\mathbb{C}^U$ of all $\mathbb{C}$-valued functions on U.

Proposition 5.16. *For a nonempty open subset U of $\mathbb{C}$, TFAE:*
(i) U is connected.
(ii) $\mathrm{Hol}(U)$ *is a domain.*

Proof. (i) $\implies$ (ii): For any $f \in C(U, \mathbb{C})$ let $Z(f) = \{z \in U \mid f(z) = 0\}$ be the zero set of f. Since f is continuous, $Z(f)$ is a closed subset of U. If f is moreover holomorphic, then $Z(f)$ has no accumulation point in U, i.e., $f \neq 0 \implies Z(f)$ is discrete – [28] in particular $Z(f)$ is countable. Moreover, for any $f, g \in C(U, \mathbb{C})$ we have $Z(fg) = Z(f) \cup Z(g)$, so if $f, g \in \mathrm{Hol}(U)^\bullet$ then $Z(fg)$ is at most countable, whereas U is uncountable, so $fg \neq 0$.
(ii) $\implies$ (i): we argue by contrapositive. If U is not connected, it is of the form $V_1 \cup V_2$ where V_1 and V_2 are disjoint open subsets. Let χ_i be the characteristic function of V_i for $i = 1, 2$. Then each χ_i is locally constant on U – hence holomorphic, and nonzero, but $\chi_1 \chi_2 = 0$. □

Recall that in complex function theory it is common to call a nonempty open subset U of $\mathbb{C}$ a **domain**. In this language, Proposition 5.16 simply asserts that U is a domain iff $\mathrm{Hol}(U)$ is a domain. Henceforth we assume that U is a domain.

[28] Recall that this is proved by considering the Taylor series development of f about any accumulation point.

For every $z \in U$ there is a function $\mathrm{ord}_z : \mathrm{Hol}(U)^\bullet \to \mathbb{N}$, the **order of vanishing of f at z**. Precisely, we exand f into a power series at z: $f(\zeta) = \sum_{n=0}^\infty a_n(\zeta - z)^n$ and put $\mathrm{ord}_z(f)$ to the least n for which $a_n \neq 0$. Compiling all these together we may associate to each $f \in \mathrm{Hol}(U)^\bullet$ its **total order** $\mathrm{Ord}(f) : U \to \mathbb{N}$ given by $\mathrm{Ord}(f)(z) = \mathrm{ord}_z(f)$.

Consider the set $\mathbb{N}^U$ of all functions from U to $\mathbb{N}$. For $O \in \mathbb{N}^U$, we define the **support** of O to be the set of $z \in U$ such that $O(z) > 0$.

Recall that a *meromorphic function* on U is a function which is holomorphic on U except for isolated finite order singularities. More precisely, a meromorphic function is a function which is holomorphic on $U \setminus Z$ for some discrete closed subset Z of U and such that for all $z_0 \in Z$, there exists $n \in \mathbb{Z}^+$ such that $(z - z_0)^n f(z)$ extends to a holomorphic function on a neighborhood of z. If the least n as above is positive, we say that f has a pole at z_0, and we employ the convention that $f(z_0) = \infty$. Let $\mathrm{Mer}(U)$ be the set of all meromorphic functions on U; it is a ring under pointwise addition and multiplication, under the conventions that for all $z \in \mathbb{C}$,

$$z + \infty = \infty + \infty = z \cdot \infty = \infty \cdot \infty = \infty.$$

Theorem 5.17. *Let U be a domain in the complex plane.*
a) (Weierstrass) For each $O \in \mathbb{N}^U$ with closed, discrete support, there exists $f \in \mathrm{Hol}(U)^\bullet$ with $\mathrm{Ord}(f) = O$.
b) (Weierstrass + Mittag-Leffler) Let $Z \subset U$ be a closed subset without limit points. To each $z \in Z$ we associate a natural number n_z and for all $0 \leq k \leq n_z$, a complex number $w_{z,k}$. Then there exists $f \in \mathrm{Hol}(U)$ such that for all $z \in Z$ and $0 \leq k \leq n_z$, $f^{(k)}(z) = k! w_{z,k}$.

Proof. Part a) is of the two main results in Weierstrass' Factorization Theory: see e.g. [Ru87, Thm. 15.11]. Part b) is proved by combining part a) with Mittag-Leffler's famous result on the existence of meromorphic functions with prescribed principal parts: see e.g. [Ru87, Thm. 15.13]. □

Corollary 5.18. *The ring $\mathrm{Mer}(U)$ of meromorphic functions on U is a field, and indeed is the field of fractions of $\mathrm{Hol}(U)$.*

Exercise 5.21: Prove Proposition 5.18.

Exercise 5.22: Fix $z_0 \in U$. For $f \in \mathrm{Mer}(U)$, choose $n \in \mathbb{N}$ such that $(z - z_0)^n f$ is holomorphic at z_0, and put $\mathrm{ord}_{z_0}(f) = \mathrm{ord}_{z_0}((z - z_0)^n f) - n$.
a) Show that this gives a well-defined function $\mathrm{ord}_{z_0} : \mathrm{Mer}(U)^\bullet \to \mathbb{Z}$ (i.e., independent of the choice of n in the definition).
b) Show that for all $f, g \in \mathrm{Mer}(U)^\times$, $\mathrm{ord}_{z_0}(fg) = \mathrm{ord}_{z_0}(f) + \mathrm{ord}_{z_0}(g)$.
c) We formally extend ord_{z_0} to a function from $\mathrm{Mer}(U)$ to $\mathbb{Z} \cup \{\infty\}$ by setting $\mathrm{ord}_{z_0}(0) = \infty$. Show that, under the convention that $\infty + n = \infty + \infty = \infty$, we have for all $f, g \in \mathrm{Mer}(U)$ that $\mathrm{ord}_{z_0}(f + g) \geq \min \mathrm{ord}_{z_0}(f), \mathrm{ord}_{z_0}(g)$.
d) Show that if $\mathrm{ord}_{z_0}(f) \neq \mathrm{ord}_{z_0}(g)$ then $\mathrm{ord}_{z_0}(f + g) = \min \mathrm{ord}_{z_0} f, \mathrm{ord}_{z_0}(g)$.

Similarly we may extend Ord to a function from $\mathrm{Mer}(U)^\bullet$ to $\mathbb{Z}^U$.

Lemma 5.19. *For $f, g \in \mathrm{Hol}(U)^\bullet$, TFAE:*
(i) $\mathrm{Ord}(f) = \mathrm{Ord}(g)$.
(ii) $f = ug$ *for* $u \in \mathrm{Hol}(U)^\times$.
(iii) $(f) = (g)$.

Proof. (ii) $\iff$ (iii) for elements of any integral domain.
(ii) $\implies$ (i) is easy and left to the reader.
(i) $\implies$ (ii): The meromorphic function $\frac{f}{g}$ has identically zero order, hence is nowhere vanishing and is thus a unit u in $\mathrm{Hol}(U)$. □

Theorem 5.20. *(Helmer* [Hel40]*) For a domain U in the complex plane, every finitely generated ideal of* $\mathrm{Hol}(U)$ *is principal. More precisely, for any $f_1, \ldots, f_n \in \mathrm{Hol}(U)^\bullet$, there exists $f \in \mathrm{Hol}(U)$ such that* $\mathrm{Ord}(f) = \min_i \mathrm{Ord}(f_i)$*, unique up to associates, and then $\langle f_1, \ldots, f_n \rangle = \langle f \rangle$.*

Proof. Step 1: Suppose that $f_1, f_2 \in \mathrm{Hol}(U)^\bullet$ do not simultaneously vanish at any point of U. We CLAIM that $\langle f_1, f_2 \rangle = \mathrm{Hol}(R)$.
PROOF OF CLAIM Let Z be the zero set of f_1, so that for all $z \in Z$, $f_2(z) \neq 0$. By Theorem 5.17b) there exists $g_2 \in \mathrm{Hol}(U)$ such that for all $z \in Z$, $\mathrm{ord}_z(1 - g_2 f_2) \geq \mathrm{ord}_z(f_1)$. Thus $\mathrm{Ord}(1 - g_2 f_2) \geq \mathrm{Ord}(f_1)$, so that $g_1 := \frac{1 - g_2 f_2}{f_1} \in \mathrm{Hol}(U)$ and thus $f_1 g_1 + f_2 g_2 = 1$.
Step 2: Now let $f_1, f_2 \in \mathrm{Hol}(U)^\bullet$ be arbitrary. By Theorem 5.17a), there exists $f \in \mathrm{Hol}(U)$ with $\mathrm{Ord}(f) = \min \mathrm{Ord}(f_1), \mathrm{Ord}(f_2)$. For $i = 1, 2$, put $g_i = \frac{f_i}{f}$. Then g_1 and g_2 are holomorphic and without a common zero, so by Step 1 $\langle g_1, g_2 \rangle = \mathrm{Hol}(U)$. Multiplying through by f gives $\langle f_1, f_2 \rangle = \langle f \rangle$.
Step 3: An easy induction argument shows that in a ring R in which every ideal of the form $\langle x_1, x_2 \rangle$ is principal, every finitely generated ideal is principal. By Step 2, this applies in particular to $\mathrm{Hol}(U)$. Moreover, if the ideal $\langle f_1, \ldots, f_n \rangle$ is generated by any single element f, then we must have $\mathrm{Ord}\, f = \min \mathrm{Ord}\, f_i$. □

Exercise 5.23: Explain carefully why in Step 1 of the above proof, Theorem 5.17b) implies the existence of g_2.

Of course the most familiar class of domains in which every finitely generated ideal is principal are those domains in which *every* ideal is principal: PIDs! But as the reader has probably already suspected, $\mathrm{Hol}(U)$ is not a PID.

One way to see this is to show that $\mathrm{Hol}(U)$ is not even a UFD. Remarkably, this is an immediate consequence of the Weierstrass Factorization Theory, which succeeds in decomposing every holomorphic function into a product of prime elements! The catch is that most holomorphic functions require *infinite* products, a phenomenon which is not countenanced in the algebraic theory of factorization.

Exercise 5.24: Let $f \in \mathrm{Hol}(U)^\bullet$.
a) Show that f is an irreducible element of $\mathrm{Hol}(U)$ – i.e., if $f = g_1 g_2$ then exactly one of g_1, g_2 is a unit – iff it has exactly one simple zero.
b) Suppose f is irreducible. Show that $\mathrm{Hol}(U)/(f) = \mathbb{C}$. In particular, (f) is a prime ideal.
c) Show that f admits a (finite!) factorization into irreducible elements iff it has only finitely many zeros. Conclude that $\mathrm{Hol}(U)$ is not a UFD.

Exercise 5.25: Extract from the previous exercise an explicit ideal of $\mathrm{Hol}(\mathbb{C})$ which is not finitely generated.

Exercise 5.26*: Show that all of the results of this section extend to the ring of holomorphic functions on a noncompact Riemann surface.

Exercise 5.27*: Investigate the extent to which the results of this section continue to hold for Stein manifolds. (Step 1: learn the definition of a Stein manifold!)

5.4. **Polynomial rings.**

Let R be a ring (possibly non-commutative, but – as ever – with identity). Then $R[t]$ denotes the ring of univariate polynomials with R-coefficients.

We assume the reader knows what this means in at least an informal sense: an element of R will be an expression of the form $a_n t^n + \ldots + a_1 t + a_0$, where n is some non-negative integer and $a_n, \ldots, a_0$ are in R. The degree of a polynomial is the supremum over all numbers n such that $a_n \neq 0$. We say "supremum" rather than "maximum" as an attempt to justify the convention that the degree of the 0 polynomial should be $-\infty$ (for that is the supremum of the empty set). A polynomial of degree 0 is called **constant**, and we can view R as a subset of $R[t]$ by mapping $a \in R$ to the constant polynomial a. As an abelian group, $R[t]$ is canonically isomorphic to $\bigoplus_{n=0}^{\infty} R$, the isomorphism being given by $\sum_n a_n t^n \mapsto (a_0, a_1, \ldots)$. (The key point here is that on both sides we have $a_n = 0$ for all sufficiently large n.) Multiplication of polynomials is obtained by applying the relations $t^0 = 1$, $t^{i+j} = t^i t^j$ $at = ta$ for all $a \in R$, and distributivity, i.e.,

$$(a_n t^n + \ldots + a_n t^1 + a_0) \cdot (b_m t^m + \ldots + b_1 t + b_0) = \sum_{0 \leq i \leq n,\ 0 \leq j \leq m} a_i b_j t^{i+j}.$$

For any $P \in R[t]$, the identity $1 \in R$ has the property $1 \cdot P = P \cdot 1 = 1$.

Unfortunately there are some minor annoyances of rigor in the previous description. The first one – which a sufficiently experienced reader will immediately either dismiss as silly or know how to correct – is that it is not *set-theoretically correct*: technically speaking, we need to say what $R[t]$ is as a set and this involves saying what t "really is." It is common in abstract algebra to refer to t is an **indeterminate**, a practice which is remarkably useful despite being formally meaningless: essentially it means "Don't worry about what t is; it can be anything which is not an element of R. All we need to know about t is encapsulated in the multiplication rules $at = ta$, $t^0 = 1$, $t^i t^j = t^{i+j}$." In other words, t is what in the uncomplicated days of high school algebra was referred to as a **variable**.

If someone insists that $R[t]$ be some particular set – a rather unenlighened attitude that we will further combat later on – then the solution has already been given: we can take $R[t] = \bigoplus_{n=0}^{\infty} R$. (It is fair to assume that we already know what direct sums of abelian groups "really are", but in the next section we will give a particular construction which is in fact rather useful.) This disposes of the set-theoretic objections.

Not to be laughed away completely is the following point: we said $R[t]$ was a ring, but how do we know this? We did explain the group structure, defined a multiplication operation, and identified a multiplicative identity. It remains to verify the distributivity of multiplication over addition (special cases of which motivated our definition of multiplication, but nevertheless needs to be checked in general) and also the *associativity* of multiplication.

Neither of these properties are at all difficult to verify. In fact:

Exercise 5.28: a) Show that $R[t]$ is a ring.
b) Show that $R[t]$ is commutative iff R is commutative.

Let us now attempt a "conceptual proof" of the associativity of polynomial multiplication. For this we shall assume that R is commutative – this is the only case we will be exploring further anyway. Then we can, as the $P(t)$ notation suggests, view an element of $R[t]$ as a function from R to R. Namely, we just plug in values:

$$a \in R \mapsto P(a) \in R.$$

To be clear about things, let us denote this associated function from R to R by $\underline{P}$. As we saw above, the set of all functions R^R from R to R forms a commutative ring under pointwise addition and multiplication: $(f+g)(a) := f(a) + g(a)$, $(fg)(a) := f(a) \cdot g(a)$. In particular, it really is obvious that the multiplication of functions is associative. Let $\mathcal{P}$ be the subset of R^R of functions of the form $\underline{P}$ for some $P \in R[t]$. More concretely, we are mapping the constant elements of $R[t]$ to constant functions and mapping t to the identity function. This makes it clear that $\mathcal{P}$ is a subring of R^R: in fact it is the subring of R^R generated by the constant functions and the identity function.

So why don't we just define $R[t]$ to be $\mathcal{P}$, i.e., identify a polynomial with its associated function?

The problem is that the map $R[t] \to \mathcal{P}$ need not be an injection. Indeed, if R is finite (but not the zero ring), $\mathcal{P}$ is a subring of the finite ring R^R so is obviously finite, whereas $R[t]$ is just as obviously infinite. If R is a domain this turns out to be the only restriction.

Proposition 5.21. *Let R be an integral domain.*
a) Suppose that R is infinite. Then the canonical mapping $R[t] \to \mathcal{P}$ is a bijection.
b) Suppose that R is finite, say of order q, and is therefore a field. Then the kernel of the canonical mapping $R[t] \to \mathcal{P}$ is the principal ideal generated by $t^q - t$.

We leave the proof as a (nontrivial) exercise for the interested reader.

Exercise 5.29: Exhibit an infinite commutative ring R for which the map $R[t] \to \mathcal{P}$ is not injective. (Suggestion: find an infinite ring all of whose elements x satisfy $x^2 = x$.)

Exercise 5.30: Show that the map $R[t] \to \mathcal{P}$ is a homomorphism of rings.

So if we restrict to infinite integral domains, the map $R[t] \to \mathcal{P}$ is an isomorphism of rings. Thus we see, after the fact, that we could have defined the ring structure in terms of pointwise multiplication.

5.5. **Semigroup algebras.**

A **semigroup** M is a set equipped with a single binary operation $\cdot$, which is required (only!) to be associative. A **monoid** is a semigroup with a two-sided identity.

Exercise 5.31: Show that a semigroup has at most one two-sided identity, so it is unambiguous to speak of "the" identity element in a monoid. We will denote it by e (so as not to favor either addditive or multiplicative notation).

Example: Let $(R, +, \cdot)$ be an algebra. Then $(R, \cdot)$ is a semigroup. If R is a ring (i.e., has an identity 1) then $(R, \cdot)$ is a monoid, with identity element 1.

Example: Any group is a monoid. In fact a group is precisely a monoid in which each element has a two-sided inverse.

Example: The structure $(\mathbb{N}, +)$ of natural numbers under addition is a monoid; the identity element is 0.

Example: The structure $(\mathbb{Z}^+, \cdot)$ of positive integers under multiplication is a monoid; the identity element is 1.

Let M and N be two semigroups. Then the Cartesian product $M \times N$ becomes a semigroup in an obvious way: $(m_1, n_1) \cdot (m_2, n_2) := (m_1 \cdot m_2, n_1 \cdot n_2)$. If M and N are monoids with identity elements e_M and e_N, then $M \times N$ is a monoid, with identity element (e_M, e_N). Exactly the same discussion holds for any finite set $M_1, \ldots, M_N$ of semigroups: we can form the direct sum $M = \bigoplus_{i=1}^n M_i$, i.e., the Cartesian product of sets with componentwise operations; if all the M_i's are monoids, so is M.

If we instead have an infinite family $\{M_i\}_{i \in I}$ of semigroups indexed by a set I, we can define a semigroup structure on the Cartesian product $\prod_{i \in I} M_i$ in the obvious way, and if each M_i is a monoid with identity e_i, then the product semigroup is a monoid with identity $(e_i)_{i \in I}$. If each M_i is a monoid, we can also define the **direct sum** $\bigoplus_{i \in I} M_i$, which is the subset of the direct product $\prod_{i \in I} M_i$ consisting of all I-tuples $(m_i \in M_i)_{i \in I}$ such that $m_i = e_i$ for all but finitely many i. Then we have that $\bigoplus_{i \in I} M_i$ is a submonoid of the **direct product** monoid $\prod_{i \in I} M_i$.

If M and N are semigroups, then a map $f : M \to N$ is a homomorphism of semigroups if $f(m_1 \cdot m_2) = f(m_1) \cdot f(m_2)$ for all $m_1,\ m_2 \in M$. If M and N are monoids, a homomorphism of monoids is a homomorphism of semigroups such that moreover $f(e_M) = e_N$. A homomorphism $f : M \to N$ of semigroups (resp. of monoids) is an isomorphism iff there exists a homomorphism of semigroups (resp. monoids) $g : N \to M$ such that $g \circ f = \mathrm{Id}_M$, $f \circ g = \mathrm{Id}_N$.

Exercise 5.32: a) Exhibit monoids M and N and a homomorphism of semigroups $f : M \to N$ which is not a homomorphism of monoids.

b) Show that a homomorphism of semigroups $f : M \to N$ is an isomorphism iff it is bijective. Same for monoids.

Exercise 5.33: Show that the monoid $(\mathbb{Z}^+, \cdot)$ of positive integers under multiplication is isomorphic to $\bigoplus_{i=1}^{\infty}(\mathbb{N}, +)$, i.e., the direct sum of infinitely many copies of the natural numbers under addition. (Hint: a more natural indexing set for the direct sum is the set of all prime numbers.)

Now let R be an algebra and M be a semigroup. We suppose first that M is finite. Denote by $R[M]$ the set of all functions $f : M \to R$.

As we saw, using the operations of pointwise addition and multiplication endow this set with the structure of an associative algebra (which has an identity iff M does). We are going to keep the pointwise addition but take a different binary operation $* : R[M] \times R[M] \to R[M]$.

Namely, for $f, g \in R[M]$, we define the **convolution product** $f * g$ as follows:

$$(f * g)(m) := \sum_{(a,b) \in M^2 \ | \ ab=m} f(a)g(b).$$

In other words, the sum extends over all ordered pairs (a, b) of elements of M whose product (in M, of course), is m.

Proposition 5.22. *Let R be an associative algebra and M a finite semigroup. The structure $(R[M], +, *)$ whose underlying set is the set of all functions from M to R, and endowed with the binary operations of pointwise addititon and convolution product, is an associative algebra. If R is a ring and M is a monoid with identity e, then $R[M]$ is a ring with multiplicative identity the function I which takes e_M to 1_R and every other element of M to 0_R.*

Proof. First, suppose that R is a ring and M is a monoid, then for any $f \in R[M]$ and $m \in M$, we have

$$(f*I)(m) = \sum_{(a,b) \in M^2 \ | \ ab=m} f(a)I(b) = f(m)I(1) = f(m) = I(1)f(m) = \ldots = (I*f)(m).$$

We still need to check the associativity of the convolution product and the distributivity of convolution over addition. We leave the latter to the reader but check the former: if $f, g, h \in R[M]$, then

$$((f * g) * h)(m) = \sum_{xc=m} (f * g)(x)h(c) = \sum_{xc=m} \sum_{ab=x} f(a)g(b)h(c)$$

$$= \sum_{abc=m} f(a)g(b)h(c)$$

$$= \sum_{ay=m} \sum_{bc=y} f(a)g(b)h(c) = \sum_{ay=m} f(a)(g * h)(y) = (f * (g * h))(m).$$

□

A special case of this construction which is important in the representation theory of finite groups is the ring $k[G]$, where k is a field and G is a finite group.

Now suppose that M is an infinite semigroup. Unless we have some sort of extra structure on R which allows us to deal with convergence of sums – and, in this level of generality, we do not – the above definition of the convolution product $f * g$ is problematic because the sum might be infinite. For instance, if $M = G$ is any group, then our previous definition of $(f * g)(m)$ would come out to be $\sum_{x \in G} f(x)g(x^{-1}m)$, which is, if G is infinite, an infinite sum.

Our task therefore is to modify the construction of the convolution product so as to give a meaningful answer when the semigroup M is infinite, but in such a way that agrees with the previous definition for finite M.

Taking our cue from the infinite direct sum, we restrict our domain: define $R[M]$ to be subset of all functions $f : M \to R$ such that $f(m) = 0$ except for finitely many m (or, for short, **finitely nonzero functions**). Restricting to such functions,

$$(f * g)(m) := \sum_{ab=m} f(a)g(b)$$

makes sense: although the sum is apparently infinite, all but finitely terms are zero.

Proposition 5.23. *Let R be an associative algebra and M a semigroup. The structure $(R[M], +, *)$ whose underlying set is the set of all finitely nonzero functions from M to R, and endowed with the binary operations of pointwise addition and convolution product, is an associative algebra. If R is a ring and M is a monoid with identity element e, then $R[M]$ is a ring with multiplicative identity the function I which takes e_M to 1_R and every other element of M to 0_R.*

Exercise 5.34: Prove Proposition 5.23. More precisely, verify that the proof of Proposition 5.22 goes through completely unchanged.

Note that as an abelian group, $R[M]$ is naturally isomorphic to the direct sum $\bigoplus_{m \in M} R$, i.e., of copies of R indexed by M. One can therefore equally well view an element $R[M]$ as a formal finite expressions of the form $\sum_{m \in M} a_m m$, where $a_m \in R$ and all but finitely many are 0. Written in this form, there is a natural way to define the product

$$\left(\sum_{m \in M} a_m m \right) \left(\sum_{m \in M} b_m m \right)$$

of two elements f and g of $R[M]$: namely we apply distributivity, use the multiplication law in R to multiply the a_m's and the b_m's, use the operation in M to multiply the elements of M, and then finally use the addition law in R to rewrite the expression in the form $\sum_m c_m m$. But a moment's thought shows that c_m is nothing else than $(f * g)(m)$. On the one hand, this makes the convolution product look very natural. Conversely, it makes clear:

The polynomial ring $R[t]$ is canonically isomorphic to the monoid ring $R[\mathbb{N}]$. Indeed, the explict isomorphism is given by sending a polynomial $\sum_n a_n t^n$ to the function $n \mapsto a_n$.

This gives a new proof of the associativity of the product in the polynomial ring $R[t]$. We leave it to the reader to decide whether this proof is any easier than direct

verification.. Rather the merit is that this associativity computation has been done once and for all in a very general context.

As an aside, let me point out something very curious: in searching for a slick proof of associativity of multiplication in the polynomial ring $R[t]$, we attempted to show that the multiplication was just multiplication of the associated functions $f : R \to R$. As we saw, this works in many but not all cases (because the homomorphism from $R[t]$ to the ring of functions R^R is not always surjective). Then we observed that the associativity of multiplication of polynomials is a special case of associativity of the product in a semigroup ring. What is strange is that the elements of this semigroup ring $R[\mathbb{N}]$ are themselves defined as functions, but functions from $\mathbb{N}$ to R, and the product is not the most obvious (pointwise) one – which has nothing to do with the semigroup structure on $\mathbb{N}$ – but rather a "funny" convolution product. Suitably mathematically urbane readers will, upon seeing a homomorphism from an abelian group (here $R[t]$) to another abelian group (here $\mathcal{P}$) which converts a "convolution product" on the first group to a "pointwise product" on the second group, be tempted to view the mapping $R[t] \to \mathcal{P}$ as some sort of **Fourier transform**. If I understood this phenomenon more completely myself, I might be more willing to digress to explain it (but I don't, so I won't).

The semigroup algebra construction can be used to define several generalizations of the polynomial ring $R[t]$.

Exercise 5.35: For any ring R, identify the monoid ring $R[\mathbb{Z}]$ with the ring $R[t, t^{-1}]$ of Laurent polynomials.

First, let $T = \{t_i\}$ be a set. Let $FA(T) := \bigoplus_{i \in T} (\mathbb{N}, +)$ be the direct sum of a number of copies of $(\mathbb{N}, +)$ indexed by T. Let R be a ring, and consider the monoid ring $R[FA(T)]$. Let us write the composition law in $FA(T)$ multiplicatively; moreover, viewing an arbitrary element I of $FA(T)$ as a finitely nonzero function from T to $\mathbb{N}$, we use the notation t^I for $\prod_{t \in T} t^{I(t)}$. Then an arbitrary element of $R[FA(T)]$ is a finite sum of the form $\sum_{k=1}^n r_k t^{I_k}$, where $I_1, \ldots, I_k$ are elements of $FA(t)$. This representation of the elements should make clear that we can view $R[FA(T)]$ as a polynomial ring in the indeterminates $t \in T$: we use the alternate notation $R[\{t_i\}]$.

Let us go back to the monoid ring $R[\mathbb{N}]$, whose elements are finitely nonzero functions $f : R \to \mathbb{N}$. Notice that in this case the precaution of restricting finitely nonzero functions is not necessary: the monoid $(\mathbb{N}, +)$, although infinite, has the property that for any $m \in \mathbb{N}$, the set of all $x, y \in \mathbb{N}$ such that $x + y = m$ is finite (indeed, of cardinality $m + 1$). Let us call an arbitrary monoid M **divisor-finite** if for each m in M, the set $\{(x, y) \in M^2 \mid xy = m\}$ is finite.

Exercise 5.36: a) For any set T, $FA(T) = \bigoplus_{t \in T} (\mathbb{N}, +)$ is divisor-finite.
b) A group is divisor-finite iff it is finite.

For a divisor-finite monoid M, and any ring R, we may define the **big monoid ring** $R[[M]]$ to be the collection of all functions $M \to R$, with pointwise addition and convolution product.

For example, if $M = (\mathbb{N}, +)$, then writing M multiplicatively with $n \in N \mapsto t^n$ for some formal generator t, an element of the ring $R[[M]]$ is an infinite formal sum $\sum_{n\in\mathbb{N}} r_n t^n$. Such sums are added coordinatewise and multiplied by distributivity:

$$(\sum_{n\in\mathbb{N}} r_n t^n)(\sum_{n\in\mathbb{N}} s_n t^n) = r_0 s_0 + (r_0 s_1 + r_1 s_0)t + \ldots + (\sum_{k=0}^{n} r_k s_{n-k})t^n + \ldots.$$

This ring is denoted by $R[[t]]$ and called the **formal power series ring** over R.

Exercise 5.37: Using Exercise 5.36, define, for any set $T = \{t_i\}$ and any ring R, a formal power series ring $R[[\{t_i\}]]$.

Here is yet another variation on the construction: suppose M is a commutative, cancellative divisor-finite monoid endowed with a total order relation $\leq$. (Example: $(\mathbb{N}, +)$ or $FA(T)$ for any T.) There is then a group completion $G(M)$ together with an injective homomorphism of monoids $M \to G(M)$. If M is finite and cancellative, it is already a group. If M is infinite, then so is $G(M)$, so it cannot be divisor-finite. Nevertheless, the ordering $\leq$ extends uniquely to an ordering on $G(M)$, and we can define a ring $R((G(M))$ whose elements are the functions from $f : G(M) \to R$ such that $\{x \in G(M) \mid x < 0,\ f(x) \neq 0\}$ is finite, i.e., f is finitely nonzero on the negative values of $G(M)$.

Exercise 5.38: a) Show that under the above hypotheses, the convolution product on $R((G(M))$ is well-defined, and endows $R((G(M))$ with the structure of a ring.
b) When $M = (\mathbb{N}, +)$, identify $R((M))$ as $R((t))$, the ring of formal finite-tailed Laurent series with coefficients in R. Give a multi-variable analogue of this by taking $M = FA(T)$ for arbitrary T.

Exercise 5.39: Let R be a possibly non-commutative ring. Give a rigorous definition of the ring $R\langle t_1, t_2\rangle$ of "noncommutative polynomials" – each t_i commutes with each element of R, but t_1 and t_2 do not commute – as an example of a small monoid ring $R[M]$ for a suitable monoid M. Same question but with an arbitrary set $T = \{t_i\}$ of noncommuting indeterminates.

The universal property of semigroup rings: Fix a commutative ring R. Let B be a commutative R-algebra and M a commutative monoid. Let $f : R[M] \to B$ be an R-algebra homomorphism. Consider f restricted to M; it is a homomorphism of monoids $M \to (B, \cdot)$. Thus we have defined a mapping

$$\mathrm{Hom}_{\text{R-alg}}(R[M], B) \to \mathrm{Hom}_{\text{Monoid}}(M, (B, \cdot)).$$

Interestingly, this map has an inverse. If $g : M \to B$ is any homomorphism satisfying $g(0) = 0$, $g(m_1 + m_2) = g(m_1) + g(m_2)$, then g extends to a unique R-algebra homomorphism $R[M] \to B$: $\sum_{m\in M} r_m m \mapsto \sum_m r_m g(m)$. The uniqueness of the extension is immediate, and that the extended map is indeed an R-algebra homomorphism can be checked directly (please do so).

In more categorical language, this canonical bijection shows that the functor $M \mapsto$

$R[M]$ is the **left adjoint** to the forgetful functor $(S, +, \cdot) \mapsto (S, \cdot)$ from R-algebras to commutative monoids. Yet further terminology would express this by saying that $R[M]$ is a "free object" of a certain type.

Theorem 5.24. *(Universal property of polynomial rings) Let $T = \{t_i\}$ be a set of indeterminates. Let R be a commutative ring, and S an R-algebra. Then each map of sets $T \mapsto S$ extends to a unique R-algebra homomorphism $R[T] \to S$.*

Proof: By the previous result, each monoid map from the free commutative monoid $\bigoplus_{t \in T} \mathbb{Z}$ to S extends to a unique R-algebra homomorhpism. So what is needed is the fact that every set map $T \to M$ to a commutative monoid extends uniquely to a homomorphism $\bigoplus_{t \in T} \mathbb{Z} \to M$ (in other words, we pass from the category of sets to the category of commutative R-algebras by passing through the category of commutative monoids, taking the free commutative monoid associated to a set and then the free R-algebra associated to the monoid). As before, the uniqueness of the extension is easy to verify.

Exercise 5.40: a) Formulate analogous universal properties for Laurent polynomial rings, and non-commutative polynomial rings.
b) Suppose M is a divisor-finite monoid. Is there an analogous extension property for the big monoid ring $R[[M]]$?

This result is of basic importance in the study of R-algebras. For instance, let S be an R-algebra. A generating set for S, as an R-algebra, consists of a subset T of S such that the least R-subalgebra of S containing T is S itself. This definition is not very concrete. Fortunately, it is equivalent to the following:

Theorem 5.25. *Let R be a commutative ring, S a commutative R-algebra, and T a subset of S. TFAE:*
(i) T generates S as an R-algebra.
(ii) The canonical homomorphism of R-algebras $R[T] \to S$ – i.e., the unique one sending $t \mapsto t$ – is a surjection.

Exercise 5.41: Prove Theorem 5.25.

In particular, a commutative R-algebra S is finitely generated iff it is a quotient ring of some polynomial ring $R[t_1, \ldots, t_n]$.

Another application is that every commutative ring whatsoever is a quotient of a polynomial ring (possibly in infinitely many indeterminates) over $\mathbb{Z}$. Indeed, for a ring R, there is an obvious surjective homomorphism from the polynomial ring $\mathbb{Z}[R]$ – here R is being viewed as a set of indeterminates – to R, namely the one carrying $r \mapsto r$.

A ring R is said to be **absolutely finitely generated** if it is finitely generated as a $\mathbb{Z}$-algebra; equivalently, there exists an $n \in \mathbb{N}$ and an ideal I in $\mathbb{Z}[t_1, \ldots, t_n]$ such that $\mathbb{Z}[t_1, \ldots, t_n]$ is isomorphic to R.

Exercise 5.42: a) Show that every finitely generated ring has finite or countably infinite cardinality.

b) Find all fields which are finitely generated as rings. (N.B.: In field there is another notion of absolute finite generation for a field. This a much weaker notation: e.g. $\mathbb{Q}(x)$ is absolutely finitely generated as a field but not as a ring.)

6. Swan's Theorem

We now digress to discuss an important theorem of R.G. Swan on projective modules over rings of continuous functions.

Throughout this section K denotes either the field $\mathbb{R}$ or the field $\mathbb{C}$, each endowed with their standard Euclidean topology. For a topological space X, the set $C(X)$ of all continuous functions $f : X \to K$ forms a commutative ring under pointwise addition and multiplication.

6.1. **Introduction to (topological) vector bundles.**

Recall[29] the notion of a **K-vector bundle** over a topological space X. This is given by a topological space E (the "total space"), a surjective continuous map $\pi : E \to X$ and on each fiber $E_x := \pi^{-1}(x)$ the structure of a finite-dimensional K-vector space satisfying the following local triviality property: for each $x \in X$, there exists an open neighborhood U containing x and a homeomorphism $f : \pi^{-1}U \to U \times K^n$ such that for all $y \in U$ f carries the fiber E_y over y to $\{y\} \times K^n$ and induces on these fibers an isomorphism of K-vector spaces. (Such an isomorphism is called a **local trivialization** at x.) As a matter of terminology we often speak of "the vector bundle E on X" although this omits mention of some of the structure.

On any K-vector bundle E over X we have a **rank function** $r : X \to \mathbb{N}$, namely we define $r(x)$ to be the dimension of the fiber E_x. We say that E is a **rank n** vector bundle if the rank function is constantly equal to n. The existence of local trivializations implies that the rank function is locally constant – or equivalently, continuous when $\mathbb{N}$ is given the discrete topology, so if the base space X is connected the rank function is constant.

As a basic and important example, for any $n \in \mathbb{N}$ we have the **trivial rank n vector bundle** on X, with total space $X \times K^n$ and such that π is just projection onto the first factor.

If $\pi : E \to X$ and $\pi' : E' \to X$ are two vector bundles over X, a **morphism** of vector bundles $f : E \to E'$ is a continuous map of topological spaces from E to E' *over* X in the sense that $\pi = \pi' \circ f$ – equivalently f sends the fiber E_x to the fiber E'_x – and induces a K-linear map on each fiber. In this way we get a category $\mathrm{Vec}(X)$ of K-vector bundles on X. If we restrict only to rank n vector bundles and morphisms between them we get a subcategory $\mathrm{Vec}_n(X)$. A vector bundle E on X is said to be trivial (or, for emphasis, "globally trivial") if it is isomorphic to the trivial rank n vector bundle for some n.

Many of the usual linear algebraic operations on vector spaces extend immediately to vector bundles. Most importantly of all, if E and E' are two vector bundles on

[29] from a previous life, if necessary

X, we can define a direct sum $E \oplus E'$, whose defininining property is that its fiber over each point $x \in X$ is isomorphic to $E_x \oplus E_{x'}$. This not being a topology/geometry course, we would like to evade the precise construction, but here is the idea: it is obvious how to define the direct sum of trivial bundles. So in the general case, we define the direct sum by first restricting to a covering family $\{U_i\}_{i \in I}$ of simultaneous local trivializations of E and E' and then *glue together* these vector bundles over the U_i's. In a similar way one can define the tensor product $E \otimes E'$ and the dual bundle $E^\vee$.

For our purposes though the direct sum construction is the most important. It gives $\mathrm{Vec}(X)$ the structure of an additive category: in addition to the existence of direct sums, this means that each of the sets $\mathrm{Hom}(E, E')$ of morphisms from E to E' form a commutative group. (In fact $\mathrm{Hom}(E, E')$ naturally has the structure of a K-vector space.) Decategorifying, the set of all isomorphism classes of vector bundles on X naturally forms a commutative monoid under direct sum (the identity is the trivial vector bundle $X \to X$ where each one point fiber is identified – uniquely! – with the zero vector space). The Grothendieck group of this monoid is $K(X)$: this is the beginning of **topological K-theory**.

6.2. **Swan's Theorem.**

But we digress from our digression. A **(global) section** of a vector bundle $\pi : E \to X$ is indeed a continuous section σ of the map π, i.e., a continuous map $\sigma : X \to E$ such that $\pi \circ \sigma = 1_X$. The collection of all sections to E will be denoted $\Gamma(E)$. Again this is a commutative group and indeed a K-vector space, since we can add two sections and scale by elements of K.

But in fact more is true. The global sections form a module over the ring $C(X)$ of continuous K-valued functions, in a very natural way: given a section $\sigma : X \to E$ and $f : X \to K$, we simply define $f\sigma : X \to E$ by $x \mapsto f(x)\sigma(x)$. Thus $\Gamma : E \to \Gamma(E)$ gives a map from vector bundles over X to $C(X)$-modules.

In fancier language, Γ gives an additive functor from the category of vector bundles on X to the category of $C(X)$-modules; let us call it the **global section functor**. (Indeed, if we have a section $\sigma : E \to X$ of E and a morphism of vector bundles $f : E \to E'$, $f(\sigma) = f \circ \sigma$ is a section of E'. No big deal!)

Theorem 6.1. *(Swan* [Sw62]*) Let X be a compact space. Then the global section functor Γ gives an equivalence of categories from* $\mathrm{Vec}(X)$ *to the category of finitely generated projective $C(X)$-modules.*

In other words, at least for this very topologically influenced class of rings $C(X)$, we may entirely identify finitely generated projective bundles with a basic and important class of geometric objects, namely vector bundles.

There is a special case of this result which is almost immediately evident. Namely, suppose that E is a trivial vector bundle on X, i.e., up to isomorphism E is simply $X \times K^n$ with $\pi = \pi_1$. Thus a section σ is nothing else than a continuous function $\sigma : X \to K^n$, which in turn is nothing else than an n-tuple $(f_1, \ldots, f_n)$ of elements of $C(X)$. Thus if we define $\sigma_i \in \Gamma(E)$ simply to be the section which takes each point to the ith standard basis vector e_i of K^n, we see immediately that $(\sigma_1, \ldots, \sigma_n)$

is a basis for $\Gamma(E)$, i.e., $\Gamma(E)$ is a free $C(X)$-module of rank n. Moreover, we have

$$\mathrm{Hom}(X \times K^n, X \times K^m) \cong \mathrm{Map}(X, \mathrm{Hom}_K(K^n, K^m))$$

$$\cong C(X) \otimes_K \mathrm{Hom}(K^n, K^w) \cong \mathrm{Hom}_{C(X)}(\Gamma(X \times K^n), \Gamma(X \times K^m)).$$

Thus we have established that Γ gives an additive equivalence from the category of trivial vector bundles on X to the category of finitely generated free $C(X)$-modules. We wish to promote this to an equivalence from locally trivial vector bundles (i.e., all vector bundles) to finitely generated projective modules. Oh, if only we had some nice "geometric" characterization of finitely generated projective modules!

But we do: namely Proposition 3.11 characterizes finitely generated projective modules over any commutative ring R as being precisely the images of projection operators on finitely generated free modules. Thus the essence of what we want to show is that for any vector bundle E over X (a compact space), there exists a trivial vector bundle T and a projection $P : T \to T$ – i.e., an element of $\mathrm{Hom}(T, T)$ with $P^2 = P$ such that the image of P is a vector bundle isomorphic to E. Indeed, if we can establish this, then just as in the proof of 3.11 we get an internal direct sum decomposition $T = P(T) \oplus (1 - P)(T)$ and an isomorphism $P(T) \cong E$, and applying the additive functor Γ this gives us that $\Gamma(E)$ is isomorphic to a direct summand of the finitely generated free $C(X)$-module $\Gamma(T)$. A little thought shows that in fact this proves the entire result, because we have characterized $\mathrm{Vec}(X)$ as the "projection category" of the additive category trivial vector bundles, so it must be equivalent to the "projection category" of the equivalent additive category of finitely generated free $C(X)$-modules. So from this point on we can forget about projective modules and concentrate on proving this purely topological statement about vector bundles on a compact space.[30]

6.3. **Proof of Swan's Theorem.**

Unfortunately the category of vector bundles over X is not an abelian category. In particular, it can happen that a morphism of vector bundles does not have either a kernel or image. Swan gives the following simple example: let $X = [0, 1]$, $E = X \times K$ the trivial bundle, and $f : E \to E$ be the map given by $f(x, y) = (x, xy)$. Then the image of f has rank one at every $x \neq 0$ but has rank 0 at $x = 0$. Since X is connected, a vector bundle over X should have constant rank function. Exactly the same considerations show that the kernel of f is not a vector bundle. However, nothing other than this can go wrong, in the following sense:

Proposition 6.2. *For a morphism $f : E \to E'$ of vector bundles over X, TFAE:*
(i) The image of f is a subbundle of E'.
(ii) The kernel of f is a subbundle of E.
(iii) The function $x \mapsto \dim_K(\mathrm{Im}\, f)_x$ is locally constant.
(iv) The function $x \mapsto \dim_K(\mathrm{Ker}\, f)_x$ is locally constant.

[30]We note that [Sw62] takes a more direct approach, for instance proving by hand that the global section functor Γ is fully faithful. In our use of projection operators and projection categories to prove Swan's theorem we follow Atiyah [At89, §1.4]. Aside from being a bit shorter and slicker, this approach really brings life to Proposition 3.11 and thus seems thematic in a commutative algebra course. But it is not really more than a repackaging of Swan's proof.

Proof. Step 1: We first wish to prove a special case: namely that if $f : E \to E'$ is a monomorphism of vector bundles (i.e., it induces an injection on all fibers) then $(\operatorname{Im} f)$ is a subbundle of E' and $f : E \to (\operatorname{Im} f)$ is an isomorphism. The issues of whether $\operatorname{Im} f$ is a vector bundle and f is an isomorphism are both local ones, so it suffices to treat the case where E and E' are trivial bundles. Suppose $E' = X \times V$, and let $x \in X$. Choose $W_x \subset V$ a subspace complementary to $(\operatorname{Im} f)_x$. Then $G := X \times W_x$ is a sub-bundle of E; let $\iota : G \to E$ be the inclusion map. Define $\theta : E \oplus G \to E'$ by $\theta((a, b)) = f(a) + \iota(b)$. Then θ_x is an isomorphism, so there exists an open neighborhood U of x such that $\theta|_U$ is an isomorphism. Since E is a subbundle of $E \oplus G$, $\theta(E) = f(E)$ is a subbundle of $\theta(E \oplus G) = E'$ on U.
Step 2: Since the rank function on a vector bundle is locally constant, (i) $\implies$ (iii), (ii) $\implies$ (iv), and (by simple linear algebra!) (iii) $\iff$ (iv).
(iv) $\implies$ (i): Again the issue of whether $\operatorname{Im} f$ is a vector bundle is a local one, so we may assume that $E = X \times V$ is a trivial bundle. For $x \in X$, let $W_x \subset V$ be a complementary subspace to $(\operatorname{Ker} f)_x$. Let $G = X \times W_x$, so that f induces a homomorphism $\psi : G \to E'$ whose fiber at x is a monomorphism. Thus ψ is a monomorphism on some neighborhood U of x, so $\psi(G)|_U$ is a subbundle of $E'|_U$. However $\Psi(G) \subset f(E)$, and since $f(E)$ has constant rank, and

$$\dim \psi(G)_y = \dim \psi(G)_x = \dim f(E)_x = \dim f(E)_y$$

for all $y \in U$, $\psi(G)|_U = f(E)|_U$. so $f(E)$ is a subbundle of E'.
(iv) $\implies$ (ii): here we exploit dual bundles. The hypothesis implies that the kernel of $f^\vee : (E')^\vee \to E^\vee$ has constant rank function. Since $E^\vee \to \operatorname{Coker} f^\vee$ is an epimorphism, $(\operatorname{Coker} f^\vee)^\vee \to E^{\vee\vee}$ is a monomorphism: by Step 1, its image is a subbundle. But the natural map $E \to E^{\vee\vee}$ is an isomorphism, the restriction of which to $\operatorname{Ker} f$ gives an isomorphism to the vector bundle $(\operatorname{Coker} f^\vee)^\vee$. So $\operatorname{Ker} f$ is a vector bundle. □

The proof yields the following additional information.

Corollary 6.3. *For any morphism of vector bundles, the rank function of the image is upper semi-continuous: that is, for any $x \in X$, there exists a neighborhood U of x such that for all $y \in U$, $\dim_K(\operatorname{Im} f)_y \geq \dim_K(\operatorname{Im} f)_x$.*

Exercise 6.1: Prove Corollary 6.3.

Proposition 6.4. *Let E be a vector bundle over X, and let $P \in \operatorname{End}(E) = \operatorname{Hom}(E, E)$ be a projection, i.e., $P^2 = P$. Then:*
a) We have $\operatorname{Ker}(P) = \operatorname{Im}(1 - P)$.
b) $\operatorname{Im} P$ and $\operatorname{Im}(1 - P)$ are both subbundles of E.
c) There is an internal direct sum decomposition $E = \operatorname{Im} P \oplus \operatorname{Im}(1 - P)$.

Proof. a) For all $x \in X$ linear algebra gives us an equality of fibers $\operatorname{Ker}(P)_x = \operatorname{Im}(1 - P)_x$. This suffices!
b) From part a) we deduce an equality of rank functions

$$r_{\operatorname{Im} P} + r_{\operatorname{Im}(1-P)} = r_E.$$

By Corollary 6.3, for all $x \in X$, there is a neighborhood U of x on which $r_{\operatorname{Im} P}$ is at least as large as $r_{\operatorname{Im} P}(x)$, $r_{\operatorname{Im}(1-P)}$ is at least as large as $r_{\operatorname{Im}(1-P)}(x)$ and r_E is constantly equal to $r_E(x)$. On this neighborhood the ranks of $\operatorname{Im} P$ and $\operatorname{Im}(1 - P)$ must be constant, and therefore by Proposition 6.2 $\operatorname{Im} P$ and $\operatorname{Im}(1 - P)$ are both

subbundles.
c) Again it is enough to check this fiber by fiber, which is simple linear algebra. □

An inner product on a finite-dimensional $\mathbb{R}$-vector space V is, as usual, a symmetric $\mathbb{R}$-bilinear form $\langle , \rangle : V \times V \to \mathbb{R}$ which is positive definite in the sense that for all $x \in V \setminus \{0\}$, $\langle x, x \rangle = 0$. An inner product on a finite-dimensional $\mathbb{C}$-vector space V is a positive definite sesquilinear form: i.e., it is $\mathbb{C}$-linear in the first variable, conjugate-linear in the second variable and again we have $\langle x, x \rangle > 0$ for all $x \in V \setminus \{0\}$.

Now let E be a K-vector bundle on X. An **inner product** on E is a collection of inner products $\langle , \rangle_x : E_x \times E_x \to K$ on each of the fibers which vary continuously in x. Formally this means the following: let $E \times_X E$ be the subset of $(e_1, e_2) \in E \times E$ such that $\pi(e_1) = \pi(e_2)$; then such a fiberwise family of inner products defines a function from $E \times_X E$ to K, and this function is required to be continuous.

Let us say that a **metrized vector bundle** E on X is a vector bundle together with an inner product. (Again, this is an abuse of terminology: we do not speak of the inner product by name.)

Proposition 6.5. *Let E be a metrized line bundle on X.*
a) If E' is a subbundle of E, fiberwise orthogonal projection onto E' defines a projection operator $P \in \mathrm{End}(E)$ with image E'.
b) All short exact sequences $0 \to E' \to E \to E'' \to 0$ of vector bundles are split.
c) If M is another vector bundle on X and there exists an epimorphism of bundles $q : E \to M$, then M is isomorphic to the image of a projection operator on E.

Proof. a) This is mostly a matter of understanding and unwinding the definitions, and we leave it to the reader.
b) Let P be orthogonal projection onto E'. The restriction of the map $E \to E''$ to $\operatorname{Ker} P$ is an isomorphism of vector bundles. The inverse of this isomorphism gives a splitting of the sequence.
c) By Proposition 6.2, since $\operatorname{Im} q = M$ is a vector bundle, so is $\operatorname{Ker} q$, whence a short exact sequence

$$0 \to \operatorname{Ker} q \to E \to M \to 0.$$

By part b), there exists a splitting $\sigma : M \to E$ of this sequence. Then, as usual, $P = \sigma \circ q$ is a projection operator on E and $q|_{\operatorname{Im} P} : \operatorname{Im} P \xrightarrow{\sim} M$. □

Proposition 6.6. *If X is a paracompact topological space, then every vector bundle over X admits an inner product.*

Proof. This is a rather standard topological argument which we just sketch here. Let M be a vector bundle on X, and let $\{U_i\}_{i \in I}$ be an open covering of X such that the restriction of M to each U_i is a trivial bundle. On a trivial bundle there is an obvious inner product, say $\langle , \rangle_x$. Now, since X is paracompact, there exists a partition of unity $\{\varphi_i\}_{i \in I}$ subordinate to the open covering $\{U_x\}$: that is,
• each $\varphi_i : X \to [0, 1]$ is continuous,
• for all $x \in X$ we have $\operatorname{supp}(\varphi_i) \subset U_i$
• for all $x \in X$ there exists an open neighborhood V of x on which all but finitely many φ_i's vanish identically, and

• for all $x \in X$, $\sum_{i \in I} \varphi_i(x) = 1$.[31]
Then, for $x \in X$ and $e_1, e_2 \in M_x$, define

$$\langle e_1, e_2 \rangle_x := \sum_i \varphi_i(x) \langle e_1, e_2 \rangle_i;$$

the sum extends over all $i \in I$ such that $x \in U_i$. This is an inner product on M. □

To complete the proof of Swan's Theorem, it suffices to show that if X is compact, every vector bundle M on X is the epimorphic image of a trivial bundle. In particular, Proposition X.X then shows that M is a direct summand of a trivial vector bundle T and thus $\Gamma(M)$ is a direct summand of the finitely generated free $C(X)$-module $\Gamma(T)$, hence is finitely generated projective.

Proposition 6.7. *Let X be a compact space and M a vector bundle on X. Then there exists an epimorphism of bundles from a trivial vector bundle $X \times V$ to M.*

Proof. Step 1: We CLAIM that for each $x \in X$, there exists a neighborhood U_x of x and finite set of global sections $S_x = \{s_{x,1}, \ldots, s_{x,k_x}\}$ of M such that for all $y \in U$, $s_{x,1}(y), \ldots, s_{x,k_x}(y)$ is a K-basis for M_y.
PROOF OF CLAIM: Let U be an open neighborhood of x on which M is a trivial bundle. Certainly then there exist finitely many sections $s_1, \ldots, s_n$ of M over U which when evaluated at any $y \in U$ give a basis of M_y. We need to show that there exists an open set W with $x \in W \subset U$ and global sections $s_1', \ldots, s_n'$ such that for all i, $s_i'|_W = s_i|_W$. For this it suffices to work one section at a time: let s be a section of M over U. Since X is paracompact, it is normal, so there exist open neighborhoods W and V of x with $\overline{W} \subset V$, $\overline{V} \subset U$. By Urysohn's Lemma, there is a continuous function $\omega : X \to [0,1]$ such that $\omega|_{\overline{W}} \equiv 1$ and $\omega|_{X \setminus V} \equiv 0$. If we then define $s' : X \to M$ by $s'(y) = \omega(y)s(y)$ for $y \in U$ and $s'(y) = 0$ for $y \in X \setminus U$, then this s does the job.
Step 2: By compactness of X, there exists a finite subset I of X such that $\{U_x\}_{x \in I}$ covers X. So $S = \bigcup_{i \in I} S_x$ is a finite set of global sections of M which when evaluated at any $x \in X$, span the fiber M_x. So the K-subspace V of $\Gamma(M)$ spanned by S is finite-dimensional. We define a map $q : X \times V \to M$ by $q(x,s) = s(x)$. This is a surjective bundle map from a trivial vector bundle to M! □

Remark: In the above proof the paracompactness of X seems to have been fully exploited, but the need for compactness is less clear. In fact, at the end of [Sw62], Swan remarks that if you replace the last step of the proof by an argument from Milnor's 1958 lecture notes *Differential Topology*, one gets a categorical equivalence between vector bundles *with bounded rank function* on a paracompact space X and finitely generated projective $C(X)$-modules.

Remark: A more straightforward variant of Swan's theorem concerns the case where X is a compact differentiable manifold (say of class C^∞). In this case the equivalence is between differentiable K-vector bundles on X and modules over the ring of K-valued C^∞-functions. Looking over the proof, one sees that the only part that needs additional attention is the existence of differentiable partitions of unity. Such things indeed exist and are constructed in many of the standard texts on geometry and analysis on manifolds. We recommend [Wel80], which has a particularly clear and complete discussion.

[31] See e.g. Exercise 5 in §4.5 of Munkres' *Topology: a first course* for a proof of this fact.

6.4. **Applications of Swan's Theorem.**

6.4.1. *Vector bundles and homotopy.*

Vector bundles on a space are of interest not only to differential topologists and geometers but also to algebraic geometers. This is because pullback of vector bundles behaves well under homotopy.

First, suppose that $f : X \to Y$ is a continuous map of topological spaces and $\pi : E \to Y$ is a vector bundle on Y. We may **pullback** π to a vector bundle $\pi_X : E \times_Y X \to X$ just by taking $E \times_Y X$ to be the fiber product of the maps f and π, namely the subspace of $X \times E$ consisting of all pairs (x, v) such that $f(x) = \pi(v) \in Y$. The map $\pi_X : E \times_Y X \to X$ is just restriction of the projection map: $(x, v) \mapsto x$.

Exercise 6.2: Show that $\pi_X : E \times_Y X \to X$ is indeed a vector bundle on X. We abbreviate it by either $f^*\pi$ or (more abusively) f^*E.

Exercise 6.3: Show that the pullback of any trivial bundle is a trivial bundle.

Theorem 6.8. *(Covering Homotopy Theorem) Let X and Y be topological spaces with X paracompact. Let $\pi : E \to Y$ be a vector bundle on Y, and let $f, g : X \to Y$ be homotopic maps. Then the pullbacks $f^*\pi$ and $g^*\pi$ are isomorphic vector bundles on X.*

Proof. See for instance [Hus66, Thm. 4.7]. □

For our applications, it is enough to know that compact spaces are paracompact. But for culture we also remark that any regular σ-compact space is paracompact, e.g. any CW-complex with only finitely many cells of any given dimension.

Corollary 6.9. *If X is a contractible paracompact space, then every vector bundle on X is trivial.*

Proof. Choose any point $x_0 \in X$, let $f : X \to X$ be the map which sends every point of X to x_0,and let $g : X \to X$ be the identity map. If $\pi : E \to X$ is any vector bundle on X, then by Theorem 6.8 we have $f^*\pi = g^*\pi$. Since g is the identity map, $g^*\pi = \pi$. On the other hand, tracking through the definitions shows $f^*\pi = X \times \pi^{-1}(x_0)$, a trivial bundle. So π is trivial. □

6.5. **Stably Free Modules.**

Recall that an R-module M is **stably free** if there is a finitely generated free module F such that $M \oplus F$ is free. This definition is natural from the perspective of K-theory: the class $[P]$ in $\widetilde{K_0(R)}$ of a finitely generated projective module P is trivial iff P is stably free.

Exercise: Let $0 \to A \to B \to P \to 0$ be a short exact sequence of R-modules, with P stably free. Show: A is stably free $\iff$ B is stably free.

Certainly we have

$$\text{projective} \implies \text{stably free} \implies \text{free}.$$

Asking to what extent these implications can be reversed brings us quickly to some deep and beautiful mathematics.

6.5.1. *Finite Generation.*

We begin by addressing finite generation conditions.

Exercise (**Eilenberg Swindle**): Let us say that a projective module P is **weakly stably free** if there exists a not necessarily finitely generated free module F such that $P \oplus F$ is free. Show that every projective module is weakly stably free.
(Hint: if $P \oplus Q$ is free, take $F = P \oplus Q \oplus P \oplus Q \oplus \ldots$.)

Exercise: Show that for a finitely generated projective module P, TFAE:
(i) P is stably free.
(ii) P admits a **finite free resolution**: for some $n \in \mathbb{N}$ there is an exact sequence

$$0 \to F_n \to \ldots \to F_0 \to P \to 0,$$

with each F_i a finitely generated free module.

This explains why the free module we take the direct sum with in the definition of stably free is required to be finitely generated. What happens if we take the module P to be infinitely generated? Here let us be sure that by an **infinitely generated R-module**, we mean an R-module which is *not* finitely generated.[32]

Theorem 6.10. *(Gabel) Each infinitely generated stably free module is free.*

Proof. Let M be infinitely generated and stably free. Choose $a \in \mathbb{N}$ such that $F = M \oplus R^a$ is free. Let $\{a_i\}_{i \in I}$ be a basis for F. Since F has an infinitely generated homomorphic image, I is infinite. Let $p : F \to R^a$ be the natural projection map $(x, y) \mapsto y$. For each standard basis element e_k of R^a lift it to $\widetilde{e_k}$ in F and let J_k be the "support" of $\widetilde{e_k}$, i.e., the set of indices i such that the coefficient of a_i in $\widetilde{e_k}$ is nonzero. Then $J = \bigcup_{k=1}^a J_k$ is finite. Let $F' = \langle a_i \rangle_{i \in J}$, so that F' is free of finite rank and F/F' is free of infinite rank. By construction $q(F') = R^a$; it follows that

$$F = F' + M.$$

Put $N = M \cap F'$, so

$$F'/N \cong R^a.$$

Since R^a is projective, the sequence

$$0 \to N \to F' \to R^a \to 0$$

splits, giving

$$F' \cong N \oplus R^a.$$

Further

$$F/F' \cong M/N,$$

so M/N is infinitely generated free: $M/N \cong R^a \oplus F''$ for a free module F''. In particular M/N is projective, so the sequence

$$0 \to N \to M \to M/N \to 0$$

[32] *A priori* it would be reasonable to take "infinitely generated R-module" to mean a module which possesses an infinite generating set, but a moment's thought shows that an R-module has this property iff it is infinite, so it is more useful to define "infinitely generated" as we have.

splits. Putting all this together we get

$$M \cong N \oplus M/N \cong N \oplus R^a \oplus F'' \cong F' \oplus F''.$$

□

The following result – which we will not prove here – shows that for a large class of "reasonable rings" infinitely generated projective modules are much less interesting objects than finitely generated projectives, and thus gives further motivation to our restriction to the finitely generated case.

Theorem 6.11. *(Bass* [Bas63]*) Let R be connected (i.e., without nontrivial idempotents) Noetherian ring. Then any infinitely generated projective R-module is free.*

However, we can use Swan's Theorem to exhibit a nonfree infinitely generated projective module. Let $[0,1]$ be the closed unit interval with its topology: a compact, contractible space. By Corollary 6.9, every vector bundle over $[0,1]$ is trivial. By Swan's Theorem, this implies that every finitely generated projective module over the ring $R = C([0,1])$ of continuous functions $f : [0,1] \to \mathbb{R}$ is free.

But now – as in §3.9 – consider the ideal I of all functions $f \in R$ which vanish *near zero*, i.e., for which there exists $\epsilon(f) > 0$ such that $f|_{[0,\epsilon(f)]} \equiv 0$. By Exercise X.X, I is a projective R-module. Moreover, I is not a free R-module: indeed, any $f \in I$ is annihilated by any continuous function with support lying in $[0, \epsilon(f)]$, and nonzero such functions clearly exist. On the other hand, any nonzero free module has elements with zero annihilator: take any basis element.

Thus $C([0,1])$ is a connected ring over which every finitely generated projective module is free, but the infinitely generated projective module I is not free. (Recall that Theorem 6.11 says that no such modules exist over connected *Noetherian* rings.) Moreover I is therefore clearly not a direct sum of finitely generated modules, since by what we have established any such module over $C([0,1])$ would be free!

Exercise 6.4: Use Corollary 3.47 to give a purely algebraic proof that I is not a direct sum of finitely generated submodules.

Exercise 6.5*: Find necessary and sufficient conditions on a compact, contractible space X for there to exist a nonfree projective module.

6.5.2. *Ranks.*

Later we will attach to a finitely generated projective module over any ring R a rank *function* (on $\operatorname{Spec} R$). However, for a stably free module we can – as for free modules – simply assign a rank. Namely, if we put $\operatorname{rank} P = b - a$.

Exercise: Show that the rank of a finitely generated stably free module is well-defined.

Exercise: Show that for an R-module M, the following are equivalent:
(i) M is stably free of rank zero.
(ii) $M = 0$.
Comment: This will be quite routine once we have the theory of localization. If you

have trouble with the general case now, just show that $M \oplus R \cong R \implies M = 0$, which is easier: every cyclic module is isomorphic to R/I for some ideal I of R; now consider annihilators.

6.5.3. *Digression: the least number of generators.*

For a finitely generated R-module M we denote by $\operatorname{mg} M$ the minimal number of generators of M, i.e., the least n such that $R^n \twoheadrightarrow M$.

From a naive perspective this is perhaps the most natural numerical invariant associated to a finitely generated R-module. But in fact it behaves badly. Essentially its only good property is the obvious one: if $M_1 \twoheadrightarrow M_2$, then $\operatorname{mg}(M_2) \leq \operatorname{mg}(M_1)$. However, if $M_1 \hookrightarrow M_2$, then we certainly *need not have* $\operatorname{mg}(M_1) \leq \operatorname{mg}(M_2)$: let I be a finitely generated but nonprincipal ideal, and let $M_1 = I$, $M_2 = R$.

One may momentarily hope that for finitely generated R-modules M_1 and M_2 we at least have $\operatorname{mg}(M_1 \oplus M_2) = \operatorname{mg}(M_1) + \operatorname{mg}(M_2)$ but in fact this is false even over the simplest rings: take $R = \mathbb{Z}$, $M_1 = \mathbb{Z}/2\mathbb{Z}$, $M_2 = \mathbb{Z}/3\mathbb{Z}$. But it gets even worse:

Exercise: Let R be a ring and M_1, M_2 be finitely generated R-modules.
a) Suppose R is local. Show: $\operatorname{mg}(M_1 \oplus M_2) = \operatorname{mg}(M_1) + \operatorname{mg}(M_2)$. In fact, show that if $0 \to M' \to M \to M'' \to 0$ is a short exact sequence of finitely generated R-modules then $\operatorname{mg}(M) = \operatorname{mg}(M') + \operatorname{mg}(M'')$.
b) Suppose R is a PID. Show: $\operatorname{mg}(M_1 \oplus M_1) = 2\operatorname{mg}(M_1)$.
c) Suppose R is a Dedekind domain,[33] and $\mathfrak{l}\, I$ is a nonzero proper ideal of R. Show:
(i) • If I is principal, $\operatorname{mg}(I) = 1$.
• If I is not principal, $\operatorname{mg}(I) = 2$.
(ii) • If I^2 is principal, $\operatorname{mg}(I \oplus I) = 2$.
(iii) • If I^2 is not principal, $\operatorname{mg}(I \oplus I) = 3$.
d) Deduce: For a nonprincipal ideal I in a Dedekind domain R, $\operatorname{mg}(I \oplus I) < 2\operatorname{mg}(I)$.

Later we will see "better" invariants for certain subclasses of finitely generated R-modules, namely the rank for projective modules and the length for...finite length modules. Over a Dedekind domain every finitely generated module can be decomposed into the direct sum of a projective module and a finite length module. This does not hold over more general rings, e.g. the $\mathbb{C}[x,y]$-module $\mathbb{C}[x]$ is a torsion module of infinite length so cannot be so expressed.

Proposition 6.12. *A rank one stably free module is free.*

We will come back to prove this later once we have developed localization.

6.5.4. *Around Hermite's Lemma.*

In number theory and related branches of mathematics one studies sublattices Λ of the standard integral lattice $\mathbb{Z}^n$, i.e., rank n $\mathbb{Z}$-submodules of $\mathbb{Z}^n$. Their structure is surprisingly rich – for instance, the function $L_n(k)$ which counts the number of

[33]This exercise is stated now for continuity purposes, but to solve it you will probably want to use the theory of finitely generated modules over a Dedekind domain detailed in § 20.6.

index k sublattices of $\mathbb{Z}^n$ is arithmetically interesting and nontrivial. In particular, one question that comes up in the study of integer lattices is: which vectors $v \in \mathbb{Z}^n$ can be part of a $\mathbb{Z}$-basis of $\mathbb{Z}^n$? Unlike the answer for modules over a field (all nonzero vectors), there is an obvious obstruction: for instance there is no basis (v_1, v_2) of $\mathbb{Z}^2$ with $v_1 = (2, 0)$. For if so, the linear transformation $T : \mathbb{Z}^2 \to \mathbb{Z}^2$ given by $T((1, 0)) = (2, 0)$, $T((0, 1)) = v_2 = (a, b)$ has determinant $2b$. Since this is not a unit in $\mathbb{Z}$, T is not invertible, which is a contradiction (make sure you see why, e.g. by using the universal property of free modules).

This observation can be vastly generalized, as follows: for a domain R and $n \in \mathbb{Z}^+$, we say $v = (x_1, \ldots, x_n) \in R^n$ is **a primitive vector** if $v \neq 0$ and $\langle x_1, \ldots, x_n \rangle = R$.

Exercise: Let K be the fraction field of R. Show that $v \in (R^n)^\bullet$ is primitive iff $Kv \cap R^n = Rv$.

Exercise: Let R be a domain, and let $(b_1, \ldots, b_n)$ be a basis for R^n. Show that each b_i is a primitive vector.

In 1850 Hermite proved that for integer lattices this is the only obstruction.

Proposition 6.13. *(Classical Hermite Lemma) For a vector $v \in \mathbb{Z}^n$, TFAE:*
(i) There is $M \in \mathrm{GL}_n(\mathbb{Z})$ with $M(e_1) = v$, i.e., the first column of M is v.
(ii) There is a basis for $\mathbb{Z}^n$ containing v.
(iii) v is a primitive vector.

For a proof of Proposition 6.13 in the classical style, see [**?**, § 1.3.3]. In fact the methods of module theory allow for a much slicker proof of a more general result.

Proposition 6.14. *Let R be a PID. For a vector $v \in R^n$, TFAE:*
(i) There is $M \in \mathrm{GL}_n(R)$ with $M(e_1) = v$, i.e., the first column of M is v.
(ii) There is a basis for R^n containing v.
(iii) v is a primitive vector.

Proof. Any two bases of R^n are equivalent under $\mathrm{GL}_n(R)$. So (i) $\iff$ (ii).
(ii) $\implies$ (iii): If $v, v_2, \ldots, v_n$ is a basis for R^n and v were not primitive, then we would have $v = \alpha w$ for some $\alpha \in R^\bullet \setminus R^\times$. Then $w = \frac{1}{\alpha} v$ expresses w as a K-linear combination of the basis vectors with a nonintegral coefficient. This is a contadiction.
(iii) $\implies$ (ii): Step 1: For a domain R and $v \in (R^n)^\bullet$, we claim that v is a primitive vector iff $R^n/\langle v \rangle$ is torsionfree.
Proof: Suppose v is not primitive: $v = \alpha v'$ for some $\alpha \in R^\bullet \setminus R^\times$. Then v' is a torsion element of $R^n/\langle v \angle$. Conversely, suppose v is primitive. If$n = 1$ then $\langle v \rangle = R$ and the result holds trivially, so assume $n \geq 2$. Suppose there is $w \in R^n$ and $\alpha \in \mathbb{R}^\bullet$ such that $\alpha w = \beta v$ for some $\beta \in R$. Thus $w = \frac{\beta}{\alpha} v$. Since v is primitive, $\alpha \mid \beta$ and the image of w in $R^n/\langle v \rangle$ is zero.
Step 2: Consider the short exact sequence

$$0 \to \langle v \rangle \to R^n \to M \to 0,$$

with $M = R^n/\langle v \rangle$. By Step 1, M is a finitely generated torsionfree module over a PID, so it is free: indeed, tensoring to K and applying linear algebra we see that

$M \cong R^{n-1}$. Thus the sequence splits: $R^n = \langle v \rangle \oplus M'$, with $M' \cong R^{n-1}$. Thus if $v_2, \ldots, v_n$ is an R-basis for M', $v, v_2, \ldots, v_n$ is an R-basis for R^n. □

Proposition 6.15. *Let R be a commutative ring, and let $n \in \mathbb{Z}^+$. TFAE:*
(i) If for an R-module M we have $M \oplus R \cong R^n$ then M is free.
(ii) Every primitive vector $v \in R^n$ is part of a basis for R^n.

Proof. We follow a treatment of K. Conrad [Cd-SF]. First we observe that when $n = 1$ both (i) and (ii) hold for all R-modules M: indeed, by Exercise X.X, if $M \oplus R \cong R$ then $M = 0$, whereas (ii) is completely vacuous in this case.
(i) $\implies$ (ii): Assume (i). For $\mathbf{v} = (v_1, \ldots, v_n)$, $\mathbf{w} = (w_1, \ldots, w_n) \in R^n$, let $\mathbf{v} \cdot \mathbf{w} = \sum_{i=1}^n v_i w_i$. Let $\mathfrak{a} = (a_1, \ldots, a_n) \in R^n$ be a primitive vector. Observe that this is equivalent to the existence of $\mathfrak{b} = (b_1, \ldots, b_n) \in R^n$ with $\mathfrak{a} \cdot \mathfrak{b} = 1$ and fix such a $\mathfrak{b}$. Consider the R-linear functional $f : R^n \to R$ given by $\mathbf{v} \mapsto \mathbf{v} \cdot \mathfrak{b}$. Since $f(\mathfrak{a}) = 1$ it is nonzero and thus there is a short exact sequence

$$0 \to \operatorname{Ker} f \to R^n \xrightarrow{f} R \to 0.$$

Since R is projective, this sequence splits, giving $R^n \cong \operatorname{Ker} f \oplus R$. More concretely a splitting is given by a section $\sigma : R \to R^n$ of f which is determined by mapping $1 \in R$ to any $v \in R^n$ with $f(v) = 1$. Thus $1 \mapsto \mathfrak{a}$ gives an internal direct sum decomposition

$$R^n = \operatorname{Ker} f \oplus \langle \mathfrak{a} \rangle \cong \operatorname{Ker} f \oplus R.$$

By our hypothesis (i), $\operatorname{Ker} f$ is free, and if $\mathfrak{b}_2, \ldots, \mathfrak{b}_n$ is a basis for $\operatorname{Ker} f$ then $\mathfrak{a}, \mathfrak{b}_2, \ldots, \mathfrak{b}_n$ is a basis for R^n containing $\mathfrak{a}$.
(ii) $\implies$ (i): Let $g : M \oplus R \xrightarrow{\sim} R^n$ be an R-module isomorphism. Put $\mathfrak{a} = (a_1, \ldots, a_n) = g(0,1)$. We claim that $\mathfrak{a}$ is a primitive vector. If not, there is a maximal ideal $\mathfrak{m}$ such that $\langle a_1, \ldots, a_n \rangle \subset \mathfrak{m}$. But

$$g|_{\mathfrak{m}(M \oplus R^n)} : \mathfrak{m}M \oplus \mathfrak{m} \xrightarrow{\sim} (\mathfrak{m}R)^n,$$

and $g(0,1) = \mathfrak{a} \in (\mathfrak{m}R)^n$, so $(0,1) \in \mathfrak{m}M \oplus (\mathfrak{m}R)^n$, a contradiction. Thus by (ii) there is a basis $\mathfrak{a}, \mathfrak{b}_2, \ldots, \mathfrak{b}_n$ of R^n, so that $g^{-1}(\mathfrak{a}), g^{-1}(\mathfrak{b}_2), \ldots, g^{-1}(\mathfrak{b}_n)$ is a basis of $M \oplus R$. For $2 \leq i \leq n$ we write $g^{-1}(\mathfrak{b}_i) = (x_i, c_i)$. Subtracting off from each of these vectors a suitable scalar multiple of $g^{-1}(\mathfrak{a}) = (0,1)$ we get a new basis $(0,1), (x_2, 0), \ldots, (x_n, 0)$ of $M \oplus R$. A moment's thought shows that then $x_2, \ldots, x_n$ is a basis for M. □

Theorem 6.16. *For a commutative ring R, the following are equivalent:*
(i) For all R-modules M, if $M \oplus R$ is free, then M is free.
(ii) For all $n \in \mathbb{Z}^+$, every primitive vector $v \in R^n$ is part of a basis of R^n.
(iii) Every stably free R-module M is free.

Proof. In view of Gabel's Theorem (Theorem 6.10), conditions (i) and (iii) necessarily hold if M is finitely generated, so we may assume this throughout. Then:
(i) $\iff$ (ii) is immediate from Proposition 6.15.
(i) $\implies$ (iii): It suffices to show that for all finitely generated modules M and all $a \in \mathbb{N}$, if $M \oplus R^a$ is free then M is free. We go by induction on n, the case $n = 0$ being trivial. Suppose the result holds for $a \in \mathbb{N}$. Then $M \oplus R^{a+1} \cong (M \oplus R^a) \oplus R$ is free, so by (i) $M \oplus R^a$ is free, and then by induction M is free.
(iii) $\implies$ (i) is immediate. □

6.5.5. *Swan's Construction.*

For $n \in \mathbb{N}$, let

$$R_n = \mathbb{R}[t_0, \ldots, t_n]/\langle t_0^2 + \ldots + t_n^2 - 1\rangle.$$

Exercise: Show that R_n is a domain iff $n \geq 1$.

Consider the map $H : R_n^{n+1} \to R_n$ obtained by taking the dot product of $\mathbf{v} = (v_1, \ldots, v_{n+1})$ with $\mathbf{t} = (t_0, \ldots, t_n)$. For $0 \leq i \leq n$, let e_i be the ith standard basis vector of R_n^{n+1}; then $H(e_i) = t_i$, so the image of H contains $\langle t_0, \ldots, t_n\rangle = R_n$: H is surjective. Let $P_n = \operatorname{Ker} H$, so we have a short exact sequence

$$0 \to P_n \to R_n^{n+1} \stackrel{H}{\to} R_n \to 0.$$

As above, this sequence splits and since $\mathbf{t} \cdot \mathbf{t} = 1$, a canonical section is given by mapping $1 \in R_n$ to $\mathbf{t}$. In particular

$$P_n \oplus R_n \cong R_n^{n+1}$$

so P_n is stably free. When is it free?

Theorem 6.17. *(Swan) The stably free R_n-module P_n is free iff $n = 0, 1, 3$ or 7.*

Proof. Step 0: Since $P_0 = 0$, it is free. Moreover P_1 has rank 1 so is free by general principles (Proposition 6.12). But this is overkill: in fact one sees that $-t_1 e_0 + t_0 e_1$ is a basis for P_1. Similarly one can simply write down bases for P_3 and P_7 in a concrete manner: we leave this as an exercise for the reader.
Step 1: Suppose $n \notin \{0, 1, 3, 7\}$, so we wish to show that P_n is *not* free. The key observation is that it is enough to show this after any base change: that is, if $R_n \to S$ is a ring map and M is an R-module such that $M \otimes_{R_n} S$ is not a free S-module, then M is not a free R-module. What is the natural base change to make?

Notice that R_n is nothing else than the ring of polynomial functions on the unit sphere $S^n \subset \mathbb{R}^{n+1}$. For those unitiated in the above jargon we spell it out more explicitly: every $f \in \mathbb{R}[t_0, \ldots, t_{n+1}]$ induces a function from $\mathbb{R}^{n+1} \to \mathbb{R}$ and thus by restriction a function $S^n \to \mathbb{R}$. We wish to identify polynomials which define the same function on S^n, and to do so we should at least impose the relation $t_0^2 + \ldots + t_n^2 - 1 = 0$ since this function vanishes identically on S^n. As we will see later when we study the Nullstellensatz, since by Exericse X.X the ideal $I = \langle t_0^2 + \ldots + t_n^2 - 1\rangle$ is prime, it is radical and thus the relation $I(V(I)) = I$ tells us that the only polynomials which vanish identically on S^n are those in I.

Since every polynomial function is a continuous function for the Euclidean topology on S^n, we get an extension of rings $R_n \to C(S^n)$. So our bright idea is to show insteaad that the finitely generated projective $C(S^n)$-module

$$T_n = P_n \otimes_{R_n} C(S^n)$$

is not free. By Swan's Theorem, T_n corresponds to a vector bundle on S^n and it is equivalent to show that this vector bundle is nontrivial. [34]
Step 3: We claim that in fact T_n is nothing else but the tangent bundle of S^n. Indeed, we have $S^n \subset \mathbb{R}^{n+1}$. The tangent bundle to $\mathbb{R}^{n+1}$ is trivial, hence so is its pullback to S^n, say F^{n+1}. Further, there is a surjective bundle map from F^{n+1} to

[34]Thus in summary we have just accomplished the following exciting maneuver: using basic affine algebraic geometry, we have completely transferred our problem from the domain of commutative algebra to that of differential topology!

the rank one trivial bundle F^1: at every point of S^n we orthogonally project to the outward normal vector. The kernel of this bundle map is $T(S^n)$. Thus we have a short exact sequence of vector bundles

$$0 \to TS^n \to F^{n+1} \to F \to 0.$$

We claim that under the Swan's Theorem equivalence of categories, this split exact sequence corresponds to the split exact sequence

$$0 \to T_n \to C(S^n)^{n+1} \stackrel{H}{\to\to} C(S^n) \to 0$$

which is the base change to $C(S^n)$ of the defining short exact sequence of S^n. We leave it to the interested reader to piece this together from our consruction of P_n.
Step 4: By a classical theorem of Bott and Milnor [BM58], the tangent bundle of S^n is trivial iff $n \in \{0, 1, 3, 7\}$. □

Exercise: Show that P_n is free for $n = 3$ and $n = 7$.

Exercise*: Find stably free but not free modules of ranks 3 and 7 over some ring.

The Bott-Milnor Theorem is a deep and celebrated result. Their original proof used the recently developed tools of midcentury differential topology: Stiefel-Whitney and Pontrjagin classes, cohomology operations, and so forth. In 1962 J.F. Adams determined for each n the largest rank of a trivial subbundle of $T(S^n)$ [Ad62]. The K-theory developed in the 1960's gave more graceful proofs: we recommend that the interested reader consult, for instance, [Ka, § V.2].

If one merely wants *some* values of n for which P_n is not free, one can use much lower technology. for instance, the Poincare-Hopf Theorem [Mi, p. 35] implies that a closed n-manifold which admits a nowhere vanishing vector field (equivalently a trivial rank one subbundle of its tangent bundle; this is much weaker than the tangent bundle being trivial) must have zero Euler characteristic. The Euler characteristic of S^n is $1 + (-1)^n$, so it is nonzero forall even n.

Further, a purely algebraic proof of Theorem 6.17 when $n = 2$. But to the best of my knowledge the full result still requires these topological techniques.

6.6. **The Theorem of Bkouche and Finney-Rotman.**

Let X be a Hausdorff topological space. One says that a function $f \in C(X)$ has **compact support** if $\{x \in X \mid f(x) \neq 0\}$ has compact closure.

Exercise: Let J be the set of functions in $C(X)$ with compact support. Show that J is an ideal of $C(X)$.

Theorem 6.18. *(Bkouche* [Bk70]*, Finney-Rotman* [FR70]*) For a locally compact space X, the following are equivalent:*
(i) J is a projective $C(X)$-module.
(ii) X is paracompact.

Exercise: Let X be a connected topological manifold.
a) Show that J is a projective $C(X)$-module iff X is second countable.
b) Exhibit a connected manifold for which J is not a projective $C(X)$-module.

7. Localization

7.1. **Definition and first properties.**

As we have seen, one way to "simplify" the study of ideals in a ring R is to pass to a quotient ring R/I: as we have seen, this has the (often useful) effect of "cutting off the bottom" of the ideal lattice by keeping only ideals $J \supset I$. There is another procedure, **localization**, which effects the opposite kind of simplification: given a **prime** ideal P of R, there is a ring R_P together with a canonical map $\iota : R \to R_P$ such that $\iota^* : \mathcal{I}(R_P) \to \mathcal{I}(R)$ is an injection whose image is precisely the ideals $J \subset P$. As usual, ι^* carries prime ideals to prime ideals. In particular, assuming only that P is prime, we get a corresponding ideal – rather inelegantly but standardly denoted PR_P – which is the **unique maximal** ideal of R_P. If we can take $P = (0)$ – i.e., if R is a domain – this means that PR_P is the only ideal of R_P, which is therefore a field. In fact it is nothing else than the quotient field of the integral domain R, and – with one exception – all the secrets of localization are already present in this very familiar special case.

In fact the localization construction is a bit more general than this: given an arbitrary ring R (of course commutative with unity!) and an arbitrary **multiplicative subset** S of R – this just means that $1 \in S$ and $SS \subset S$ – we will define a new ring R_S together with a canonical homomorphism $\iota : R \to R_S$ (for which ι^* will still be an injection with explicitly given image). In fact, just as in the case of quotients, ι satisfies a certain universal mapping property, but let us sacrifice some elegance for intelligibility by working our way up to this crisp definition.

Indeed, first consider the special case in which R is a domain, with fraction field F. Then R_S will be an extension ring of R, still with fraction field F, which is obtained by adjoining to R all elements $\frac{1}{s}$ for $s \in S$.

Example: Suppose $R = \mathbb{Z}$, $S = \{2^n\}_{n \in \mathbb{N}}$. Then $R_S = \mathbb{Z}[\frac{1}{2}]$. Indeed we see that for any nonzero element f, we can take S to be the multiplicative set consisting of the powers of f, and then the localization is just $R[\frac{1}{f}]$.

What if in the example above, instead of taking the multiplicative subset generated by 2, we took the multiplicative subset generated by 2^2, or 2^{127}? Clearly it wouldn't matter: if we have $\frac{1}{2^k}$ for any k in our subring of $\mathbb{Q}$, we also have $\frac{2^{k-1}}{2^k} = \frac{1}{2}$. To generalize this idea, define the **saturation** $\mathbb{S}$ of a multiplicatively closed subset S of a domain R to be the set $\{a \in R \mid \exists b \in R \mid ab \in S\}$, i.e., the set of all divisors of elements of S. The same observation as above shows that $R_S = R_{\mathbb{S}}$, so if we like we can restrict to consideration of saturated multiplicatively closed subsets.

Example, continued: The saturated, multiplicatively closed subsets of $\mathbb{Z}$ correspond to (arbitary) subsets $\mathcal{P}$ of the prime numbers (exercise!). In particular $\mathbb{Z}$ itself corresponds to $\mathcal{P} = \emptyset$, $\mathbb{Z}[\frac{1}{p}]$ corresponds to $\mathcal{P} = \{p\}$, $\mathbb{Q}$ corresponds to the set of all primes. Most interestingly, fix any prime p and let $\mathcal{P}$ be the set of all primes **except** p: then the corresponding ring, which is confusingly denoted $\mathbb{Z}_{(p)}$ is the set of all rational numbers of the form $\frac{x}{y}$ where p does not divide y. Notice that such rings are the maximal subrings of $\mathbb{Q}$ which are not fields. Moreover, the units

of $\mathbb{Z}_{(p)}$ are precisely the elements of the form $\frac{x}{y}$ with $(p,x) = 1$. The nonunits a are all of the form pa' for $a' \in \mathbb{Z}_{(p)}$, so therefore the unique maximal ideal is the principal ideal $(p) = p\mathbb{Z}_{(p)}$.

Exercise 7.1: Show that the only ideals in $\mathbb{Z}_{(p)}$ are those of the form $(p)^k$ for some $k \in \mathbb{N}$. Notice that this set happens to be identifiable with the set of all ideals I of $\mathbb{Z}$ which are disjoint from the multiplicative set $S(\mathcal{P})$.

Now let R be any ring and S a multiplicatively closed subset of R. We would still like to define a ring $S^{-1}R$ which is, roughly speaking, obtained by adjoining to R all inverses of elements of S. We can still define $S^{-1}R$ in terms of formal quotients, i.e., as equivalence classes of elements (a,b) with $a \in R$, $b \in S$. However, if we define $(a,b) \sim (c,d)$ to be $ad = bc$, then unfortunately we find that this need not be an equivalence relation! Therefore we need to enlarge the relation a bit: we put $(a,b) \sim (c,d)$ iff there exists $s \in S$ such that $sad = sbc$. We then define

$$\frac{a}{s} + \frac{b}{t} := \frac{at + bs}{st},$$

$$\frac{a}{s} \cdot \frac{b}{t} := \frac{ab}{st}.$$

We must check that these operations are well-defined on equivalence classes; this is left as a (perhaps somewhat tedious, but not difficult) exercise for the reader.

Exercise 7.2: Indeed, check that $S^{-1}R$ is a ring and that $x \mapsto \frac{x}{1}$ defines a homomorphism of rings $R \to S^{-1}R$. Thus $S^{-1}R$ is an R-algebra, and in particular an R-module.

Exercise 7.3: Let R be a domain and $S = R^\bullet = R \setminus \{0\}$. Show that $S^{-1}R$ is indeed the fraction field of R.

When $f \in R$, we denote the localization of R at the multiplicative subset generated by f as R_f.

Example: Suppose $f \in R$ is a nilpotent element: $f^n = 0$ for some $n \in \mathbb{Z}^+$. Then $1 = \frac{f^{n-1}}{f^{n-1}}$ whereas $0 = \frac{0}{f}$. Since $(f^{n-1} \cdot f - f^{n-1} \cdot 0) = 0$, we have that $1 = 0$, i.e., R_f is the zero ring. Conversely, if f is not nilpotent, then if it is a unit, $R_f = R$. Otherwise, all the powers of f are distinct, and then $\frac{1}{f} \neq \frac{1}{1}$, since for any $n \in \mathbb{N}$, $f^n(1-f) \neq 0$, so that R_f is not the zero ring. In general, $S^{-1}R$ is the zero ring iff S contains 0. This is to be regarded as a trivial case, and may safely be tacitly excluded in the sequel.

Exercise 7.4: a) Show that the kernel of the natural map $R \to S^{-1}(R)$ is the set of all $r \in R$ such that for some $s \in S$, $sr = 0$.
b) The map $R \to S^{-1}(R)$ is injective iff S has no zerodivisors.
c) Show that the subset Q of all nonzerodivisors of a ring R is multiplicatively closed. The localization $Q^{-1}R$ is called the **total fraction ring** of R. Show that $Q^{-1}(R)$ is a field iff R is an integral domain.

Exercise 7.5: Show that the homomorphism $R \to S^{-1}R$ is universal for homomorphisms $R \to T$ with $f(S) \subset T^\times$.

7.2. **Pushing and pulling via a localization map.**

Let R be a ring and S a multiplicatively closed subset. Let $\iota : R \to S^{-1}R$ be the natural map. As for any homomorphism of rings, ι induces maps between the sets of ideals of R and the set of ideals of $S^{-1}R$, in both directions:

$$\iota_* : \mathcal{I}_R \to \mathcal{I}_{S^{-1}R},\ I \mapsto IS^{-1}R,$$

$$\iota^* : \mathcal{I}_{S^{-1}R} \to \mathcal{I}_R,\ J \mapsto \iota^{-1}(J).$$

Lemma 7.1. *Let $\iota : R \to S^{-1}R$ be a localization map. Then for any ideal I of R,*

$$\iota_*(I) = \{\frac{x}{s} \in S^{-1}R \mid x \in I,\ s \in S\}.$$

Proof. Let us temporarily write

$$\mathcal{I} = \{\frac{x}{s} \in S^{-1}R \mid x \in I,\ s \in S\}.$$

We want to show that $\mathcal{I} = \iota_*(I) = \langle \iota(I) \rangle_{S^{-1}R}$. It is clear that $\iota(I) \subset \mathcal{I} \subset \iota_*(I)$, so it is enough to show that $\mathcal{I}$ is itself an ideal of $S^{-1}R$. No problem: if $\frac{x_1}{s_1},\ \frac{x_2}{s_2} \in \mathcal{I}$,

$$\frac{x_1}{s_1} + \frac{x_2}{s_2} = \frac{x_1 s_2 + x_2 s_1}{s_1 s_2} \in \mathcal{I},$$

and if $\frac{y}{s} \in S^{-1}R$, then

$$\frac{y}{s}\frac{x_1}{s_1} = \frac{x_1 y}{s s_1} \in \mathcal{I}.$$

□

Like quotient maps, any localization map has the **pull-push property**.

Proposition 7.2. *Let $\iota : R \to S^{-1}R$ be a localization. For any ideal J of $S^{-1}R$,*

$$J = \iota_* \iota^* J.$$

Proof. We have seen before that for any homomorphism $\iota : R \to R'$ of rings and any ideal J of R' we have

$$\overline{J} := \iota_* \iota^* J \subset J.$$

Thus it is enough to show the reverse containment. For this, consider an arbitrary element $\frac{x}{s} \in J$. Then $x = s\frac{x}{s} \in J$ hence also $x \in \iota^*(J)$, so $\iota(x) \in \overline{J}$. But since $\overline{J}$ is an ideal and s is a unit in $S^{-1}R$, we then also have $\frac{1}{s}x = \frac{x}{s} \in \overline{J}$. □

Lemma 7.3. *Let $\iota : R \to S^{-1}R$ be a localization map and I an ideal of R. TFAE:*
(i) $I \cap S \neq \emptyset$.
(ii) $\iota_*(I) = S^{-1}R$.

Proof. (i) $\implies$ (ii): If $s \in S \cap I$, then $s \in IS^{-1}R$, so $1 = \frac{s}{s} \in \iota_*(I)$.
(ii) $\implies$ (i): Suppose $1 \in \iota_*(I)$. By Lemma 7.1, $\frac{1}{1} = \frac{x}{s}$ for some $x \in I$ and $s \in S$. Clearing denominators, there is $s' \in S$ such that $ss' = s'x$ and thus $ss' \in I \cap S$. □

Proposition 7.4. *Let $\iota : R \to S^{-1}R$ be a localization homomorphism.*
a) For a prime ideal $\mathfrak{p}$ of R, TFAE:
(i) The pushforward $\iota_*\mathfrak{p}$ is prime in $S^{-1}R$.
(ii) The pushforward $\iota_*\mathfrak{p}$ is proper in $S^{-1}R$.
(iii) We have $\mathfrak{p} \cap S = \varnothing$.
b) If $\mathfrak{p}$ is prime and disjoint from S, then $\iota^*(\iota_*\mathfrak{p}) = \mathfrak{p}$.

Proof. a) (i) $\implies$ (ii) since prime ideals are proper.
(ii) $\iff$ (iii) for all ideals of R by Lemma 7.3.
(iii) $\implies$ (i): Suppose $\mathfrak{p}$ is a prime ideal of R, and suppose we have $\frac{a_1}{s_1}, \frac{a_2}{s_2} \in S^{-1}R$ with $\frac{a_1}{s_1}\frac{a_2}{s_2} = \frac{x}{s} \in \iota_*(\mathfrak{p})$. Clearing denominators, there is $s' \in S$ such that

$$ss'a_1a_2 = s's_1s_2x \in \mathfrak{p}.$$

Since $S \cap \mathfrak{p} = \varnothing$, $(ss') \notin \mathfrak{p}$, and since $\mathfrak{p}$ is prime, we conclude that $a_1a_2 \in \mathfrak{p}$ and then that $a_i \in \mathfrak{p}$ for some i, hence $\frac{a_i}{s_i} \in \iota_*\mathfrak{p}$ for some i and $\iota_*(\mathfrak{p})$ is prime. This completes the proof of part a).
b) Recall: for any homomorphism $\iota : R \to R'$ and any ideal I of R we have

$$\iota^*(\iota_*(I)) \supset I,$$

so taking $I = \mathfrak{p}$ to be prime it suffices to show the inverse inclusion. Suppose $x \in \iota^*\iota_*\mathfrak{p}$, i.e., there exist $a \in \mathfrak{p}$, $s \in S$ such that $\iota(x) = \frac{x}{1} = \frac{a}{s}$. By definition, this means that there exists some $s' \in S$ such that $s'sx = s'a \in \mathfrak{p}$. Therefore either $s's \in \mathfrak{p}$ or $x \in \mathfrak{p}$, but since $s's \in S$ and S is disjoint from $\mathfrak{p}$, we must have $x \in \mathfrak{p}$. □

Corollary 7.5. *The maps ι^* and ι_* give mutually inverse bijections from the set of prime ideals of $S^{-1}R$ to the set of prime ideals of R which are disjoint from S.*

Therefore we may – and shall – view $\operatorname{Spec} S^{-1}R$ as a subset of $\operatorname{Spec} R$.

Exercise 7.6:
a) Show that the results of Proposition 7.4 extend to all *primary* ideals of R.[35]
b) Let I be *any* ideal of R. Show that

$$\iota^*\iota_*I = \{x \in R \mid \exists s \in S \text{ such that } sx \in I\}.$$

Comment: in class I remarked that there is no nice push-pull formula for an arbitrary ideal in a localization map. Whether this exercise contradicts that assertion depends upon how nice you find this formula to be! Try it out on the following:
c) Exhibit a map $\iota : R \to S^{-1}R$ and a (nonprimary) ideal I of R such that $\iota^*\iota_*I \supsetneq I$.

7.3. **The fibers of a morphism.**

Let $f : R \to S$ be a homomorphism of rings, and let $\mathfrak{p} \in \operatorname{Spec} R$. Consider the "fiber of $f^* : \operatorname{Spec} S \to \operatorname{Spec} R$ over $\mathfrak{p}$", i.e.,

$$f_{\mathfrak{p}} = (f^*)^{-1}(\mathfrak{p}) = \{\mathcal{P} \in \operatorname{Spec} S \mid f^*(\mathcal{P}) = \mathfrak{p}\}.$$

We claim that $f_{\mathfrak{p}}$ is canonically isomorphic to the spectrum of a certain ring. Namely, let $k(\mathfrak{p})$ be the fraction field of the domain $R/\mathfrak{p}$. Then we wish to identify $f_{\mathfrak{p}}$ with $\operatorname{Spec}(S \otimes_R k(\mathfrak{p}))$.

[35]Recall $\mathfrak{p}$ is primary if for $a, b \in R$ such that $ab \in \mathfrak{p}$, either $a \in \mathfrak{p}$ or $b^n \in \mathfrak{p}$ for some $n \in \mathbb{Z}^+$. We have not yet done much with this concept, and will not really address it squarely until the section on primary decomposition.

Let $\iota_1 : S \to S \otimes_R k(\mathfrak{p})$ and $\iota_2 : k(\mathfrak{p}) \to S \otimes_R k(\mathfrak{p})$ be the canonical maps. The tensor product of R-algebras fits into a commutative square (INSERT) and is indeed the categorical **pushout**: in other words, given any ring A and homomorphisms $\varphi_1 : A \to S$ $\varphi_2 : A \to k(\mathfrak{p})$ such that the composite homomorphisms $\iota_1 \circ \varphi_1 = \iota_2 \circ \varphi_2$ are equal, there exists a unique homomorphism $\Phi : A \to R$ such that $f \circ \Phi = \varphi_1$ and $q \circ \Phi = \varphi_2$, where $q : R \to R/\mathfrak{p}$ is the quotient map.

On the spectral side, all the arrows reverse, and the corresponding diagram is (INSERT), which expresses $\operatorname{Spec}(S \otimes_R k(\mathfrak{p}))$ as the fiber product of $\operatorname{Spec} S$ and $\operatorname{Spec} k(\mathfrak{p})$ over $\operatorname{Spec} R$.

Observe that the map $\iota_1 : S \to S \otimes_R k(\mathfrak{p})$ is the composite of the surjective map $q_1 : S \to S \otimes_R R/\mathfrak{p}$ with the map $\ell_2 : S \otimes_R R/\mathfrak{p} \to (S \otimes_R R/\mathfrak{p}) \otimes_{R/\mathfrak{p}} k(\mathfrak{p})$, the latter map being localization with respect to the multiplicatively closed subset $q_1(R \setminus \mathfrak{p})$. Both q_1^* and ℓ_2^* are injections, and therefore $\iota_1 * = q_1^* \circ \ell_2^*$ is injective. Similarly $\operatorname{Spec} k(\mathfrak{p}) \hookrightarrow \operatorname{Spec} R$ (this is just the special case of the above with $R = S$). It follows that the above diagram identifies $\operatorname{Spec} S \otimes_R k(\mathfrak{p})$ with the prime ideals $\mathcal{P}$ of $\operatorname{Spec} S$ such that $f^*\mathcal{P} = \mathfrak{p}$.

7.4. **Commutativity of localization and passage to a quotient.**

Lemma 7.6. *Let R be a ring, $S \subset R$ a multiplicatively closed subset, and I an ideal of A. Write $q : R \to R/I$ for the quotient map and put $\overline{S} := q(S)$. Then there is a canonical isomorphism*

$$S^{-1}R/IS^{-1}R \cong \overline{S}^{-1}(R/I).$$

Proof. Explicitly, we send $\frac{a}{s} \pmod{I}S^{-1}R$ to $\frac{\overline{a}}{\overline{s}}$, where $\overline{a} = a + I$, $\overline{s} = s + I$. It is straightforward to check that this an isomorphism. □

Remark: Matsumura makes the following nice comment: both sides satisfy the universal property for homomorphisms $f : R \to R'$ such that $f(S) \subset (R')^\times$ and $f(I) = 0$. Therefore they must be canonically isomorphic.

7.5. **Localization at a prime ideal.**

An extremely important example of a multiplicative subset of R is the complement $R \setminus \mathfrak{p}$ of a prime ideal $\mathfrak{p}$. As a matter of notation, we write $R_\mathfrak{p}$ for $(R \setminus \mathfrak{p})^{-1}R$.[36]

Proposition 7.7. *If $\mathfrak{p}$ is a prime ideal of R, then the localization $R_\mathfrak{p}$ is a local ring with unique maximal ideal $\mathfrak{p}R_\mathfrak{p}$.*

Proof. We know that the primes of the localized ring are precisely the pushforwards of the prime ideals of R which are disjoint from the muliplicatively closed set. Here $S = R \setminus \mathfrak{p}$, so being disjoint from S is equivalent to being contained in $\mathfrak{p}$. Thus the unique maximal such element is indeed $\mathfrak{p}R_\mathfrak{p}$. □

[36]This is inevitably a bit confusing at first, but our choice of notation for a loacalization is designed to make this less confusing. The other common notation for the localization, R_S, creates a notational nightmare. As a mnemonic, remember that we gain nothing by localizing at a subset S containing 0, since the corresponding localization is the trivial ring.

Remark: We will simply write $\mathfrak{p}$ for the maximal ideal $\mathfrak{p}R_{\mathfrak{p}}$ of $R_{\mathfrak{p}}$.

Proposition 7.7, simple though it is, is of inestimable importance. It shows that the effect of localization at a prime ideal on the lattice of ideals is dual to that of passage to the quotient: if we mod out by a prime $\mathfrak{p}$, we get a ring $R/\mathfrak{p}$ whose ideals are precisely the ideals of R containing $\mathfrak{p}$. However, if we localize at $R \setminus \mathfrak{p}$, we get a ring whose ideals are precisely the ideals of R contained in $\mathfrak{p}$. In particular, this construction motivates us to develop an especially detailed theory of local rings, by assuring us that such a theory could be put to good use in the general case.

7.6. **Localization of modules.** If S is any multiplicative subset and M is any R-module, we can also construct a localized R-module $S^{-1}M$. One the one hand, we can construct this exactly as we did $S^{-1}R$, by considering the appropriate equivalence relation on pairs $(m, s) \in M \times S$. On the other hand, we can just take the base extension $S^{-1}R \otimes M$. We are left with the task of showing that these two constructions are "the same".

Exercise 7.7: Formulate a universal mapping property for the localization morphism $M \to S^{-1}M$. Check that both of the above constructions satisfy this universal mapping property, and deduce that they are canonically isomorphic.

Exercise 7.8: a) Show that the kernel of $M \to S^{-1}M$ is the set of $m \in M$ such that $\operatorname{ann}(m) \cap S \neq \emptyset$.
b) Let R be a domain with fraction field K. Let M be an R-module. Show:

$$\operatorname{Ker}(M \to M \otimes K) = M[\text{tors}].$$

c) Use part b) to give a new proof of Proposition 3.8b).

Exercise 7.9: Let N be any $S^{-1}R$-module. Show that there exists an R-module M such that $N \cong S^{-1}R \otimes_R M$.

Generally speaking, thinking of $S^{-1}M$ as $S^{-1}R \otimes_R M$ is more convenient for proving results, because it allows us to employ the theory of tensor products of modules that we developed in §X.X above. For example:

Proposition 7.8. *For any ring R and multiplicatively closed subset S of R, $S^{-1}R$ is a flat R-module. Equivalently, if*

$$0 \to M' \to M \to M'' \to 0$$

is a short exact sequence of R-modules, then

$$0 \to S^{-1}M' \to S^{-1}M \to S^{-1}M'' \to 0$$

is a short exact sequence of R-modules (or equivalently, of $S^{-1}R$-modules).

Proof. Tensor products are always right exact, so we need only show $S^{-1}M' \hookrightarrow S^{-1}M$. Suppose not: then there exists $m' \in M'$ and $s \in S$ such that $\frac{m'}{s} = 0 \in M$. Thus there is $g \in S$ such that $gm' = 0$, but if so, then $\frac{m'}{s} = 0$ in M'.[37] □

[37]Note also that the exactness of a sequence of R-modules does not depend on the R-module structure but only on the underlying abelian group structure. Thus if we have a sequence of abelian groups which can be viewed as a sequence of R-modules and also as a sequence of R'-modules, then exactness as R-modules is equivalent to exactness as R'-modules.

Corollary 7.9. *Let N and P be submodules of an R-module M. Then:*
a) $S^{-1}(N+P) = S^{-1}N + S^{-1}P$.
b) $S^{-1}(N \cap P) = S^{-1}N \cap S^{-1}P$.
c) $S^{-1}(M/N) \cong_{S^{-1}R} S^{-1}M/S^{-1}N$.

Exercise 7.10: Prove Corollary 7.9.

Proposition 7.10. *Let M and N be R-modules and S a multiplicatively closed subset of R. Then the mapping*

$$\frac{m}{s} \otimes \frac{n}{t} \mapsto \frac{m \otimes n}{st}$$

induces an isomorphism of $S^{-1}(R)$-modules

$$S^{-1}M \otimes_{S^{-1}R} S^{-1}N \xrightarrow{\sim} S^{-1}(M \otimes_R N).$$

In particular, for any prime ideal $\mathfrak{p}$ of R, we have

$$M_{\mathfrak{p}} \otimes_{R_{\mathfrak{p}}} N_{\mathfrak{p}} \xrightarrow{\sim} (M \otimes_R N)_{\mathfrak{p}}.$$

Exercise 7.11: Prove Proposition 7.10.

Exercise 7.12: Let R be a ring, $S \subset R$ multiplicative, and M an R-module.
a) If M is finitely generated, then $S^{-1}M$ is a finitely generated $S^{-1}R$-module.
b) If M is finitely presented, then $S^{-1}M$ is a finitely presented $S^{-1}R$-module.[38]

7.7. **Local properties.**

We say that a property P of a ring R is **localizable** if whenever R satisfies property P, so does $R_{\mathfrak{p}}$ for every prime ideal $\mathfrak{p}$ of R. We say that a property P is **local-to-global** if whenever $R_{\mathfrak{p}}$ has property P for all prime ideals $\mathfrak{p}$ of R, then R has that property. Finally, we say a property is **local** if it is both localizable and local-to-global. There are similar definitions for properties of R-modules.

One of the most important themes in commutative algebra is the recognition of the importance of local properties for rings and modules.

Remark: Very often it is true that if P is a local property, then R has property P iff $R_{\mathfrak{m}}$ has property P for all maximal ideals $\mathfrak{m}$ of R. We will not introduce terminology for this, but watch for it in the upcoming results.

First of all, for an R-module, **being trivial** is a local property.

Proposition 7.11. *For an R-module M, TFAE:*
(i) $M = 0$.
(ii) $M_{\mathfrak{p}} = 0$ *for all primes* $\mathfrak{p}$ *of* R.
(iii) $M_{\mathfrak{m}} = 0$ *for all maximal ideals* $\mathfrak{m}$ *of* R.

Proof. Clearly (i) $\implies$ (ii) $\implies$ (iii), so asume that $M_{\mathfrak{m}} = 0$ for all maximal ideals $\mathfrak{m}$ of R. Suppose there exists $0 \neq x \in M$, and let I be the annihilator of x, so that I is a proper ideal of R and thus contained in some maximal ideal $\mathfrak{m}$. Then x is

[38]Actually both parts hold for any base change $R \to R'$! We record it in this form since it will be used later.

not killed by any element of the multiplicative subset $R \setminus \mathfrak{m}$ and therefore maps to a nonzero element of $M_{\mathfrak{m}}$: contradiction. □

Proposition 7.12. *Let $f : M \to N$ be an R-module homomorphism.*
a) TFAE:
(i) f is injective.
(ii) For all prime ideals $\mathfrak{p}$ of R, $f_{\mathfrak{p}} : M_{\mathfrak{p}} \to N_{\mathfrak{p}}$ is injective.
(iii) For all maximal ideals $\mathfrak{m}$ of R, $f_{\mathfrak{m}} : M_{\mathfrak{m}} \to N_{\mathfrak{m}}$ is injective.
b) Part a) holds with "injective" replaced everywhere by "surjective", and thus also if "injective" is replaced everywhere by "is an isomorphism."

Proof. a) (i) $\implies$ (ii) by the exactness of localization, and obviously (ii) $\implies$ (iii). Assume (iii), and let $M' = \mathrm{Ker}(f)$. Then $0 \to M' \to M \to N$ is exact, hence for all $\mathfrak{m}$ we have $0 \to M'_{\mathfrak{m}} \to M_{\mathfrak{m}} \to N_{\mathfrak{m}}$ is exact. So, by our assumption, $M'_{\mathfrak{m}} = 0$ for all maximal ideals $\mathfrak{m}$, and thus by Proposition 7.11 we have $M' = 0$. The proof of part b) is virtually identical and left to the reader. □

Warning: Note that Proposition 7.12 **does not say** the following: if M and N are R-modules such that $M_{\mathfrak{p}} \cong N_{\mathfrak{p}}$ as $R_{\mathfrak{p}}$ modules for all $\mathfrak{p} \in \operatorname{Spec} R$, then $M \cong N$. This is being asserted only when there is a map $f : M \to N$ inducing all the isomorphisms between localized modules.

Exercise 7.13: Exhibit finitely generated R-modules M and N which are "locally isomorphic" – i.e., $M_{\mathfrak{p}} \cong N_{\mathfrak{p}}$ for all $\mathfrak{p} \in \operatorname{Spec} R$ – but are not isomorphic.[39]

Corollary 7.13. *Let R be an integral domain with fraction field K. Then as $\mathfrak{m}$ ranges over all maximal ideals of R, $\bigcap_{\mathfrak{m}} R_{\mathfrak{m}} = R$.*

Proof. Consider the injection $f : R \hookrightarrow S := \bigcap_{\mathfrak{m}} R_{\mathfrak{m}}$. Let $\mathfrak{p}$ and $\mathfrak{q}$ be distinct maximal ideals. Then $R_{\mathfrak{q}} \otimes_R R_{\mathfrak{p}} = K$, so for any maximal ideal $\mathfrak{m}$, $S_{\mathfrak{m}} = R_{\mathfrak{m}}$ and the localized map $f_{\mathfrak{m}} : R_{\mathfrak{m}} \to R_{\mathfrak{m}}$ is an isomorphism. Therefore f itself is an isomorphism, i.e., surjective. □

We give an application in the theory of stably free modules.

Proposition 7.14. *A stably free module of rank one is free.*

Proof. The natural proof uses exterior products of modules, which we have unfortunately not defined in these notes. For the basics here see BOURBAKI or [Eis, Appendix A2]. Especially, all the properties of exterior powers that we use appear in [Eis, Prop. A2.2].

Now suppose that P is such that $P \oplus R^{n-1} \cong R^n$. Taking top exterior powers we get

$$R \cong \bigwedge^n R^n \cong \bigwedge^n (P \oplus R^{n-1}) \cong \bigoplus_{i+j=n} \bigwedge^i P \otimes \bigwedge^j R^{n-1}$$
$$\cong M \oplus \left(\bigwedge^2 M \otimes \bigwedge^{n-2} R^{n-1} \right) \oplus \dots.$$

For any prime ideal $\mathfrak{p}$ of M, $M_{\mathfrak{p}}$ is free of rank one over $R_{\mathfrak{p}}$. Thus $\bigwedge^i M_{\mathfrak{p}} = (\bigwedge^i M)_{\mathfrak{p}} = 0$ for all $i \geq 2$. By Proposition 7.11, $\bigwedge^i M = 0$ for all $i \geq 2$, so $R \cong M$. □

[39] In mantra form: "being isomorphic" is not a local property, but "being an isomorphism" is.

7.7.1. *Local nature of flatness.*

Proposition 7.15. *For an R-module M, TFAE:*
(i) M is flat.
(ii) For all prime ideals $\mathfrak{p}$ of R, $M_{\mathfrak{p}}$ is flat.
(iii) For all maximal ideals $\mathfrak{m}$ of R, $M_{\mathfrak{m}}$ is flat.

Proof. (i) $\implies$ (ii) is a special case of Proposition 7.8; (ii) $\implies$ (iii) is immediate. So assume (iii), and let $N \hookrightarrow P$ be any injective R-module homomorphism. Then, by exactness of localization, for all maximal ideals $\mathfrak{m}$ we have $N_{\mathfrak{m}} \hookrightarrow P_{\mathfrak{m}}$. Since $M_{\mathfrak{m}}$ is assumed to be flat, we have $(N \otimes_R M)_{\mathfrak{m}} = N_{\mathfrak{m}} \otimes_{R_{\mathfrak{m}}} M_{\mathfrak{m}} \hookrightarrow P_{\mathfrak{m}} \otimes_{R_{\mathfrak{m}}} M_{\mathfrak{m}} = (P \otimes_R M)_{\mathfrak{m}}$. Applying Proposition 7.12 we conclude that $N \otimes_R M \to P \otimes_R P$ is injective, and therefore M is flat over R. □

Corollary 7.16. *Let R be a ring, $S \subset R$ a multiplicative subset. If M is a flat R-module, then $S^{-1}M$ is a flat $S^{-1}R$-module.*

Proof. If M is flat, so is $M_{\mathfrak{p}}$ for each prime ideal $\mathfrak{p}$ of M, but since the primes of $S^{-1}R$ are a subset of the primes of R, this implies that $S^{-1}M$ is flat. □

When a property P of rings or modules is *not* local, it is often of interest to study also its "localized version": we say that an R-module M is **locally P** if for all prime ideals $\mathfrak{p}$ of R, $M_{\mathfrak{p}}$ has property $\mathfrak{p}$ (and similarly for rings).

7.7.2. *Absolute flatness revisited.*

Lemma 7.17. *Suppose an absolutely flat ring R is either local or a domain. Then R is a field.*

Proof. The idea is that an absolutely flat ring must have many idempotent ideals, whereas a local ring or a domain has no nontrivial idempotents. More precisely, suppose R is not a field, and let $x \in R$ be a nonzero, nonunit. Then $I = (x)$ is a proper ideal, and by Proposition X.X we would have $R \cong I \oplus J$, contradiction. □

Lemma 7.18. *Let R be a ring.*
a) If R is absolutely flat and $S \subset R$ is any multiplicative subset, then $S^{-1}R$ is absolutely flat.
b) R is absolutely flat iff for every maximal ideal $\mathfrak{m}$ of R, $R_{\mathfrak{m}}$ is a field.

Proof. a) By Exercise X.X, every $S^{-1}R$-module is of the form $S^{-1}R \otimes_R M$ for some R-module M. By hypothesis M is flat, so by Corollary 7.16, so is $S^{-1}M$.
b) If R is absolutely flat, and $\mathfrak{m}$ is a maximal ideal of R, then by part a) $R_{\mathfrak{m}}$ is absolutely flat. On the other hand it is a local ring, so by Lemma 7.17, $R_{\mathfrak{m}}$ is a field. Conversely, assume that each $R_{\mathfrak{m}}$ is a field, and let M be an R-module. Then for all $\mathfrak{m} \in \operatorname{MaxSpec} R$, $M_{\mathfrak{m}}$ is a flat $R_{\mathfrak{m}}$-module, so M is a flat R-module. □

Theorem 7.19. *For a ring R, the following are equivalent:*
(i) $R/\operatorname{nil} R$ is absolutely flat, i.e., every $R/\operatorname{nil} R$-module is flat.
(ii) Every prime ideal of R is maximal.

Proof. Since the prime ideals of R are the same as those of $R/\operatorname{nil} R$, it is equivalent to prove the following simpler assertion: if R is reduced, it is absolutely flat if and only if every prime ideal of R is maximal. Suppose R is absolutely flat and $\mathfrak{p} \in \operatorname{Spec} R$. Then $R/\mathfrak{p}$ is an absolutely flat domain, hence a field by Lemma 7.17,

hence $\mathfrak{p}$ is maximal. Let $\mathfrak{m}$ be a maximal ideal of R. Then $R_{\mathfrak{m}}$ is a reduced local ring, hence a field. By Lemma 7.18, R is absolutely flat. □

Of course it is natural to ask about whether freeness and projectivity are local properties. We devote the following section to an analysis of this question.

7.8. **Local characterization of finitely generated projective modules.**

7.8.1. *Z-local properties.*

Let us call a family of $\{f_i\}_{i \in I}$ of elements of R a **Z-family** if $\langle f_i \rangle = 1$. Clearly for every Z-family there is a finite subset $J \subset I$ such that $\{f_i\}_{i \in J}$ is also a Z-family. (Later on, this trivial observation will be dressed up in rather fancy attire: this gives the quasi-compactness of the Zariski topology on $\operatorname{Spec} R$.)

A property P of rings or modules will be said to be **Z-local** if it holds over R iff it holds over all R_{f_i} for some Z-family $\{f_i\}$ of R.

Proposition 7.20.
Let $u : M \to N$ be a homomorphism of R-modules, and let $\mathfrak{p} \in \operatorname{Spec} R$.
a) If N is finitely generated and $u_{\mathfrak{p}}$ is surjective, there exists $f \in R \setminus \mathfrak{p}$ such that $u_f : M_f \to N_f$ is surjective.
b) The surjectivity of u is a Z-local property.
c) If M is finitely generated, N is finitely presented and $u_{\mathfrak{p}}$ is an isomorphism, then there exists $f \in R \setminus \mathfrak{p}$ such that $u_f : M_f \to N_f$ is an isomorphism.
d) If M is finitely generated and N is finitely presented, then the bijectivity of u is a Z-local property.

Proof. Write out the exact sequence

$$0 \to \ker u \to M \stackrel{u}{\to} N \to \operatorname{coker} u \to 0.$$

By the flatness of localization, this sequence remains exact upon being tensored with R_f for any $f \in R$ or with $R_{\mathfrak{p}}$ for any $\mathfrak{p} \in R$. It follows that passage to the kernel and cokernel commutes with localization.
a) We're assuming $0 = \operatorname{coker}(u_{\mathfrak{p}}) = (\operatorname{coker} u)_{\mathfrak{p}}$, i.e., for each $x \in \operatorname{coker} u$ there exists $f_x \in R \setminus \mathfrak{p}$ such that $f_x x = 0$. Since $\operatorname{coker} u$ is a quotient of the finitely generated module N, it is finitely generated, say by $x_1, \ldots, x_n$. Then $f = f_{x_1} \cdots f_{x_n} \in R \setminus \mathfrak{p}$ is such that $f \operatorname{coker} u = 0$, so $0 = (\operatorname{coker} u)_f = \operatorname{coker}(u_f)$ and u_f is surjective.
b) It is clear that if u is surjective, then for any $f \in R$, u_f is surjective. Conversely, let $\{f_i\}_{i \in I}$ be a Z-family such that u_{f_i} is surjective for all i. Then for any $\mathfrak{p} \in \operatorname{Spec} R$ there exists $i \in I$ such that $f_i \in R \setminus \mathfrak{p}$, so that $u_{\mathfrak{p}}$ is a further localization of u_{f_i} and thus the surjectivity of u_{f_i} implies that of $u_{\mathfrak{p}}$. By Proposition 7.12, u is surjective.
c) By part a), there exists $f_1 \in R \setminus \mathfrak{p}$ such that $\operatorname{coker} u_{f_1} = 0$, and thus we have an exact sequence

$$0 \to (\ker u)_{f_1} \to M_{f_1} \to N_{f_1} \to 0.$$

Since N is finitely presented over R, N_{f_1} is finitely presented over R_{f_1} and thus $(\ker u)_{f_1}$ is finitely generated. Arguing as in part b), we get $f_2 \in R \setminus \mathfrak{p}$ such that $f_1 f_2 \ker u = 0$. Taking $f = f_1 f_2$ we get $u_f : M_f \stackrel{\sim}{\to} N_f$.
d) This is proved analogously to part b) and is left to the reader. □

Corollary 7.21. *For a finitely presented R-module M, TFAE:*
(i) There is a Z-family $\{f_i\}_{i\in I}$ of R such that for all $i \in I$, M_{f_i} is a free R_{f_i}-module.
(ii) For every prime ideal $\mathfrak{p}$ of R, $M_\mathfrak{p}$ is a free $R_\mathfrak{p}$-module.
(iii) For every maximal ideal $\mathfrak{m}$ of R, $M_\mathfrak{m}$ is a free $R_\mathfrak{m}$-module.

Proof. (i) $\implies$ (ii): For each prime ideal $\mathfrak{p}$ there exists at least one i such that $f_i \notin \mathfrak{p}$; equivalently, the multiplicative subset generated by f_i is contained in $R \setminus \mathfrak{p}$. Thus $M_\mathfrak{p} = M_{f_i} \otimes_{R_{f_i}} R_\mathfrak{p}$ and since M_{f_i} is free, so is $M_\mathfrak{p}$.
(ii) $\implies$ (i): It is enough to find for each prime ideal $\mathfrak{p}$ an element $f_\mathfrak{p} \in R \setminus \mathfrak{p}$ such that $M_{f_\mathfrak{p}}$ is free: for if so, then $\{f_\mathfrak{p}\}_{\mathfrak{p}\in \operatorname{Spec} R}$ is a Z-family. Choose $x_1, \ldots, x_n \in M$ whose images in $M_\mathfrak{p}$ give an $R_\mathfrak{p}$-basis, and define $u : R^n \to M$ via $e_i \mapsto x_i$. Then $u_\mathfrak{p}$ is an isomorphism, so by Proposition 7.20c) we may choose $f_\mathfrak{p} \in R \setminus \mathfrak{p}$ such that $u_{f_\mathfrak{p}}$ is an isomorphism and thus $M_{f_\mathfrak{p}}$ is free.
(ii) $\iff$ (iii): this follows from Proposition 7.12. □

Exercise 7.14: Let $R_1, \ldots, R_n$ be rings and for $1 \leq i \leq n$, M_i a finitely generated projective R_i-module. Show that $M = \prod_{i=1}^n M_i$ is a finitely generated projective $R = \prod_{i=1}^n R_i$-module.

We can now prove one of the major results of this text.

Theorem 7.22. *Let R be a ring and M an R-module. The following are equivalent:*
(i) M is finitely generated and projective.
(ii) M is finitely presented *and for all $\mathfrak{m} \in \operatorname{MaxSpec} R$, $M_\mathfrak{m}$ is a free $R_\mathfrak{m}$-module.*
(iii) For every maximal ideal $\mathfrak{m}$ of R, there exists $f \in R \setminus \mathfrak{m}$ such that M_f is a locally free R_f-module of finite rank.
(iv) There exists a finite Z-family $\{f_1, \ldots, f_n\}$ of R such that $\langle f_1, \ldots, f_n\rangle = R$ and for all i, M_{f_i} is a finitely generated free R_{f_i}-module.

Proof. (i) $\implies$ (ii): Let M be finitely generated and projective. There exists a finitely generated free module F and a surjection $q : F \to M$. Since M is projective, q splits and $\operatorname{Ker}(q)$ is not just a submodule of F but also a quotient and thus finitely generated. So M is finitely presented. Since projectivity is preserved by base change and any finitely generated projective module over a local ring is free (Theorem 3.16), for all maximal ideals $\mathfrak{m}$ of R, $M_\mathfrak{m}$ is free.
(ii) $\implies$ (iii): this follows immediately from Corollary 7.21.
(iii) $\implies$ (iv): For each $\mathfrak{m} \in \operatorname{MaxSpec} R$, choose $f_\mathfrak{m} \in R \setminus \mathfrak{m}$ such that $M_{f_\mathfrak{m}}$ is a finitely generated free $R_{f_\mathfrak{m}}$-module. Then $\{f_\mathfrak{m}\}_{\mathfrak{m}\in \operatorname{MaxSpec} R}$ is a Z-family of R, and as remarked above, every Z-family contains a finite subfamily.
(iv) $\implies$ (i): Put $S = \prod_{i=1}^n R_{f_i}$ and let $f : R \to S$ be the natural map.
Step 1: First note that

$$\ker f = \bigcap_{i=1}^n \ker(R \to R_{f_i}) = \bigcap_{i=1}^n \operatorname{ann}(f_i) = \operatorname{ann}\langle f_1, \ldots, f_n\rangle = \operatorname{ann} R = 0,$$

so f is injective, and thus S is an extension ring of R.
Step 2: We CLAIM $f : R \hookrightarrow S$ is a faithfully flat extension. Since localizations are flat and direct sums of flat algebras are flat, S/R is a flat extension. So by Theorem 3.101, it is enough to show that $f^* : \operatorname{Spec} S \to \operatorname{Spec} R$ is surjective. But $\operatorname{Spec} S = \coprod_{i=1}^n \operatorname{Spec} R_{f_i}$ and $f^*(\operatorname{Spec} R_{f_i})$ is the subset of $\mathfrak{p} \in \operatorname{Spec} R$ such that $f_i \notin \mathfrak{p}$. Since $\{f_1, \ldots, f_n\}$ forms a Z-family, no proper ideal can contain all the f_i's,

and therefore $\mathfrak{p}$ lies in at least one $f^*(\operatorname{Spec} R_{f_i})$.
Step 3: We have a faithfully flat ring extension $f : R \hookrightarrow S$ and an R-module M such that $M \otimes_R S = \prod_{i=1}^n M_{f_i}$ is finitely generated and projective as an $S = \prod_{i=1}^n R_{f_i}$-module (Exercise X.X). By Theorem 3.104, M is finitely generated and projective! □

Corollary 7.23. *Every finitely presented flat R-module is projective.*

Proof. Let M be a finitely presented, flat R-module. For each maximal ideal $\mathfrak{m}$ of R, $M_{\mathfrak{m}}$ is a finitely presented flat module over the local ring $R_{\mathfrak{m}}$, hence is free by Theorem 3.49. Therefore by criterion (iii) of Theorem 7.22, M is projective. □

Corollary 7.24. *Let M be finitely generated over the Noetherian ring R. TFAE:*
(i) M is projective.
(ii) M is locally free.
(iii) M is flat.

Exercise 7.15: Prove Corollary 7.24. Corollary 7.24 is the last word on finitely generated projective modules over Noetherian rings. In the non-Noetherian case, Corollary 7.23 leaves a little room for improvement: could it be true that every finitely *generated* flat module is projective? This is not true in general but it is true for some important classes of non-Noetherian rings, e.g. any connected ring. To see this we need to make a topological study of the **rank function** on a finitely generated projective module. This is taken up later on in §$X.X$.

Theorem 7.25. *For an R-module A, TFAE:*
(i) A is finitely generated projective.
(ii) For all R-modules B, the natural map

$$\Phi : A^\vee \otimes_R B \to \operatorname{Hom}_R(A, B)$$

induced by $(f, b) \mapsto (a \mapsto f(a)b)$ is an isomorphism.
(iii) The map $\Phi : A^\vee \otimes_R A \to \operatorname{Hom}_R(A, A)$ is an isomorphism.

Proof. (i) $\implies$ (ii): It is enough to show that for all $\mathfrak{p} \in \operatorname{Spec} R$, $\Phi_{\mathfrak{p}}$ is an isomorphism. Since A is finitely generated projective, it is finitely presented; moreover $R_{\mathfrak{p}}$ is a flat R-module, so by Theorem 3.96 we have a canonical isomorphism $\operatorname{Hom}_R(A, N) \otimes_R R_{\mathfrak{p}} = \operatorname{Hom}_{R_{\mathfrak{p}}}(A_{\mathfrak{p}}, N_{\mathfrak{p}})$. Also tensor products commute with base change, so it is enough to show

$$\Phi_{\mathfrak{p}} : A_{\mathfrak{p}}^\vee \otimes_{R_{\mathfrak{p}}} B_{\mathfrak{p}} \to \operatorname{Hom}_{R_{\mathfrak{p}}}(A_{\mathfrak{p}}, B_{\mathfrak{p}})$$

is an isomorphism. Since A is finitely generated projective, $A_{\mathfrak{p}}$ is finitely generated and free. We are thus essentially reduced to a familiar fact from linear algebra, namely the canonical isomorphism $V^\vee \otimes W \xrightarrow{\sim} \operatorname{Hom}(V, W)$ for vector spaces over a field, with V finite-dimensional. We leave the details to the reader as an exercise.
(ii) $\implies$ (iii): This is immediate.
(iii) $\implies$ (i): Let $\Phi^{-1}(1_A) = \sum_{i=1}^m f_i \otimes a_i$. Then we have that for all $a \in A$, $a = \sum_{i=1}^m f_i(a)a_i$. By the Dual Basis Lemma, A is finitely generated projective. □

7.8.2. *Infinitely generated locally free modules.*

Let M be an R-module which is not necessarily finitely generated. Since projectivity is preserved by base change and by Theorem X.X every projective module over a local ring is free, it follows that if M is projective it is locally free. What

about the converse?

It need not hold: for infinitely generated modules, being locally free can be a much weaker property. Consider:

Proposition 7.26. *For a ring R, the following are equivalent:*
(i) R is absolutely flat.
(ii) Every R-module is locally free.

Proof. (i) $\implies$ (ii): By Lemma 7.18, for $\mathfrak{m} \in \operatorname{MaxSpec} R$, $R_{\mathfrak{m}}$ is a field, so every $R_{\mathfrak{m}}$-module is free. By Theorem 7.19 every prime ideal of R is maximal, so every R-module is locally free.
(ii) $\implies$ (i): Applying Lemma 7.18 again, if R is *not* absolutely flat, there is $\mathfrak{m} \in \operatorname{MaxSpec} R$ such that $R_{\mathfrak{m}}$ is not a field, and thus there exists a nonfree $R_{\mathfrak{m}}$-module $M_{\mathfrak{m}}$. By Exercise X.X, there is an R-module M such that $M \otimes_R R_{\mathfrak{m}} \cong R_{\mathfrak{m}}$ and thus M is not locally free. □

As we have seen, there are plenty of rings which are absolutely flat but not absolutely projective. For instance an absolutely projective ring is Noetherian, so an infinite product of fields or an infinite Boolean ring will carry locally free, non-projective modules.

8. Noetherian rings

We have already encountered the notion of a Noetherian ring, i.e., a ring in which each ideal is finitely generated; or equivalently, a ring which satisfies the ascending chain condition (ACC) on ideals. Our results so far have given little clue as to the importance of this notion. But in fact, as Emmy Noether showed, consideration of rings satisfying (ACC) is a major unifying force in commutative algebra.

In this section we begin to see why this is the case. After giving an introductory examination of chain conditions on rings and modules, we are able to make the key definitions of *height* of a prime ideal and *dimension* of a ring, which we will slowly but surely work towards understanding throughout the rest of these notes. Indeed we begin by giving a reasonably complete analysis of the structure theory of Artinian rings, which, as we will show, really is our first order of business in attempting the systematic study of Noetherian rings, since according to the Akizuki-Hopkins theorem the Artinian rings are precisely the Noetherian rings of dimension zero. We are then able to state and prove three of the most important and useful theorems in the entire subject. Whereas the first theorem, the Hilbert basis theorem, gives us a large supply of Noetherian rings, the latter two theorems, Krull's intersection theorem and Krull's principal ideal theorem, are basic results about the structure theory of Noetherian rings.

8.1. **Chain conditions on partially ordered sets.**

Proposition 8.1. *For a partially ordered set $(S, \leq)$, the following are equivalent:*
*(i) S satisfies the **Ascending Chain Condition** (ACC): there is no infinite sequence $\{x_i\}_{n=1}^{\infty}$ of elements of S with $x_n < x_{n+1}$ for all $n \in \mathbb{Z}^+$.*
(ii) Every nonempty subset $T \subset S$ has a maximal element.
*A partially ordered set satisfying these equivalent conditions is called **Noetherian**.*

Proof. (i) $\implies$ (ii): Let T be a nonempty subset of S without a maximal element. Since T is nonempty, choose $x_1 \in T$. Since T has no maximal elements, choose $x_2 > x_1$. Since T has no maximal elements, choose $x_3 > x_2$. And so on: we get an infinite strictly ascending chain in S.
(ii) $\implies$ (i): Indeed, an infinite strictly ascending chain is a nonempty subset without a maximal element. □

Similarly, we say that a partially ordered set satisfies the **Descending Chain Condition** (DCC) –if there is no infinite sequence $\{y_j\}_{j=1}^{\infty}$ of elements of S such that $y_j > y_{j+1}$ for all $j \in \mathbb{Z}^+$. As above, this holds iff every nonempty subset of S has a minimal element, and a partially ordered set satisfying these equivalent conditions is called **Artinian**.

Every partially ordered set $(S, \leq)$ has an **order dual** $S^\vee$: the underlying set is S, and we put $x \leq_\vee y \iff y \leq x$. Clearly S is Noetherian (resp. Artinian) iff $S^\vee$ is Artinian (resp. Noetherian). Thus at this level of abstraction we really have one notion here, not two. Nevertheless in our applications to rings and modules the two conditions remain quite distinct.

Examples: If S is finite it satisfies both ACC and DCC. With the usual orderings, the positive integers $\mathbb{Z}^+$ satisfy DCC but not ACC, the negative integers $\mathbb{Z}^-$ (or equivalently, $\mathbb{Z}^+$ with the opposite ordering) satisfy ACC but not DCC, and the integers $\mathbb{Z}$ satisfy neither.

Exercise 8.1: Let S be a poset.
a) Show that S satisfies (ACC) (resp. (DCC)) iff there is no order embedding $\mathbb{Z}^+ \hookrightarrow S$ (resp. $\mathbb{Z}^- \hookrightarrow S$).
b) Suppose S is totally ordered. Show that S satisfies (DCC) iff it is well-ordered: i.e., every nonempty subset has a minimal element.

8.2. **Chain conditions on modules.**

Let R be a ring, and M a (left) R-module. It makes sense to speak of the (ACC) and (DCC) for R-submodules of M. Indeed, we will call M a **Noetherian module** if it satisfies (ACC) and an **Artinian module** if it satisfies (DCC).

Exercise 8.2: Show that an R-module M is Noetherian iff every R-submodule M' of M is finitely generated.

Example: As a $\mathbb{Z}$-module, the integers $\mathbb{Z}$ are Noetherian but not Artinian.

Example: As a $\mathbb{Z}$-module, the group of all p-power roots of unity in the complex numbers – in other words, $\lim_{n\to\infty} \mu_{p^n}$ – is Artinian but not Noetherian.

Every ring R is naturally an R-module, and the R-submodules of R are precisely the ideals. Thus it makes sense to say whether R is a Noetherian or Artinian R-module, and – thank goodness – this is visibly consistent with the previous terminology.

Exercise 8.3: Let $M' \subset M$ be R-modules, and $\varphi : M \to M/M'$ be the quotient

map. If N_1 and N_2 are submodules of M such that $N_1 \subset N_2$, $N_1 \cap M' = N_2 \cap M'$ and $\varphi(N_1) = \varphi(N_2)$, show that $N_1 = N_2$.

Theorem 8.2. *Let $0 \to M' \to M \to M'' \to 0$ be a short exact sequence of R-modules. Then M is Noetherian (resp. Artinian) iff both M' and M'' are Noetherian (resp. Artinian).*

Proof. We do the Noetherian case, leaving the similar Artinian case as an exercise for the reader. First, since an infinite ascending chain in a submodule or quotient module of M gives rise to an infinite ascending chain in M, if M is Noetherian, both M' and M'' are. Conversely, suppose $N_1 \subsetneq N_2 \subsetneq \dots$ is an infinite ascending chain of submodules of M. Consider the chain $(N_i + M')/M'$ in $M'' = M/M'$. By hypothesis, this chain eventually stabilizes, i.e., for sufficiently large i and j, $N_i + M' = N_j + M'$. Similarly, by intersecting with M' we get that for sufficiently large i and j $N_i \cap M' = N_j \cap M'$. Applying Exercise 8.3 we conclude $N_i = N_j$ for all sufficiently large i, j. □

A ring R is **Noetherian** if R is a Noetherian R-module. A ring R is **Artinian** if R is an Artinian R-module.

Exercise 8.4: Let R be a ring.
a) Show that R is Noetherian iff every finitely generated R-module is Noetherian.
b) Show that R is Artinian iff every finitely generated R-module is Artinian.
c) Exhibit a ring R which is Noetherian but not Artinian.
d) Can you find a ring R which is Artinian but not Noetherian?[40]

8.3. **Semisimple modules and rings.**

In this section we allow *not necessarily commutative rings* R. By a "module over R" we mean a *left* R-module unless otherwise indicated.

A module M is **simple** if it is nonzero and has no proper, nonzero submodules.

This definition is of course made in analogy to that of a *simple group*, namely a nontrivial group possessing no nontrivial proper normal subgroups. And indeed many of the results in this and subsequent sections were first proved in the context of groups. It is even possible to work in a single context that simultaneously generalizes the case of groups and modules (over a not necessarily commutative ring), the key concept being that of **groups with operators**. For more on this perspective we invite the reader to consult any sufficiently thick all-purpose graduate level algebra text, the gold standard here being [J1], [J2].

Exercise 8.5 (**Schur's Lemma**): Let M be a simple R-module. Show that $\mathrm{End}_R(M)$ is a division ring.

Theorem 8.3. *For an R-module M, TFAE:*
(i) M is a direct sum of simple submodules.
(ii) Every submodule of M is a direct summand.
(iii) M is a sum of simple submodules.
*A modules satisfying these equivalent conditions is called **semisimple**.*

[40] More on this later!

Proof. (i) $\implies$ (ii): Suppose $M = \bigoplus_{i \in I} S_i$, with each S_i a simple submodule. For each $J \subset I$, put $M_J = \bigoplus_{i \in J} S_i$. Now let N be an R-submodule of M. An easy Zorn's Lemma argument gives us a maximal subset $J \subset I$ such that $N \cap M_J = 0$. For $i \notin J$ we have $(M_J \oplus S_i) \cap N \neq 0$, so choose $0 \neq x = y + z$, $x \in N$, $y \in M_J$, $z \in S_i$. Then $z = x - y \in (M_j + N) \cap S_i$, and if $z = 0$, then $x = y \in N \cap M_j = 0$, contradiction. So $(M_J \oplus N) \cap S_i \neq 0$. Since S_i is simple, this forces $S_i \subset M_J \oplus N$. It follows that $M = M_J \oplus N$.
(ii) $\implies$ (i): First observe that the hypothesis on M necessarily passes to all submodules of M. Next we CLAIM that every nonzero submodule $C \subset M$ contains a simple module.

PROOF OF CLAIM: Choose $0 \neq c \in C$, and let D be a submodule of C which is maximal with respect to not containing c. By the observation of the previous paragraph, we may write $C = D \oplus E$. Then E is simple. Indeed, suppose not and let $0 \subsetneq F \subsetneq E$. Then $E = F \oplus G$ so $C = D \oplus F \oplus G$. If both $D \oplus F$ and $D \oplus G$ contained c, then $c \in (D \oplus F) \cap (D \oplus G) = D$, contradiction. So either $D \oplus F$ or $D \oplus G$ is a strictly larger submodule of C than D which does not contain c, contradiction. So E is simple, establishing our claim.

Now let $N \subset M$ be maximal with respect to being a direct sum of simple submodules, and write $M = N \oplus C$. If $C \neq 0$, then by the claim C contains a nonzero simple submodule, contradicting the maximality of N. Thus $C = 0$ and M is a direct sum of simple submodules.
(i) $\implies$ (iii) is immediate.
(iii) $\implies$ (i): as above, by Zorn's Lemma there exists a submodule N of M which is maximal with respect to being a direct sum of simple submodules. We must show $N = M$. If not, since M is assumed to be generated by its simple submodules, there exists a simple submodule $S \subset M$ which is not contained in N. But since S is simple, it follows that $S \cap N = 0$ and thus $N \oplus S$ is a strictly larger direct sum of simple submodules: contradiction. □

Corollary 8.4. *An R-module M has a unique maximal semisimple submodule, called the* ***socle of M*** *and written* $\operatorname{Soc} M$. *Thus M is semisimple iff $M = \operatorname{Soc} M$.*

Exercise 8.6: Prove Corollary 8.4.

Exercise 8.7: Let $N \in \mathbb{Z}^+$. Compute the socle of the $\mathbb{Z}$-module $\mathbb{Z}/N\mathbb{Z}$. Show in particular that $\mathbb{Z}/N\mathbb{Z}$ is semisimple iff N is squarefree.

A not necessarily commutative ring R is **left semisimple** if R is semisimple as a left R-module.

Theorem 8.5. *For a nonzero not necessarily commutative ring R, TFAE:*
(i) R is left semisimple.
(ii) Every left ideal of R is a direct summand.
(iii) Every left ideal of R is an injective module.
(iv) All left R-modules are semisimple.
(v) All short exact sequences of left R-modules split.
(vi) All left R-modules are projective.
(vii) All left R-modules are injective.

Proof. We will show (i) $\iff$ (ii), (iv) $\iff$ (v) $\iff$ (vi) $\iff$ (vii) and (ii) $\implies$ (vii) $\implies$ (iii) $\implies$ (ii), which suffices.

(i) $\implies$ (ii) follows immediately from Theorem 8.3.
(iv) $\iff$ (v) follows immediately from Theorem 8.3.
(v) $\iff$ (vi) and (v) $\iff$ (vii) are immediate from the definitions of projective and injective modules.
(ii) $\implies$ (vii): Let I be a left ideal of R and $f : I \to M$ an R-module map. By hypothesis, there exists J such that $I \oplus J = R$, so f extends to $F : R = I \oplus J \stackrel{\pi_1}{\to} I \to M$. By Baer's Criterion, M is injective.
(vii) $\implies$ (iii) is immediate.
(iii) $\implies$ (ii) is immediate from the definition of injective modules. □

Lemma 8.6. *Let R be a ring and $\{M_j\}_{j \in J}$ be an indexed family of nonzero R-modules. The following are equivalent:*
(i) I is finite and each M_j is finitely generated.
(ii) $M = \bigoplus_{j \in J} M_j$ is finitely generated.

Proof. (i) $\implies$ (ii) is left to the reader as an easy exercise.
(ii) $\implies$ (i): Each M_j is isomorphic to a quotient of M, so if M is finitely generated, so is M_j. Now let $X = \{x_1, \ldots, x_n\}$ be a finite generating set for M, and for each $1 \leq 1 \leq n$, let x_{ij} be the j-component of x_i, so $x_i = \sum_{j \in J} x_{ij}$. This sum is of course finite, and therefore the set $J' \subset J$ of indices j such that $x_{ij} \neq 0$ for some $1 \leq i \leq n$ is finite. It follows that $\langle X \rangle \subset \bigoplus_{j \in J'} M_j \subsetneq M$, contradiction. □

Lemma 8.7. *Let $R_1, \ldots, R_n$ be finitely many not necessarily commutative rings, and put $R = \prod_{i=1}^n R_i$. Then R is semisimple iff $R_i$is semisimple for all $1 \leq i \leq n$.*

Exercise 8.8: Prove Lemma 8.7.

We now quote the following basic result from noncommutative algebra.

Theorem 8.8. *(Wedderburn-Artin) For a ring R, TFAE:*
(i) R is semisimple as a left R-module (left semisimple).
(ii) R is semisimple as a right R-module (right semisimple).
(iii) There are $N, n_1, \ldots, n_N \in \mathbb{Z}^+$ and division rings $D_1, \ldots, D_N$ such that

$$R \cong \prod_{i=1}^N M_{n_i}(D_i).$$

Combining Theorems 8.5 and 8.8 gives us a tremendous amount of information. First of all, a ring is left semisimple iff it is right semisimple, so we may as well speak of **semisimple rings**. A ring is semisimple iff it is **absolutely projective** iff it is **absolutely injective**.

Coming back to the commutative case, the Wedderburn-Artin theorem tells us that the class of semisimple / absolutely projective / absolutely injective rings is extremely restricted.

Corollary 8.9. *A commutative ring is semisimple iff it is a finite product of fields.*

However it is significantly easier to give a proof of Wedderburn-Artin in the commutative case, so we will give a direct proof of Corollary 8.9

Proof. Step -1: Officially speaking the theorem holds for the zero ring because it is an empty product of fields. In any event, we may and shall assume henceforth that

our semisimple ring is nonzero.
Step 0: A field is a semisimple ring: e.g. every module over a field is free, hence projective. By Lemma 8.7, a finite direct product of fields is therefore semisimple.
Step 1: Let R be a semisimple ring, and let $R = \bigoplus_{i \in I} M_i$ be a direct sum decomposition into simple R-modules. R is a finitely generated R-module, by Lemma 8.6 I is finite, and we may identify it with $\{1, \ldots, n\}$ for some $n \in \mathbb{Z}^+$: $R = M_1 \oplus \ldots \oplus M_n$.
Step 2: We may uniquely write $1 = e_1 + \ldots + e_n$ with $e_i \in M_i$. Then for all $i \neq j$, $e_i e_j = 0$, and this together with the identity $1 \cdot 1 = 1$ implies that $e_i^2 = e_i$ for all i. As usual for idempotent decompositions, this expresses R as a direct product of the subrings $R_i = M_i = e_i R$. Moreover, since M_i is a simple R-module, R_i has no proper nonzero ideals, and thus it is a field, say k_i. □

Exercise 8.9: Exhibit an absolutely flat commutative ring which is not semisimple.

8.4. **Normal Series.**

If M is an R-module a **normal series** is a finite ascending chain of R-submodules $0 = M_0 \subsetneq M_1 \subsetneq \ldots \subsetneq M_n = M$. We say that n is the **length** of the series. (The terminology is borrowed from group theory, in which one wants a finite ascending chain of subgroups with each normal in the next. Of course there is no notion of "normal submodule", but we keep the group-theoretic terminology.)

There is an evident partial ordering on the set of normal series of a fixed R-module M: one normal series $\{M_i\}_{i=0}^n$ is less than another normal series $\{M_j'\}_{j=0}^{n'}$ if for all $1 \leq i \leq n$, M_i is equal to M_j' for some (necessarily unique) j. Rather than saying that $\{M_i\} \leq \{M_j'\}$, it is traditional to say that the larger series $\{M_j'\}$ **refines** the smaller series $\{M_i\}$.

Given any normal series $\{M_i\}$ we may form the associated **factor sequence** $M_1/M_0 = M_1, M_2/M_1, \ldots, M_n/M_{n-1} = M/M_{n-1}$. Two normal series $\{M_i\}_{i=0}^n, \{M_j'\}_{j=0}^{n'}$ are **equivalent** if $n = n'$ and there is a permutation σ of $\{1, \ldots, n\}$ such that for all $1 \leq i \leq n$, the factors M_i/M_{i-1} and $M'_{\sigma(i)}/M'_{\sigma(i)-1}$ are isomorphic. In other words, if we think of the factor sequence of a normal series as a **multiset** of isomorphism classes of modules, then two normal series are equivalent if the associated multisets of factors are equal.

Exercise 8.10: Show that refinement descends to a partial ordering on equivalence classes of normal series of a fixed R-module M.

The following theorem is the basic result in this area.

Theorem 8.10. *(Schreier Refinement) For any R-module M, the partially ordered set of equivalence classes of normal series of submodules of M is* directed*: that is, any two normal series admit equivalent refinements.*

Proof. For a proof in a context which simultaneously generalizes that of modules and groups, see e.g. [J2, p. 106]. □

For an R-module M, a **composition series** is a maximal element in the poset of normal series: that is, a composition series which admits no proper refinement.

Exercise 8.11: Show that a normal series $\{M_i\}_{i=0}^n$ for an R-module M is a composition series iff for all $1 \leq i \leq n$, the factor module M_i/M_{i-1} is simple.

Theorem 8.11. *(Jordan-Hölder) Let M be an R-module. Then any two composition series for M are* equivalent*: up to a permutation, their associated factor series are term-by-term isomorphic.*

Proof. This is an immediate consequence of Schreier Refinement: any two normal series admit equivalent refinements, but no composition series admits a proper refinement, so any two composition series must already be equivalent. □

Thus for a module M which admits a composition series, we may define the **length** $\ell(M)$ of M to be the length of any composition series. One also speaks of the **Jordan-Hölder factors of M** or the **composition factors of M**, i.e., the unique multiset of isomorphism classes of simple R-modules which must appear as the successive quotients of any composition series for M.

If a module does not admit a composition series, we say that it has infinite length.

And now a basic question: which R-modules admit a composition series?

Exercise 8.12: a) Show that any finite[41] module admits a composition series.
b) Show that if a module M admits a composition series, it is finitely generated.
c) Show that a $\mathbb{Z}$-module M admits a composition series iff it is finite.
d) Let k be a field. Show that a k-module admits a composition series iff it is finitely generated (i.e., iff it is finite-dimensional).

Exercise 8.13: An R-module M admits a composition series iff there exists $L \in \mathbb{Z}^+$ such that every normal series in M has length at most L.

Theorem 8.12. *For an R-module M, TFAE:*
(i) M is both Noetherian and Artinian.
(ii) M admits a composition series.

Proof. Assume (i). Since M satisfies (DCC), there must exist a minimal nonzero submodule, say M_1. If M_1 is a maximal proper submodule, we have a composition series. Otherwise among all proper R-submodules strictly containing M_1, by (DCC) we can choose a minimal one M_2. We continue in this way: since M also satisfies (ACC) the process must eventually terminate, yielding a composition series.

(ii) $\implies$ (i): This follows easily from Exercise 8.13. □

Exercise 8.14: Exercise 8.13 makes use of Schreier Refinement. Give a proof that (ii) $\implies$ (i) in Theorem 8.12 which is independent of Schreier Refinement. (Suggestion: try induction on the length of a composition series.)

Proposition 8.13. *Let $0 \to M' \to M \to M'' \to 0$ be a short exact sequence of R-modules. Then:*
a) M admits a composition series iff both M' and M'' admit composition series.
b) If M admits a composition series, then

$$\ell(M) = \ell(M') + \ell(M'').$$

[41] Recall that by a "finite module" we mean a module whose underlying set is finite!

Exercise 8.15: Prove Proposition 8.13.

Remark: Although it will not play a prominent role in our course, the length of an R-module M is an extremely important invariant, especially in algebraic geometry: it is is used, among other things, to keep track of intersection multiplicities and to quantitatively measure the degree of singularity of a point.

8.5. **The Krull-Schmidt Theorem.**

The material in this section follows [J2, §3.4] very closely. In particular, very exceptionally for us – but as in *loc. cit.* – in this section we work with left modules over a *possibly noncommutative ring* R. The reason: not only does the desired result carry over verbatim to the noncommutative case (this is not in itself a good enough reason, as the same holds for a positive proportion of the results in these notes) but the proof requires us to consider noncommutative rings!

A module M is **decomposable** if there are nonzero submodules $M_1, M_2 \subset M$ such that $M = M_1 \oplus M_2$; otherwise M is **indecomposable**.

Theorem 8.14. *(Krull-Schmidt) Let M be an R-module of finite length. Then:*
a) There are indecomposable submodules $M_1, \ldots, M_m$ such that $M = \bigoplus_{i=1}^m M_i$.
b) If there are indecomposable submodules $N_1, \ldots, N_n$ such that $M = \bigoplus_{i=1}^n N_i$, then $m = n$ and there exists a bijection σ of $\{1, \ldots, n\}$ such that for all i, $M_i \cong N_{\sigma(i)}$.

The *Proof* of Theorem 8.14a) is easy, and we give it now. If M is a finite length module and we write $M = M_1 \oplus M_2$ then $0 < \ell(M_1), \ell(M_2) < \ell(M)$. Thus an evident induction argument shows that any sequence of moves, each one of which splits a direct summand of M into two nontrivial direct subsummands of M, must terminate after finitely many steps, leaving us with a decomposition of M into a finite direct sum of indecomposable submodules. □

As one might suspect, the second part of Theorem 8.14 concerning the uniqueness of the indecomposable decomposition is more subtle. Indeed, before giving the proof we need some preparatory considerations on endomorphism rings of modules.

Proposition 8.15. *For an R-module M, TFAE:*
(i) M is decomposable.
(ii) The (possibly noncommutative, even if R is commutative) ring $\mathrm{End}_R(M) = \mathrm{Hom}_R(M, M)$ has a nontrivial idempotent, i.e., an element $e \neq 0, 1$ with $e^2 = e$.

Exercise 8.16: Prove Proposition 8.15.

A (not necessarily commutative) ring R is **local** if the set of nonunits $R \setminus R^\times$ forms a two-sided ideal of R.

Exercise 8.17: Let R be a local, not necessarily commutative ring.
a) Show that $R \neq 0$.
b) Show that R has no nontrivial idempotents.

An R-module M is **strongly indecomposable** if $\mathrm{End}_R(M)$ is local. Thus it follows from Proposition 8.15 and Exercise 8.17 that a strongly indecomposable

module is indecomposable.

Example: The $\mathbb{Z}$-module $\mathbb{Z}$ is indecomposable: any two nonzero submodules (a) and (b) have a nontrivial intersection (ab). On the other hand $\mathrm{End}_{\mathbb{Z}}(\mathbb{Z}) = \mathbb{Z}$ is not a local ring, so $\mathbb{Z}$ is not strongly indecomposable.

Thus "strongly indecomposable" is, in general, a stronger concept than merely "indecomposable". Notice though that the Krull-Schmidt theorem applies only to finite length modules – equivalently to modules which are both Noetherian and Artinian – and $\mathbb{Z}$ is not an Artinian $\mathbb{Z}$-module. In fact, it shall turn out that any finite length indecomposable module is strongly indecomposable, and this will be a major step towards the proof of the Krull-Schmidt Theorem.

But we are not quite ready to prove this either! First some Fitting theory.

For an R-module M and $f \in \mathrm{End}_R(M)$, we put

$$f^\infty(M) = \bigcap_{n=1}^{\infty} f^n(M).$$

The set $f^\infty(M)$ is the intersection of a descending chain

$$M \supset f(M) \supset f^2(M) \supset \ldots \supset f^n(M) \supset \ldots$$

of submodules of M, and is thus an f-stable submodule of M. The restriction of f to $f^\infty(M)$ is surjective. Moreover, if M is an Artinian module, there exists $s \in \mathbb{Z}^+$ such that $f^s(M) = f^{s+1}(M) = \ldots$.

Exercise 8.18: Find a commutative ring R, an R-module M and $f \in \mathrm{End}_R(M)$ such that for no $n \in \mathbb{Z}^+$ is the submodule $f^n(M)$ f-stable.

Similarly, for M and f as above, we put

$$f_{-\infty}(0) = \bigcup_{n=1}^{\infty} \ker f^n.$$

Here each $\ker f^n$ is an f-stable submodule of M on which f is *nilpotent*. The set $f_{-\infty}(0)$ is the union of an ascending chain of submodules

$$0 \subset \ker f \subset \ker f^2 \subset \ldots \subset \ker f^n \subset \ldots$$

of M and is thus an f-stable submodule of M on which f acts as a *nil* endomorphism: i.e., every element of M is killed by some power of f. Moreover, if M is a Noetherian module, there exists $t \in \mathbb{Z}^+$ such that $\ker f^t = \ker f^{t+1} = \ldots$ and thus f is a nilpotent endomorphism of $f_{-\infty}(0)$.

Exercise 8.19: Find a commutative ring R, an R-module M and $f \in \mathrm{End}_R(M)$ such that f is *not* a nilpotent endomorphism of $f_{-\infty}(0)$.

Theorem 8.16. *(Fitting's Lemma) Let M be a finite length module over the not necessarily commutative ring R, and let $f \in \mathrm{End}_R(M)$.*
a) There exists a ***Fitting Decomposition***

$$M = f^\infty(M) \oplus f^{-\infty}(0). \tag{17}$$

b) $f|_{f^\infty(M)}$ is an isomorphism and $f|_{f_{-\infty}(0)}$ is nilpotent.

Proof. Since M has finite length it is both Noetherian and Artinian. Thus there exists $r \in \mathbb{Z}^+$ such that

$$f^r(M) = f^{r+1}(M) = \ldots = f^\infty(M)$$

and

$$\ker f^r = \ker f^{r+1} = \ldots = f_{-\infty}(0).$$

Let $x \in f^\infty(M) \cap f_{-\infty}(0)$. Then there exists $y \in M$ such that $x = f^r(y)$; moreover $0 = f^r(x) = f^{2r}(y)$. But $f^{2r}(y) = 0$ implies $x = f^r(y) = 0$, so $f^\infty(M) \cap f_{-\infty}(0) = 0$.

Let $x \in M$. Then $f^r(x) \in f^r(M) = f^{2r}(M)$, so there exists $y \in M$ with $f^r(x) = f^{2r}(y)$ and thus $f^r(x - f^r(y)) = 0$. so

$$x = f^r(y) + (x - f^r(y)) \in f^\infty(M) + f^{-\infty}(0),$$

completing the proof of part a). As for part b), we saw above that the restriction of f to $f^\infty(M)$ is surjective. It must also be injective since every element of the kernel lies in $f^{-\infty}(0)$. Thus $f|_{f^\infty(M)}$ is an isomorphism. Finally, as observed above, since $f_{-\infty}(0) = \ker f^r$, $f|_{f_{-\infty}(0)}$ is nilpotent. □

Lemma 8.17. *Let x and y be nilpotent elements in a not necessarily commutative ring (which is not the zero ring). Then $x + y$ is* not *a unit of R.*

Proof. Assume to the contrary that $x + y = u \in R^\times$. Dividing through by u we reduce to showing that we cannot have two nilpotent elements $x, y \in R$ such that $x + y = 1$. But if x is nilpotent, the "infinite geometric series" $\sum_{n=0}^\infty 1 + x + \ldots + x^n + \ldots$ is in fact finite, hence perfectly legal in our abstract algebraic context, and it is immediate to check that the familiar calculus identity

$$(1 - x)(\sum_{n=0}^\infty x^n) = 1$$

holds here. Thus $y = 1 - x$ is both a unit of R and a nilpotent element, contradiction. □

Corollary 8.18. *Let M be a finite length indecomposable R-module. Then every $f \in \mathrm{End}_R(M)$ is either an automorphism or nilpotent. Moreover M is is strongly indecomposable.*

Proof. Since M is indecomposable, Fitting's Lemma implies that for $f \in \mathrm{End}_R(M)$ we must have either $M = f^\infty(M)$ – in which case f is an automorphism – or $M = f^{-\infty}(0)$ – in which case f is nilpotent. We must show that $I = \mathrm{End}_R(M) \setminus \mathrm{End}_R(M)^\times$ is a two-sided ideal of $\mathrm{End}_R(M)$. Note that I is precisely the set of endomorphisms of M which are not automorphisms, hence every element of I is nilpotent. By Lemma 8.17, I is a subgroup of $(R, +)$. Moreover, for $f \in I$, $g \in \mathrm{End}_R(M)$, since f is neither injective nor surjective, gf is not injective and fg is not surjective, so neither is an automorphism and both lie in I. □

Lemma 8.19. *Let M be a nonzero R-module and N an indecomposable R-module. Suppose we have homomorphisms $f : M \to N$, $g : N \to M$ such that gf is an automorphism of M. Then both f and g are isomorphisms.*

Proof. Let $h = (gf)^{-1}$, $l = hg : N \to M$ and $e = fl : N \to N$. Then $lf = hgf = 1_M$ and $e^2 = flfl = f1_M l = fl = e$. Since M is indecomposable, either $e = 1$ or $e = 0$, and the latter implies $1_M = 1_M^2 = lflf = lef = 0$, i.e., $M = 0$. So $fl = e = 1_N$, so f is an isomorphism and thus so too is $(f(gf)^{-1})^{-1} = g$. □

Theorem 8.20. *Let $M \cong N$ be isomorphic modules, and let $M = \bigoplus_{i=1}^m M_i$ and $N = \bigoplus_{i=1}^n N_i'$ with each M_i strongly indecomposable and each N_i indecomposable. Then $m = n$ and there is a bijection σ of $\{1, \dots, m\}$ such that for all i, $M_i \cong N_{\sigma(i)}$.*

Proof. By induction on m: $m = 1$ is clear. Suppose the result holds for all direct sums of fewer than m strongly indecomposable submodules.
Step 1: Let $e_1, \dots, e_m \in \mathrm{End}_R(M)$ and $f_1, \dots, f_n \in \mathrm{End}_R(N)$ be the idempotent elements corresponding to the given direct sum decompositions (i.e., projection onto the corresponding factor). Let $g : M \xrightarrow{\sim} N$, and put

$$h_j := f_j g e_1 \in \mathrm{Hom}_R(M, N),\ k_j = e_1 g^{-1} f_j \in \mathrm{Hom}_R(N, M),\ 1 \le j \le n.$$

Then

$$\sum_{j=1}^n k_j h_j = \sum_j e_1 g^{-1} f_j g e_1 = e_1 g^{-1} \sum_j f_j g e_1 = e_1 g^{-1} 1_N g e_1 = e_1.$$

The restrictions of e_1 and $k_j h_j$ to M_1 stabilize M_1 so may be regarded as endomorphisms of M_1, say e_1' and $(k_j h_j)'$, and we have

$$\sum_{j=1}^n (k_j h_j)' = e_1' = 1_{M_1}.$$

By assumption $\mathrm{End}_R M_1$ is local, so for at least one j, $(k_j h_j)'$ is a unit, i.e., an automorphism of M_1. By reordering the N_j's we may assume that $j = 1$, so $(k_1 h_1)' \in \mathrm{Aut}_R M_1$. We may regard the restriction h_1' of h_1 to M_1 as a homomorphism from M_1 to N_1 and similarly the restriction k_1' of k_1 to N_1 as a homomorphism from N_1 to M_1, and then $k_1' h_1' = (k_1 h_1)'$ is an automorphism. By Lemma 8.19, $h_1' = (f_1 g e_1') : M_1 \xrightarrow{\sim} N_1$ and $k_1' = (e_1 g^{-1} f_1)' : N_1 \xrightarrow{\sim} M_1$.
Step 2: We claim that

$$M = g^{-1}(N_1) \oplus \bigoplus_{i=2}^m M_i. \tag{18}$$

To see this, let $x \in g^{-1}N_1 \cap (\bigoplus_{i=2}^m M_i)$, so $x = g^{-1}y$ for some $y \in N_1$. Because $x \in \bigoplus_{i=2}^m M_i$, $e_1 x = 0$. Thus

$$0 = e_1 x = e_1 g^{-1} y = e_1 g^{-1} f_1 y = k_1 y = k_1' y.$$

Since k_1' is an isomorphism, $y = 0$ and thus $x = 0$, so the sum in (18) is direct. Now put $M' = g^{-1}(N_1) \oplus \bigoplus_{i=2}^m M_i$, so we wish to show $M' = M$. Let $x \in g^{-1}N_1$. Then $x, e_2 x, \dots, e_m x \in M'$, so $e_1 x = (1 - e_2 - \dots - e_m)x \in M'$. So

$$M' \supset e_1 g^{-1} N_1 = e_1 g^{-1} f_1 N_1 = k_1 N_1 = k_1' N_1 = M_1$$

and thus $M' \supset \bigoplus_{i=1}^m M_i = M$.
Step 3: The isomorphism $g : M \xrightarrow{\sim} N$ carries $g^{-1}N_1$ onto N_1 hence induces an isomorphism $\frac{M}{g^{-1}N_1} \xrightarrow{sim} N/N_1$. Using Step 2, we have

$$\bigoplus_{j=2}^n N_i = \frac{N}{N_1} \cong \frac{M}{g^{-1}N_1} \cong \bigoplus_{i=2}^m M_i.$$

We are done by induction. □

Exercise 8.20: Please confirm that we have proved the Krull-Schmidt Theorem!

Exercise 8.21: Let M and N be R-modules such that $M \times M \cong N \times N$.
a) If M and N are both of finite length, show that $M \cong N$.
b) Must we have $M \cong N$ in general?

Remark: Part b) is far from easy! If you give up, see [Cor64].

Exercise 8.22: a) Let R be a PID and M an R-module. a) Show that M has finite length iff it is a finitely generated torsion module.
b) Show that a finitely generated torsion module is indecomposable iff it is isomorphic to $R/(p^a)$ for some prime element p of R and some $a \in \mathbb{Z}^+$.
c) Did you use the structure theorem for finitely generated modules over a PID to prove parts a) and b)? If so, try to prove these results without it.
d) Take as given parts a) and b) of this exercise, and use the Krull-Schmidt Theorem to deduce the structure theorem for finitely generated modules over a PID.

Remark: Later we *will* use these ideas to give an independent proof of the structure theorem for finitely generated modules over a PID, using one extra idea: reduction to the case of a *local PID*, in which case there is only one nonzero prime ideal and the module theory becomes especially simple.

8.6. **Some important terminology.**

All we aspire to do in this section is to introduce some terminology, but it is so important that we have isolated it for future reference.

Let R be a ring and $\mathfrak{p}$ a prime ideal of R. The **height** of $\mathfrak{p}$ is the supremum of all lengths of finite chains of prime ideals of the form $\mathfrak{p}_0 \subsetneq \mathfrak{p}_1 \subsetneq \ldots \subsetneq \mathfrak{p}_n = \mathfrak{p}$ (the length of the indicated chain being n; i.e., it is the number of $\subsetneq$'s appearing, which is one less than the number of elements). Thus the height is either a non-negative integer or ∞; the latter transpires iff there exist arbitrarily long finite chains of prime ideals descending from $\mathfrak{p}$ (and of course, this need not imply the existence of an infinite chain of prime ideals descending from $\mathfrak{p}$).

A prime ideal of height 0 is called a **minimal prime**. In an integral domain R, the unique minimal prime is (0), so the concept is of interest only for rings which are not domains. If I is a proper ideal of R, we also speak of a **minimal prime over** I, which means a prime $\mathfrak{p} \supset I$ such that there is no prime ideal $\mathfrak{q}$ with $I \subsetneq \mathfrak{q} \subsetneq \mathfrak{p}$. Note that $\mathfrak{p}$ is a minimal prime over I iff $\mathfrak{p}$ is a minimal prime in the quotient ring R/I. This remark simultaneously explains the terminology "minimal over" and gives a hint why it is useful to study minimal prime ideals even if one is ultimately most interested in integral domains.

The **dimension** of a ring R is the supremum of all the heights of its prime ideals. The full proper name here is **Krull dimension** of R, which is of course useful when one has other notions of dimension at hand. Such things certainly do exist but will not be considered here. Moreover, as will shortly become apparent, the need to include Krull's name here so as to ensure that he gets proper recognition

for his seminal work in this area is less than pressing. Therefore we use the full name "Krull dimension" only rarely as a sort of rhetorical flourish.

One also often speaks of the **codimension** of a prime ideal $\mathfrak{p}$ of R, which is the dimension of R minus the height of $\mathfrak{p}$. This is especially natural in applications to algebraic geometry, of which the present notes allude to only in passing. Note that this is *not* necessarily equal to the Krull dimension of $R/\mathfrak{p}$ – or what is the same as that, the maximal length of a finite chain of prime ideals ascending from $\mathfrak{p}$ – although in reasonable applications, and especially in geometry, one is certainly entitled to hope (and often, to prove) that this is the case.

Remark: All of these definitions would make perfect sense for arbitrary partially ordered sets and their elements, but the terminology is not completely consistent with order theory. Namely, the height of an element in an arbitrary poset *is* defined as the supremum of lengths of chains descending from that element, but the order theorists would cringe to hear the supremum of all heights of elements called the "dimension" of the poset. They would call that quantity the height of the poset, and would reserve dimension for any of several more interesting invariants. (Roughly, the idea is that a chain of any finite length is one-dimensional, whereas a product of d chains should have dimension d.)

8.7. **Introducing Noetherian rings.**

The following is arguably the most important single definition in all of ring theory.

A ring R is said to be **Noetherian** if the poset $\mathcal{I}(R)$ of all ideals of R satisfies the ascending chain condition.

Exercise 8.23: **FIX ME!**.

Theorem 8.21. *A finitely generated module over a Noetherian ring is Noetherian.*

Proof. If M is a finitely generated module over R, then we may represent it as R^n/K for some submodule K of R^n. An immediate corollary of the preceding theorem is that finite direct sums of Noetherian modules are Noetherian, and by assumption R itself is a Noetherian R-module, hence so is R^n and hence so is the quotient $R^n/K = M$. □

Thus so long as we restrict to Noetherian rings, submodules of finitely generated modules remain finitely generated. This is extremely useful even in the case of $R = \mathbb{Z}$: a subgroup of a finitely generated abelian group remains finitely generated. Needless(?) to say, this does not hold for all nonabelian groups, e.g. not for a finitely generated free group of rank greater than 1.

Theorem 8.22. *(Characterization of Noetherian rings) For a ring R, TFAE:*
(i) Every nonempty set of ideals of R has a maximal element.
(ii) There are no infinite ascending chains

$$I_1 \subsetneq I_2 \subsetneq \ldots \subsetneq I_n \subsetneq \ldots$$

of ideals of R.
(iii) Every ideal of R is finitely generated.
(iv) Every prime ideal of R is finitely generated.

Proof. (i) $\iff$ (ii) is a special case of Proposition 8.1.
(ii) $\iff$ (iii) is a special case of Exercise 8.2.
(iii) $\iff$ (iv) is Cohen's Theorem (Theorem 4.26). □

Exercise 8.24: Suppose a ring R satisfies the ascending chain condition on prime ideals. Must R be Noetherian?

Proposition 8.23. *Let R be a Noetherian ring.*
a) If I is any ideal of R, the quotient R/I is Noetherian.
b) If $S \subset R$ is any multiplicative subset, the localization $S^{-1}R$ is Noetherian.

Proof. Any ideal of R/I is of the form J/I for some ideal $J \supset I$ of R. By assumption J is finitely generated, hence J/I is finitely generated, so R/I is Noetherian. A similar argument holds for the localization; details are left to the reader. □

Exercise 8.25: Let k be a field, let S be an infinite set, and put $R = \prod_{s \in S} k$, i.e., the infinite product of $\#S$ copies of k. Show that R is not Noetherian, but the localization $R_{\mathfrak{p}}$ at each prime ideal is Noetherian.

Thus Noetherianity is a localizable property but not a local property.

8.8. **Theorems of Eakin-Nagata, Formanek and Jothilingam.**

In 1968, P.M. Eakin, Jr. [Ea68] and M. Nagata [Nag68] independently showed that if a ring R admits an extension ring S which is Noetherian and finitely generated as an R-module, then R is Noetherian.

Several years later, E. Formanek [For73] gave a stronger result. His improvement is a nice instance of the philosophy of "modulization": where possible one should replace theorems about rings with theorems about modules over rings. He writes: "The object of this paper is to present a simple and elementary proof of the Eakin-Nagata theorem which generalizes the original version in a new direction. The proof is essentially a contraction of Eakin's proof as presented by Kaplansky in [K, Exc. 14-15, p. 54] based on the observation that much of the proof disappears if one is not 'handicapped' by the hypothesis that T is a ring."

More recently, P. Jothilingam [Jo00] gave a result which simultaneously generalizes Formanek's Theorem and Cohen's Theorem that a ring in which all prime ideals are finitely generated is Noetherian. Finally(?), several years ago A. Naghipour [Nag05] found a significantly shorter, simpler proof of Jothilingam's Theorem, which we will present here. All in all, this provides a nice case study of how even very basic results get improved and simplified as time passes.

Having told the story in correct chronological order, we now reverse it: we will prove Jothilingam's Theorem and swiftly deduce the earlier results as corollaries. First a couple of easy preliminaries.

Lemma 8.24 (Kaplansky)**.** *For a ring R, the following are equivalent:*
(i) R is Noetherian.
(ii) R admits a faithful *Noetherian module.*

Proof. (i) $\implies$ (ii): If R is Noetherian, then R is a faithful Noetherian R-module.
(ii) $\implies$ (i): Let M be a faithful Noetherian R-module. In particular M is finitely generated, say by $x_1, \ldots, x_n$. Let $\varphi : R \to M^n$ by $r \mapsto (rx_1, \ldots, rx_n)$. Since M is Noetherian, so is M^n, and since M is faithful, φ is injective, and thus R is isomorphic to a submodule of a Noetherian module, hence Noetherian. □

Exercise 8.26:
a) Show that any ring R admits a Noetherian module.
b) Show that if M is a Noetherian R-module, $R/\operatorname{ann} M$ is Noetherian.

Let M be an R-module. An R-submodule of M is **extended** if it is of the form IM for some ideal I of R. This is a generalization of a previous use of the term: if $\iota : R \to T$ is a map of rings, then the *extended ideals* of T are those of the form $\iota_* I = IT$ for an ideal I of R.

Proposition 8.25. *For a finitely generated R-module M, let $\mathcal{E}_M$ be the family of extended submodules of M, partially ordered under inclusion. TFAE:*
(i) $\mathcal{E}_M$ is Noetherian: i.e., extended submodules satisfy (ACC).
(ii) Every extended submodule of M is finitely generated.

Proof. $\neg$ (ii) $\implies$ $\neg$ (i): Let I be an ideal of R such that IM is not finitely generated. Let $a_1 \in I$. Then, since M is finitely generated, $a_1 M$ is a finitely generated submodule of IM, hence proper: there exists $a_2 \in I$ such that $a_1 M \subsetneq \langle a_1, a_2 \rangle M$. Again, $\langle a_1, a_2 \rangle M$ is finitely generated, so is proper in IM. Continuing in this way we get a sequence $\{a_n\}_{n=1}^{\infty}$ in I such that

$$a_1 M \subsetneq \langle a_1, a_2 \rangle M \subsetneq \ldots \subsetneq \langle a_1, \ldots, a_n \rangle M \subsetneq \ldots,$$

so $\mathcal{E}_M$ is not Noetherian.
(ii) $\implies$ (i): Let $I_1 M \subseteq I_2 M \subseteq \ldots \subseteq I_n M \subseteq \ldots$ be an ascending chain in $\mathcal{E}_M$. Let $N = \sum_n I_n M$ and $I = \sum_n I_n$, so $N = IM \in \mathcal{E}_M$. By assumption, N is finite generated, so there is $n \in \mathbb{Z}^+$ with $N = I_1 M + \ldots + I_n M$. Since $I_k M \subset I_{k+1} M$ for all k, $N = I_n M$ and thus $I_n M = I_{n+k} M$ for $k \in \mathbb{N}$: the chain stabilizes at n. $\square$

Theorem 8.26 (Jothilingam)**.** *For a finitely generated R-module M, TFAE:*
(i) M is Noetherian.
(ii) For every prime ideal $\mathfrak{p}$ of R, the submodule $\mathfrak{p}M$ is finitely generated.

Proof. We follow [Nag05].
(i) $\implies$ (ii): If M is Noetherian, then every submodule of M is finitely generated.
$\neg$ (i) $\implies$ $\neg$ (ii): Suppose M is not Noetherian: we will find a prime ideal $\mathfrak{p}$ of R such that $\mathfrak{p}M$ is infinitely generated.
Step 0: Since the union of a chain of infinitely generated submodules of M is an infinitely generated submodule of M, by Zorn's Lemma there is a submodule $N \subset M$ maximal with respect to being infinitely generated.
Step 1: Let $\mathfrak{p} = \operatorname{ann}(M/N) = \{x \in R \mid xM \subset N\}$. We will show that $\mathfrak{p}$ is a prime ideal: indeed, seeking a contradiction suppose there are $a, b \in R \setminus \mathfrak{p}$ such that $ab \in \mathfrak{p}$. Then $N + aM, B + bM \supsetneq N$ so are both finitely generated: write $N + aM = \langle n_1 + am_1, \ldots, n_\ell + am_\ell \rangle$ with $n_i \in N$, $m_i \in M$. Put

$$L = \{m \in M : am \in N\};$$

then L is an R-submodule of M containing N and bM and hence also $N + bM \supsetneq N$, so L is finitely generated. We CLAIM

$$N = \sum_{i=1}^{\ell} Rn_i + aL.$$

If so, then N is finitely generated, a contradiction, and thus $\mathfrak{p}$ is prime. Since $abM \subset N$, we have $\sum_{i=1}^{\ell} Rn_i + aL \subset N$. Conversely, let $y \in N$. Since $y \in N + aM$,

there are $b_1, \ldots, b_\ell \in R$ such that

$$y = \sum_{i=1}^{\ell} b_i(n_i + am_i) = \sum_{i=1}^{\ell} b_i n_i + a \sum_{i=1}^{\ell} b_i m_i.$$

Thus

$$a \sum_{i=1}^{\ell} b_i m_i = y - \sum_{i=1}^{\ell} b_i n_i \in N,$$

so $\sum_{i=1}^{\ell} b_i m_i \in L$ and $y \in \sum_{i=1}^{\ell} Rn_i + aL$.
Step 2: For $x \in M$, write $\overline{x}$ for the canonical image of x in M/N. Now we use that M is finitely generated: write $M = \langle x_1, \ldots, x_n \rangle_R$, so $M/N = \langle \overline{x_1}, \ldots, \overline{x_n} \rangle_R$, so $\mathfrak{p} = \bigcap_{i=1}^{n} \operatorname{ann} R\overline{x_i}$. Because $\mathfrak{p}$ is prime, we must have $\mathfrak{p} = \operatorname{ann} R\overline{x_j}$ for some j. Since $N + Rx_i \supsetneq N$, $N + Rx_i$ is finitely generated, say by $y_1 + r_1 x_j, \ldots, y_k + r_k x_j$, with $y_i \in N$, $r_i \in R$. Arguing as in Step 1 we get

$$N = \sum_{i=1}^{k} Ry_i + \mathfrak{p}x_j.$$

Since $\mathfrak{p}M \subset N$, we have

$$N = \sum_{i=1}^{k} Ry_i + \mathfrak{p}x_j \subset \sum_{i=1}^{k} Ry_i + \mathfrak{p}M \subset \sum_{i=1}^{k} Ry_i + N \subset N,$$

and thus

$$N = \sum_{i=1}^{k} Ry_i + \mathfrak{p}M. \tag{19}$$

Since N is infinitely generated, (19) implies $\mathfrak{p}M$ is infinitely generated. □

Corollary 8.27. *(Formanek's Theorem) Let R be a ring, and let $M = \langle a_1, \ldots, a_n \rangle$ be a faithful finitely generated R-module. Suppose M satisfies (ACC) on "extended submodules" – i.e., submodules of the form IM for I an ideal of R. Then M is Noetherian, hence so is R.*

Proof. By Proposition 8.25, all extended submodules are finitely generated, hence *a fortiori* all submodules of the form $\mathfrak{p}M$ for $\mathfrak{p} \in \operatorname{Spec} R$ are finitely generated. By Theorem 8.26, M is Noetherian, and then by Lemma 8.24, R is Noetherian. □

Corollary 8.28. *(Eakin-Nagata Theorem) Let $R \subset S$ be an ring extension, with S finitely generated as an R-module. Then R is Noetherian iff S is Noetherian.*

Proof. $\implies$ If R is Noetherian, then S is a finitely generated module over a Noetherian ring so S is a Noetherian R-module. That is, (ACC) holds on R-submodules of S, hence *a fortiori* it holds on S-submodules of S.
$\impliedby$ Apply Formanek's Theorem with $M = S$. □

Exercise 8.28: Investigate the possibility of proving Jothilingam's Theorem using the Prime Ideal Principle of §4.5.

8.9. **The Bass-Papp Theorem.**

We now present a beautiful characterization of Noetherian rings in terms of properties of injective modules, due independently to Z. Papp [Pa59] and H. Bass [Bas59].

Theorem 8.29. *(Bass-Papp Theorem) For a ring R, TFAE:*
(i) A direct limit of injective modules is injective.
(ii) A direct sum of injective modules is injective.
(iii) A countable direct sum of injective modules is injective.
(iv) R is Noetherian.

Proof.
(i) $\implies$ (ii): A direct sum is a kind of direct limit.
(ii) $\implies$ (iii) is immediate.
(iii) $\implies$ (iv): Let $I_1 \subset I_2 \subset \ldots \subset I_n \subset \ldots$ be an infinite ascending chain of ideals of R, and let $I = \bigcup_n I_n$. We define

$$E = \bigoplus_{n=1}^{\infty} E(R/I_n).$$

For $n \in \mathbb{Z}^+$, let $f_n : I \to E(R/I_n)$ be the composite map $I \to R \to R/I_n \to E(R/I_n)$. There is then a unique map $\prod f : I \to \prod_{n=1}^{\infty} E(R/I_n)$. But indeed, for each fixed $x \in I$, x lies in I_n for sufficiently large n and thus $f_n(x) = 0$. It follows that $\prod f$ actually lands in the direct sum, and we have thus defined a map

$$f : I \to E.$$

By hypothesis, E is a countable direct sum of injective modules and therefore injective, so f extends to an R-module map with domain all of R and is thus of the form $f(x) = xf(1) = xe$ for some fixed $e \in E$. Let N be sufficiently large so that for $n \geq N$, the nth component e_n of e is zero. Then for all $x \in I$,

$$0 = xe_n = f_n(x) = x + I_n \in R/I_n,$$

and thus $x \in I_n$. That is, for all $n \geq N$, $I_n = I$.
(iv) $\implies$ (i): let $\{E_\alpha\}$ be a directed system of injective modules with direct limit E. For $\alpha \leq \beta$ we denote the transition map from E_α to E_β by $\iota_{\alpha\beta}$ and the natural map from E_α to E by ι_α. We will show E is injective by Baer's Criterion (Theorem 3.20), so let I be any ideal of R and consider an R-module map $f : I \to E$. Since R is Noetherian, I is finitely generated, and it follows that there exists an index α such that $f(I) \subset \iota_\alpha(E_\alpha)$. Let M be a finitely generated submodule of E_α such that $f(I) \subset \iota_\alpha(M)$. Consider the short exact sequence

$$0 \to K \to M \xrightarrow{\iota_\alpha} f(I) \to 0.$$

Since M is finitely generated and R is Noetherian, K is finitely generated. Moreover K maps to 0 in the direct limit, so there exists $\beta \geq \alpha$ such that $\iota_{\alpha\beta}K = 0$. Let $M' = \iota_{\alpha\beta}M$, so by construction

$$\iota_\beta : M' \xrightarrow{\sim} f(I).$$

Taking $g = \iota_\beta|_{M'}^{-1} \circ f$ we get a map $g : I \to E_\beta$ such that $f = \iota_\beta \circ g$. Since E_β is injective, g extends to a map $G : R \to E_\beta$ and thus $F = \iota_\beta \circ G$ extends f to R. $\square$

8.10. **Artinian rings: structure theory.**

A ring R which satisfies the descending chain condition (DCC) on ideals is called **Artinian** (or sometimes, "an Artin ring").

Exercise 8.29:
a) Show that a ring with only finitely many ideals is Artinian.
b) Show that the ring of integers $\mathbb{Z}$ is *not* Artinian.
c) Show that a quotient of an Artinian ring is Artinian.
d) Show that a localization of an Artinian ring is Artinian.

Obviously any finite ring has only finitely many ideals and is Artinian. It is not difficult to give examples of infinite rings with finitely many ideals. For instance, let k be a field and let $0 \neq f \in k[t]$. Then $R = k[t]/(f)$ has only finitely many ideals. Indeed, if we factor $f = f_1^{a_1} \cdots f_r^{a_r}$ into irreducible factors, then the Chinese Remainder Theorem gives

$$k[t]/(f) \cong k[t]/(f_1^{a_1}) \times \ldots \times k[t]/(f_r^{a_r}).$$

Each factor ring $k[t]/(f_i^{a_i})$ is a local ring with maximal ideal (f_1), and the ideals are precisely

$$(0) \subsetneq (f_i)^{a_i - 1} \subsetneq \ldots \subsetneq f_i.$$

Since every ideal in a product is a direct sum of ideals of the factors, there are then precisely $\prod_{i=1}^r (a_i + 1)$ ideals of R.

A bit of reflection reveals that – notwithstanding their very similar definitions – requiring (DCC) on ideals of a ring is considerably more restrictive than the (ACC) condition. For instance:

Proposition 8.30. *A domain R is Artinian iff it is a field.*

Proof. Obviously a field satisfies (DCC) on ideals. Conversely, if R is a domain and not a field, there exists a nonzero nonunit element a, and then we have $(a) \supsetneq (a^2) \supsetneq (a^3) \supsetneq \ldots$. Indeed, if $(a^k) = (a^l)$, suppose $k \leq l$ and write $l = k + n$, and then we have $ua^k = a^k a^n$ for some $u \in A^\times$, and then by cancellation we get $a^n = u$, so a^n is unit and thus a is a unit, contradiction. □

The result collects several simple but important properties of Artinian rings.

Theorem 8.31. *Let R be an Artinian ring.*
a) R has dimension zero: prime ideals are maximal.
b) Therefore the Jacobson radical of R coincides with its nilradical.
c) R has only finitely many maximal ideals, say $\mathfrak{m}_1, \ldots, \mathfrak{m}_n$.
d) Let $\mathcal{N} = \bigcap_{i=1}^n \mathfrak{m}_i$ be the nilradical. Then it is a nilpotent ideal: there exists $k \in \mathbb{Z}^+$ such that $\mathcal{N}^k = 0$.

Proof. a) If $\mathfrak{p}$ is a prime ideal of A, then $A/\mathfrak{p}$ is an Artinian domain, which by Proposition 8.30 is a field, so $\mathfrak{p}$ is maximal.

b) By definition, the Jacobson radical is the intersection of all maximal ideals and the nilradical is the intersection of all prime ideals. Thus the result is immediate from part a).

c) Suppose $\mathfrak{m}_i$ is an infinite sequence of maximal ideals. Then

$$R \supsetneq \mathfrak{m}_1 \supsetneq \mathfrak{m}_1 \cap \mathfrak{m}_2 \cdots$$

is an infinite descending chain. Indeed, equality at any step would mean $\mathfrak{m}_{N+1} \supset \bigcap_{i=1}^N \mathfrak{m}_i = \prod_{i=1}^N \mathfrak{m}_i$, and then since $\mathfrak{m}_{N+1}$ is prime it contains $\mathfrak{m}_i$ for some $1 \leq i \leq N$, contradiction.

d) Applying DCC on the powers of $\mathcal{N}$, it must be the case that there exists some k with $\mathcal{N}^k = \mathcal{N}^{k+n}$ for all $n \in \mathbb{Z}^+$. Put $I = \mathcal{N}^k$. Suppose $I \neq 0$, and let Σ be the set of ideals J such that $IJ \neq 0$. Evidently $\Sigma \neq \emptyset$, for $I \in \Sigma$. By DCC we are entitled to a minimal element J of Σ. There exists $0 \neq x \in J$ such that $xI \neq 0$. For such an x, we have $(x) \in \Sigma$ and by minimality we must have $J = (x)$. But $(xI)I = xI \neq 0$, so $xI \subset (x)$ and thus $xI = (x)$ by minimality. So there exists $y \in I$ with $xy = x$ and thus we have

$$x = xy = xy^2 = \ldots = xy^k = \ldots.$$

But $y \in I \subset \mathcal{N}$, hence y is nilpotent and the above equations give $x = 0$, a contradiction. □

Lemma 8.32. *Suppose that in a ring R there exists a finite sequence $\mathfrak{m}_1, \ldots, \mathfrak{m}_n$ of maximal ideals such that $0 = \prod_i \mathfrak{m}_i$. Then R is Noetherian iff it is Artinian.*

Proof. Consider the chain of ideals

$$R \supset \mathfrak{m}_1 \supset \mathfrak{m}_1\mathfrak{m}_2 \supset \ldots \supset \prod_i \mathfrak{m}_i = 0.$$

Each quotient $Q_i := \mathfrak{m}_1 \cdots \mathfrak{m}_{i-1}/\mathfrak{m}_1 \cdots \mathfrak{m}_i$ is an $R/\mathfrak{m}_i$-vector space. Now R satisfies (ACC) (resp. (DCC)) for ideals iff each Q_i satisfies (ACC) (resp. (DCC)). But since each Q_i is a vector space, (ACC) holds iff (DCC) holds. □

Theorem 8.33. *(Akizuki-Hopkins) For a ring R, TFAE:*
(i) R is Artinian.
(ii) R is Noetherian, and prime ideals are maximal.

Proof. (i) $\implies$ (ii): Suppose R is Artinian. By Theorem 8.31, prime ideals in R are maximal, so it suffices to show that R is Noetherian. Let $\mathfrak{m}_1, \ldots, \mathfrak{m}_n$ be the distinct maximal ideals of R. For any $k \in \mathbb{Z}^+$ we have $\prod_{i=1}^n \mathfrak{m}_i^k \subset \left(\bigcap_{i=1}^n \mathfrak{m}_i\right)^k$. Applying Theorem 8.31d), this shows that for sufficiently large k we have $\prod_{i=1}^n \mathfrak{m}_i^k = 0$. We can now apply Lemma 8.32 to conclude that R is Artinian.
(ii) $\implies$ (i): Suppose R is Noetherian and zero-dimensional. A bit later on (sorry!) we will see that any Noetherian ring has only finitely many minimal prime ideals (Corollary **??**), so R has only finitely many minimal prime ideals, each of which is maximal by zero-dimensionality. Therefore $\mathcal{N} = \bigcap_{i=1}^n \mathfrak{m}_i$ is the nilradical of a Noetherian ring, hence a nilpotent ideal. As above, we deduce that for sufficiently large k we have $\prod_{i=1}^n \mathfrak{m}_i^k = 0$. By Lemma 8.32, R is Artinian. □

Exercise 8.30: Consider the ring $R = \mathbb{C}[x,y]/(x^2, xy, y^2) = \mathbb{C}[x,y]/I$.
a) Show that $\dim_{\mathbb{C}} R = 3$ and that a $\mathbb{C}$-basis is given by $1 + I$, $x + I$, $y + I$.
b) Deduce that R is Artinian.
c) Show that the proper ideals of R are precisely the $\mathbb{C}$-subspaces of $\langle x + I, y + I\rangle_{\mathbb{C}}$.
d) Deduce that R has infinitely many ideals.

Exercise 8.31: Let k be a field and $A = k[\{x_i\}_{i=1}^{\infty}]$ a polynomial ring over k in

a countable infinite number of indeterminates. Let $\mathfrak{m} = (\{x_i\})$ be the ideal of all polynomials with zero constant term, and put $R = A/\mathfrak{m}^2$. Show that R is a ring with a unique prime ideal which is not Noetherian (so also not Artinian).

Exercise 8.32: Let $n \in \mathbb{Z}^+$. Suppose R is a Noetherian domain with exactly n prime ideals. Must R be Artinian?

Proposition 8.34. *Let $(R, \mathfrak{m})$ be a Noetherian local ring.*
a) Either:
(i) $\mathfrak{m}^k \neq \mathfrak{m}^{k+1}$ for all $k \in \mathbb{Z}^+$, or
(ii) $\mathfrak{m}^k = 0$ for some k.
b) Moreover, condition (ii) holds iff R is Artinian.

Proof. a) Suppose there exists k such that $\mathfrak{m}^k = \mathfrak{m}^{k+1}$. By Nakayama's Lemma, we have $\mathfrak{m}^k = 0$. If $\mathfrak{p}$ is any prime ideal of R, then $\mathfrak{m}^k \subset \mathfrak{p}$, and taking radicals we have $\mathfrak{m} \subset \mathfrak{p}$, so $\mathfrak{p} = \mathfrak{m}$ and R is a Noetherian ring with a unique prime ideal, hence an Artinian local ring. b) If R is Artinian, then (i) cannot hold, so (ii) must hold. Conversely, if (ii) holds then $\mathfrak{m}$ is a nil ideal, hence contained in the intersection of all prime ideals of R, which implies that $\mathfrak{m}$ is the only prime ideal of R, and R is Artinian by the Akizuki-Hopkins theorem. □

Theorem 8.35. *(Structure theorem for Artinian rings) Let R be an Artinian ring.*
a) There exist finitely many local Artinian rings R_i such that $R \cong \prod_{i=1}^n R_i$.
b) Moreover, the decomposition is unique in the sense that if $R \cong \prod_{j=1}^m S_j$ is another decomposition, then $n = m$ and there exists a permutation σ of $\{1, \ldots, n\}$ such that $R_i \cong S_{\sigma(i)}$ for all i.

Proof. a) Let $(\mathfrak{m}_i)_{i=1}^n$ be the distinct maximal ideals of R. We have seen that there exists $k \in \mathbb{Z}^+$ such that $\prod_{i=1}^n \mathfrak{m}_i^k = 0$. By Proposition 4.16, the ideals $\mathfrak{m}_i^k$ are pairwise comaximal, so so $\bigcap_i \mathfrak{m}_i^k = \prod_i \mathfrak{m}_i^k$. Therefore by CRT the natural mapping

$$R \to \prod_{i=1}^n \frac{R}{\mathfrak{m}_i^k}$$

is an isomorphism. Each $\frac{R}{\mathfrak{m}_i^k}$ is local Artinian, so this gives part a).
b) The proof requires **primary decomposition**, so must be deferred to §10.5. □

Exercise 8.33: Let R be an Artinian ring.
a) Show that every element of R is either a unit or a zero divisor.
b) Show that R is its own total fraction ring.

Exercise 8.34:[42] For a ring R, TFAE:
(i) R is semilocal, i.e., $\operatorname{MaxSpec} R$ is finite.
(ii) $R/\operatorname{rad} R$ is Artinian.

8.11. **The Hilbert Basis Theorem.**

The following result shows in one fell swoop that the majority of the rings that one encounters in classical algebraic geometry and number theory are Noetherian.

[42]This exercise should be compared to Exercise 4.14, which gives a criterion for semilocality in terms of the quotient by the Jacobson radical.

Theorem 8.36. *(Hilbert Basis Theorem) If R is Noetherian, so is $R[t]$.*

Proof. Seeking a contradiction, suppose J is an ideal of $R[t]$ which is not finitely generated. We inductively construct a sequence $f_0, f_1, \ldots, f_n, \ldots$ of elements of J and a sequence of ideals $J_n = \langle f_0, \ldots, f_n \rangle$ of $R[t]$ as follows: $f_0 = 0$, and for all $i \in \mathbb{N}$, f_{i+1} is an element of minimal degree in $J \setminus J_i$. Moreover, for all $i \in \mathbb{Z}^+$ let a_i be the leading coefficient of f_i, and let I be the ideal $\langle a_1, a_2, \ldots, a_N, \ldots \rangle$ of R. However, R is Noetherian, so there exists $N \in \mathbb{Z}^+$ such that $I = \langle a_1, \ldots, a_N \rangle$. In particular, there are $u_1, \ldots, u_N \in R$ such that $a_{N+1} = u_1 a_1 + \ldots + u_N a_N$. Define

$$g = \sum_{i=1}^{N} u_i f_i t^{\deg f_{N+1} - \deg f_i}.$$

Since $g \in J_N$ and $f_{N+1} \in J \setminus J_N$, $f_{N+1} - g \in J \setminus J_N$. Moreover, g and f_{N+1} have the same degree and the same leading term, so $\deg f_{N+1} - g < \deg f_{N+1}$, hence f_{N+1} does not have minimal degree among polynomials in $J \setminus J_N$, contradiction. □

Exercise 8.35: Prove the converse of the Hilbert Basis Theorem: if R is a ring such that either $R[t]$ or $R[[t]]$ is Noetherian, then R is Noetherian.

Corollary 8.37. *A finitely generated algebra over a Noetherian ring is Noetherian.*

Proof. Let R be Noetherian and S a finitely generated R-algebra, so that $S \cong R[t_1, \ldots, t_n]/I$ for some $n \in \mathbb{Z}^+$ and some ideal I. By the Hilbert Basis Theorem (and induction), $R[t_1, \ldots, t_n]$ is Noetherian, hence so is its quotient ring S. □

Theorem 8.38. *Let R be a ring, let $\mathcal{P}$ be a prime ideal of $R[[t]]$, and let $\mathfrak{p}$ be the set of constant coefficients of elements of $\mathcal{P}$.*
a) Suppose that for some $k \in \mathbb{N}$, $\mathfrak{p}$ can be generated by k elements. Then $\mathcal{P}$ can be generated by $k+1$ elements. Moreover, if $t \notin \mathcal{P}$, $\mathcal{P}$ can be generated by k elements.
b) If R is Noetherian, then so is $R[[t]]$.

Proof. Let $\iota : R \to R[[t]]$ be the inclusion map, so $\mathfrak{p} = \iota^* \mathcal{P}$.
a) Suppose $\mathfrak{p} = \langle a_1, \ldots, a_k \rangle$, and let I be the ideal $\langle a_1, \ldots, a_k, t \rangle$ of $R[[t]]$.
Case 1: If $t \in \mathcal{P}$, we claim $I = \mathcal{P}$, which suffices. That $I \subset \mathcal{P}$ is clear; conversely, writing $f = \sum_{n=0}^{\infty} a_n t^n \in \mathcal{P}$ as $a_0 + t(a_1 + a_2 t + \ldots)$ shows $f \in I$.
Case 2: Suppose $t \notin \mathcal{P}$. Let $f_1, \ldots, f_k \in \mathcal{P}$ with constant terms $a_1, \ldots, a_k$, respectively. We CLAIM $\mathcal{P} = \langle f_1, \ldots, f_k \rangle$. To see this, let $g_1 = \sum_{n=0}^{\infty} b_n t^n \in \mathcal{P}$. Since $b_0 \in \mathfrak{p}$, there are $r_{1,1}, \ldots, r_{k,1} \in R$ with

$$b_0 = r_{1,1} a_1 + \ldots + r_{k,1} a_k,$$

and thus

$$g_1 - (r_{1,1} f_1 + \ldots + r_{k,1} f_k) = t g_2$$

for some $g_2 \in R[[t]]$. Since $\mathcal{P}$ is prime, $t g_2 \in \mathcal{P}$ and $t \notin \mathcal{P}$, we must have $g_2 \in \mathcal{P}$. Applying the above argument to g_2 we find $r_{1,2}, \ldots, r_{k,2} \in R$ and $g_3 \in \mathcal{P}$ such that $g_2 - (r_{1,2} f_1 + \ldots + r_{1,k} f_k) = t g_3$. Continuing in this way, we generate, for $1 \leq i \leq k$, a power series $h_i = \sum_{n=0}^{\infty} r_{i,n} t^n$, such that

$$g = h_1 f_1 + \ldots + h_k f_k,$$

establishing the claim.
b) If R is Noetherian, then by part a) every prime ideal of $R[[t]]$ is finitely generated. By Cohen's Theorem (Theorem 4.26), $R[[t]]$ is Noetherian. □

Exercise 8.36: Show that for a ring R, TFAE:
(i) R is Noetherian.
(ii) For all $n \geq 1$, $R[t_1, \ldots, t_n]$ is Noetherian.
(iii) For all $n \geq 1$, $R[[t_1, \ldots, t_n]]$ is Noetherian.

Exercise 8.37: Let k be a field, and consider the subring $R = k[y, xy, x^2y, \ldots]$ of $k[x, y]$. Show that R is not Noetherian.

Therefore, a subring of a Noetherian ring need not be Noetherian. Thinking that this ought to be the case is one of the classic "rookie mistakes" in commutative algebra. In general though, it is the exception rather than the rule that a nice property of a ring R is inherited by all subrings of R, and one gets used to this.

8.12. **The Krull Intersection Theorem.**

8.12.1. *Preliminaries on Graded Rings.*

In the proof of the theorem of this section we will need a little fact about homogeneous polynomials. So here we discuss some rudiments of this theory by embedding it into its natural context: **graded rings**. The notion of graded ring is of the utmost importance in various applications of algebra, from algebraic geometry to algebraic topology and beyond. It would certainly be nice to give a comprehensive exposition of graded algebra but at the moment this is beyond the ambition of these notes, so we content ourselves with the bare minimum needed for our work in the next section.

Let R be a ring, $n \in \mathbb{Z}^+$, and denote by $R[t] = R[t_1, \ldots, t_n]$ the polynomial ring in n indeterminates over R. For a polynomial $P = P(t)$ in several variables, we have the notion of the **degree of P** with respect to the variable t_i: thinking of P as an element of $R[t_1, \ldots, t_{i-1}, t_{i+1}, \ldots, t_n][t_i]$ it is just the largest m such that the coefficient of t_i^m is nonzero, as usual. For any monomial term $c_I t_1^{i_1} \cdots t_n^{i_n}$ we define the **total degree** to be $d = i_1 + \ldots + i_n$.

A nonzero polynomial $P = \sum_I c_I t_1^{i_1} \cdots t_n^{i_n}$ is **homogeneous** if all of its monomial terms have the same total degree, and this common number is called the **degree of the homogeneous polynomial** P. By convention the zero polynomial is regarded as being homogeneous total degree d for all $d \in \mathbb{N}$.

A general polynomial $P \in R[t]$ can be written as a sum of homogeneous polynomials $P = \sum_{d=0}^{\infty} P_d(t)$ with each P_d homogeneous of degree d (and of course $P_d = 0$ for all sufficiently large d). This sum is *unique*. One way to see this is to establish the following more structural fact: for any $d \in \mathbb{N}$, let $P[t]_d$ be the set of all polynomials which are homogeneous of degree d. Then each $P[t]_d$ is an R-submodule of $P[t]$ and we have a direct sum decomposition

$$P[t] = \bigoplus_{d=0}^{\infty} P[t]_d. \tag{20}$$

Moreover, for all $d_1, d_2 \in \mathbb{N}$ we have

$$P[t]_{d_1} \cdot P[t]_{d_2} \subset P[t]_{d_1+d_2}. \tag{21}$$

In general, if R is a ring and S is an algebra admitting an R-module direct sum decomposition $S = \bigoplus_{d=0}^{\infty} S_d$ satisfying $S_{d_1} \cdot S_{d_2} \subset S_{d_1+d_2}$, then we say that S is an $(\mathbb{N})$-**graded R-algebra**. Taking $R = \mathbb{Z}$ we get the notion of a **graded ring**.

Exercise 8.38: Let $S = \bigoplus_{d=0}^{\infty} S_d$ be a graded R-algebra. Show that the R-submodule S_0 is in fact an R-algebra.

Let $S = \bigoplus_{d=0}^{\infty} S_d$ be a graded ring. We say that $x \in S$ is **homogeneous of degree d** if $x \in S_d$. An ideal I of S is **homogeneous** if it has a generating set $I = \langle x_i \rangle$ with each x_i a homogeneous element.

Exercise 8.39: Let S be a graded R-algebra and let I be a homogeneous ideal of S. Show that

$$S/I = \bigoplus_{d=0}^{\infty} (S_d + I)/I$$

and thus S/I is a graded R-algebra.

Now back to the case of polynomial rings.

Lemma 8.39. *Let S be a graded ring, let $f_1, \ldots, f_n$ be homogeneous elements of S, and put $I = \langle f_1, \ldots, f_n \rangle$. Let $f \in I$ be homogeneous. Then there are homogeneous elements $g_1, \ldots, g_n \in R$ such that*

$$f = \sum_{i=1}^{n} g_i f_i$$

and for all $1 \leq i \leq n$,

$$\deg g_i = \deg f - \deg f_i.$$

Proof. Since $f \in I$, there exist $X_1, \ldots, X_n \in S$ such that

$$f = X_1 f_1 + \ldots + X_n f_n.$$

For each $1 \leq i \leq n$, let $X_i = \sum_j x_{i,j}$ with $\deg x_{i,j} = j$ be the canonical decomposition of X_i into a sum of homogeneous elements: i.e., $\deg x_{i,j} = j$. Then

$$f = \sum_{d=0}^{\infty} \sum_{i=1}^{n} x_{i,d-\deg f_i} f_i. \tag{22}$$

Since f is homogeneous of degree $\deg(f)$, only the $d = \deg(f)$ in the right hand side of (22) is nonzero, so

$$f = \sum_{i=1}^{n} x_{i,\deg f - \deg f_i} f_i.$$

□

8.12.2. *The Krull Intersection Theorem.*

Theorem 8.40. *Let R be a Noetherian ring, and I an ideal of R. Suppose there is an element x of R such that $x \in \bigcap_{n=1}^{\infty} I^n$. Then $x \in xI$.*

Proof. The following miraculously short and simple proof is due to H. Perdry [Pe04]. Suppose $I = \langle a_1, \ldots, a_r \rangle$. For each $n \geq 1$, since $x \in I^n$ there is a homogeneous degree n polynomial $P_n(t_1, \ldots, t_r) \in R[t_1, \ldots, t_r]$ such that

$$x = P_n(a_1, \ldots, a_n).$$

By the Hilbert Basis Theorem (Theorem 8.36), $R[t_1, \ldots, t_r]$ is Noetherian. Therefore, defininining $J_n = \langle P_1, \ldots, P_n \rangle$, there exists N such that $J_N = J_{N+1}$. By Lemma 8.39 we may write

$$P_{N+1} = Q_N P_1 + \ldots + Q_1 P_N,$$

with Q_i homogeneous of degree $i > 0$. Plugging in $t_i = a_i$ for $1 \leq i \leq n$, we get

$$x = P_{N+1}(a_1, \ldots, a_n) = x \left(Q_1(a_1, \ldots, a_n) + \ldots + Q_N(a_1, \ldots, a_N) \right).$$

Since each Q_i is homogeneous of positive degree, we have $Q_i(a_1, \ldots, a_n) \in I$. □

Corollary 8.41. *Let I be an ideal in a Noetherian ring R. Suppose* either
(i) R is a domain and I is a proper ideal; or
(ii) I is contained in the Jacobson radical $J(R)$ of R.
Then $\bigcap_{n=1}^{\infty} I^n = 0$.

Proof. Either way, let $x \in \bigcap_{n=1}^{\infty} I^n$ and apply Theorem 8.40 to obtain an element $a \in I$ such that $x = xa$. Thus $(a-1)x = 0$. Under assumption (i), we obtain either $a = 1$ – so $I = R$, contradicting the properness of I – or $x = 0$. Under assumption (ii), $a \in J(R)$ implies $a - 1 \in R^\times$, so that we may multiply through by $(a-1)^{-1}$, again getting $x = 0$. □

Exercise 8.40 (Suárez-Alvarez): Exhibit an ideal I in a Noetherian ring such that $\bigcap_{n=1}^{\infty} I^n \supsetneq \{0\}$. (Hint: idempotents!)

Exercise 8.41: Let R be the ring of all C^∞ functions $f : \mathbb{R} \to \mathbb{R}$.
Let $\mathfrak{m} = \{f \in R \mid f(0) = 0\}$.
a) Show that $\mathfrak{m} = xR$ is a maximal ideal of R.
b) Show that for all $n \in \mathbb{Z}^+$, $\mathfrak{m}^n = \{f \in R \mid f(0) = f'(0) = \ldots = f^{(n)}(0)\}$.
c) Deduce that $\bigcap_{n=1}^{\infty} \mathfrak{m}^n$ is the ideal of all smooth functions with identically zero Taylor series expansion at $x = 0$. Conclude that $\bigcap_{n=1}^{\infty} \mathfrak{m}^n \neq 0$.
d) Let $f(x) = e^{\frac{-1}{x^2}}$ for $x \neq 0$ and 0 for $x = 0$. Show that $f \notin f\mathfrak{m}$.
e) Deduce that R is not Noetherian.

Exercise 8.42: Let $R = \bigcup_{n=1}^{\infty} \mathbb{C}[[t^{\frac{1}{n}}]]$ be the Puiseux series ring. Show that R is a domain with a unique maximal ideal $\mathfrak{m}$ and that for all $n \in \mathbb{Z}^+$, $\mathfrak{m}^n = \mathfrak{m}$. Deduce from the Krull Intersection Theorem that R is not Noetherian.

Remark: The preceding exercise will become much more routine when we study valuation rings in §17. In that language, one can show that if R is a valuation ring with divisible value group, then $(R, \mathfrak{m})$ is a local domain and $\bigcap_{n=1}^{\infty} \mathfrak{m}^n = \mathfrak{m}$.

8.13. **Krull's Principal Ideal Theorem.**

Theorem 8.42. *(The Principal Ideal Theorem, a.k.a. Krull's Hauptidealsatz) Let x be a nonunit in a Noetherian ring R, and let $\mathfrak{p}$ be minimal among prime ideals containing x. Then $\mathfrak{p}$ has height at most one.*

Remark: A prime $\mathfrak{p}$ which is minimal among primes containing x will be called a **minimal prime over x**. Note that an equivalent condition is that $\mathfrak{p}$ is a minimal prime in the quotient ring $R/(x)$. Note also that if x is nilpotent, every prime of $\mathfrak{p}$ contains x so the height of any minimal prime is 0.

Our strategy of proof follows Kaplansky, who follows D. Rees. We need a preliminary result:

Lemma 8.43. *Let u and y be nonzero elements in a domain R. Then:*
a) The R-modules $\langle u, y\rangle/(u)$ and $\langle u^2, uy\rangle/(u^2)$ are isomorphic.
b) If we assume further that for all $t \in R$, $tu^2 \in (y)$ implies $tu \in (y)$, then the R-modules $(u)/(u^2)$ and $\langle u^2, y\rangle/\langle u^2, uy\rangle$ are isomorphic.

Proof. a) The isomorphism is simply induced by multiplication by u.
b) The module $(u)/(u^2)$ is cyclic with annihilator (u), and conversely any such module is isomorphic to $R/(u)$. Moreover $M := \langle u^2, y\rangle/\langle u^2, uy\rangle$ is also cyclic, being generated simply by y. Certainly u annihilates M, so it suffices to show that the annihilator is exactly (u). More concretely, given $ky = au^2 + buy$, we must deduce that $k \in (u)$. But we certainly have $au^2 \in (y)$, so by hypothesis $au \in (y)$, say $au = cy$. Then $ky = cuy + buy$. Since $0 \neq y$ in our domain R, we may cancel y to get $k = (c + b)u \in (u)$. □

Proof of Krull's Hauptidealsatz: Under the given hypotheses, assume for a contradiction that we have

$$\mathfrak{p}_2 \subsetneq \mathfrak{p}_1 \subsetneq \mathfrak{p}.$$

Note first that we can safely pass to the quotient $R/\mathfrak{p}_2$ and thus assume that R is a domain. Dually, it does not hurt any to localize at $\mathfrak{p}$. Therefore we may assume that we have a Noetherian local domain R with maximal ideal $\mathfrak{m}$, an element $x \in \mathfrak{m}$, and a nonzero prime ideal, say $\mathfrak{p}$, with $x \in \mathfrak{p} \subsetneq \mathfrak{m}$, and our task is now to show that this setup is impossible. Now for the clever part: let $0 \neq y$ be any element of $\mathfrak{p}$, and for $k \in \mathbb{Z}^+$, let I_k denote the ideal of all elements t with $tx^k \in (y)$. Then $\{I_k\}_{k=1}^{\infty}$ is an ascending chain of ideals in the Noetherian ring R so must stabilize, say at $k = n$. In particular, $tx^{2n} \in (y)$ implies $tx^n \in (y)$. Putting $u = x^n$, we have $tu^2 \in (y)$ implies $(tu) \in (y)$.

Since $\mathfrak{m}$ is a minimal prime over (x), the quotient ring $T = R/(u^2)$ has exactly one prime ideal, $\mathfrak{m}$, and is therefore, by the Akizuki-Hopkins Theorem, an Artinian ring, so that any finitely generated T-module has finite length. In particular, $M := \langle u, y\rangle/(u^2)$, which can naturally be viewed as a T-module, has finite length, and hence so does its T-submodule $M' := \langle u^2, y\rangle/(u^2)$. Put $N = \langle u^2, y\rangle\langle u^2, uy\rangle$. Then

$$\ell(M') = \ell(N) + \ell(\langle u^2, uy/(u^2)) = \ell((u)/(u^2)) + \ell(\langle u, y\rangle/(u)) = \ell(M);$$

in the second equality we have used Lemma 8.43. The only way that M could have the same length as its submodule M' is if $\langle u, y\rangle = \langle u^2, y\rangle$, i.e., if there exist $c, d \in R$ such that $u = cu^2 + dy$, or $u(1 - cu) = -dy$. Since u lies in the maximal ideal of the local ring R, $1 - cu \in R^\times$, and thus $u \in (y) \subset \mathfrak{p}$. But $\mathfrak{m}$ is minimal over x and hence, being prime, also minimal over $u = x^n$, contradiction! □

Corollary 8.44. *With hypotheses as in Theorem 8.42, suppose that x is not a zero-divisor. Then any prime $\mathfrak{p}$ which is minimal over x has height one.*

Exercise 8.43: Use the Akizuki-Hopkins theorem and Proposition 8.34 to give a proof of Corollary 8.44.

Again we need a small preliminary result.

Lemma 8.45. *(Prime Avoidance) Let R be a ring, and $I_1, \ldots, I_n, J$ be ideals of R. Suppose that all but at most two of the I_i's are prime and that $J \subset \bigcup_{i=1}^n I_i$. Then $J \subset I_i$ for some i.*

Proof. We go by induction on n, the case $n = 1$ being trivial.
$n = 2$: Seeking a contradiction, suppose there is $x_1 \in J \setminus I_2$ and $x_2 \in J \setminus I_1$. Since $J \subset I_1 \cup I_2$ we must have $x_1 \in I_1$ and $x_2 \in I_2$. Then $x_1 + x_2 \in J \subset I_1 \cup I_2$. If $x_1 + x_2 \in I_1$, then since $x_1 + x_2, x_1 \in I_1$, so is x_2, contradiction; whereas if $x_1 + x_2 \in I_2$, then since $x_1 + x_2, x_2 \in I_1$, so is x_1.[43]
$n \geq 3$: We may suppose that I_n is prime and also that for all proper subsets $S \subset \{1, \ldots, n\}$, $J \not\subset \bigcup_{i \in S} I_i$; otherwise we would be done by induction. So for $1 \leq i \leq n$, there is $x_i \in J \setminus \bigcup_{j \neq i} I_j$, and then $x_i \in I_i$. Consider $x = x_1 \cdots x_{n-1} + x_n$. Then $x \in J$, so $x \in I_i$ for some i.
Case 1: $x \in I_n$. Then since $x_n \in I_n$, $x_1 \cdot x_{n-1} \in I_n$, and since I_n is prime $x_i \in I_n$ for some $1 \leq i \leq n-1$, contradiction.
Case 2: $x \in I_j$ for some $1 \leq j \leq n-1$. Then $x_1 \cdots x_{n-1} \in I_j$, so $x_n \in I_j$, contradiction. □

Exercise 8.44 ([CDVM13, Prop. 2.2]) Let R be a UFD and not a field. Suppose $R^\times$ is finite. Show that R has infinitely many principal prime ideals.

(HINT: Suppose R has finitely many principal nonzero principal prime ideals, say $(\pi_1), \ldots, (\pi_n)$. Let $\mathfrak{m} \in \operatorname{MaxSpec} R$. By choosing $x \in \mathfrak{m}^\bullet$ and applying unique factorization, show $\mathfrak{m} \subset \bigcup_{i=1}^n$. Apply Prime Avoidance and then Theorem 4.20.)

We can now give a striking structural result about primes in a Noetherian ring. First a piece of notation: for any elements x, y in a poset S we define the "interval" (x, y) to be the set of all $z \in S$ such that $x < z < y$. For prime ideals $\mathfrak{p}$ and $\mathfrak{q}$, we denote by $(\mathfrak{p}, \mathfrak{q})$ the set of all prime ideals $\mathcal{P}$ with $\mathfrak{p} \subset \mathcal{P} \subset \mathfrak{q}$.

Corollary 8.46. *Let $\mathfrak{p} \subset \mathfrak{q}$ be prime ideals in a Noetherian ring R. Then the interval $(\mathfrak{p}, \mathfrak{q})$ is either empty or infinite.*

Proof. Proof of Corollary 8.46: As usual, by correspondence we may pass to $R/\mathfrak{p}$ and therefore assume WLOG that $\mathfrak{p} = 0$. Suppose that for some $n \geq 1$, $[0, \mathfrak{q}] = \{\mathfrak{p}_1, \ldots, \mathfrak{p}_n\}$. According to Lemma 8.45 we cannot then have $\mathfrak{q} \subset \bigcup_{i=1}^n \mathfrak{p}_i$, so choose $x \in \mathfrak{q} \setminus \bigcup_{i=1}^n \mathfrak{p}_i$. Then $\mathfrak{q}$ is a prime of R, of height at least 2, which is minimal over (x), contradicting Theorem 8.42. □

In particular, if R is Noetherian and $\operatorname{Spec} R$ is finite, then $\dim R \leq 1$.

Theorem 8.47. *(Generalized Principal Ideal Theorem) Let R be a Noetherian ring, and let $I = \langle a_1, \ldots, a_n \rangle$ be a proper ideal of R. Let $\mathfrak{p}$ be a minimal element of the set of all prime ideals containing I. Then $\mathfrak{p}$ has height at most n.*

[43] In fact this works for any subgroups I_1, I_2, J of a group G with $J \subset I_1 \cup I_2$.

Proof. As usual, we may localize at $\mathfrak{p}$ and suppose that R is local with $\mathfrak{p}$ as its maximal ideal. Suppose to the contrary that there exists a chain $\mathfrak{p} = \mathfrak{p}_0 \supsetneq \mathfrak{p}_1 \supsetneq \ldots \supsetneq \mathfrak{p}_{n+1}$. Because R is Noetherian, we may arrange for $(\mathfrak{p}_1, \mathfrak{p}) = \emptyset$. Because $\mathfrak{p}$ is minimal over I, I cannot be contained in $\mathfrak{p}_1$; without loss of generality we may suppose that a_1 is not in $\mathfrak{p}_1$. Put $J := \langle \mathfrak{p}_1, a_1 \rangle$; then J strictly contains $\mathfrak{p}_1$ so $\mathfrak{p}$ is the unique prime of R containing J. So the ring R/J is an Artin local ring, and then by Proposition 8.34 for sufficiently large k we have $\mathfrak{p}^k \subset J$. Then by taking t to be sufficiently large we can write, for $2 \leq i \leq n$,

$$a_i^t = c_i a_1 + b_i, \ c_i \in R, b_i \in \mathfrak{p}_1.$$

Put $K = \langle b_2, \ldots, b_n \rangle \subset \mathfrak{p}_1$. Since the height of $\mathfrak{p}_1$ exceeds $n-1$, by induction on n we may assume that $\mathfrak{p}_1$ properly contains a prime ideal Q which contains J. The ideal $Q' := \langle a_1, Q \rangle$ contains some power of each a_i and therefore $\mathfrak{p}$ is the unique prime ideal containing Q'. So in the quotient R/Q, the prime $\mathfrak{p}/Q$ is minimal over the principal ideal Q'/Q. By Krull's Hauptidealsatz (Theorem 8.42) $\mathfrak{p}/Q$ has height 1. On the other hand, we have $\mathfrak{p}/Q \supsetneq \mathfrak{p}_1/Q \supsetneq 0$, a contradiction. □

8.14. **The Dimension Theorem, following** [BMRH]**.**

The following is a very basic theorem about Noetherian rings:

Theorem 8.48. *(Dimension Theorem) Let R be a Noetherian ring.*
a) We have $\dim R[t] = \dim R + 1$.
b) We have $\dim R[[t]] = \dim R + 1$.

Remark: For a non-Noetherian ring R, one has the inequalities

$$\dim R + 1 \leq \dim R[t] \leq 2 \dim R[t] + 1,$$

and indeed there are rings for which $\dim R[t] = 2 \dim R + 1$.

Of course, an immediate induction argument gives:

Corollary 8.49. *Let k be a field. Then*

$$\dim k[t_1, \ldots, t_n] = \dim k[[t_1, \ldots, t_n]] = n.$$

Traditional proofs of the Dimension Theorem require significant development of the dimension *theory* of commutative rings, a topic which is not covered here. Happily, a striking alternate approach to the Dimension Theorem was given by Brewer, Heinzer, Montgomery and Rutter in [BMRH]. We follow their treatment here.

COMPLETE ME! ♣

8.15. **The Artin-Tate Lemma.**

Theorem 8.50. *(Artin-Tate* [AT51]*) Let $R \subset T \subset S$ be a tower of rings such that:*
(i) R is Noetherian,
(ii) S is finitely generated as an R-algebra, and
(iii) S is finitely generated as a T-module.
Then T is finitely generated as an R-algebra.

Proof. Let $x_1, \ldots, x_n$ be a set of generators for S as an R-algebra, and let $\omega_1, \ldots, \omega_m$ be a set of generators for S as a T-module. For all $1 \leq i \leq n$, we may write

$$x_i = \sum_j a_{ij}\omega_j, \ a_{ij} \in T. \tag{23}$$

Similarly, for all $1 \leq i, j \leq m$, we may write

$$\omega_i\omega_j = \sum_{i,j,k} b_{ijk}\omega_k, \ b_{ijk} \in T. \tag{24}$$

Let T_0 be the R-subalgebra of T generated by the a_{ij} and b_{ijk}. Since T_0 is a finitely generated algebra over the Noetherian ring R, it is itself a Noetherian ring by the Hilbert Basis Theorem. Each element of S may be expressed as a polynomial in the x_i's with R-coefficients. Making substitutions using (23) and then (24), we see S is generated as a T_0-module by $\omega_1, \ldots, \omega_m$, and in particular that S is a finitely generated T_0-module. Since T_0 is Noetherian, the submodule T is also finitely generated as a T_0-module. This immediately implies that T is finitely generated as a T_0-algebra and then in turn that T is finitely generated as an R-algebra. □

9. Boolean rings

9.1. **First Properties.**

Let R be a ring, not necessarily commutative, but with a multiplicative identity 1, with the property that $x^2 = x$ for all $x \in R$. Then $(1+1) = (1+1)^2 = 1+1+1+1$, so $1 + 1 = 0$. It follows that $-x = x$ for all $x \in R$. Moreover for any $x, y \in R$, $(x+y) = (x+y)^2 = x^2+xy+yx+y^2 = x+y+xy+yx$, so $xy+yx = 0$ or $xy = yx$. Therefore such a ring is necessarily commutative.

With this remark in mind, define a **Boolean ring** to be a commutative ring with identity such that $x^2 = x$ for all elements x.

Exercise 9.1: Show that the group of units of a Boolean ring is trivial.

Exercise 9.2: a) Show that any quotient ring of a Boolean ring is Boolean.
b) Show that any subring of a Boolean ring is Boolean.

Exercise 9.3: Show that a Boolean ring is absolutely flat.

9.2. **Boolean Algebras.**

A Boolean ring is an object of commutative algebra. It turns out that there is a completely equivalent class of structures of an order-theoretic nature, called **Boolean algebras**. In some ways the concept of a Boolean algebra is more intuitive and transparent – e.g., starting directly from the definition, it is perhaps easier to give examples of Boolean algebras. Moreover it is not at all difficult to see how to pass from a Boolean ring to a Boolean algebra and conversely.

A **Boolean algebra** is a certain very nice partially ordered set $(B, \leq)$. Recall that for any partially orderet set B and any subset S, we have the notion of the

supremum $\sup S$ and the **infimum** $\inf S$. To define these it is convenient to extend the inequality notation as follows: if S, T are subsets of B, we write

$$S < T$$

to mean that for all $s \in S$ and $t \in T$, $s < t$, and similarly

$$S \leq T$$

to mean that for all $s \in S$ and $t \in T$, $s \leq t$.
Then we say that $z = \sup S$ if $S \leq z$ and if w is any element of B with $S \leq w$, then $z \leq w$. Similarly $z = \inf S$ if $z \leq S$ and if w is any element of B with $w \leq S$ then $w \leq Z$. For a given subset S, neither $\sup S$ nor $\inf S$ need exist, but if either exists it it is plainly unique. In particular if $\sup \varnothing$ exists, it is necessarily a bottom element, called 0, and if $\inf \varnothing$ exists, it is necessarily a top element called 0.
A partially ordered set $(L, \leq)$ is called a **lattice** if for all $x, y \in L$, $\sup\{x, y\}$ and $\inf\{x, y\}$ both exist. We give new notation for this: we write

$$x \vee y := \sup\{x, y\},$$

the **join** of x and y and

$$x \wedge y := \inf\{x, y\},$$

the **meet** of x and y.
A lattice is said to be **bounded** if it contains a bottom element 0 and a top element 1: equivalently, $\sup S$ and $\inf S$ exist for every finite subset S.

Exercise 9.4: Let L be a lattice containing 0 and 1, and let $x \in L$. Then:
a) $x \vee 1 = 1$,
b) $x \wedge 1 = x$,
c) $x \vee 0 = x$,
d) $x \wedge 0 = 0$.

A lattice L is **complemented** if it has a bottom element 0, a top element 1, and for each $x \in L$ there exists $y \in L$ such that $x \vee y = 1$, $x \wedge y = 0$.

A lattice is **distributive** if $\forall x, y, z \in L$,

$$(x \vee y) \wedge z = (x \wedge z) \vee (y \wedge z),$$

$$(x \wedge y) \vee z = (x \vee z) \wedge (y \vee z).$$

Proposition 9.1. *Let L be a distributive complemented lattice. Then for all $x \in L$, the complement of x is unique.*

Proof. Suppose that y_1 and y_2 are both complements to x, so

$$x \vee y_1 = x \vee y_2 = 1,\ x \wedge y_1 = x \wedge y_2 = 0.$$

Then

$$y_2 = 1 \wedge y_2 = (x \vee y_1) \wedge y_2 = (x \wedge y_2) \vee (y_1 \wedge y_2) = 0 \vee (y_1 \wedge y_2) = y_1 \wedge y_2,$$

so $y_2 \leq y_1$. Reasoning similarly, we get $y_1 \leq y_2$, so $y_1 = y_2$. □

By virtue of Proposition 9.1 we denote the complement of an element x in a distributive complemented lattice as x^*.

Exercise 9.5: Show that for every element x of a distributive complemented lattice we have $(x^*)^* = x$.

A **Boolean algebra** is a complemented distributive lattice with $0 \neq 1$.

Exercise 9.6: Show that **DeMorgan's Laws** hold in any Boolean algebra B: for all $x, y \in B$, we have
a) $(x \wedge y)^* = x^* \vee y^*$ and
b) $(x \vee y)^* = x^* \wedge y^*$.

The shining example of a Boolean algebra is the powerset algebra 2^S for a nonempty set S. In the special case in which $|S| = 1$, we denote the corresponding Boolean algebra (the unique totally ordered set on two elements) simply as 2.

Not every Boolean algebra is isomorphic to a power set Boolean algebra.

Example: Let S be a set, and let $Z(S) \subset 2^S$ be the collection of all finite and cofinite subsets of S. It is easily checked that $(Z(S), \subset) \subset (2^S, \subset)$ is a sub-Boolean algebra. However, $|Z(S)| = |S|$, so if $|S| = \aleph_0$, then $Z(S)$ is not isomorphic to any power set Boolean algebra.

Boolean algebras form a full subcategory of the category of partially ordered sets. In other words, we define a morphism $f : B \to B'$ of Boolean algebras simply to be an isotone (or order-preserving) map: $\forall x, y \in B, x \leq y \implies f(x) \leq f(y)$. One can (and sometimes does, e.g. for model-theoretic purposes) also axiomatize Boolean algebras as a structure $(B, \vee, \wedge, *, 0, 1)$, the point being that $x \leq y$ iff $x \vee y = y$ iff $x \wedge y = x$, so the partial ordering can be recovered from the wedge or the join.

Proposition 9.2. *The category of Boolean rings is equivalent to the category of Boolean algebras.*

In other words, we can define a functor F from Boolean rings to Boolean algebras and a functor G from Boolean algebras to Boolean rings such that for every Boolean ring R, R is naturally isomorphic to $G(F(R))$ and for every Boolean algebra B, B is naturally isomorphic to $F(G(B))$.

Let us sketch the basic construction, leaving the details to the reader. Suppose first that R is a Boolean ring. Then we associate a Boolean algebra $F(R)$ with the same underlying set as R, endowed with the following operations: $\forall x, y \in R$,

$$x \wedge y = xy,$$

$$x^* = 1 - x.$$

We should also of course define the join operation, but the point is that it is forced on us be DeMorgan's Laws:

$$x \vee y = (x^* \wedge y^*)^* = x + y - xy.$$

Exercise 9.7: Check that $(F(R), \wedge, \vee, *)$ is indeed a Boolean algebra, and that the bottom element 0 in $F(R)$ (resp. the top element 1) is indeed the additive identity 0 (resp. the multiplicative identity 1).

Conversely, suppose that we have a Boolean algebra $(B, \wedge, \vee, *)$. Then we define a Boolean ring $G(B)$ on the same underlying set B, by taking

$$x + y := (x \wedge y^*) \vee (y \wedge x^*)$$

$$xy := x \wedge y.$$

Note that the addition operation corresponds to the Boolean operation "exclusive or" or, in more set-theoretic language, **symmetric difference** $x \Delta y$.

Exercise 9.8: check that $(G(B), +, \cdot)$ is indeed a Boolean ring with additive identity the bottom element 0 of B and multiplicative identity the top element 1 of B.

Exercise 9.9:
a) Let R be a Boolean ring. Show that the identity map 1_R on R is an isomorphism of Boolean rings $R \to G(F(R))$.
b) Let B be a Boolean algebra. Show that the identity map 1_B on B is an isomorphism of Boolean algebras $B \to G(F(B))$.

Exercise 9.10: Let X be a nonempty set, let B_X be the Boolean algebra of subsets of X, partially ordered by inclusion. Show that the corresponding Boolean ring may be identified with the ring 2^X of all functions from X to $\mathbb{F}_2$ under pointwise addition and multiplication.

Exercise 9.11: Show that every finite Boolean algebra is isomorphic to a power-set algebra. Conclude that every finite Boolean ring R is isomorphic to the ring of binary functions on a finite set of cardinality $\log_2(\#R)$. In fact, try to show this both on the Boolean algebra side and on the Boolean ring side. (Hint for the Boolean ring side: use the decomposition into a direct product afforded by an idempotent element.)

Exercise 9.12: Show that an arbitrary direct product of Boolean algebras (or, equivalently, Boolean rings) is a Boolean algebra (or...).

As we saw above, cardinality considerations already show that not every Boolean algebra is the power set Boolean algebra, and hence not every Boolean ring is the full ring of binary functions on some set X. However, in view of results like Cayley's theorem in basic group theory, it is a reasonable guess that every Boolean algebra is *an* algebra of sets, i.e., is a sub-Boolean algebra of a power set algebra. We proceed to prove this important result on the Boolean ring side.

9.3. **Ideal Theory in Boolean Rings.**

Proposition 9.3. *Let R be a Boolean ring.*
a) For all $x \in \mathbb{N}$ and all $n \geq 2$, $x^n = x$.
b) A Boolean ring is reduced, i.e., has no nonzeronilpotent elements.
c) Every ideal in a Boolean ring is a radical ideal.

Proof. a) The case $n = 2$ is the definition of a Boolean ring, so we may assume $n \geq 3$. Assume the result holds for all $x \in R$ and all $2 \leq k < n$. Then $x^n = x^{n-1}x = x \cdot x = x$.

b) If $x \in R$ is such that $x^n = 0$ for some positive integer n, then either $n = 1$ or $n \geq 2$ and $x^n = x$; either way $x = 0$.
c) Let I be an ideal in the Boolean ring R. Then $I = \mathrm{rad}(I)$ iff R/I is reduced, but R/I is again a Boolean ring and part b) applies. □

The ring $\mathbb{Z}/2\mathbb{Z}$ is of course a Boolean ring. It is also a field, hence certainly a local ring and an integral domain. We will shortly see that it is unique among Boolean rings in possessing *either* of the latter two properties.

Proposition 9.4. *a) The only Boolean domain is $\mathbb{Z}/2\mathbb{Z}$.*
b) Every prime ideal in a Boolean ring is maximal.

Proof. a) Let R be a Boolean domain, and let x be an element of R. Then $x(x-1) = 0$, so in a domain R this implies $x = 0$ or $x = 1$, so that $R \cong \mathbb{Z}/2\mathbb{Z}$.

b) If $\mathfrak{p}$ is a prime ideal in the Boolean ring R, then $R/\mathfrak{p}$ is a Boolean domain, hence – by part a) – is simply $\mathbb{Z}/2\mathbb{Z}$. But this ring is a field, so $\mathfrak{p}$ is maximal. □

Proposition 9.5. *Let R be a local Boolean ring. Then $R \cong \mathbb{Z}/2\mathbb{Z}$.*

Proof. Let $\mathfrak{m}$ be the unique maximal ideal of R. By Proposition 9.4, $\mathfrak{m}$ is moreover the unique prime ideal of R. It follows from Proposition 4.12d) that $\mathfrak{m} = \mathrm{nil}\, R$ is the set of all nilpotent elements, so by Proposition 9.3b) $\mathfrak{m} = 0$. Thus R is a field and thus, by Proposition 9.4 must be $\mathbb{Z}/2\mathbb{Z}$. □

Exercise 9.13: Let R be a Boolean ring, let I be an ideal of R.
a) Show that $x, y \in I \implies x \vee y \in I$.
b) Show in fact that $\langle x, y \rangle = \langle x \vee y \rangle$.
c) Deduce that any finitely generated ideal of R is principal.

Thus, for a Boolean ring R, all ideals of R are principal iff R is Noetherian. But in fact very few Boolean rings are Noetherian: we have already seen them all in Exercise X.X.

Proposition 9.6. *For a Boolean ring R, the following conditions are equivalent:*
(i) R is finite.
(ii) R is Noetherian.
(iii) R has finitely many maximal ideals.
If these equivalent conditions hold, then $R \cong (\mathbb{Z}/2\mathbb{Z})^n$, with $n = \log_2 \#R$.

Proof. That (i) $\implies$ (ii) is clear.
(ii) $\implies$ (iii): Since R is Noetherian and prime ideals are maximal, by the Akizuki-Hopkins Theorem (Theorem 8.33) R is Artinian. Thus by Theorem 8.35 R is a finite product of local Boolean rings, and thus finally by Proposition 9.5 $R \cong \bigoplus_{i=1}^n \mathbb{Z}/2\mathbb{Z}$.
(iii) $\implies$ (i): Suppose that R has precisely $N < \infty$ maximal ideals and suppose for a contradiction that R is infinite. Then we may choose $x \in R \setminus \{0, 1\}$, i.e., a nontrivial idempotent. This leads to a direct product decomposition $R = xR \times (1-x)R$. Here xR and $(1-x)R$ are subrings of R, hence at least one of them is an infinite Boolean ring. It follows that this decomposition process can be continued indefinitely, or more precisely until we get to the point of writing $R = \bigoplus_{i=1}^{N+1} R_i$ as a product of $N+1$ Boolean rings. For $i = 1, \ldots, N+1$, let $\mathfrak{m}_i$ be a maximal ideal of R_i. Then

for $i = 1, \ldots, N+1$, $\mathfrak{M}_i = \prod_{j \neq i} R_j \times \mathfrak{m}_i$ are distinct maximal ideals of R, which thus has at least $N+1$ maximal ideals, contradiction. □

Lemma 9.7. *Let $\mathfrak{m}$ be an ideal in the Boolean ring R. TFAE:*
(i) $\mathfrak{m}$ is maximal.
(ii) For all $x \in R$, either $x \in R$ or $1 - x \in R$ (and not both!).

Proof. $(i) \implies (ii)$: Of course no proper ideal in any ring can contain both x and $1 - x$ for then it would contain 1. To see that at least one must lie in $\mathfrak{m}$, it is certainly no loss to assume that x is neither 0 nor 1, hence $R = xR \times (1-x)R$. Recall that in a product $R_1 \times R_2$ of rings, every ideal I is itself a product $I_1 \times I_2$, where I_i is an ideal of R_i. Then $R/I \cong R_1/I_1 \times R_2/I_2$. So I is prime iff R/I is a domain iff either (i) I_1 is prime in R_1 and $I_2 = R_2$ or (ii) $I_1 = R_1$ and I_2 is prime in R_2. In particular, every maximal ideal of $R_1 \times R_2$ contains either R_1 or R_2: done. (i) $\implies$ (ii):[44] We prove the contrapositive: if $\mathfrak{m}$ is not maximal, there exists a maximal ideal $\mathfrak{M}$ properly containing $\mathfrak{m}$. Let $x \in \mathfrak{M} \setminus \mathfrak{m}$. Since $\mathfrak{M}$ is proper, it does not also contain $1 - x$, hence neither does the smaller ideal $\mathfrak{m}$. □

Exercise 9.14 (Kernel of a homomorphism): Let $f : R \to \mathbb{F}_2$ be a homomorphism of Boolean rings.
a) Show that $\operatorname{Ker} f$ is $\vee$-closed: if $x, y \in \operatorname{Ker} f$, then $x \vee y \in \operatorname{Ker} f$.
b) Show that $\operatorname{Ker} f$ is downward-closed: if $x \in \operatorname{Ker} f$ and $y \leq x$, then $y \in \operatorname{Ker} f$.
c) Explain why parts a) and b) are equivalent to showing that $\operatorname{Ker} f$ is an ideal of the Boolean ring R.
d) Show that $\operatorname{Ker} f$ is in fact a maximal ideal of R.
e) Conversely, for every maximal ideal $\mathfrak{m}$ of R, show that $R/\mathfrak{m} = \mathbb{F}_2$ and thus the quotient map $q : R \to R/\mathfrak{m}$ is a homomorphism from R to $\mathbb{F}_2$.

Exercise 9.15 (Shell of a homomorphism): Let $f : R \to \mathbb{F}_2$ be a homomorphism of Boolean rings. Define the **shell** $\operatorname{Sh} f$ to be $f^{-1}(1)$.
a) Show that $\operatorname{Sh} f$ is wedge-closed: if $x, y \in \operatorname{Sh} f$, so is $x \wedge y$.
b) Show that $\operatorname{Sh} f$ is upward-closed: if $x \in \operatorname{Sh} f$ and $x \leq y$, then $y \in \operatorname{Sh} f$.
c) A nonempty, proper subset of a Boolean algebra which is wedge-closed and upward-closed is called a **filter**, so by parts a) and b) $\operatorname{Sh} f$ is a filter on B. Show that in fact it is an **ultrafilter** on B, i.e., that it is not properly contained in any other filter. (Suggestion: use Lemma 9.7.)
d) Show that every ultrafilter on B is the shell of a unique homomorphism of Boolean algebras $f : B \to \mathbb{F}_2$.

9.4. **The Stone Representation Theorem.**

Let R be a Boolean ring. We would like to find an embedding of R into a Boolean ring of the form 2^X. The key point of course, is to conjure up a suitable set X. Can we find any clues in our prior work on Boolean rings?
indent Well, finite Boolean rings we understand: the proof of Proposition 9.6 gives us that every finite Boolean ring is of the form $\bigoplus_{i \in X} \mathbb{Z}/2\mathbb{Z}$, where the elements of X correspond to the maximal ideals of R. The isomorphism $\bigoplus_{i \in X} \mathbb{Z}/2\mathbb{Z} \cong 2^X$ amounts to taking each element x of R and recording which of the maximal ideals it lies in: namely, x lies in the ith maximal ideal $\mathfrak{m}_i$ of all elements having a zero

[44] Note that this direction holds in any ring.

in the ith coordinate iff its image in the quotient $R/\mathfrak{m}_i = \mathbb{Z}/2\mathbb{Z}$ is equal to 0.

This motivates the following construction. For any Boolean ring, let $M(R)$ be the set of all maximal ideals of R, and define a map $E : R \to M(R)$ by letting $E(x)$ be the set of maximal ideals of R which *do not* contain x. This turns out to be very fruitful:

Theorem 9.8. *(Stone Representation Theorem) Let R be a Boolean ring and $M(R)$ the set of maximal ideals. The map $E : R \to 2^{M(R)}$ which sends an element x of R to the collection of all maximal ideals of R which* do not *contain x is an injective homomorphism of Boolean rings. Therefore R is isomorphic to the Boolean ring associated to the algebra of sets $E(R) \subset 2^{M(R)}$.*

In particular this shows that every Boolean algebra is an algebra of sets.

Proof. Step 1: We check that the map E is a homomorphism of Boolean algebras. Above we saw $E(0) = \emptyset$; also $E(1) = M(R)$. Also, for $x, y \in R$, $E(xy)$ is the set of maximal ideals which do not contain xy; since maximal ideals are prime this is the set of maximal ideals which contain neither x nor y, i.e., $E(x) \cap E(y) = E(x) \cdot E(y)$. Finally, $E(x) + E(y) = E(x) \ \Delta \ E(y)$ is the set of maximal ideals which contain exactly one of x and y, whereas $E(x+y)$ is the set of maximal ideals not containing $x + y$. For $\mathfrak{m} \in M(R)$, consider the following cases:
(i) $x, y \in \mathfrak{m}$. Then $\mathfrak{m}$ is not in $E(x) \ \Delta \ E(y)$. On the other hand $x + y \in \mathfrak{m}$, so $\mathfrak{m}$ is not in $E(x + y)$.
(ii) Neither x nor y is in $\mathfrak{m}$. Certainly then $\mathfrak{m}$ is not in $E(x) \ \Delta \ E(y)$. On the other hand, remembering that $R/\mathfrak{m} \cong \mathbb{Z}/2\mathbb{Z}$, both x and y map to 1 in the quotient, so $x + y$ maps to $1 + 1 = 0$, i.e., $x + y \in \mathfrak{m}$, so $\mathfrak{m}$ is not in $E(x + y)$.
(iii) Exactly one of x and y lies in $\mathfrak{m}$. Then $\mathfrak{m} \in E(x) \ \Delta E(y)$ and as above, $x + y$ maps to 1 in $R/\mathfrak{m}$, so $x + y$ is not in $\mathfrak{m}$ and $\mathfrak{m} \in E(x + y)$.
Step 2: We show that the map E is injective. In other words, suppose we have two elements x and y of R such that a maximal ideal $\mathfrak{m}$ of R contains x iff it contains y. Then

$$(x) = \mathrm{rad}(x) = \bigcap_{\mathfrak{m} \in M(R) \ | \ x \in \ \mathfrak{m}} \mathfrak{m} = \bigcap_{\mathfrak{m} \in M(R) \ | \ y \in \ \mathfrak{m}} \mathfrak{m} = \mathrm{rad}(y) = (y).$$

So there exist $a, b \in R$ with $y = ax$, $x = by$, and then

$$x = by = by^2 = xy = ax^2 = ax = y.$$

□

Let us comment a bit on the proof. Although Step 1 is longer, it is clearly rather routine. They key is of course that E gives an embedding, which as we saw is equivalent to the much gutsier statement that an element of a Boolean ring is entirely determined by the family of maximal ideals containing it. From the standpoint of the more "conventional" rings one encounters in number theory and algebraic geometry, this is a very strange phenomenon. First of all, it can only be true in a ring R which has trivial unit group, since if u is a nontrivial unit of course we will not be able to distinguish 1 and u using ideals! Moreover it implies that every prinicpal ideal is radical, which is impossible in any integral domain. Finally it implies that every radical ideal is the intersection of the maximal ideals which

contain it, a property which we *will* meet later on the course: such rings are called **Jacobson rings**.

9.5. **Boolean Spaces.**

We will now digress a bit to talk (not for the first or last time!) about topological spaces. Following Bourbaki, for us **compact** means quasi-compact and Hausdorff. Further a **locally compact space** is a Hausdorff space in which each point admits a local base of compact neighborhoods. A subset of a topological space is **clopen** if it is both closed and open.

A topological space X is **totally disconnected** if the only connected subsets of X are the singleton sets $\{x\}$.[45] Note that a totally disconnected space is necessarily **separated** (older terminology that I am not fond of: T_1): i.e., singleton sets are closed. Indeed, the closure of every connected set is connected, so the closure of a non-closed point would give a connected set which is larger than a point. On the other hand a space X is **zero-dimensional** if it admits a base of clopen sets.

Proposition 9.9. *Let X be a locally compact space. Then X is totally disconnected iff it is zero-dimensional.*

Proof. Exercise! (This is not used in the sequel.) □

A space X is called **Boolean**[46] if it is compact and zero-dimensional; in particular a Boolean space admits a base for the topology consisting of *compact open* sets.

Exercise 9.16: a) A finite space is Boolean iff it is discrete.
b) A Boolean space is discrete iff it is finite.
c) An arbitrary direct product of Boolean spaces is Boolean.
d) The usual Cantor space is homeomorphic to a countably infinite direct product of copes of a discrete, two-point space and thus is a Boolean space.

Exercise 9.17: Show that a topological space is Boolean iff it is homeomorphic to an inverse limit of finite, discrete spaces.

To every topological space X we may associate a Boolean algebra: namely, the subalgebra of 2^X consisting of compact open subsets. Thus in particular we may associate a Boolean ring, say $\mathcal{C}(X)$, the **characteristic ring** of X. (We also ourselves to pass between $\mathcal{C}(X)$ and the associated Boolean algebra on the same set and call the latter the **characteristic algebra**.)

Exercise 9.18: Show that the assignment $X \mapsto \mathcal{C}$ extends to a contravariant functor from the category of topological spaces to the category of Boolean rings. (In other words, show that a continuous map $f : X \to Y$ of topological spaces induces a "pullback" homomorphism $\mathcal{C}(f) : \mathcal{C}(Y) \to \mathcal{C}(x)$ of Boolean rings.)

If X is itself a Boolean space, then the characteristic algebra $\mathcal{C}(X)$ is indeed *characteristic* of X in the following sense.

[45]Following Qiaochu Yuan, we take the convention that the empty space is *not* connected: it has zero connected components, not one!

[46]There are many synonyms: e.g. **Stone space**, **profinite space**.

Proposition 9.10. *Let X be a Boolean space, and let $\mathcal{A}$ be a Boolean algebra of subsets of X which is also a base for the topology of X. Then $\mathcal{A} = \mathcal{C}(X)$.*

Proof. By hypothesis the elements of $\mathcal{A}$ are open sets in X. Moreover, since $\mathcal{A}$ is closed under complementation, the elements are also closed. Thus $\mathcal{A} \subset \mathcal{C}(X)$.

Conversely, suppose $Y \in \mathcal{C}(X)$. Since Y is open and $\mathcal{A}$ is a base for the topology on X, for each $y \in Y$ there is $A_y \in \mathcal{A}$ with $y \in A_y \subset Y$. Thus $\{A_y\}_{y \in Y}$ is an open cover for Y. But Y is also closed in a compact space hence itself compact, so we may extract a finite subcover, say $Y = \bigcup_{i=1}^n A_{y_i}$. Since $\mathcal{A}$ is a subalgebra, it is closed under finite unions, so $Y \in \mathcal{A}$. Thus $\mathcal{C}(X) \subset \mathcal{A}$. □

To every Boolean ring R we may associate a Boolean space: namely there is a natural topology on $M(R)$, the set of maximal ideals of R, with respect to which $M(R)$ is a Boolean space. This topology can be described in many ways.

First Approach: by the Stone Representation Theorem we have an embedding $R \hookrightarrow 2^{M(R)}$ and thus every element $x \in R$ determines a function $x : M(R) \to \mathbb{F}_2$. We may endow $\mathbb{F}_2$ with the discrete topology (what else?) and then give $M(R)$ the **initial topology** for the family of maps $\{x : M(R) \to \mathbb{F}_2\}_{x \in R}$, that is the finest topology which makes each of these maps continuous.

Here is a more concrete description of this initial topology: for each $x \in R$, put

$$U_x = \{\mathfrak{m} \in M(R) \mid x \notin \mathfrak{m}\}$$

$$V_x = \{\mathfrak{m} \in M(R) \mid x \in \mathfrak{m}\}.$$

Then the topology in question is the one generated by $\{U_x, V_x\}_{x \in X}$.

Second Approach: for any Boolean ring R, to give a maximal ideal $\mathfrak{m}$ of R is equivalent to giving a homomorphism of Boolean rings $f : R \to \mathbb{F}_2$. Namely, to a maximal ideal $\mathfrak{m}$ we associate the quotient map, and to $f : R \to \mathbb{F}_2$ we associate the kernel $f^{-1}(0)$. In this way we get an embedding $\iota : M(R) \hookrightarrow 2^R$. Now we endow each copy of $\mathbb{F}_2$ with the discrete topology and 2^R with the product topology: this makes it into a Boolean space.

Lemma 9.11. *The image $\iota(M(R))$ of ι is a closed subspace of 2^R.*

Exercise 9.19: Prove Lemma 9.11.

Thus if we endow $M(R)$ with the topology it inherits via the embedding ι, it is itself a Boolean space.

Exercise 9.20: Show that the topology on $M(R)$ defined via Lemma 9.11 coincides with the initial topology on $M(R)$ defined above.

It turns out to be important to consider a distinguished base for the topology on $M(R)$, which we now define. Since for a prime ideal $\mathfrak{m}$ we have $xy \notin \mathfrak{m} \iff x \notin \mathfrak{m}$ and$y \notin \mathfrak{m}$, we have for all $x, y \in R$ that

$$U_x \cap U_y = U_{xy}.$$

Moreover, by Lemma 9.7, $M(R) \setminus V_x = U_x$. It follows that the $\{U_x\}_{x \in X}$ form a base of clopen sets for the topology on $M(R)$.

To show the utility of this base, let us use it to show directly that $M(R)$ is a Boolean space.

Hausdorff: Let $\mathfrak{m}_1$ and $\mathfrak{m}_2$ be distinct maximal ideals of R. Choose $x \in \mathfrak{m}_2 \setminus \mathfrak{m}_1$, so by Lemma 9.7 $1 - x \in \mathfrak{m}_1 \setminus \mathfrak{m}_2$. Thus $\mathfrak{m}_1 \in U_x$ $\mathfrak{m}_2 \in U_{1-x}$ and

$$U_x \cap U_{1-x} = U_{x(1-x)} = U_0 = \varnothing,$$

so we have separated $\mathfrak{m}_1$ and $\mathfrak{m}_2$ by open sets.

Quasi-compact: As is well-known, it is enough to check quasi-compactness of a space using covers by elements of any fixed base. We certainly have a preferred base here, namely $\{U_x\}_{x \in X}$, so let's use it: suppose that we have a collection $\{x_i\}_{i \in I}$ such that $\bigcup_{i \in I} U_{x_i} = M(R)$. Now again (and not for the last...) we exploit the power of DeMorgan:

$$M(R) = \bigcup_i U_{x_i} = \bigcup_i (M(R) \setminus V_{x_i}) = M(R) \setminus \bigcap_i V_{x_i},$$

so that $\bigcap_i V_{x_i} = \varnothing$. This means that there is no maximal ideal containing every x_i. But *that* means that the ideal generated by the x_i's contains 1: there exists a finite subset $J \subset I$ and $a_j \in R$ such that $\sum_j a_j x_j = 1$, and thus $\bigcap_{j \in J} V_{x_j} = \varnothing$: equivalently $\bigcup_{j \in J} U_{x_j} = M(R)$.

Thus we have shown that the correspondence $R \mapsto M(R)$ associates to every Boolean ring a Boolean topological space, its **Stone space**.

Exercise 9.21: Show that the assignment $R \mapsto M(R)$ extends to a functor from the category of Boolean rings to the category of Boolean spaces.

9.6. **Stone Duality.**

Theorem 9.12. *(Stone Duality): The functors $\mathcal{C}$ and M give a duality between the category of Boolean spaces and the category of Boolean algebras. More concretely:*
a) For every Boolean algebra B, the map $B \to \mathcal{C}(M(B))$ given by $x \in B \mapsto U_x$ is an isomorphism of Boolean algebras.
b) For every Boolean space X, the map $m : X \to M(\mathcal{C}(X))$ given by $x \in X \mapsto \mathfrak{m}_x := \{U \in \mathcal{C}(X) \mid x \notin U\}$ is a homeomorphism of Boolean spaces.

Proof. a) The map $e : x \in B \mapsto U_x \in 2^{M(B)}$ is nothing else than the embedding e of the Stone Representation Theorem. In particular it is an embedding of Boolean algebras. Its image $e(B)$ is a subalgebra of the characteristic algebra of the Boolean space $M(B)$ which is, by definition, a base for the topology of $M(B)$. By Proposition 9.10 we have $e(B) = \mathcal{C}(M(B))$ so e is an isomorphism of Boolean algebras.
b) First we need to show that $\mathfrak{m}_x$ is a maximal ideal in the characteristic ring $\mathcal{C}(X)$. It seems more natural to show this on the Boolean algebra side, i.e., to show that $\mathfrak{m}_x$ is downward closed and union-closed. Indeed, $U \in \mathfrak{m}_x$ means $x \notin U$, so if $V \subset X$ then certainly $x \notin V$, i.e., $V \in \mathfrak{m}_x$; moreover, $U, V \in \mathfrak{m}_x \iff x \notin U$ and $x \notin V \iff x \notin U \cup V \iff U \cup V \in \mathfrak{m}_x$. Thus $\mathfrak{m}_x$ is an ideal of $\mathcal{C}(X)$. Applying Lemma 9.7, one easily sees that is maximal, so the map m is well-defined.
indent The injectivity of m follows immediately from the Hausdorff property of X.

Surjectivity: Let $\mathfrak{m} \in M(\mathcal{C}(X))$. By Exercise X.X, we may identify $\mathfrak{m}$ with a

homomorphism of Boolean algebras $f_{\mathfrak{m}} : \mathcal{C}(X) \to \mathbb{F}_2$. Let $\mathcal{F} = f_{\mathfrak{m}}^{-1}(1)$ be the shell of $f_{\mathfrak{m}}$, an ultrafilter on the Boolean algebra of sets $\mathcal{C}(X)$. In particular $\mathcal{F}$ is wedge-closed, i.e., it is a family of clopen subsets of the compact space X satisfying the finite intersection property. Therefore there exists $x \in \bigcap_{U \in \mathcal{F}} U$. On the other hand, the collection $\mathcal{F}_x$ of all clopen sets in X containing x is also a filter on $\mathcal{C}(X)$ with $\mathcal{F} \subset \mathcal{F}_x$. But since $\mathcal{F}$ is an *ultra*filter – i.e., a maximal filter – we have $\mathcal{F} = \mathcal{F}_x$. Thus $\mathfrak{m}$ and $\mathcal{F}_x$ are respectively the kernel and shell of the homomorphism $f : \mathcal{C}(X) \to \mathbb{F}_2$, so

$$\mathfrak{m} = \mathcal{C}(X) \setminus \mathcal{F}_x = \{U \in \mathcal{C}(X) \mid x \notin U\} = m(x).$$

Finally, since m is surjective, we have that for each $A \in \mathcal{C}(X)$,

$$\{U \in M(\mathcal{C}(X)) \mid A \in U\} = \{m(x) \mid x \in A\},$$

so that m maps the base $\mathcal{C}(X)$ for the topology on X onto the base $\mathcal{C}(M(\mathcal{C}(X)))$. □

Exercise 9.22: Let X be a topological space, and let $C(X, 2)$ be the ring of all continuous functions $f : X \to \mathbb{F}_2$ ($\mathbb{F}_2$ being given the discrete topology).
a) Show that $C(X, 2)$ is a Boolean ring.
b) Suppose that $X = M(R)$ is the maximal ideal space of the Boolean ring R. Show that $C(X, 2)$ is canonically isomorphic to R itself. Thus every Boolean ring *is* the ring of continuous Boolean-valued functions on its Stone space of maximal ideals.

9.7. **Topology of Boolean Rings.**

Proposition 9.13. *Let R be a Boolean ring and $\mathfrak{m}$ a maximal ideal of R. TFAE:*
(i) $\mathfrak{m}$ is an isolated point in the Stone space $M(R)$.
(ii) $\mathfrak{m} = Rx$ is a principal ideal.

Exercise 9.23: Prove Proposition 9.13.

A Boolean ring R is **atomic** if for every $x \neq 1$ there exists a principal maximal ideal $\mathfrak{m}$ with $x \in \mathfrak{m}$.

Exercise 9.24: For any nonempty set S, show that $2^S = \prod_{s \in S} \mathbb{Z}/2\mathbb{Z}$ is atomic.

A Boolean ring is called **atomless** if it contains no maximal principal ideals.

Exercise 9.25: Show that a Boolean algebra B is atomless if for all $x \in B$, if $x < 1$, there exists $y \in B$ with $x < y < 1$.

Proposition 9.14. *A Boolean ring R is atomless iff its Stone space $M(R)$ is* ***perfect****, i.e., without isolated points.,*

Exercise 9.26: Prove Proposition 9.14.

Corollary 9.15. *Any two countably infinite atomless Boolean rings are isomorphic.*

Exercise 9.27: Prove Corollary 9.15. (Suggestion: show that the Stone space of any countably infinite atomless Boolean ring is isomorphic to the Cantor set.)

Exercise 9.28 (for those who know some model theory):
a) Show that there is a first order theory in the language $(\vee, \wedge, *, 0, 1)$ whose models

are precisely the atomless Boolean algebras.
b) Use Vaught's Test to show that this theory is complete.

Exercise 9.29: Let S be a nonempty set and consider $R = 2^S = \prod_{s \in S} \mathbb{Z}/2\mathbb{Z}$.
a) Show that there is a natural bijective correspondence between elements of S and *principal* maximal ideals of R.
b) Deduce that there is an embedding $\iota : S \hookrightarrow M(R)$ such that the induced topology on S is discrete.
c) Show that $\iota(S)$ is dense in $M(R)$. (Hint: R is atomic.)
d) Show that ι is a homeomorphism iff S is finite.
e)* Show that ι is the **Stone-Cech compactification** of the discrete space S.

10. Associated Primes and Primary Decomposition

10.1. **Associated Primes.**

Let M be an R-module. A prime ideal $\mathfrak{p}$ of R is an **associated prime** of M if there is $m \in M$ with $\mathfrak{p} = \operatorname{ann} m = \{x \in R \mid xm = 0\}$. The set of associated primes of M is denoted (unfortunately) by $\operatorname{Ass} M$.

Thus when R is a domain and M is torsionfree, (0) is the only associated prime of M. In particular this holds for ideals of R. We hope this motivates the following definition: for an ideal I of a ring R, the associated primes of the ideal I are the associated primes of the module R/I.

Proposition 10.1. *Let M be an R-module and $\mathfrak{p}$ a prime ideal of R. TFAE:*
(i) $\mathfrak{p} \in \operatorname{Ass} M$.
(ii) There is an injection of R-modules $R/\mathfrak{p} \hookrightarrow M$.

Proof. (i) $\implies$ (ii): Let $\mathfrak{p} \in \operatorname{Ass} M$, and let $m \in M$ be such that $\mathfrak{p} = \operatorname{ann} m$. Define $\iota : R \to M$ by $x \mapsto xm$. Then $\operatorname{Ker} \iota = \mathfrak{p}$, so ι gives an injection from $R/\mathfrak{p}$ to M.
(ii) $\implies$ (i): If $\iota : R/\mathfrak{p} \hookrightarrow M$, let $m = \iota(1 + \mathfrak{p})$. Then $\mathfrak{p} = \operatorname{ann} m$. □

We immediately deduce:

Corollary 10.2. *If $N \subset M$ are R-modules, then $\operatorname{Ass} N \subset \operatorname{Ass} M$.*

Proposition 10.3. *For a prime ideal $\mathfrak{p}$ of R, $\operatorname{Ass} R/\mathfrak{p} = \{\mathfrak{p}\}$.*

Proof. Proposition 10.1 gives $\mathfrak{p} \in \operatorname{Ass} R/\mathfrak{p}$. Conversely, suppose there is $x \in R$ with $\operatorname{ann}(x + \mathfrak{p}) = \mathfrak{q}$ a prime ideal. Since $\mathfrak{p}$ is prime $y \in \mathfrak{q} \iff yx \in \mathfrak{p} \iff y \in \mathfrak{p}$. □

For an R-module M, a **zero divisor** of M is an element $x \in R$ such that $xm = 0$ for some $m \in M^\bullet$. We write $ZD(M)$ for the set of all zero divisors of M.

Proposition 10.4. *For a nonzero R-module M, let $\mathcal{F} = \{\operatorname{ann} m \mid m \in M^\bullet\}$.*
a) Every maximal element of $\mathcal{F}$ is a prime ideal.
b) If R is Noetherian, then $\operatorname{Ass} M \neq \varnothing$.

Proof. a) Let I be an ideal of R of the form $\operatorname{ann} m$ for some $x \in M^\bullet$ and not properly contained in $\operatorname{ann} x'$ for any $x' \in M^\bullet$. Let $a, b \in R$ be such that $ab \in I$ but $b \notin I$. Then $bx \in M^\bullet$. Since $0 = abx = a(bx)$, $a \in \operatorname{ann}(bx)$. But clearly $I = \operatorname{ann} x \subset \operatorname{ann}(bx)$, so by maximality of I we have $I = \operatorname{ann}(bx)$ and thus $a \in I$.
b) If $M \neq 0$, then $\mathcal{F}$ is a nonempty family of ideals in a Noetherian ring so has a maximal element. Apply part a). □

Exercise: a) Let $X \subset M$ be a nonempty subset such that $RX \subset X$. Show that the proof of Proposition 10.4 immediately adapts to show that a maximal element among annihilators of nonzero elements of X is prime.
b) Deduce part a) from the Lam-Reyes Prime Ideal Principle.

Proposition 10.5. *Let M be an R-module.*
a) We have $\bigcup_{\mathfrak{p} \in \operatorname{Ass} M} \mathfrak{p} \subset ZD(M)$.
b) If R is Noetherian, then $\bigcup_{\mathfrak{p} \in \operatorname{Ass} M} \mathfrak{p} = ZD(M)$.

Proof. a) If $\mathfrak{p} = \operatorname{ann} m$, then $xm = 0$ for all $x \in \mathfrak{p}$, so $\mathfrak{p} \subset ZD(M)$.
b) Let $x \in ZD(M)$, so that there is $m \in M^\bullet$ with $xm = 0$. By Proposition 10.4 applied to $N = \langle m \rangle$, there is $\mathfrak{p} \in \operatorname{Ass} N$, i.e., there is $y \in R$ such that $ym \neq 0$ and $\mathfrak{p} = \operatorname{ann} ym$. Since $xm = 0$, $xym = 0$ and $x \in \mathfrak{p}$. By Proposition 10.2 $\mathfrak{p} \in \operatorname{Ass} M$ and thus $x \in \bigcup_{\mathfrak{p} \in \operatorname{Ass} M} \mathfrak{p}$. □

Proposition 10.6. *Let $N \subset M$ be R-modules. Then:*
a) $\operatorname{Ass} M \subset \operatorname{Ass} N \cup \operatorname{Ass} M/N$.
b) $\operatorname{Ass}\left(\bigoplus_{i \in I} M_i\right) = \bigcup_{i \in I} \operatorname{Ass} M_i$.

Proof. a) For $\mathfrak{p} \in \operatorname{Ass} M$, let $\iota : R/\mathfrak{p} \subset M$ be an R-module monomorphism. Put $H = \iota(R/\mathfrak{p})$ and $L = H \cap N$.
Case 1: Suppose $L = 0$. Then the natural map $\alpha : H \to M/N$ is a monomorphism, so $\alpha \circ \iota : R/\mathfrak{p} \to M/N$ is a monomorphism and $\mathfrak{p} \in \operatorname{Ass} M/N$.
Case 2: Let $x \in L^\bullet$. Then $x \in H^\bullet \cong (R/\mathfrak{p})^\bullet$, so $\operatorname{ann} x = \mathfrak{p}$. Since $x \in N$, $\mathfrak{p} \in \operatorname{Ass} N$.
b) Put $M = \bigoplus_{i \in I} M_i$. Since each M_i is a submodule of $\bigoplus_{i \in I} M_i$, $\bigcup_{i \in I} \operatorname{Ass} M_i \subset \operatorname{Ass} M$ follows from Proposition 10.2. The containment $\operatorname{Ass} M \subset \bigcup_{i \in I} \operatorname{Ass} M_i$ follows from part a) when I is finite. In the general case, let $\mathfrak{p} \in \operatorname{Ass} M$. Then there is an R-module monomorphism $\iota : R/\mathfrak{p} \hookrightarrow M = \bigoplus_{i \in I} M_i$. The image $\iota(R/\mathfrak{p})$ lies in the submodule generated by $\iota(1 + \mathfrak{p})$, hence lies in $\bigoplus_{i \in J} M_i$ for some finite subset $J \subset I$. This reduces us to the finite case. □

Theorem 10.7. *Let R be a Noetherian ring and M a nonzero, finitely generated R-module. a) There is a chain of submodules*

$$0 = M_0 \subsetneq M_1 \subsetneq \ldots \subsetneq M_n = M$$

such that for all $0 \leq i \leq n-1$ there is a prime ideal $\mathfrak{p}_i$ of R with $M_{i+1}/M_i \cong \mathfrak{p}_i$.
b) For any such chain, $\operatorname{Ass} M \subset \{\mathfrak{p}_1, \ldots, \mathfrak{p}_{n-1}\}$.
c) In particular, $\operatorname{Ass} M$ is finite.

Proof. a) By Proposition 10.5 M has an associated prime $\mathfrak{p}_1 = \operatorname{ann} m_1$. Put $M_0 = \{0\}$ and $M_1 = \langle m_1 \rangle$; note $M_1/M_0 = M_1 \cong R/\mathfrak{p}_1$. If $M_1 = M$ we're done; if not, M/M_1 is finitely generated and nonzero so has an associated prime $\mathfrak{p}_2 = \operatorname{ann}(m_2 + M_1)$. Put $M_2 = \langle m_1, m_2 \rangle$, so that $M_2/M_1 \cong R/\mathfrak{p}_2$. We continue in this way, getting an increasing chain of submodules M_i in M. Since M is Noetherian, we must have $M_n = M$ for some m.
b) By Proposition 10.3, for all $0 \leq i \leq n-1$ we have $\operatorname{Ass} M_{i+1}/M_i = \operatorname{Ass} R/\mathfrak{p}_i = \{\mathfrak{p}_i\}$. By Proposition 10.6 we have for all $0 \leq i \leq n-1$, $\operatorname{Ass} M_{i+1} \subset \operatorname{Ass} M_i \cup \{\mathfrak{p}_{i+1}\}$, and from this $\operatorname{Ass} M = \operatorname{Ass} M_n \subset \{\mathfrak{p}_1, \ldots, \mathfrak{p}_n\}$ follows.
c) This follows immediately. □

Corollary 10.8. *Let $(R, \mathfrak{m})$ be a Noetherian local ring. If $\mathfrak{m} \setminus \mathfrak{m}^2$ consists entirely of zero-divisors, then there is $x \in R^\bullet$ with $x\mathfrak{m} = 0$.*

Proof. If $\mathfrak{m} = 0$ we may take $x = 1$. Henceforth we assume $\mathfrak{m} \neq 0$, so by Nakayama's Lemma there is $a \in \mathfrak{m} \setminus \mathfrak{m}^2$. By Theorem 10.7 and Proposition 10.5, $\operatorname{Ass} R = \{\mathfrak{p}_1, \ldots, \mathfrak{p}_n\}$ is finite and $\operatorname{ZD}(R) = \bigcup_{i=1}^n \mathfrak{p}_i$. Thus by hypothesis

$$\mathfrak{m} \setminus \mathfrak{m}^2 \subset \bigcup_{i=1}^n \mathfrak{p}_i.$$

For $y \in \mathfrak{m}^2$ and $p \in \mathbb{Z}^+$, $a + y^p \in \mathfrak{m} \setminus \mathfrak{m}^2$, so by the Pigeonhole Principle there are $1 \leq p < q \in \mathbb{Z}^+$ such that $a + y^p, a + y^q \in \mathfrak{p}_i$ for some i. Then $y^p(1 - y^{q-p}) \in \mathfrak{p}_i$; since $y^{q-p} \in \mathfrak{m}$ and R is local, $1 - y^{q-p} \in R^\times$; thus $y^p \in \mathfrak{p}_i$ and, since $\mathfrak{p}_i$ is prime, $y \in \mathfrak{p}_i$. This shows

$$\mathfrak{m} \subset \bigcup_{i=1}^n \mathfrak{p}_i.$$

By Prime Avoidance (Lemma 8.45), there is at least one i such that $\mathfrak{m} \subset \mathfrak{p}_i$. By definition $\mathfrak{p}_i = \operatorname{ann} x$ for some $x \in R^\bullet$: we're done. □

Proposition 10.9. *Let $S \subset R$ be multiplicative.*
a) If M is an $S^{-1}R$-module, then $\operatorname{Ass}_R M = \operatorname{Ass}_{S^{-1}R} M$.
b) If M is an R-module, then

$$\operatorname{Ass}_R M \cap \operatorname{Spec} S^{-1}R \subset \operatorname{Ass}_{S^{-1}R} S^{-1}M.$$

c) If R is Noetherian and M is an R-module, then

$$\operatorname{Ass}_R M \cap \operatorname{Spec} S^{-1}R = \operatorname{Ass}_{S^{-1}R} S^{-1}M.$$

Let M be an R-module. A **weakly associated prime of M** is a prime ideal $\mathfrak{p}$ of R such that there is $x \in M$ with $\mathfrak{p} = r(\operatorname{ann} x)$. Thus the definition differs from the usual one in that we are permitted to pass from $\operatorname{ann} x$ to its radical. We denote by $\operatorname{weakAss} M$ the set of weakly associated primes of M.

Exercise: Show that for an R-module M and $\mathfrak{p} \in \operatorname{Spec} R$, TFAE:
(i) $\mathfrak{p}$ is weakly associated to M.
(ii) There is an ideal I of R with $r(I) = \mathfrak{p}$ and an R-module injection $R/I \hookrightarrow M$.

Exercise: Show that parts a) and b) of Proposition 10.9b) hold if we replace Ass by weakAss throughout.

Proposition 10.10. *Let M be an R-module.*
a) We have $\operatorname{Ass} M \subset \operatorname{weakAss} M$.
b) If R is Noetherian, then $\operatorname{Ass} M = \operatorname{weakAss} M$.

Proof. a) As the terminology suggests, this is immediate: if $\mathfrak{p} = \operatorname{ann} x$, then $\operatorname{ann} x$ is prime, hence radical, so $\mathfrak{p} = r(\operatorname{ann} x)$.
b) By Proposition 10.9 it is enough to show that $\mathfrak{p} \in \operatorname{Ass}_{R_\mathfrak{p}} M_\mathfrak{p}$: replacing R by $R_\mathfrak{p}$ we may assume R is Noetherian local with maximal ideal $\mathfrak{p}$. Since $\mathfrak{p} \in \operatorname{weakAss} M$, there is $x \in M$ with $r(\operatorname{ann} x) = \mathfrak{p}$. Since R is Noetherian, by Proposition 4.13g) we have that $\mathfrak{p}^n \subset \operatorname{ann} x$ for some $n \in \mathbb{Z}^+$. Again using the Noetherian hypothesis, the set $\{\operatorname{ann} y \mid y \in R \text{ is such that } \operatorname{ann} y \supset \operatorname{ann} x\}$ has a maximal element $\operatorname{ann} y$, and by Proposition 10.4, $\mathfrak{q} = \operatorname{ann} y$ is prime. Then we have $\mathfrak{p}^n \subset \operatorname{ann} x \subset \mathfrak{q}$, and since $\mathfrak{q}$ is prime and $\mathfrak{p}$ is maximal, we have $\mathfrak{q} = \mathfrak{p}$ and thus $\mathfrak{p} \in \operatorname{Ass} M$. □

Exercise: Let k be a field and $R = k[t_1, t_2, \ldots]$ be the polynomial ring in a countably infinite set of indeterminates over k. Let $I = \langle t_1^2, t_2^2, \ldots \rangle$, and let $\mathfrak{p} = r(I) = \langle t_1, t_2, \ldots \rangle$. Show that $\mathfrak{p} \in \operatorname{weakAss} R/I \setminus \operatorname{Ass} R/I$.

10.2. **The support of a module.**

For a module M over a ring R, we define its **support**

$$\operatorname{supp} M = \{\mathfrak{p} \in \operatorname{Spec} R \mid M_{\mathfrak{p}} \neq 0\}.$$

Proposition 10.11. *For a finitely generated R-module M,*

$$\operatorname{supp} M = \{\mathfrak{p} \in \operatorname{Spec} R \mid \mathfrak{p} \supset \operatorname{ann} M\}.$$

Proof. Write $M = \langle \omega_1, \ldots, \omega_n \rangle_R$. For $\mathfrak{p} \in \operatorname{Spec} R$, we have $\mathfrak{p} \in \operatorname{supp} M$ iff $M_{\mathfrak{p}} \neq 0$ iff there exists i such that the image of ω_i in $M_{\mathfrak{p}}$ is not zero iff there exists i such that $\operatorname{ann}(\omega_i) \subset \mathfrak{p}$ iff

$$\operatorname{ann} M = \bigcap_{i=1}^{n} \operatorname{ann}(\omega_i) \subset \mathfrak{p}.$$

□

Theorem 10.12. *Let M be an R-module.*
a) We have $\operatorname{weakAss} M \subset \operatorname{supp} M$.
b) If R is Noetherian, the minimal elements of $\operatorname{Ass} M$ *are precisely the minimal elements of* $\operatorname{supp} M$.
c) The minimal associated primes of R are precisely the minimal primes of R.

Proof. a) Let $\mathfrak{p} \in \operatorname{weakAss} M$. By Exercise X.X, there is an ideal I of R with $r(I) = \mathfrak{p}$ and an R-module embedding $R/I \hookrightarrow M$. Tensoring with the flat R-module $R_{\mathfrak{p}}$ gives an injection $R_{\mathfrak{p}}/IR_{\mathfrak{p}} \hookrightarrow M_{\mathfrak{p}}$. Since $r(I) = \mathfrak{p}$, $I \subset \mathfrak{p}$ and thus $IR_{\mathfrak{p}} \subset \mathfrak{p}R_{\mathfrak{p}} \subsetneq R_{\mathfrak{p}}$ and $M_{\mathfrak{p}} \supset R_{\mathfrak{p}}/IR_{\mathfrak{p}} \neq 0$.
b) Recall that under the Noetherian assumption $\operatorname{weakAss} M = \operatorname{Ass} M$.
Step 1: We claim that every prime in $\operatorname{supp} M$ contains an element of $\operatorname{Ass} M$. Indeed, let $\mathfrak{p} \in \operatorname{supp} M$, so $M_{\mathfrak{p}} \neq 0$. Since $R_{\mathfrak{p}}$ is Noetherian, by Proposition 10.4b) and 10.9c) we have

$$\varnothing \neq \operatorname{Ass}_{R_{\mathfrak{p}}} M_{\mathfrak{p}} = \operatorname{Ass}_R M \cap \operatorname{Spec} R_{\mathfrak{p}},$$

and an element of the latter set is precisely an associated prime $\mathfrak{q}$ of M with $\mathfrak{q} \subset \mathfrak{p}$.
Step 2: Let $\mathfrak{p} \in \operatorname{Ass} M$ be minimal, so by part a) $\mathfrak{p} \in \operatorname{supp} M$. If there were $\mathfrak{p}' \in \operatorname{supp} M$ with $\mathfrak{p}' \subsetneq \mathfrak{p}$ then there is no element in $\operatorname{Ass} M$ which is contained in $\mathfrak{p}'$, contradicting Step 1.
Step 3: Let $\mathfrak{p} \in \operatorname{supp} M$ be minimal. By Step 1, $\mathfrak{p}$ contains an element $\mathfrak{p}'$ of $\operatorname{Ass} M$, but since $\operatorname{Ass} M \subset \operatorname{supp} M$ and $\mathfrak{p}$ is minimal we must have $\mathfrak{p} = \mathfrak{p}'$.
c) Apply part b) to $M = R$. □

Theorem 10.13. *If R is Noetherian,* $\operatorname{MinSpec} R$ *is finite.*

Proof. Combine Theorem 10.7c) and Theorem 10.12c). □

Later we will give a second, quite diferent proof of Theorem 10.13: we will use topological methods!

10.3. **Primary Ideals.**

Recall that a proper ideal $\mathfrak{q}$ of a ring R is **primary** if for all $x, y \in R$, $xy \in \mathfrak{q}$ implies $x \in \mathfrak{q}$ or $y^n \in \mathfrak{q}$ for some $n \in \mathbb{Z}^+$.

Exercise 10.1: a) Show that a prime ideal is primary. (Trivial but important!)
b) Show that an ideal $\mathfrak{q}$ of R is primary iff every zerodivisor in $R/\mathfrak{q}$ is nilpotent.

Neither the definition or primary ideal nor the characterization given in the above exercise is particularly enlightening, so one natural question is: which ideals are primary? (And, of course, another natural question is: what's the significance of a primary ideal?) Here are some simple results which give some information on primary ideals, sufficient to determine all the primary ideals in some simple rings.

Proposition 10.14. *Let $\mathfrak{q}$ be an ideal in a ring R. If $r(\mathfrak{q}) = \mathfrak{m}$ is a maximal ideal, then $\mathfrak{q}$ is primary. In particular, any power of a maximal ideal is primary.*

Proof. Since $r(\mathfrak{q})$ is the intersection of all prime ideals containing $\mathfrak{q}$, if this intersection is a maximal ideal $\mathfrak{m}$, then $\mathfrak{m}$ is the unique prime ideal containing $\mathfrak{q}$ and $R/\mathfrak{q}$ is a local ring with $\mathrm{nil}(R/\mathfrak{q}) = J(R/\mathfrak{q}) = \mathfrak{m}/\mathfrak{q}$. In such a ring an element is a zero-divisor iff it is a nonunit iff it is nilpotent, so $\mathfrak{q}$ is primary. The "in particular" follows since by Proposition 4.13f), $r(\mathfrak{m}^n) = r(\mathfrak{m}) = \mathfrak{m}$. □

Proposition 10.15. *If $\mathfrak{q}$ is a primary ideal, then its radical $r(\mathfrak{q})$ is a prime ideal, the smallest prime ideal containing $\mathfrak{q}$.*

Proof. Let $xy \in r(\mathfrak{q})$, so that $(xy)^m = x^m y^m \in \mathfrak{p}$ for some $m \in \mathbb{Z}^+$. If x^m is in $\mathfrak{q}$ then $x \in r(\mathfrak{q})$, so assume that x^m is not in $\mathfrak{q}$. Then y^m is a zero divisor in $R/\mathfrak{q}$, so by definition of primary there exists $n \in \mathbb{Z}^+$ such that $(y^m)^n \in \mathfrak{q}$, and then $y \in r(\mathfrak{q})$. The second statement holds for any ideal I whose radical is prime, since $r(I)$ is the intersection of all prime ideals containing I. □

A primary ideal is said to be $\mathfrak{p}$-**primary** if its radical is the prime ideal $\mathfrak{p}$.

Lemma 10.16. *If $\mathfrak{q}_1, \ldots, \mathfrak{q}_n$ are $\mathfrak{p}$-primary ideals, then $\mathfrak{q} = \bigcap_{i=1}^n \mathfrak{q}_i$ is $\mathfrak{p}$-primary.*

Proof. Let x, y be elements of the ring R such that $xy \in \mathfrak{q}$ and $x \in R \setminus \mathfrak{q}$. Then for all $1 \leq i \leq n$, there exists $a_i \in \mathbb{Z}^+$ such that $y^{a_i} \in I_i$, and then $y^{\prod_{i=1}^n a_i} \in \mathfrak{q}$, so $\mathfrak{q}$ is primary. Moreover, by Proposition 4.13b),

$$r(\mathfrak{q}) = r(\bigcap_{i=1}^n \mathfrak{q}_i) = \bigcap_{i=1}^n r(\mathfrak{q}_i) = \bigcap_{i=1}^n \mathfrak{q} = \mathfrak{q}.$$

□

Exercise 10.2: Give an example of primary ideals $\mathfrak{q}, \mathfrak{q}'$ such that $\mathfrak{q} \cap \mathfrak{q}'$ is not primary.

Proposition 10.17. *If $\mathfrak{q}$ is a primary ideal, the quotient ring $R/\mathfrak{q}$ is connected.*

Proof. Indeed, a ring is disconnected if and only if it has an idempotent element e different from 0 or 1. Such an element is certainly not nilpotent $e^n = e$ for all n – but is a zero-divisor, since $e(1-e) = e - e^2 = 0$. □

Exercise 10.3: Let k be a field, let $R = k[x, y]$ and put $I = (xy)$. Show that I is not primary but "nevertheless" R/I is connected.

Example: We will find all primary ideals in the ring $\mathbb{Z}$ of integers. Evidently (0) is prime and hence primary. If $\mathfrak{q}$ is any nonzero primary ideal, then its radical $\mathfrak{p} = r(\mathfrak{q})$ is a nonzero prime ideal, hence maximal. So, combining Propositions 10.14 and 10.15 we find that a nonzero ideal in $\mathbb{Z}$ is primary iff its radical is maximal. Moreover, for any prime power (p^n), $r((p^n)) = r((p)) = (p)$ is maximal – we use here the elementary and (we hope) familiar fact that if p is a prime number, (p) is a prime ideal (Euclid's Lemma); such matters will be studied in more generality in §X.X on factorization – so (p^n) is a primary ideal. Conversely, if n is divisible by more than one prime power, then applying the Chinese Remainder Theorem, we get that $\mathbb{Z}/n$ is disconnected.

Exercise 10.4: a) Let R be an integral domain for which each nonzero ideal is a (finite, of course) product of maximal ideals. Use the above argument to show that an ideal $\mathfrak{q}$ of R is primary iff it is a prime power.
b) (For those who know something about PIDs) Deduce in particular that primary = prime power in any principal ideal domain.

Remark: Consider the following property of an integral domain:

(DD) Every ideal can be expressed as a product of prime ideals.

This is *a priori* weaker than the hypothesis of Exericse X.Xa). Later we will devote quite a lot of attention to the class of domains satisfying (DD), the **Dedekind domains**. Among their many properties is that a Dedekind domain is (either a field or) a domain in which each nonzero prime ideal is maximal. Thus in fact the hypothesis of Exercise 10.4a) is equivalent to assuming that R is a Dedekind domain.

Remark(ably): Another characterization theorem says that any Noetherian domain in which each primary ideal is a prime power is a Dedekind domain. In particular, any polynomial ring $k[x_1, \ldots, x_n]$ in $2 \leq n < \infty$ variables over a field admits primary ideals which are not prime powers.

Exercise 10.5: Let $R = Z[t]/(t^2 + 3)$ (or, equivalently, $\mathbb{Z}[\sqrt{-3}]$). Let $\mathfrak{q} = (2)$.
a) Show that there is a unique ideal $\mathfrak{p}_2$ with $R/\mathfrak{p}_2 = \mathbb{Z}/2\mathbb{Z}$. Evidently $\mathfrak{p}_2$ is maximal.
b) Show that $r(\mathfrak{q}) = \mathfrak{p}_2$, and deduce that I is primary.
c) Show that $\mathfrak{q}$ is not a prime power, and indeed, cannot be expressed as a product of prime ideals.

The ring R of Exercise 10.5 is a good one to keep in mind: it is simple enough to be easy to calculate with, but it already displays some interesting general phenomena. This is a Noetherian domain in which every nonzero prime ideal is maximal. It is therefore "close" to being a Dedekind domain but it does not satisfy one other property ("integral closure") which will be studied later. It will turn out to be an immediate consequence of the main result of this section that, notwithstanding the fact that there are ideals which do not factor into a product of primes, nevertheless

every proper ideal in $R = \mathbb{Z}[\sqrt{-3}]$ can be written as a product of *primary* ideals. This, finally, is some clue that the notion of a primary ideal is a fruitful concept. The following exercise gives an even simpler (and more explicit) example of a ring R and a primary ideal $\mathfrak{q}$ of R which is not a prime power.

Having seen examples of a primary ideals which are not prime powers, what about the converse? Is it at any rate the case that any prime power is a primary ideal? We know that this is indeed the case for powers of a maximal ideal. However, the answer is again negative in general:

Example (Atiyah-MacDonald, p. 51): Let k be a field; put $R = k[x, y, z]/(xy - z^2)$. Denote by $\overline{x}$, $\overline{y}$, and $\overline{z}$ the images of x, y, z in R. Put $\mathfrak{p} = \langle \overline{x}, \overline{z} \rangle$. Since $R/\mathfrak{p} = k[x, y, z]/(x, z, xy - z^2) = k[y]$ is a domain, $\mathfrak{p}$ is a prime ideal. Now consider the ideal $\mathfrak{p}^2$: we have $\overline{xy} = \overline{z}^2 \in \mathfrak{p}^2$, but $\overline{x} \notin \mathfrak{p}^2$ and $\overline{y} \notin \mathfrak{p} = r(\mathfrak{p}^2)$, so $\mathfrak{p}^2$ is not primary.

10.4. **Primary Decomposition, Lasker and Noether.**

Let R be a ring and I an ideal of R. A **primary decomposition** of I is an expression of I as a finite intersection of primary ideals, say $I = \bigcap_{i=1}^n \mathfrak{q}_i$.

An ideal which admits at least one primary decomposition is said to be **decomposable**. This is not a piece of terminology that we will use often, but the reader should be aware of its existence.

For any ring R, let us either agree that R itself admits the "empty" primary decomposition or that R has no primary decomposition (i.e., it doesn't matter either way) and thereafter restrict our attention to proper ideals.

It may not be too surprising that not every ideal in every ring admits a primary decomposition. Indeed, we will see later that if R is a ring for which (0) admits a primary decomposition, then the ring R has finitely many minimal primes.

The first important result in this area was proved by Emanuel Lasker in 1905, roughly in the middle of his 27 year reign as world chess champion. Here it is.

Theorem 10.18. *(Lasker* [Las05]*) Let R be a polynomial ring in finitely many variables over a field. Every proper ideal I of R admits a primary decomposition.*

Lasker's proof of this theorem was a long and intricate calculation. As we will shortly see, a broader perspective yields considerably more for considerably less effort. In Lasker's honor a ring R in which every proper ideal admits a primary decomposition is called a **Laskerian ring**.

Exercise 10.6: If R is Laskerian and I is an ideal of R, then R/I is Laskerian.

Combining Lasker's theorem with this Exercise, we get that every finitely generated algebra over a field admits a primary decomposition. This result is of fundamental (indeed, foundational) importance in algebraic geometry.

However, in 1921 Lasker's triumph was undeniably trumped by Emmy Noether.

To see how, we need one further concept. An ideal I is **irreducible** if whenever I is written as an intersection of two ideals – i.e., $I = J \cap K$ – then $I = J$ or $I = K$.

Exercise 10.7: Let I be a proper ideal in a principal ideal domain R. TFAE:
(i) I is primary.
(ii) I is irreducible.
(iii) I is a prime power: there exists a in R and $n \in \mathbb{Z}^+$ such that (a) is prime and $I = (a)^n = (a^n)$.

Proposition 10.19. *a) A prime ideal is irreducible.*
b) An irreducible ideal in a Noetherian ring is primary.

Proof. a) Let $\mathfrak{p}$ be a prime ideal, and write $\mathfrak{p} = I \cap J$. Since then $\mathfrak{p} \supset IJ$, by Proposition 4.9 we have $\mathfrak{p} \supset I$ or $\mathfrak{p} \supset J$; WLOG say $\mathfrak{p} \supset I$. Then $\mathfrak{p} = I \cap J \subset I \subset \mathfrak{p}$, so that we must have $I = \mathfrak{p}$.

b) By passage to the quotient, we may assume that the 0 ideal is irreducible and show that it is primary. So suppose $xy = 0$ and $x \neq 0$. Consider the chain of ideals

$$\operatorname{ann}(y) \subset \operatorname{ann}(y^2) \subset \ldots \subset \operatorname{ann}(y^n) \subset \ldots.$$

Since R is Noetherian, this chain stabilizes: there exists n such that $\operatorname{ann}(y^n) = \operatorname{ann}(y^{n+k})$ for all k. We claim that $(x) \cap (y^n) = 0$. Indeed, if $a \in (x)$ then $ay = 0$, and if $a \in (y^n)$ then $a = by^n$ for some $b \in R$, hence $by^{n+1} = ay = 0$, so $b \in \operatorname{ann}(y^{n+1}) = \operatorname{ann}(y^n)$, hence $a = by^n = 0$. Since the (0) ideal is irreducible, we must then have $y^n = 0$, and this shows that (0) is primary. □

Exercise:[47] Let k be a field, $R = k[x, y]$ and $I = \langle x^2, xy, y^2 \rangle$.
a) Show that I is primary. (Hint: use Proposition 10.14.)
b) Show that $I = \langle x, y^2 \rangle \cap \langle x^2, y \rangle$.
c) Deduce that I is an ideal in a (very nice) Noetherian domain which is primary but not irreducible.

Theorem 10.20. *(Noether) Any proper ideal in a Noetherian ring admits a primary decomposition.*

Proof. Let I be a proper ideal in the Noetherian ring R. We claim I is a finite intersection of *irreducible* ideals; in view of Proposition 10.19 this gives the desired result. To see this: suppose that the set of proper ideals which cannot be written as a finite intersection of irreducible ideals is nonempty, and choose a maximal element I. Then I is reducible, so we may write $I = J \cap K$ where each of J and K is strictly larger than I. But being strictly larger than I each of J and K can be written as a finite intersection of irreducible ideals, and hence so can I. Contradiction! □

In other words, a Noetherian ring is Laskerian. Therefore Lasker's Theorem is an immediate consequence of Noether's Theorem together with the Hilbert Basis Theorem, which we recall, was proved in 1888 and whose remarkably short and simple – but nonconstructive – proof engendered first controversy and later deep admiration. The same is true for Noether's theorem: it is from this theorem, and the ridiculous simplicity of its proof, that Noetherian rings get their name.

[47] This exercise is taken from a post of E. Merkulova on http://math.stackexchange.com/questions/28620

10.5. **Irredundant primary decompositions.**

If an ideal can be expressed as a product of prime ideals, that product is in fact unique. We would like to have similar results for primary decomposition. Unfortunately such a uniqueness result is clearly impossible. Indeed, if $I = \mathfrak{q}_1 \cap \ldots \cap \mathfrak{q}_n$ is a primary decomposition of I and $\mathfrak{p}$ is any prime containing I, then $\mathfrak{q}_1 \cap \ldots \cap \mathfrak{q}_n \cap \mathfrak{p}$ is also a primary decomposition, and clearly a different one if $\mathfrak{p} \neq \mathfrak{q}_i$ for any i. A proper ideal I may well be contained in infinitely many primes – e.g. by X.X this occurs with $I = (0)$ for any Noetherian domain of dimension at least 2 – so there may well be infinitely many different primary decompositions.

But of course throwing in extra primes is both frivolous and wasteful. The following definition formalizes the idea of a primary decomposition which is "frugal" in two reasonable ways.

A primary decomposition is said to be **irredundant**[48] (or **minimal**, or **reduced**) if both of the following properties hold:

(IPD1) For all $i \neq j$, $r(\mathfrak{q}_i) \neq r(\mathfrak{q}_j)$.
(IPD2) For all i, $\mathfrak{q}_i$ does not contain $\bigcap_{j \neq i} \mathfrak{q}_j$.

If wastefulness succeeds, so does frugality:

Lemma 10.21. *An ideal which admits a primary decomposition admits an irredundant primary decomposition.*

Proof. By Lemma 10.16, we may replace any collection of primary ideals $\mathfrak{q}_i$ with a common radical with their intersection and still have a primary ideal, thus satisfying (IPD1). Then if (IPD2) is not satisfied, there is some $\mathfrak{q}_i$ which contains the intersection of all the other $\mathfrak{q}_j$'s, hence it can be removed to obtain a primary decomposition satisfying (IPD1) and with a smaller number of primary ideals. Proceeding in this way we eventually arrive at an irredundant primary decomposition. □

The question is now to what extent an irredundant primary decomposition is unique. The situation here is significantly better: although the primary decomposition is not in all cases unique, it turns out that there are some important quantities which are defined in terms of a primary decomposition and which can be shown to be independent of the choice of irredundant decomposition, i.e., are invariants of the ideal. Such uniqueness results are pursued in the next section.

10.6. **Uniqueness properties of primary decomposition.**

Recall that for ideals I and J of a ring R, $(I : J) = \{x \in R \mid xJ \subset I\}$, which is also an ideal of R. We abbreviate $(I : (x))$ to $(I : x)$ and $((x) : J)$ to $(x : J)$.

Exercise 10.8: Show that for ideals I and J, $I \subset (I : J)$.

Lemma 10.22. *Let $\mathfrak{q}$ be a $\mathfrak{p}$-primary ideal and $x \in R$.*
a) If $x \in \mathfrak{q}$ then $(\mathfrak{q} : x) = R$.

[48]It is amusing to note that most dictionaries do not recognize "irredundant" as an English word, but mathematicians have been using it in this and other contexts for many years.

b) If $x \notin \mathfrak{q}$ then $(\mathfrak{q} : x)$ is $\mathfrak{p}$-primary.
c) If $x \notin \mathfrak{p}$ then $(\mathfrak{q} : x) = \mathfrak{q}$.

Proof. a) If $x \in \mathfrak{q}$ then $1(x) = x \subset \mathfrak{q}$, so $1 \in (\mathfrak{q} : x)$.
b) If $y \in (\mathfrak{q} : x)$, then $xy \in \mathfrak{q}$; by assumption $x \notin \mathfrak{q}$, so $y^n \in \mathfrak{q}$ for some n and thus $y \in r(\mathfrak{q}) = \mathfrak{p}$. So $\mathfrak{q} \subset (\mathfrak{q} : x) \subset \mathfrak{p}$; taking radicals we get $r((\mathfrak{q} : x)) = \mathfrak{p}$. Moreover, if $yz \in (\mathfrak{q} : x)$ with $y \notin (\mathfrak{q} : x)$, then $xyz = y(xz) \in \mathfrak{q}$, so $(xz)^n = x^n z^n \in \mathfrak{q}$ for some n, and $x^n \notin \mathfrak{q} \implies (z^m)^n \in \mathfrak{q}$ for some $n \in \mathbb{Z}^+$, thus $z^{mn} \in \mathfrak{q} \subset (\mathfrak{q} : x)$.
c) We have in all cases that $\mathfrak{q} \subset (\mathfrak{q} : x)$. If $x \notin \mathfrak{p} = r(\mathfrak{q})$ and $y \in (\mathfrak{q} : x)$, then $xy \in \mathfrak{q}$; since no power of x is $\mathfrak{q}$, we must have $y \in \mathfrak{q}$. □

Theorem 10.23. *(First Uniqueness Theorem) Let $I = \bigcap_{i=1}^n \mathfrak{q}_i$ be any irredundant primary decomposition of the ideal I. Let $\mathfrak{p}_i = r(\mathfrak{q}_i)$. Then the $\mathfrak{p}_i$'s are precisely the prime ideals of the form $r((I : x))$ as x ranges through elements of R. In particular, they are independent of the choice of irredundant primary decomposition.*

Proof. For $x \in R$ we have $(I : x) = (\bigcap_i \mathfrak{q}_i : x) = \bigcap_i (\mathfrak{q}_i : x)$, so

$$r((I : x)) = \bigcap_i r((q_i : x)) = \bigcap_{x \notin \mathfrak{q}_j} \mathfrak{p}_j$$

by Lemma 10.22. If $r(I : x)$ is prime, then $r(I : x) =$
p_j for some j. Conversely, for each i, by irredundancy of the decomposition there exists $x_i \in \bigcap_{j \neq i} \mathfrak{q}_j \setminus \mathfrak{q}_i$ and then the Lemma implies $r(I : x_i) = \mathfrak{p}_i$. □

Corollary 10.24. *Let R be Noetherian, and let $I \subsetneq R$ be a proper ideal. Let $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ be the radicals of the primary ideals in an(y) irredundant primary decomposition of I. Then*

$$\{\mathfrak{p}_1, \ldots, \mathfrak{p}_r\} = \operatorname{Ass} R/I.$$

Proof. By Theorem 10.23 the $\mathfrak{p}_i$'s are precisely the elements of $\operatorname{weakAss} R/I$. Since R is Noetherian, so is R/I and thus by Proposition 10.10b) $\operatorname{weakAss} R/I = \operatorname{Ass} R/I$. □

Proposition 10.25. *Let $I = \bigcap_{i=1}^n \mathfrak{q}_i$ be a primary decomposition of an ideal I, with $\mathfrak{p}_i = r(\mathfrak{q}_i)$. Then any prime ideal $\mathfrak{p}$ containing I contains $\mathfrak{p}_i$ for some i.*

Proof. If $\mathfrak{p} \supset I = \bigcap_i \mathfrak{q}_i$, then

$$\mathfrak{p} = r(\mathfrak{p}) \supset \bigcap_i r(\mathfrak{q}_i) = \bigcap_i \mathfrak{p}_i.$$

Since $\mathfrak{p}$ is prime, $\mathfrak{p} \supset \mathfrak{p}_i$ for some i. □

Exercise 10.9: Show that an infinite Boolean ring is not Laskerian.

Proposition 10.26. *Let $I \subset R$ be a decomposable ideal, $I = \bigcap_{i=1}^n \mathfrak{q}_i$ an irredundant primary decomposition, and $\mathfrak{p}_i = r(\mathfrak{q}_i)$. Then*

$$\bigcup_{i=1}^n \mathfrak{p}_i = \{x \in R : (I : x) \neq I\}.$$

In particular, if the zero ideal is decomposable, then the set of zero divisors of R is the union of the minimal associated primes of R.

Proof. By passage to the quotient ring R/I, we may assume that $I = 0$. Let $0 = \bigcap_{i=1}^r \mathfrak{q}_i$ be a primary decomposition, with $\mathfrak{p}_i = r(\mathfrak{q}_i)$. For $x \in R$, $((0) : x) \neq (0)$ iff x is a zero-divisor, so it suffices to show the last statement of the proposition, that the union of the minimal primes is the set of all zero-divisors. Let D be the set of all zero divisors, so from Exercise 3.X and the proof of Theorem 10.23 we have

$$D = r(D) = \bigcup_{0 \neq x} r((0 : x)) = \bigcup_{0 \neq x} \bigcap_{x \notin \mathfrak{q}_j} \mathfrak{p}_j \subset \bigcup_j \mathfrak{p}_j.$$

Conversely, by Theorem 10.23 each $\mathfrak{p}_i$ is of the form $r((0 : x))$ for some $x \in R$. □

Theorem 10.27. *(Second Uniqueness Theorem) Let I be an ideal of R, and let*

$$\bigcap_{i=1}^n \mathfrak{q}_i = I = \bigcap_{j=1}^m \mathfrak{r}_j$$

be two irredundant primary decompositions for an ideal I. By Theorem 10.23 we know that $m = n$ and that there is a reordering $\mathfrak{r}_1, \ldots, \mathfrak{r}_n$ of the $\mathfrak{r}_j$'s such that for $1 \leq i \leq n$, $r(\mathfrak{q}_i) = \mathfrak{p}_i = r(\mathfrak{r}_i)$. Moreover, if $\mathfrak{p}_i$ is minimal, then $\mathfrak{q}_i = \mathfrak{r}_j$.

In other words, the primary ideals corresponding to the minimal primes are independent of the primary decomposition.

We will use the technique of localization to prove this result, so first we need some preliminaries on the effect of localization on a primary decomposition.

Proposition 10.28. *Let R be a ring, $S \subset R$ a multiplicatively closed set, and $\mathfrak{q}$ be a $\mathfrak{p}$-primary ideal. Write $\iota : R \to S^{-1}R$ for the localization map.*
a) If $S \cap \mathfrak{p} \neq \emptyset$, then $\iota_*(\mathfrak{q}) = S^{-1}R$.
b) If $S \cap \mathfrak{p} = \emptyset$, then $\iota_*(\mathfrak{q})$ is $\iota_*(\mathfrak{p})$-primary, and $\iota^*(\iota_*(\mathfrak{q})) = \mathfrak{q}$.

Proof. a) If $x \in S \cap \mathfrak{p}$, then for some $n \in \mathbb{Z}^+$, $x^n \in S \cap \mathfrak{q}$, so $\iota_*(\mathfrak{q})$ contains a unit of $S^{-1}R$ and is therefore $S^{-1}R$. Part b) follows immediately from Proposition 7.2 and Proposition 7.4a). □

Proposition 10.29. *Let $S \subset R$ be a multiplicatively closed set, and let $I = \bigcap_{i=1}^n \mathfrak{q}_i$ be an irredundant primary decomposition of an ideal I. Put $\mathfrak{p}_i = r(\mathfrak{q}_i)$ and suppose that the numbering is such that $S \cap \mathfrak{p}_i = \emptyset$ for $i \leq m$ and $S \cap \mathfrak{p}_i \neq \emptyset$ for $i > m$. Then:*

$$\iota_*(I) = \bigcap_{i=1}^m \iota_*(\mathfrak{q}_i),$$

$$\iota^*\iota_*(I) = \bigcap_{i=1}^m \mathfrak{q}_i,$$

and both of these are irredundant primary decompositions.

Exercise 10.10: Prove Proposition 10.29.

Proof of Theorem 10.27: let $\mathfrak{p}_i$ be a minimal associated prime, and put $S = R \setminus \mathfrak{p}_i$. Certainly S is a multiplcatively closed set, and moreover by minimality $\mathfrak{p}_i$ is the

unique associated prime which is disjoint from S. Applying Proposition 10.29 to both primary decompositions gives

$$\mathfrak{q}_i = \iota^* \iota_*(I) = \mathfrak{r}_i.$$

□

10.7. **Applications in dimension zero.**

We now give the proof of the uniqueness portion of Theorem 8.35. Let $\mathfrak{m}_1, \ldots, \mathfrak{m}_n$ be the distinct maximal ideals of the Artinian ring R. As in the proof of Theorem 8.35a) there exists $k \in \mathbb{Z}^+$ such that $\prod_{i=1}^n \mathfrak{m}_i^k = \cap_{i=1}^n \mathfrak{m}_i^k = 0$. For each i, the radical $r(\mathfrak{m}_i^k)$ is the maximal ideal $\mathfrak{m}_i$, so by Proposition 10.14 each $\mathfrak{m}_i^k$ is an $\mathfrak{m}_i$-primary ideal. Thus $0 = \bigcap_{i=1}^n \mathfrak{m}_i^k$ is a primary decomposition of the zero ideal which is moreover immediately seen to be irredundant. Since all the primes $\mathfrak{m}_i$ are maximal, the desired uniqueness statement of Theorem 8.35b) follows from the Second Uniqueness Theorem (Theorem 10.27) for primary decompositions.

10.8. **Applications in dimension one.**

Let R be a one-dimensional Noetherian domain, and I a nonzero ideal. Then by Theorem 10.20, I has a primary decomposition: $I = \bigcap_{i=1}^n \mathfrak{q}_i$, where $\mathfrak{p}_i = r(\mathfrak{q}_i) \supset \mathfrak{q}_i \supset I$ is a nonzero prime ideal. But therefore each $\mathfrak{p}_i$ is maximal, so that the $\mathfrak{p}_i$'s are pairwise comaximal. By Proposition 4.16, so too are the $\mathfrak{q}_i$'s, so the Chinese Remainder Theorem applies to give

$$I = \bigcap_{i=1}^n \mathfrak{q}_i = \prod_{i=1}^n \mathfrak{q}_i,$$

and

$$R/I \cong \prod_{i=1}^n R/\mathfrak{q}_i.$$

Thus in this case we can decompose any proper ideal as a finite *product* of primary ideals and not just a finite intersection. Moreover, for $I \neq 0$, all the associated primes are minimal over I, so the Uniqueness Theorems (Theorems 10.23 and 10.27) simply assert that the ideals $\mathfrak{q}_i$ are unique. This observation will be very useful in our later study of ideal theory in one dimensional Noetherian domains.

11. Nullstellensätze

Let k be a field. By an **affine algebra over k** we simply mean a finitely generated k-algebra. Of all the various and sundry classes of commutative rings we have met and will meet later in these notes, affine algebras are probably the most important and most heavily studied, because of their connection to algebraic geometry.

11.1. **Zariski's Lemma.**

In 1947 Oscar Zariski published a short note [Zar47] proving the following result.

Theorem 11.1. *(Zariski's Lemma) Let k be a field, A a finitely generated k-algebra, and $\mathfrak{m} \in \operatorname{MaxSpec} A$. Then $A/\mathfrak{m}$ is a finite degree field extension of k.*

Exercise 11.1: Show that the following is an equivalent restatement of Zariski's Lemma: let K/k be a field extension such that K is finitely generated as a k-algebra. Then K/k is an algebraic field extension.

Notwithstanding its innocuous appearance, Zariski's Lemma is a useful result on affine algebras over any field. Further, when k is algebraically closed, it carries all of the content of Hilbert's Nullstellensatz, the main theorem of this section.

So how do we prove Zariski's Lemma?

Oh, let us count the ways! The literature contains many interesting proofs, employing an impressively wide range of ideas and prior technology. We will in fact give several different proofs during the course of these notes. Of course some pride of place goes to the *first proof* that we give, so after much thought (and after changing our mind at least once!) we have decided on the following.

11.1.1. *Proof of Zariski's Lemma via the Artin-Tate Lemma.*

As in Exercise 11.1, it suffices to prove the following: let K/k be a field extension which is finitely generated as a k-algebra. We claim K/k is algebraic.

Indeed, if not, let $x_1, \ldots, x_n$ be a transcendence basis for K/k ($n \geq 1$ since K/k is transcendental), put $k(x) = k(x_1, \ldots, x_n)$ and consider the tower of rings

$$k \subset k(x) \subset K. \tag{25}$$

To be sure, we recall the definition of a transcendence basis: the elements x_i are algebraically independent over k and $K/k(x)$ is algebraic. But since K is a finitely generated k-algebra, it is certainly a finitely generated $k(x)$-algebra and thus $K/k(x)$ is a finite degree field extension. Thus the Artin-Tate Lemma applies to (25): we conclude that $k(x)/k$ is a finitely generated k-algebra. But this is absurd. It implies the much weaker statement that $k(x) = k(x_1, \ldots, x_{n-1})(x_n)$ is finitely generated as a $k(x_1, \ldots, x_{n-1})[x_n]$-algebra, or weaker yet, that there exists some field F such that $F(t)$ is finitely generated as an $F[t]$-algebra: i.e., there exist finitely many rational functions $\{r_i(t) = \frac{p_i(t)}{q_i(t)}\}_{i=1}^N$ such that every rational function is a polynomial in the r_i's with k-coefficients. But $F[t]$ is a PID with infinitely many nonassociate nonzero prime elements q (e.g. adapt Euclid's argument of the infinitude of the primes), so we may choose a nonzero prime element q which does not divide $q_i(t)$ for any i. It is then clear that $\frac{1}{q}$ cannot be a polynomial in the $r_i(t)$'s: for instance, evaluation at a root of q in $\overline{F}$ leads to a contradiction. $\square$

Remark: The phenomenon encountered in the endgame of the preceding proof will be studied in great detail in §12. What we are actually showing is that for any field F, the polynomial ring $F[t]$ is not a **Goldman domain**, and indeed this is closely related to the fact that $\operatorname{Spec} F[t]$ is infinite. More on this later.

11.1.2. *McCabe's Proof of Zariski's Lemma.*

We will give one further proof of Zariski's Lemma now (and more later...), an extremely elegant and simple one due to J. McCabe [McC76].

Let K/k be a field extension which is finitely generated as a K-algebra, say by $x_1, \ldots, x_n$. Reorder the x_i's so that $x_1, \ldots, x_t$ are algebraically independent over k and $x_{t+1}, \ldots, x_n$ are algebraic over $k(x_1, \ldots, x_n)$. We may assume $t \geq 1$, for otherwise K/k is finitely generated algebraic field extension, hence of finite degree.

Let $S = k[x_1, \ldots, x_t]$, so S is a polynomial ring and *is not* a field. There is $y \in S^\bullet$ such that $yx_{t+1}, \ldots, yx_n$ are all integral over $S[\frac{1}{y}]$. We have $k \subset S[\frac{1}{y}]$ and $x_1, \ldots, x_t \in S[\frac{1}{y}]$, so $K = k[x_1, \ldots, x_n]$ is integral over $S[\frac{1}{y}]$. Since K is a field, by Proposition 1.6 so is $S[\frac{1}{y}]$.

Let $\mathfrak{m} \in \operatorname{MaxSpec} S$. Since $t \geq 1$, $\mathfrak{m} \neq (0)$, so let $f \in \mathfrak{m}^\bullet$. Then f is invertible in the field $S[\frac{1}{y}]$ so there is $g \in S$ and $N \in \mathbb{Z}^+$ such that $\frac{1}{f} = \frac{g}{y^N}$ and thus $y^N = fg$. Since $f \in \mathfrak{m}$ and maximal ideals are prime, $y \in \mathfrak{m}$. It follows that y lies in every maximal ideal of S, hence $1 + y$ lies in no maximal ideal and is thus a unit in S. But $S^\times = k[x_1, \ldots, x_n]^\times = k^\times$, so $1 + y \in k^\times$ and $y \in k^\bullet$. Thus $k[x_1, \ldots, x_t] = k[x_1, \ldots, x_t, \frac{1}{y}] = S[\frac{1}{y}]$ is a field: contradiction!

11.2. **Hilbert's Nullstellensatz.**

Let k be a field, let $R_n = k[t_1, \ldots, t_n]$, and write $\mathbb{A}^n$ for k^n. We introduce an antitone Galois connection (V, I) between subsets of R_n and subsets of $\mathbb{A}^n$. Namely:

For $S \subset \mathbb{A}^n$, we put

$$I(S) = \{f \in R_n \mid \forall x \in S,\ f(x) = 0\}.$$

In other words, $I(S)$ is the set of polynomials which vanish at every element of S. Conversely, for $J \subset R_n$, we put

$$V(J) = \{x \in \mathbb{A}^n \mid \forall f \in J,\ f(x) = 0\}.$$

This is nothing else than the Galois relation associated to the relation $f(x) = 0$ on the Cartesian product $R_n \times \mathbb{A}^n$.

As usual, we would like to say something about the induced closure operators on R_n and $\mathbb{A}^n$. First, for any subset S of $\mathbb{A}^n$, $I(S)$ is not just a subset but an ideal of R_n. In fact $I(S)$ is a radical ideal: indeed, if $f^n \in I(S)$ then f^n vanishes on every point of S, so f vanishes at every point of S.

This little bit of structure pulled from thin air will quicken the heart of any Bourbakiste. But beyond the formalism, the key question is: exactly which sets are closed? Without knowing this, we haven't proved the Nullstellensatz any more than the analogous formalities between sets and groups of automorphisms prove the Galois correspondence for Galois field extensions.

Indeed, an ideal I is radical if $f^n \in I$ implies $f \in I$. But if f^n vanishes identically on S, then so does f.

The closed subsets of $\mathbb{A}^n$ are closed under arbitrary intersections (including the "empty intersection": $\mathbb{A}^n = V((0))$ and under finite unions (including the "empty union": $\emptyset = V(\{1\}) = V(R_n)$, and therefore form the closed sets for a unique topology on $\mathbb{A}^n$, the **Zariski topology**.

Exercise 11.2: a) Prove these facts.
b) Show that the Zariski topology on $\mathbb{A}^n_{/k}$ coincides with the topology it inherits as a subset of $\mathbb{A}^n_{/\overline{k}}$.
c) Show that the Zariski topology is T_1: i.e., singleton subsets are closed.
d) Show that when $n = 1$, the Zariski topology is the coarsest T_1 topology on k: namely, the topology in which a proper subset is closed iff it is finite.
e) For any $n \geq 1$, show that the Zariski topology on k^n is discrete iff k is finite.
f) For any infinite field and $m, n \geq 1$, show that the Zariski topology on k^{m+n} is strictly finer than the product of the Zariski topologies on k^m and k^n.

Remark: It is often lamented that the Zariski topology (especially when $k = \mathbb{C}$) is so "coarse". It is true that it is much coarser than the "analytic topology" on k^n when k is a topological field (i.e., the product topology from the topology on k). But from an algebraic perspective the Zariski topology is if anything too fine: we will see why later on when we extend the topology to all prime ideals on an affine algebra. Moreover, the fact that the Zariski topology on $\mathbb{F}_q^n$ is discrete creates many geometric problems.

Exercise 11.3: Let k be a field, $n \in \mathbb{Z}^+$ as above. Explicitly compute the ideal $I(k^n)$, i.e., the set of all polynomials which vanish at *every* point of k^n. Do we necessarily have $I(k^n) = \{0\}$?

Lemma 11.2. *For $a = (a_1, \ldots, a_n) \in k^n$, put $\mathfrak{m}_a = \langle x_1 - a_1, \ldots, x_n - a_n \rangle$. Then:*
a) We have $R_n/\mathfrak{m}_a = k$. In particular $\mathfrak{m}_a$ is maximal.
b) $\mathfrak{m}_a = I(\{a\})$ is the ideal of all functions vanishing at a.
c) The assignment $a \mapsto \mathfrak{m}_a$ is a bijection from k^n to the set of all maximal ideals $\mathfrak{m}$ of R_n such that $R_n/\mathfrak{m} = k$.

Proof. Part a) is obvious (but important).
b) Certainly each $x_i - a_i$ vanishes at a, so $\mathfrak{m}_a \subset I(\{a\})$. But by part a) $\mathfrak{m}_a$ is a maximal ideal, whereas $1 \notin I(\{a\})$, so we must have $\mathfrak{m}_a = I(\{a\})$.
c) The mapping $a \mapsto \mathfrak{m}_a$ is an injection from k^n to the set of maximal ideals with residue field k. Conversely, let $\mathfrak{m}$ be an ideal of R_n with $R_n/\mathfrak{m} = k$. For $1 \leq i \leq n$ let a_i be the image of x_i in $R_n/\mathfrak{m} = k$. Then $\mathfrak{m} \supset \mathfrak{m}_a$ so we must have equality. □

We now pause for a very important definition. A ring R is a **Jacobson ring** if it is "sufficiently many maximal ideals": more precisely, such that every prime ideal $\mathfrak{p}$ of R is the intersection of the maximal ideals that contain it.

Exercise 11.4: a) Show that a ring R is a Jacobson ring iff for every ideal I, the intersection of all maximal ideals containing I is $\mathrm{rad}(I)$.
b) Show that every homomorphic image of a Jacobson ring is Jacobson.

Proposition 11.3. *(Rabinowitsch Trick* [Ra30]*) Let k be any field and $n \in \mathbb{Z}^+$.*
a) The ring $R = k[x_1, \ldots, x_n]$ is a Jacobson ring.
b) It follows that any affine algebra is a Jacobson ring.

Proof. a) It is sufficient to show that for each prime ideal $\mathfrak{p}$ of R and $a \in R \setminus \mathfrak{p}$, there exists a maximal ideal $\mathfrak{m}$ containing $\mathfrak{p}$ and not containing a.

To show this, put $R_a := R[\frac{1}{a}]$, and let $\mathfrak{p}_a = \mathfrak{p}R_a$ be the pushed forward ideal. Since $\mathfrak{p}$ does not meet the multiplicative set generated by a, $\mathfrak{p}_a$ is still prime in

R_a. Let $\mathfrak{m}_a$ be any maximal ideal of R_a conaining $\mathfrak{p}_a$, and let $\mathfrak{m} = \mathfrak{m}_a \cap R$ be its contraction to R: *a priori*, this is a prime ideal. There is an induced k-algebra embedding $R/\mathfrak{m} \hookrightarrow R_a/\mathfrak{m}_a$. But R_a is still a finitely generated algebra so by Zariski's Lemma (Theorem 11.1) $R_a/\mathfrak{m}_a$ is finite dimensional as a k-vector space, hence so is the subspace $R/\mathfrak{m}$. Thus the domain $R/\mathfrak{m}$ must be a field: let $x \in (R/\mathfrak{m})^\bullet$, and write out a linear dependence relation of minimal degree among the powers of x:

$$x^n + c_{n-1}x^{n-1} + \ldots + c_1 x + c_0,\ c_i \in k,\ c_0 \neq 0.$$

Thus

$$x\left(x^{n-1} + c_{n-1}x^{n-2} + \ldots + c_1\right) = \frac{-1}{c_0},$$

so x is invertible. Thus $\mathfrak{m}$ is the desired maximal ideal.
b) This follows immediately from Exercise 11.4. □

Remark: It seems that "J.L. Rabinowitsch", the author of [Ra30], is the same person as *George Yuri Rainich*, a distinguished Russian-American mathematician of the early twentieth century.

We prove one last fact before imposing the hypothesis that k is algebraically closed.

Proposition 11.4. *Let k be any field and J an ideal of $k[x] = k[x_1, \ldots, x_n]$. Then:*
a) $V(J) = V(\operatorname{rad} J)$.
b) For any subset $S \subset k^n$, $I(S)$ is a radical ideal.
v) $I(V(J))$ is a radical ideal containing $\operatorname{rad} J$.

Proof. The underlying mechanism here is the following truly basic observation: for $f \in k[x]$, $P \in k^n$ and $m \in \mathbb{Z}^+$, we have

$$f(P) = 0 \iff f^m(P) = 0.$$

a) Since $J \subset \operatorname{rad} J$ we have $V(J) \supset V(\operatorname{rad} J)$. Conversely, let $P \in V(J)$ and $f \in \operatorname{rad} J$. Then there exists $m \in \mathbb{Z}^+$ such that $f^m \in J$, so $f^m(P) = 0$ and thus $f(P) = 0$. It follows that $P \in V(\operatorname{rad} J)$.
b) Similarly, for any $f \in k[x]$ and $m \in \mathbb{Z}^+$, if $f^m \in I(S)$, then for all $P \in S$, $f^m(P) = 0$. But this implies $f(P) = 0$ for all $P \in S$ and thus $f \in I(S)$.
c) This follows immediately from parts a) and b) and the tautological fact that for any ideal J of $k[x]$, $I(V(J)) \supset J$. □

Finally we specialize to the case in which the field k is algebraically closed. We have done almost all the work necessary to establish the following fundamental result.

Theorem 11.5. *(Hilbert's Nullstellensatz) Let k be an algebraically closed field, let $k[x] = k[x_1, \ldots, x_n]$. Then:*
a) I induces a bijective correspondence between the singleton sets of k^n and the maximal ideals: $a \in k^n \mapsto \mathfrak{m}_a = \langle x_1 - a_1, \ldots, x_n - a_n \rangle$.
b) For any Zariski-closed subset $S \subset k^n$, $V(I(S)) = S$.
c) For any ideal J of R_n, $I(V(J)) = \operatorname{rad}(J)$.
*Thus there is an inclusion-reversing, bijective correspondence between Zariski-closed subsets of k^n and **radical** ideals of $k[x]$.*

Proof. a) Let $\mathfrak{m}$ be a maximal ideal of $k[x]$. By Theorem 11.1, the residue field $k[x]/\mathfrak{m}$ is a finite degree extension of k. Since k is algebraically closed, this forces $k[x]/\mathfrak{m} = k$, and now Lemma 11.2 applies.

b) There is no content here: it is part of the formalism of Galois connections.
c) By Proposition 11.4, it is no loss of generality to assume that J is a radical ideal. Further, by Proposition 11.3, $k[x]$ is a Jacobson ring, so any radical ideal J is the intersection of the maximal ideals $\mathfrak{m}$ containing it. This is true over any field k. But combining with part a), we get that J is an intersection of maximal ideals of the form $\mathfrak{m}_a$ for certain points $a \in k^n$. Since $\mathfrak{m}_a = I(\{a\})$, $J \subset \mathfrak{m}_a$ iff every element of J vanishes at a, in other words iff $a \in V(J)$. Thus J is equal to the set of all polynomials $f \in R_n$ which vanish at every point of $V(J)$: $J = I(V(J))$! □

Exercise 11.5: Let k be any field. Show that if either part a) or part c) of Theorem 11.5 holds for the rings $k[x_1, \ldots, x_n]$, then k is algebraically closed. (Hint: in fact both parts fail for each $n \in \mathbb{Z}^+$, including $n = 1$.)

Exercise 11.6: Show that Zariski's Lemma in the case that k is algebraically closed is equivalent to the following statement: let $J = \langle f_1, \ldots, f_m \rangle$ be an ideal in $k[x_1, \ldots, x_n]$. Then either there exists a simultaneous zero a of $f_1, \ldots, f_m$ or there exist polynomials $g_1, \ldots, g_m$ such that $g_1 f_1 + \ldots + g_m f_m = 1$.

11.2.1. *The Semirational Nullstellensatz.*

Lemma 11.6. *(Lang's Lemma) Let k be a field, L an algebraically closed field, $\varphi : k \to L$ a field embedding, and R a finitely generated k-algebra. Then there is a homomorphism $\Phi : R \to L$ extending φ.*

Proof. Let $\mathfrak{m}$ be a maximal ideal of k. By Zariski's Lemma, $R/\mathfrak{m}$ is a finite degree field extension of k, so by basic field theory it embeds as a k-algebra into any algebraically closed field containing k. □

Remark: In [Lan02, § IX.1], Lang gives a direct proof of Lemma 11.6. It is easy to see that Lemma 11.6 implies Zariski's Lemma, so this gives another way to proceed.

Corollary 11.7. *Let k be a field, and let R be a domain which is finitely generated as a k-algebra. For any $y_1, \ldots, y_n \in R^\bullet$, there is a homomorphism $\psi : R \to \overline{k}$ such that $\psi(y_i) \neq 0$ for $1 \leq i \leq n$.*

Proof. Apply Lang's Lemma to the ring $R[\frac{1}{y_1}, \ldots, \frac{1}{y_n}]$. □

Corollary 11.8. *Let J be a proper ideal of $k[t_1, \ldots, t_n]$. Then there is $x \in \overline{k}^n$ such that for all $f \in J$, $f(x) = 0$.*

Proof. Let $\mathfrak{m}$ be a maximal ideal containing J. Zariski's Lemma gives a k-algebra embedding $\psi : k[t_1, \ldots, t_n]/\mathfrak{m} \hookrightarrow \overline{k}$. Let $(x_1, \ldots, x_n) = (\psi(t_1), \ldots, \psi(t_n))$. □

For an ideal J of $k[t_1, \ldots, t_n]$, let $V^a(J)$ be the set of $x = (x_1, \ldots, x_n) \in \overline{k}^n$ with $g(x) = 0$ for all $g \in J$. For $S \subset \overline{k}^n$, let $I(S)$ be the set of $g \in k[t_1, \ldots, t_n]$ such that $g(x) = 0$ for all $x \in S$. (Notice that we are extending to the algebraic closure on the affine space side but not on the ring side, hence the term "semirational".)

Theorem 11.9. *(Semirational Nullstellensatz) For all ideals J of $k[t_1, \ldots, t_n]$, we have $I(V^a(J)) = \operatorname{rad} J$.*

Proof. It is easy to see that $I(V^a(J))$ is a radical ideal containing J and thus $I(V^a(J)) \supset \operatorname{rad} J$. Conversely, let $f \in I(V^a(J))$. We must show that there is $N \in \mathbb{Z}^+$ such that $f^m \in J$. We may assume $f \neq 0$. We introduce a new indeterminate

t_{n+1} and let J' be the ideal $\langle J, 1 - t_{n+1}f \rangle$ of $k[t_1, \ldots, t_n, t_{n+1}]$. Let $Z \subset \overline{k}^n$ be the zero set of J, so $f|_Z \equiv 0$. Let $(x_1, \ldots, x_n, x_{n+1}) \in \overline{k}^{n+1}$. If $(x_1, \ldots, x_n) \notin Z$, then there is $g \in J \subset J'$ such that $g(x_1, \ldots, x_n, x_{n+1}) \neq 0$. If $(x_1, \ldots, x_n) \in Z$, then $1 - x_{n+1}f(x_1, \ldots, x_n) = 1 \neq 0$. By Corollary 11.8, $J' = k[t_1, \ldots, t_n, t_{n+1}]$, so there are $g_i \in k[t_1, \ldots, t_n, t_{n+1}]$ and $h_i \in J$ such that

$$1 = g_0(1 - t_{n+1}f) + g_1h_1 + \ldots + g_rh_r.$$

Now substitute $t_{n+1} = f^{-1}$ and multiply by an appropriate power f^N of f to clear denominators: we get $f^N \in J$. □

Exercise: The argument used in the proof of Theorem 11.9 is also called the **Rabinowitsch Trick**. Explain its relation to the proof of Proposition 11.3.

Exercise: Can you deduce Theorem 11.9 from Hilbert's Nullstellensatz?

11.3. **The Real Nullstellensatz.**

Recall that a field k is **formally real** if it is *not* possible to express -1 as a sum of (any finite number of) squares in k.

Exercise 11.7: Let k be a formally real field.
a) Show that k is not algebraically closed.
b) Show that any subfield of k is formally real.

A field k is **real closed** if it is formally real and admits no proper formally real algebraic extension. So e.g. $\mathbb{R}$ is real closed and $\mathbb{Q}$ is formally real but not real closed.

As we saw, even the weak Nullstellensatz fails for polynomial rings over any non-algebraically closed field k. However, when k is formally real one can find counterexamples to the Nullstellensatz of a particular form, and when k is real closed one can show that these counterexamples are in a certain precise sense the only ones, leading to an identification of the closure operation $J \mapsto I(V(J))$ in this case.

In any commutative ring R, an ideal I is **real** if for all $n \in \mathbb{Z}^+$ and $x_1, \ldots, x_n \in R$, $x_1^2 + \ldots + x_n^2 \in I$ implies $x_1, \ldots, x_n \in I$.

A domain R is **real** if the zero ideal is real.

Exercise 11.8: a) Show that a domain is real iff its fraction field is formally real.
b) Let R be a ring. Show that $\mathfrak{p} \in \operatorname{Spec} R$ is real iff the fraction field of $R/\mathfrak{p}$ is formally real.

Exercise 11.9: Show that any real ideal is a radical ideal.

So what? The following result gives the connection to the closure operator on ideals in $k[t_1, \ldots, t_n]$.

Proposition 11.10. *Let k be a formally real field and $k[x] = k[x_1, \ldots, x_n]$. For any ideal J of $k[x]$, its closure $\overline{J} = I(V(J))$ is a real ideal.*

Proof. Let $f_1, \ldots, f_m \in k[x]$ be such that $f_1^2 + \ldots + f_m^2 \in \overline{J}$. Then for any $P \in V(J)$, we have $f_1(P)^2 + \ldots + f_m(P)^2 = 0$. Since k is formally real, this implies $f_1(P) = \ldots = f_m(P)$, and thus $f_1, \ldots, f_m \in I(V(J)) = \overline{J}$. □

Exercise: Find a real prime ideal $\mathfrak{p} \in \mathbb{Q}[t]$ which is not closed.

For an ideal I of a ring R, define the **real radical**

$$\mathbb{R}\operatorname{ad}(I) = \{x \in R \mid \exists n \in \mathbb{Z}^+ \; \exists b_1, \ldots, b_m \in R \mid x^{2n} + b_1^2 + \ldots + b_m^2 \in I\}.$$

Proposition 11.11. [BCR, Prop. 4.1.7] *Let I be an ideal in a ring R.*
a) A real ideal J contains I iff $J \supset \mathbb{R}\operatorname{ad}(I)$ i.e., $\mathbb{R}\operatorname{ad}(I)$ is the unique minimal real ideal containing I.
b) $\mathbb{R}\operatorname{ad}(I)$ is equal to the intersection of all real prime ideals $\mathfrak{p} \supset I$.
c) It follows that every real ideal is equal to the intersection of all the real prime ideals containing it.

Remark: If there are no real prime ideals containing I, then the intersection over this empty set is taken to be R.

Proof. Step 1: we show that $\mathbb{R}\operatorname{ad}(I)$ is an ideal. The only nonobvious part of this is closure under addition. Suppose that

$$a^{2n} + b_1^2 + \ldots + b_m^2, \; A^{2N} + B_1^2 + \ldots + B_M^2 \in I.$$

We may write

$$(a + A)^{2(n+N)} + (a - A)^{2(n+N)} = a^{2m}c + A^{2M}C,$$

with c, C sums of squares in R. Then

$$(a + A)^{2(n+N)} + (a - A)^{2(n+N)} + c(b_1^2 + \ldots + b_m^2) + C(B_1^2 + \ldots + B_M^2) \in I,$$

so $a + A \in \mathbb{R}\operatorname{ad}(I)$.
Step 2: $\mathbb{R}\operatorname{ad}(I)$ is a real ideal. Indeed, if $x_1^2 + \ldots + x_k^2 \in \mathbb{R}\operatorname{ad}(I)$, then there exists $n \in \mathbb{Z}^+$ and $b_1, \ldots, b_m \in R$ such that

$$(x_1^2 + \ldots + x_k^2)^{2m} + b_1^2 + \ldots + b_m^2 \in I;$$

for each $1 \leq i \leq k$, we may rewrite this as $x_i^{4m} + B_1^2 + \ldots + B_N^2$, so $x_i \in \mathbb{R}\operatorname{ad}(I)$.
Step 3: Since every real ideal is radical, it is clear that any real ideal containing I also contains $\mathbb{R}\operatorname{ad}(I)$.
Step 4: Let $a \in R \setminus \mathbb{R}\operatorname{ad}(I)$. By Zorn's Lemma, the set of real ideals containing I but not a has a maximal element, say J. We claim that J is prime. If not, there exist $b, b' \in R \setminus J$ such that $bb' \in J$. Then $a \in \mathbb{R}\operatorname{ad}(J + bR)$ and $a \in \mathbb{R}\operatorname{ad}(J + b'R)$, hence there are $j, j' \in J$ such that

$$a^{2m} + c_1^2 + \ldots + c_q^2 = j + bd, \; a^{2m'} + c_1'^2 + \ldots + c_q'^2 = j' + b'd'.$$

It follows that

$$a^{2(m+m')} + \text{ a sum of squares } = jj' + jb'd' + j'bd + bb'dd' \in J,$$

and thus $a \in \mathbb{R}\operatorname{ad}(J) = J$, contradiction. Thus $\mathbb{R}\operatorname{ad}(I)$ is the intersection of all real prime ideals containing I. □

Theorem 11.12. *(Artin-Lang Homomorphism Theorem)*
a) Let $k \hookrightarrow L$ be a map of real-closed fields, and let R be a finitely generated k-algebra. If there is a k-algebra homomorphism $\varphi : R \to L$, then there is a k-algebra homomorphism $\psi : R \to k$.
b) Let k be a real-closed field, and let R be a domain which is a finitely generated k-algebra. If R is real, there is a k-algebra homomorphism $\varphi : R \to k$.

Proof. a) For a proof using model-theoretic methods, see e.g. [BCR, Thm. 4.1.2].
b) The fraction field K of R is formally real: let L be a real closure of K. Apply part a) to the composite k-algebra homomorphism $\varphi : R \to K \to L$. □

Remark: For a direct algebraic proof of Theorem 11.12b), see e.g. [S, § 3.3].

Exercise: Let $R = \mathbb{R}[x,y]/(x^2 + y^2)$.
a) Show that R is a domain.
b) Show that R is not real.
c) Show that there is a (unique!) $\mathbb{R}$-algebra homomorphism $\varphi : R \to \mathbb{R}$.
(Thus the converse of Theorem 11.12b) does not hold.)

Remark: In [La53], Lang actually proved the following stronger result than Theorem 11.12b), which we state in more geometric language: the domain R above corresponds to an integral affine variety V over the real closed field k, and Lang showed that the function field $k(V)$ is formally real iff V has a *nonsingular* k-rational point.

Theorem 11.13. *(The Nullstellensatz for Real-Closed Fields) Let k be a real-closed field, and J an ideal in $k[t] = k[t_1, \ldots, t_n]$. Then $\overline{J} = \mathbb{R}\operatorname{ad}(J)$.*

Proof. Step 1: Suppose J is a real prime ideal. Let $R = k[t]/J$, and let K be the fraction field of R; by Exercise 11.8, K is formally real; let L be a real closure of K. For $f \in R \setminus J$, let S be the localization $R[\frac{1}{q(f)}]$, so $S \subset L$. By Theorem 11.12a) there is a k-algebra homomorphism $\psi : S \to k$; let $x = (\psi(\overline{t_1}), \ldots, \psi(\overline{t_n}))$. Then $x \in V(J)$ and $f(x) \neq 0$, so $f \notin I(V(J))$. It follows that $\overline{J} = I(V(J)) = J$.
Step 2: Suppose J is a real ideal, and let X_J be the set of all real prime ideals containing J. By Proposition 11.11c), $J = \bigcap_{\mathfrak{p} \in X_J} \mathfrak{p}$, and thus

$$\overline{J} = I(V(J)) = I(V(\bigcap_{\mathfrak{p} \in X_J} \mathfrak{p})) = I(\bigcup_{\mathfrak{p} \in X_J} V(\mathfrak{p})) = \bigcap_{\mathfrak{p} \in X_J} I(V(\mathfrak{p})) = \bigcap_{\mathfrak{p} \in X_J} \mathfrak{p} = J.$$

Step 3: Now let J be arbitrary. By Proposition 11.10, $\overline{J}$ is a real ideal containing J, so by Proposition 11.11a), $\mathbb{R}\operatorname{ad}(J) \subset \overline{J}$. On the other hand, part b) gives

$$\overline{J} \subset \overline{\mathbb{R}\operatorname{ad}(J)} = \mathbb{R}\operatorname{ad}(J),$$

so $\overline{J} = \mathbb{R}\operatorname{ad}(J)$. □

11.4. **The Combinatorial Nullstellensatz.**

In this section we describe one of the most recent Nullstellensätze, a celebrated result of Noga Alon that has served as a powerful technical tool and organizing principle in combinatorics and additive number theory (!).

Lemma 11.14. *(Alon-Tarsi) Let k be a field, $n \in \mathbb{Z}^+$, and $f(t) \in k[t] = k[t_1, \ldots, t_n]$; for $1 \leq i \leq n$, let d_i be the t_i-degree of f, let S_i be a subset of k with $\#S_i > d_i$, and let $S = \prod_{i=1}^n S_i$. If $f(x) = 0$ for all $x \in S$, then $f = 0$.*

Proof. We go by induction on n. The case $n = 1$ is truly basic: a nonzero univariate polynomial over a field has no more roots than its degree. Now suppose $n \geq 2$ and that the result holds for polynomials in $n-1$ variables. The basic idea is the identity $k[t_1, \ldots, t_{n-1}, t_n] = k[t_1, \ldots, t_{n-1}][t_n]$: thus we write

$$f = \sum_{i=0}^{t_n} f_i(t_1, \ldots, t_{n-1}) t_n^i$$

with $f_i \in k[t_1, \ldots, t_{n-1}]$. If $(x_1, \ldots, x_{n-1}) \in k^{n-1}$, the polynomial $f(x_1, \ldots, x_{n-1}, t_n) \in k[t_n]$ vanishes for all $\#S_n > d_n$ elements $x_n \in S_n$ and thus is identically zero, i.e., $f_i(x_1, \ldots, x_{n-1}) = 0$ for all $0 \leq i \leq t_n$. By induction, each $f_i(t_1, \ldots, t_{n-1})$ is the zero polynomial and thus f is the zero polynomial. □

Theorem 11.15. *(Combinatorial Nullstellensatz* [Al99]*) Let k be a field, $S_1, \ldots, S_n$ be nonempty finite subsets of k, and put $S = \prod_{i=1}^n S_i$. For $1 \leq i \leq n$, put*

$$g_i(t_i) = \prod_{s_i \in S_i} (t_i - s_i) \in k[t_i] \subset k[t] = k[t_1, \ldots, t_n]$$

and

$$\mathfrak{g} = \langle g_1(t_1), \ldots, g_n(t_n) \rangle.$$

Then

$$S = V(\mathfrak{g})$$

and

$$\overline{\mathfrak{g}} = I(V(\mathfrak{g})) = \mathfrak{g}.$$

Proof. That $S = V(\mathfrak{g})$ is immediate, as is $\mathfrak{g} \subset \overline{\mathfrak{g}}$. Conversely, suppose $f \in \overline{\mathfrak{g}} = I(S)$, i.e., $f(s) = 0$ for all $s = (s_1, \ldots, s_n) \in S$. We must show that there are polynomials $h_1(t), \ldots, h_n(t)$ such that $f(t) = \sum_{i=1}^n h_i(t) g_i(t)$.

For $1 \leq i \leq n$, put $d_i = \#S_i - 1$; we may write

$$g_i(t_i) = t_i^{d_i+1} - \sum_{j=0}^{d_i} g_{ij} t_i^j.$$

Observe that if $s_i \in S_i$, then $g_i(x_i) = 0$, i.e.,

$$x_i^{d_i+1} = \sum_{j=0}^{d_i} g_{ij} x_i^j. \tag{26}$$

Let $\overline{f}$ be the polynomial obtained from f by writing f as a sum of monomials and repeatedly substituting each instance of $t_i^{e_i}$ with $e_i > d_i$ with a k-linear combination of smaller powers of t_i using (26). Then $\overline{f}$ has degree at most d_i in t_i and $f - \overline{f}$ is of the form $\sum_{i=1}^n h_i g_i$. Further, for all $s = (s_1, \ldots, s_n) \in S$, $\overline{f}(s) = f(s) = 0$. Thus Lemma 11.14 applies to give $\overline{f} = 0$ and thus $f = \sum_{i=1}^n h_i g_i$. □

Exercise: a) Show that, in the notation of the proof of Theorem 11.13, the polynomials $h_1, \ldots, h_n$ satisfy $\deg h_i \leq \deg f - \deg g_i$ for all $1 \leq i \leq n$.
b) Show that the coefficients of $h_1, \ldots, h_n$ lie in the subring of k generated by the coefficients of $f, g_1, \ldots, g_n$.

Corollary 11.16. *(Polynomial Method) Let k be a field, $n \in \mathbb{Z}^+$, $a_1, \ldots, a_n \in \mathbb{N}$, and let $f \in k[t] = k[t_1, \ldots, t_n]$. We suppose:*
(i) $\deg f = a_1 + \ldots + a_n$.
(ii) The coefficient of $t_1^{a_1} \cdots t_n^{a_n}$ in f is nonzero.
Then, for any subsets $S_1, \ldots, S_n$ of k with $\#S_i > a_i$ for $1 \leq i \leq n$, there is $s = (s_1, \ldots, s_n) \in S = \prod_{i=1}^n S_i$ such that $f(s) \neq 0$.

Proof. It is no loss of generality to assume that $\#S_i = a_i + 1$ for all i, and we do so. We will show that if (i) holds and $f|_S \equiv 0$, then (ii) does *not* hold, i.e., the coefficient of $t_1^{a_1} \cdots t_n^{a_n}$ in f is 0.

Define, for all $1 \leq i \leq n$, $g_i(t_i) = \prod_{s_i \in S_i} t_i - s_i$. By Theorem 11.13 and the preceding exercise, there are $h_1, \ldots, h_n \in k[t]$ such that

$$f = \sum_{i=1}^n h_i g_i$$

and

$$\deg h_i \leq (a_1 + \ldots + a_n) - \deg g_i, \ \forall 1 \leq i \leq n,$$

so

$$\deg h_i g_i \leq \deg f. \tag{27}$$

Thus if $h_i g_i$ contains any monomial of degree $\deg f$, such a monomial would be of maximal degree in $h_i g_i = h_i \prod_{s_i \in S_i} (t_i - s_i)$ and thus be divisible by $t_i^{a_i+1}$. It follows that for all i, the coefficient of $t_1^{a_1} \cdots t_n^{a_n}$ in $h_i g_i$ is zero, hence the coefficient of $t_1^{a_1} \cdots t_n^{a_n}$ in f is zero. □

11.5. **The Finite Field Nullstellensatz.**

For a prime power q, let $\mathbb{F}_q$ be a finite field of cardinality q. We will characterize the closure operation $J \mapsto \overline{J} = I(V(J))$ for ideals in $\mathbb{F}_q[t] = \mathbb{F}_q[t_1, \ldots, t_n]$.

Let $I_0 = \langle t_1^q - t_1, \ldots, t_n^q - t_n \rangle$. Then the key observation is that for any ideal J of $\mathbb{F}_q[t]$, $\overline{J} \supset I_0$. Indeed, since $x^q = x$ for all $x \in \mathbb{F}_q$, the polynomials $t_1^q - t_1, \ldots, t_n^q - t_n$ each vanish at every point of $\mathbb{F}_q^n$, so $\overline{J} = I(V(J)) \supset I(\mathbb{F}_q^n) \supset I_0$. Since of course $\overline{J} \supset J$, it follows that for all ideals J of $k[t]$ we have

$$\overline{J} \supset J + I_0. \tag{28}$$

Proposition 11.17. *(Finite Field Weak Nullstellensatz) Let $\mathbb{F}_q$ be a finite field, and let $n \in \mathbb{Z}^+$. For $1 \leq i \leq n$, let $g_i = t_i^q - t_i \in \mathbb{F}_q[t_1, \ldots, t_n]$, and put $I_0 = \langle g_1, \ldots, g_n \rangle$. Then $I_0 = I(\mathbb{F}_q^n)$ is the ideal of all functions vanishing at every point of $\mathbb{F}_q^n$.*

Exercise: Deduce Proposition 11.17 from the Combinatorial Nullstellensatz.

Proposition 11.17 asserts that the containment of (28) is an equality when $J = (0)$. In fact, this holds in all cases.

Lemma 11.18. *Let J be an ideal of $\mathbb{F}_q[t_1, \ldots, t_n]$. If J contains the ideal $I_0 = \langle t_1^q - t_1, \ldots, t_n^q - t_n \rangle$, then $\operatorname{rad} J = J$.*

Proof. Suppose that for $x \in R$, there is $n \in \mathbb{Z}^+$ with $x^n \in J$. Then also $x^{q^n} = (x^{q^{n-1}})^q \in J$. By Corollary 11.17, for all $x \in R$, $f^q - f \in I_0 \subset J$: applying this with $f = x^{q^{n-1}}$, we find that $x^{q^n} - x \in I$ and thus $x^{q^n} - (x^{q^n} - x) = x \in J$. □

Theorem 11.19. *(Finite Field Nullstellensatz) For any ideal J of $R = \mathbb{F}_q[t_1, \ldots, t_n]$,*

$$\overline{J} = I(V(J)) = J + I_0 = \langle J, t_1^q - t_1, \ldots, t_n^q - t_n \rangle.$$

We will give two proofs: one using the Semirational Nullstellensatz, and one usin the Finite Field Weak Nullstellensatz.

Proof. By the Semirational Nullstellensatz (Theorem 11.9) and Lemma 11.18,

$$I(V^a(J + I_0)) = \operatorname{rad}(J + I_0) = J + I_0.$$

Since $V^a(I_0) = \mathbb{F}_q^n$, we have

$$I(V(J)) = I(V^a(J) \cap \mathbb{F}_q^n) = I(V^a(J) \cap V^a(I_0)) = I(V^a(J + I_0)) = J + I_0.$$

□

Proof. By (28) $\overline{J} \supset J + I_0$, it suffices to show that for all $J \supseteq I_0$, $J = \overline{J}$.

By Proposition 11.17, $I_0 = I(\mathbb{F}_q^n)$. For $P = (x_1, \ldots, x_n) \in \mathbb{F}_q^n$, let

$$\mathfrak{m}_P = I(\{P\}) = \langle t_1 - x_1, \ldots, t_n - x_n \rangle.$$

Thus $\{\mathfrak{m}_P\}_{P \in \mathbb{F}_q^n}$ are finitely many pairwise comaximal ideals with $I_0 = \bigcap_{P \in \mathbb{F}_q^n} \mathfrak{m}_P$. By the Chinese Remainder Theorem,

$$R/I_0 = R/\bigcap_{P \in \mathbb{F}_q^n} \mathfrak{m}_P \cong \prod_{P \in \mathbb{F}_q^n} R/\mathfrak{m}_P \cong k^{\#\mathbb{F}_q^n}. \tag{29}$$

The Correspondence Theorem now gives us canonical bijections between the set of ideals containing I_0 and the set of subsets of $\mathbb{F}_q^n$. Since every subset of the finite set $\mathbb{F}_q^n$ is Zariski closed, there are precisely $2^{\#\mathbb{F}_q^n}$ Zariski-closed subsets and therefore precisely $2^{\#\mathbb{F}_q^n}$ ideals J with $J = \overline{J}$. By (29) there are precisely $2^{\#\mathbb{F}_q^n}$ ideals J containing I_0, so we must have $J = \overline{J}$ for all such ideals. □

Remark: It seems that Theorem 11.19 was first stated and proved (as in the first proof above) in a 1991 technical report of R. Germundsson [Ge91].

11.6. **Terjanian's Homogeneous p-Nullstellensatz.**

Theorem 11.20. *(Homogeneous Nullstellensatz) Let k be an algebraically closed field, $m, n \in \mathbb{Z}^+$, and let $f_1, \ldots, f_m \in k[t_0, \ldots, t_n]$ be homogeneous polynomials of positive degree. If $m \leq n$, then there is $0 \neq x \in k^{n+1}$ such that*

$$f_1(x) = \ldots = f_n(x) = 0.$$

Proof. Step 0: It is no loss of generality to assume $m = n$, and we shall do so.
Step 1: Let $J = \langle f_1, \ldots, f_n \rangle$ and let

$$Z = V(J) = \{x \in k^{n+1} \mid f_1(x) = \ldots = f_n(x) = 0\}.$$

Since each f_i is homogeneous, $Z \supset \{0\}$; seeking a contradiction, we suppose $Z = \{0\}$. Then by Hilbert's Nullstellensatz, $\operatorname{rad} J = I(V(J)) = I(Z) = I(\{0\}) =$

$\langle t_0, t_1, \ldots, t_n \rangle$, i.e., there is $k \in \mathbb{Z}^+$ such that $t_0^k, \ldots, t_n^k \in J$, and thus there are polynomials g_{ij} such that for all $0 \leq i \leq n$,

$$t_i^k = \sum_{j=1}^n g_{ij} f_j$$

we may assume that each g_{ij} is homogeneous of degree $k - \deg f_j < k$.
Step 2: Let $B = k[t_0, \ldots, t_n]$, and let $m_1, \ldots, m_s$ be the monomials in B of degree less than $k(n+1)$. Put $A = k[f_1, \ldots, f_n]$ and $M = \langle m_1, \ldots, m_s \rangle_A$.
We CLAIM $M = k[t_0, \ldots, t_n]$.
SUFFICIENCY OF CLAIM: By the claim, $B = k[t_0, \ldots, t_n]$ is a finitely generated A-module, and thus B/A is an integral extension of domains. Let E and F be the fraction fields of A and B respectively; then F/E is an algebraic field extension. But $\operatorname{trdeg} E/k \leq n$ and $\operatorname{trdeg} F/k = n+1$, contradiction.
Step 3: PROOF OF CLAIM: It suffices to show that M contains all monomials $t_0^{a_0} \cdots t_n^{a_n}$. This is true by definition when $\delta = a_0 + \ldots + a_n < k(n+1)$; in general, we go by induction on δ. Suppose $\delta \geq k(n+1)$; then $a_i \geq k$ for some i; relabelling if necessary, we may assume that $a_0 \geq k$. Since $t_0^k = \sum g_{1j} f_j$, we have

$$t_0^{a_0} \cdots t_n^{a_n} = \sum_{j=1}^n (g_{1j} t_0^{v_0 - k} t_1^{v_1} \cdots t_n^{v_n}) f_j.$$

The coefficient of each f_j is homogeneous of degree less than δ, hence by induction is contained in M. Since M is an A-module, it follows that $t_0^{a_0} \cdots t_n^{a_n} \in M$. □

While Theorem 11.20 is a very classical result – it was used (not necessarily with proper justification) by 19th century mathematicians studying varieties in projective space – the following generalization is a 1972 theorem of G. Terjanian.

Let p be a prime number. We say that a field k is a **p-field** if every every finite extension l/k has degree a power of p.

Examples: a) Every separably closed field is a p-field.
b) Every real-closed field is a 2-field.
c) A perfect field k is a p-field iff $\operatorname{Gal}(\overline{k}/k)$ is a pro-p-group.

Theorem 11.21. *(Terjanian's Homogeneous p-Nullstellensatz) Let k be a p-field, and let $n \in \mathbb{Z}^+$. For $1 \leq i \leq n$, let $f_i \in k[t_0, \ldots, t_n]$ be homogeneous of degree d_i indivisible by p. Then there is $0 \neq x = (x_1, \ldots, x_n) \in k^n$ such that*

$$f_1(x) = \ldots = f_n(x) = 0.$$

The proof given in [Te72] was rather involved; a significantly simpler proof is given in [P], but even this involves more graded algebra than we wish to discuss here.
However, following Arason and Pfister [AP82] we will now deduce some striking consequences of the Homogeneous 2-Nullstellensatz for real-closed fields.

Exercise 11.10: Let k be a field of characteristic different from 2, and let $f \in k[t_1, \ldots, t_n]$. We say that f is an **odd polynomial** if $f(-t) = -f(t)$. Show that an odd polynomial is a sum of monomials each of odd total degree.

Theorem 11.22. *(Algebraic Borsuk-Ulam) Let k be a real closed field, $n \in \mathbb{Z}^+$, and for $1 \leq i \leq n$, let $f_i \in k[t_1, \ldots, t_{n+1}]$ be an* odd *polynomial: $f_i(-t) = -f_i(t)$. Then there is $x = (x_1, \ldots, x_{n+1}) \in k^{n+1}$ such that*

$$x_1^2 + \ldots + x_{n+1}^2 = 1, \ f_1(x) = \ldots = f_n(x) = 0.$$

Proof. So as to be able to apply Terjanian's Homogeneous p-Nullstellensatz, we homogenize: let t_0 be an additional indeterminate and let $\tilde{f}_i \in k[t_0, \ldots, t_{n+1}]$ be the unique homogeneous polynomial such that $\tilde{f}_i(1, t_1, \ldots, t_{n+1}) = f_i$, of degree $d_i = \deg f_i$. Being an odd polynomial, each f_i only contains monomials of odd degree; thus each d_i is odd and t_0 occurs in $\tilde{f}_i$ to even powers only. Thus we may make the change of variables $t_0^2 \mapsto t_1^2 + \ldots + t_{n+1}^2$ in each $\tilde{f}_i$, leading to homogeneous polynomials $g_1, \ldots, g_n \in k[t_1, \ldots, t_{n+1}]$ of odd degrees $d_1, \ldots, d_n$. Applying Theorem 11.21 with $p = 2$, we get $0 \neq a \in k^{n+1}$ such that $g_1(a) = \ldots = g_n(a) = 0$. Since the g_i's are homogeneous, we may scale by $\left(a_1^2 + \ldots + a_{n+1}^2\right)^{-1}$ to get an a such that $a_1^2 + \ldots + a_{n+1}^2 = 1$ and $g_1(a) = \ldots = g_n(a) = 0$. Thus $f_i(a) = \tilde{f}_i(1, a) = g_i(a) = 0$ for all i, and we're done. □

We now revert to the case of $k = \mathbb{R}$. As usual, for $x = (x_1, \ldots, x_n) \in \mathbb{R}^n$, we put

$$||x|| = \sqrt{x_1^2 + \ldots + x_n^2}\};$$

for $x, y \in \mathbb{R}^n$, we put

$$d(x, y) = ||x - y||,$$

and we define the **unit sphere**

$$S^n = \{x \in \mathbb{R}^n \mid ||x|| = 1\}$$

and the **unit disk**

$$D^n = \{x \in \mathbb{R}^n \mid ||x|| \leq 1\}.$$

A subset $S \subset \mathbb{R}^n$ is **symmetric** if $x \in S \implies -x \in S$. If $S \subset \mathbb{R}^m$ and $T \subset \mathbb{R}^n$ are symmetric subsets, then $f : S \to T$ is **odd** if for all $x \in S$, $f(-x) = -f(x)$. For $x \in S^n$, x and $-x$ are **antipodal**, and $\{x, -x\}$ is called an **antipodal pair**.

Corollary 11.23. *(Topological Borsuk-Ulam)*
Let $f : S^n \to \mathbb{R}^n$ be a continuous, odd map. Then there is $x \in S^n$ with $f(x) = 0$.

Proof. Write $f = (f_1, \ldots, f_n)$, for $f_i : S^n \to \mathbb{R}$ an odd continuous map. Seeking a contradiction, we suppose f has no zero. Since S^n is compact, there is $\delta > 0$ such that for all $x \in S^n$, $\max_i |f_i(x)| \geq \delta$. Choose $0 < \epsilon < \delta$ and apply the Weierstrass Approximation Theorem to the continuous functions $f_1, \ldots, f_n$ on the compact space S^n: there are $p_1, \ldots, p_n \in \mathbb{R}[t_1, \ldots, t_{n+1}]$ such that $|f_i(x) - p_i(x)| < \epsilon$ for all i and all $x \in S^n$. Put $q_i(t) = \frac{1}{2}(p_i(t) - p_i(-t))$; then for $x \in S^n$,

$$|f_i(x) - q_i(x)| = \frac{|f_i(x) - f_i(-x) - p_i(x) + p_i(-x)|}{2}$$

$$\leq \frac{|f_i(x) - p_i(x)| + |f_i(-x) - p_i(-x)|}{2} < \epsilon.$$

It follows that for all $x \in S^n$, $\max_i |q_i(x)| \geq \delta - \epsilon > 0$, so the q_i's have no simultaneous zero on S^n, contradicting Theorem 11.22. □

Corollary 11.24.
The following statements are equivalent – and hence, by Corollary 11.23, all true.
(i) Every continuous, odd map $f : S^n \to \mathbb{R}^n$ has a zero.
(ii) There is no continuous, odd map $g : S^n \to S^{n-1}$.
(iii) Every continuous map $f : S^n \to \mathbb{R}^n$ identifies an antipodal pair.
(iv) (Lusternik-Schnirelmann-Borsuk) Let $\{F_1, \ldots, F_{n+1}\}$ be a covering family of closed subsets of S^n. Then some member of the family contains an antipodal pair.

Proof. (i) $\implies$ (ii): Let $\iota : S^{n-1} \hookrightarrow \mathbb{R}^n$ be the natural inclusion. If $g : S^n \to S^{n-1}$ is continuous and odd, $\iota \circ g : S^n \to \mathbb{R}^n$ is continuous and odd with no zero.
(ii) $\implies$ (iii): If f identifies no antipodal pair, then $g : S^n \to S^{n-1}$ by $x \mapsto \frac{f(x)-f(-x)}{||f(x)-f(-x)||}$ is continuous and odd.
(iii) $\implies$ (i): Let $f : \mathbb{R}^n \to S^n$ be odd. By assumption, there is $x \in S^n$ such that $f(x) = f(-x)$, but since also $f(x) = -f(-x)$, we conclude $f(x) = 0$.
(iii) $\implies$ (iv): Let $F_1, \ldots, F_{n+1}$ be closed subsets of S^n such that $\bigcup_{i=1}^{n+1} F_i = S^n$; suppose that none of the sets $F_1, \ldots, F_n$ contains an antipodal pair: equivalently, putting $E_i = -F_i$, we have that $E_i \cap F_i = \varnothing$ for $1 \leq i \leq n$. For a point x and a subset Y of S^n, put $d(x, Y) = \inf\{d(x, y) \mid y \in Y\}$. For $1 \leq i \leq n+1$, define $f_i : S^n \to \mathbb{R}$ by $f_i(x) = d(x, E_i) - d(x, F_i)$. Observe that

$$x \in F_i \implies f_i(-x) < 0 < f_i(x),$$

$$x \in E_i \implies f_i(x) < 0 < f_i(-x).$$

Applying condition (iii) to $f = (f_1, \ldots, f_n) : S^n \to \mathbb{R}^n$, we get $x_0 \in S^n$ such that $f(-x_0) = f(x_0)$. Thus neither x_0 nor $-x_0$ lies in any F_i with $1 \leq i \leq n$, hence both x_0 and $-x_0$ must lie in F_{n+1}.
(iv) $\implies$ (ii): Let $f : S^n \to S^{n-1}$ be continuous. Observe the following "converse" to Lusternik-Schnirelmann-Borsuk: there is a covering family $\{E_i\}_{i=1}^{n+1}$ of closed subsets of S^{n-1}, each of diameter less than 2. (We leave the verification of this as an exercise.) For $1 \leq i \leq n+1$, put $F_i = f^{-1}(E_i)$. Thus $\{F_i\}_{i=1}^{n+1}$ is a covering of S^n by closed subsets, so by condition (iv) for some $1 \leq i \leq n+1$ and $x_0 \in S^n$ we have $x_0, -x_0 \in F_i$, i.e., $f(x_0), f(-x_0) \in E_i$. Since E_i has diameter less than 2, it contains no antipodal pair, and thus f cannot be odd, for otherwise $f(x_0), -f(x_0) \in E_i$. □

Exercise 11.11: Verify that for any $n \in \mathbb{Z}^+$, S^n can be covered by $n+2$ closed subsets each of diameter less than 2. (Suggestion: take a regular simplex inscribed in D^n and consider the projections of its faces onto S^n.)

For a function $f : \mathbb{R}^n \to \mathbb{R}$, let us put

$$f^+ = \{x \in \mathbb{R}^n \mid f(x) > 0\},$$

$$f^0 = \{x \in \mathbb{R}^n \mid f(x) = 0\},$$

$$f^- = \{x \in \mathbb{R}^n \mid f(x) < 0\}.$$

For a Lebesgue measurable subset $S \subset \mathbb{R}^n$, we denote its measure by $\mathrm{Vol}(S)$.

The following result is due to Stone and Tukey [ST42].

Corollary 11.25. *(Polynomial Ham Sandwich Theorem) Let $d, n \in \mathbb{Z}^+$ and put $N = \binom{n+d}{d} - 1$. Let $U_1, \ldots, U_N \in \mathbb{R}^n$ be measurable, finite volume subsets. There*

*is a polynomial $P \in \mathbb{R}[t_1, \ldots, t_n]$ of degree at most d which **bisects** each U_i:*

$$\forall 1 \leq i \leq N,\ \mathrm{Vol}(U_i \cap P^+) = \mathrm{Vol}(U_i \cap P^-).$$

Proof. Let $V_d \subset \mathbb{R}[t_1, \ldots, t_n]$ be the $\mathbb{R}$-subspace of polynomials of total degree at most d, so $\dim V_d = N + 1$. Endow V_d with a norm $||\cdot||$ (all norms on a finite-dimensional real vector space are *equivalent*, so we need not be more specific than this). Let S^N be the unit sphere in V_d. We define a function

$$f = (f_1, \ldots, f_N) : S^N \to \mathbb{R}^N$$

by

$$f_i(P) = \mathrm{Vol}(U_i \cap P^+) - \mathrm{Vol}(U_i \cap P^-).$$

Step 1: We CLAIM that f is continous.
PROOF OF CLAIM: One easily reduces to the claim that for any measurable, finite volume subset $U \subset \mathbb{R}^n$, the mapping

$$M : P \in V_d^\bullet \mapsto \mathrm{Vol}(U \cap P^+)$$

is continuous. For this, let $\{P_n\}$ be a sequence in V_d such that $P_n \to P$ with respect to $||\cdot||$. It follows that $P_n \to P$ pointwise on ($\mathbb{R}^n$ hence in particular on) U. Since $\mathrm{Vol}(U) < \infty$, we may apply Egorov's Theorem: for each $\epsilon > 0$, there is a measurable subset $E \subset U$ with $\mathrm{Vol}(E) < \epsilon$ and such that $P_n \to P$ uniformly on $U \setminus E$. Since $\mathrm{Vol}(P^0) = 0$ and $\mathrm{Vol}(U) < \infty$, there is $\delta > 0$ such that

$$\mathrm{Vol}(\{x \in U \mid |P(x)| < \delta\}) < \epsilon.$$

Take $N \in \mathbb{Z}^+$ such that for all $n \geq N$, $|P_n(x) - P(x)| < \delta$ for all $x \in U \setminus E$. Then

$$|\mathrm{Vol}(U \cap P_n^+) - \mathrm{Vol}(U \cap P^+)| < 2\epsilon.$$

Step 2: It is immediate that f is odd. By Corollary 11.23, there is $P \in S^N$ such that $f(P) = 0$, and such a P bisects each U_i. □

Corollary 11.26. *(No Retraction Theorem) There is no **retraction** from D^n to S^{n-1}, i.e., no continuous map $r : D^n \to S^{n-1}$ such that $r|_{S^{n-1}} = 1_{S^{n-1}}$.*

Proof. Let $\pi : \mathbb{R}^{n+1} \to \mathbb{R}^n$, $(x_1, \ldots, x_n, x_{n+1}) \mapsto (x_1, \ldots, x_n)$, and let

$$H_n^+ = \{(x_1, \ldots, x_{n+1}) \in S^n \mid x_{n+1} \geq 0\},\ H_n^- = \{(x_1, \ldots, x_{n+1}) \in S^n \mid x_{n+1} \leq 0\}.$$

Suppose $r : D^n \to S^{n-1}$ is a retraction, and define $g : S^n \to S^{n-1}$ by

$$g(x) = \begin{cases} r(-\pi(x)),\ x \in H_n^+, \\ -r(\pi(x)),\ x \in H_n^- \end{cases}$$

Then g is well-defined, continuous and odd, contradicting Corollary 11.24b). □

Corollary 11.27. *(Brauer Fixed Point Theorem) Each continuous function $f : D^n \to D^n$ has a fixed point.*

Proof. Suppose $f : D^n \to D^n$ is continuous with $f(x) \neq x$ for all $x \in D^n$. For $x \in D^n$, consider the ray $\mathfrak{r}_x$ with initial point $f(x)$ and lying on the line determined by $f(x)$ and x. Then $\mathfrak{r}_x$ intersects S^{n-1} at a unique point, say $r(x)$, and $x \mapsto r(x)$ defines a retraction $r : D^n \to S^{n-1}$, contradicting Corollary 11.26. □

12. Goldman domains and Hilbert-Jacobson rings

12.1. **Goldman domains.**

Lemma 12.1. *Let R be a domain with fraction field K. TFAE:*
(i) K is finitely generated as an R-algebra.
(ii) There exists $f \in K$ such that $K = R[f]$.

Proof. Of course (ii) $\implies$ (i). Conversely, if $K = R[f_1, \ldots, f_n]$, then write $f_i = \frac{p_i}{q_i}$, and then $K = R[\frac{1}{q_1 \cdots q_n}]$. □

A ring satisfying the conditions of Lemma 12.1 will be called a **Goldman domain**.

Exercise 12.1: Show: an overring[49] of a Goldman domain is a Goldman domain.

Lemma 12.2. *Let R be a domain with fraction field K, and $0 \neq x \in R$. TFAE:*
(i) Any nonzero prime ideal of R contains x.
(ii) Any nonzero ideal contains a power of x.
(iii) $K = R[x^{-1}]$.

Proof. (i) $\implies$ (ii): let I be a nonzero ideal. If I is disjoint from $\{x^n\}$, then by Multiplicative Avoidance (4.8), I can be extended to a prime ideal disjoint from $\{x^n\}$, contradicting (i).

(ii) $\implies$ (iii): Let $0 \neq y \in R$. By (ii), we have (y) contains some power of x, say $x^k = yz$. But this implies that y is a unit in $R[x^{-1}]$.

(iii) $\implies$ (i): The prime ideals killed in the localization map $R \mapsto R[x^{-1}]$ are precisely those which meet the multiplicatively closed set $\{x^k\}$, i.e., contain x. □

Corollary 12.3. *For an integral domain R, TFAE:*
(i) R is a Goldman domain.
(ii) The intersection of all nonzero prime ideals of R is nonzero.

Exercise 12.2: Prove Corollary 12.3. Easy examples of Goldman domains: a field, $k[[t]]$, $\mathbb{Z}_{(p)}$. In fact we have developed enough technology to give a remarkably clean characterization of Noetherian Goldman domains.

Theorem 12.4. *Let R be an integral domain.*
a) If R has only finitely many primes, then R is a Goldman domain.
b) If R is a Noetherian Goldman domain, then R has finitely many primes.
c) A Noetherian Goldman domain is either a field or a one-dimensional domain.

Proof. It is harmless to assume throughout that R is not a field, and we do so.

a) Suppose that R has only finitely many primes, and let $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$ be the nonzero prime ideals of R. For $1 \leq i \leq n$, let $0 \neq x_i \in \mathfrak{p}_i$, and put $x = x_1 \cdots x_n$. Then the multiplicative set S generated by x meets every nonzero prime of R, so that $S^{-1}R$ has only the zero ideal. In other words, $R[\frac{1}{x}]$ is the fraction field of R, so R is a Goldman domain. (Alternately, this follows quickly from Corollary 12.3.)

b) Similarly, for a Goldman domain R we can write $K = R[\frac{1}{x}]$ for $x \in R$ and then every nonzero prime of R contains x. Suppose first that (x) itself is prime, necessarily of height one by the Hauptidealsatz (Theorem 8.42), hence if R has any primes other than (0) and (x) – especially, if it has infinitely many primes – then it has a height two prime $\mathfrak{q}$. But by Corollary 8.46 a Noetherian ring cannot have a

[49] An overring of a domain R is a ring intermediate between R and its fraction field K.

height two prime unless it has infinitely many height one primes, a contradiction. So we may assume that (x) is not prime, and then the minimal primes of the Noetherian ring $R/(x)$ are finite in number – say $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$ – and correspond to the primes of R which are minimal over x, so again by the Hauptidealsatz they all have height one. Similarly, if R has infinitely many primes there would be, for at least one i (say $i = 1$), a height two prime $\mathfrak{q} \supset \mathfrak{p}_1$. But then by Corollary 8.46 the "interval" $(0, \mathfrak{q})$ is infinite. Each element of this set is a height one prime ideal containing (x), i.e., is one of the $\mathfrak{p}_i$'s, a contradiction. Part c) follows by again applying Corollary 8.46: a Noetherian ring of dimension at least two must have infinitely many primes. □

Remark: a non-Noetherian Goldman domain can have infinitely many primes and/or primes of arbitrarily large height.

Proposition 12.5. *Let R be an integral domain. Then the polynomial ring $R[t]$ is* not *a Goldman domain.*

Proof. Let K be the fraction field of R. If $R[t]$ is a Goldman domain, then by Exercise 12.1, so is $K[t]$. But $K[t]$ is a Noetherian domain with infinitely many primes – e.g., Euclid's proof of the infinitude of primes in $\mathbb{Z}$ carries over verbatim to $K[t]$ – so Theorem 12.4 applies to show that $K[t]$ is not a Goldman domain. □

Proposition 12.6. *Let R be a domain, and $T \supset R$ an extension domain which is algebraic and finitely generated as an R-algebra. Then R is a Goldman domain iff T is a Goldman domain.*

Proof. Let K and L be the fraction fields of R and T, respectively. Suppose first that R is a Goldman domain: say $K = R[\frac{1}{u}]$. Then $T[\frac{1}{u}]$ is algebraic over the field K, so is a field, hence we have $L = T[\frac{1}{u}]$. Conversely, suppose that T is a Goldman domain: say $L = T[\frac{1}{v}]$; also write $T = R[x_1, \ldots, x_k]$. The elements $v^{-1}, x_1, \ldots, x_k$ are algebraic over R hence satisfy polynomial equations with coefficients in R. Let a be the leading coefficient of a polynomial equation for v^{-1} and $b_1, \ldots, b_k$ be the leading coefficients of polynomial equations for $x_1, \ldots, x_k$. Let $R_1 := R[a^{-1}, b_1^{-1}, \ldots, b_k^{-1}]$. Now L is generated over R_1 by $x_1, \ldots, x_k, v^{-1}$, all of which are integral over R_1, so L is integral over R_1. Since L is a field, it follows that R_1 is a field, necessarily equal to K, and this shows R is a Goldman domain. □

Corollary 12.7. *Let $R \subset S$ be an inclusion of domains, with R a Goldman domain. Suppose that $u \in S$ is such that $R[u]$ is a Goldman domain. Then u is algebraic over R, and R is a Goldman domain.*

Theorem 12.8. *For an integral domain R, TFAE:*
(i) R is a Goldman domain.
(ii) There exists a maximal ideal $\mathfrak{m}$ of $R[t]$ such that $\mathfrak{m} \cap R = (0)$.

Proof. (i) $\implies$ (ii): We may assume WLOG that R is not a field. Write $K = R[\frac{1}{u}]$. Define a homomorphism $\varphi : R[t] \to K$ by sending $t \mapsto \frac{1}{u}$. Evidently φ is surjective, so its kernel $\mathfrak{m}$ is a maximal ideal, and clearly we have $\mathfrak{m} \cap R = 0$.

(ii) $\implies$ (i): Suppose $\mathfrak{m}$ is a maximal ideal of $R[t]$ such that $\mathfrak{m} \cap R = (0)$. Let v be the image of t under the natural homomorphism $R[t] \to R[t]/\mathfrak{m}$. Then $R[v]$ is a field, so by Corollary 12.7, R is a Goldman domain. □

We define a prime ideal $\mathfrak{p}$ of a ring R to be a **Goldman ideal** if $R/\mathfrak{p}$ is a Goldman domain. Write $G\operatorname{Spec} R$ for the set of all Goldman ideals. Thus a Goldman ideal is more general than a maximal ideal but much more special than a prime ideal.

Proposition 12.9. *Let R be a ring and I an ideal of R.*
a) The nilradical of R is the intersection of all Goldman ideals of R.
b) The radical of I is the intersection of all Goldman ideals containing I.

Proof. a) We know that $N = \bigcap_{\mathfrak{p} \in \operatorname{Spec} R} \mathfrak{p}$, so certainly $N \subset \bigcap_{\mathfrak{p} \in G\operatorname{Spec} R} \mathfrak{p}$. Conversely, suppose $x \in R \setminus N$. The ideal (0) is then disjoint from the multiplicative set $S = \{x^n\}$. By multiplicative avoidance, we can extend (0) to an ideal $\mathfrak{p}$ maximal with respect to disjointness from S. We showed earlier that $\mathfrak{p}$ is prime; we now claim that it is a Goldman ideal. Indeed, let $\overline{x}$ denote the image of x in $\overline{R} = R/\mathfrak{p}$. By maximality of $\mathfrak{p}$, every nonzero prime of $\overline{R}$ contains $\overline{x}$. By Lemma 12.2, this implies $\overline{R}[\overline{x}^{-1}]$ is a field, thus $\overline{R}$ is a Goldman domain, and therefore $\mathfrak{p}$ is a Goldman ideal which does not contain x. Part b) follows by correspondence, as usual. □

The following result may seem completely abstruse at the moment, but soon enough it will turn out to be the key:

Corollary 12.10. *An ideal I in a ring R is a Goldman ideal iff it is the contraction of a maximal ideal in the polynomial ring $R[t]$.*

Proof. This follows from Theorem 12.8 by applying the correspondence principle to the quotient ring R/I. □

Theorem 12.11. *a) Let $\mathcal{M}$ be a maximal ideal in $R[t]$, and **suppose** that its contraction $\mathfrak{m} = \mathcal{M} \cap R$ is maximal in R. Then $\mathcal{M}$ can be generated by $\mathfrak{m}$ and by one additional element f, which can be taken to be a monic polynomial which maps modulo $\mathfrak{m}$ to an irreducible polynomial in $R/\mathfrak{m}[t]$.*
b) If, moreover, we suppose that $R/\mathfrak{m}$ is algebraically closed, then $\mathcal{M} = \langle \mathfrak{m}, t - a \rangle$ for some $a \in R$.

Proof. a) Since $\mathcal{M}$ contains $\mathfrak{m}$, by correspondence $\mathcal{M}$ may be viewed as a maximal ideal of $R[t]/\mathfrak{m}R[t] \cong (R/\mathfrak{m})[t]$, a PID, so corresponds to an irreducible polynomial $\overline{f} \in R/\mathfrak{m}[t]$. If f is any lift of f to $R[t]$, then $\mathcal{M} = \langle \mathfrak{m}, f \rangle$. Part b) follows immediately from the observation that an irreducible univariate polynomial over an algebraically closed field is linear. □

The following more elementary result covers the other extreme.

Theorem 12.12. *Let R be a domain, with fraction field K. Let $\iota : R[t] \to K[t]$ be the natural inclusion. Then ι_* induces a bijection between the prime ideals $\mathcal{P}$ of $R[t]$ such that $\mathcal{P} \cap R = \{0\}$ and the prime ideals of $K[t]$.*

Proof. Let $S = R \setminus \{0\}$. The key observation is that $S^{-1}R[t] = K[t]$. Recall (Proposition 7.4) that in any localization map $R \mapsto S^{-1}R$, the prime ideals which push forward to the unit ideal are precisely those which meet S, whereas the localization map restricted to all other prime ideals is a bijection onto the set of prime ideals of $S^{-1}R$. Applying that in this case gives the desired result immediately! □

12.2. **Hilbert rings.**

To put Theorem 12.11 to good use, we need to have a class of rings for which the contraction of a maximal ideal from a polynomial ring is again a maximal ideal. It turns out that the following is the right class of rings:

Definition: A **Hilbert ring** is a ring in which every Goldman ideal is maximal.

Proposition 12.13. *Any quotient ring of a Hilbert ring is a Hilbert ring.*

Proof. This follows immediately from the correspondence between ideals of R/I and ideals of R containing I. □

A direct consequence of the definition and Proposition 12.9 is the following:

Proposition 12.14. *Let I be an ideal in a Hilbert ring R. Then the intersection $\bigcap_{\mathfrak{m} \sup I} \mathfrak{m}$ of all maximal ideals $\mathfrak{m}$ containing I is* $\mathrm{rad}(I)$.

Examples: Any zero dimensional ring is a Hilbert ring. Especially, a field is a Hilbert ring, as is any Artinian ring or any Boolean ring.

Exercise 12.3: a) Let R be a one-dimensional Noetherian domain. TFAE:
(i) R is a Hilbert ring.
(ii) The Jacobson radical of R is 0.
(iii) R has infinitely many prime ideals.
(iv) R is not a Goldman domain.
b) Deduce that the ring $\mathbb{Z}$ of integers is a Hilbert domain.

Theorem 12.15. *Let R be a Hilbert ring, and S a finitely generated R-algebra. Then:*
a) S is also a Hilbert ring.
b) For every maximal ideal $\mathfrak{P}$ of S, $\mathfrak{p} := \mathfrak{P} \cap R$ is a maximal ideal of R.
c) The degree $[S/\mathfrak{P} : R/\mathfrak{p}]$ is finite.

Proof. a) It suffices to show that R is a Hilbert ring iff $R[t]$ is a Hilbert ring, for then, if R is a Hilbert ring, by induction any polynomial ring $R[t_1, \ldots, t_n]$ is a Hilbert ring, and any finitely generated R-algebra is a quotient of $R[t_1, \ldots, t_n]$ and thus a Hilbert ring. Note also that since R is a homomorphic image of $R[t]$, if $R[t]$ is a Hilbert domain, then so also is R.

So suppose R is a Hilbert ring, and let $\mathfrak{q}$ be a Goldman ideal in $R[t]$; we must show $\mathfrak{q}$ is maximal. Put $\mathfrak{p} = \mathfrak{q} \cap R$. As above, we can reduce to the case $\mathfrak{p} = 0$, so in particular R is a domain. Let a be the image of t in the natural homomorphism $R[t] \to R[t]/\mathfrak{q}$. Then $R[a]$ is a Goldman domain. By Corollary 12.7, a is algebraic over R, and R is a Goldman domain. But since we assumed that R was a Hilbert ring, this means that R is a field, and thus $R[a] = R[t]/\mathfrak{q}$ is a field, so $\mathfrak{q}$ is maximal.

b) We may write $S = R[t_1, \ldots, t_n]/I$. A maximal ideal $\mathfrak{m}$ of S is just a maximal ideal of $R[t_1, \ldots, t_n]$ containing I. By Corollary 12.10, the contraction $\mathfrak{m}'$ of $\mathfrak{m}$ to $R[t_1, \ldots, t_{n-1}]$ is a Goldman ideal of the Hilbert ring $R[t_1, \ldots, t_{n-1}]$, so is therefore maximal. Moreover, by Theorem 12.11, $\mathfrak{m}$ is generated by $\mathfrak{m}'$ and an irreducible polynomial in $R/\mathfrak{m}'[t]$, so that the residual extension $R[t_1, \ldots, t_n]/\mathfrak{m}$ has finite degree over $R[t_1, \ldots, t_{n-1}/\mathfrak{m}'$. Again, induction gives the full result. □

Applying Theorem 12.15c) in the case $R = k$ is a field, we deduce our second proof of **Zariski's Lemma** (Lemma 11.1).

Theorem 12.16. *Let R be a Noetherian Hilbert ring. Then*

$$\dim(R[t]) = \dim R + 1.$$

Proof. Let $0 = \mathfrak{p}_0 \subsetneq \mathfrak{p}_1 \subsetneq \ldots \subsetneq \mathfrak{p}_d$ be a chain of prime ideals in R. Then, with $\iota : R \hookrightarrow R[t]$ the natural inclusion,

$$\iota_* \mathfrak{p}_0 \subsetneq \ldots \subsetneq \iota_* \mathfrak{p}_n \subsetneq \langle \iota_*(\mathfrak{p}_n), t \rangle$$

is a chain of prime ideals of $R[t]$ of length $d+1$, hence for any ring R we have $\dim R[t] \geq \dim R + 1$. Conversely, it suffices to show that the height of any maximal ideal $\mathcal{P}$ of $R[t]$ is at most $d+1$. For this, put $\mathfrak{p} = \mathcal{P} \cap R$. By Theorem 12.15, $\mathfrak{p}$ is maximal in R, so Theorem 12.11 tells us that there exists $f \in R[t]$ such that $\mathcal{P} = \langle \iota_* \mathfrak{p}, f \rangle$. Applying Krull's Hauptidealsatz (Theorem 8.42) in the quotient ring $R[t]/\iota_* \mathfrak{p}$, we get that the height of $\mathcal{P}$ is at most one more than the height of $\mathfrak{p}$. □

Corollary 12.17. *Let k be a field, and put $R = k[t_1, \ldots, t_n]$.*
a) Then every maximal ideal of R has height n and can be generated by n elements (and no fewer, by Theorem 8.47).
b) In particular, $\dim R = n$.

Exercise 12.4: Prove Corollary 12.17.

12.3. **Jacobson Rings.**

Theorem 12.18. *For a ring R, TFAE:*
(i) For all $I \in \mathcal{I}(R)$, $r(I)$ is the intersection of all maximal *ideals containing I.*
(i′) In every quotient ring of R, the nilradical equals the Jacobson radical.
(ii) Every prime ideal $\mathfrak{p}$ of R is the intersection of all maximal ideals containing $\mathfrak{p}$.
(iii) Every non*maximal prime ideal $\mathfrak{p}$ of R is equal to the intersection of all prime ideals strictly containing $\mathfrak{p}$.*
If R satisfies these equivalent properties it is called a ***Jacobson ring****.*

Proof. (i) $\iff$ (i′) is immediate from the Correspondence Theorem.
(i) $\implies$ (ii): If (i) holds, then in particular for any radical ideal I, $I = \bigcap_{\mathfrak{m} \supset I} \mathfrak{m}$, and prime ideals are radical.
(ii) $\implies$ (i): for any ideal I of R,

$$\operatorname{rad} I = \bigcap_{\mathfrak{p} \supset I} \mathfrak{p} = \bigcap_{\mathfrak{p} \supset I} \bigcap_{\mathfrak{m} \supset \mathfrak{p}} \mathfrak{m} = \bigcap_{\mathfrak{m} \supset I} \mathfrak{m}.$$

(ii) $\implies$ (iii): If $\mathfrak{p}$ is prime but not maximal, then $\mathfrak{p} = \bigcap_{\mathfrak{m} \supset \mathfrak{p}} \mathfrak{m}$ and all the maximal ideals containing $\mathfrak{p}$ strictly contain $\mathfrak{p}$.
$\neg$ (ii) $\implies$ $\neg$ (iii): Let $\mathfrak{p}$ be a prime which is *not* the intersection of the maximal ideals containing it. Replacing R with $R/\mathfrak{p}$, we may assume R is a domain with nonzero Jacobson radical $J(R)$. Let $x \in J(R) \setminus \{0\}$, and choose, by Multiplicative Avoidance, an ideal $\mathfrak{p}$ which is maximal with respect to the property that $x \notin \mathfrak{p}$. Since $x \notin J(R) \setminus \mathfrak{p}$, $\mathfrak{p}$ is not maximal; since x lies in every ideal properly containing $\mathfrak{p}$, $\mathfrak{p}$ is not equal to the intersection of prime ideals strictly containing it. □

Corollary 12.19. *Every quotient ring of a Jacobson ring is Jacobson.*

Proof. This is immediate from condition (i′) of Theorem 12.18. □

12.4. **Hilbert-Jacobson Rings.**

Proposition 12.20. *Suppose R is both a Goldman domain and a Jacobson ring. Then R is a field.*

Proof. Let K be the fraction field of R, and suppose for a conradiction that $R \neq K$. Then there exists a nonzero nonunit $f \in R$ such that K is the localization of R at the multiplicative subset $S = \{f, f^2, \ldots\}$. Let $\mathfrak{m}$ be a maximal ideal of R. Since R is not a field, $\mathfrak{m}$ is not zero, and thus the pushforward of R to $S^{-1}R$ is the unit ideal. By Proposition 7.4, $\mathfrak{m}$ meets S. Since $\mathfrak{m}$ is prime, we conclude $f \in \mathfrak{m}$. It follows that the Jacobson radical of R contains f is accordingly nonzero. On the other hand R, being a domain, has zero nilradical. Thus R is not Jacobson. □

Finally we are prepared to prove the main result of this section, which shows the equivalence of four important properties of commutative rings.

Theorem 12.21. *For a commutative ring R, TFAE:*
(i) R is a Hilbert ring.
(ii) R is a Jacobson ring.
(iii) For all maximal ideals $\mathfrak{m}$ of $R[t]$, $\mathfrak{m} \cap R$ is a maximal ideal of R.
(iv) (Zariski's Lemma) Let K be a field which is finitely generated as an R-algebra. Then K is finitely generated as a R-module.

Proof. (i) $\implies$ (ii) by Proposition 12.14.
(ii) $\implies$ (i): Suppose R is Jacobson and $\mathfrak{p}$ is a Goldman ideal of R. Then $R/\mathfrak{p}$ is a Goldman domain (by definition of Goldman ideal) and a Jacobson ring (by Corollary 12.19), hence a field (by Proposition 12.20), so $\mathfrak{p}$ is maximal.
(ii) $\implies$ (iii) is Theorem 12.15b).
(iii) $\implies$ (i): Suppose R is a ring such that every maximal ideal of $R[t]$ contracts to a maximal ideal of R, and let $\mathfrak{p}$ be a Goldman ideal of R. By Corollary 12.10, $\mathfrak{p}$ is the contraction of a maximal ideal of $R[t]$, hence by assumption $\mathfrak{p}$ is maximal.
(i) $\implies$ (iv) by Theorem 12.15c).
(iv) $\implies$ (ii): By Theorem 12.18, it suffices to show that every nonmaximal prime $\mathfrak{p}$ is the intersection of the prime ideals strictly containing it. That is, let $x \in R \setminus \mathfrak{p}$: we will find a prime ideal $\mathfrak{q} \supsetneq \mathfrak{p}$ such that $x \notin \mathfrak{q}$. Let B be the domain $R/\mathfrak{p}$, so the image of x in B (which we continue to denote by x) is nonzero. Then $B' = B[\frac{1}{x}]$ is a finitely generated R-algebra. If B' is a field, then by hypothesis B' is finitely generated as an R-module and thus, equivalently, finitely generated as a B-module. But this implies that B is a field, a basic fact about integral extensions which will be proved later on in the notes (Theorem 14.1, Propostion 14.8a)) and thus $\mathfrak{p}$ is maximal, contradiction. So B' is not a field and thus it contains a nonzero maximal ideal, whose pullback to B is a prime ideal $\overline{\mathfrak{q}}$ not containing x. The ideal $\overline{\mathfrak{q}}$ corresponds to a prime ideal $\mathfrak{q} \supsetneq \mathfrak{p}$ of R not containing x. □

In the sequel we will use the consolidated terminology **Hilbert-Jacobson ring** for a ring satisfying the equivalent conditions of Theorem 12.21.

13. Spec R as a topological space

13.1. **The Zariski spectrum.**

For a ring R, we denote the set of all prime ideals of R by $\operatorname{Spec} R$. Moreover, we refer to $\operatorname{Spec} R$ as the **Zariski spectrum** – or **prime spectrum** – of R.

It is important to notice that $\operatorname{Spec} R$ comes with additional structure. First, it has a natural partial ordering, in which the maximal elements are the maximal ideals, and the minimal elements are (by definition) the **minimal primes**. Also, as O. Zariski first observed, $\operatorname{Spec} R$ can be endowed with a **topology**. To see this, for any ideal I of R, put $V(I) = \{\mathfrak{p} \in \operatorname{Spec} R \mid \mathfrak{p} \supset I\}$.

Proposition 13.1. *For ideals I and J of R, we have $V(I) = V(J)$ iff $\operatorname{rad} I = \operatorname{rad} J$.*

Proof. For any ideal I and any prime ideal $\mathfrak{p}$, $\mathfrak{p} \supset I$ iff $\mathfrak{p} \supset \operatorname{rad} I$, and therefore $V(I) = V(\operatorname{rad} I)$. Conversely, if $V(I) = V(J)$, then the set of prime ideals containing I is the same as the set of prime ideals containing J. So

$$\operatorname{rad} I = \bigcap_{\mathfrak{p} \supset I} \mathfrak{p} = \bigcap_{\mathfrak{p} \supset J} \mathfrak{p} = \operatorname{rad} J.$$

□

Exercise 13.1: Show that $I \subset J$ iff $V(I) \supset V(J)$.

Now we claim that the family of subsets $V(I)$ of $\operatorname{Spec} R$ has the following properties:

(ZT1) $\emptyset = V(R)$, $\operatorname{Spec} R = V((0))$.
(ZT2) If $\{I_i\}$ is any collection of ideals of R, then $\bigcap_i V(I_i) = V(\langle I_i \rangle)$.
(ZT3) If $I_1, \ldots, I_n$ are ideals of R, then $\bigcup_{i=1}^n V(I_i) = V(I_1 \cdots I_n) = V(\bigcap_{i=1}^n I_i)$.

(ZT1) is obvious. As for (ZT2), let $\mathfrak{p}$ be a prime ideal of R. Then $\mathfrak{p} \in \bigcap_i V(I_i)$ for all i iff $\mathfrak{p} \supset I_i$ for all i iff $\mathfrak{p}$ contains the ideal generated by all I_i. As for (ZT3), $\mathfrak{p}$ contains a product of ideals iff it contains one of the ideals of the product.

Therefore there is a unique topology on $\operatorname{Spec} R$ in which the closed sets are precisely those of the form $V(I)$. This is called the **Zariski topology**.

It is of course natural to ask for a characterization of the open sets. Recall that a **base** for the open sets of a topology is a collection $\{B_i\}$ of open sets such that:

(BT1) for any point $x \in B_i \cap B_j$, there exists a k such that $x \in B_k \subset B_i \cap B_j$;
(BT2) every open set is a union of the B_i's contained in it.

For $f \in R$, we define $U(f) := \operatorname{Spec} R \setminus V((f))$. In other words, $U(f)$ is the collection of all prime ideals which *do not* contain the element f. For $f, g \in R$, $U(f) \cap U(g)$ is the set of prime ideals $\mathfrak{p}$ containing neither f nor g; since $\mathfrak{p}$ is prime, this is equivalent to $\mathfrak{p}$ not containing fg, thus

$$U(f) \cap U(g) = U(fg),$$

which is a stronger property than (BT1). Moreover, any open set U is of the form $\operatorname{Spec} R \setminus V(I)$. Each ideal I is the union of all of its elements f_i, so $V(I) = \bigcap_i V(f_i)$,

so that

$$U = \operatorname{Spec} R \setminus V(I) = \operatorname{Spec} R \setminus \bigcap_i V(f_i) = \bigcup_i (\operatorname{Spec} R \setminus V(f_i)) = \bigcup_i U(f_i).$$

Proposition 13.2. *Let R be any ring, and consider the canonical homomorphism $f : R \to R^{\mathrm{red}} = R/\operatorname{nil}(A)$. Then $f^{-1} : \operatorname{Spec} R^{\mathrm{red}} \to \operatorname{Spec} R$ is a homeomorphism.*

Exercise 13.2: Prove Proposition 13.2.

Exercise 13.3: Let $R_1, \ldots, R_n$ be finitely many rings. Show that $\operatorname{Spec}(R_1 \times \ldots \times R_n)$ is canonically homeomorphic to the topological space $\coprod_{i=1}^n \operatorname{Spec} R_i$.

Exercise 13.4: Let R be a Boolean ring. Earlier we defined a topology on the set "$M(R)$" of all maximal ideals of R. But, as we know, a Boolean ring all prime ideals are maximal, so as sets $M(R) = \operatorname{Spec} R$. Show that moreover the topology we defined on $M(R)$ is the Zariski topology on $\operatorname{Spec} R$.

13.2. **Properties of the spectrum: quasi-compactness.**

More than sixty years ago now, N. Bourbaki introduced the term **quasi-compact** for a topological space X for which any open covering has a finite subcovering. The point of this terminology is to reserve **compact** for a space which is both quasi-compact and Hausdorff, and thus emphasize that most of the nice properties of compact spaces in classical topology do rely on the Hausdorff axiom. Nowhere is this terminology more appropriate than in the class of spectral spaces, which as we have seen above, are only Hausdorff in the comparatively trivial case of a zero-dimensional ring. On the other hand:

Proposition 13.3. *For any commutative ring R, $\operatorname{Spec} R$ is quasi-compact.*

Proof. Let $\{U_i\}$ be any open covering of $\operatorname{Spec} R$. For each $\mathfrak{p} \in \operatorname{Spec} R$, there exists an element U of the cover containing $\mathfrak{p}$, and thus a principal open set $X(f)$ containing $\mathfrak{p}$ and contained in U. Therefore there is a refinement of the cover consisting of principal open subsets, and if this refinement has a finite cover, then the original cover certainly does as well. Thus it suffices to assume that the U_i's are basic open sets.[50] So now suppose that $\operatorname{Spec} R = \bigcup_i X(f_i)$. Then we have

$$\operatorname{Spec} R = \bigcup_i X(f_i) = \bigcup_i (\operatorname{Spec} R \setminus V(f_i)) = \operatorname{Spec} R \setminus \bigcap_i V(f_i),$$

so that $\emptyset = \bigcap_i V(f_i) = V(\langle f_i \rangle)$. Therefore the ideal $I = \langle f_i \rangle$ contains 1, and this means that there is some finite subset $f_1, \ldots, f_n$ of I such that $\langle f_1, \ldots, f_n \rangle = R$. Thus $\bigcap_{i=1}^n V(f_i) = \emptyset$, or equivalently, $\operatorname{Spec} R = \bigcup_{i=1}^n X(f_i)$. □

[50] This is just the familiar, and easy, fact that it suffices to verify quasi-compactness on any base for the topology. It is also true, but deeper, that one can verify quasi-compactness on any subbase: Alexander's Subbase Theorem.

13.3. **Properties of the spectrum: separation and specialization.**

For the reader's convenience we briefly recall the "lower" separation axioms:

A topological space X is **Kolmogorov** – or T_0 – if for any distinct points $x, y \in X$, the **system of neighborhoods** $\mathcal{N}_x$ and $\mathcal{N}_y$ do not coincide. In plainer language, either there exists an open set U containing x and not containing y, or conversely.

A topological space X is **separated** – or T_1 – if for any distinct points $x, y \in X$, there exists both an open set U containing x and not y and an open set V containing y and not x. A space is separated iff all singleton sets $\{x\}$ are closed iff for all $x \in X$, $\bigcap_{U \in \mathcal{N}_x} U = \{x\}$.

A topological space X is **Hausdorff** – or T_2 – if for any distinct points $x, y \in X$, there exist open neighborhoods U of x and V of y with $U \cap V = \emptyset$. A space is Hausdorff iff for all $x \in X$, the intersection of all closed neighborhoods of x is $\{x\}$.

Easily Hausdorff implies separated implies Kolmogorov. In a general topology course one learns that neither of the converse implications holds in general. On the other hand most of the spaces one encounters in analysis and geometry are Hausdorff, and certainly are if they are Kolmogorov. We are about to see that yet a third state of affairs transpires when we restrict attention to spectra of rings.

Let X be a topological space. We define a relation $\mapsto$ on X by decreeing that for $x, y \in X$, $x \mapsto y$ iff y lies in the closure of the singleton set $\{x\}$. This relation is called **specialization**, and we read $x \mapsto y$ as "x specializes to y".

The reader who is familiar with topology but has not seen the specialization relation before will find an explanation in part f) of the following exercise.

Exercise 13.5:
a) Show that $x \mapsto y$ iff $\mathcal{N}_x \subset \mathcal{N}_y$.
b) Show that specialization satisfies the following properties:
(i) reflexivity: $x \mapsto x$; (ii) transitivity $x \mapsto y,\ y \mapsto z \implies x \mapsto z$.
A relation R with these properties is called a **quasi-ordering**. Note that a partial ordering is a quasi-ordering with the additional axiom of anti-symmetry: $xRy,\ yRx \implies x = y$.
c) Show that specialization is a partial ordering on X iff X is Kolmogorov.
d) Show that a point y is closed[51] iff $y \mapsto x \implies x = y$.
e) A point x for which $x \mapsto y$ holds for all $y \in X$ is called **generic**. Give an example of a topological space in which every point is generic.
f) Show that X is separated iff $x \mapsto y \implies x = y$.

Exercise 13.6: Let X be any set endowed with a quasi-ordering R. Define a new relation $x \equiv y$ if $x\ R\ y$ and $y\ R\ x$.
a) Show that $\equiv$ is an equivalence relation on X.
b) Write X' for the set of $\equiv$ equivalence classes, and let $q : X \to X'$ be the natural

[51]Strictly speaking we mean $\{y\}$ is closed, but this terminology is common and convenient.

map – i.e., $x \mapsto \{y \in X \mid y \equiv x\}$. Show that the relation R descends to a relation $\leq$ on X': i.e., for $s_1,\ s_2 \in X'$, then by choosing $x_1 \in s_1, x_2 \in s_2$ and putting

$$s_1 \leq s_2 \iff x_1\ R\ x_2,$$

the relation $\leq$ is well-defined independent of the choices of x_1 and x_2. Show that moreover $\leq$ is a partial ordering on X'.
c) Let X be a topological space and R be the specialization relation. Endowing X' with the quotient topology via q, show that the induced relation $\leq$ on X' is the specialization relation on X', and accordingly by the previous exercise X' is a Kolmogorov space. If it pleases you, show that $q : X \to X'$ is **universal** for maps from X into a Kolmogorov space Y, hence X' (or rather, $q : X \to X'$) can be regarded as the **Kolmogorov quotient** of X.

Exercise 13.7: Let (X, μ) be a measure space, and let $\mathcal{L}^1$ be the space of all measurable functions $f : X \to \mathbb{R}$ with $\int_X |f| d\mu < \infty$. For $f \in \mathcal{L}^1$, define $||f|| := \int_X |f| d\mu$, and for $\epsilon > 0$, put $B(f, \epsilon) = \{g \in \mathcal{L}^1 \mid ||g - f|| < \epsilon\}$. Show that the $B(f, \epsilon)$'s form a base for a topology on $\mathcal{L}^1$, but that this topology is, in general, not Kolmogorov. Show that the Kolmogorov quotient is precisely the usual Lebesgue space L^1, whose elements are not functions but classes of functions modulo μ a.e. equivalence.

Proposition 13.4. *For any ring R, the spectrum* $\operatorname{Spec} R$ *is a Kolmogorov space. Indeed, for prime ideals $\mathfrak{p},\ \mathfrak{q}$ of R, we have $\mathfrak{p} \mapsto \mathfrak{q}$ iff $\mathfrak{q} \supset \mathfrak{p}$, i.e., the specialization relation is precisely the opposite relation to the containment of prime ideals.*

Proof. For prime ideals $\mathfrak{p}$ and $\mathfrak{q}$ we have

$$\mathfrak{p} \mapsto \mathfrak{q} \iff \mathfrak{q} \in \overline{\{\mathfrak{p}\}} = \{\mathfrak{f} \in \operatorname{Spec} R \mid \mathfrak{f} \supset \mathfrak{p}\} \iff \mathfrak{q} \supset \mathfrak{p}.$$

Thus the specialization relation is just reverse containment of ideals, which certainly satisfies antisymmetry: $\mathfrak{q} \subset \mathfrak{p},\ \mathfrak{p} \subset \mathfrak{q} \implies \mathfrak{p} = \mathfrak{q}$. Now apply Exercise 13.6c). □

Theorem 13.5. *For a commutative ring R, TFAE:*
(i) $R/\operatorname{nil} R$ is absolutely flat, i.e., every $R/\operatorname{nil} R$-module is flat.
(ii) R has Krull dimension zero.
(iii) $\operatorname{Spec} R$ *is a separated space.*
(iv) $\operatorname{Spec} R$ *is a Hausdorff space.*
(v) $\operatorname{Spec} R$ *is a Boolean space.*

Proof. (i) $\iff$ (ii) This is Theorem 7.19.
(ii) $\iff$ (iii): A space is separated iff all of its singleton sets are closed. But if $\mathfrak{p}$ is prime, $V(\mathfrak{p})$ consists of all primes containing $\mathfrak{p}$, so $V(\mathfrak{p}) = \{\mathfrak{p}\}$ iff $\mathfrak{p}$ is maximal. Certainly (v) $\implies$ (iv) $\implies$ (iii).
(i) $\implies$ (v): Since $\operatorname{Spec} R = \operatorname{Spec}(R/\operatorname{nil} R)$, we may well assume that R itself is absolutely flat. Let $\mathfrak{p}$ and $\mathfrak{q}$ be distinct prime ideals; since both are maximal, there exists an element $f \in \mathfrak{p} \setminus \mathfrak{q}$. By Proposition 3.93, there is an idempotent e with $(e) = (f)$, and therefore $e \in \mathfrak{p} \setminus \mathfrak{q}$. Then $D(1-e)$, $D(e)$ is a separation of $\operatorname{Spec} R$. More precisely, $D(e) \cap D(1-e) = D(e(1-e)) = D(e - e^2) = D(0) = \emptyset$, whereas for any prime ideal $\mathfrak{p}$, since $0 = e(1-e) \in \mathfrak{p}$, we must have $e \in \mathfrak{p}$ or $1 - e \in \mathfrak{p}$. By construction, $\mathfrak{p} \in D(1-e),\ \mathfrak{q} \in D(e)$. This shows $\operatorname{Spec} R$ is Hausdorff, and more: given points $P \neq Q$ of X, we found a separation $X = U \coprod V$ with $P \in U,\ Q \in V$, so X is zero-dimensional. By Proposition 13.3, every ring has quasi-compact spectrum, so $\operatorname{Spec} R$ is Hausdorff, zero-dimensional and quasi-compact, i.e., Boolean. □

Exercise 13.8:
a) Let R be an arbitrary product of fields. Show that $\operatorname{Spec} R$ is a Boolean space.
b) Let $\{R_i\}_{i \in I}$ be a family of rings, each of which has Krull dimension 0, and put $R = \prod_i R_i$. Must $\operatorname{Spec} R$ be Boolean?

13.4. **Irreducible spaces.**

A topological space is **irreducible** if it is nonempty and if it cannot be expressed as the union of two proper closed subsets.

Exercise 13.9: Show that for a Hausdorff topological space X, TFAE:
(i) X is irreducible.
(ii) $\#X = 1$.

Proposition 13.6. *For a topological space X, TFAE:*
(i) X is irreducible.
(ii) Every finite intersection of nonempty open subsets (including the empty intersection!) is nonempty.
(iii) Every nonempty open subset of X is dense.
(iv) Every open subset of X is connected.

Exercise 13.10: Prove Proposition 13.6.

Proposition 13.7. *Let X be a nonempty topological space.*
a) If X is irreducible, every nonempty open subset of X is irreducible.
b) If a subset Y of X is irreducible, so is its closure $\overline{Y}$.
c) If $\{U_i\}$ is an open covering of X such that $U_i \cap U_j \neq \emptyset$ for all i, j and each U_i is irreducible, then X is irreducible.
d) If $f : X \to Y$ is continuous and X is irreducible, then $f(X)$ is irreducible in Y.

Proof. a) Let U be a nonempty open subset of X. By Proposition 13.6, it suffices to show that any nonempty open subset V of U is dense. But V is also a nonempty open subset of the irreducible space X.
b) Suppose $\overline{Y} = A \cup B$ where A and B are each proper closed subsets of $\overline{Y}$; since $\overline{Y}$ is itself closed, A and B are closed in X, and then $Y = (Y \cap A) \cup (Y \cap B)$. If $Y \cap A = Y$ then $Y \subset A$ and hence $\overline{Y} \subset \overline{A} = A$, contradiction. So A is proper in Y and similarly so is B, thus Y is not irreducible.
c) Let V be a nonempty open subset of X. Since the U_i's are a covering of X, there exists at least one i such that $V \cap U_i \neq \emptyset$, and thus by irreducibility $V \cap U_i$ is a dense open subset of U_i. Therefore, for any index j, $V \cap U_i$ intersects the nonempty open subset $U_j \cap U_i$, so in particular V intersects every element U_j of the covering. Thus for all sets U_i in an open covering, $V \cap U_i$ is dense in U_i, so V is dense in X.
d) If $f(X)$ is not irreducible, there exist closed subsets A and B of Y such that $A \cap f(X)$ and $B \cap f(X)$ are both proper subsets of $f(X)$ and $f(X) \subset A \cup B$. Then $f^{-1}(A)$ and $f^{-1}(B)$ are proper closed subsets of X whose union is all of X. □

Let x be a point of a topological space, and consider the set of all irreducible subspaces of X containing x. (Since $\{x\}$ itself is irreducible, this set is nonempty.) The union of a chain of irreducible subspaces being irreducible, Zorn's Lemma says that there exists at least one maximal irreducible subset containing x. A maximal irreducible subset (which, by the above, is necessarily closed) is called an **irreducible**

component of X. Since irreducible subsets are connected, each irreducible component lies in a unique connected component, and each connected component is the union of its irreducible components.

However, unlike connected components, it is possible for a given point to lie in more than one irreducible component. We will see examples shortly.

In the case of a Zariski topology $\operatorname{Spec} R$, there is an important algebraic interpretation of the irreducible components. Namely, the irreducible components Y of $\operatorname{Spec} R$ correspond to $V(\mathfrak{p})$ where $\mathfrak{p}$ ranges through the **minimal primes**.

Indeed, we claim that a closed subset $V(I)$ is irreducible iff $\operatorname{rad} I = \mathfrak{p}$ is prime. First, if $\operatorname{rad} I = \mathfrak{p}$ is prime, then by Proposition 13.1 $V(I) = V(\mathfrak{p})$, so it suffices to show that $V(\mathfrak{p})$ is irreducible. If not, there are ideals I and J such that $V(I)$ and $V(J)$ are both proper subsets of $V(\mathfrak{p})$ and $V(\mathfrak{p}) = V(I) \cup V(J) = V(IJ)$. But then $\mathfrak{p} = \operatorname{rad}(IJ) \supset IJ$ and since $\mathfrak{p}$ is prime this implies $\mathfrak{p} \supset I$ or $\mathfrak{p} \supset J$. WLOG, suppose $\mathfrak{p} \supset I$; then $V(\mathfrak{p}) \subset V(I)$, so that $V(I)$ is not proper in $V(\mathfrak{p})$, contradiction.

Next, suppose that $V(I)$ is irreducible, and suppose that $ab \in \operatorname{rad}(I)$. If neither a nor b is in $\operatorname{rad}(I)$, then $V((a)), V((b))$ do not contain $V(I)$, but $V(a) \cup V(b) = V(ab) \supset V(I)$. Therefore $V(a) \cap V(I) = V(aI)$ and $V(b) \cap V(I) = V(bI)$ are two proper closed subsets of $V(I)$ whose union is $V(I)$, thus $V(I)$ is reducible.

It follows that the irreducible components – i.e., the maximal irreducible subsets – are precisely the sets of the form $V(\mathfrak{p})$ as $\mathfrak{p}$ ranges over the distinct minimal prime ideals. Note that we can now deduce that minimal prime ideals exist in any ring as a special case of the existence of irreducible components in any topological space, an example of the use of topological methods to prove purely algebraic results.[52]

Proposition 13.8. *For any commutative ring, the map $\mathfrak{p} \mapsto V(\mathfrak{p})$ gives a bijection from $\operatorname{Spec} R$ to the set of irreducible closed subsets of $\operatorname{Spec} R$.*

Exercise 13.11: Prove Proposition 13.8.

Exercise 13.12: Explain why Proposition 13.8 is, in some sense, a Nullstellensatz for an arbitrary commutative ring.

13.5. **Noetherian spaces.**

We wish to introduce a property of topological spaces which, from the standpoint of conventional geometry, looks completely bizarre:

Proposition 13.9. *For a topological space X, TFAE:*
(i) Every ascending chain of open subsets is eventually constant.
(ibis) Every descending chain of closed subsets is eventually constant.
(ii) Every nonempty family of open subsets has a maximal element.
(iibis) Every nonempty family of closed subsets has a minimal element.
(iii) Every open subset is quasi-compact.
(iv) Every subset is quasi-compact.
*A space satisfying any (and hence all) of these conditions is called **Noetherian**.*

[52] In this case, the same Zorn's Lemma argument establishes the existence of minimal primes, so the topology is not making anything essentially easier for us...yet.

Proof. The equivalence of (i) and (ibis), and of (ii) and (iibis) is immediate from taking complements. The equivalence of (i) and (ii) is a general property of partially ordered sets discussed in section X.X above.

(i) $\iff$ (iii): Assume (i), let U be any open set in X and let $\{V_j\}$ be an open covering of U. We assume for a contradiction that there is no finite subcovering. Choose any j_1 and put $U_1 := V_{j_1}$. Since $U_1 \neq U$, there exists j_2 such that U_1 does not contain V_{j_2}, and put $U_2 = U_1 \cup V_{j_2}$. Again our assumpion implies that $U_2 \supsetneq U$, and continuing in this fashion we will construct an infinite properly ascending chain of open subsets of X, contradiction. Conversely, assume (iii) and let $\{U_i\}_{i=1}^{\infty}$ be an infinite properly ascending chain of subsets. Then $U = \bigcup_i U_i$ is not quasi-compact.

Obviously (iv) $\implies$ (iii), so finally we will show that (iii) $\implies$ (iv). Suppose that $Y \subset X$ is not quasi-compact, and let $\{V_i\}_{i \in I}$ be a covering of Y by relatively open subsets without a finite subcover. We may write each V_i as $U_i \cap Y$ with U_i open in Y. Put $U = \bigcup_i U_i$. Then, since U is quasi-compact, there exists a finite subset $J \subset I$ such that $U = \bigcup_{j \in J} U_j$, and then $Y = U \cap Y = \bigcup_{j \in J} U_j \cap Y = \bigcup_{j \in J} V_j$. □

Corollary 13.10. *A Noetherian Hausdorff space is finite.*

Proof. In a Hausdorff space every quasi-compact subset is closed. Therefore, using the equivalence (i) $\iff$ (iv) in Proposition 13.9, in a Noetherian Hausdorff space every subset is closed, so such a space is discrete. But it is also quasi-compact, so it is finite. □

Proposition 13.11. *For a ring R, TFAE:*
(i) R satisfies the ascending chain condition on radical ideals.
(ii) $\operatorname{Spec} R$ is a Noetherian space.
In particular if R, or even $R^{\mathrm{red}} = R/\operatorname{nil}(R)$, is a Noetherian ring, $\operatorname{Spec} R$ is a Noetherian space.

Proof. Since $I \mapsto V(I)$ gives a bijection between radical ideals and Zariski closed subsets, (ACC) on radical ideals is equivalent to (DCC) on closed subsets. Evidently these conditions occur if R is itself Noetherian, or, since $\operatorname{Spec} R$ is canonically homeomorphic to $\operatorname{Spec} R^{\mathrm{red}}$, if R^{red} is Noetherian. □

Proposition 13.12. *Let X be a Noetherian topological space.*
a) There are finitely many closed irreducible subsets $\{A_i\}_{i=1}^n$ such that $X = \bigcup_{i=1}^n A_i$.
b) Starting with any finite family $\{A_i\}_{i=1}^n$ as in part a) and eliminating all redundant sets – i.e., all A_i such that $A_i \subset A_j$ for some $j \neq i$ – we arrive at the set of irreducible components of X. In particular, the irreducible components of a Noetherian space are finite in number.

Proof. a) Let X be a Noetherian topological space. We first claim that X can be expressed as a finite union of irreducible closed subsets. Indeed, consider the collection of closed subsets of X which cannot be expressed as a finite union of irreducible closed subsets. If this collection is nonempty, then by Proposition 13.9 there exists a minimal element Y. Certainly Y is not itself irreducible, so is the union of two strictly smaller closed subsets Z_1 and Z_2. But Z_1 and Z_2, being strictly smaller than Y, must therefore be expressible as finite unions of irreducible closed subsets and therefore so also can Y be so expressed, contradiction.

b) So write

$$X = A_1 \cup \ldots \cup A_n$$

where each A_i is closed and irreducible. If for some $i \neq j$ we have $A_i \subset A_j$, then we call A_i **redundant** and remove it from our list. After a finite number of such removals, we may assume that the above finite covering of X by closed irreducibles is **irredundant** in the sense that there are no containment relations between distinct A_i's. Now let Z be any irreducible closed subset. Since $Z = \bigcup_{i=1}^n (Z \cap A_i)$ and Z is irreducible, we must have $Z = Z \cap A_i$ for some i, i.e., $Z \subset A_i$. It follows that the "irredundant" A_i's are precisely the maximal irreducible closed subsets, i.e., the irreducible components. □

We deduce the following important result, which is not so straightforward to prove using purely algebraic methods:

Corollary 13.13. *Let I be a proper ideal in a Noetherian ring R. The set of prime ideals $\mathfrak{p}$ which are minimal over I (i.e., minimal among all prime ideals containing I) is finite and nonempty.*

Exercise 13.13: Prove Corollary 13.13.

13.6. **Hochster's Theorem.**

A topological space X is **sober** if for every irreducible closed subspace Y of X, there exists a unique point $y \in Y$ such that $Y = \overline{\{y\}}$. Equivalently, a sober space is one for which every irreducible closed subset has a unique generic point.

Exercise 13.14:
a) Show that any Hausdorff space is sober.
b) Show that a sobser space is Kolmogorov.
c) Show that the cofinite topology on an infinite set is separated but not sober.

Exercise 13.15 (Sobrification): For any topological space X, let X^t be the set of irreducible closed subsets of X. There is a natural map $t : X \to X^t$ via $x \mapsto \overline{\{x\}}$. Give X^t the final topology with respect to t, i.e., the finest topology that makes t continuous. (Explicitly, a subset V of X^t is open iff its preimage in X is open.)
a) Show the map t induces a bijection from the open subsets of X to the open subsets of X^t.
b) Show that X^t is a sober space.
c) Show that t is *universal* for continuous maps from X to a sober topological space: i.e., for every sober space Y and continuous $f : X \to Y$, there exists a unique continuous $F : X^t \to Y$ such that $f = F \circ t$. Thus X^t is (unfortunately!) called the **sobrification** of X.

A topological space X is **spectral** if:
(SS1) X is quasi-compact,
(SS2) X is sober, and
(SS3) The family of quasi-compact open subsets of X is closed under finite intersections and is a base for the topology.

Remark: A Bourbakiste would insist that (SS3) $\implies$ (SS1) by taking the empty intersection. But we will not do so.

Exercise 13.16: Show that a finite space is spectral iff it is T_0.

The following result gives an arguably cleaner characterization of spectral spaces.

Proposition 13.14. *. For a topological space X, TFAE:*
(i) X is homeomorphic to an inverse limit of finite T_0 spaces.
(ii) X is spectral.

Exercise 13.17: Prove Proposition 13.14.

Proposition 13.15. *For any ring R,* $\operatorname{Spec} R$ *is spectral.*

Exercise 13.18: Prove Proposition 13.15. (Hint: you will find the needed results in the previous subsections. Especially, use Proposition 13.8 to prove sobriety.)

For any ring R we endow the set $\operatorname{MaxSpec}(R)$ of maximal ideals of R with the topology it inherits as a subset of $\operatorname{Spec}(R)$. When necessary, we describe $\operatorname{MaxSpec} R$ as the "maximal spectrum" of R.

Proposition 13.16. *For any ring R,* $\operatorname{MaxSpec} R$ *is separated and quasi-compact.*

Exercise 13.19: Prove Proposition 13.16.

Theorem 13.17. *(Hochster's Thesis* [Ho69]*)*
a) A spectral topological space is homeomorphic to the prime spectrum of some ring.
b) A separated quasi-compact space is homeomorphic to the maximal spectrum of some ring.

We do not aspire to give a proof of Theorem 13.17 at this time.

Exercise 13.20: Show that every compact space X is homeomorphic to $\operatorname{MaxSpec}(C(X))$, where $C(X)$ is the ring of continuous $\mathbb{R}$-valued functions on X.

Exercise 13.21:
a) Show that the specialization relation gives an equivalence of categories between the category of T_0 finite spaces and the category of finite partially ordered sets.
b)* Formulate a generalization of part a) in which T_0 finite spaces are replaced by T_0 **Alexandroff spaces**. (A topological space is Alexandroff if an arbitrary intersection of closed subsets is closed.)

Exercise 13.22: Let $n \in \mathbb{Z}^+$.
a) Use Hochster's Thesis and the previous exercise to show that there exists a ring R with exactly n prime ideals $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$ such that $\mathfrak{p}_1 \subset \mathfrak{p}_2 \subset \ldots \subset \mathfrak{p}_n$.
b) For $n = 1, 2$, exhibit Noetherian rings with these properties. For $n \geq 3$, show that there is no such Noetherian ring.

13.7. **Rank functions revisited.**

Theorem 13.18. *Let M be a finitely generated module over a ring R.*
a) For each $n \in \mathbb{N}$, the set

$$U_r = \{\mathfrak{p} \in \operatorname{Spec} R \mid M_{\mathfrak{p}} \text{ can be generated over } R_{\mathfrak{p}} \text{ by at most } r \text{ elements}\}$$

is open in $\operatorname{Spec} R$.
b) If M is finitely presented (e.g. if R is Noetherian), then the set

$$U_F = \{\mathfrak{p} \in \operatorname{Spec} R \mid M_{\mathfrak{p}} \text{ is a free } R_{\mathfrak{p}}\text{-module}\}$$

is open in $\operatorname{Spec} R$.

Proof. (Matsumura) Suppose $M_{\mathfrak{p}} = \langle \omega_1, \ldots, \omega_r \rangle_{R_{\mathfrak{p}}}$. Each ω_i is of the form $\frac{m_i}{s_i}$ with $m_i \in M$ and $s_i \in R \setminus \mathfrak{p}$. But since $s_i \in R_{\mathfrak{p}}^{\times}$ for all i, we also have $\langle m_1, \ldots, m_r \rangle_{R_{\mathfrak{p}}} = M_{\mathfrak{p}}$. Thus it is no loss of generality to assume that each ω_i is the image in $M_{\mathfrak{p}}$ of an element of M. Let $\varphi : R^r \to M$ be the R-linear map given by $(a_1, \ldots, a_r) \mapsto \sum_i a_i \omega_i$, and put $C = \operatorname{coker} \varphi$, whence an exact sequence

$$R^r \to M \to C \to 0.$$

Localizing this at a prime $\mathfrak{q}$ of R gives an exact sequence

$$R_{\mathfrak{q}}^r \to M_{\mathfrak{q}} \to C_{\mathfrak{q}} \to 0.$$

When $\mathfrak{q} = \mathfrak{p}$ we of course have $C_{\mathfrak{q}} = 0$. Moreover, C is a quotient of M hence a finitely generated R-module, so by Proposition 10.11 its support $\operatorname{supp} C$ is a Zariski-closed set. It follows that there exists an open neighborhood V of $\mathfrak{p}$ such that $C_{\mathfrak{q}} = 0$ for all $\mathfrak{q} \in V$.
b) Suppose that $M_{\mathfrak{p}}$ is a free $R_{\mathfrak{p}}$-module with basis $\omega_1, \ldots, \omega_r$. As above it is no loss of generality to assume that each ω_i is the image in $M_{\mathfrak{p}}$ of an element of M. Moreover, as we have also just seen, there exists a basic open neighborhood $U(f)$ such that for all $\mathfrak{q} \in U(f)$, the images of $\omega_1, \ldots, \omega_r$ in $M_{\mathfrak{q}}$ generate $M_{\mathfrak{q}}$ as an $R_{\mathfrak{q}}$-module. Replacing R by R_f and M by M_f we may assume that this occurs for all $\mathfrak{q} \in \operatorname{Spec} R$. Thus $M/\langle \omega_1, \ldots, \omega_r \rangle_R$ is everywhere locally zero, so it is locally zero: $M = \langle \omega_1, \ldots, \omega_r \rangle$. Defining an R-linear map $\varphi : R^r \to M$ as above and setting $K = \operatorname{Ker} \varphi$, we have the exact sequence

$$0 \to K \to R^r \to M \to 0.$$

Since M is finitely *presented*, according to Proposition 3.6 K is a finitely generated R-module. Moreover we have $K_{\mathfrak{p}} = 0$ hence as above $K_{\mathfrak{q}} = 0$ for all $\mathfrak{q}$ on some open neighborhood V of $\mathfrak{p}$. By construction, for each $\mathfrak{q} \in V$, the images of $\omega_1, \ldots, \omega_r$ in $M_{\mathfrak{q}}$ give an $R_{\mathfrak{q}}$-basis for $M_{\mathfrak{q}}$. □

Let M be a finitely generated, locally free module over a ring R. Earlier we defined the rank function $r : \operatorname{Spec} R \to \mathbb{N}$. Applying Theorem 13.18a) to the locally free module M says that the rank function is *lower-semicontinuous*: it can jump up upon specialization, but not jump down.

We now ask the reader to look back at Theorem 7.22 and see that for a finitely generated module M over a general ring R, M is projective iff it is locally free and finitely presented. When R is Noetherian, being finitely presented is equivalent to being finitely generated, so being projective is the same as being locally free. However, in the general case we have had little to say about the distinction between finitely presented and finitely generated modules. Is there some way to rephrase the subtly stronger property of finite presentation, perhaps a more geometric way?

Indeed there is:

Theorem 13.19. *Let M be a finitely generated locally free R-module. TFAE:*
(i) The rank function $r_M : \operatorname{Spec} R \to \mathbb{N}$ is locally constant.
(ii) M is a projective module.

Proof. (i) $\implies$ (ii): By Theorem 7.22, it is enough to show that for all $\mathfrak{m} \in \operatorname{MaxSpec} R$, there is $f \in R \setminus \mathfrak{m}$ such that M_f is a free module. Let $n = r(\mathfrak{m})$, and let $x_1, \ldots, x_n$ be an $R_{\mathfrak{m}}$-basis for $M_{\mathfrak{m}}$. Choose $X_1, \ldots, X_n \in M$ such that for all i, the image of X_i in $M_{\mathfrak{m}}$ is of the form $u_i x_i$ for $u_u \in R_{\mathfrak{m}}^\times$. Let $u : R^n \to M$ be the map sending the ith standard basis element e_i to X_i. Since M is finitely generated, by Proposition 7.20 there is $f \in R \setminus \mathfrak{m}$ such that $u_f : R_f^n \to M_f$ is surjective. It follows that for all $g \in R \setminus \mathfrak{m}$, u_{fg} is surjective. Moreover, by hypothesis there is some such g such that $r(\mathfrak{p}) = n$ for all $\mathfrak{p} \in X(g)$. Replacing f by fg we may assume that $r(\mathfrak{p}) = n$ for all $\mathfrak{p} \in X(f)$. For all such $\mathfrak{p}$, $u_{\mathfrak{p}} : R_{\mathfrak{p}}^n \to M_{\mathfrak{p}}$ is therefore a surjective endomorphism from a rank n free module to itself. Since finitely generated modules are Hopfian, $u_{\mathfrak{p}}$ is an isomorphism. By the local nature of isomorphisms (Proposition 7.12) we conclude u_f is an isomorphism, so M_f is free.
(ii) $\implies$ (i): By Theorem 7.22, M is Z-locally free: there exists a finite Z-family $\{f_i\}_{i \in I}$ such that for all $i \in I$, M_{f_i} is finitely generated and free. Thus the module $\prod_{i=1}^n M_{f_i}$ is finitely generated and projective over the faithfully flat R-algebra $\prod_{i=1}^n R_{f_i}$, so by faithfully flat descent (Theorem 3.104) M itself is projective. □

Corollary 13.20. *Let R be a ring with* $\operatorname{Spec} R$ *irreducible (e.g. a domain). For a finitely generated R-module M, TFAE:*
(i) R is projective.
(ii) R is Z-locally free.
(iii) R is locally free.
(iv) R is flat.

Exercise 13.24: Prove Corollary 13.20.

14. Integrality in Ring Extensions

14.1. First properties of integral extensions.

If S is a ring extension of R – i.e., $R \subset S$ – we will say that an element α of S is **integral** over R if there exist $a_0, \ldots, a_{n-1} \in R$ such that

$$\alpha^n + a_{n-1}\alpha^{n-1} + \ldots + a_1\alpha + a_0 = 0.$$

Note that every element $\alpha \in R$ satisfies the monic polynomial $t - \alpha = 0$, so is integral over R.

Theorem 14.1. *Let $R \subset T$ be an inclusion of rings, and $\alpha \in T$. TFAE:*
(i) α is integral over R.
(ii) $R[\alpha]$ is finitely generated as an R-module.
(iii) There exists an intermediate ring $R \subset S \subset T$ such that $\alpha \in S$ and S is finitely generated as an R-module.
(iv) There exists a faithful $R[\alpha]$-submodule M of T which is finitely generated as an R-module.

Proof. (i) $\implies$ (ii): If α is integral over R, there exist $a_0, \ldots, a_{n-1} \in R$ such that

$$\alpha^n + a_{n-1}\alpha^{n-1} + \ldots + a_1\alpha + a_0 = 0,$$

or equivalently

$$\alpha^n = -a_{n-1}\alpha^{n-1} - \ldots - a_1\alpha - a_0.$$

This relation allows us to rewrite any element of $R[\alpha]$ as a polynomial of degree at most $n-1$, so that $1, \alpha, \ldots, \alpha^{n-1}$ generates $R[\alpha]$ as an R-module.

(ii) $\implies$ (iii): Take $T = R[\alpha]$.
(iii) $\implies$ (iv): Take $M = S$.
(iv) $\implies$ (i): Let $m_1, \ldots, m_n$ be a finite set of generators for M over R, and express each of the elements $m_i\alpha$ in terms of these generators:

$$\alpha m_i = \sum_{j=1}^{n} r_{ij} m_j, \ r_{ij} \in R.$$

Let A be the $n \times n$ matrix $\alpha I_n - (r_{ij})$; then recall from linear algebra that

$$AA^* = \det(A) \cdot I_n,$$

where A^* is the "adjugate" matrix (of cofactors). If $m = (m_1, \ldots, m_n)$ (the row vector), then the above equation implies $0 = mA = mAA^* = m \det(A) \cdot I_n$. The latter matrix equation amounts to $m_i \det(A) = 0$ for all i. Thus $\bullet \det(A) = \bullet 0$ on M, and by faithfulness this means $\det(A) = 0$. Since so that α is a root of the monic polynomial $\det(T \cdot I_n - (a_{ij}))$. □

Exercise 14.1: Let S be a finitely generated R-algebra. Show that TFAE:
(i) S/R is integral.
(ii) S is finite over R (as an R-module!).
In particular, if S/R is an extension and $\alpha_1, \ldots, \alpha_n$ are all integral over R, then $R[\alpha_1, \ldots, \alpha_n]$ is a finitely generated R-module.

Proposition 14.2. *(Integrality is preserved under quotients and localizations) Let S/R be an integral ring extension.*
a) Let J be an ideal of S. Then S/J is an integral extension of $R/(J \cap R)$.
b) Let T be a multiplicatively closed subset of nonzero elements of R. Then S_T is an integral extension of R_T.

Proof. a) First note that the kernel of the composite map $R \hookrightarrow S \to S/J$ is $J \cap R$, so that $R/(J \cap R) \hookrightarrow S/J$ is indeed a ring extension. Any element of S/J is of the form $x + J$ for $x \in S$, and if $P(t)t^n + a_{n-1}t^{n-1} + \ldots + a_1 t + a_0 = 0 \in R[t]$ is a polynomial satisfied by x, then reducing coefficientwise gives a monic polynomial $\overline{P}(t) \in R/(J \cap R)$ satisfied by x.

b) Let $J = \{s \in S \mid \exists t \in T \mid ts = 0\}$, an ideal of S. Let $\overline{T}$ be the image of T in $R/(J \cap R)$. Then $S_T \cong (S/J)_{\overline{T}}$ and $J_T \cong (R/(J \cap R))_{\overline{T}}$, so we may assume that the maps $R \to R_T$ and $S \to S_T$ are injective. Let $\frac{x}{y} \in S_T$ with $x \in S, \ y \in T$. Let $P(t) = t^n + a_{n-1}t^{n-1} + \ldots + a_0 \in R[t]$ be a monic polynomial satisfied by x. Then

$$\left(\frac{x}{y}\right)^n + \frac{a_{n-1}}{y}\left(\frac{x}{y}\right)^{n-1} + \ldots + \frac{a_0}{y^n} = 0,$$

showing that $\frac{x}{y}$ is integral over R_T. □

Lemma 14.3. *Let $R \subset S \subset T$ be an inclusion of rings. If $\alpha \in T$ is integral over R, then it is also integral over S.*

Proof. If α is integral over R, there exists a monic polynomial $P \in R[t]$ such that $P(\alpha) = 0$. But P is also a monic polynomial in $S[t]$ such that $P(\alpha) = 0$, so α is also integral over S. □

Lemma 14.4. *Let $R \subset S \subset T$ be rings. If S is a finitely generated R-module and T is a finitely generated S-module, then T is a finitely generated R-module.*

Proof. If $\alpha_1, \ldots, \alpha_r$ generates S as an R-module and $\beta_1, \ldots, \beta_s$ generates T as an S-module, $\{\alpha_i \beta_j\}_{1 \leq i \leq r, 1 \leq j \leq s}$ generates T as an R-module: for $\alpha \in T$,

$$\alpha = \sum_j b_j \beta_j = \sum_i \sum_j (a_{ij} \alpha_i) \beta_j,$$

with $b_j \in S$ and $a_{ij} \in R$. □

Corollary 14.5. *(Transitivity of integrality) If $R \subset S \subset T$ are ring extensions such that S/R and T/S are both integral, then T/R is integral.*

Proof. For $\alpha \in S$, let $\alpha^n + b_{n-1}\alpha^{n-1} + \ldots + b_1 \alpha + b_0 = 0$ be an integral dependence relation, with $b_i \in S$. Thus $R[b_1, \ldots, b_{n-1}, \alpha]$ is finitely generated over $R[b_1, \ldots, b_{n-1}]$. Since S/R is integral, $R[b_1, \ldots, b_{n-1}]$ is finite over R. By Lemma 14.4, $R[b_1, \ldots, b_{n-1}, \alpha]$ is a subring of T containing α and finitely generated over R, so by Theorem 14.1, α is integral over R. □

Corollary 14.6. *If S/R is a ring extension, then the set $I_S(R)$ of elements of S which are integral over R is a subring of S, the **integral closure of** R **in** S. Thus $R \subset I_S(R) \subset S$.*

Proof. If $\alpha \in S$ is integral over R, $R[\alpha_1]$ is a finitely generated R-module. If α_2 is integral over R it is also integral over $R[\alpha_1]$, so that $R[\alpha_1][\alpha_2]$ is finitely generated as an $R[\alpha_1]$-module. By Lemmma 14.4, this implies that $R[\alpha_1,\ \alpha_2]$ is a finitely generated R-module containing $\alpha_1 \pm \alpha_2$ and $\alpha_1 \cdot \alpha_2$. By Theorem 14.1, this implies that $\alpha_1 \pm \alpha_2$ and $\alpha_1 \alpha_2$ are integral over R. □

If $R \subset S$ such that $I_S(R) = R$, we say R is **integrally closed** in S.

Proposition 14.7. *Let S be a ring. The operator $R \mapsto I_S(R)$ on subrings of R is a closure operator in the abstract sense, namely it satisfies:*
(CL1) $R \subset I_S(R)$,
(CL2) $R_1 \subset R_2 \implies I_S(R_1) \subset I_S(R_2)$.
(CL3) $I_S(I_S(R)) = I_S(R)$.

Proof. (CL1) is the (trivial) Remark 1.1. (CL2) is obvious: evidently if $R_1 \subset R_2$, then every element of S which satisfies a monic polynomial with R_1-coefficients also satisfies a monic polynomial with R_2-coefficients. Finally, suppose that $\alpha \in S$ is such that $\alpha^n + a_{n-1}\alpha^{n-1} + \ldots + a_1 \alpha + a_0 = 0$ for $a_i \in I_S(R)$. Then each a_i is integral over R, so $R[a_1, \ldots, a_n]$ is finitely generated as an R-module, and since $R[a_1, \ldots, a_n, \alpha]$ is finitely generated as an $R[a_1, \ldots, a_n]$-module, applying Lemma 14.4 again, we deduce that α lies in the finitely generated R-module $R[a_1, \ldots, a_n, \alpha]$ and hence by Theorem 14.1 is integral over R. □

14.2. **Integral closure of domains.**

Until further notice we restrict to the case in which $R \subset S$ are **integral domains**.

Proposition 14.8. *Let $R \subset S$ be an integral extension of domains.*
a) R is a field iff S is a field.
b) An extension of fields is integral iff it is algebraic.

Proof. a) Suppose first that R is a field, and let $0 \neq \alpha \in S$. Since α is integral over R, $R[\alpha]$ is finitely generated as an R-module, and it is well-known in field theory that

this implies $R[\alpha] = R(\alpha)$. Indeed, taking the polynomial of least degree satisfied by α, say $\alpha(\alpha^{n-1} + a_{n-1}\alpha^{n-2} + \ldots + a_1) = -a_0$, then $0 \neq a_0 \in R$ is invertible, so

$$\frac{-(\alpha^{n-1} + a_{n-1}\alpha^{n-2} + \ldots + a_1)}{a_0} = \frac{1}{\alpha},$$

and S is a field. Conversely, if S is a field and $a \in R$, then $R[a^{-1}]$ is finite-dimensional over R, i.e., there exist $a_i \in R$ such that

$$a^{-n} = a_{n-1}a^{-n+1} + \ldots + a_1 a^{-1} + a_0.$$

Multiplying through by a^{n-1} gives

$$a^{-1} = a_{n-1} + a_{n-2}a + \ldots + a_1 a^{n-2} + a_0 a^{n-1} \in R,$$

completing the proof of part a). Over a field every polynomial relation can be rescaled to give a monic polynomial relation, whence part b). □

Remark: A more sophisticated way of expressing Proposition 14.8 is that if S/R is an integral extension of domains, then $\dim R = 0$ iff $\dim S = 0$. Later we will see that in fact $\dim R = \dim S$ under the same hypotheses.

If $R \subset S$ are fields, $I_S(R)$ is called the **algebraic closure** of R in S.

Exercise 14.2:
a) Let S/R be an extension of fields. If S is algebraically closed, then so is $I_S(R)$.
b) Deduce that if $R = \mathbb{Q}$, $S = \mathbb{C}$, then $I_S(R)$ is an algebraically closed, algebraic extension of $\mathbb{Q}$, denoted $\overline{\mathbb{Q}}$ and called the field of all algebraic numbers.

Theorem 14.9. *Let S/R be an extension of integral domains, and let $T \subset R$ be a multiplicatively closed subset. Then $I_{T^{-1}S}(T^{-1}R) = T^{-1}I_S(R)$. In other words, localization commutes with integral closure.*

Proof. Let K be the fraction field of R and L the fraction field of S. Then $T^{-1}I_S(R)$ is the subring of L generated by T^{-1} and the elements of S which are integral over R. Since both of these kinds of elements of $T{-}1S$ are integral over $T^{-1}R$ and integral elements form a subring, we must have $T^{-1}I_S(R) \subset I_{T^{-1}S}(T^{-1}R)$. Conversely, let $x \in T^{-1}S$ be integral over $T^{-1}(R)$, so there are $b_0, \ldots, b_{n-1} \in T^{-1}(R)$ such that

$$x^n + b_{n-1}x^{n-1} + \ldots + b_1 x + b_0 = 0.$$

We may take a common denominator $t \in T$ such that $x = \frac{s}{t}$ and for all $0 \leq i \leq n{-}1$, $b_i = \frac{a_i}{t}$. Making this substitution and multiplying through by t^n, we get

$$s^n + a_{n-1}s^{n-1} + ta_{n-2}s^{n-2} + \ldots + t^{n-2}a_1 s + t^{n-1} = 0.$$

Thus s is integral ove R and $x = \frac{s}{t} \in T^{-1}I_S(R)$. □

Proposition 14.10. *Let S/R be an extension of domains. Let K be the fraction field of R and M the fraction field of S. Then the fraction field of $I_S(R)$ is $I_M(K)$.*

Proof. We write L for the fraction field of $I_S(R)$. First we show $I_M(K) \subset L$: let $x \in I_S(K)^\bullet$, so there are $a_0, \ldots, a_{n-1} \in K$ such that $x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0 = 0$. After clearing denominators and relabelling, we get $a_0, \ldots, a_n \in R$ such that

$$a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0 = 0.$$

Multiplying through by a_n^{n-1}, we get

$$(a_n x)^n + a_{n-1}(a_n x)^{n-1} + \ldots + a_1 a_n^{n-2}(a_n x) + a_n^{n-1} a_0 = 0,$$

which shows $a_n x \in I_S(R)$, so $x \in I_S(R) \cdot (R \setminus 0)^{-1} \subset L$.

The reverse inclusion $L \subset I_M(K)$ is quite similar, since an arbitrary nonzero element x of L is of the form $\frac{\alpha}{\beta}$ with α, β integral over R. But then certainly α and β are both integral over K – i.e., algebraic over K, and then so also are β^{-1} and $x = \frac{\alpha}{\beta}$. So again x satisfies a polynomial $a_n t^n + \ldots$ with coefficients in R and then $a_n x$ is integral over R, hence $a_n x$ and a_n are algebraic over K and thus $x = \frac{a_n x}{x}$ is algebraic over K so lies in $I_M(K)$. □

Example: If $R = \mathbb{Z}$, $S = \mathbb{C}$, then $I_S(R)$ is called **the ring of all algebraic integers**, and often denoted $\overline{\mathbb{Z}}$. By Proposition 14.10, its fraction field is the field $\overline{\mathbb{Q}}$ of all algebraic numbers. This turns out to be a very interesting ring, and it will crop up several times in the sequel as an example or counterexample. For instance:

Exercise 14.3: Show that $\overline{\mathbb{Z}}$ is not finitely generated as a $\mathbb{Z}$-module.[53]

Corollary 14.11. *Let R be a domain with fraction field K and M/K an arbitrary field extension. Put $S = I_M(R)$. Then S is integrally closed.*

Proof. By Proposition 14.10, the field of fractions L of S is the algebraic closure of K in M. If $x \in L$ is integral over R, then since $L \subset M$ it lies in $I_M(R) = S$. □

Remark on terminology: It is unfortunate that the word "integral" in commutative algebra is used both to describe rings without zero divisors and also – quite distinctly – to describe an extension satisfying a certain kind of finiteness condition. The first use of the word "integral" is essentially redundant in the algebraic setting: if we just said "domain" instead of "integral domain", the meaning would be the same. However, in geometric language one has the notion of an "integral scheme"; in the case of the affine scheme $\operatorname{Spec} R$ associated to a commutative ring R, the meaning of this is precisely that R be a domain, and because of this it is undesirable to banish the "integral" from "integral domain." Perhaps it would be better instead to replace the term "integral extension." We leave it as an exercise to the reader to suggest some alternate terminology: this is less silly than it sounds, because in order to do this one needs to grapple with the question, "What is an integral extension, really?" It is perhaps telling that there is, so far as I know, no notion of an "integral scheme extension" in algebraic geometry.

Let R be an integral domain with fraction field K. We say that R is **integrally closed** if $I_K(R) = R$, i.e., if any element of the fraction field satisfying a monic integral polynomial with R-coefficients already belongs to R. It follows immediately from Proposition 14.7 that in any case $I_K(R)$ is integrally closed.

Exercise 14.4: Let $R = \mathbb{Z}[\sqrt{-3}] = \mathbb{Z}[t]/(t^2 + 3)$. Show that R is not integrally closed, and compute its integral closure.

The geometric terminology for an integrally closed domain is **normal**. The process of replacing R by its integral closure $I_K(R)$ is often called **normalization**.

[53] In fact it is not even a Noetherian ring, so not even finitely generated as a $\mathbb{Z}$-algebra.

14.3. **Spectral properties of integral extensions.**

Going down (GD): If we have $I_1 \supset I_2$ of R and $J_1 \in \operatorname{Spec} S$ such that $J_1 \cap R = I_1$, there exists $J_2 \in \operatorname{Spec} S$ such that $J_2 \subset J_1$ and $J_2 \cap R = I_2$.

Lemma 14.12. *Let R be a local ring with maximal ideal $\mathfrak{p}$ and S/R an integral extension. Then the pushed forward ideal $\mathfrak{p}S$ is proper.*

Proof. Suppose not: then there exist $p_i \in \mathfrak{p}$, $s_i \in S$ such that $1 = \sum_i s_i p_i$. Therefore any counterxample would take place already in the finite R-module $R[s_1, \ldots, s_d]$. By induction on d, it is enough to consider the case of $n = 1$: $S = R[s]$. Consider as usual a relation

$$s^n = a_{n-1}s^{n-1} + \ldots + a_1 s + a_0,\ a_i \in R \tag{30}$$

of minimal possible degree n. If $1 \in \mathfrak{p}S$ then we have

$$1 = p_0 + p_1 s + \ldots + p_k s^k,\ p_i \in \mathfrak{p}. \tag{31}$$

In view of (30) we may assume $k \leq n-1$. Since $1 - p_0$ is not in the maximal ideal of the local ring R, it is therefore a unit; we may therefore divide (31) by $1 - p_0$ and get an equation of the form

$$1 = p_1' s + \ldots + p_q' s^q,\ p_i' \in \mathfrak{p}.$$

This shows that $s \in S^\times$. Replacing $a_0 = a_0 \cdot 1$ in (30) by $a_0(p_1' s + \ldots + p_q' s^q)$, we get an integral dependence relation which is a polynomial in s with no constant term. Since s is a unit, we may divide through by it and get an integral dependence relation of smaller degree, contradiction. □

Theorem 14.13. *An integral ring extension S/R satisfies property (LO):*[54] *every prime ideal $\mathfrak{p}$ of R is of the form $S \cap \mathcal{P}$ for a prime ideal $\mathcal{P}$ of S.*

Proof. For $\mathfrak{p}$ a prime ideal of R, we denote – as usual – by $R_\mathfrak{p}$ the localization of R at the multiplicatively closed subset $R \setminus \mathfrak{p}$. Then $R_\mathfrak{p}$ is local with unique maximal ideal $\mathfrak{p}R_\mathfrak{p}$, and if we can show that there exists a prime ideal $\mathcal{Q}$ of $S_\mathfrak{p}$ lying over $\mathfrak{p}R_\mathfrak{p}$, then the pullback $\mathcal{P} = \mathcal{Q} \cap S$ to S is a prime ideal of S lying over $\mathfrak{p}$. By Lemma 14.12, there exists a maximal ideal $\mathcal{Q} \supset \mathfrak{p}S$ and then $\mathcal{Q} \cap R$ is a proper ideal containing the maximal ideal $\mathfrak{p}$ and therefore equal to it. □

Corollary 14.14. *(Going up theorem of Cohen-Seidenberg* [CS46]*) Let S/R be an integral extension and $\mathfrak{p} \subset \mathfrak{q}$ be two prime ideals of R. Let $\mathcal{P}$ be a prime ideal of S lying over $\mathfrak{p}$ (which necessarily exists by Theorem 14.13). Then there exists a prime ideal $\mathcal{Q}$ of S containing $\mathcal{P}$ and lying over $\mathfrak{q}$.*

Proof. Apply Theorem 14.13 with $R = R/\mathfrak{p}$ $S = S/\mathcal{P}$ and $\mathfrak{p} = \mathfrak{q}/\mathfrak{p}$. □

Corollary 14.15. *(Incomparability) Suppose S/R is integral and $\mathcal{P} \subset \mathcal{Q}$ are two primes of S. Then $\mathcal{P} \cap R \neq \mathcal{Q} \cap R$.*

Proof. By passage to $S/\mathcal{P}$, we may assume that $\mathcal{P} = 0$ and S is an integral domain, and our task is to show that any nonzero prime ideal $\mathcal{P}$ of S lies over a nonzero ideal of R. Indeed, let $0 \neq x \in \mathcal{P}$, and let $P(t) = t^n + a_{n-1}t^{n-1} + \ldots + a_0 \in R[t]$ be a monic polynomial satisfied by x; we may assume $a_0 \neq 0$ (otherwise divide by t). Then $a_0 \in xS \cap R \subset \mathcal{P} \cap R$. □

[54] Or, **lying over**.

Corollary 14.16. *Let S/R be an integral extension, $\mathcal{P}$ a prime ideal of S lying over $\mathfrak{p}$. Then $\mathcal{P}$ is maximal iff $\mathfrak{p}$ is maximal.*

Proof. First proof: Consider the integral extension $S/\mathcal{P}/(R/\mathfrak{p})$; the assertion to be proved is that $S/\mathcal{P}$ is a field iff $R/\mathfrak{p}$ is a field. But this is precisely Proposition 14.8a).

Second proof: If $\mathfrak{p}$ is not maximal, it is properly contained in some maximal ideal $\mathfrak{q}$. By the Going Up Theorem, there exists a prime $\mathcal{Q} \supset \mathcal{P}$ lying over $\mathfrak{q}$, so $\mathcal{P}$ is not maximal. Conversely, suppose that $\mathfrak{p}$ is maximal but $\mathcal{P}$ is not, so there exists $\mathcal{Q} \supsetneq \mathcal{P}$. Then $\mathcal{Q} \cap R$ is a proper ideal containing the maximal ideal $\mathfrak{p}$, so $\mathcal{Q} \cap R = \mathfrak{p} = \mathcal{P} \cap R$, contradicting the Incomparability Theorem. □

Invoking Going Up and Incomparability to (re)prove the elementary Corollary 14.16 is overkill, but these more sophisticated tools also prove the following

Corollary 14.17. *Let S/R be an integral extension of rings. Then the Krull dimensions of R and S are equal.*

Proof. Recall that the Krull dimension of a ring is the supremum of the length of a finite chain of prime ideals. Suppose $\mathfrak{p}_0 \subsetneq \mathfrak{p}_1 \subsetneq \ldots \subsetneq \mathfrak{p}_d$ are primes in R. Applying Theorem 14.1, we get a prime $\mathcal{P}_0$ of S lying over $\mathfrak{p}_0$, and then repeated application of the Going Up Theorem yields a chain of primes $\mathcal{P}_0 \subsetneq \mathcal{P}_1 \subsetneq \ldots \subsetneq \mathcal{P}_d$, so that $\dim(S) \geq \dim(R)$. Similarly, if we have a chain of prime ideals $\mathcal{P}_0 \subsetneq \ldots \subsetneq \mathcal{P}_d$ of length d in S, then Theorem 14.15 implies that for all $0 \leq i < d$, $\mathcal{P}_i \cap R \subsetneq \mathcal{P}_{i+1}$. □

14.4. **Integrally closed domains.**

Let S/R be an extension of integral domains. Immediately from the definition of integrality, there is a concrete way to show that $x \in S$ is integral over R: it suffices to exhibit a monic polynomial $P \in R[t]$ with $P(x) = 0$. What if we want to show that $x \in S$ is *not* integral over R? It would suffice to show that $R[x]$ is not a finitely generated R-module, but exactly how to do this is not clear.

As an example, it is obvious that $\alpha = \sqrt{2}$ is an algebraic integer, but unfortunately it is not obvious that $\beta = \frac{\sqrt{2}}{2}$ is not an algebraic integer. (And of course we need to be careful, because e.g. $\gamma = \frac{1+\sqrt{5}}{2}$ is an algebraic integer, since it satisfies $t^2 + t - 1 = 0$.) One thing to notice is that unlike α and γ, the minimal polynomial of β, $t^2 - \frac{1}{2}$, does not have $\mathbb{Z}$-coefficients. According to the next result, this is enough to know that β is not integral over $\mathbb{Z}$.

Theorem 14.18. *Let R be a domain with fraction field K, S/R an extension ring, and $x \in S$ an integral element over R.*
a) Let $P(t) \in K[t]$ be the minimal polynomial of x over K. Then $P(t) \in I_K(R)[t]$.
b) If R is integrally closed, the minimal polynomial of x has R-coefficients.

Proof. a) We may assume without loss of generality that $S = R[x]$; then, by integrality, S is a finite R-module. Let L be the fraction field of S, $d = [L : K]$, and let $s_1, \ldots, s_d$ be a K-basis for L consisting of elements of S. Because the minimal polynomial $P(t)$ is irreducible over K, it is also the characteristic polynomial of $x\cdot$ viewed as a K-linear automorphism of L. Evidently the matrix M_x of $x\cdot$ with

respect to the basis $s_1, \ldots, s_d$ has coefficients in $S \cap K$, hence in $I_K(R)$. The coefficients of $P(t)$ are polynomials in the entries of the matrix M_x, hence they also lie in $I_K(R)$. Part b) follows immediately. □

Exercise 14.5: Let R be a domain with fraction field K. Let S/R be an extension such that for every $x \in S$ which is integral over R, the minimal polynomial $P(t) \in K[t]$ has R-coefficients. Show that R is integrally closed.

Theorem 14.19. *(Local nature of integral closure) For a domain R, TFAE:*
(i) R is integrally closed.
(ii) For all prime ideals $\mathfrak{p}$ of R, $R_{\mathfrak{p}}$ is integrally closed.
(iii) For all maximal ideals $\mathfrak{m}$ of R, $R_{\mathfrak{m}}$ is integrally closed.

Proof. Let K be the fraction field of R. Assume (i), and let $\mathfrak{p} \in \operatorname{Spec} R$. By Theorem 14.9, the integral closure of $R_{\mathfrak{p}}$ in K is $R_{\mathfrak{p}}$. Evidently (ii) $\implies$ (iii). Assume (iii), and let x be an element of K which is integral over R. Then for every maximal ideal $\mathfrak{m}$ of R, certainly x is integral over $R_{\mathfrak{m}}$, so by assumption $x \in R_{\mathfrak{m}}$ and thus $x \in \bigcap_{\mathfrak{m}} R_{\mathfrak{m}}$. By Corollary 7.13 we have $\bigcap_{\mathfrak{m}} R_{\mathfrak{m}} = R$. □

Exercise 14.6: Let R be an integrally closed domain with fraction field K, L/K an algebraic field extension, S the integral closure of R in L and $G = \operatorname{Aut}(L/K)$.
a) Show that for every $\sigma \in G$, $\sigma(S) = S$.
b) For $\mathcal{P} \in \operatorname{Spec} S$ and $\sigma \in G$, show $\sigma(\mathcal{P}) = \{\sigma(x) \mid x \in \mathcal{P}\}$ is a prime ideal of S.
c) Show that $\mathcal{P} \cap R = \sigma(\mathcal{P}) \cap R$.
In conclusion, for every $\mathfrak{p} \in \operatorname{Spec} R$, there is a well-defined action of G on the (nonempty!) set of prime ideals $\mathcal{P}$ of S lying over $\mathfrak{p}$.

Lemma 14.20. *Let R be a domain with fraction field K of characteristic $p > 0$, let L/K be a purely inseparable algebraic extension of K (possibly of infinite degree), and let S be the integral closure of R in L. For any $\mathfrak{p} \in \operatorname{Spec} R$, $\operatorname{rad}(\mathfrak{p}R)$ is the unique prime of S lying over $\mathfrak{p}$.*

Exercise 14.7: Prove Lemma 14.20. (Suggestions: recall that since L/K is purely inseparable, for every $x \in L$, there exists $a \in \mathbb{N}$ such that $x^{p^a} \in K$. First observe that $\operatorname{rad}(\mathfrak{p}R)$ contains every prime ideal of S which lies over $\mathfrak{p}$ and then show that $\operatorname{rad}(\mathfrak{p}R)$ is itself a prime ideal.)

Theorem 14.21. *(Going Down Theorem of Cohen-Seidenberg* [CS46]*) Let R be an integrally closed domain with fraction field K, and let S be an integral extension of R. If $\mathfrak{p}_1 \subset \mathfrak{p}_2$ are prime ideals of R and $\mathcal{P}_2$ is a prime ideal of S lying over $\mathfrak{p}_2$, then there exists a prime ideal $\mathcal{P}_1$ of S which is contained in $\mathcal{P}_2$ and lies over $\mathfrak{p}_1$.*

Proof. Let L be a normal extension of K containing S, and let T be the integral closure of R in L. In particular T is integral over S, so we may choose $\mathcal{Q}_2 \in \operatorname{Spec} T$ lying over $\mathcal{P}_2$ and also $\mathcal{Q}_1 \in \operatorname{Spec} T$ lying over $\mathfrak{p}_1$. By the Going Up Theorem there exists $\mathcal{Q}' \in \operatorname{Spec} T$ containing $\mathcal{Q}_1$ and lying over $\mathfrak{p}_2$. Both $\mathcal{Q}_2$ and $\mathcal{Q}'$ lie over $\mathfrak{p}_2$, so by Theorem 14.36 there exists $\sigma \in \operatorname{Aut}(L/K)$ such that $\sigma(\mathcal{Q}') = \mathcal{Q}_2$. Thus $\sigma(\mathcal{Q}_1) \subset \sigma(\mathcal{Q}') = \mathcal{Q}_2$ and $\sigma(\mathcal{Q}_1)$ lies over $\mathfrak{p}_1$, so that setting $\mathcal{P}_1 = \sigma(\mathcal{Q}_1) \cap S$ we have $\mathcal{P}_1 \cap R = \mathfrak{p}_1$ and $\mathcal{P}_1 \subset \sigma(\mathcal{Q}') \cap S = \mathcal{Q}_2 \cap S = \mathcal{P}_2$. □

Remark: In [AM, Chapter 5] one finds a proof of Theorem 14.21 which avoids all Galois-theoretic considerations. However it is significantly longer than the given proofs of Theorems 14.36 and 14.21 combined and – to me at least – rather opaque.

14.5. **The Noether Normalization Theorem.**

14.5.1. *The classic version.*

Theorem 14.22. *(Noether Normalization) Let k be a field, $R = k[x_1, \ldots, x_m]$ an integral domain which is a finitely generated k-algebra,*[55] *and let K be the fraction field of R.*
a) There exists $d \in \mathbb{Z}$, $0 \leq d \leq m$, and algebraically independent elements $y_1, \ldots, y_d \in R$ such that R is finitely generated as a module over the polynomial ring $k[y_1, \ldots, y_d]$ – or equivalently, that $R/k[y_1, \ldots, y_d]$ is an integral extension.
b) The integer d is equal to both the Krull dimension of R and the transcendence degree of K/k.

Proof. a) (Jacobson) The result is trivial if $m = d$, so we may suppose $m > d$. Then the y_i are algebraically dependent over k: there exists a nonzero polynomial

$$f(s_1, \ldots, s_m) = \sum a_J s_1^{j_1} \cdots s_m^{j_m}, a_J \in k[s_1, \ldots, s_m]$$

with $f(x_1, \ldots, x_m) = 0$. Let X be the set of monomials $s^J = s_1^{j_1} \cdots s_m^{j_m}$ occuring in f with nonzero coefficients. To each such monomial we associate the univariate polynomial

$$j_1 + j_2 t + \ldots + j_m t^{m-1} \in \mathbb{Z}[t].$$

The polynomials obtained in this way from the elements of X are distinct. Since a univariate polynomial over a field has only finitely many zeroes, it follows that there exists $a \geq 0$ such that the integers $j_1 + j_2 a + \ldots + j_m a^{m-1}$ obtained from the monomials in X are distinct. Now consider the polynomial

$$f(s_1, s_1^a + t_1, \ldots, s_1^{a^{m-1}} + t_m) \in k[s, t].$$

We have

$$f(s_1, s_1^a + t_1, \ldots, s_1^{a^{m-1}} + t_m) = \sum_J a_J s_1^{j_1} (s_1^d + t_2)^{j_2} \cdots (s_1^{a^{m-1}} + t_m)^{j_m}$$

$$= \sum_J a_J s_1^{j_1 + j_2 a + \ldots + j_m a^{m-1}} + g(s_1, t_2, \ldots, y_m),$$

in which the degree of g in s_1 is less than that of $\sum_J a_J s_1^{j_1 + j_2 a + \ldots + j^m a^{m-1}}$. Hence for suitable $\beta \in k^\times$, $\beta f(s_1, s_1^a + t_2, \ldots, s_1^{a^{m-1}} + t_m)$ is a monic polynomial in x_1 with $k[t_2, \ldots, t_m]$-coefficients. Putting $w_i = x_i - x_1^{a^{i-1}}$ for $2 \leq i \leq m$, we get

$$\beta f(x_1, x_1^d + w_2, \ldots, x_1^{a^{m-1}} + w_m) = 0,$$

so that x_1 is integral over $R' = k[w_2, \ldots, w_m]$. By induction on the number of generators, R' has a transcendence base $\{y_i\}_{i=1}^d$ such that R' is integral over $k[y_1, \ldots, y_d]$. Thus R is integral over $k[y_1, \ldots, y_d]$ by transitivity of integrality.
b) Since $R/k[y_1, \ldots, y_d]$ is integral, by Corollary 14.17 the Krull dimension of R is equal to the Krull dimension of $k[y_1, \ldots, y_d]$, which by Corollary 12.17 is d. Since R is finitely generated as a $k[y_1, \ldots, y_d]$ algebra, by Proposition 14.10 K is finitely generated as a $k(y_1, \ldots, y_d)$-module, so $\operatorname{trdeg} K/k = \operatorname{trdeg} k(y_1, \ldots, y_d) = d$. □

[55] Here the x_i's are *not* assumed to be independent indeterminates.

14.5.2. *Separable Noether Normalization.*

Let K be a field and let $\overline{K}$ an algebraic closure of K. A field extension L/K is **regular** if $L \otimes_K \overline{K}$ is a field (equivalently, a domain).

For a field extension L/K, we say **K is algebraically closed in L** if any element of L which is algebraic over K lies in K. It is an easy exercise to show that if L/K is regular, K is algebraically closed in L. The converse is true in characteristic zero, but in positive characteristic we need a further hypothesis:

Theorem 14.23. *Let L/K be a field extension.*
a) The following are equivalent:
(i) L/K is regular.
(ii) L/K is separable and K is algebraically closed in L.
b) In particular, if K is perfect and algebraically closed in L, then L/K is regular.

Proof. a) The key result here is **Mac Lane's Theorem** [FT, §12]: a field extension L/K is separable iff L and $K^{p^{-\infty}}$ are linearly disjoint over K.
(i) $\implies$ (ii): If L/K is regular, then as above K is algebraically closed in K. Further, since L and $\overline{K}$ are linearly disjoint over K, certainly L and $K^{p^{-\infty}}$ are linearly disjoint over K.
(ii) $\implies$ (i): Let $K' = K^{p^{-\infty}}$ and $L' = L \otimes_K K'$. Since $L \otimes_K \overline{K} = (L \otimes_K K') \otimes_{K'} \overline{K} = L' \otimes_{K'} \overline{K}$, it is enough to show that L' is a field and $L' \otimes_{K'} \overline{K}$ is a field. Now L' is a field by Mac Lane's Theorem, and since K' is perfect, $\overline{K}/K'$ is a Galois extension, and thus by [FT, §12.3], since $L' \cap \overline{K} = K'$, L' and $\overline{K}$ are linearly disjoint over K'.
b) If K is perfect, every extension of K is separable. Apply part a). □

Theorem 14.24. *(Separable Noether Normalization) Let k be a field, and let R be a domain which is finitely generated as a k-algebra. Assume moreover that the fraction field L of R is a* regular *extension of k.*
a) There exists $d \in \mathbb{Z}$, $0 \leq d \leq m$, and algebraically independent elements $y_1, \ldots, y_d \in R$ such that R is finitely generated as a $k[y_1, \ldots, y_d]$-module and $L/k(y_1, \ldots, y_d)$ is a finite separable *field extension.*
b) The integer d is equal to both the Krull dimension of R and the transcendence degree of K/k.

For now we refer the reader to [Eis, Cor. 16.18] for the proof.

14.5.3. *Noether normalization over a domain.*

Theorem 14.25. *(Noether Normalization II) Let $R \subset S$ be domains with S finitely generated as an R-algebra. There exists $a \in R^\bullet$ and $y_1, \ldots, y_d \in S$ algebraically independent over the fraction field of R such that S_a (the localization of S at the multiplicative subset generated by a) is finitely generated as a module over $T = R_a[y_1, \ldots, y_d]$.*

Proof. (K.M. Sampath) Let K be the fraction field of R and let $x_1, \ldots, x_m$ be a set of R-algebra generators for S. Then

$$S' := S \otimes_R K = K[x_1, \ldots, x_m]$$

is finitely generated over K (as above, the x_i's need not be algebraically independent). Applying Theorem 14.22, we get algebraically independent elements $y_1, \ldots, y_d \in S'$ such that S' is a finitely generated $T' := K[y_1, \ldots, y_d]$-module.

Multiplying by a suitable element of $R^\times$, we may assume $y_i \in S$ for all i.

Since S' is finitely generated as a T'-module, it is integral over T'. For $1 \leq i \leq m$, x_i satisfies a monic polynomial equation with coefficients in T':

$$y_1^n + P_{i,1}(y_1, \ldots, y_d)y_i^{n-1} + \ldots + P_{i,n} = 0.$$

Let a be the product of the denominators of all coefficients of all the polynomials $P_{i,k}$. It follows that S_a is integral and finitely generated as a $T = R_a[y_1, \ldots, y_d]$-algebra, hence it is finitely generated as a T-module. □

Exercise 14.8: In the setting of Theorem 14.25 suppose that S is a graded R-algebra. Show that we may take all the y_i to be homogeneous elements.

14.5.4. *Applications.*

The Noether Normalization Theorem is one of the foundational results in algebraic geometry: geometrically, it says that every integral affine variety of dimension d is a finite covering of affine d-space $\mathbb{A}^d$. Thus it allows us to study arbitrary varieties in terms of rational varieties via branched covering maps. It is almost as important as a theorem of pure algebra, as even the "soft" part of the result, that the Krull dimension of an integral affine k-algebra is equal to the transcendence degree of its fraction field, is basic and useful.

One of the traditional applications of Noether Normalization is to prove Hilbert's Nullstellensatz. As we have seen, it is fruitful to channel proofs of the Nullstellensatz through Zariski's Lemma, and this is no exception.

Proposition 14.26. *Noether Normalization implies Zariski's Lemma.*

Exercise 14.9: Prove Proposition 14.26.

Theorem 14.27. *Let k be a field, and let R be a domain which is finitely generated as a k-algebra, with fraction field K. Then:*
a) The Krull dimension of R is equal to the transcendence degree of K/k.
b) Every maximal chain of prime ideals in R has length $\dim R$.

Proof. a) By Noether normalization, R is finite over $k[t_1, \ldots, t_d]$, so K is finite over $k(t_1, \ldots, t_d)$. Thus the transcendence degree of K/k is d. On the other hand, R is integral over $k[t_1, \ldots, t_d]$ so by Theorem 14.17 $\dim R = \dim k[t_1, \ldots, t_d]$. By Corollary 12.17, $\dim k[t_1, \ldots, t_d] = d$.
b) See Madapusi-Sampath, p. 119... □

14.6. **Some Classical Invariant Theory.**

Let R be a commutative ring, let G be a finite group, and suppose G acts on R by automorphisms, i.e., we have a homomorphism $\rho : G \to \mathrm{Aut}(R)$. We define

$$R^G = \{x \in R \mid \forall g \in G,\ gx = x\},$$

the **ring of G-invariants** – it is indeed a subring of R.

Remark: As in the case of rings acting on commutative groups, we say that G-action on R is **faithful** if the induced homomorphism $\rho : G \to \mathrm{Aut}(R)$ is injective. Any G-action induces a faithful action of $G/\ker(\rho)$, so it is no real loss of generality to restrict to faithful G-actions. We will do so when convenient and in such a

situation identify G with its isomorphic image in $\mathrm{Aut}\, R$.

The simplest case is that in which $R = K$ is a field. Then K^G is again a field and K/K^G is a finite Galois extension. Conversely, for any finite Galois extension K/F, $F = K^{\mathrm{Aut}(K/F)}$. This characterization of Galois extensions was used by E. Artin as the foundation for an especially elegant development of Galois theory (which swiftly became the standard one). Note also the analogy to topology: we have the notion of a finite Galois covering $Y \to X$ of topological spaces as one for which the group $G = \mathrm{Aut}(Y/X)$ of deck transformations acts freely and properly discontinuously on Y such that $Y/G = X$.

The branch of mathematics that deals with invariant rings under linear group actions is called **classical invariant theory**. Historically it was developed along with basic commutative algebra and basic algebraic geometry in the early 20th century, particularly by Hilbert. Especially, Hilbert's work on the finite generation of invariant rings was tied up with his work on the Basis Theorem.

For $a \in R$, put $N_G(a) = \prod_{\sigma \in G} \sigma(a)$. Then $N_G(a) \in R^G$, so we have a map

$$N_G : R \to R^G.$$

Note that N_G is *not* a homomorphism of additive groups. However, when R is a domain, there is an induced map

$$N_G : R^\bullet \to (R^G)^\bullet$$

which is a homomorphism of monoids, so induces a homomorphism on unit groups.

Exercise 14.10: Let $R[t]$ be the univariate polynomial ring over R. Show that there is a unique action of G by automorphisms of G on $R[t]$ extending the G-action on R and such that $gt = t$. Show that $(R[t])^G = R^G[t]$.

Proposition 14.28. *For a finite group G acting on R, R/R^G is integral.*

Proof. For $x \in R$, define

$$\Phi_x(t) = N_G(t - x) = \prod_{g \in G} (t - gx),$$

so $\Phi_x(t) \in (R[t])^G = R^G[t]$. Thus $\Phi_x(t)$ is a monic polynomial with R^G-coefficients which is satisfied by x. □

Base extension: Suppose that G is a finite group acting faithfully on R. Moreover, let A be a ring and $f : A \to R$ be a ring homomorphism, so R is an A-algebra. Suppose moreover that $f(A) \subset R^G$. In such a situation we say that G acts on R by A-automorphisms and write $G \subset \mathrm{Aut}(R/A)$.

Suppose we have another A-algebra A'. We can define an action of G on $R \otimes_A A'$ by putting $g(x \otimes y) := gx \otimes y$. We say that the G-action is **extended to** A'.

Proposition 14.29. *In the above setup, suppose that A' is a flat A-algebra. Then there is a natural isomorphism*

$$R^G \otimes_A A' \xrightarrow{\sim} (R \otimes_A A')^G.$$

Proof. Madapusi p. 65-66. □

Corollary 14.30. *Let G be a finite group acting on the ring R, and let $S \subset R^G$ be a multiplicatively closed set. Then $(S^{-1}R)^G = S^{-1}R^G$.*

Exercise 14.11: Prove Corollary 14.30.

In particular, suppose R is a domain with fraction field K, and let F be the fraction field of R^G. Then the G-action on R extends to a G-action on K, and Corollary 14.30 gives $K^G = F$. Thus the invariant theory of integral domains is compatible with the Galois theory of the fraction fields.

Proposition 14.31. *If R is integrally closed, so is R^G.*

Proof. Let $x \in K$ be integral over R^G. Then x is also integral over R, and since R is integally closed in L we have $x \in R$. Thus $x \in R \cap K = R \cap L^G = R^G$. □

Theorem 14.32. *(Noether* [No26]*) Suppose that R is a finitely generated algebra over some field k with $k = k^G$. Then:*
a) R is finitely generated as an R^G-module.
b) R^G is a finitely generated k-algebra.

Proof. a) Since R is a finitely generated k-algebra and $k \subset R^G$, R is a finitely generated R^G-algebra. But by Proposition 14.28 R/R^G is integral. So R is finitely generated as an R^G-module.
b) By part a), the Artin-Tate Lemma (Theorem 8.50) applies to the tower of rings $k \subset R^G \subset R$. The conclusion is as desired: R^G is a finitely generated k-algebra. □

Remark: The title of [No26] mentions "characteristic p". In fact, when k has characteristic 0 the result had been proven by Hilbert significantly earlier [Hi90], and moreover for certain actions of infinite linear groups, like $\mathrm{SL}_n(k)$. But Noether's formulation and proof give an excellent illustration of the economy and power of the commutative algebraic perspective.

Let us make contact with the setup of *classical invariant theory*: let k be a field, V a finite-dimensional vector space and $\rho : G \to \mathrm{Aut}_k(V)$ a linear representation of G on V. Let $k[V] = \mathrm{Sym}(V^\vee)$ be the algebra of polynomial functions on V. If we choose a k-basis $e_1, \ldots, e_n$ of V and let $x_1, \ldots, x_n$ be the dual basis of $V^\vee$, then $k[V] = k[x_1, \ldots, x_n]$ is a polynomial ring in n independent indeterminates. There is an induced action of G on $k[V]$, namely for $f \in k[V]$ we put $(gf)(x) = f(g^{-1}x)$.

All of our above results apply in this situation. Especially, Theorem 14.32 applies to tell us that the ring $k[V]^G$ is finitely generated as a k-algebra, or a **finite system of invariants**. Of course, we did not so much as crease our sleeves, let alone roll them up, to establish this: for a concretely given finite group G and action on a k-vector space V, it is of interest to explicitly compute such a finite system. Moreover, the polynomial ring $k[V]$ is integrally closed: in the next section we will see that it is a unique factorization domain and that this is a stronger property. Therefore Proposition 14.31 applies to show that $k[V]^G$ is integrally closed. This is actually quite a robust and useful procedure for producing integrally closed rings.

Example: Let k be a field, $n \in \mathbb{Z}^+$, let $V = k^n$, $G = S_n$ be the symmetric group,

and let G act on V by permuting the standard basis elements $e_1, \ldots, e_n$. We will compute $k[V]^G$. Namely, for $1 \leq i \leq n$, we define the **ith elementary symmetric function** $s_i(t_1, \ldots, t_n)$ as follows: let X be an independent indeterminate and put

$$f(X) = \prod_{i=1}^{n}(X - t_i) = X^n + \sum_{i=1}^{n}(-1)^i s_i(t_1, \ldots, t_n)X^{n-i}.$$

Theorem 14.33. *The invariant ring $k[V]^{S_n}$ is a polynomial k-algebra on the elementary symmetric functions $s_1, \ldots, s_n$.*

Proof. Step 1: Explicitly, we have

$$s_1 = t_1 + \ldots + t_n,$$
$$s_2 = \sum_{i<j} t_i t_j;$$

each s_i is the sum of all $\binom{n}{k}$ monomials of degree k. Clearly $k[s_1, \ldots, s_n] \subset k[V]^{S_n}$.
Step 2: For any finite group G of automorphisms of a field L, L/K^G is a Galois extension with $\mathrm{Aut}(L/L^G) = G$. Take $L = k(V)$ and note that $k(V)$ is the splitting field of the separable polynomial $f \in k(s_1, \ldots, s_n)[x]$, so $k(V)^G = k(s_1, \ldots, s_n)$.
Step 3: Because $k(t_1, \ldots, t_n)/k(s_1, \ldots, s_n)$ is a finite extension, the transcendence degree of $k(s_1, \ldots, s_n)/k$ is equal to the transcendence degree of $k(t_1, \ldots, t_n)/k$, namely n. It follows that the elements $s_1, \ldots, s_n$ are algebraically independent, i.e., $k[s_1, \ldots, s_n]$ is a polynomial ring.
Step 4: As in the proof of Proposition 14.31,

$$k[t_1, \ldots, t_n]^{S_n} = k[t_1, \ldots, t_n] \cap k(s_1, \ldots, s_n) = k[s_1, \ldots, s_n].$$

□

The above example is well-known and extremely useful, but gives a misleadingly simple impression of classical invariant theory. One can ask how often the ring of invariants of a finite group action on a polynomial ring is again a polynomial ring, and there is a nice answer to this. But let's back up a step and go back to "rational invariant theory": if G acts on $k[x_1, \ldots, x_n]$, then as above it also acts on the fraction field $k(x_1, \ldots, x_n)$ and we know that $k(x_1, \ldots, x_n)/k(x_1, \ldots, x_n)^G$ is a finite Galois extension. But must $k(x_1, \ldots, x_n)^G$ itself be a rational function field, as it was in the example above? This is known as **Noether's Problem**: it was first posed by E. Noether in 1913. It is natural and important, for an affirmative answer would allow us to realize every finite group as a Galois group (i.e., the automorphism group of a Galois extension) of $\mathbb{Q}$ thanks to a famous theorem of Hilbert. For more than half of the twentieth century, Noether's problem remained open. Finally, in 1969 R.G. Swan (yes, the same Swan as before!) found a representation of the cyclic group of order 47 on a finite-dimensional $\mathbb{Q}$-vector space for which the invariant field is not a rational function field [Sw69]. Too bad – this was arguably the best shot that anyone has ever taken at the Inverse Galois Problem over $\mathbb{Q}$.[56]

Example: Let k be a field of characteristic different from 2, let $V = k^2$, and consider the action of the two-element group $G = \{\pm 1\}$ on V by -1 acting as the

[56]Actually, Serre's *Topics in Galois Theory* describes a conjecture of J.-L. Colliot-Thélène – roughly a weaker form of Noether's problem – which would still imply that every finite group is a Galois group over $\mathbb{Q}$. I am not aware of any progress on this conjecture.

scalar matrix -1. The induced action on $k[V] = k[x,y]$ takes $x \mapsto -x$ and $y \mapsto -y$. This is, apparently, a not very interesting representation of a not very ineresting group. But the invariant theory is very interesting!

Exercise 14.12: a) Show $k[V]^G$ is generated as a k-algebra by x^2, y^2 and xy.
b) Show $k[V]^G$ is isomorphic to the k-algebra $k[A,B,C]/(AB - C^2)$.
c) Show that nevertheless the fraction field of $k[V]^G$ is rational, i.e., is isomorphic to $k(X,Y)$ for independent indeterminates X and Y.

Before signing off on our quick glimpse of classical invariant theory, we cannot resist mentioning one more classic theorem in the subject. It answers the question: when is the invariant subalgebra $k[V]^G$ isomorphic to a polynomial algebra over k?

Let $\rho : G \hookrightarrow \mathrm{GL}(V)$ be a faithful representation of G on a finite-dimensional k-vector space V. An element $g \in \mathrm{GL}(V)$ is a **pseudoreflection** if it has finite order and pointwise fixes a hyperplane W in V. (Equivalently, a pseudoreflection has characteristic polynomial $(t-1)^{\dim V - 1}(t - \zeta)$, where ζ is a root of unity in k.)

Exercise 14.13: If k is formally real, any nontrivial pseudoreflection has order 2 – i.e., it really is a hyperplane reflection.

A faithful representation ρ of G is a **pseudoreflection representation** of G if $\rho(G)$ is generated by pseudorflections.

Theorem 14.34. *(Shephard-Todd-Chevalley-Serre) Let k be a field, and let $\rho : G \hookrightarrow \mathrm{GL}(V)$ be a faithful finite-dimensional k-linear representation.*
a) If $k[V]^G$ is a polynomial algebra, then ρ is a pseudoreflection representation.
b) If ρ is a pseudoreflection representation and $\mathrm{char}\, k \nmid \#G$, then $k[V]^G$ is a polynomial algebra.

Proof. See [Be, §7.2]. □

In the **modular** case $\mathrm{char}\, k \mid \#G$, there are pseudoreflection representations for which $k[V]^G$ is not a polynomial algebra. However, work of Kemper and Malle [KM99] shows that even in the modular case, if ρ is an irreducible pseudoreflection representation then the invariant *field* $k(V)^G$ is purely transcendental over k.

Exercise 14.14: It follows from Theorem 14.34 the fundamental theorem on symmetric functions that the standard permutation representation of the symmetric group S_n on k^n is a pseudoreflection representation. Show this directly.

14.7. **Galois extensions of integrally closed domains.**

Proposition 14.35. *Let G be a finite group acting by automorphisms on a ring R, with invariant subring R^G. Let $\iota : R^G \hookrightarrow R$, and let $\mathfrak{p} \in \mathrm{Spec}\, R^G$.*
a) There is a natural action of G on the fiber $(\iota^*)^{-1}(\mathfrak{p})$ – i.e., on the set of primes $\mathcal{P}$ of R such that $\iota^*\mathcal{P} = \mathfrak{p}$.
b) The G-action on the fiber $(\iota^*)^{-1}(\mathfrak{p})$ is transitive.

Proof. Let $\mathcal{P} \in \mathrm{Spec}\, R$ and $\sigma \in G$. Define

$$\sigma\mathcal{P} = \{\sigma x \mid x \in \mathcal{P}\}.$$

It is straightforward to verify that $\sigma\mathcal{P}$ is a prime ideal of R (if you like, this follows from the fact that Spec is a functor). Moreover $(\sigma\mathcal{P}) \cap R^G$ is the set of all elements σx with $x \in \mathcal{P}$ such that for all $g \in G$, $g\sigma x = \sigma x$. As g runs through all elements of G, so does $g\sigma^{-1}$, hence $(\sigma\mathcal{P}) \cap R^G = \mathcal{P} \cap R^G = \mathfrak{p}$.
b) Let $\mathcal{P}_1, \mathcal{P}_2$ be two primes of R lying over a prime $\mathfrak{p}$ of R^G. Let $x \in \mathcal{P}_1$. Then $N_G(x) \in \mathcal{P}_1 \cap R^G = \mathfrak{p} \subset \mathcal{P}_2$. Since $\mathcal{P}_2$ is prime, there exists at least one $\sigma \in G$ such that $\sigma x \in \mathcal{P}_2$, and thus $\mathcal{P}_1 \subset \bigcup_{\sigma \in G} \sigma\mathcal{P}_2$. By Prime Avoidance (Lemma 8.45), there exists $\sigma \in G$ such that $\mathcal{P}_1 \subset \sigma\mathcal{P}_2$. Since R/R^G is integral, Incomparability (Corollary 14.15) yields $\mathcal{P}_1 = \sigma\mathcal{P}_2$. □

Theorem 14.36. *Let R be an integrally closed domain with fraction field K, let L/K be a normal algebraic field extension (possibly of infinite degree), and let S be the integral closure of R in L. Let $\mathfrak{p} \in \operatorname{Spec} R$, and let $X_{\mathfrak{p}}$ be the set of all prime ideals of S lying over $\mathfrak{p}$. Then $G = \operatorname{Aut}(L/K)$ acts transitively on $X_{\mathfrak{p}}$.*

Proof. Step 1: Suppose $[L : K] = n < \infty$, and write $G = \{\sigma_1 = 1, \ldots, \sigma_r\}$.[57] Seeking a contradiction, suppose there are $\mathcal{P}_1, \mathcal{P}_2 \in X_{\mathfrak{p}}$ such that $\mathcal{P}_2 \neq \sigma_j^{-1}\mathcal{P}_1$ for all j. By Corollary 14.15, $\mathcal{P}_2$ is not contained in any $\sigma_j^{-1}\mathcal{P}_1$, so by Prime Avoidance (Lemma 8.45) there is $x \in \mathcal{P}_2 \setminus \bigcup_j \sigma_j^{-1}\mathcal{P}_1$. Let q be the inseparable degree of L/K and put $y = \left(\prod_j \sigma_j(x)\right)^q$. Thus $y = N_{L/K}(x)$, so $y \in K$. Moreover y is integral over R, so $y \in R$. Since $\sigma_1 = 1$, $y \in \mathcal{P}_2$, so $y \in \mathcal{P}_2 \cap R = \mathfrak{p} \subset \mathcal{P}_1$, and thus, since $\mathcal{P}_1$ is prime, $\sigma_j(x) \in \mathcal{P}_1$ for some j: contradiction!
Step 2: We will reduce to the case in which L/K is a Galois extension. Let $G = \operatorname{Aut}(L/K)$ and $K' = L^G$, so that L/K' is Galois and K'/K is purely inseparable. Let R' be the integral closure of R in K'. Then by Lemma 14.20 $\operatorname{Spec} R' \to \operatorname{Spec} R$ is a bijection. So we may as well assume that $K' = K$ and L/K is Galois.
Step 3: For each finite Galois subextension M of L/K, consider the subset

$$F(M) := \{\sigma \in G \mid \sigma(\mathcal{P}_1 \cap M) = \mathcal{P}_2 \cap M\}.$$

Observe that $F(M)$ is a union of cosets of $\operatorname{Gal}(L/M)$ hence is (open and) closed in the Krull topology. By Step 1, we have $F(M) \neq \emptyset$. Moreover, the compositum $M = \prod_i M_i$ of any finite number $\{M_i\}$ of finite Galois subextenions is again a finite Galois subextension, and we have $\bigcap_i F(M_i) \supset F(M) \neq \varnothing$. Therefore as M_i ranges through all finite Galois subextensions of L/K, $\{F(M_i)\}_{i \in I}$ is a family of closed subsets of the compact space G satisfying the finite intersection condition, and it follows that there exists $\sigma \in \bigcap_i F(M_i) = F(L)$ i.e., $\sigma \in G$ such that $\sigma\mathcal{P}_1 = \mathcal{P}_2$. □

14.8. **Almost Integral Extensions.**

We come now to a technical variant of the notion of integrality. This variant will not be used until §19.4 on divisorial ideals. We honestly recommend that the reader skip past this section for now and return only when the concept of complete integral closure is needed and used.

Let $R \subset S$ be rings. An element $x \in S$ is **almost integral** over R if there is a finitely generated R-submodule of S which contains x^n for all $n \in \mathbb{Z}^+$. We say that S is **almost integral** over R if every element of S is almost integral over R.

[57] We are assuming that L/K is normal, so L/K is separable iff L/K is Galois iff $r = n$.

Proposition 14.37. *Let $R \subset S$ be rings, and let $x \in S$.*
a) If x is integral over R, it is almost integral over R.
b) If R is Noetherian and x is almost integral over R, then x is integral over R.

Proof. Let $M = \langle R, x \rangle$. By Theorem 14.1, x is integral over R iff M is a finitely generated R-module.
a) If x is integral over R, then M is a finitely generated R-submodule of S containing x^n for all $n \in \mathbb{Z}^+$, so x is almost integral over R.
b) Suppose x is almost integral over R: there is a finitely generated R-submodule N of S containing x^n for all $n \in \mathbb{Z}^+$. Then $M \subset N$, and since R is Noetherian and N is finitely generated, M is finitely generated and x is integral over R. □

Remark: As the proof shows, an equivalent – and perhaps more perspicuous – way of expressing the almost integrality condition is that, while integrality of x means that $M = \langle R, x \rangle_R$ is a finitely generated submodule of S, almost integrality means that there is *some* finitely generated R-submodule of S containing M.

For rings $R \subset S$, the **complete integral closure** of R in S is the set of all elements of S which are almost integral over R. A domain R is **completely integrally closed** if its complete integral closure in its fraction field is R itself.

Theorem 14.38. *Let R be a domain with fraction field K. The complete integral closure of R is the set of all $x \in K$ such that there is $r \in R^\bullet$ with $rx^n \in R$ for all $n \in \mathbb{Z}^+$.*

Proof. Let $x \in K$ be almost integral over R. Then there are $h_1, \ldots, h_s \in K$ such that $R[x] \subset \langle h_1, \ldots, h_s \rangle_R$. If r is the product of the denominators of the h_i, then $rx^n \in R$ for all $n \in \mathbb{Z}^+$.
Let $x \in K$ be such that there is $r \in R^\bullet$ with $rx^n \in R$ or all $n \in \mathbb{Z}^+$. Then $R[x] \subset r^{-1}R$. □

Tournant dangereux: If $R \subset S$ and R' is the complete integral closure of R in S, then R' is integrally closed in S [LM, Prop. 4.18]. However, the complete integral closure of a domain in its fraction field *need not* be completely integrally closed [LM, Exc. IV.14]! In other words, complete integral closure is unfortunately not a closure operator on the set of subrings of a field in the sense of §2.1.

15. Factorization

Let R be an integral domain, and x a nonzero, nonunit element of R. We say that x is **irreducible** if for any $y, z \in R$ such that $x = yz$, one of y or z is a unit.

For any unit $u \in R^\times$, we get factorizations of the form $x = u \cdot (u^{-1}x)$, so every x has at least these factorizations, which we wish to regard as "trivial". On the other hand, y and z cannot both be units, for then x would also be a unit. Let us then define a **factorization** of a nonzero nonunit $a \in R$ as a product

$$a = x_1 \cdots x_n,$$

such that each x_i is irreducible. We say that two factorizations

$$a = x_1 \cdots x_n = y_1 \cdots y_m$$

are **equivalent** if the multisets of associated principal ideals $\{\{(x_i)\}\} = \{\{(y_j)\}\}$ are equal. More concretely, this means that $m = n$ and that there is a bijection

$\sigma : \{1, \ldots, n\} \to \{1, \ldots, m\}$ such that $(y_{\sigma(i)}) = (x_i)$ for all $1 \leq i \leq n$.

If factorizations always exist and any two factorizations of a given element are equivalent, we say R is a **unique factorization domain** (UFD).

15.1. **Kaplansky's Theorem (II).**

A basic and important result that ought to get covered at the undergraduate level is that PID implies UFD. In fact this is easy to prove. What is more difficult is to get a sense of exactly how UFDs are a more general class of rings than PIDs. In this regard, an elegant theorem of Kaplansky seems enlightening.

Exercise 15.1: Let x be an element of a domain which can be expressed as

$$x = p_1 \cdots p_n,$$

such that for $1 \leq i \leq n$, $\mathfrak{p}_i = (p_i)$ is a prime ideal. If then there exist principal prime ideals $\mathfrak{q}_1, \ldots, \mathfrak{q}_m$ such that $(x) = \mathfrak{q}_1 \cdots \mathfrak{q}_m$, then $m = n$ and there exists a permutation σ of the integers from 1 to n such that $\mathfrak{q}_i = \mathfrak{p}_{\sigma(i)}$ for all i.

Exercise 15.2: Let R be a domain, and let S be the set of all nonzero elements x in R such that (x) can be expressed as a product of principal prime ideals. Show that S is a saturated multiplicatively closed subset.

Theorem 15.1. *(Kaplansky) An integral domain is a UFD iff every nonzero prime ideal in R contains a prime element.*

Proof. Suppose R is a UFD and $0 \neq \mathfrak{p} \in \operatorname{Spec} R$. Let $x \in \mathfrak{p}^\bullet$, and write

$$x = p_1 \cdots p_r$$

a product of prime elements. Then $x \in \mathfrak{p}$ implies $p_i \in \mathfrak{p}$ for some i, so $(p_i) \subset \mathfrak{p}$.

Conversely, assume each nonzero prime ideal of R contains a principal prime. Let S be the set of all products of prime elements, so that by Exercise 15.2, S is a saturated multiplicative subset. By Exercise 15.1, it is enough to show that S contains all nonzero nonunits of R. Suppose for a contradiction that there exists a nonzero nonunit $x \in R \setminus S$. The saturation of S implies $S \cap (x) = \emptyset$, and then by Theorem 4.8 there is a prime ideal $\mathfrak{p}$ containing x and disjoint from S. But by hypothesis, $\mathfrak{p}$ contains a prime element p, contradicting its disjointness from S. □

We deduce immediately:

Corollary 15.2. *Let R be a domain.*
a) If every ideal of R is principal, R is a UFD.
b) Conversely, if R is a UFD of dimension one, every ideal of R is principal.

Proof. a) Recall that a height one prime is a prime ideal $\mathfrak{p}$ of R which does not strictly contain any nonzero prime ideal. Applying Kaplansky's theorem, we get a prime element x such that $0 \subsetneq (x) \subset \mathfrak{p}$, and height one forces equality. For part b), it clearly suffices to show that a Noetherian domain in which each height one prime is principal is a UFD. But let $\mathfrak{p}$ be any nonzero prime ideal; since R is Noetherian, (DCC) holds on prime ideals, so $\mathfrak{p}$ contains a prime ideal which has height one, hence contains a prime element and we are done by Kaplansky's theorem. □

15.2. **Atomic domains, (ACCP).** If every nonzero nonunit admits at least one factorization, we say R is an **atomic domain**[58].

Exercise 15.3: Show that the ring $\overline{\mathbb{Z}}$ of all algebraic integers is not an atomic domain. Indeed, since for every algebraic integer x, there exists an algebraic integer y such that $y^2 = x$, there are no irreducible elements in $\overline{\mathbb{Z}}$!

The condition of factorization into irreducibles (in at least one way) holds in every Noetherian domain. In fact, a much weaker condition than Noetherianity suffices:

Proposition 15.3. *Let R be a domain in which every ascending chain of **principal** ideals stabilizes. Then every nonzero nonunit factors into a product of irreducible elements. In particular, a Noetherian domain is atomic.*

Proof. Let R be a domain satisfying the ascending chain condition for principal ideals (ACCP for short), and suppose for a contradiction that R is *not* an atomic domain. Then the set of principal ideals generated by unfactorable elements is nonempty, so by our assumption there exists a maximal such element, say $I = (a)$. Evidently a is not irreducible, so we can begin to factor a: $a = xy$ where x and y are nonunits. But this means precisely that both principal ideals (x) and (y) properly contain (a), so that by the assumed maximality of (a), we can factor both x and y into irreducibles: $x = x_1 \cdots x_m$, $y = y_1 \cdots y_n$. But then

$$a = x_1 \cdots x_m y_1 \cdots y_n$$

is a factorization of a, contradiction. □

This proposition motivates us to consider also the class of domains which satisfy the **ascending chain condition for principal ideals** (ACCP).

Exercise 15.4: Suppose that $R \hookrightarrow S$ is an exension of rings such that $S^\times \cap R = R^\times$. (In particular, this holds for integral extensions.) Show that S satisfies (ACCP) implies R satisfies (ACCP). Does the converse hold?

We have just seen that (ACCP) implies atomicity. The proof shows that under (ACCP) we can always obtain an expression of a given nonzero nonunit by a finite sequence of "binary factorizations" i.e., replacing an element x with $y_1 \cdot y_2$, where y_1 and y_2 are nonunits whose product is x. After a bit of thought, one is inclined to worry that it may be possible that this factorization procedure fails but nevertheless irreducible factorizations exist. This worry turns out to be justified:

Theorem 15.4. *There exists an atomic domain which does not satisfy (ACCP).*

Proof. See [Gr74]. □

However, the following strenghtening of atomicity does imply ACCP:

A domain R is a **bounded factorization domain** BFD if it is atomic and for each nonzero nonunit $a \in R$, there exists a positive integer $N(a)$ such that in any irreducible factorization $a = x_1 \cdots x_r$ we have $r \leq N(a)$.

[58]In the first pass on these notes, I used the sensible name "factorization domain." But apparently atomic domain is what is used in the literature, and since we find this terminology unobjectionable, we might as well use it here.

Proposition 15.5. *A UFD is a BFD.*

Proof. An immediate consequence of the definitions. □

Proposition 15.6. *A BFD satisfies (ACCP).*

Proof. Let R be a BFD. Suppose for a contradiction that $(x_i)_{i \in \mathbb{Z}^+}$ is a strictly ascending chain of principal ideals. We therefore have

$$x_0 = y_1 x_1 = y_1 y_2 x_2 = \ldots = y_1 \cdots y_n x_n = \cdots,$$

with each x_i, y_i a nonunit. Since R is atomic, we can refine each factorization into an irreducible factorization, but clearly an irreducible refinement of $y_1 \cdots y_n x_n$ has at least $n+1$ irreducible factors, contradicting BFD. □

15.3. **EL-domains.**

An element x of a domain R is **prime** if the principal ideal (x) is a prime ideal. Equivalently, x satisfies **Euclid's Lemma**: if $x \mid yz$, then $x \mid y$ or $x \mid z$.

Proposition 15.7. *A prime element is irreducible.*

Proof. If x is reducible, then $x = yz$ with neither y nor z a unit, so that $yz \in (x)$ but $y \notin (x)$, $z \notin (x)$. □

However, it need not be the case that irreducible elements are prime!

Example: Let $R = \mathbb{Z}[\sqrt{-5}]$. Then $2, 3$ and $1 \pm \sqrt{-5}$ are all irreducible, but

$$2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5})$$

shows that none of them are prime.

Exercise 15.5: Check all these assertions. Hint: Define $N(a + b\sqrt{-5}) = a^2 + 5b^2$. Check that $N((a + b\sqrt{-5})(c + d\sqrt{-5})) = N(a + b\sqrt{-5})N(c + d\sqrt{-5})$. Show that $\alpha \mid \beta$ (in R) $\implies N(\alpha) \mid N(\beta)$ (in $\mathbb{Z}$), and use this to show that $2, 3, 1 \pm \sqrt{-5}$ are irreducible but not prime.

It is tempting to call a domain in which all irreducible elements are prime "Euclidean", but this terminology is already taken for domains satisfying a generalization of the Euclidean algorithm (c.f. §16.3). So we will, provisionally, call a ring in which irreducible elements are prime an **EL-domain**. (EL = Euclid's Lemma).

Theorem 15.8. *For an integral domain R, TFAE:*
(i) R is a UFD.
(ii) R satisfies (ACCP) and is an EL-domain.
(iii) R is an atomic EL-domain.

Proof. i) $\implies$ (ii): In the previous section we saw UFD $\implies$ BFD $\implies$ (ACCP). We show UFD implies EL-domain: let $x \in R$ be irreducible and suppose $x \mid yz$. Let $y = y_1 \cdots y_m$ and $z = z_1 \cdots z_n$ be irreducible factorizations of y and z. Then the uniqueness of irreducible factorization means that x must be associate to some y_i or to some z_j, and hence $x \mid y$ or $x \mid z$: R is an EL-domain.

(ii) $\implies$ (iii) follows immediately from Proposition 15.3.

(iii) $\implies$ (i): This is nothing else than the usual deduction of the fundamental theorem of arithmetic from Euclid's Lemma: in a factorization domain we have at

least one irreducible factorization of a given nonzero nonunit x. If we also assume irreducibles are prime, we may compare any two irreducible factorizations: suppose

$$x = y_1 \cdots y_m = z_1 \cdots z_n.$$

Then y_1 is a prime element so divides z_j for some j. WLOG, relabel to assume $j = 1$. Since z_1 is irreducible, we have $y_1 = u_1 z_1$ and thus we may cancel to get

$$y_2 \cdots y_m = (u_1^{-1} z_2) z_3 \cdots z_n.$$

Continuing in this way we find that each y_i is associate to some z_j; when we get down to $1 = \prod_j z_j$ we must have no factors of z_j left, so $m = n$ and R is a UFD. □

We can now deduce the following important result, a characterization of Noetherian UFDs among all Noetherian domains.

Theorem 15.9. *For a Noetherian domain R, TFAE:*
(i) Every height one prime ideal of R is principal.
(ii) R is a UFD.

Proof. (i) $\implies$ (ii): By Theorem 15.8, it is sufficient to prove that R is an EL-domain, so let $x \in R$ be irreducible. Let $\mathfrak{p}$ be a minimal prime containing x. By Krull's Hauptidealsatz (Theorem 8.42), $\mathfrak{p}$ has height one, so by assumption $\mathfrak{p} = (p)$ is principal. Thus $x = up$ for some $u \in R$, and since x and p are both irreducible, $u \in R^\times$, $(x) = \mathfrak{p}$, and x is a prime element.
(ii) $\implies$ (i): This implication is a special case of Kaplansky's Theorem 15.1 (and thus holds without the Noetherian assumption on R). □

15.4. **GCD-domains.**

For elements a and b of a domain R, a **greatest common divisor** is an element d of R such that: $d \mid a$, $d \mid b$ and for $e \in R$ with $e \mid a$, $e \mid b$, $e \mid d$.

Exercise 15.6: Show that if d is a gcd of a and b, then an element d' of R is a gcd of a and b iff $(d) = (d')$. In particular, any two gcd's are associate.

If a and b have a gcd, it would be more logically sound to write $\gcd(a, b)$ to mean the unique principal ideal whose generators are the various gcd's of a and b. It is traditional however to use the notation $\gcd(a, b)$ to denote an element, with the understanding that in general it is only well-defined up to multiplication by a unit.[59]

More generally, for elements $a_1, \ldots, a_n$ in a domain R, a greatest common divisor is an element d of R such that $d \mid a_i$ for all i and if $e \mid a_i$ for all i then $e \mid d$. If a GCD of $(a_1, \ldots, a_n)$ exists, it is unique up to associates, and we denote it by $\gcd(a_1, \ldots, a_n)$. As above, it can be characterized as the unique minimal *principal* ideal containing $\langle a_1, \ldots, a_n \rangle$. Moreover, these setwise GCDs can be reduced to pairwise GCDs.

Exercise 15.7: Let a, b, c be elements of a domain R and assume that all pairwise GCD's exist in R. Then $\gcd(a, b, c)$ exists and we have $\gcd(a, \gcd(b, c)) =$

[59] In some rings, principal ideals have canonical generators: e.g. in the integers we may take the unique positive generator and in $k[t]$ we may take the unique monic generator. Under these circumstances, a common convention is to let $\gcd(a, b)$ stand for this canonical generator.

$\gcd(a,b,c) = \gcd(\gcd(a,b),c)$.

A domain R is a **GCD-domain** if for all $a, b \in R$, $\gcd(a,b)$ exists. By the above remarks, it would be equivalent to require that $\gcd(a_1, \ldots, a_n)$ for all n-tuples of elements in R.

Proposition 15.10. *(GCD Identities) Let R be a GCD-domain. Then:*
a) For all $a, b, c \in R$, $\gcd(ab, ac) = a\gcd(b,c)$.
b) For all $a, b \in R \setminus \{0\}$, $\gcd(\frac{a}{\gcd(a,b)}, \frac{b}{\gcd(a,b)}) = 1$.
c) For all $a, b, c \in R$, $\gcd(a,b) = \gcd(a,c) = 1$, then $\gcd(a,bc) = 1$.
d) For all $a, b, c \in R$, $\gcd(a, b+ac) = gcd(a,b)$.
e) For all $a, a_1, \ldots, a_n, b_1, \ldots, b_n, c \in R$, $\gcd(a, b_1+ca_1, \ldots, b_n+ca_n) = \gcd(a, b_1, \ldots, b_n)$.

Proof. a) Let $x = \gcd(ab, ac)$. Then $a \mid ab$ and $a \mid ac$ so $a \mid x$: say $ay = x$. Since $x \mid ab$ and $x \mid ac$, $y \mid b$ and $y \mid c$, so $y \mid \gcd(b,c)$. If $z \mid b$ and $z \mid c$, then $az \mid ab$ and $az \mid ac$, so $az \mid x = ay$ and $z \mid y$. Therefore $\gcd(b,c) = y = \frac{1}{a}\gcd(ab, ac)$.
b) This follows immediately from part a).
c) Suppose $\gcd(a,b) = \gcd(a,c) = 1$, and let t divide a and bc. Then t divides ab and bc so $t \mid \gcd(ab, bc) = b\gcd(a,c) = b$. So t divides $\gcd(a,b) = 1$.
d) If d divides both a and b, it divides both a and $b + ac$. If d divides both a and $b + ac$, it divides $b + ac - c(a) = b$.
e) We have

$$\gcd(a, b_1 + ca_1, \ldots, b_n + ca_n) = \gcd(a, \gcd(a, b_1 + ac_1), \ldots, \gcd(a, b_n + ac_n))$$
$$= \gcd(a, \gcd(a, b_1), \ldots, \gcd(a, b_n)) = \gcd(a, b_1, \ldots, b_n). \qquad \square$$

Proposition 15.11. *A GCD-domain is an EL-domain.*

Proof. This follows from the fact $\gcd(x,y) = \gcd(x,z) = 1 \implies \gcd(x, yz) = 1$. $\square$

Theorem 15.12. *Consider the following conditions on a domain R:*
(i) R is a UFD.
(ii) R is a GCD-domain.
(iii) R is an EL-domain: irreducible elements are prime.
a) We have (i) $\implies$ (ii) $\implies$ (iii).
b) If R is an ACCP-domain, (iii) $\implies$ (i).

Proof. a) (i) $\implies$ (ii): Let x, y be nonzero elements of R. We may write

$$x = f_1 \cdots f_r g_1 \cdots g_s, \ y = u f_1 \cdots f_r h_1 \cdots h_t,$$

where the f's, g's and h's are prime elements, $(g_j) \neq (h_k)$ for all j, k and $u \in R^\times$. Then $f_1 \cdots f_r$ is a gcd for x and y.
(ii) $\implies$ (iii): This is Proposition 15.11.
b) (iii) + (ACCP) $\implies$ (i): This is Theorem 15.8. $\square$

Corollary 15.13. *For a Noetherian domain R, TFAE:*
(i) R is a UFD.
(ii) R is a GCD-domain.
(iii) R is an EL-domain.

We now present some simple results that are long overdue. An extremely useful fact in algebra is that any UFD is integrally closed in its fraction field. We give a slightly stronger result and then recall a classical application.

Theorem 15.14. *A GCD-domain is integrally closed.*

Proof. Let R be a GCD-domain with fraction field K. Suppose $x \in K$ satisfies

$$x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0 = 0,\ a_i \in R.$$

Write $x = \frac{s}{t}$ with $s, t \in R,\ t \neq 0$. By Proposition 15.10b), after dividing by the gcd we may assume $\gcd(s,t) = 1$. Plugging in $x = \frac{s}{t}$ and clearing denominators gives

$$s^n = -\left(a_{n-1}ts^{n-1} + \ldots + a_1 t^{n-1}s + a_0 t^n\right),$$

so $t \mid s^n$. But by Proposition 15.10c) $\gcd(s^n, t) = 1$, so $t \in R^\times$ and $x \in R$. □

Corollary 15.15. *An algebraic integer which is a rational number is an integer:* $\overline{\mathbb{Z}} \cap \mathbb{Q} = \mathbb{Z}$.

Exercise 15.8: Prove Corollary 15.15.

Thus e.g. one can derive the irrationality of $\sqrt{2}$: it is a root of the monic polynomial equation $t^2 - 2 = 0$ but evidently not an integer, so cannot be rational.

Proposition 15.16. *(Compatibility of GCD's with localization) Let R be a GCD-domain and S a multiplicative subset of R. Then:*
a) The localization $S^{-1}R$ is again a GCD-domain.
b) For all $x, y \in R^\bullet$, if d is a GCD for x and y in R, then it is also a GCD for x and y in $S^{-1}R$.

Exercise 15.9: Prove Proposition 15.16.

15.5. **GCDs versus LCMs.**

The definition of GCDs in a domain has an evident analogue for least common multiples. Namely, if a and b are elements of a domain R, a **least common multiple** of a and b is an element l such that for all $m \in R$ with $a \mid m$ and $b \mid m$ then $l \mid m$.

Many of the properties of GCD's carry over immediately to LCM's. For instance, if l is an LCM of a and b, then $l' \in R$ is an LCM of a and b iff l' is associate to l.

Proposition 15.17. *Let a and b be elements in a domain R. Then* $\operatorname{lcm}(a,b)$ *exists iff the ideal $(a) \cap (b)$ is principal, in which case the set of all LCM's of a and b is the set of all generators of $(a) \cap (b)$.*

Proof. This is straightforward and left to the reader. □

LCM's exist in any UFD: if

$$a = x_1^{a_1} \cdots x_r^{a_r},\ b = x_1^{b_1} \cdots x_r^{b_r},$$

with $a_i, b_i \in \mathbb{N}$. Then

$$l = x_1^{\max(a_1,b_1)} \cdots x_r^{\max(a_r,b_r)}$$

is a greatest common divisor of a and b. Now the simple identity

$$\forall a, b \in \mathbb{N}, \min(a,b) + \max(a,b) = a + b$$

implies that for a, b in any UFD R we have

$$\gcd(a,b)\operatorname{lcm}(a,b) \sim ab.$$

This identity further suggests that the existence of either one of $\gcd(a,b)$, $\operatorname{lcm}(a,b)$ implies the existence of the other. However, this turns out only to be half correct!

Theorem 15.18. *For a, b in a domain R, TFAE:*
(i) $\operatorname{lcm}(a,b)$ *exists.*
(ii) For all $r \in R \setminus \{0\}$, $\gcd(ra, rb)$ *exists.*

Proof. Step 1: i) $\implies$ (ii). Suppose that there exists a least common multiple of a and b, say l. We claim that $d := \frac{ab}{l}$ is a greatest common divisor of a and b. (Note that since ab is a common divisor of a and b, $l \mid ab$, so indeed $d \in R$.) Indeed, suppose that $e \mid a$ and $e \mid b$. Then since $\frac{ab}{e}$ is a common multiple of a and b, we must have $l \mid \frac{ab}{e}$ and this implies $e \mid \frac{ab}{l}$. Thus d is a GCD of a and b.
Step 2: Suppose that for $r \in R \setminus \{0\}$ and $a, b \in R$, $\gcd(ra, rb)$ exists. Then we claim that $\gcd(a,b)$ exists and $\gcd(ra, rb) = r \gcd(a,b)$. Put $g := \frac{\gcd(ra,rb)}{r}$, which is clearly an element of D. Since $\gcd(ra, rb)$ divides ra and rb, g divides a and b. Conversely, if $e \mid a$ and $e \mid b$, then $re \mid ra$ and $re \mid rb$ so $er \mid \gcd(ra, rb)$ and $e \mid g$.
Step 3: We claim that if $l := \operatorname{lcm}(a,b)$ exists then so does $\operatorname{lcm}(ra, rb)$ for all $r \in R \setminus \{0\}$. First note that rl is a common multiple of ra and rb. Now suppose m is a common multiple of ra and rb, say $m = xra = yrb = r(xa - yb)$. Thus $r \mid m$ and $a \mid \frac{m}{r}$, $b \mid \frac{m}{r}$. So $l \mid \frac{m}{r}$ and $rl \mid m$. Thus $\operatorname{lcm}(ra, rb) = r \operatorname{lcm}(a,b)$.
Step 4: (ii) $\implies$ (i). We may assume that a and b are nonzero, since the other cases are trivial. Suppose $\gcd(ra, rb)$ exists for all $r \in R \setminus \{0\}$. We claim that $l := \frac{ab}{\gcd(a,b)}$ is an LCM of a and b. Clearly l is a common multiple of a and b. Now suppose that m is a common multiple of a and b. Then ab divides both ma and mb, so $ab \mid \gcd(ma, mb)$. By Step 2, $\gcd(ma, mb) = m \gcd(a,b)$. Thus $\frac{ab}{\gcd(a,b)} \mid m$. □

Theorem 15.19. *(Khurana,* [Kh03, Thm. 4]*) Let $d \geq 3$ be an integer such that $d+1$ is not prime, and write $d+1 = pk$ for a prime number p and $k \geq 2$. Then in the domain $R = \mathbb{Z}[\sqrt{-d}]$, the elements p and $1 + \sqrt{-d}$ have a GCD but no LCM.*

Proof. Step 1: We claim that p is irreducible as an element of R. Indeed, if it were reducible, then by the multiplicativity of the norm map $N(a + b\sqrt{-d}) = a^2 + dp^2$ we could write it as $p = \alpha\beta$, with

$$p^2 = N(p) = N(\alpha\beta) = N(\alpha)N(\beta),$$

and, since α, β are nonunits, $N(\alpha), N(\beta) > 1$. But then $N(\alpha) = N(\beta) = p$, i.e., there would be $a, b \in \mathbb{Z}$ such that $a^2 + db^2 = p$. But this is not possible: either $ab = 0$, in which the left hand side is a perfect square, or $a^2 + db^2 \geq d + 1 > p$.
Step 2: $\gcd(p, 1 + \sqrt{-d}) = 1$. Indeed, since $\frac{1}{p} + \frac{1}{p}\sqrt{-d} \notin R$, $p \nmid 1 + \sqrt{-d}$.
Step 3: We claim that kp and $k(1 + \sqrt{-d})$ do not have a GCD. Indeed, by Step 2 of the proof of Theorem 15.18, if any GCD exists then k is a GCD. Then, since $1 + \sqrt{-d}$ divides both $(1 - \sqrt{-d})(1 + \sqrt{-d}) = 1 + d = kp$ and $k(1 + \sqrt{-d})$, $1 + \sqrt{-d}$ divides $\gcd(kp, k(1 + \sqrt{-d}) = k$, i.e., there exist $a, b \in \mathbb{Z}$ such that

$$k = (1 + \sqrt{-d})(a + b\sqrt{-d}) = (a - db) + (a + b)\sqrt{-d},$$

i.e., $a = -b$ and $k = a - db = a + da = a(1 + d)$ and $d + 1 \mid k$, contradicting the fact that $1 < k < d + 1$.
Step 4: It follows from Theorem 15.18 that $\operatorname{lcm}(p, 1 + \sqrt{-d})$ does not exist. □

Khurana produces similar examples even when $d+1$ is prime, which implies that for no $d \geq 3$ is $R_d = \mathbb{Z}[\sqrt{-d}]$ a GCD-domain. (In fact, since $(R_d, +) \cong \mathbb{Z}^2$, R_d is an abstract number ring and hence Noetherian, so the notions of EL-domain, GCD-domain and UFD are all equivalent.) Let us give an independent proof:

Theorem 15.20. *For no $d \geq 3$ is $R_d = \mathbb{Z}[\sqrt{-d}]$ an EL-domain.*

Proof. As in the proof of Theorem 15.19 above, the easy observation that the equation $a^2 + db^2 = 2$ has no integral solutions implies that the element 2 is irreducible in R_d. Now, since (quite trivially) $-d$ is a square modulo 2, there exists $x \in \mathbb{Z}$ such that $2 \mid x^2 + d = (x + \sqrt{-d})(x - \sqrt{-d})$. But now, if R_d were an EL-domain, the irreducible element 2 would be prime and hence Euclid's Lemma would apply to show that $2 \mid x \pm \sqrt{-d}$, i.e., that $\frac{x}{2} + \frac{1}{2}\sqrt{-d} \in R_d$, which is a clear contradiction ($\frac{1}{2}$ is not an integer!). □

Theorem 15.18 has the following immediate consequence:

Corollary 15.21. *(Cohn,* [Coh68, Thm. 2.1]*) For an integral domain R, TFAE:*
(i) Any two elements of R have a greatest common divisor.
(ii) Any two elements of R have a least common multiple.

Thus we need not define an "LCM-domain": these are precisely the GCD domains.

15.6. **Polynomial rings over UFDs.**

Our goal in this section to show that if R is a UFD, then a polynomial ring in any number (possibly infinite) of indeterminates is again a UFD. This result generalizes a familiar fact from undergraduate algebra: if k is a field, $k[t]$ is a UFD. The corresponding fact that polynomials in $k[t_1, \ldots, t_n]$ factor uniquely into irreducibles is equally basic and important, and arguably underemphasized at the pre-graduate level (including high school, where factorizations of polynomials in at least two variables certainly do arise).

If we can establish that R a UFD implies $R[t]$ a UFD, then an evident induction argument using $R[t_1, \ldots, t_n, t_{n+1}] = R[t_1, \ldots, t_n][t_{n+1}]$ gives us the result for polynomials in finitely many indeterminates over a UFD. It is then straightforward to deduce the case for an arbitrary set of indeterminates.

There are several ways to prove the univariate case. Probably the most famous is via Gauss's Lemma. For this we need some preliminary terminology.

Let R be any integral domain, and consider a nonzero polynomial

$$f = a_n t^n + \ldots + a_1 t + a_0 \in R[t].$$

We say f is **primitive** if $x \in R$, $x \mid a_i$ for all i implies $x \in R^\times$. In a GCD-domain, this is equivalent to $\gcd(a_1, \ldots, a_n) = 1$. In a PID, this is equivalent to $\langle a_0, \ldots, a_n \rangle = R$. For a general domain, this latter condition is considerably stronger: e.g. the polynomial $xt + y \in k[x, y][t]$ is primitive but the coefficients do not generate the unit ideal. Let us call this latter – usually too strong condition – **naively primitive**.

Proposition 15.22. *Let R be a domain, and $f, g \in R[t]$ be naively primitive. Then fg is naively primitive.*

Proof. Suppose f and g are naively primitive but fg is not. Then by definition the ideal generated by the coeffiicents of f is proper, so lies in some maximal ideal $\mathfrak{m}$ of R. For $g \in R[t]$, write $\overline{g}$ for its image in the quotient ring $(R/\mathfrak{m})[t]$. Then our assumptions give precisely that $\overline{f}, \overline{g} \neq 0$ but $\overline{fg} = \overline{f}\overline{g} = 0$. Thus $\overline{f}$ and $\overline{g}$ are zero divisors in the integral domain $(R/\mathfrak{m})[t]$, a contradiction. □

If R is a GCD-domain and $0 \neq f \in R[t]$, we can define the **content** $c(f)$ of f to be the gcd of the coefficients of f, well-determined up to a unit. Thus a polynomial is primitive iff $c(f) = 1$.

Exercise 15.10: Let R be a GCD-domain and $0 \neq f \in R[t]$.
a) Show that f factors as $c(f)f_1$, where f_1 is primitive.
b) Let $0 \neq a \in R$. Show that $c(af) = ac(f)$.

Theorem 15.23. *(Gauss's Lemma) Let R be a GCD-domain. If $f, g \in R[t]$ are nonzero polynomials, we have $c(fg) = c(f)c(g)$.*

If we assume the stronger hypothesis that R is a UFD, we can give a very transparent proof along the lines of that of Proposition 15.22 above. Since this special case may be sufficient for the needs of many readers, we will give this simpler proof first, followed by the proof in the general case.

Proof. (Classical proof for UFDs) The factorization $f = c(f)f_1$ of Exercise 15.10 reduces us to the following special case: if f and g are primitive, then so is fg. Suppose that fg is not primitive, i.e., there exists a nonzero nonunit x which divides all of the coefficients of fg. Since R is a UFD, we may choose a prime element $\pi \mid x$. Now we may argue exactly as in the proof of Proposition 15.22: $(R/(\pi)[t]$ is an integral domain, $\overline{f}$ and $\overline{g}$ are nonzero, but $\overline{f}\overline{g} = \overline{fg} = 0$, a contradiction. □

The proof of the general case uses the GCD identities of Proposition 15.10.

Proof. (Haible) As above, we may assume that $f = a_n t^n + \ldots + a_1 t + a_0, g = b_m t^m + \ldots + b_1 t + b_0 \in R[t]$ are both primitive, and we wish to show that $fg = c_{m+n}t^{m+n} + \ldots + c_1 t + c_0$ is primitive. We go by induction on n. Since a primitive polynomial of degree 0 is simply a unit in R, the cases $m = 0$ and $n = 0$ are both trivial; therefore the base case $m + n = 0$ is doubly so. So assume $m, n > 0$. By Proposition 15.10, we have

$$c(fg) = \gcd(c_{n+m}, \ldots, c_0) =$$

$$\gcd(a_n b_m, \gcd(c_{n+m-1}, \ldots, c_0)) \mid \gcd(a_n, \gcd(c_{n+m-1}, \ldots, c_0)) \cdot \gcd(b_m, \gcd(c_{n+m-1}, \ldots, c_0)).$$

Now

$$\gcd(a_n, \gcd(c_{n+m-1}, \ldots, c_0)) = \gcd(a_n, c_{n+m-1}, \ldots, c_0)$$

$$= \gcd(a_n, c_{n+m-1} - a_n b_{m-1}, \ldots, c_n - a_n b_0, c_{n-1}, \ldots, c_0)$$

$$= \gcd(a_n, c((f - a_n t^n)g).$$

Our induction hypothesis gives $c((f - a_n t^n)g) = c(f - a_n t^n)c(g) = c(f - a_n t^n)$, so

$$\gcd(a_n, c_{n+m-1} - a_n b_{m-1}, \ldots, c_n - a_n b_0, c_{n-1}, \ldots, c_0) = \gcd(a_n, c(f - a_n t^n)) = c(f) = 1.$$

Similarly we have $\gcd(b_m, \gcd(c_{n+m-1}, \ldots, c_0)) = 1$, so $c(fg) = 1$. □

Corollary 15.24. *Let R be a GCD-domain with fraction field K, and let $f \in R[t]$ be a polynomial of positive degree.*
a) The following are equivalent:
(i) f is irreducible in $R[t]$.
(ii) f is primitive and irreducible in $K[t]$.
b) The following are equivalent:
(i) f is reducible in $K[t]$.
(ii) There exist $g, h \in R[t]$ such that $\deg(g), \deg(h) < \deg(f)$ and $f = gh$.

Proof. a) Assume (i). Clearly an imprimitive polynomial in $R[t]$ would be reducible in $R[t]$, so f irreducible implies $c(f) = 1$. Suppose f factors nontrivially in $K[t]$, as $f = gh$, where both $g, h \in K[t]$ and have smaller degree than f. By Exercise 15.10, we may write $g = c(g)g_1$, $h = c(h)h_1$, with g_1, h_1 primitive, and then $f = c(g)c(h)g_1h_1$. But then g_1, h_1, being primitive, lie in $R[t]$, and $c(f) = c(g)c(h) = c(gh) \in R$, so the factorization takes place over $R[t]$, contradiction. (ii) $\implies$ (i) is similar but much simpler and left to the reader.
b) That (ii) $\implies$ (i) is obvious, so assume (i). Because we can factor out the content, it is no loss of generality to assume that f is primitive. Let $f = g_1h_1$ with $g_1, h_1 \in K[t]$ and $\deg(g_1), \deg(h_1) < \deg(f)$. Because R is a GCD-domain, we may write $g = \frac{\tilde{g}}{d_1}$, $h = \frac{\tilde{h}}{d_2}$ with $\tilde{g}, \tilde{h} \in R[t]$ primitive. Then we have $d_1d_2f = \tilde{g}\tilde{h}$, and equating contents gives $(d_1d_2) = (1)$, so $d_1, d_2 \in R^\times$ and thus the factorization $f = gh$ has the properties we seek. □

We now give Gauss's proof that a univariate polynomial ring over a UFD is a UFD.

Theorem 15.25. *If R is a UFD, so is $R[t]$.*

Proof. Let K be the fraction field of R, and let $f \in R[t]^\bullet$. We know that $K[t]$ is a PID hence a UFD, so we get a factorization

$$f = cg_1 \cdots g_r,$$

with $c \in R$ and each $g_i \in R[t]$ is primitive and irreducible. Then factoring c into irreducibles gives an irreducible factorization of f. If we had another irreducible factorization $f = dh_1 \cdots h_s$, then unique factorization in $K[t]$ gives that we have $r = s$ and after permuting the factors have $g_i = u_ih_i$ for all i, where $u_i \in K^\times$. Since both g_i and h_i are primitive, we must have $u_i \in R^\times$, whence the uniqueness of the factorization. □

This proof relies on knowing that $K[t]$ is a UFD, which of course follows from the fact that polynomial division gives a Euclidean algorithm, as one learns in an undergraduate course. This is of course an adaptation of the proof that the ring $\mathbb{Z}$ is a UFD (the **Fundamental Theorem of Arithmetic**) essentially due to Euclid.

It is interesting to find alternate routes to such basic and important results.

Theorem 15.26. *Let R be a domain with fraction field K.*
a) If R is an ACCP-domain, so is $R[t]$.
b) If R is a GCD-domain, so is $R[t]$.
c) Thus, once again, if R is a UFD, so is $R[t]$.

Proof. a) In an infinite ascending chain $\{(P_i)\}$ of principal ideals of $R[t]$, $\deg P_i$ is a descending chain of non-negative integers, hence eventually constant. Therefore for sufficiently large n we have $P_n = a_nP_{n+1}$ with $a_n \in R$ and $(a_{n+1}) \supset (a_n)$. Since

R is an ACCP domain, we have $(a_n) = (a_{n+1})$ for sufficiently large n, hence also $(P_n) = (P_{n+1})$ for sufficiently large n.
b) (Haible, [Hai94]) Let $f, g \in R[t]$. We may assume that $fg \neq 0$. As usual, write $f = c(f)\tilde{f}$ and $g = c(g)\tilde{g}$. Since $K[t]$ is a PID, may take the gcd of $\tilde{f}$ and $\tilde{g}$ in $K[t]$, say $\tilde{d}$. The choice of $\tilde{d}$ is unique only up to an element of $K^\times$, so by choosing the unit appropriately we may assume that $\tilde{d}$ lies in $R[t]$ and is primitive. We put $d = \gcd(c(f), c(g)))\tilde{d}$.

Step 1: We claim that $\tilde{d}$ is a gcd of $\tilde{f}$ and $\tilde{g}$ in $R[t]$. Since $\tilde{d} \mid f$ in $K[t]$, we may write $\frac{\tilde{f}}{\tilde{d}} = \frac{a}{b}q$ with $a, b \in R \setminus \{0\}$ and $q \in R[t]$ primitive. Since $b\tilde{f} = a\tilde{d}$, we have $(b) = c(b\tilde{f}) = c(a\tilde{d}) = (a)$, i.e., $\frac{b}{a} \in R^\times$ and thus $\tilde{d} \mid \tilde{f}$ in $R[t]$. Similarly $\tilde{d} \mid \tilde{g}$. Moreover, sice $\tilde{d} \in \tilde{f}K[t] + \tilde{g}K[t]$, there exist $u, v \in R[t]$ and $c \in R \setminus \{0\}$ with $c\tilde{d} = u\tilde{f} + v\tilde{g}$. Suppose $h \in R[t]$ divides both $\tilde{f}$ and $\tilde{g}$. Then $h \mid c\tilde{d}$, and $c(h) \mid c(\tilde{f}) = (1)$. Writing $\frac{cd}{h} = \frac{a}{b}q$ with $q \in R[t]$ primitive, and equating contents in $bc\tilde{d} = ahq$, we get $(bc) = (a)$, hence $\frac{\tilde{d}}{h} = \frac{ab}{c}q \in R[t]$, so $h \mid \tilde{d}$.
Step 2: We claim that d is a gcd of f and g in $R[t]$. Certainly we have

$$(d) = (\gcd(c(f), c(g)\tilde{d}) \mid (c(f)\tilde{f}) = (f),$$

so $d \mid f$. Similarly $d \mid g$. Conversely, let $h \in R[t]$ divide f and g. Write $h = c(h)\tilde{h}$ for $\tilde{h} \in R[t]$ primitive. From $h \mid f$ it follows that $c(h) \mid c(f)$ and thus $\tilde{h} \mid \tilde{f}$. Similarly $h \mid f$ so $\tilde{h} \mid \tilde{g}$. Thus $c(h) \mid \gcd(c(f), c(g))$, $\tilde{h} \mid \tilde{d}$ and thus finally $h \mid d$.
c) If R is a GCD domain and an ACCP domain, it is also an atomic EL domain, hence a UFD by Theorem 15.8. □

Lindemann [Li33] and Zermelo [Ze34] (independently) gave (similar) striking proofs of the Fundamental Theorem of Arithmetic avoiding all lemmas and packaging the Euclidean division into a single inductive argument. Later several authors have recorded analogous proofs of Gauss's Theorem (Theorem 15.25): the earliest instance we are aware of in the literature is due to S. Borofsky [Bor50]. We give a third, "lemmaless" proof of Theorem 15.25 here.

Proof. It suffices to show that $R[t]$ is an ACCP domain and an EL-domain. By Theorem 15.26a), $R[t]$ is an ACCP domain. Now, seeking a contradiction, we suppose that R is an EL-domain but $R[t]$ is not. Among the set of all elements in $R[t]$ admitting inequivalent irreducible factorizations, let p be one of minimal degree. We may assume

$$p = f_1 \cdots f_r = g_1 \cdots g_s,$$

where for all i, j, $(f_i) \neq (g_j)$ and

$$m = \deg f_1 \geq \deg f_2 \geq \ldots \geq \deg f_r,$$

$$n = \deg g_1 \geq \deg g_2 \geq \ldots \geq \deg g_s,$$

with $n \geq m > 0$. Suppose the leading coefficient of f_1 (resp. g_1) is a (resp. b). Put

$$q = ap - bf_1x^{n-m}g_2 \cdots g_s = f_1(af_2 \cdots f_r - bx^{n-m}g_2 \cdots g_s) = (ag_1 - bf_1x^{n-m})g_2 \cdots g_s.$$

Thus $q = 0$ implies $ag_1 = bf_1x^{n-m}$. If, however, $q \neq 0$, then

$$\deg(ag_1 - bf_1x^{n-m}) < \deg g_1,$$

hence $\deg q < \deg p$ and q has a unique factorization into irreducibles, certainly including $g_2, \cdots, g_s$ and f_1. But then f_1 must be a factor of $ag_1 - bf_1x^{n-m}$ and

thus also of ag_1. Either way $ag_1 = f_1 h$ for some $h \in R[t]$. Since a is constant and f_1 is irreducible, this implies $h = ah_2$, so $ag_1 = f_1 a h_2$, or $g_1 = f_1 h_2$, contradiction. □

Corollary 15.27. *Let R be a UFD and let $\{t_i\}_{i \in I}$ be any set of indeterminates. Then $S = R[\{t_i\}]$ is a UFD.*

Proof. When I is finite, apply Theorem 15.25 and induction. When I is infinite, $S = \bigcup_J R[\{t_j\}]$, as J ranges over all finite subsets of I: any given polynomial can only involve finitely many indeterminates. For $f \in S$, let J be such that $f \in R[\{t_j\}]$, so $f = p_1 \cdots p_r$ is a factorization into prime elements of $R[\{t_j\}]$. Any two factorizations in S would themselves lie in some subalgebra involving finitely many determinates, so the factorization must be unique. □

So a polynomial ring in infinitely many indeterminates over a field k is a non-Noetherian UFD. This is an important example to keep in mind: the UFD condition is in many ways a very delicate one, but it can still be satisfied by very "large"

We mention without proof two negative results.

Theorem 15.28.
a) (Roitman [Roi93]*) There exists an integrally closed atomic domain R such that $R[t]$ is not atomic.*
b) (Anderson-Quintero-Zafrullah) There exists an EL domain R such that $R[t]$ is not an EL domain.

15.7. **Application: the Schönemann-Eisenstein Criterion.**

The most famous criterion for irreducibility of univariate polynomials is named after Ferdinand Eisenstein [Ei50]. However, the version for polynomials over $\mathbb{Z}$ was proven several years earlier by Theodor Schönemann [Sc45], [Sc46]. For many years now few anglophone texts have associates Schönemann's name with this result, and his contribution might have been in real danger of being forgotten were it not for the beautiful recent article of D.A. Cox [Cox11] on the early history of this result.

Nowadays it is common to state and prove a version of Eisenstein's criterion with respect to a prime ideal in a UFD. We give a slight generalization:

Theorem 15.29. *(Schönemann-Eisenstein Criterion) Let R be a domain with fraction field K, and let $f(t) = a_d t^d + \ldots + a_1 t + a_0 \in R[t]$. Suppose that there exists a prime ideal $\mathfrak{p}$ of R such that $a_d \notin \mathfrak{p}$, $a_i \in \mathfrak{p}$ for all $0 \leq i < d$ and $a_0 \notin \mathfrak{p}^2$.*
a) If f is primitive, then f is irreducible over $R[t]$.
b) If R is a GCD-domain, then f is irreducible over $K[t]$.

Proof. a) Suppose to the contrary that f is primitive and reducible over $R[t]$: i.e., there exists a factorization $f = gh$ with $g(t) = b_m t^m + \ldots + b_1 t + b_0$, $h(t) = c_n t^m + \ldots + c_1 t + c_0$, $\deg(g), \deg(h) < \deg(f)$ and $b_m c_n \neq 0$. Since $a_0 = b_0 c_0 \in \mathfrak{p} \backslash \mathfrak{p}^2$, it follows that exactly one of b_0, c_0 lies in $\mathfrak{p}$: say it is c_0 and not b_0. Moreover, since $a_d = b_m c_n \notin \mathfrak{p}$, $c_n \notin \mathfrak{p}$. Let k be the least index such that $c_k \notin \mathfrak{p}$, so $0 < k \leq n$. Then $b_0 c_k = a_k - (b_1 c_{k-1} + \ldots + b_k c_0) \in \mathfrak{p}$. Since $\mathfrak{p}$ is prime, it follows that at least one of b_0, c_k lies in $\mathfrak{p}$, a contradiction.
b) Suppose R is a GCD-domain and (seeking a contradiction) that f is reducible over $K[t]$. By Corollary 15.24b), we may write $f = gh$ with $g, h \in R[t]$ and $\deg(g), \deg(h) < \deg(f)$. Then the proof of part a) goes gives a contradiction. □

Corollary 15.30. *Let R be a GCD-domain containing a prime element π (e.g. a UFD that is not a field). Then the fraction field K of R is not separably closed.*

Proof. To say that π is a prime element is to say that the principal ideal $\mathfrak{p} = (\pi)$ is a nonzero prime ideal. Then $\pi \notin \mathfrak{p}^2$, so for all $n > 1$, $P_n(t) = t^n - \pi$ is Eisenstein with respect to $\mathfrak{p}$ and hence irreducible in $K[t]$. Choosing n to be prime to the characteristic of K yields a degree n separable field extension $L_n := K[t]/(P_n)$. □

15.8. **Application: Determination of** $\operatorname{Spec} R[t]$ **for a PID** R**.**

Let R be a PID. We wish to determine all prime ideals of the ring $R[t]$. Let us begin with some general structural considerations. First, R is a one-dimensional Noetherian UFD; so by Theorems 8.36, 15.26 and 8.48, $R[t]$ is a two-dimensional Noetherian UFD. Being a UFD, its height one ideals are all principal. Since it has dimension two, every nonprincipal prime ideal is maximal. Therefore it comes down to finding all the maximal ideals.

However, to avoid assuming the Dimension Theorem, we begin with milder hypotheses on a prime ideal $\mathcal{P}$, following [R, pp. 22-23].

Namely, let $\mathcal{P}$ be a nonzero prime ideal of $R[t]$. We assume – only! – that $\mathcal{P}$ is not principal. By Theorem 15.1, we are entitled to a prime element f_1 of $\mathcal{P}$. Since $\mathcal{P} \neq (f_1)$, let $f_2 \in \mathcal{P} \setminus (f_1)$. Then $\gcd(f_1, f_2) = 1$: since $\gcd(f_1, f_2) \mid f_1$, the only other possibility is $(\gcd(f_1, f_2)) = (f_1)$, so $f_1 \mid f_2$ and $f_2 \in (f_1)$, contradiction.

FIRST CLAIM Let K be the fraction field of R. The elements f_1 and f_2 are also relatively prime in the GCD-domain $K[t]$. Indeed, suppose that $f_1 = hg_1$, $f_2 = hg_2$ with $h, g_1, g_2 \in K[t]$ and h a nonunit. By Gauss' Lemma, we may write $h = ah_0$, $g_1 = b_1\gamma_1$, $g_2 = b_2\gamma_2$ with $a_1, b_1, b_2 \in K$ and h_0, γ_1, γ_2 primitive elements of $R[t]$. Again by Gauss' Lemma, $h_0\gamma_1$ and $h_0\gamma_2$ are also primitive, so $f_1 = hg_1 = (ab_1)(h_0\gamma_1) \in R[t]$, which implies that $ab_1 \in R$. Similarly, $ab_2 \in R$, so h_0 is a nonunit of $R[t]$ which divides both f_1 and f_2, contradiction.

Let $\mathcal{M} := \langle f_1,\ f_2 \rangle$, and put $\mathfrak{m} = \mathcal{M} \cap R$. It remains to show that, as the notation suggests, $\mathcal{M}$ is a maximal ideal of $R[t]$ and $\mathfrak{m}$ is a maximal ideal of R.

SECOND CLAIM $\mathfrak{m} \neq 0$. Since $K[t]$ is a PID and $f_1,\ f_2$ are relatively prime in $K[t]$, there exist $a, b \in K[t]$ such that $af_1 + bf_2 = 1$. Let $0 \neq c \in R$ be an element which is divisible by the denominator of each coefficient of a and b: then $(ca)f_1 + (cb)f_2 = c$ with $ca, cb \in R$, so that $c \in \mathfrak{m}$.

Now put $\mathfrak{p} = \mathcal{P} \cap R$, so $\mathfrak{p} = (p)$ is a prime ideal of the PID R. Moreover,

$$\mathfrak{p} = \mathcal{P} \cap R \supset \mathcal{M} \cap R = \mathfrak{m} \supsetneq 0,$$

so $\mathfrak{p}$ is maximal. Since $\mathcal{P} \supset \mathfrak{p}$, $\mathcal{P}$ corresponds to a prime ideal in $R[t]/\mathfrak{p}R[t] = (R/\mathfrak{p})[t]$, a PID. Therefore $\mathcal{P}$ is generated by $p \in \mathfrak{p}$ and an element $f \in R[t]$ whose image in $(R/\mathfrak{p})[t]$ is irreducible.

We therefore have proved:

Theorem 15.31. *Let R be a PID, and $\mathcal{P} \in \operatorname{Spec} R[t]$. Then exactly one of the following holds:*

(0) $\mathcal{P}$ has height 0: $\mathcal{P} = (0)$.
(i) $\mathcal{P}$ has height one: $\mathcal{P} = (f)$, for a prime element $f \in R[t]$.
(ii) $\mathcal{P}$ has height two: $\mathcal{P} = \langle p, f \rangle$, where p is a prime element of R and $f \in R[t]$ is an element whose image in $(R/p)[t]$ is irreducible. Moreover both $\mathcal{P}$ and $\mathfrak{p} := \mathcal{P} \cap R$ are maximal, and $[R[t]/\mathcal{P} : R/\mathfrak{p}] < \infty$.

Exercise 15.11: Suppose R has only finitely prime ideals, so is not a Hilbert-Jacobson ring. By Theorem 12.21, there $\mathfrak{m} \in \operatorname{MaxSpec} R[t]$ such that $\mathfrak{m} \cap R = (0)$. Find one, and explain where $\mathfrak{m}$ fits in to the classification of Theorem 15.31.

15.9. **Power series rings over UFDs.**

Exercise 15.12: Show that if R is ACCP, so is $R[[t]]$.

In particular, if R is a UFD, $R[[t]]$ is ACCP. But of course the more interesting question is the following: *Must $R[[t]]$ be a UFD?*

In contrast to Gauss's Theorem, whether a formal power series ring over a UFD must be a UFD was a perplexing problem to 20th century algebraists and remained open for many years. Some special cases were known relatively early on.

Theorem 15.32. *(Rückert* [Rü33]*, Krull* [Kr37]*) Let k be a field, and let n be a positive integer. Then $k[[t_1, \ldots, t_n]]$ is a UFD.*

A significant generalization was proved by Buchsbaum and Samuel, independently, in 1961. A Noetherian domain R is **regular** if for every maximal ideal $\mathfrak{m}$ of R, the height of $\mathfrak{m}$ is equal to the dimension of $\mathfrak{m}/\mathfrak{m}^2$ as a vector space over the field $R/\mathfrak{m}$.

Theorem 15.33. *(*[Buc61]*,* [Sa61]*) If R is a regular UFD, then so is $R[[t]]$.*

The paper [Sa61] also exhibits a UFD R for which $R[[t]]$ is *not* a UFD.

What about formal power series in countably infinitely many indeterminates? Let k be a field. There is more than one reasonable way to define such a domain. One the one hand, one could simply take the "union" (formally, direct limit) of finite formal power series rings $k[[t_1, \ldots, t_n]]$ under the evident inclusion maps. In any element of this ring, only finitely many indeterminates appear. However, it is useful also to consider a larger ring, in which the elements are infinite formal k-linear combinations of monomials $t_{i_1} \cdots t_{i_n}$. Let us call this latter domain $k[[t_1, \ldots, t_n, \ldots]]$.

In fact, we have seen this domain before: it is isomorphic to the Dirichlet ring $\mathcal{D}_k$ of functions $f : \mathbb{Z}^+ \to k$ with pointwise addition and convolution product. To see this, we use unique factorization in $\mathbb{Z}$! Namely, write enumerate the prime numbers $\{p_i\}_{i=1}^{\infty}$ and write $n \in \mathbb{Z}^+$ as $n = \prod_{i=1}^{\infty} p_i^{a_i}$, where $a_i \in \mathbb{Z}^+$ and $a_i = 0$ for all sufficiently large i. Then the map which sends $f \in \mathcal{D}_k$ to the formal power series $\sum_{n \in \mathbb{Z}^+} f(n) \prod_{i=1}^{\infty} t_i^{a_i}$ gives an isomorphism from $\mathcal{D}_k$ to $k[[t_1, \ldots, t_n, \ldots]]$. In 1959, E.D. Cashwell and C.J. Everett used Theorem 15.32 to prove the following result. A key part of their proof was later simplified by C.F. Martin, who pointed out the applicability of König's Infinity Lemma.

Theorem 15.34. *(*[CE59]*,* [Mar71]*)*
a) For any field k, the ring of formal power series $k[[t_1, \ldots, t_n, \ldots]]$ is a UFD.
b) In particular, the ring $\mathcal{D}_{\mathbb{C}} = \{f : \mathbb{Z}^+ \to \mathbb{C}\}$ of arithmetic functions is a UFD.

In almost any first number theory course one studies unique factorization and also arithmetic functions, including the Dirichlet ring structure (which e.g. leads to an immediate proof of the Möbius Inversion Formula). That arithmetic functions are themselves an example of unique factorization is however a very striking result that does not seem to be well-known to most students or practitioners of number theory. I must confess, however, that I (a number theorist) know of no particular application of Theorem 15.34. I would be interested to learn of one!

15.10. **Nagata's Criterion.**

Proposition 15.35. *Let R be a domain, S a saturated multiplicative subset, and $f \in R \setminus S$. If f is prime as an element of R, it is also prime as an element of R_S.*

Proof. Since $f \in R \setminus S$, f is not a unit in R_S. Let $\alpha, \beta \in R_S$ be such that $f \mid \alpha\beta$ in R_S. So there exists $\gamma \in R_S$ such that $\gamma f = \alpha\beta$; putting $\alpha = \frac{x_1}{s_1}$, $\beta = \frac{x_2}{s_2}$, $\gamma = \frac{x_3}{s_3}$ and clearing denominators, we get $s_1 s_2 x_3 f = s_3 x_1 x_2$, so $f \mid r_3 x_1 x_2$. If $f \nmid s_3$, then since S is saturated, $f \in S$, contradiction. So, being prime, f divides x_1 or x_2 in R, hence *a fortiori* in R_S and therefore it also divides either $\frac{x_1}{s_1}$ or $\frac{x_2}{s_2}$ in R_S, since these are associates to x_1 and x_2. □

Theorem 15.36. *Every localization of a UFD is again a UFD.*

Exercise 15.13: Prove Theorem 15.36. (Suggestions: one gets an easy proof by combining Theorem 15.1 with Proposition 15.35. But the result is also rather straightforward to prove directly.)

A saturated multiplicative subset S of R is **primal**[60] if it is generated by the units of R and by the prime elements of S.

Lemma 15.37. *An irreducible element of a primal subset is prime.*

Proof. Suppose S is primal and $f \in S$ is irreducible. By definition, there exists a unit u and prime elements $\pi_1, \ldots, \pi_n$ such that $f = u\pi_1 \cdots \pi_n$. Since $u\pi_1$ is also prime, we may as well assume that $u = 1$. Then, since f is irreducible, we must have $n = 1$ and $f = \pi_1$. □

Theorem 15.38. *For an atomic domain R, the following are equivalent:*
(i) Every saturated multiplicative subset of R is primal.
(ii) R is a UFD.

Proof. Since the set $R^\times$ of units is trivially generated by the empty set of prime elements, both conditions hold if R is a field, so let us now assume otherwise.

Assume (i). Then, since R is a factorization domain which is not a field, there exists an irreducible element f of R. Let S be the saturated multiplicative subset generated by S, which consists of all units of R together with all divisors of positive powers f^n of f. Since S is primal and strictly contains $R^\times$, there must exist a prime element π which divides f^n for some n. In other words, $f^n \in \pi R$, and since πR is prime, we must have that $f = x\pi$ for some $x \in R$. Since f is irreducible we must have $x \in R^\times$, i.e., $f \sim \pi$ and is therefore a prime element. So R is an ACCP domain and an EL-domain and hence a factorization domain by Theorem 3.3.

Assume (ii), let S be a saturated multiplicative subset of R, and suppose that $f \in S \setminus R^\times$. Then $f = u\pi_1^{a_1} \cdots \pi_n^{a_n}$ where the π_i's are prime elements. Since each

[60] This terminology is my invention: do you like it?

$\pi_i \mid f$, $\pi_i \in S$ for all i. It follows that indeed S is generated by its prime elements together with the units of R. □

Because of Theorem 15.38, it is no loss of generality to restate Theorem 15.36 as: the localization of a UFD at a primal subset is again a UFD. The following elegant result of Nagata may be viewed as a converse.

Theorem 15.39. *(Nagata* [Nag57]*) Let R be a factorization domain and $S \subset R$ a primal subset. If the localized domain R_S is a UFD, then so is R.*

Proof. By Theorem 15.8 it suffices to show that if $f \in R$ is irreducible, f is prime. Case 1: $f \notin S$, so f is not a unit in R_S. Since R_S is a UFD, it is enough to show that f is irreducible in R_S. So assume not: $f = \frac{x_1}{s_1} \cdot \frac{x_2}{s_2}$ with $x_1, x_2 \in R \setminus S$ and $s_1, s_2 \in S$. hen $s_1 s_2 f = x_1 x_2$. By assumption, we may write $s_1 = u p_1 \cdots p_m$ and $s_2 = v q_1 \cdots q_n$, where $u, v \in R^\times$ and p_i, q_j are all prime elements of R. So $p_1 \mid x_1 x_2$; since p_1 is a prime, we must have either $\frac{x_1}{p_1} \in R$ or $\frac{x_2}{q_2} \in R$. Similarly for all the other p_i's and q_j's, so that we can at each stage divide either the first or the second factor on the right hand side by each prime element on the left hand side, without leaving the ring R. Therefore we may write $f = (\frac{1}{uv})\frac{x_1}{t_1}\frac{x_2}{t_2}$ where t_1, t_2 are each products of the primes p_i and q_j, hence elements of S, and also such that $t_1 \mid x_1$, $t_2 \mid x_2$, i.e., the factorization takes place in R. Moreover, since $x_i \in R \setminus S$ and $t_i \in S$, $\frac{x_i}{t_i}$ is not even a unit in R_S, hence *a fortiori* not a unit in R. Therefore we have exhibited a nontrivial factorization of f in R, contradiction.
Case 2: $f \in S$. Since S is primal, by Lemma 15.37, f is prime. □

Remark: If S is the saturation of a finitely generated multiplicative set, the hypothesis that R is a factorization domain can be omitted.

Application: Let A be a UFD and consider $R = A[t]$. Put $S = A \setminus \{0\}$. As for any multiplicative subset of a UFD, S is generated by prime elements. But moreover, since $A[t]/(\pi A[t]) \cong (A/\pi A)[t]$, every prime element π of A remains prime in $A[t]$, so viewing S as the multiplicative subset of $A[t]$ consisting of nonzero constant polynomials, it too is generated by prime elements. But if F is the fraction field of A, $R_S = (A[t])_S = F[t]$ which is a PID and hence a UFD. Nagata's theorem applied to R and S now tells us – for the third time! – that $R = A[t]$ is a UFD.

Nagata used Theorem 15.39 to study the coordinate rings of affine quadric cones.

Let k be a field of characteristic different from 2, and let $f(x) = f(x_1, \ldots, x_n) \in k[x_1, \ldots, x_n]$ be a **quadratic form**, i.e., a homogeneous polynomial of degree 2 with k coefficients. We assume that f the associated bilinear form $(x, y) \mapsto \frac{1}{2}(f(x+y) - f(x) - f(y))$ is nonsingular. Equivalently, by making an invertible linear change of variables every quadratic form can be diagonalized, and a quadratic form is nonsingular iff it admits a diagonalization

$$f(x) = a_1 x_1^2 + \ldots + a_n x_n^2 \text{with} a_1, \ldots, a_n \in k^\times. \tag{32}$$

We wish to study the **affine quadric cone** associated to f, namely $R_f = k[x]/(f)$. Note that if quadratic forms f and g are isometric – i.e., differ by an invertible linear change of variables – then $R_f \cong R_g$, so we assume if we like that f is in diagonal form as in (32) above. If $n \geq 3$ then every nonsingular diagonal quadratic polynomial is irreducible, so R_f is a domain. If k is quadratically closed – i.e., admits no proper quadatic extension – then conversely any binary ($n = 2$) quadratic

form is reducible, so R_f is not a domain. (If f is not quadratically closed, there exist irreducible binary quadratic forms, but we will not consider them here.)

Theorem 15.40. *Let $f = f(x_1, \ldots, x_n) \in \mathbb{C}[x_1, \ldots, x_n]$ be a nondegenerate quadratic form. Then $R_f = k[x]/(f)$ is a UFD iff $n \geq 5$.*

Proof. By the remarks above, R_f is a domain iff $n \geq 3$, so we may certainly restrict to this case. Because $\mathbb{C}$ is algebraically closed, every quadratic form in $n \geq 2$ variables is **isotropic**, i.e., there exists $0 \neq a \in k^n$ such that $f(a) = 0$: indeed, the first $n-1$ coordinates of a may be chosen arbitrarily. By an elementary theorem in the algebraic theory of quadratic forms [Lam06, Thm. I.3.4], we may make a change of variables to bring f into the form:

$$f(x) = x_1 x_2 + g(x_3, \ldots, x_n).$$

Case 1: Suppose $n = 3$, so that

$$f(x) = x_1 x_2 - a x_3^2$$

for some $a \in k^\times$. In this case, to show that R_f is not a UFD it suffices to show that the images $\overline{x_1}, \overline{x_2}, \overline{x_3}$ of x_1, x_2, x_3 in R_f are nonassociate irreducibles, for then $\overline{x_1 x_2} = a\overline{x_3}^2$ exhibits a non-unique factorization! To establish this, regard $k[x_1, x_2, x_3]$ as a graded $\mathbb{C}$-algebra in the usual way – with x_1, x_2, x_3 each of degree 1 – so that the quotient R_f by the homogeneous ideal (f) inherits a grading. Since $\overline{x_1}$ has degree 1, if it were reducible, it would factor as the product of a degree one element $c_1 x_1 + c_2 x_2 + x_3 x_3 + (f)$ and a degree zero element $r + (f)$, and thus

$$(rc_1 - 1)x_1 + rc_2 x_2 + rc_3 x_3 \in (f).$$

But the left hand side has degree 1, whereas all nonzero elements in (f) have degree 2 or higher, so $r \in \mathbb{C}[x]^\times$ and therefore the factorization is trivial. The irreducibility of $\overline{x_2}$ and $\overline{x_3}$ is proved in the same way. If $\overline{x_1} \sim \overline{x_3}$ in R_f, then we may divide both sides of $\overline{x_1 x_2} - a\overline{x_3}^2$ by $\overline{x_1}$ and deduce that also $\overline{x_2} \sim \overline{x_3}$. But in the quotient ring $R_f/(\overline{x_3})$, $\overline{x_3}$ maps to 0 and $\overline{x_1}$ and $\overline{x_2}$ do not, contradiction. So R_f is not a UFD.
Case 2: Suppose $n = 4$, so $f(x) = x_1 x_2 + g(x_3, x_4)$, where $g(x_3, x_4)$ is a nonsingular binary form. Here for the first time we use the full strength of the quadratic closure of k: since $k^\times = k^{\times 2}$, any two nonsingular quadratic forms in the same number of variables are isometric, so we may assume WLOG that

$$f(x) = x_1 x_2 - x_3 x_4.$$

Now we argue exactly as in Case 1 above: in R_f, the images $\overline{x_1}, \overline{x_2}, \overline{x_3}, \overline{x_4}$ are all non-associate irredcuble elements, so $\overline{x_1 x_2} = \overline{x_3 x_4}$ is a non-unique factorization.
Case 3: $n \geq 5$. Then $n - 2 \geq 3$, so g is irreducible in the UFD $\mathbb{C}[x_3, \ldots, x_n]$, hence also in $\mathbb{C}[x_2, x_3, \ldots, x_n]$. Therefore $R_f/(\overline{x_1}) = \mathbb{C}[x_1, \ldots, x_n]/(x_1, f) = \mathbb{C}[x_2, \ldots, x_n]/(g)$ is a domain, i.e., $\overline{x}_1$ is a prime element. Moreover,

$$R[\overline{x_1}^{-1}] = \mathbb{C}[x_1, \ldots, x_n, x_1^{-1}]/(x_1 x_2 - g)$$

$$\cong \mathbb{C}[x_1, \ldots, x_n, x_1^{-1}]/(x_2 - \frac{g}{x_1}) \cong \mathbb{C}[x_1, x_3, \ldots, x_n, x_1^{-1}]$$

is a localization of the UFD $\mathbb{C}[x_1, x_3, \ldots, x_n]$ hence a UFD. By Nagata's Criterion (Theorem 15.39), R_f itself is a UFD. □

Now let k be a field of characteristic not 2 and $f \in k[x_1, \ldots, x_n]$ a nondegenerate quadratic form. Without changing the isomorphism class of R_q we may diagonalize f; moreover without changing the ideal (f) we may scale by any element of $k^\times$, so without loss of generality we need only consider forms $x_1^2 + a_2x_2^2 + \ldots + a_nx_n^2$.

Theorem 15.41. *Let k be a field of characteristic different from 2 and $f = x_1^2 + a_2x_2^2 + \ldots + a_nx_n^2$ a nonsingular quadratic form over k. Put $R_f = k[x]/(f)$.*
a) If $n \leq 2$ then R_f is not an integrally closed domain.
b) If $n = 3$, R_f is a UFD iff f is anistropic: $\forall a \in k^n,\ f(a) = 0 \implies a = 0$.
c) (i) Suppose $f = x_1^2 - ax_2^2 - bx_3^2 - cx_4^2$. If a is a square in k, then R_f is a UFD iff $-bc$ is not a square in k.
(i) If none of a, b, c, $-ab$, $-ac$, $-bc$ is a square in k, then R_f is a UFD iff $-abc$ is not a square.
d) If $n \geq 5$, R_f is a UFD.

Proof. a) If $n \leq 2$, R_f is never an integrally closed domain.
b) The proof of Theorem 15.40 goes through to show that if f is isotropic (i.e., not anisotropic), R_f is not a UFD. The anisotropic case is due to Samuel [Sa64].
Part c) is due to T. Ogoma [O74].
Part d) goes back at least to van der Waerden [vdW39]. In [Nag57], M. Nagata gives a short proof using Theorem 15.39. □

It is also interesting to consider affine rings of inhomogeneous quadric hypersurfaces. For instance, we state without proof the following result.

Theorem 15.42. *For $n \geq 1$, let $R_n := \mathbb{R}[t_1, \ldots, t_{n+1}]/(t_1^2 + \ldots + t_{n+1}^2 - 1)$ be the ring of polynomial functions on the n-sphere S^n.*
a) (Bouvier [Bou78]*) If $n \geq 2$, then R_n is a UFD.*
b) (Trotter [Tr88]*) R_1 is isomorphic to the ring $\mathbb{R}[\cos\theta, \sin\theta]$ of real trigonometric polynomials, in which $(\sin\theta)(\sin\theta) = (1+\cos\theta)(1-\cos\theta))$ is an explicit non-unique factorization into irreducible elements. Hence R_1 is not a UFD.*

16. Principal rings and Bézout domains

A ring R in which every ideal is principal is called a **principal ring**. If R is moreover a domain, it is called a **principal ideal domain** (PID).

16.1. Principal ideal domains.

Proposition 16.1. *a) A PID has dimension at most one.*
b) A UFD is a PID iff it has dimension at most one.

Proof. a) Any domain has positive Krull dimension. Moreover, if $(x) \subset (y)$ are two nonzero principal prime ideals, then we may write $x = cy$ for some $0 \neq c \in R$. Since x is prime, either $x \mid c$ or $x \mid y$. If $dx = c$, then $dcy = dx = c$, and cancellation gives that y is a unit, contradiction. Therefore $y = dx = dcy$ and cancellation gives $dc = 1$, i.e., $c, d \in R^\times$ and $(x) = (y)$.
b) We recall only that by Kaplansky's Theorem 15.1, any nonzero ideal in a UFD contains a prime element. □

Exercise 16.1: Let R be a PID and let $S \subset R \setminus \{0\}$ be a multiplicative subset. Show that the localization $S^{-1}R$ is a PID (which is a field iff $S \cap R^\times \neq \emptyset$).

Corollary 16.2. *A UFD in which each maximal ideal is principal is a PID.*

Proof. Let R be a UFD in which each maximal ideal is principal. Seeking a contradiction, suppose R is not a PID: then, by Theorem 4.25 there is a nonprincipal prime ideal $\mathfrak{p}$. Let $\mathfrak{m}$ be a maximal ideal containing $\mathfrak{p}$, which by assumption is principal, say $\mathfrak{m} = (x)$. By Kaplansky's Theorem 15.1, $\mathfrak{p}$ contains a prime element y. Thus $x \mid y$, but since both are prime elements we conclude $(x) = (y)$ and thus $\mathfrak{p} = (x)$ is principal, contradiction. □

Exercise 16.2: We develop an alternate proof of Corollary 16.2 following W. Dubuque.
a) Let R be a UFD, and let $S \subset R^\bullet$ be any subset. Show that $\gcd(S)$ exists.
b) Let R be a UFD in which all maximal ideals are principal, let I be a nonzero ideal in R. Show that we may write $I = \gcd(I)J$ for an ideal J which is not contained in any proper principal ideal, and conclude that $I = \gcd(I)$ is principal.

We now follow with some very familiar examples.

Proposition 16.3. *The integer ring $\mathbb{Z}$ is a principal ideal domain.*

To be honest, I can hardly imagine a reader without prior knowledge of this result (a staple of undergraduate mathematics) who has made it this far. Therefore, with our tongue slightly in cheek, we present a "structural" proof. To make clear the rules of our little game, let us say in advance that the only "prior knowledge" we will require about the ring $\mathbb{Z}$ is that for any positive integer n, the quotient $\mathbb{Z}/n\mathbb{Z}$ has (finite!) order n. To show this, let z be any nonzero integer; note that the set of integers k such that $z - kn \geq 0$ is bounded above so therefore has a largest element K; and thus $0 \leq z - Kn < n$.

Lemma 16.4. *The integer ring $\mathbb{Z}$ is a unique factorization domain.*

Proof. Concretely, we claim that for every integer $n > 1$, there exist not necessarily distinct prime numbers $p_1, ..., p_r$ such that $n = p_1 \cdots p_r$ and also that if we have any s prime numbers $q_1, \ldots, q_s$ such that $n = q_1 \cdots q_s$, then $r = s$ and there exists a permutation σ of $\{1, \ldots, r\}$ such that for all $1 \leq i \leq r$ we have $q_i = p_{\sigma(i)}$. □

Here are two proofs which the reader may not have seen before:

First proof: Indeed a decomposition $n = p_1 \cdots p_r$ corresponds to a composition series for the $\mathbb{Z}$-module $\mathbb{Z}/n\mathbb{Z}$. Since $\mathbb{Z}/n\mathbb{Z}$ is finite, it is certainly Noetherian and Artinian, so composition series exist. Moreover the Jordan-Hölder theorem implies that any two composition series have the same number of terms – i.e., $r = s = \ell(\mathbb{Z}/n\mathbb{Z})$ – and that after a permutation the sequences of isomorphism classes of composition factors become identical.

Second proof (Lindemann [Li33], Zermelo [Ze34]): We prove both the existence and uniqueness of the factorization by an inductive argument, specifically by appeal to the well-ordering of the positive integers under $\leq$.

Existence: let S be the set of integers $n > 1$ which *do not* have at least one prime factorization. We wish to show that S is empty so, seeking a contradiction, suppose not. Then by well-ordering S has a least element, say N. If N is prime, then we have found a prime factorization, so suppose it is not prime: that is, we may write $N = N_1 N_2$ with $1 < N_1, N_2 < N$. Thus N_1 and N_2 are too small to lie in S so each have prime factorizations, say $N_1 = p_1 \cdots p_r$, $N_2 = q_1 \cdots q_s$, and then $N = p_1 \cdots p_r q_1 \cdots q_s$ gives a prime factorization of N, contradiction!

Uniqueness: we claim that the factorization of a positive integer is unique. Assume not; then the set of positive integers which have at least two different standard form factorizations is nonempty, so has a least element, say N, where:

$$N = p_1 \cdots p_r = q_1 \cdots q_s. \tag{33}$$

Here the p_i's and q_j's are prime numbers, not necessarily distinct from each other. However, we must have $p_1 \neq q_j$ for any j. Indeed, if we had such an equality, then we could cancel and, by an inductive argument we have already rehearsed, reduce to a situation in which the factorization must be unique. In particular $p_1 \neq q_1$. Without loss of generality, assume $p_1 < q_1$. Then, if we subtract $p_1 q_2 \cdots q_s$ from both sides of (33), we get

$$M := N - p_1 q_2 \cdots q_s = p_1(p_2 \cdots p_r - q_2 \cdots q_s) = (q_1 - p_1)(q_2 \cdots q_s). \tag{34}$$

By the assumed minimality of N, the prime factorization of M must be unique. However, (34) gives two different factorizations of M, and we can use these to get a contradiction. Specifically, $M = p_1(p_2 \cdots p_r - q_2 \cdots q_s)$ shows that $p_1 \mid M$. Therefore, when we factor $M = (q_1 - p_1)(q_2 \cdots q_s)$ into primes, at least one of the prime factors must be p_1. But $q_2, \ldots, q_j$ are already primes which are different from p_1, so the only way we could get a p_1 factor is if $p_1 \mid (q_1 - p_1)$. But this implies $p_1 \mid q_1$, and since q_1 is also prime this implies $p_1 = q_1$. Contradiction!

Now we come to the proof of Proposition 16.3. Applying the lemma together with Kaplansky's Theorem (Theorem 15.1), we see that every nonzero prime ideal $\mathfrak{p}$ of $\mathbb{Z}$ contains a prime element, say p. But the quotient $\mathbb{Z}/(p)$ is a finite integral domain, hence a field, hence (p) is maximal and therefore $(p) = \mathfrak{p}$. This shows that every prime ideal of $\mathbb{Z}$ is principal, and now finally we apply Theorem 4.25.

Proposition 16.5. *For any field k, the ring $R = k[t]$ is a principal ideal domain.*

Proof. By Theorem 15.26, R is a UFD. The remainder of the argument is quite similar to the case of $R = \mathbb{Z}$. Namely it suffices to show that the ideal generated by any prime element is maximal. But a prime element of $k[t]$ is, among other things, a polynomial $p(t)$ of positive degree d, and the quotient $R/(p(t))$, being finite dimensional over a field k, is an Artinian integral domain. Thus $R/(p(t))$ is a field and $(p(t))$ is maximal. □

Conversely:

Exercise 16.3: Let R be a ring, and suppose that the univariate polynomial ring $R[t]$ is a PID. Show that R is a field.

Proposition 16.6. *Let R be a Noetherian local ring with a principal maximal ideal $\mathfrak{m} = (a)$. Then every nonzero ideal of R is of the form (a^i) for some $i \in \mathbb{N}$. In particular, R is a principal ring.*

Proof. The key is the Krull intersection theorem: $\bigcap_i \mathfrak{m}^i = \bigcap_i (a^i) = 0$. It follows that for any nonzero $r \in R$, there exists a largest $i \in \mathbb{N}$ such that $r \in (a^i)$, i.e., there exists $s \in R$ such that $r = sa^i$. But if s were not a unit then it would lie in $\mathfrak{m}$ and thus r would lie in $\mathfrak{m}^{i+1}$, contradiction. So s is a unit and $(r) = \mathfrak{m}^i$. Thus to every nonzero element r of I we attach a non-negative integer i_r. Now if I is any nonzero ideal of R, choose a nonzero element r of I with i_r minimal among elements of I. Then $I \supset (r) = \mathfrak{m}^i$, and the other containment follows by minimality of i_r. □

Corollary 16.7. *For any field k, the formal power series ring $k[[t]]$ is a PID.*

Proof. We have seen that a power series ring over a domain is a domain. By Theorem 8.36b), $k[[t]]$ is Noetherian. Quite generally, for a ring R the units of $R[[t]]$ are precisely those formal power series $f = a_0 + a_1 t + \ldots$ with $a_0 \in R^\times$; since k is a field this means that the units are those with nonzero constant term. The complement of the set of units is the principal ideal (t), so $k[[t]]$ satisfies all the hypotheses of Proposition 16.6 and is therefore a PID. □

Remark: If we had available the theory of completions, we could deduce Corollary 16.7 directly from Proposition 16.5.

16.2. **Some structure theory of principal rings.**

Proposition 16.8. *Let R be a principal ring.*
a) For any multiplicative subset S, the localization R_S is principal.
b) For any ideal I of R, the quotient R/I is principal.

Exercise 16.4: Prove Proposition 16.8.

Proposition 16.9. *Let $R_1, \ldots, R_n$ be finitely many rings. TFAE:*
(i) Each R_i is a principal ring.
(ii) The direct product $\prod_{i=1}^n R_i$ is a principal ring.

Exercise 16.5: a) Prove Proposition 16.9.
b) Exhibit an infinite direct product of PIDs which is not a principal ring.

Definition: A principal ring $(R, \mathfrak{m})$ is **special** if it is a local Artinian ring, i.e., if it is local and the maximal ideal is principal and nilpotent. The complete structure of ideals in special principal rings can be deduced from Proposition 16.6: if n is the least positive integer such that $\mathfrak{m}^n = 0$, then the ideals of R are precisely the powers $\mathfrak{m}^i = (\pi^i)$ for $0 \leq i \leq n$.

We can now state a structure theorem for principal rings, which appears in Zariski and Samuel (so far as I know, for the first time).

Theorem 16.10. *(Zariski-Samuel) Every principal ring is the direct product of a finite number of PIDs and special principal rings.*

Much of the work of the proof is contained in the following preparatory result:

Lemma 16.11. *Let R be a principal ring.*
a) Let $\mathfrak{p} \subsetneq \mathfrak{q}$ be prime ideals of R. Then $\mathfrak{q}$ contains no prime ideals other than itself and $\mathfrak{p}$ and every primary ideal contained in $\mathfrak{q}$ contains $\mathfrak{p}$.
b) If $\mathfrak{p}$ is a non-maximal prime ideal and $\mathfrak{a} \subset \mathfrak{p}$ is a primary ideal, then $\mathfrak{a} = \mathfrak{p}$.
c) Any two incomparable prime ideals of R are comaximal.

Proof. a) Suppose that we have $\mathfrak{p} \subsetneq \mathfrak{q}$ and also $\mathfrak{q} \supsetneq \mathfrak{r}$, where $\mathfrak{r}$ is a prime ideal. Write $\mathfrak{p} = (p)$, $\mathfrak{q} = (q)$ and $\mathfrak{r} = (r)$. There exists $a \in R$ such that $p = aq$. Since p is a prime element and p does not divide q, we must have $p \mid a$, so that there exists $b \in R$ with $a = pb$ and thus $p = pbq$. Now since $p(1 - bq) = 0 \in \mathfrak{r} \subset \mathfrak{q}$ and $1 - bq \in R \setminus \mathfrak{q}$, $\mathfrak{r}$ does not contain $1 - bq$ and therefore we must have $p \in \mathfrak{r}$, i.e., $\mathfrak{p} \subset \mathfrak{r} \subset \mathfrak{q}$. But now modding out by $\mathfrak{p}$ we get $0 \subset \mathfrak{r}/\mathfrak{p} \subset \mathfrak{q}/\mathfrak{p}$ in the principal ideal domain $R/\mathfrak{p}$, which is a one-dimensional ring, and therefore $\mathfrak{r} = \mathfrak{p}$ or $\mathfrak{r} = \mathfrak{q}$.

b) ...
c) Now let $\mathfrak{p}_1$ and $\mathfrak{p}_2$ be incomparable prime ideals. If $\mathfrak{p}_1$ is maximal, then it is comaximal with any prime ideal which is not contained in it. Similarly, $\mathfrak{p}_2$ is not maximal either. So if they are not comaximal, there exists a maximal ideal $\mathfrak{q}$ strictly containing both $\mathfrak{p}_1$ and $\mathfrak{p}_2$. Applying part a) to $\mathfrak{p}_1 \subsetneq \mathfrak{q}$ gives a contradiction. □

Proof of Theorem 16.10: Let

$$(0) = \bigcap_{i=1}^{n} \mathfrak{a}_i$$

be an irredundant primary decomposition of (0), and let $\mathfrak{p}_i = \mathrm{rad}(\mathfrak{a}_i)$. Then the $\mathfrak{p}_i$'s are pairwise comaximal; otherwise, for any distinct $\{i, j\}$, by Lemma 16.11 we would have, say, $\mathfrak{p}_i \subsetneq \mathfrak{p}_j$ and then part b) of the lemma gives $\mathfrak{p}_i = \mathfrak{a}_i \subset \mathfrak{a}_j$, contradicting irredundancy. Since the radicals of the $\mathfrak{a}_i$'s are pairwise comaximal, so are the $\mathfrak{a}_i$'s (Proposition 4.16). So we may apply the Chinese Remainder Theorem, getting

$$R = R/(0) = R/\bigcap_{i=1}^{n} \mathfrak{a}_i = \prod_{i=1}^{n} R/\mathfrak{a}_i.$$

Each factor is, of course, a principal ring. Fix any $1 \leq i \leq n$.
Case 1: Suppose first that $\mathfrak{p}_i$ is maximal. If $\mathfrak{a}_i$ were contained in any other prime ideal $\mathfrak{p}$, then $\mathrm{rad}(\mathfrak{a}_i) = \mathfrak{p}_i \subset \mathrm{rad}(\mathfrak{p}) = \mathfrak{p}$, contradiction. So $R/\mathfrak{a}_i$ is a special PIR.
Case 2: Otherwise, $\mathfrak{p}_i = \mathfrak{a}_i$, so that $R/\mathfrak{a}_i$ is a PID. □

We quote without proof the following somewhat stronger result:

Theorem 16.12. *(Hungerford structure theorem* [Hun68]*)*
For a commutative ring R, TFAE:
(i) R is a principal ring.
(ii) $R \cong \prod_{i=1}^{n} R_i$, and each R_i is a quotient of a PID.

Exercise 16.6: Derive Theorem 16.10 from Theorem 16.12.

Exercise 16.7: Show that for a commutative ring R, TFAE:
(i) R is a special principal ring.
(ii) R is the quotient of a DVR by a nonzero ideal.

Exercise 16.8: Let k be a field. Let $R = k[x, y]$, and $\mathfrak{m}$ be the maximal ideal $\langle x, y \rangle$ in R. Show that the quotient ring $S = R/\mathfrak{m}^2$ is nonprincipal. In particular, if k is finite, then S is a finite nonprincipal local ring.

Exercise:[61] Show that for a ring R the following are equivalent:
(i) The polynomial ring $R[t]$ is principal.
(ii) R is a finite product of fields.

16.3. **Euclidean functions and Euclidean rings.**

THIS SECTION WILL SOON BE REWRITTEN

If R is an integral domain, then a **Euclidean function** is a function $N : R\backslash\{0\} \to \mathbb{N}$

[61] Inspired by `http://math.stackexchange.com/questions/361258`.

such that: for all $a \in R$ and $b \in R \setminus \{0\}$, there exists $q,\ r \in R$ such that $a = qb + r$ with $r = 0$ or $N(r) < N(b)$.

Exercise 16.9: For each of the following rings R, we give a function $N : R \setminus \{0\} \to \mathbb{N}$. Verify that N is a Euclidean function on R.
a) $R = \mathbb{Z}$, $N(a) = |a|$.
b) $R = k[t]$, $N(p(t)) = \deg(p(t))$.
c) $R = k[[t]]$, $N(\sum_{n=0}^{\infty} a_n t^n) :=$ the least n such that $a_n \neq 0$.
d) For $d \in \{-2, -1, 2, 3\}$, $R = \mathbb{Z}[\sqrt{d}] = \mathbb{Z}[t]/(t^2 - d)$, $N(a + b\sqrt{d}) = |a^2 - db^2|$.

Exercise 16.10: Let R be a local PID. Use Proposition 16.6 to construct a Euclidean function on R.

The virtue of Euclidean functions lies in the following result:

Proposition 16.13. *A domain R which admits a Euclidean function is a PID.*

Proof. Let I be any nonzero ideal of R, and choose an element x in I such that $N(x)$ is minimal. For any $y \in I$, by definition of a Euclidean function we may write $y = qx + r$ with $r = 0$ or $N(y) < N(x)$. Our choice of x rules out the second alternative and thus we have $y = qx$, i.e., $y \in (x)$. □

Remark: It is common to define a **Euclidean domain** as a domain which admits some Euclidean function. In my opinion, this definition is somewhat of a false step in the theory. The merit of the notion of a Euclidean function is that for certain rings R there is an evident Euclidean function (e.g. for $\mathbb{Z}$ and $k[t]$), and when this occurs one deduces immediately that R is a PID. Moreover, if the Euclidean function is (in some sense) computable, the **Euclidean algorithm** can be used to find greatest common divisors and, accordingly, generators of ideals.

In contrast, since the specific Euclidean function is not part of the definition of a Euclidean domain, in order to show that a given ring R is *not* Euclidean one needs to argue that no Euclidean function can exist. Evidently if R is not a PID, no such function can exist. However, there are PIDs which admit no Euclidean function (more details are given below).

One way to assess the naturality of the notion Euclidean domain is to examine its stability under small perturbations of the definition. In other words, to what extent do similar axioms for a "Euclidean function" lead to an equivalent class of rings?

There are several results to the effect that a certain weakening of the definition of a Euclidean function captures precisely the class of all PIDs. For example:

Theorem 16.14. *(Dedekind-Hasse) For a domain R with fraction field K, TFAE:*
(i) There exists a function $N : K \to \mathbb{Q}$ satisfying:
(QN1) $\forall x \in K,\ N(x) \geq 0;\ N(x) = 0 \iff x = 0$.
(QN2) $\forall x, y \in K,\ N(xy) = N(x)N(y)$.
(QN3) $\forall x \in R,\ N(x) \in \mathbb{Z}$.
(QN4) $\forall x \in R, N(x) = 1 \iff x \in R^\times$.
(QN5) $\forall x \in K \setminus R,\ \exists\ a, b \in R$ *such that* $0 < N(ax - b) < 1$.
(ii) R is a principal ideal domain.

Exercise 16.11: Prove Theorem 16.14. (Suggestions: (i) $\implies$ (ii) is the usual argument that an ideal is generated by any element of minimal norm. Conversely, if R is a PID, define N on $R \setminus \{0\}$ by, e.g., setting $N(x)$ to be 2^r, where $r = \ell(R/xR)$ is the number of irreducibles appearing in a factorization of x and extend this map to K.)

In another direction, P. Samuel considered the notion of a **W-Euclidean function** on a domain R. Here W is a well-ordered set and $N : R \to W$ is a function such that for all $a \in R, b \in R \setminus \{0\}$ such that $b \nmid a$, $\exists\ q, r \in R$ with $a = qb + r$ and $N(r) < N(b)$. If R admits, for some W, a W-Euclidean function, then R is a PID.

Exercise 16.12: Show that a domain is W-Euclidean for some finite W iff it is a field.

Say that a domain is **Samuel-Euclidean** if it is W-Euclidean for some well-ordered set W. Samuel remarks that the an imaginary quadratic fields $\mathbb{Q}(\sqrt{-d})$ has a Samuel-Euclidean ring of integers R_d iff $d = 1, 2, 3, 7, 11$. On the other hand, it goes back at least to Gauss that for each of $d = 19, 43, 67, 163$ the ring R_d is a PID. Thus there are PIDs which are not Samuel-Euclidean. Samuel further showed that any Samuel-Euclidean ring is W-Euclidean for a unique minimal well-ordered set (up to canonical order isomorphism) W_R and asked the question of whether one has $W_R \leq \mathbb{N}$ for all domains R. This was answered in the negative by Hiblot [Hi75], [Hi77].

16.4. **Bézout domains.**

Proposition 16.15. *Let a, b be elements of a domain. If the ideal $\langle a, b\rangle$ is principal, then its generator is a greatest common divisor of a and b.*

Proof. In other words, we are assuming the existence of some $d \in R$ such that $dR = aR + bR$. Then $a, b \in dR$, so d is a common divisor of a and b. If $e \mid a$ and $e \mid b$ then $e \in aR + bR = dR$, so $e \mid d$. □

Corollary 16.16. *For a domain R, TFAE:*
(i) Every finitely generated ideal is principal.
(ii) For any two elements a and b of R, $\gcd(a, b)$ exists and is an R-linear combination of a and b.

Proof. (i) $\implies$ (ii) is immediate from Proposition XX: $\gcd(a, b)$ will be a generator of the ideal $\langle a, b\rangle$. Conversely, if $d = \gcd(a, b)$ exists and is of the form $d = xa + yb$ for some $x, y \in R$, then clearly $(d) = \langle a, b\rangle$, so that every ideal with two generators is principal. By an obvious induction argument, we conclude that any finitely generated ideal is principal. □

At least according to some, it was Étienne Bézout who first explicitly noted that for polynomials $P, Q \in k[t]$, $\gcd(a, b)$ exists and is a linear combination of a and b: this fact is called **Bézout's identity** or **Bézout's Lemma**. For this (somewhat tenuous) reason, a possibly non-Noetherian domain satisfying the equivalent conditions of Corollary 16.16 is called a **Bézout domain**.

Exercise 16.13: Show: any localization of a Bézout domain is Bézout.

Theorem 16.17. *For a Bézout domain R, the following are equivalent:*
(i) R is a PID.

(ii) R is Noetherian.
(iii) R is a UFD.
(iv) R is an ACCP domain.
(v) R is an atomic domain.

Proof. (i) $\iff$ (ii) immediately from the definitions.
(i) $\implies$ (iii): this is Corollary 15.2.
(iii) $\implies$ (iv) $\implies$ (v) holds for all domains.
(v) $\implies$ (iii): A Bézout domain is a GCD-domain is an EL-domain, so a Bézout atomic domain is a UFD.
(iv) $\implies$ (ii): assume that R is *not* Noetherian. Then it admits an ideal I which is not finitely generated, which we can use to build an infinite strictly ascending chain of finitely generated ideals $I_1 \subsetneq I_2 \subsetneq \ldots \subsetneq I$. But since R is Bézout, each I_i is principal, contradicting ACCP. □

Let us say that a domain is **properly Bézout** if it is Bézout but not a PID.

We have already seen some examples of properly Bézout domains: the ring of entire functions (Theorem 5.20) and the ring of all algebraic integers (Theorem 5.1). To get further examples we move on to the next topic: valuation rings.

17. Valuation rings

17.1. **Basic theory.**

Consider the divisibility relation – i.e., $a \mid b$ – on a domain R. Evidently it is reflexive and transitive, so is a **quasi-ordering**.[62] Divisibility need *not* be a partial ordering because $a \mid b$ and $b \mid a$ does not imply that $a = b$ but only that a and b are associates: $(a) = (b)$. However, one of the first ideas of ideal theory is to view associate elements as being somehow "equivalent." This motivates us to consider the equivalence relation on R in which $a \sim b$ iff $(a) = (b)$. This is easily seen to be a **monoidal equivalence relation**. In plainer language, if $(a_1) = (a_2)$ and $(b_1) = (b_2)$, then $(a_1b_1) = (a_2b_2)$. We can therefore consider the commutative monoid of principal ideals of R under multiplication, on which the divisibility relation is a partial ordering.

Having made a quasi-ordering into a partial ordering, it is natural to ask for conditions under which the divisibility relation induces a **total ordering**. Equivalently, for any $a, b \in R$ either $a \mid b$ or $b \mid a$.

Proposition 17.1. *Let R be a domain with fraction field K. TFAE:*
(i) For every $a, b \in R$, $a \mid b$ or $b \mid a$.
(ii) For every $0 \neq x \in K$, $x \in R$ or $x^{-1} \in R$.

Exercise 17.1: Prove Proposition 17.1.

A domain R satisfying the conditions of Proposition 17.1 is called a **valuation domain** or **valuation ring**.

Note that any field is a valuation ring. This is a trivial example which is often implicitly excluded from consideration (we will try our best to be explicit in our

[62] By definition, a quasi-ordering is a reflexive, transitive binary relation on a set.

exclusion of trivial cases). Apart from this, in a first algebra course one may not see examples of valuation rings. But we have: if p is a prime number, then the ring $\mathbb{Z}_{(p)}$ of integers localized at p is such an example. Define $x \mid_p y$ if $\mathrm{ord}_p(\frac{y}{x}) \geq 0$. Then p-divisibility is immediately seen to be a total quasi-ordering: given two integers, at least one p-divides the other. The fundamental theorem of arithmetic implies

$$x \mid y \iff \forall \text{ primes } p,\ x \mid_p y.$$

However, in $\mathbb{Z}_{(p)}$, we have $x \mid y \iff x \mid_p y$, i.e., we have localized the divisibility relation to get a total quasi-order: $\mathbb{Z}_{(p)}$ is a valuation domain.

This argument generalizes as follows: let R be a PID[63] and $\mathfrak{p} = (\pi)$ be a prime ideal of R. We define $\mathrm{ord}_{\mathfrak{p}}(x)$ to be the least n such that $(x) \supset \mathfrak{p}^n$, and extend it to a map on $K^\times$ by $\mathrm{ord}_{\mathfrak{p}}(\frac{x}{y}) = \mathrm{ord}_{\mathfrak{p}}(x) - \mathrm{ord}_{\mathfrak{p}}(y)$. (One should check that this is well-defined; this is easy.) Finally, we define $x \mid_{\mathfrak{p}} y$ to mean $\mathrm{ord}_{\mathfrak{p}}(\frac{y}{x}) \geq 0$. Arguing as above, we see that the localization $R_{\mathfrak{p}}$ is a valuation ring.

Note that in showing that $R_{\mathfrak{p}}$ was a valuation domain we proceeded by constructing a map $\mathrm{ord}_{\mathfrak{p}}$ on the nonzero elements of the fraction field K. This can be generalized, as follows: if R is a domain with quotient field K, we can extend the divisibility relation to $K^\times$ by saying that $x \mid y$ iff $\frac{y}{x} \in R$. Clearly $x \mid y$ and $y \mid x$ iff $\frac{y}{x}$ is a unit in R. Therefore the quotient of $(K^\times, \cdot)$ on which divisibility (from R!) becomes a partial ordering is precisely the quotient group $K^\times/R^\times$.

For $[x], [y] \in K^\times/R^\times$, let us write $[x] \leq [y]$ if $[\frac{y}{x}] \in R$. (Take a second and check that this is well-defined.)

Exercise 17.2: Show that the divisibility quasi-ordering on R is a total ordering iff the ordering on $K^\times/R^\times$ is a total ordering.

In other words, if R is a valuation ring, then the canonical map $v : K^\times \to K^\times/R^\times$ is a homomorphism onto a totally ordered abelian group. Let us relabel the quotient group by G and denote the group law by addition, so that the homomorphism property gets recorded as

(VRK1) $\forall x, y \in K^\times\ v(ab) = v(a) + v(b)$.

We recover R as

$$R = \{x \in K^\times \mid v(x) \geq 0\} \cup \{0\}.$$

Everything that has been said so far takes into account only the multiplicative structure on R. So the following additional property is very important:

(VRK2) $\forall x, y \in K^\times \mid x + y \neq 0,\ v(x + y) \geq \min(v(x), v(y))$.

Indeed, suppose WLOG that $v(x) \leq v(y)$, i.e., $\frac{y}{x} \in R$. Then $\frac{x+y}{x} = 1 + \frac{y}{x} \in R$ so $v(x) \leq v(x + y)$.

[63] In fact we can take R to be any Dedekind domain, as soon as we know what such a thing is. See §18.

Exercise 17.3: Suppose that $v(x) \neq v(y)$. Show that $v(x+y) = \min(v(x), v(y))$.

Let $(G, +, \leq)$ be a totally ordered abelian group. We write $G^+ = \{g \in G \mid g \geq 0\}$, so G^+ is a totally ordered submonoid of G. A **(G-valued) valuation** on a field K is a surjective map $v : K^\times \to G$ satisfying (VRK1) and (VRK2) above.

Exercise 17.4: Let $v : K^\times \to G$ be a valuation. Let R be the set of elements of $K^\times$ with non-negative valuation, together with 0. Show that R is a valuation ring with fraction field K.

Exercise 17.5: Let R be a domain, G a totally ordered group and $v : R \setminus \{0\} \to G^+$ be a map which satisfies all of the following properties:
(VRR1) $\forall x, y \in R \setminus \{0\},\ v(ab) = v(a) + v(b)$.
(VRR2) $\forall x, y \in R \setminus \{0\} \mid x + y \neq 0,\ v(x+y) \geq \min(v(x), v(y))$.
(VRR3) $v(R \setminus \{0\}) \supset G^+$.
Show that there is a unique extension of v to a valuation $v : K^\times \to G$, namely $v(x/y) = v(x) - v(y)$.

Proposition 17.2. *A valuation ring is a local domain, in which the unique maximal ideal $\mathfrak{m}$ consists of elements of positive valuation.*

Proof. The set of elements of strictly positive valuation form an ideal $\mathfrak{m}$ of R. Its complement, the set of elements of zero valuation, is the group of units. □

Proposition 17.3. *Let I be a finitely generated ideal in a valuation ring. Then the set $v(I)$ has a least element, and for any $x \in I$ of minimal valuation, $I = v(x)$.*

Proof. Write $I = \langle x_1, \ldots, x_n \rangle$ with $v(x_1) \leq \ldots \leq v(x_n)$. Then for any $r_1, \ldots, r_n \in R$, $v(r_1 x_1 + \ldots + r_n x_n) \geq \min_i v(r_i x_i) \geq v(x_1)$, so x_1 is an element of I of minimal valuation. Thus for all $i > 1$, $v(\frac{x_i}{x_1}) \geq 0$, so $\frac{x_i}{x_1} \in R$ and $x_1 \mid x_i$. So $I = \langle x_1 \rangle$. □

Corollary 17.4. *A valuation ring is a Bézout domain. In particular, a Noetherian valuation ring is a PID.*

Conversely:

Proposition 17.5. *A local Bézout domain is a valuation domain.*

Proof. Let x, y be elements of a local Bézout domain, and suppose $d = \gcd(x, y)$. Then $\frac{x}{d}$ and $\frac{y}{d}$ are coprime. Since in a local ring the nonunits form an ideal, this implies that at least one of $\frac{x}{d}$ and $\frac{y}{d}$ is a unit. In other words, up to associates, $d = x$ (so $x \mid y$) or $d = y$ (so $y \mid x$). □

A **valued field** is a field together K together with a valuation $v : K^\times \to G$. An isomorphism of valued fields $(K, v) \to (K', v')$ is an isomorphism $f : K \to K'$ of fields such that $v = v' \circ f$. A valued field is **trivial** if G is the trivial group. Evidently each field carries a unique trivial valuation up to isomorphism: the valuation ring is K itself. The reader will lose nothing by making the tacit assumption that all valuations are nontrivial.

Exercise 17.6: A **chain ring** is a ring R in which the partially ordered set $\mathcal{I}(R)$ of ideals of R is linearly ordered.
a) Show that for a ring R, TFAE:

(i) R is a chain ring.
(ii) For all $x, y \in R$, either $xR \subset yR$ or $yR \subset xR$.
b) Show that a domain R is a chain ring iff it is a valuation ring.

17.2. **Ordered abelian groups.**

Let $(G, +)$ be an abelian group, written additively. In particular the identity element of G will be denoted by 0. As for rings, we write $G^\bullet$ for $G \setminus \{0\}$.

By an **ordering** on G we mean a total (a.k.a. linear) ordering $\leq$ on G which is compatible with the addition law in the following sense:

(OAG) For all $x_1, x_2, y_1, y_2 \in G$, $x_1 \leq x_2$ and $y_1 \leq y_2$ implies $x_1 + y_1 \leq x_2 + y_2$.

One has the evident notions of a homomorphism of ordered abelian groups, namely an isotone group homomorphism.

Exercise 17.7: Let $(G, \leq)$ be an ordered abelian group.
a) Let $x \in G^\bullet$. Show that either $x > 0$ or $-x > 0$ but not both.
b) Show that for all $x, y \in G$, $x \leq y \iff -y \leq -x$.

Exercise 17.8: Let $(G, \leq)$ be an ordered abelian group, and let H be a subgroup of G. Show that the induced order on H makes H into an ordered abelian group.

Example: For any ordered field $(F, \leq)$, the additive group $(F, +)$ is an ordered abelian group. In particular, the additive group $(\mathbb{R}, +)$ of the real numbers is an ordered abelian group, as is any subgroup. In particular, $(\mathbb{Z}, +)$ and $(\mathbb{Q}, +)$ are ordered abelian groups.

Exercise 17.9: Exhibit an abelian group which admits two nonisomorphic orderings.

Example (Lexicographic ordering): Let $\{G_i\}_{i \in I}$ be a nonempty indexed family of ordered abelian groups. Suppose that we are given a well-ordering on the index set I. We may then endow the direct product $G = \prod_{i \in I} G_i$ with the structure of an ordered abelian group, as follows: for $(g_i), (h_i) \in G$, we decree $(g_i) < (h_i)$ if for the least index i such that $g_i \neq h_i$, $g_i < h_i$.

Exercise 17.10: Check that the lexicographic ordering on the product $\prod_{i \in I} G_i$ is indeed a total ordering on G.

Theorem 17.6. *(Levi* [Lev43]*) For an abelian group G, TFAE:*
(i) G admits at least one ordering.
(ii) G is torsionfree.

Proof. (i) $\implies$ (ii) Suppose $<$ is an ordering on G and let $x \in G^\bullet$. Then exactly one of $x, -x$ is positive; without loss of generality say it is x. Then for all $n \in \mathbb{Z}^+$, $nx = x + \ldots x$ (n times) must be positive, so x has infinite order in G.
(ii) $\implies$ (i): Let G be a torsionfree abelian group. By Corollary 3.88, G is a flat $\mathbb{Z}$-module. Tensoring the injection $\mathbb{Z} \hookrightarrow \mathbb{Q}$ gives us an injection $G \hookrightarrow G \otimes \mathbb{Q}$. Since $\mathbb{Q}$ is a field, the $\mathbb{Q}$-module $G \otimes \mathbb{Q}$ is free, i.e., it is isomorphic to $\bigoplus_{i \in I} \mathbb{Q}$. Choose a

total ordering on I. Give each copy of $\mathbb{Q}$ its standard ordering as a subfield of $\mathbb{R}$ and put the lexicographic ordering on $\bigoplus_{i \in \mathbb{Q}} \mathbb{Q} \cong G \otimes \mathbb{Q}$. Via the injection $G \hookrightarrow G \otimes \mathbb{Q}$ this induces an ordering on G. □

Exercise 17.11: a) Show that the abelian group $\mathbb{Z}$ admits exactly one ordering (here when we say "ordering", we always mean "ordering compatible with the group structure in the sense of (OAG).
b) Give an example of an abelian group which admits two distinct – even nonisomorphic – orderings.

An ordered abelian group $(G, +)$ is **Archimedean** if for all $x, y \in G$ with $x > 0$, there exists $n \in \mathbb{Z}^+$ with $nx > y$.

Exercise 17.12:
a) Suppose H is a subgroup of the Archimedean ordered group $(G, +)$. Show that the induced ordering on G is Archimedean.
b) Let $(G, +)$ be an ordered abelian group such that there exists an embedding $(G, +) \hookrightarrow (\mathbb{R}, +)$ into the additive group of the real numbers. Deduce that G is Archimedean.

Conversely:

Theorem 17.7. *(Hölder* [Hö01]*) Let $(G, +)$ be an ordered abelian group. If G is Archimedean, there exists an embedding $(G, +) \hookrightarrow (\mathbb{R}, +)$.*

Proof. We may assume G is nontrivial. Fix any positive element x of G. We will construct an order embedding of G into $\mathbb{R}$ mapping x to 1.

Namely, let $y \in G$. Then the set of integers n such that $nx \leq y$ has a maximal element n_0. Put $y_1 = y - n_0 x$. Now let n_1 be the largest integer n such that $nx \leq 10y_1$: observe that $0 \leq n_1 < 10$. Continuing in this way we get a set of integers $n_1, n_2, \ldots \in \{0, \ldots, 9\}$. We define $\varphi(y)$ to be the real number $n_0 + \sum_{k=1}^{\infty} \frac{n_k}{10^k}$. It is not hard to show that φ is isotone – $y \leq y' \implies \varphi(y) \leq \varphi(y')$ – and also that φ is injective: we leave these tasks to the reader.

But let us check that φ is a homomorphism of groups. For $y \in G$, and $r \in \mathbb{Z}^+$, let $\frac{n}{10^r}$ be the rational number obtained by truncating $\varphi(y)$ at r decimal places. The numerator n is characterized by $nx \leq 10^r y < (n+1)x$. For $y' \in G$, if $n'x \leq 10^r y' \leq (n'+1)x$, then

$$(n + n')x \leq 10^r(y + y') < (n + n' + 2)x,$$

so

$$\varphi(y + y') - (n + n')10^{-r} < \frac{2}{10^r}$$

and thus

$$|\varphi(y + y') - \varphi(y) - \varphi(y')| < \frac{4}{10^r}.$$

Since r is arbitrary, we conclude $\varphi(y + y') = \varphi(y) + \varphi(y')$. □

A nontrivial ordered abelian group which can be embedded in $\mathbb{R}$ is said to have **rank one**. For many applications this is by far the most important case. Later we will give the general definition of the rank of an ordered abelian group.

The following result gives another characterization of valuation rings of rank one.

Lemma 17.8. *Let R be a domain, $(G, \leq)$ a totally ordered commutative group, and let $G^+ = \{g \in G \mid g \geq 0\}$. Then:*
a) G^+ is an ordered commutative monoid.
b) The monoid ring $R[G^+]$ is an integral domain.
c) The group ring $R[G]$ is naturally isomorphic to the localization of $R[G^+]$ at the multiplicative subset G^+. In particular, $R[G]$ is an integral domain.

Exercise 17.13: a) Write out the statements of Lemma 17.8 when $G = \mathbb{Z}$.
b) Prove Lemma 17.8.

Theorem 17.9. *(Malcev, Neumann) For any ordered abelian group G, there exists a valuation domain with value group isomorphic to G.*

Proof. It suffices to construct a field K and a surjective map $v : K^\times \to G$ satisfying (VD1K) and (VD2K). Let k be any field and put $A = k[G^{\geq 0}]$. By Lemma 17.8, A is a domain; let K be its fraction field. Define a map $v : A^\bullet \to G$ by sending a nonzero element $\sum_{g \in G} a_g g$ to the least g for which $a_g \neq 0$. Then v satisfies the three properties of Exercise 17.5 and therefore extends uniquely to a valuation $v : K^\times \to G$, where K is the fraction field of R. □

Recall from §5.5 the notion of a "big monoid ring" $k[[\Gamma]]$, the collection of *all* functions $f : \Gamma \to k$ under pointwise addition and convolution product. As we saw though, in order for the convolution product to be defined "purely algebraically" – i.e., without recourse to some limiting process – we need to impose the condition of *divisor finiteness* on Γ. It follows easily from Proposition 17.18 that for $\Gamma = G^{\geq 0}$ the monoid of non-negative elements in a totally ordered abelian group, divisor finiteness holds iff $G = \mathbb{Z}$, i.e., iff the valuation is discrete.

However, Malcev [Mal48] and Neumann [Neum49] independently found a way around this by considering a set in between $k[G^{\geq 0}]$ and $k[[G^{\geq 0}]]$. Namely, define $k_{\mathrm{MN}}[G^{\geq 0}]$ to be the set of all functions $f : G^{\geq 0} \to k$ such that the *support* of f – i.e., the set of $g \in G^{\geq 0}$ such that $f(g) \neq 0$ – is well-ordered. It turns out that on such functions the convolution product can be defined and endows $k_{\mathrm{MN}}[G^{\geq 0}]$ with an integral domain. The fraction field $k_{\mathrm{MN}}(G)$ is simply the collection of all functions $f : G \to k$ with well-ordered support. Moreover, mapping each such nonzero function to the least element of G in its support gives a G-valued valuation. The elements of such rings are called **Malcev-Neumann series**.

17.2.1. *Convex Subgroups.*

A subset S of a totally ordered set $(X, \leq)$ is **convex** if for all $x < y < z \in X$, if $x, z \in S$, then $y \in S$.

Exercise: Let H be a subgroup of an ordered abelian group $(G, \leq)$. Show that H is convex iff for all $x, y \in G$ with $0 \leq x \leq y$, if $y \in H$ then also $x \in H$.

Proposition 17.10. *Let $(G, \leq)$ be an ordered abelian group, and let $\mathcal{C}(G)$ be the family of convex subgroups of G. Then $\mathcal{C}(G)$ is totally ordered under inclusion.*

Proof. Let H_1 and H_2 be convex subgroups. Seeking a contradiction, we suppose there is $h_1 \in H_1 \setminus H_2$ and $h_2 \in H_2 \setminus H_1$. Since subgroups are closed under inversion, we may assume that $h_1, h_2 \geq 0$ and then, without loss of generality, that $0 \leq h_1 \leq h_2$. Since H_2 is a convex subgroup, it follows that $h_1 \in H_2$, contradiction. □

For an ordered abelian group G, we define $r(G)$ to be the order isomorphism type of the linearly ordered set $\mathcal{C}(G)^\bullet = \mathcal{C}(G) \setminus \{\{0\}\}$ of nontrivial convex subgroups of G. When this set is finite we may view $r(G)$ as a natural number. In particular, $r(G) = 1$ iff G is nontrivial and has no proper, nontrivial convex subgroups.

Exercise: a) Let G_1 and G_2 be ordered abelian groups, and let $G = G_1 \times G_2$ be lexicographically ordered. Show that $r(G) = r(G_1) + r(G_2)$, where on the right hand side we have the ordered sum: every element of the first linearly ordered set is less than every element of the second linearly ordered set.
b) Let $n \in \mathbb{Z}^+$. Show that $r(\mathbb{Z}^n) = n$.

Proposition 17.11. *For a nontrivial ordered abelian group G, TFAE:*
(i) G is Archimedean.
(ii) $r(G) = 1$.

Proof. □

In view of Proposition 17.11 it makes sense to call $r(G)$ the **rank** of the linearly ordered group G: indeed we have already defined a group to have rank one if it is nontrivial and can be order embedded in $(\mathbb{R}, +)$. By Theorem 17.7, G is Archimedean iff it can be order embedded in $(\mathbb{R}, +)$, so by Proposition 17.11 our new notion of rank coincides with our old notion of rank one.

Theorem 17.12. *Let $v : K^\times \to (G, \leq)$ be a valuation on a field K, with valuation ring R. There is an inclusion reversing bijection $\Phi : \operatorname{Spec} R \to \mathcal{C}(G)$ given by*

$$\mathfrak{p} \mapsto G \setminus \pm v(\mathfrak{p}).$$

Proof. Step 1: We claim that for $\mathfrak{p} \in \operatorname{Spec} R$, $\Phi(\mathfrak{p})$ is a convex subgroup. Clearly $\Phi(\mathfrak{p})$ contains 0 and is closed under inversion, so suppose $\sigma_1, \sigma_2 \in \Phi(\mathfrak{p})$. Since $\Phi(\mathfrak{p})$ is closed under inversion, we may assume that either $\sigma_1, \sigma_2 > 0$ or $\sigma_1 > 0$, $\sigma_2 < 0$ and $\sigma_1 + \sigma_2 > 0$.
Case 1: Suppose $\sigma_1, \sigma_2 > 0$. Choose $x_1, x_2 \in R$ with $v(x_i) = \sigma_i$ for $i = 1, 2$. If $\sigma_1 + \sigma_2 \notin \Phi(\mathfrak{p})$, then there is $x \in \mathfrak{p}$ with $v(x) = \sigma_1 + \sigma_2 = v(x_1 x_2)$. Thus $ux = x_1 x_2$ for some $u \in R^\times$, so $x_1 x_2 \in \mathfrak{p}$. Since $\mathfrak{p}$ is prime this implies that at least one of x_1, x_2 lies in $\mathfrak{p}$, hence at least one of σ_1, σ_2 does not lie in $\Phi(\mathfrak{p})$, contradiction.
Case 2: Suppose $\sigma_1 > 0$, $\sigma_2 < 0$, $\sigma_1 + \sigma_2 > 0$. If $\sigma_1 + \sigma_2 \notin \Phi(\mathfrak{p})$, then there is $x \in \mathfrak{p}$ with $v(x) = \sigma_1 + \sigma_2$. Choose $y \in R$ with $v(y) = -\sigma_2$. Then $yx \in \mathfrak{p}$ and $v(yx) = \sigma_1$, so $\sigma_1 \in v(\mathfrak{p})$, contradiction.

To show convexity: let $0 \leq \sigma_1 \leq \sigma_2 \in G$, and suppose $\sigma_2 \in \Phi(\mathfrak{p})$. If $\sigma_1 \in v(\mathfrak{p})$, then there exists $x \in \mathfrak{p}$ with $v(x) = \sigma_1$. There is $y \in R$ such that $v(y) = \sigma_2 - \sigma_1$, and thus $v(yx) = \sigma_2$, so $\sigma_2 \notin \Phi(\mathfrak{p})$, contradiction.
Step 2: To a convex subgroup H of G, we associate

$$\Psi(H) = \{x \in R^\bullet \mid v(x) \notin H\} \cup \{0\}.$$

By similar – but easier – reasoning to the above, one checks that $\Psi(H) \in \operatorname{Spec} R$.
Step 3: One checks that Φ and Ψ are mutually inverse maps, hence Φ is a bijection. □

Exercise: Supply the details of Steps 2 and 3 in the proof of Theorem 17.12.

Exercise: Show that the maps Φ and Ψ are obtained by restricting the Galois connection associated to a relation on $R \times G$.

Corollary 17.13. *For a valuation ring R, TFAE:*
(i) R has rank one, i.e., the value group is Archimedean.
(ii) R has Krull dimension one.

17.3. **Connections with integral closure.**

Let $(R, \mathfrak{m}_R)$ and $(T, \mathfrak{m}_T)$ be local rings with $R \subset T$. We say that **T dominates R**, and write $R \leq T$, if $\mathfrak{m}_T \cap R = \mathfrak{m}_R$.

Lemma 17.14. *Let R be a subring of a field K, and let $\mathfrak{p} \in \operatorname{Spec} R$. Then there exists a valuation ring T of K such that $R \subset T$ and $\mathfrak{m}_T \cap R = \mathfrak{p}$.*

Proof. (Matsumura)
Step 0: We may replace R by $R_{\mathfrak{p}}$ and thus asume that $(R, \mathfrak{p})$ is a local ring. In this case, what we are trying to show is precisely that there exists a valuation ring of K dominating R.
Step 1: Let $\mathcal{F}$ be the set of all rings R' with $R \subset R' \subset K$ such that $\mathfrak{p}R' \subsetneq R'$, partially ordered by inclusion. We have $R \in \mathcal{F}$, so $\mathcal{F} \neq \varnothing$. Moreover the union of a chain in $\mathcal{F}$ is again an element of $\mathcal{F}$, so Zorn's Lemma gives us a maximal element T of $\mathcal{F}$. Since $\mathfrak{p}T \subsetneq T$, there exists a maximal ideal $\mathfrak{m}$ of T containing $\mathfrak{p}T$. Since $T \subset T_{\mathfrak{m}}$ and $T_{\mathfrak{m}} \in \mathcal{F}$, by maximality of T we have $T = T_{\mathfrak{m}}$, so $(T, \mathfrak{m})$ is a local ring dominating $(R_{\mathfrak{p}}, \mathfrak{p})$.
Step 2: We CLAIM that T is a valuation ring.
PROOF OF CLAIM: Let $x \in K^\times$. We wish to show that at least one of x, x^{-1} lies in T. Seeking a contradiction, assume neither is the case. Then $T[x]$ properly contains T, so by maximality of T we have $1 \in \mathfrak{p}T[x]$, i.e., we get a relation of the form

$$1 = a_0 + a_1 x + \ldots + a_n x^n, a_i \in \mathfrak{p}T.$$

Since T is local, $1 - a_0 \in T^\times$, and the relation may be rewritten in the form

$$1 = b_1 x + \ldots + b_n x^n, b_i \in \mathfrak{m}. \tag{35}$$

Among all such relations, we may choose one with minimal exponent n. In exactly the same way, $T[x^{-1}]$ properly contains T and thus there exists a relation

$$1 = c_1 x^{-1} + \ldots + c_n x^{-m}, c_i \in \mathfrak{m}, \tag{36}$$

and among all such relations we may choose one with minimal m. Without loss of generality $m \leq n$: otherwise interchange x and x^{-1}. Then multiplying (36) by $b_n x^n$ and subtracting from (35) gives another relation of the form (35) but with exponent smaller than n, contradiction. □

A subring R of a field K is a **maximal subring** if $R \subsetneq K$ and there is no ring intermediate between R and K.

Exercise 17.14: a) Show that any field K admits at least one maximal subring.
b) Show that if K is not finite of prime order, then all maximal subrings are nonzero.
c) Excluding the case in which K is finite of prime order, show that any maximal subring of K is a valuation ring of K (possibly a field).

Exercise 17.15: Let K be a field, and R a valuation ring of K. Show TFAE:
(i) R is a maximal subring of K.
(ii) R has rank at most one.

Theorem 17.15. *Let K be a field and $R \subset K$ a subring. Then the integral closure $\overline{R}$ of R in K is equal to the intersection of all valuation rings of K containing R.*

Proof. Let $\mathcal{R}$ be the intersection of all valuation rings of K containing R. Since each such ring is integrally closed in K and the intersection of a family of rings each integrally closed in K is again integrally closed in K, $\mathcal{R}$ is integrally closed in K, whence $\overline{R} \subset \mathcal{R}$.
Conversely, let $x \in K \setminus \overline{R}$. It suffices to find a valuation ring of K containing R but not x. Let $y = x^{-1}$. The ideal $yR[y]$ of $R[y]$ is proper: for if $1 = a_1 y + \ldots + a_n y^n$ with $a_i \in R$, then x would be integral over R. Let $\mathfrak{p}$ be a maximal ideal of R containing y. By Lemma 17.14, there exists a valuation ring T of K such that $R[y] \subset K$ and $\mathfrak{m}_T \cap R[y] = \mathfrak{p}$. Then $y = x^{-1} \in \mathfrak{m}_T$, so $x \notin T$. □

17.4. **Another proof of Zariski's Lemma.**

The following result is a close relative of Lemma 17.14.

Lemma 17.16. *Let K be a field and Ω an algebraically closed field. Let $\mathcal{S}$ be the set of all pairs (A, f) with A is a subring of K and $f : A \hookrightarrow \Omega$, partially ordered by*

$$(A, f) \leq (A', f') \iff A \subset A' \text{ and } f'|_A = f.$$

Then $\mathcal{S}$ contains maximal elements, and for any maximal element (B, g), B is a valuation ring of K.

Proof. An easy Zorn's Lemma argument shows that $\mathcal{S}$ has maximal elements.
Let (B, g) be a maximal element. Put $\mathfrak{p} = \mathrm{Ker}(g)$; since $g(B)$ is a subring of the field Ω, it is a domain and thus $\mathfrak{p}$ is a prime ideal of B. By functoriality of localization, G extends to a homomorphism $B_{\mathfrak{p}} \to \Omega$. By maximality of (B, g) we have $B_{\mathfrak{p}} = B$, so that B is a local ring with maximal ideal $\mathfrak{p}$. If there existed an element $x \in K$ which is transcendental over the fraction field of B, then $B[x]$ is a polynomial ring and certainly g extends to $B[x]$. So K is algebraic over the fraction field of B.

Next let $x \in K^\times$. We claim that either the ideal $\mathfrak{p}B[x]$ or $\mathfrak{p}B[x^{-1}]$ is proper. Indeed this is proved exactly as in Lemma 17.14 above.

Finally, we show that B is a valuation ring of K. Let $x \in K^\bullet$. Without loss of generality, we may assume that $\mathfrak{p}B[x]$ is a proper ideal of B (otherwise replace x by x^{-1}). Put $B' = B[x]$. By assumption, $\mathfrak{p}B[x]$ is contained in a maximal ideal $\mathfrak{m}$ of B' and $\mathfrak{m} \cap B = \mathfrak{p}$. Hence the embedding of domains $B \to B'$ induces an embedding of fields $k := B/\mathfrak{p} \hookrightarrow B'/\mathfrak{m} = k'$. Moreover k' is generated over k by the image of the algebraic element x, so k'/k is a finite degree field extension. So g induces an embedding $k \hookrightarrow \Omega$, and since Ω is algebraically closed, this extends to an embedding $k' = B'/\mathfrak{m} \hookrightarrow \Omega$. By maximality of B, this implies $x \in B$. □

Remark: It should be possible to consolidate Lemmas 17.14 and 17.16 into a single result. Let me know if you see how to do it.

Proposition 17.17. *Let $A \subset B$ be domains with B finitely generated as an A-algebra. Let $\beta \in B^\bullet$. There exists $\alpha \in A^\bullet$ satisfying the following property: any homomorphism f of A into an algebraically closed field Ω with $f(\alpha) \neq 0$ extends to a homomorphism $f : B \to \Omega$ with $f(\beta) \neq 0$.*

Proof.
Step 0: Induction on the number of generators reduces us to the case $B = A[x]$.

Step 1: Suppose that x is transcendental over A, i.e., B is a univariate polynomial ring over A. Write

$$\beta = a_n x^n + \ldots + a_1 x + a_0, a_i \in A$$

and put $\alpha = a_0$. If $f : A \to \Omega$ is such that $f(\alpha) \neq 0$, then since Ω is infinite, there exists $\zeta \in \Omega$ such that $f(a_n)\zeta^n + \ldots + f(a_1)\zeta + f(a_0) \neq 0$. Using the universal polynomial of polynomial rings, we may uniquely extend f to a homomorphism from B to Ω by putting $f(x) = \zeta$, and then $f(\beta) \neq 0$.
Step 2: Suppose that x is algebraic over the fraction field of A. Then so is β^{-1}. Hence we have equations of the form

$$a_n x^m + \ldots + a_1 x + a_0, \ a_i \in A$$

$$a'_m \beta^{-m} + \ldots + a'_1 \beta^{-1} + a'_0, a'_i \in A.$$

Put $\alpha = a_n a'_m$. Suppose $f : A \to \Omega$ is any homomorphism with $f(\alpha) \neq 0$. We may extend f to a homomorphism from $A[\alpha^{-1}] \to \Omega$ by mapping α^{-1} to $f(\alpha)^{-1}$ and then, by Lemma 17.16, to a homomorphism $f : C \to \Omega$ for some valuation ring C containing $A[\alpha^{-1}]$. By construction x is integral over $A[\alpha^{-1}]$. Since C is integrally closed, $x \in C$. Thus C contains B and in particular $\beta \in C$. Similarly, β^{-1} is integral over $A[\alpha^{-1}]$ so $\beta^{-1} \in C$. Thus $\beta \in C^\times$, so $f(\beta) \neq 0$. Restricting to B gives the desired homomorphism. □

Proof of Zariski's Lemma: Let k be a field and B a field which is finitely generated as a k-algebra. We want to show that B is a finite field extension of B. Equivalently, it is enough to show that B/k is algebraic. In Proposition 17.17 take $A = k$, $\beta = 1$ and Ω to be an algebraic closure of k. □

17.5. **Discrete valuation rings.**

17.5.1. *Introducing DVRs.*

Proposition 17.18. *For a valuation ring R with value group G, TFAE:*
(i) R is a PID.
(ii) R is Noetherian.
(iii) R is an ACCP-domain.
(iv) $G^{\geq 0} = \{x \in G \mid x \geq 0\}$ is well-ordered.
(v) G is isomorphic to $(\mathbb{Z}, \leq)$.

Proof. (i) $\iff$ (ii) $\iff$ (iii) is a special case of Theorem 16.17.
(iii) $\iff$ (iv): a totally ordered set is well-ordered iff there are no infinite strictly descending chains. But an infinite strictly descending chain in $G^{\geq 0}$ gives rise to an infinite strictly ascending chain of principal ideals in R, and conversely.
(iv) $\implies$ (v): First suppose G is Archimedean, so $G \hookrightarrow \mathbb{R}$: this endows G with a topology. If G is discrete, it is generated by its least positive element hence is order-isomorphic to $\mathbb{Z}$. If G is not discrete, there exists an infinite strictly decreasing sequence of positive elements of G converging to 0, so $G^{\geq 0}$ is not well-ordered. Next suppose that G is not Archimedean, and choose $x, y > 0$ such that for all $n \in \mathbb{Z}^+$, $nx < y$. Then $\{y - nx\}_{n \in \mathbb{Z}^+}$ is an infinite strictly descending sequence in $G^{\geq 0}$, contradicting well-ordering.
(v) $\implies$ (iv): famously, the standard ordering on $\mathbb{Z}^{\geq 0}$ is a well-ordering. □

Exercise 17.16: Show directly: a local PID is a valuation ring with value group $\mathbb{Z}$.

A valuation ring satisfying the equivalent conditions of Proposition 17.18 is called a **discrete valuation ring** (or, sometimes, a **DVR**).

17.5.2. *Further characterizations of DVRs.*

In many ways, discrete valuation rings are – excepting only fields – the simplest class of rings. Nevertheless they have an important role to play in algebra and arithmetic and algebraic geometry. One reason for this is as follows: every DVR is a one-dimensional Noetherian local ring. The converse does not hold.

Example: Let k be a field, and let R be the k-subalgebra of $k[t]$ generated by t^2 and t^3. This is a one-dimensional Noetherian domain; the ideal $\mathfrak{m}$ generated by t^2 and t^3 is a nonprincipal maximal ideal. Indeed, even in the localization $R_{\mathfrak{m}}$ the ideal $\mathfrak{m}R_{\mathfrak{m}}$ is not principal: consider what its order at 0 would be with respect to the valuation ord_t on $k(t)$: it would have to be 1, but there is no such element in $R_{\mathfrak{m}}$.

The question then is to find necessary and sufficient conditions for a one-dimensional Noetherian local domain to be a DVR. As we have seen, being a PID is enough, but again, this is not very useful as whether a one-dimensional domain is a PID is difficult to check in practice. Remarkably, it turns out if a local, one-dimensional Noetherian domain has any one of a large number of good properties, it will necessarily be a DVR. Here is the theorem.

Theorem 17.19. *(Recognition Theorem for DVRs) Let R be a one-dimensional Noetherian local domain, with maximal ideal $\mathfrak{m}$. TFAE:*
*(i) R is **regular**: the dimension of $\frac{\mathfrak{m}}{\mathfrak{m}^2}$ as an $R/\mathfrak{m}$-vector space is 1.*
(ii) $\mathfrak{m}$ is principal.
(iii) R is a PID.
(iv) R is a UFD.
(v) R is integrally closed.
(vi) Every nonzero ideal is of the form $\mathfrak{m}^n$ for some $n \in \mathbb{N}$.

Proof. (i) $\iff$ (ii): Choose $t \in \pi \setminus \pi^2$. By assumption, t generates $\mathfrak{m}/\mathfrak{m}^2$, so by Nakayama's Lemma t generates $\mathfrak{m}$. Conversely, if $\mathfrak{m}$ is monogenic as an R-module, certainly $\mathfrak{m}/\mathfrak{m}^2$ is monogenic as an $R/\mathfrak{m}$-module.
Evidently (iii) $\implies$ (ii). Proposition 16.6 gives (ii) $\implies$ (iii) and also (ii) $\implies$ (vi). Moreover (iii) $\iff$ (iv) by Proposition 16.1 and (iv) $\implies$ (v) by 15.14. Next, for all $n \in \mathbb{N}$ we have $(\pi)^n/(\pi)^{n+1} \cong R/\mathfrak{m}$, thus R is regular.

(vi) $\implies$ (i): Assume that $\dim_{R/\mathfrak{m}} \mathfrak{m}/\mathfrak{m}^2 > 1$. Choose $u \in \mathfrak{m} \setminus \mathfrak{m}^2$. Then

$$\mathfrak{m} \subsetneq \langle u, \mathfrak{m}^2 \rangle \subsetneq \mathfrak{m}^2.$$

So we have (i) $\iff$ (ii) $\iff$ (iii) $\iff$ (iv) $\iff$ (vi) $\implies$ (v).

Finally, we show (v) $\implies$ (ii): Let $0 \neq x \in \mathfrak{m}$. Since $\mathfrak{m}$ is the only prime ideal containing (x) we must have $r((x)) = \mathfrak{m}$. Since $R/(x)$ is Noetherian, its radical, $\mathfrak{m}/(x)$, is nilpotent, so there is a unique *least* $n \in \mathbb{Z}^+$ such that $\mathfrak{m}^n \subset (x)$. Let $y \in \mathfrak{m}^{n-1} \setminus (x)$ and consider the element $q = \frac{x}{y}$ of the fraction field K of R. Since $y \notin (x)$, $q^{-1} = \frac{y}{x} \notin R$; since R is integrally closed in K, q^{-1} is not integral over R. Then $\mathfrak{q}^{-1}\mathfrak{m}$ is not contained in $\mathfrak{m}$, for otherwise $\mathfrak{m}$ would be a faithful $R[q^{-1}]$-module

which is finitely generated as an R-module, contradicting Theorem 14.1. But by construction, $q^{-1}\mathfrak{m} = \frac{y}{x}\mathfrak{m} \subset R$, hence $q^{-1}\mathfrak{m} = R$ and then $\mathfrak{m} = Rx = (x)$. □

17.5.3. *Modules over DVRs.*

Lemma 17.20. *Let R be a DVR with uniformizing element π, and let $a \in \mathbb{Z}^+$. Then the ring $R_a = R/(\pi^a)$ is **self-injective** – i.e., R_a is an injective R_a-module.*

Exercise 17.17: Prove Lemma 17.20. (Hint: Baer's Criterion!)

Theorem 17.21. *Let R be a DVR with uniformizing element π, and let M be a nonzero finitely generated R-module.*
a) There is $N \in \mathbb{N}$ and positive integers $n, a_1 \geq a_2 \geq \ldots \geq a_n$ such that

$$M \cong R^N \oplus \bigoplus_{i=1}^{n} R/(\pi^{a_i}). \tag{37}$$

b) The numbers $N, n, a_1, \ldots, a_n$ are invariants of the isomorphism class of the module M: i.e., they are the same for any two decompositions of M as in (37) above.

Proof.
Step 0: Consider the canonical short exact sequence

$$0 \to M[\text{tors}] \to M \to M/M[\text{tors}] \to 0.$$

Since M is a finitely generated module over a Noetherian ring, $M[\text{tors}]$ is finitely generated. Moreover, $M/M[\text{tors}]$ is a finitely generated torsionfree module over a PID, hence is free (Proposition 3.58). Moreover, we know that the rank of a free module over any (commutative!) ring is well-defined (when R is a domain with fraction field K, the proof is especially easy: the rank of a free module M is $\dim_K M \otimes_R K$), so the invariant N in the statement of the theorem is precisely the rank of $M/M[\text{tors}]$. Moreover, since $M/M[\text{tors}]$ is free – hence projective – the sequence splits, so

$$M = R^N \oplus M[\text{tors}].$$

We are reduced to the case of a nonzero finitely generated torsion module M.
Step 1: The annihilator of M is an ideal of R, of which there aren't so many: it must be (π^{a_1}) for some $a_1 \in \mathbb{Z}^+$. Thus M may be viewed as a faithful $R_{a_1} = R/(\pi^{a_1})$-module. Moreover, choosing an element x of M which is not annihilated by π^{a_1-1}, the unique R_{a_1}-module map $R_{a_1} \to M$ which sends 1 to m is an injection. Taking $M' = M/R_{a_1}$, we get a short exact sequence

$$0 \to R_{a_1} \to M \to M' \to 0.$$

By Lemma 17.20, R_{a_1} is an injective R_{a_1}-module, so the sequence splits:

$$M \cong R_{a_1} \oplus M'.$$

Step 2: Since M is finitely generated over R_{a_1}, it is a quotient of some Artinian R_{a_1}-module $R_{a_1}^M$, hence by Theorem 8.2 M is Artinian. Moreover M is a finitely generated module over the Noetherian ring, so M is also Noetherian. By Theorem 8.12, this means that M has finite length as an R-module. Hence so does its direct summand M' and indeed clearly the length of M' is less than the length of M. This completes the proof of part a) by induction.
Step 3: So far we have that a finitely generated torsion R-module is of the form $\bigoplus_{i=1}^n R/(\pi^{a_i})$ with positive integers $a_1 \geq a_2 \geq \ldots \geq a_n$, and with $\text{ann}(M) = (\pi^{a_1})$.

In order to prove the uniqueness statement of part b), it suffices to prove that for all $0 < b \leq a$, $R/(\pi^b)$ is an indecomposable $R/(\pi^a)$-module. If so, then

$$M \cong \bigoplus_{i=1}^{n} R/(\pi^{a_i})$$

is simply the decomposition of the finite length module M into indecomposables described in the Krull-Schmidt Theorem: in particular, since clearly $R/(\pi^a) \cong R/(\pi^b)$ implies $a = b$ (consider annihilators), it is unique up to permutation of the factors. So suppose that $R/(\pi^a) = M_1 \oplus M_2$ with M_1, M_2 nonzero. If π^a does not annihilate M_1, then as above we can find a split embedding $R/(\pi^a) \hookrightarrow M_1$, which contradicts the fact that the length of M_1 must be smaller than the length of $R/(\pi^a)$. So M_1 – and similarly M_2 – is annihilated by π^{a-1} and thus $R/(\pi^a)$ would be annihilated by π^{a-1}, a contradiction. □

Remark: Theorem 17.21 is nothing else than the fundamental structure theorem for modules over a PID in the special case in which the PID has a unique maximal ideal. But we have not given a proof of this structure theorem for PIDs in these notes, whereas later we will want to use it to prove a more general structure theorem for torsion modules over a Dedekind domain. However, in both cases it is easy to reduce to the local situation, and thus we will get an independent proof.

18. Normalization theorems

We work in the following situation: R is an integrally closed domain with fraction field K, L/K is a field extension, and $S = I_L(R)$ is the integral closure of R in L. In more geometric language, S is the **normalization** of R in the extension L/K.

As above, we may as well assume that L/K is algebraic, since in the general case, if we let $L' = I_K(L)$ be the algebraic closure of K in L, then S is contained in L' anyway. So let us assume this. Then we know that S is integrally closed with fraction field L. We also know that the Krull dimensions of S and R coincide.

The major questions are the following:

(Q1) Is S finitely generated as an R-module?
(Q2) Is S Noetherian?
(Q3) If not, then can anything nice be said about S?

Note that if R is Noetherian, then an affirmative solution to (Q1) implies an affirmative answer to (Q2). Also, the example $R = \mathbb{Z}$, $K = \mathbb{Q}$, $L = \overline{\mathbb{Q}}$ shows that both (Q1) and (Q2) may have a negative answer if $[L : K]$ is infinite.

18.1. **The First Normalization Theorem.**

The first, and easiest, result is the following:

Theorem 18.1. *(First Normalization Theorem) Let R be an integrally closed domain with fraction field K, L/K a finite **separable** field extension, and $S = I_L(R)$.*
a) There exists a K-basis $x_1, \ldots, x_n$ of L such that S is contained in the R-submodule generated by $x_1, \ldots, x_n$.
b) If R is Noetherian, S is a finitely generated R-module.
c) If R is a PID, then S is a free R-module of rank $[L : K]$.

Proof. a) By the proof of Proposition 14.10, for any $x \in L$, there exists $0 \neq r \in R$ such that $rx \in S$. Therefore there exists a K-basis $u_1, \ldots, u_n$ of L such that $u_i \in S$ for all i.[64] Now take $x \in S$ and write $x = \sum_i b_i u_i$ with $b_i \in K$. Since L/K is separable there are $n = [L : K]$ distinct K-embeddings of L into $\overline{K}$, say $\sigma_1, \ldots, \sigma_n$, and the discriminant $\Delta = \Delta(u_1, \ldots, u_n) = (\det(\sigma_j(u_i)))^2$ is nonzero. We may put $\sqrt{\Delta}) = \det(\sigma_j(u_i))$. For all $1 \leq j \leq n$ we have

$$\sigma_j(x) = \sum_i b_i \sigma_j(u_i).$$

Using Cramer's rule, we may solve for the b_i to get

$$\sqrt{\Delta} b_i = \sum_j d_{ij} \sigma_j(x), \ db_i = \sum_j \sqrt{d} d_{ij} \sigma_j(x),$$

where the d_{ij}'s are polynomials in the $\sigma_j(u_i)$ with coefficients in $\mathbb{Z}$. Thus Δb_i and $\sqrt{\Delta} b_i$ are integral over R. Since $\Delta \in K$ and R is integrally closed, we have $\Delta b_i \in A$. Therefore S is contained in the R-span $\langle \frac{u_1}{\Delta}, \ldots, \frac{u_n}{\Delta} \rangle_R$, establishing part a).
b) By part a), S is a submodule of a finitely generated R-module, hence if R is Noetherian S is finitely generated.
c) We know that S is a submodule of a free rank n R-module; if R is a PID, then S is a free R-module of rank at most n. Since $S \otimes_R K = L$, the rank must be n. □

This has the following important result, which is the first of three fundamental **finiteness theorems** in algebraic number theory, the existence of a finite integral basis for the ring of integers of any algebraic number field:

Corollary 18.2. *Let $R = \mathbb{Z}$, $K = \mathbb{Q}$, L a number field of degree n. Then the ring $\mathbb{Z}_L = \overline{\mathbb{Z}} \cap K$ of all algebraic integers lying in L, is an integrally closed, Noetherian domain of Krull dimension one which is, as a $\mathbb{Z}$-module, free of rank n.*

Proof. Indeed $\mathbb{Z}_L = I_L(\mathbb{Z})$, so by Proposition 14.11, it is integrally closed in its fraction field L. Since $\mathbb{Z}$ is a PID and $L/\mathbb{Q}$ is finite separable, Theorem 18.1 applies to show that $\mathbb{Z}_L \cong \mathbb{Z}^n$ as a $\mathbb{Z}$-module. Being a finitely generated $\mathbb{Z}$-module, still more is it a finitely generated *algebra* over the Noetherian ring $\mathbb{Z}$, so it is itself Noetherian. Since $\mathbb{Z}$, like any PID, has Krull dimension one and $\mathbb{Z}_L$ is an integral extension of $\mathbb{Z}$, by Corollary 14.17 $\mathbb{Z}_L$ also has Krull dimension one. □

A **Dedekind domain** is a domain which is Noetherian, integrally closed and of Krull dimension at most one. We will systematically study Dedekind domains in §20, but for now observe that Corollary 18.2 implies that the ring of integers of an algebraic number field is a Dedekind domain. In fact, the argument establishes that the normalization S of any Dedekind domain R in a finite separable field extension L/K is again a Dedekind domain which is finitely generated as an R-module.

What about the nonseparable case?

Give Kaplansky's example. COMPLETE ME! ♣

[64]Note that we have not yet used the separability hypothesis, so this much is true in the case of an arbitrary finite extension.

18.2. **The Second Normalization Theorem.**

Theorem 18.3. *(Second Normalization Theorem) Let R be an integral domain with fraction field K. Suppose that at least one of the following holds:*
• *R is absolutely finitely generated – i.e., finitely generated as a $\mathbb{Z}$-algebra – or*
• *R contains a field k and is finitely generated as a k-algebra.*
Let L/K a finite field extension. Then $S = I_L(R)$ is a finitely generated R-module.

Proof. First suppose that R is a finitely generated algebra over a field k.
Step 0: We may assume that L/K is normal. Indeed, let M be the normal closure of L/K, so M/K is a finite normal extension. Let T be the integral closure of R in M. If we can show that T is finitely generated over R, then, since R is Noetherian, the finitely submodule S is also finitely generated over R.
Step 1: We will make use of the field-theoretic fact that if M/K is normal and L is the maximal purely inseparable subextension of M/K, then M/L is separable [FT, §6.3]. Let S be the integral closure of R in L and T the integral closure of R in T. Then T is module-finite over R iff T is module-finite over S and S is module-finite over R. Suppose we can show that S is module-finite over R. Then S is a finitely generated R-algebra so S is a Noetherian integreally closed domain, and the module finiteness of T over S follows from Theorem 18.1. Thus we are redueced to the case in which L/K is purely inseparable, say $[L : K] = q = p^a$.
Step 2: By Noether Normalization, R is module-finite over a polynomial ring $k[t_1, \ldots, t_d]$. If S is module-finite over $k[t_1, \ldots, t_d]$, then certainly it is module-finite over the larger ring R. Thus we may assume without loss of generality that $R = k[t_1, \ldots, t_d]$, $K = k(t_1, \ldots, t_d)$. In particular we may assume that R is integrally closed (in K). For all $a \in L$, $N_{L/K}(a) = a^q \in K$. Let k'/k be the extension obtained by adjoining the qth roots of the coefficients of the minimal polynomials of a finite set of generators of L/K, so k'/k is finite, so $L \subset k'(t_1^{1/q}, \ldots, t_d^{1/q})$. So it is enough to show that the integral closure of $k[t_1, \ldots, t_d]$ in $k'(t_1^{1/q}, \ldots, t_d^{1/q})$ is finite over $k[t_1, \ldots, t_d]$. But in this case the integral closure can be computed exactly: it is $k'[t_1^{1/q}, \ldots, t_d^{1/q}]$ (indeed it is at least this large, and this ring is a UFD, hence integrally closed), which is finite over $k[t_1, \ldots, t_d]$. □

18.3. **The Krull-Akizuki Theorem.**

In this section we come to one of the most beautiul and useful results in the subject, the Krull-Akizuki Theorem. Its content is essentially that normalization works magnificiently well in dimension one. Our treatment follows [M, §11].

Lemma 18.4. *For a Noetherian domain R, the following are equivalent:*
(i) R has dimension at most one.
(ii) For every nonzero ideal I of R, R/I is an Artinian ring.
(iii) For every nonzero ideal I of R, $\ell_R(R/I) < \infty$.

Proof. (i) $\implies$ (ii): R/I is Noetherian, and prime ideals of R/I correspond to prime ideals of R containing the nonzero ideal I, so are all maximal. By Theorem 8.34, R/I is Artinian.
(ii) $\implies$ (iii): Every finitely generated module over an Artinian ring is also Noetherian hence has finite length.

$\neg$ (i) $\implies$ $\neg$ (iii): If R has dimension greater than one, there is a nonzero, non-maximal prime ideal $\mathfrak{p}$ of R. The R-module $R/\mathfrak{p}$ is a domain which is not a field, hence not Artinian, hence of infinite length. □

Lemma 18.5. *Let R be a one-dimensional Noetherian domain with fraction ield K. Let M be a torsionfree R-module with $= \dim_K M \otimes_R K < \infty$. Then for all $x \in R^\bullet$, $\ell(M/xM) \leq r\ell(R/xR)$.*

Proof. Step 1: First suppose that M is finitely generated. Let $\eta_1, \ldots, \eta_r \in M$ be R-linearly independent and put $E = \langle \eta_1, \ldots, \eta_r \rangle_M$. Since $r = \dim_K M \otimes_R K$, for $\eta \in M$, there is $t \in R$ with $t\eta \in E$. Put $C = M/E$. Then C is finitely generated, so there is $t \in R^\bullet$ such that $tC = 0$. Applying Theorem 10.6 to C, there is a chain of submodules

$$0 = C_0 \subsetneq C_1 \subsetneq \ldots \subsetneq C_m = C \tag{38}$$

such that for all $0 \leq i \leq m-1$, $C_{i+1}/C_i \cong R/\mathfrak{p}_i$ for $\mathfrak{p}_i \in \operatorname{Spec} R$. Since $0 \neq t \in \mathfrak{p}_i$ for all i and $\dim R = 1$, each $\mathfrak{p}_i$ is maximal. It follows that (38) is a composition series for C, so $\ell(C) = m < \infty$. For $x \in R^\bullet$ and $n \in \mathbb{Z}^+$, the exact sequence

$$E/x^nE \longrightarrow M/x^nM \to C/x^nC$$

yields

$$\ell(M/x^nM) \leq \ell(E/x^nE) + \ell(C). \tag{39}$$

Since E and M are torsionfree, we have $x^iM/x^{i+1}M \cong M/xM$ for all $i \in \mathbb{N}$ and similarly $x^iE/x^{i+1}E \cong E/xE$; it follows that

$$n\ell(M/xM) \leq n\ell(E/xE) + \ell(C) \ \forall n \in \mathbb{Z}^+,$$

and thus

$$\ell(M/xM) \leq \ell(E/xE).$$

Since $E \cong R^r$, $E/xE \cong (R/xR)^r$, so

$$\ell(M/xM) \leq \ell((R/xR)^r) = r\ell(R/xR).$$

Step 2: In the general case, put $\overline{M} = M/xM$ and let $\overline{N} = \langle \overline{\omega_1}, \ldots, \overline{\omega_s} \rangle$ be a finitely generated submodule of $\overline{M}$. Lift each $\overline{\omega_i}$ to $\omega_i \in M$ and put $M_1 = \langle \omega_1, \ldots, \omega_s \rangle$. We get

$$\ell(\overline{N}) \leq \ell(M_1/M_1 \cap xM) \leq \ell(M_1/aM_1) \leq r\ell(R/xR),$$

the last inequality by Step 1. Because the right hand side of this inequality is independent of $\overline{N}$, by Exercise 8.13 $\ell(\overline{M}) \leq r\ell(R/xR)$.
Step 3: We have $\ell(R/xR) < \infty$ by Lemma 18.4. □

Theorem 18.6. *(Krull-Akizuki) Let R be a one-dimensional Noetherian domain with fraction field K, let L/K be a finite field extension of K, and let S be a ring with $R \subset S \subset L$. Then:*
a) S is Noetherian of dimension at most 1.
b) If J is a nonzero ideal of S, then S/J is a finite length R-module.

Proof. b) It is no loss of generality to replace L by the fraction field of S. Let $r = [L : K]$, so that S is a torsionfree R-module of rank r. By Lemma 18.5, for any

$x \in R^\bullet$ we have $\ell_R(S/aS) < \infty$. Let J be a nonzero ideal of S and $b \in J^\bullet$. Since b is algebraic over R it satisfies a relation

$$a_m b^m + \ldots + a_1 b + a_0 = 0,\ a_i \in R$$

of minimal degree. Since S is a domain, $a_0 \in (J \cap R)^\bullet$, so

$$\ell_R(S/J) \leq \ell_R(S/a_0 S) < \infty.$$

a) Since

$$\ell_S(J/a_0 S) \leq \ell_R(J/a_0 S) \leq \ell_R(S/a_0 S) < \infty,$$

$J/a_0 S$ is a finitely generated S-module. Being an extension of a finitely generated S-module by a finitely generated S-module, J is itself a finitely generated: S is Noetherian. If $\mathcal{P}$ is a nonzero prime ideal of S then $S/\mathcal{P}$ has finite length so is an Artinian domain, hence a field: S has dimension at most one. □

We remark that S need not be finitely generated as an R-module. Thus Step 2 in the proof of Lemma 18.5 is actually used in the proof of the Krull-Akizuki Theorem.

Corollary 18.7. *Let R be a one-dimensional Noetherian domain with fraction field K, let L/K be a finite field extension, and let S be the integral closure of R in L. Then S is a Dedekind ring, and for every maximal ideal $\mathfrak{p}$ of R there are only finitely many prime ideals of S lying over $\mathfrak{p}$.*

Exercise: Prove Corollary 18.7. (Hint: if a prime $\mathcal{P}$ of S lies over $\mathfrak{p}$, then $\mathfrak{p}S \subset \mathcal{P}$.)

19. The Picard Group and the Divisor Class Group

19.1. **Fractional ideals.**

Let R be an integral domain with fraction field K. A **fractional ideal** of R is a nonzero R-submodule I of K for which there exists $0 \neq a \in R$ such that $aI \subset R$ – or equivalently, if $I \subset \frac{1}{a}R$.

When one is talking about fractional R-ideals, one inevitably wants to compare them to ideals of R in the usual sense, and for this it is convenient to speak of an **integral R-ideal**, i.e., an R-submodule of R.

Exercise 19.1: Show: a finitely generated R-submodule of K is a fractional ideal.

Comment: Some references *define* a fractional R-ideal to be a finitely generated R-submodule of K, but this seems wrong because we certainly want every nonzero integral ideal of R to be a fractional ideal, but if R is not Noetherian then not every integral ideal will be finitely generated. (It is not such a big deal because most of these references are interested only in *invertible* fractional ideals – to be studied shortly – and one of the first things we will see is that an invertible fractional ideal is necessarily finitely generated as an R-module.)

We denote the set of all fractional ideals of R by $\mathrm{Frac}(R)$.

Theorem 19.1. *Let I, J, M be fractional ideals in a domain R.*
a) Then

$$I \cap J = \{x \in K \mid x \in I \text{ and } x \in J\},$$
$$I + J = \{x + y \mid x \in I,\ y \in J,$$

$$IJ = \{\sum_{i=1}^{n} x_i y_i, \mid x_i \in I,\ y_i \in J\},$$
$$(I : J) = \{x \in K \mid xJ \subset I\}$$

are all fractional ideals.
b) We may partially order $\mathrm{Frac}(R)$ *under inclusion. Then the greatest lower bound of* I *and* J *is* $I \cap J$ *and the least upper bound of* I *and* J *is* $I + J$.
c) If $I \subset J$, *then* $IM \subset JM$.
d) R *itself is a fractional ideal, and* $R \cdot I = R$. *Thus the fractional ideals form a commutative monoid under multiplication.*

Proof. a) It is immediate that $I \cap J$, $I + J$, IJ and $(I : J)$ are all R-submodules of K. It remains to be seen that they are nonzero and can be scaled to lie inside R. Suppose $I \subset \frac{1}{a}R$ and $J \subset \frac{1}{b}R$. Then:
$0 \subsetneq I \subset I + J \subset \frac{1}{ab}R$, so $I + J$ is a fractional ideal.
$0 \subsetneq IJ \subset I \cap J \subset \frac{1}{ab}R$, so IJ and $I \cap J$ are fractional ideals.
Since $I \cap R$ is a fractional ideal, there exists a nonzero $c \in R$ lying in I. Then for $y \in J$, $\frac{c}{b}y \in cR \subset I$, so $\frac{c}{b} \in (I : J)$. Similarly, if $0 \neq d \in J$, then $\frac{1}{ad}(I : J) \subset R$.
Parts b), c) and d) can be easily verified by the reader. □

Proposition 19.2. *All the above operations on fractional ideals commute with localization: that is, if* $S \subset R^\bullet$ *is a multiplicatively closed subset, then*

$$S^{-1}(I \cap J) = S^{-1}I \cap S^{-I}J,$$
$$S^{-1}(I + J) = S^{-1}I + S^{-1}J,$$
$$S^{-1}(IJ) = (S^{-1}I)(S^{-1}J),$$
$$S^{-1}(I : J) = (S^{-1}I : S^{-1}J).$$

Exercise 19.2: Prove Proposition 19.2.

A fractional ideal is **principal** if it is of the form xR for some $x = \frac{a}{b} \in K^\bullet$.

Proposition 19.3. *For a fractional ideal* I *of* R, *TFAE:*
(i) I *is principal.*
(ii) I *is monogenic as an* R*-module.*
(iii) $I \cong_R R$.

Proof. By definition a monogenic R-module M is one of the form Rx for some $x \in M$, so the equivalence of (i) and (ii) is immediate. Certainly R is monogenic as an R-module. Conversely, suppose $I = Rx$ for $x \in K^\times$. Then multiplication by x^{-1} gives an isomorphism to R. (Another way to look at it is that a module M over a domain R is isomorphic to R itself iff it is monogenic and torsionfree, and a principal fractional ideal has both of these properties.) □

If xR is a principal fractional ideal, so is $x^{-1}R$, and we have

$$(xR)(x^{-1}R) = R.$$

Thus, in $\mathrm{Frac}(R)$, every principal fractional ideal xR is a unit, with inverse $x^{-1}R$.

Let $\mathrm{Prin}(R)$ denote the set of all principal fractional ideals of the domain R.

Exercise 19.3: Show that $\mathrm{Prin}(R)$ is a subgroup of $\mathrm{Frac}(R)$, and we have a short

exact sequence $1 \to R^\times \to K^\times \to \mathrm{Prin}(R) \to 1$.

Exercise 19.4: Define the **ideal class monoid** $C(R) = \mathrm{Frac}(R)/\mathrm{Prin}(R)$.
a) Show that $C(R)$ is well-defined as a commutative monoid.
b) Show that $C(R)$ is trivial iff R is a PID.
c) Show that $C(\mathbb{Z}[\sqrt{-3}])$ is a finite commutative monoid which is not a group.

For a general domain, $C(R)$ need only be a commutative monoid. In the next section we "repair" this by defining the **Picard group** $\mathrm{Pic}(R)$.

19.2. **The Ideal Closure.**

For $I \in \mathrm{Frac}(R)$, put

$$I^* = (R : I) = \{x \in K \mid xI \subset R\}.$$

Exercise 19.5: Let R be a domain. Show that for any fractional R-ideal I, I^* is a fractional R-ideal. (Hint: if $R \subset I$, then $I^* \subset R$. Reduce the general case to this.)

The fractional ideal I^* is called[65] the **quasi-inverse** of I. As we shall see later in this section, if the ideal I has an inverse in the monoid $\mathrm{Frac}\, R$, then its inverse must be I^*: i.e. $II^* = R$. In general though all we get from the definition of I^* is the relation $II^* \subset R$. This observation motivates the following one.

Proposition 19.4. *Let R be a domain, and let $\mathcal{R} \subset K \times K$ given by $x\mathcal{R}y$ iff $xy \in R$. Let (Φ, Ψ) be the induced Galois connection from 2^K to itself. Then, for any fractional ideal I of R, $\Phi(I) = \Psi(I) = I^*$. In other words, $I \mapsto I^*$ is a self-dual antitone Galois connection on* $\mathrm{Frac}\, R$.

Exercise 19.6: Prove Proposition 19.4.

As usual, we denote the associated closure operator by $I \mapsto \overline{\overline{I}}$. Now the machinery of Galois connections gives us many facts for free that we would otherwise have to spend a little time deriving:

Corollary 19.5. *Let R be a domain and let $I, J \in \mathrm{Frac}\, R$.*
a) If $I \subset J$, then $J^* \subset I^*$.
b) We have $I^* \subset J^* \iff \overline{I} \supset \overline{J}$.
c) We have $\overline{\overline{I}} = \overline{I}$.
d) We have $(I \cap J)^* = I^* + J^*$ and $\overline{I \cap J} = \overline{I} \cap \overline{J}$.

Exercise 19.7: Prove Corollary 19.5.

Exercise 19.8: Give an example of $I, J \in \mathrm{Frac}\, R$ with $J^* \subset I^*$ but $I \not\subset J$.

Proposition 19.6. *For a domain R and $I \in \mathrm{Frac}\, R$, we have*

$$\overline{I} = \bigcap_{d \in K^\times \mid I \subset d^{-1}R} d^{-1}R.$$

[65] Unfortunately?

Proof.

$$\overline{I} = (I^*)^* = \{x \in K \mid xI^* \subset R\} = \{x \in K \mid \forall d \in K^\times, dI \subset R \implies xd \in R\}$$
$$= \bigcap_{d \in K^\times \mid I \subset d^{-1}R} d^{-1}R.$$

□

19.3. **Invertible fractional ideals and the Picard group.**

Like any monoid, $\mathrm{Frac}(R)$ has a group of units, i.e., the subset of invertible elements. Explicitly, a fractional ideal I is **invertible** if there exists another fractional ideal J such that $IJ = R$. We denote the group $\mathrm{Frac}(R)^\times$ of invertible fractional ideals by $\mathrm{Inv}(R)$.

Exercise 19.9: Let $I_1, \ldots, I_n$ be fractional ideals of R. Show that the product $I_1 \cdots I_n$ is invertible iff each I_i is invertible. (Note: this has nothing to do with fractional ideals, but is rather a fact about the units in a commutative monoid.)

It turns out that to every fractional ideal we can attach another fractional ideal I^* which will be the inverse of I iff I is invertible.

Lemma 19.7. *a) For a fractional ideal I, TFAE:*
(i) I is invertible.
(ii) $II^* = R$.
*b) (**To contain is to divide**) If $I \subset J$ are fractional ideals with J invertible, then*

$$I = J(I : J).$$

Proof. a) (i) $\implies$ (ii): As above, for any fractional ideal I we have $II^* \subset R$. Now suppose there exists some fractional ideal J such that $IJ = R$, then

$$J \subset (R : I) = I^*,$$

so

$$R = IJ \subset II^*.$$

(ii) $\implies$ (i) is obvious.
b) By definition of $(I : K)$ we have $J(I : J) \subset I$. Conversely, since $I \subset J$, $J^{-1}I \subset R$. Since $(J^{-1}I)J = I$, it follows that $J^{-1}I \subset (I : J)$ and thus $I \subset J(I : J)$. □

Proposition 19.8. *Let I be an invertible fractional ideal. Then I is a finitely generated projective rank one module.*

Proof. Step 1: We show that an invertible fractional ideal I is a finitely generated projective module. Since $II^* = R$, we may write $1 = \sum_{i=1}^n x_i y_i$ with $x_i \in I$ and $y_i \in I^*$. For $1 \leq i \leq n$, define $f_i \in \mathrm{Hom}(I, R)$ be $f_i(x) = xy_i$. Then for all $x \in I$,

$$x = \sum_i x x_i y_i = \sum_i x_i f_i(x).$$

By the Dual Basis Lemma, I is a projective R-module generated by $x_1, \ldots, x_n$.
Step 2: Recall that to show that I has rank one, we must show that for all $\mathfrak{p} \in \mathrm{Spec}\, R$, $I_\mathfrak{p}$ is free of rank one over $R_\mathfrak{p}$. But since projective implies locally free, we know that $I_\mathfrak{p}$ is a free $R_\mathfrak{p}$-module of some rank, and it is quite elementary to show that for any ring R and any ideal I, I cannot be free of rank greater than one over

R. Indeed, if so I would have two R-linearly independent elements x and y, which is absurd, since $yx + (-x)y = 0$. □

Conversely:

Proposition 19.9. *Let I be a nonzero fractional ideal of R which is, as an R-module, projective. Then I is invertible.*

Proof. We have the inclusion $\iota : II^* \subset R$ which we wish to show is an equality. This can be checked locally: i.e., it is enough to show that for all $\mathfrak{p} \in \operatorname{Spec} R$, $\iota_{\mathfrak{p}} : I_{\mathfrak{p}} I_{\mathfrak{p}}^* \to R_{\mathfrak{p}}$ is an isomorphism. By Proposition 19.2, it is equivalent to show that $I_{\mathfrak{p}}(I_{\mathfrak{p}})^* \to R_{\mathfrak{p}}$ is an isomorphism, but since I is projective, by Kaplansky's Theorem $I_{\mathfrak{p}}$ is free. As above, being a nonzero ideal, it is then necessarily free of rank one, i.e., a principal fractional ideal $xR_{\mathfrak{p}}$. It follows immediately that $(I_{\mathfrak{p}})^* = x^{-1}R_{\mathfrak{p}}$ and thus that the map is an isomorphism. □

To sum up:

Theorem 19.10. *Let I be a nonzero fractional ideal for a domain R. Then I is invertible iff it is projective, in which case it is necessarily projective of rank one.*

For any R-module M, the R-dual is defined to be $M^\vee = \operatorname{Hom}(M, R)$. There is a canonical R-bilinear map $T : M^\vee \times M \to R$ obtained by mapping $(f, x) \mapsto f(x)$. This induces an R-linear map $T : M^\vee \otimes_R M \to R$. Let us say that an R-module M is **invertible** if D is an isomorphism.

Proposition 19.11. *Consider the following conditions on an R-module M.*
(i) M is rank one projective.
(ii) M is invertible.
(iii) There exists an R-module N and an isomorphism $T : M \otimes_R N \cong R$.
Then (i) $\implies$ (ii) $\implies$ (iii) always, and (iii) $\implies$ (i) if M is finitely generated.

Proof. (i) $\implies$ (ii): We have a map $T : M^\vee \otimes M \to R$ so that it suffices to check locally that is an isomorphism, but M is locally free so this is easy.
(ii) $\implies$ (iii) is immediate.
(iii) $\implies$ (i): Since M is finitely generated, by Theorem 13.19 to show that M is projective it is enough to show that for all $\mathfrak{p} \in \operatorname{Spec} R$ $M_{\mathfrak{p}}$ is free of rank one. Thus we may as well assume that $(R, \mathfrak{m})$ is a local ring with residue field $R/\mathfrak{m} = k$. The base change of the isomorphism T to $R/\mathfrak{m}$ is an isomorphism (recall that tensor product commutes with base change)

$$T_k : M/\mathfrak{m}M \otimes_k N/\mathfrak{m}N \to k.$$

This shows that $\dim_k M/\mathfrak{m}M = \dim_k N/\mathfrak{m}N = 1$, so in particular $M/\mathfrak{m}M$ is monogenic as an $R/\mathfrak{m}$-module. By Nakayama's Lemma the lift to R of any generator x of $M/\mathfrak{m}M$ is a generator of M, so M is a monogenic R-module and is thus isomorphic to R/I for some ideal I. But indeed $I = \operatorname{ann}(M) \subset \operatorname{ann}(M \otimes_R N) = \operatorname{ann}(R) = 0$, so $M \cong R/(0) = R$ is free of rank one. □

Theorem 19.12. *(Cohen) Let R be a domain.*
a) The set of invertible ideals of R is an Oka family in the sense of § 4.5.
b) If every nonzero prime ideal of R is invertible, then every nonzero fractional ideal of R is invertible.

Proof. a) Let $I \subset J$ be ideals of R with J and $(I : J)$ invertible (this implies $I \neq 0$). By Lemma 19.7, $I = J(I : J)$ and thus, as the product of two invertible ideals, I is invertible. Since for any ideals I, J of R we have $(I : J) = (I : I + J)$, by taking $J = \langle I, x \rangle$ for any $x \in R$ we recover the Oka condition.
b) Seeking a contradiction, suppose I is a nonzero ideal of R which is not invertible. Consider the partially ordered set $\mathcal{S}$ of ideals containing I which are not invertible. Then the union of any chain in $\mathcal{S}$ is a non-invertible ideal: indeed, if it were invertible then by Proposition 19.8 it would be finitely generated and thus equal to some element in the chain: contradiction. Thus by Zorn's Lemma there is a nonzero ideal J which is maximal element in the family of ideals which are not invertible. By part a) and the Prime Ideal Principle, J is prime: contradiction. □

Theorem 19.13. *Let I and J be invertible fractional ideals. Then there is a canonical isomorphism of R-modules*

$$I \otimes_R J \xrightarrow{\sim} IJ.$$

Proof. The natural multiplication map $I \times J \to IJ$ is R-bilinear so factors through an R-module map $m : I \otimes_R J \to IJ$. Again, once we have a globally defined map, to see that it is an isomorphism it is enough to check it locally: for all $\mathfrak{p} \in \operatorname{Spec} R$,

$$m_{\mathfrak{p}} : I_{\mathfrak{p}} \otimes_{R_{\mathfrak{p}}} J_{\mathfrak{p}} \xrightarrow{\sim} I_{\mathfrak{p}} J_{\mathfrak{p}}$$

and we are thus allowed to assume that I and J are principal fractional ideals. This makes things very easy, and we leave the endgame to the reader. □

Corollary 19.14. *Let I and J be invertible fractional R-ideals. TFAE:*
(i) There exists $x \in K^\times$ such that $xI = J$.
(ii) $I \cong_R J$, i.e., I and J are isomorphic R-modules.

Proof. (i) $\implies$ (ii): If $J = xI$, then multiplication by x gives an R-module isomorphism from I to J.
(ii) $\implies$ (i): Since $I \cong_R J$ we have

$$I^{-1}J \cong I^{-1} \otimes_R J \cong I^{-1} \otimes_R I \cong II^{-1} = R.$$

By Proposition 19.3, $I^{-1}J$ is a principal fractional ideal, i.e., there exists $x \in K^\times$ such that $I^{-1}J = xR$. Multiplying through by I, we get $xI = J$. □

Proposition 19.15. *Let M be a rank one projective module over a domain R with fraction field K. Then there exists a fractional R-ideal I such that $M \cong_R I$.*

Proof. Since M is projective, it is flat, and so tensoring the injection $R \hookrightarrow K$ with M we get an injection $f : M = R \otimes_R M \hookrightarrow M \otimes_R K \cong K$, the last isomorphism since M is locally free of rank 1. Thus $f : M \xrightarrow{\sim} f(M)$, and $f(M)$ is a finitely generated R- submodule of K and thus a fractional R-ideal. □

Putting together all the pieces we get the following important result.

Theorem 19.16. *Let R be a domain. The following two commutative groups are canonically isomorphic:*
(i) $\operatorname{Inv}(R)/\operatorname{Prin}(R)$ with $[I][J] := [IJ]$.
(ii) Isomorphism classes of rank one projective R-modules under tensor product.
*We may therefore define the **Picard group** $\operatorname{Pic} R$ to be* either *the group of invertible fractional ideals modulo principal fractional ideals under multiplication or the group of isomorphism classes of rank one projective modules under tensor product.*

Lemma 19.17. *In any domain R, let $\mathcal{P}_1, \ldots, \mathcal{P}_k$ be a set of invertible prime ideals and let $\mathcal{Q}_1, \ldots, \mathcal{Q}_l$ be any set of prime ideals. Suppose that*

$$\prod_{i=1}^{k} \mathcal{P}_i = \prod_{j=1}^{l} \mathcal{Q}_j.$$

Then $i = j$ and there exists some permutation σ of the set $\{1, \ldots, k\}$ such that for all $1 \leq i \leq k$ we have $\mathcal{P}_i = \mathcal{Q}_{\sigma(i)}$.

In other words, prime factorization is unique for products of invertible primes.

Proof. Assume without loss of generality that $\mathcal{P}_1$ does not strictly contain any $\mathcal{P}_i$. Since $\prod_j \mathcal{Q}_j \subset \mathcal{P}_1$, some $\mathcal{Q}_j$, say $\mathcal{Q}_1$, is contained in $\mathcal{P}_1$. Similarly, since $\prod_i \mathcal{P}_i \subset \mathcal{Q}_1$, there exists i such that $\mathcal{P}_i \subset \mathcal{Q}_1$. Thus $\mathcal{P}_i \subset \mathcal{Q}_1 \subset \mathcal{P}_1$. By our assumption on the minimality of $\mathcal{P}_1$, we have $\mathcal{P}_1 = \mathcal{P}_i = \mathcal{Q}_1$. We can thus cancel $\mathcal{P}_1 = \mathcal{Q}_1$ and obtain the result by induction. □

Lemma 19.18. *Let R be an integrally closed Noetherian domain with fraction field K, and let I be a fractional R-ideal. Then $(I : I) := \{x \in K \mid xI \subset I\} = R$.*

Proof. Clearly $R \subset (I : I)$. Conversely, let $x \in (I : I)$. Then I is a faithful $R[x]$-module which is finitely generated over R, so x is integral over R. □

Lemma 19.19. *Let R be a domain with fraction field K, $S \subset R \setminus \{0\}$ a multiplicative subset, and I, J fractional R-ideals.*
a) We have $(I + J)_S = I_S + J_S$.
b) $(IJ)_S = I_S J_S$.
c) $(I \cap J)_S = I_S \cap J_S$.
d) If I is finitely generated, then $(I^*)_S = (I_S)^*$.

Proof. Parts a) and b) are immediate and are just recorded for future reference. For part c), we evidently have $(I \cap J)_S \subset I_S \cap J_S$. Conversely, let $x \in I_S \cap J_S$, so $x = \frac{i}{s_1} = \frac{j}{s_2}$ with $i \in I$, $j \in J$, $s_1, s_2 \in S$. Put $b = a_1 s_2 = a_2 s_1 \in I \cap J$; then $x = \frac{b}{s_1 s_2} \in (I \cap J)_S$, establishing part c). For part d), note first that $(I + J)^* = I^* \cap J^*$. Also if $0 \neq x \in K$, then $(Rx)_S = R_S x$. Hence if $I = Rx_1 + \ldots + Rx_n$, then $I_S = R_S x_1 + \ldots + R_S x_n$, so $(I_S)^* = \bigcap_{i=1}^n \frac{1}{x_i} R_S$. On the other hand, $I^* = \bigcap_{i=1}^n \frac{1}{x_i} R$, and thus part c) we have

$$(I^*)_S = \bigcap_{i=1}^{n} \frac{1}{x_i} R_S = (I_S)^*.$$

□

Lemma 19.20. *A nonzero ideal in a Noetherian domain contains a product of nonzero prime ideals.*

Proof. Assume not: let I be a nonzero ideal which is maximal with respect to the property of not containing a product of nonzero prime ideals. Then I is not prime: there exist $x_1,\ x_2 \in R \setminus I$ such that $x_1 x_2 \in I$. Now put, for $i = 1, 2$, $I_i := \langle I, x_i \rangle$, so that $I \subsetneq I_i$ and $I \supset I_1 I_2$. By maximality of I, $I_1 \supset \mathfrak{p}_1 \cdots \mathfrak{p}_\mathfrak{r}$ and $I_2 \supset \mathfrak{q}_1 \cdots \mathfrak{q}_s$ (with $\mathfrak{p}_i$, $\mathfrak{q}_j$ prime for all i, j), and then $I \supset \mathfrak{p}_1 \cdots \mathfrak{p}_\mathfrak{r} \mathfrak{q}_1 \supset \mathfrak{q}_\mathfrak{s}$, contradiction. □

Lemma 19.21. *(Jacobson) Let R be a Noetherian domain of Krull dimension at most one. Let I be a proper, nonzero ideal of R. Then $(R : I) \supsetneq R$.*

Proof. Let $0 \neq a \in I$, so $aR \subset I \subset R$. By Lemma 19.20, there are nonzero prime ideals $\mathfrak{p}_1, \ldots, \mathfrak{p}_m$ such that $aR \supset \mathfrak{p}_1 \cdots \mathfrak{p}_m$; we may assume m is minimal. Let $\mathfrak{m}$ be a maximal ideal containing I. Then $\mathfrak{m} \supset I \supset aR \supset \mathfrak{p}_1 \cdots \mathfrak{p}_m$; since nonzero prime ideals are maximal, this implies $\mathfrak{m} = \mathfrak{p}_i$ for some i, say for $i = 1$. If $m = 1$ then $I = aR$ so $(R : I) = a^{-1}R \supsetneq R$. Now suppose $m > 1$; by minimality of m, aR does *not* contain $\mathfrak{p}_2 \cdots \mathfrak{p}_m$ so we may choose $b \in \mathfrak{p}_2 \cdots \mathfrak{p}_m \setminus aR$. Put $c = a^{-1}b$. Then $c \notin R$ and $cI \subset c\mathfrak{m} = a^{-1}b\mathfrak{m} \subset a\mathfrak{m}\mathfrak{p}_2 \cdots \mathfrak{p}_m \subset a^{-1}(aR) = R$, so $c \in (R : I)$. □

The following result gives information about when a prime ideal is invertible.

Proposition 19.22. *Let R be a Noetherian domain, and $\mathfrak{p}$ a nonzero prime ideal of R. If $\mathfrak{p}$ is invertible, then it has height one and $R_{\mathfrak{p}}$ is a DVR.*

Proof. Since $\mathfrak{p}$ is invertible, $R_{\mathfrak{p}}$ is a Noetherian local domain with a principal maximal ideal $\mathfrak{p}R_{\mathfrak{p}}$. By Theorem 17.19, $R_{\mathfrak{p}}$ is a DVR, and thus $\mathfrak{p}$ has height one. □

19.4. **Divisorial ideals and the Divisor Class Group.**

For $I, J \in \mathrm{Frac}(R)$, we write $I \leq J$ if every principal fractional ideal Ra which is contained in I is also contained in J. This gives a preordering on $\mathrm{Frac}(R)$. Let R be the associated equivalence relation, i.e., $I \sim J$ if $I \leq J$ and $J \leq I$.

We write $D(R) = \mathrm{Frac}(R)/\sim$. Elements of $D(R)$ are called **divisors** on R. For a fractional ideal I, we denote its image in $D(R)$ by $\mathrm{div}(I)$, and for a principal fractional ideal aR, we write simply $\mathrm{div}(a)$. Such elements are called **principal divisors**. A fractional ideal I is **divisorial** if $\overline{I} = I$.

Exercise 19.10: Let R be a domain and I a fractional R-ideal.
a) Show that $\overline{I}$ is the unique divisorial ideal with $\mathrm{div}\,\overline{I} = \mathrm{div}\,I$.
c) Show that $\overline{I}$ is the smallest divisorial fractional ideal containing I.
c) Show that invertible fractional ideals are divisorial.

Exercise 19.11: If I is a divisorial fractional ideal and $x \in K^\bullet$, then Ix is a divisorial fractional ideal.

Exercise 19.12: Let $\{I_i\}$ be a family of divisorial fractional ideals such that $I = \bigcap_i I_i$ is nonzero. Then I is a divisorial fractional ideal.

Lemma 19.23. *Let $I, J \in \mathrm{Frac}\,R$.*
a) The following are equivalent:
(i) $I \leq J$.
(ii) $J^* \subset I^*$.
b) The following are equivalent:
(i) $I \sim J$.
(ii) $I^* = J^*$.
(iii) $\overline{I} = \overline{J}$.
(iv) $\mathrm{div}\,I = \mathrm{div}\,J$.

Exercise 19.13: Prove Lemma 19.23.

Proposition 19.24. *For $I, J, M \in \mathrm{Frac}\,R$: $\mathrm{div}\,I \leq \mathrm{div}\,J \implies \mathrm{div}\,IM \leq \mathrm{div}\,JM$.*

Proof. By hypothesis $\overline{J} \subset \overline{I}$; equivalently $(R:I) = I^* \subset J^* = (R:J)$. Then

$$(IM)^* = (R:IM) = ((R:I):M) \subset ((R:J):M) = [R:JM) = (JM)^*.$$

It follows that $\overline{JM} \subset \overline{IM}$, so $\operatorname{div} IM \leq \operatorname{div} JM$. □

Proposition 19.25. *Let R be a domain.*
a) For $\operatorname{div} I, \operatorname{div} J \in D(R)$, the operation $\operatorname{div} I + \operatorname{div} J = \operatorname{div} IJ$ is well-defined and endows $D(R)$ with the structure of a commutative monid.
b) $(D(R), +, <)$ is a lattice-ordered monoid.

Proof. We have

$$(R:IJ) = ((R:I):J) = (R:\overline{I}):J) = ((R:J):\overline{I})$$
$$= ((R:\overline{J}):\overline{I}) = (R:\overline{IJ}),$$

so $\operatorname{div} I + \operatorname{div} J = \operatorname{div} \overline{I} + \operatorname{div} \overline{J}$.
b) For $I, J, M \in \operatorname{Frac} R$ with $\operatorname{div} I \leq \operatorname{div} J$, by Proposition 19.24 and part a),

$$\operatorname{div} I + \operatorname{div} M = \operatorname{div} IM \leq \operatorname{div} JM = \operatorname{div} J + \operatorname{div} M,$$

and thus the partial ordering is compatible with the monoid structure. To show that we have a lattice, for any $I, J \in \operatorname{Frac} R$, we need to find the supremum and infimum of $\operatorname{div} I$ and $\operatorname{div} J$. We claim that in fact we have

$$\operatorname{div}(I \cap J) = \sup \operatorname{div} I, \operatorname{div} J$$
$$\operatorname{div}(I + J) = \inf \operatorname{div} I, \operatorname{div} J.$$

To see this we may assume I and J are divisorial. By Exercise 19.12, $I \cap J$ is divisorial, so it is clear that for any divisorial ideal M,

$$(\operatorname{div} I \leq M,\ \operatorname{div} J \leq M) \iff (M \subset I,\ M \subset J)$$
$$\iff (M \subset I \cap J) \iff \operatorname{div} I \cap J \leq \operatorname{div} M.$$

Next, note that since $I, J \subset I + J$, $\operatorname{div} I + J \leq \operatorname{div} I, \operatorname{div} J$, i.e., $\operatorname{div} I + J$ is a lower bound for $\{\operatorname{div} I, \operatorname{div} J\}$. Conversely, if $M \in \operatorname{Frac} R$ is such that $\operatorname{div} M \leq \operatorname{div} I,\ \operatorname{div} J$, then $I, J \subset \overline{M}$ so $I + J \subset \overline{M}$ and $\overline{I+J} \subset \overline{\overline{M}} = \overline{M}$ and $\operatorname{div} M = \operatorname{div} \overline{M} \leq \operatorname{div} \overline{I+J} = \operatorname{div} I + J$. □

Tournant Dangereux One may wonder why we work with divisors at all since every divisor is represented by a unique divisorial ideal. However, if I and J are divisorial fractional ideals, the product IJ *need not be divisorial*.

Proposition 19.26.
a) In $D(R)$ every nonempty set which is bounded above admits a least upper bound. Explicitly, if (I_i) is a nonempty family of fractional ideals which is bounded above, then $\sup_i(\operatorname{div} I_i) = \operatorname{div}(\bigcap_i \overline{I}_i)$.
b) In $D(R)$ every nonempty set which is bounded below admits a greatest lower bound. Explicitly, if (J_i) is a nonempty family of fractional ideals which is bounded below, then $\inf_i(\operatorname{div} J_i) = \operatorname{div}(\sum_i I_i)$.
c) $D(R)$ is a lattice.

Proof. Bourbaki, p. 477. **COMPLETE ME! ♣** □

Theorem 19.27. *For a domain R, the following are equivalent:*
(i) $D(R)$ is a group.
(ii) R is completely integrally closed.

Proof. (i) $\implies$ (ii): Let $x \in K^\times$. Suppose there is $d \in R^\bullet$ such that $dx^n \in R$ for all $n \in \mathbb{Z}^+$. Then $I = \langle R, a \rangle_R \in \operatorname{Frac} R$ and $aI \subset I$. Then

$$\operatorname{div} I \leq \operatorname{div} aI = \operatorname{div} a + \operatorname{div} I.$$

Since $D(R)$ is a group, $\operatorname{div} R = 0 \leq \operatorname{div} a$, and since aR and R are divisorial, $a \in R$.
(ii) $\implies$ (i): We'll show: for all divisorial fractional ideals I, $(II^*)^* = R^* = R$, hence $\operatorname{div} I + \operatorname{div} I^* = \operatorname{div} R = 0$. By Proposition 19.6, it's enough to show that II^* and R are contained in the same principal fractional ideals. Since $II^* \subset R$, any principal fractional ideal which contains R contains II^*. Thus, let $x \in K^\times$ be such that $II^* \subset xR$; we want to show $R \subset xR$, i.e., $x^{-1} \in R$. Suppose that for $y \in K^\times$ we have $I \subset yR$, so $y^{-1} \in I^*$ and thus $Iy^{-1} \subset xR$; equivalently, $x^{-1}I \subset yR$. Thus $x^{-1}I$ is contained in every principal fractional ideal containing I, so $x^{-1}I \subset \overline{I} = I$. It follows that $x^{-n}I \subset I$ for all $n \in \mathbb{Z}^+$. Let $w \in R^\bullet$ be such that $wI \subset R$. Then $dx^{-n}I \subset R$, and if $z \in I^\bullet$ then $(wz)x^{-n} \in R$ for all $n \in \mathbb{Z}^+$. Since $dc \in R^\bullet$ and R is completely integrally closed, by Theorem 14.38 $x^{-1} \in R$. □

Let $P(R)$ be the image in $D(R)$ of the principal fractional ideals. Then $P(R)$ is a subgroup of $D(R)$. Thus if R is completely integrally closed (e.g. Noetherian and integrally closed!) we may form the quotient

$$\operatorname{Cl} R = D(R)/P(R),$$

the **divisor class group** of R.

Exercise 19.14: Let R be a completely integrally closed domain. Show that there is a canonical injection

$$\operatorname{Pic} R \hookrightarrow \operatorname{Cl} R.$$

Theorem 19.28. *Let $R = \mathbb{C}[x, y, z]/(xy - z^2)$. Then R is a Noetherian integrally closed domain with $\operatorname{Pic} R = 0$ and $\operatorname{Cl} R \cong \mathbb{Z}/2\mathbb{Z}$.*

20. Dedekind domains

A **Dedekind domain** is an integral domain which is Noetherian, integrally closed, and of dimension at most one. A Dedekind domain has dimension zero iff it is a field. Although we endeavor for complete precision here (why not?), the reader should be warned that in many treatments the zero-dimensional case is ignored, when convenient, in statements of results.

20.1. Characterization in terms of invertibility of ideals.

Theorem 20.1. *For an integral domain R with fraction field K, the following are equivalent:*
(i) R is Dedekind: Noetherian, integrally closed of dimension at most one.
(ii) Every fractional R-ideal is invertible.
(iii) Every nonzero prime ideal of R is invertible.

Proof. (i) $\implies$ (ii): Let R be a Noetherian, integrally closed domain of dimension at most one, and let I be a fractional R-ideal. Then $II^* \subset R$ and hence also $II^*(II^*)^* \subset R$, so $I^*(II)^* \subset I^*$. It follows from Lemma 19.18 that $(II^*)^* \subset R$; moreover, since $II^* \subset R$, Lemma 19.21 implies $II^* = R$, i.e., I is invertible.
(ii) $\implies$ (i): Since invertible ideals are finitely generated, if every nonzero ideal is invertible, then R is Noetherian. Let $\mathfrak{p}$ be a nonzero, nonmaximal prime ideal

of R, so that there exists a maximal ideal $\mathfrak{m}$ which $0 \subsetneq \mathfrak{p} \subsetneq \mathfrak{m}$. By the mantra "to contain is to divide" for invertible fractional ideals, there exists some invertible integral ideal I such that $\mathfrak{p} = \mathfrak{m}I$. Suppose that $I \subset \mathfrak{p}$. Then $I = RI \supset \mathfrak{m}I = \mathfrak{p}$, so we would have $\mathfrak{p} = I$ and then $\mathfrak{m} = R$, contradiction. Then there exists $x \in \mathfrak{m} \setminus \mathfrak{p}$ and $y \in I \setminus \mathfrak{p}$ such that $xy \in \mathfrak{p}$, contradicting the primality of $\mathfrak{p}$.

Finally, we check that R is integrally closed: let $x = \frac{b}{c}$ be a nonzero element of K which is integral over R, so there exist $a_0, \ldots, a_{n-1} \in R$ such that

$$x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0 = 0.$$

Let M be the R-submodule of K generated by $1, x, \ldots, x^{n-1}$; since M is finitely generated, it is a fractional R-ideal. We have $M^2 = M$, and thus – since M is invertible – $M = R$. It follows that $x \in R$.
(ii) $\implies$ (iii) is immediate.
(iii) $\implies$ (ii) by Theorem 19.12. □

Recall that a ring R is **hereditary** if every ideal of R is a projective R-module.

Corollary 20.2. *A domain R is hereditary iff it is a Dedekind domain.*

Proof. By Theorem 20.1 a domain R is a Dedekind domain iff every fractional ideal of R is invertible, and clearly the latter condition holds iff every nonzero integral ideal of R is invertible. Moreover, by Theorem 19.10, a nonzero ideal of a ring is invertible iff it is projective as an R-module. □

20.2. **Ideal factorization in Dedekind domains.**

Here we will show that in a Dedekind domain every nonzero integral ideal factors uniquely into a product of primes and derive consequences for the group of invertible ideals and the Picard group. (The fact that factorization – unique or otherwise! – into products of primes implies invertibility of all fractional ideals – is more delicate and will be pursued later.)

Lemma 20.3. *Let I be an ideal in a ring R. If there exist J_1, J_2 ideals of R, each strictly containing I, such that $I = J_1 J_2$, then I is not prime.*

Proof. Choose, for $i = 1, 2$, $x_i \in J_i \setminus I$; then $x_1 x_2 \in I$, so I is not prime. □

Theorem 20.4. *Every proper integral ideal in a Dedekind domain has a unique factorization into a product of of prime ideals.*

Proof. After Lemma 19.17 it suffices to show that a nonzero proper integral ideal I in a Dedekind domain R factors into a product of primes. Suppose not, so the set of ideals which do not so factor is nonempty, and (as usual!) let I be a maximal element of this set. Then I is not prime, so in particular is not maximal: let $\mathfrak{p}$ be a maximal ideal strictly containing I, so $I = \mathfrak{p}J$. Then $J = \mathfrak{p}^{-1}I$ strictly contains I so factors into a product of primes, hence I does. □

If I is any nonzero integral ideal of I and $\mathfrak{p}$ is any nonzero prime ideal of a Dedekind domain R, then we may define $\mathrm{ord}_{\mathfrak{p}}(I)$ via the prime factorization

$$I = \prod_{\mathfrak{p}} \mathfrak{p}^{\mathrm{ord}_{\mathfrak{p}}(I)}.$$

The product extends formally over all primes, but as I is divisible by only finitely many primes, all but finitely many exponents are zero, so it is really a finite product.

Corollary 20.5. *Let R be a Dedekind domain.*
a) The monoid $\mathcal{M}(R)$ of nonzero integral ideals is a free commutative monoid on the set of nonzero prime ideals.
b) The fractional ideals form a free commutative group on the set of prime ideals:

$$\mathrm{Frac}(R) = \bigoplus_{0 \neq \mathfrak{p} \in \mathrm{Spec}\, R} \mathbb{Z}.$$

Proof. Part a) is simply the statement of unique factorization into prime elements in any commutative monoid. In the group $\mathcal{I}(R)$ of all fractional ideals, the subgroup G generated by the nonzero primes is a free commutative group on the primes: this just asserts that for primes $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ and integers $n_1, \ldots, n_r$, the equation $\mathfrak{p}_1^{n_1} \cdots \mathfrak{p}_r^{n_r} = R$ implies $n_1 = \ldots = n_r = 0$, which is easily seen – e.g. by localizing. Since any fractional ideal J is of the form $\frac{1}{x} I$ with I an integral ideal, decomposing I and (x) into their prime factorizations expresses J as a $\mathbb{Z}$-linear combination of prime ideals, so $\mathrm{Frac}(R) = G$. □

Corollary 20.5 allows us to extend the definition of $\mathrm{ord}_{\mathfrak{p}}$ to any fractional R-ideal.

Since for a Dedekind domain there is no distinction between invertible fractional ideals and all fractional ideals, the Picard group takes an especially simple form: it is the quotient of the free abelian group $\mathrm{Frac}(R)$ of all fractional ideals modulo the subgroup $\mathrm{Prin}(R) = K^\times / R^\times$ of principal fractional ideals. We therefore have a short exact sequence

$$0 \to \mathrm{Prin}(R) \to \mathrm{Frac}(R) \to \mathrm{Pic}(R) \to 0,$$

and also a slightly longer exact sequence

$$0 \to R^\times \to K^\times \to \mathrm{Frac}(R) \to \mathrm{Pic}(R) \to 0.$$

Theorem 20.6. *For a Dedekind domain R, the following are equivalent:*
(i) $\mathrm{Pic}(R) = 0$.
(ii) R is a PID.
(iii) R is a UFD.
(iv) The set of nonprincipal prime ideals is finite.

Proof. Evidently each fractional ideal is principal iff each integral ideal is principal: $(i) \equiv (ii)$. Since R has dimension at most one, (ii) $\iff$ (iii) by Proposition 16.1. Evidently (ii) $\implies$ (iv), so the interesting implication is that (iv) implies the other conditions. So assume that the set of (nonzero) nonprincipal prime ideals is nonempty but finite, and enumerate them: $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$. Let I be an integral ideal, and suppose that

$$I = \mathfrak{p}_1^{a_1} \cdots \mathfrak{p}_n^{a_n} \mathfrak{q}_1^{b_1} \cdots \mathfrak{q}_m^{b_m}.$$

(As usual, we allow zero exponents.) By the Chinese Remainder Theorem we may choose an $\alpha \in R$ such that $\mathrm{ord}_{\mathfrak{p}_i}(\alpha) = a_i$ for all i.[66] Now consider the fractional ideal $(\alpha^{-1})I$; it factors as

$$(\alpha^{-1})I = \mathfrak{q}_1^{b_1} \cdots \mathfrak{q}_m^{b_m} \mathfrak{r}_1^{c_1} \cdots \mathfrak{r}_l^{c_l},$$

[66]Note that we want equality, not just $\mathrm{ord}_{P_i}(\alpha) \geq a_i$, so you should definitely think about how to get this from CRT if you've never seen such an argument before.

where the $\mathfrak{r}_i$'s are some other prime ideals, i.e., disjoint from the $\mathfrak{p}_i$'s. But all of the (fractional) ideals in the factorization of $(\alpha^{-1})I$ are principal, so $(\alpha^{-1})I = (\beta)$ for some $\beta \in K^\times$ and then $I = (\alpha\beta)$ is principal! □

Exercise 20.1: a) Consider the ring

$$R_1 = \mathbb{Z}[\sqrt{-3}] = \mathbb{Z}[t]/(t^2+3).$$

Show that R_1 is a one-dimensional Noetherian domain with exactly one nonprincipal prime ideal, namely $\mathfrak{p}_2 = \langle 1+\sqrt{-3}, 1-\sqrt{-3}\rangle$.
b) For any $n \in \mathbb{Z}^+$, exhibit a ring R_n which is one-dimensional Noetherian and has exactly n nonprincipal prime ideals.

20.3. **Local characterization of Dedekind domains.**

Theorem 20.7. *Let R be an integral domain.*
a) If R is Dedekind and S is a multiplicative subset, then $S^{-1}R$ is Dedekind.
b) If R is a Dedekind domain and $0 \neq \mathfrak{p}$ is a prime ideal of R, then $R_\mathfrak{p}$ is a DVR.

Proof. The properties of being Noetherian, dimension at most one and integrally closed are all preserved under localization, so part a) is immediate. Similarly, if $0 \neq \mathfrak{p}$ is a prime ideal, then the localization $R_\mathfrak{p}$ is a local, one-dimensional integrally closed Noetherian domain, hence by Theorem 17.19 a DVR, establishing b). □

Exercise 20.2: Let R be Dedekind with fraction field K; let $0 \neq \mathfrak{p} \in \operatorname{Spec} R$.
a) Show that the map $\operatorname{ord}_\mathfrak{p} : K^\times \to \mathbb{Z}$ defined above is nothing else than the discrete valuation corresponding to the localization $R_\mathfrak{p}$.
b) Conversely, let $v : K^\times \to \mathbb{Z}$ be a discrete valuation. Show that the valuation ring $R_v = v^{-1}(\mathbb{N})$ is the localization of R at some maximal ideal $\mathfrak{p}$.

20.4. **Factorization into primes implies Dedekind.**

Theorem 20.8. *(Matusita* [Ma44]*) Let R be a domain with the property that every nonzero proper integral ideal is a product of prime ideals. Then R is Dedekind.*

Proof. Step 1: Let $\mathfrak{p}$ be an invertible prime of R. We show that $\mathfrak{p}$ is maximal. Let $a \in R \setminus \mathfrak{p}$, and suppose that $\langle a, \mathfrak{p}\rangle \subsetneq R$. Let us then write

$$I_1 := \langle a, \mathfrak{p}\rangle = \mathfrak{p}_1 \cdots \mathfrak{p}_m,$$
$$I_2 := \langle a^2, \mathfrak{p}\rangle = \mathfrak{q}_1 \cdots \mathfrak{q}_n,$$

where the $\mathfrak{p}_i$ and $\mathfrak{q}_j$ are prime ideals. By assumption, $I_1 \supsetneq \mathfrak{p}$, and, since $\mathfrak{p}$ is prime, we have also $I_2 \supsetneq \mathfrak{p}$. Therefore each $\mathfrak{p}_i$ and $\mathfrak{q}_j$ strictly contains $\mathfrak{p}$. In the quotient $\overline{R} = R/\mathfrak{p}$ we have

$$(\overline{a}) = a\overline{R} = \overline{\mathfrak{p}}_1 \cdots \overline{\mathfrak{p}}_m$$

and

$$(\overline{a^2}) = a^2\overline{R} = \overline{\mathfrak{q}}_1 \cdots \overline{\mathfrak{q}}_n.$$

The principal ideals $(\overline{a})$ and $(\overline{a^2})$ are invertible, and the $\overline{\mathfrak{p}}_i$ and $\overline{\mathfrak{q}}_j$ remain prime in the quotient. Therefore, we have

$$\overline{\mathfrak{q}}_1 \cdots \overline{\mathfrak{q}}_n = \overline{\mathfrak{p}}_1^2 \cdots \overline{\mathfrak{p}_m}^2.$$

Thus the multisets $\{\{\overline{\mathfrak{q}}_1, \ldots, \overline{\mathfrak{q}}_n\}$ and $\{\overline{\mathfrak{p}}_1,\ \overline{\mathfrak{p}}_1, \ldots, \overline{\mathfrak{p}}_m, \overline{\mathfrak{p}}_m\}\}$ coincide, and pulling back to R the same holds without the bars. Thus

$$I_1^2 = \langle a, \mathfrak{p}\rangle^2 = \mathfrak{p}_1^2 \cdots \mathfrak{p}_m^2 = \mathfrak{q}_1 \cdots \mathfrak{q}_n = \langle a^2, \mathfrak{p}\rangle,$$

so

$$\mathfrak{p} \subset \langle a, \mathfrak{p} \rangle^2 = a^2R + a\mathfrak{p} + \mathfrak{p}^2 \subset aR + \mathfrak{p}^2.$$

So if $p \in \mathfrak{p}$, $p = ax + y$ with $x \in R,\ y \in \mathfrak{p}^2$, so $ax \in \mathfrak{p}$, and since $a \in R \setminus \mathfrak{p}$, $x \in \mathfrak{p}$. Thus $\mathfrak{p} \subset a\mathfrak{p} + \mathfrak{p}^2 \subset \mathfrak{p}$, so $\mathfrak{p} = a\mathfrak{p} + \mathfrak{p}^2$. Multiplication by $\mathfrak{p}^{-1}$ gives $R = a + \mathfrak{p}$, contrary to hypothesis. So $\mathfrak{p}$ is maximal.

Step 2: Let $\mathfrak{p}$ be any nonzero prime ideal in R, and $0 \neq b \in \mathfrak{p}$. Then $\mathfrak{p} \supset bR$ and

$$bR = \mathfrak{p}_1 \cdots \mathfrak{p}_m,$$

with each $\mathfrak{p}_i$ invertible and prime. Thus by Step 1 the $\mathfrak{p}_i$'s are maximal. Since $\mathfrak{p}$ is prime we have $\mathfrak{p} \supset \mathfrak{p}_i$ for some i and then by maximality $\mathfrak{p} = \mathfrak{p}_i$, hence $\mathfrak{p}$ is invertible. Since by assumption every proper integral ideal is a product of primes, we conclude that every integral ideal is invertible, which, by Theorem 20.1 implies that R is Dedekind. □

Let $\mathfrak{a}$ and $\mathfrak{b}$ be ideals of a domain R. We say that $\mathfrak{b}$ **divides** $\mathfrak{a}$ if there is an ideal $\mathfrak{c}$ such that $\mathfrak{bc} = \mathfrak{a}$.

Exercise 20.3: Suppose $\mathfrak{a}, \mathfrak{b}$ are ideals of a domain R such that $\mathfrak{b}$ divides $\mathfrak{a}$.
a) Show that $\mathfrak{b} \supset \mathfrak{a}$.
b) Show that $\mathfrak{c} \subset (\mathfrak{a} : \mathfrak{b})$.
c) Can we have $\mathfrak{c} \subsetneq (\mathfrak{a} : \mathfrak{b})$?

Proposition 20.9. *For a Noetherian domain R, the following are equivalent:*
(i) R is a Dedekind domain.
(ii) ***To contain is to divide****: For all ideals $\mathfrak{a}$, $\mathfrak{b}$ of R, $\mathfrak{b} \supset \mathfrak{a} \iff \mathfrak{b}$ divides $\mathfrak{a}$.*

Proof. (i) $\implies$ (ii): The statement is trivial if $\mathfrak{b} = (0)$. Otherwise, $\mathfrak{b}$ is invertible so $\mathfrak{a} = \mathfrak{b}(\mathfrak{a} : \mathfrak{b})$ by Lemma 19.7.
(ii) $\implies$ (i): We claim that every proper nonzero ideal of R is a product of prime ideals. Since R is Noetherian, if this is not the case there is an ideal $\mathfrak{a}$ which is maximal with respect to not having this property. Let $\mathfrak{p}$ be a maximal ideal with $\mathfrak{a} \subset \mathfrak{p}$. By hypothesis, there is an ideal $\mathfrak{c}$ with $\mathfrak{a} = \mathfrak{p}_1\mathfrak{c}$. Then $\mathfrak{c} \supset \mathfrak{a}$. Suppose we had equality; then repeatedly substituting $\mathfrak{a} = \mathfrak{p}_1\mathfrak{a}$ gives $\mathfrak{a} = \mathfrak{p}_1^k\mathfrak{a}$ for all $k \in \mathbb{Z}^+$, and then by the Krull Intersection Theorem, $\mathfrak{a} \subset \bigcap_{k=1}^{\infty} \mathfrak{p}_1^k = (0)$, contradiction. So $\mathfrak{c}$ properly contains $\mathfrak{a}$, so we may write $\mathfrak{c} = \mathfrak{p}_2 \cdots \mathfrak{p}_r$ and thus $\mathfrak{a} = \mathfrak{p}_1\mathfrak{p}_2 \cdots \mathfrak{p}_r$: contradiction. □

Theorem 20.10. *For a domain R which is not a field, the following are equivalent:*
(i) R is Noetherian, integrally closed, and of Krull dimension one.
(ii) Every fractional (equivalently, every integral) R-ideal is invertible.
(iii) R is Noetherian, and the localization at every maximal ideal is a DVR.
(iv) Every nonzero proper integral ideal factors into a product of prime ideals.
(iv′) Every nonzero proper integral ideal factors uniquely *into a product of primes.*
(v) R is Noetherian, and to contain is to divide for all ideals of R.

20.5. **Generation of ideals in Dedekind domains.**

Theorem 20.11. *Let R be a Dedekind domain and I a nonzero ideal of R. Then the quotient ring R/I is a principal Artinian ring.*

Proof. Write $I = \prod_{i=1}^r \mathfrak{p}_i^{a_i}$. By the Chinese Remainder Theorem,

$$R/I \cong \prod_{i=1}^r R/\mathfrak{p}_i^{a_i}.$$

Each factor $R/\mathfrak{p}_i^{a_i}$ is also a quotient of the localized ring $R_{\mathfrak{p}}/\mathfrak{p}_i^{a_i}$, which shows that it is Artinian and principal. Finally, a finite product of Artinian (resp. principal ideal rings) remains Artinian (resp. a principal ideal ring). □

This has the following striking consequence:

Theorem 20.12. *(C.-H. Sah) For a domain R, the following are equivalent:*
(i) R is a Dedekind domain.
(ii) For any nonzero ideal I of R and any nonzero element $a \in I$, there exists $b \in I$ such that $I = \langle a, b \rangle$.

Proof. The direction (i) $\implies$ (ii) follows immediately from Theorem 20.11. Conversely, assume condition (ii) holds. By Theorem 20.10 it suffices to show that R is Noetherian and that its localization at each nonzero prime ideal $\mathfrak{p}$ is a DVR. Certainly condition (ii) implies Noetherianity; moreover it continues to hold for nonzero ideals in any localization. So let I be a nonzero ideal in the Noetherian local domain $(R_{\mathfrak{p}}, \mathfrak{p})$. It follows that there exists $b \in \mathfrak{p}$ such that $\mathfrak{p} = I\mathfrak{p} + bR_{\mathfrak{p}}$. By Nakayama's Lemma, $I = bR_{\mathfrak{p}}$, so $R_{\mathfrak{p}}$ is a local PID, hence a DVR. □

Proposition 20.13. *(*[J2, Ex. 10.2.11]*) Let R be a Dedekind domain, I a fractional ideal of R and J a nonzero integral ideal of R. Then there exists $a \in I$ such that $aI^{-1} + J = R$.*

Proof. Let $\mathfrak{p}_1, \ldots, \mathfrak{p}_s$ be the prime ideals of R dividing J. For each $1 \leq i \leq r$, choose $a_i \in I\mathfrak{p}_1 \cdots \mathfrak{p}_r \mathfrak{p}_i^{-1} \setminus I\mathfrak{p}_1 \cdots \mathfrak{p}_r$. Put $a = a_1 + \ldots + a_r$. We claim that $aI^{-1} + J = R$. It is enough to check this locally. For every prime $\mathfrak{q} \neq \mathfrak{p}_i$, we have $JR_{\mathfrak{q}} = R_{\mathfrak{q}}$. On the other hand, for all $1 \leq i \leq r$, aI^{-1} is not contained in $\mathfrak{p}_i$, so its pushforward to $R_{\mathfrak{p}_i}$ is all of $R_{\mathfrak{p}_i}$. □

20.6. **Finitely generated modules over a Dedekind domain.**

The aim of this section is to prove the following important result.

Theorem 20.14. *Let M be a finitely generated module over a Dedekind domain.*
a) $P = M/M[\mathrm{tors}]$ is a finitely generated projective R-module, say of rank r.
b) If $r = 0$ then of course $M = M[\mathrm{tors}]$. If $r \geq 1$ then

$$M \cong M[\mathrm{tors}] \oplus P \cong M[\mathrm{tors}] \oplus R^{r-1} \oplus I,$$

with I a nonzero ideal of R.
c) The class $[I]$ of I in $\operatorname{Pic} R$ is an invariant of M.
d) There exists $N \in \mathbb{Z}^+$, maximal ideals $\mathfrak{p}_i$ and positive integers n_i such that

$$M[\mathrm{tors}] \cong \bigoplus_{i=1}^N R/\mathfrak{p}_i^{n_i}.$$

Much of the content of the main theorem of this section lies in the following converse of Proposition 3.8b) for finitely generated modules over a Dedekind domain.

Theorem 20.15. *For a finitely generated module M over a Dedekind domain, the following are equivalent:*
(i) M is projective.
(ii) M is flat.
(iii) M is torsionfree.

Proof. Of course (i) $\implies$ (ii) $\implies$ (iii) for modules over any domain, and we have seen that (i) $\equiv$ (ii) for finitely generated modules over a Noetherian ring. So it suffices to show (iii) $\implies$ (i).

Suppose R is a Dedekind domain and M is a finitely generated nonzero torsionfree R-module. By Proposition 3.8c), we may assume that $M \subset R^n$ for some $n \geq 1$. We prove the result by induction on n. If $n = 1$, then M is nothing else than a nonzero ideal of R, hence invertible by Theorem 20.10 and thus a rank one projective module by Theorem 19.10. So we may assume that $n > 1$ and that every finitely generated torsionfree submodule of R^{n-1} is projective. Let $R^{n-1} \subset R^n$ be the span of the first $n-1$ standard basis elements. Let $\pi_n : R^n \to R$ be projection onto the nth factor, and consider the restriction of π_n to M:

$$0 \to M \cap R^{n-1} \to M \stackrel{\pi_n}{\to} \pi_n(M) \to 0.$$

Put $I = \pi_n(M)$. Then I is an ideal of R, hence projective, so the sequence splits:

$$M \to (M \cap R^{n-1}) \oplus I.$$

Now $M \cap R^{n-1}$ is a torsionfree, finitely generated (since M is finitely generated and R is Noetherian) submodule of R^{n-1}, hence is projective by induction. Certainly a direct sum of projective modules is projective, so we're done. □

The method of proof immediately yields the following important corollary:

Corollary 20.16. *Let P be a finitely generated rank r projective module over a Dedekind domain R. Then we have a direct sum decomposition $P \cong \bigoplus_{i=1}^r I_i$, where each I_i is a nonzero rank one projective R-module.*

Let M a finitely generated module over the Dedekind domain R. We have:

$$0 \to M[\text{tors}] \to M \to M/M[\text{tors}] \to 0.$$

Put $P := M/M[\text{tors}]$. Then P is finitely generated and torsionfree by Proposition 3.8a), hence projective (by Theorem 20.15), and the sequence splits:

$$M \cong M[\text{tors}] \oplus P.$$

Lemma 20.17. *$I_1, \ldots, I_n$ be fractional ideals in the Dedekind domain R. Then the R-modules $\bigoplus_{i=1}^n I_i$ and $R^{n-1} \oplus I_1 \cdots I_n$ are isomorphic.*

Proof. We will prove the result when $n = 2$. The general case follows by an easy induction argument left to the reader.
Choose $0 \neq a_1 \in I_1$. Applying Proposition 20.13 with $I = I_2$ and $J = a_1 I_1^{-1} \subset R$, that there exists $a_2 \in I_2$ such that $a_1 I_1^{-1} + a_2 I_2^{-1} = R$. That is there exist $b_i \in I_i^{-1}$ such that $a_1 b_1 + a_2 b_2 = 1$. The matrix

$$\begin{bmatrix} b_1 & -a_2 \\ b_2 & a_1 \end{bmatrix}$$

is invertible with inverse

$$A^{-1} = \begin{bmatrix} a_1 & a_2 \\ -b_2 & b_1 \end{bmatrix}.$$

For $(x_1, x_2) \in I_1 \oplus I_2$, we have

$$y_1 = x_1 b_1 + x_2 \in R,\ y_2 = -x_1 a_2 + x_2 a_1 \in I_1 I_2.$$

On the other hand, if $y_1 \in R$ and $y_2 = c_1 c_2 \in I_1 I_2$, then

$$x_1 = a_1 y_1 - b_2 c_1 c_2 \in I_1,\ x_2 = a_2 y_1 + b_1 c_1 c_2 \in I_2.$$

Thus $[x_1 x_2] \mapsto [x_1 x_2]A$ gives an R-module isomorphism from $I_1 \oplus I_2$ to $R \oplus I_1 I_2$. □

Thus we may write

$$M = M[\text{tors}] \oplus M/M[\text{tors}] \cong M[\text{tors}] \oplus \bigoplus_{i=1}^{r} I_i = M[\text{tors}] \oplus R^{r-1} \oplus (I_1 \cdots I_r),$$

which establishes Theorem 20.14a).

As for part b) of the theorem, let T be a finitely generated torsion R-module. Note that the statement of the classification is identical to that of finitely generated torsion modules over a PID. This is no accident, as we can easily reduce to the case of a PID – and indeed to that of a DVR, which we have already proven (Theorem 17.21). Namely, let I be the annihilator of T, and (assuming $T \neq 0$, as we certainly may) write $I = \prod_{i=1}^{r} \mathfrak{p}_i^{a_i}$. Then T is a module over $R/I \cong R/\prod_{i=1}^{r} \mathfrak{p}_i^{r_i} \cong \bigoplus_{i=1}^{r} R/\mathfrak{p}_i^{a_i}$. By Exercise X.X in §3.1, T naturally decomposes as $T = \bigoplus_{i=1}^{r} T_i$, where T_i is a module over $R/\mathfrak{p}_i^{a_i}$. This gives the primary decomposition of T. Moreover, each T_i is a module over the DVR $R_{\mathfrak{p}}$, so Theorem 17.21 applies.

Corollary 20.18. *For any Dedekind domain R, the Picard group* $\operatorname{Pic} R$ *is canonically isomorphic to the reduced K_0-group $\widetilde{K_0(R)}$.*

Proof. Let P be a finitely generated projective R-module of rank $r \geq 1$. According to Theorem 20.14c) the monoid of isomorphism classes of finitely generated projective R-modules is *cancellative*: this means that the canonical map $\varphi : \operatorname{Pic}(R) \to K_0(R)$ is injective. It follows easily that the composite map $\Phi : \operatorname{Pic}(R) \xrightarrow{\varphi} K_0(R) \to \widetilde{K_0(R)}$ is an injection: indeed, for $\varphi(I)$ to be killed in $\widetilde{K_0(R)}$ but not $K_0(R)$ it would have to be a fractional ideal which has rank zero as an R-module, and there are no such things. Now an arbitrary nonzero finitely generated projective R-module is isomorphic to $R^{r-1} \oplus I$, hence becomes equal to the class of the rank one module I in $\widetilde{K_0(R)}$, so Φ is surjective. To check that it is a homomorphism of groups we may look on a set of generators – namely, the classes of rank one projective modules. Let us use $[P]$ for the class of the projective module P in $K_0(R)$ and $[[P]]$ for its image in $\widetilde{K_0(R)}$. Then by Lemma 20.17 we have

$$\Phi([I_1 \otimes I_2]) = [[I_1 \otimes I_2]] = [[I_1 I_2]] = [[R \oplus I_1 I_2]] = [[I_1 \oplus I_2]] = [[I_1]] + [[I_2]]. \quad \square$$

20.7. **Injective Modules.**

Theorem 20.19. *For a domain R with fraction field K, TFAE:*
(i) R is Dedekind.
(ii) Every divisible R-module is injective.

Proof. (i) $\implies$ (ii): Let D be a divisible R-module. We will show D is injective using Baer's Criterion: let I be an ideal of R and $f : I \to D$ a module map. We may assume that I is nonzero and thus, since R is a Dedekind domain, invertible: if $I = \langle a_1, \ldots, a_n \rangle$, there are $b_1, \ldots, b_n \in K$ such that $b_i I \subset R$ for all i and

$1 = \sum_{i=1}^n a_i b_i$. Since D is divisible, there are $d_1, \ldots, d_n \in D$ with $f(a_i) = a_i d_i$ for all i. Then for $x \in I$,

$$f(x) = f(\sum_i b_i a_i x) = \sum (b_i x) f(a_i) = \sum_i (b_i x) a_i d_i = x \sum_i (b_i a_i) e_i.$$

Put $d = \sum_{i=1}^n (b_i a_i) d_i$. Thus $F : R \to D$ by $x \mapsto dx$ lifts f.
(ii) $\implies$ (i): Let I be injective. Then I is divisible and a quotient of a divisible module is divisible, so every quotient of I is divisible, and thus by assumption every quotient of I is injective. By Corollaries 3.55 and 20.2, R is Dedekind. □

As an application, we will prove a generalization to Dedekind domains of a nontrivial result in abelian group theory. Given an abelian group A, it is natural to ask when its torsion subgroup $A[\text{tors}]$ is a direct summand of A, so that A is the direct sum of a torsion group and a torsionfree group. It is easy to see that this happens when A is finitely generated, because then $A/A[\text{tors}]$ is a finitely generated torsionfree module over a PID, hence projective. The following exercise shows that some condition is necessary.

Exercise 20.4: Let $A = \prod_p \mathbb{Z}/p\mathbb{Z}$, where the product extends over all prime numbers. Show that $A[\text{tors}]$ is not a direct summand of A.

These considerations should serve to motivate the following result.

Theorem 20.20. *Let M be a module over a Dedekind domain R. If $M[\text{tors}] = M[r]$ for some $r \in R$, then $M[\text{tors}]$ is a direct summand of M.*

Proof. Step 1: We CLAIM that if A is a torsionfree R-module, then for every R-module N, $\text{Ext}^1_R(M, N)$ is divisible.
PROOF OF CLAIM Let $V = A \otimes_R K$. Since A is torsionfree, we have an exact sequence

$$0 \to A \to V \to V/A \to 0.$$

Applying the cofunctor $\text{Hom}(\cdot, B)$, a portion of the long exact Ext sequence is

$$\text{Ext}^1_R(V, B) \to \text{Ext}^1_R(A, B) \to \text{Ext}^2_R(V/A, B).$$

Since R is hereditary, by Proposition X.X, $\text{Ext}^2_R(A, B) = 0$ so $\text{Ext}^1_R(A, B)$ is a quotient of $\text{Ext}^1_R(V, B)$. Since V is a K-module, so is $\text{Ext}^1_R(V, B)$ and thus $\text{Ext}^1_R(V, B)$ and its quotient $\text{Ext}^1_R(A, B)$ is a divisible module, hence injective by Theorem 20.19.
Step 2: Let $T = M[\text{tors}] = M[r]$. We will show that the sequence

$$0 \to T \to M \to M/T \to 0$$

splits by computing $\text{Ext}^1_R(M/T, T) = 0$. Since M/T is torsionfree, by Step 1 $\text{Ext}^1_R(M/T, T)$ is divisible. On the other hand, since $T = T[r]$, $\text{Ext}^1_R(M/T, T) = \text{Ext}^1_R(M/T, T)[r]$. Thus multiplication by r on $\text{Ext}^1_R(M/T, T)$ is on the one hand surjective and on the other hand identically zero, so $\text{Ext}^1_R(M/T, T) = 0$. By Theorem 3.82 the sequence splits. □

21. Prüfer domains

A **Prüfer domain** is a domain in which each finitely generated ideal is invertible.[67]

Exercise 21.1: Show that every Bézout domain is a Prüfer domain.

21.1. Characterizations of Prüfer Domains.

One might be forgiven for thinking the invertibility of finitely generated ideals is a somewhat abstruse condition on a domain. The following result shows that, on the contrary, this determines a very natural class of domains.

Theorem 21.1. *(Characterization of Prüfer Domains) For a domain R, TFAE:*
(i) R is a Prüfer domain: every nonzero finitely generated ideal is invertible.
(i′) Every nonzero ideal of R generated by two elements is invertible.
(ii) Nonzero finitely generated ideals are cancellable: if $\mathfrak{a}, \mathfrak{b}, \mathfrak{c}$ are ideals of R and $\mathfrak{a}$ is finitely generated and nonzero, then $\mathfrak{ab} = \mathfrak{ac} \implies \mathfrak{b} = \mathfrak{c}$.
(iii) For every $\mathfrak{p} \in \operatorname{Spec} R$, $R_{\mathfrak{p}}$ is a valuation ring.
(iii′) For every $\mathfrak{m} \in \operatorname{MaxSpec} R$, $R_{\mathfrak{m}}$ is a valuation ring.
(v) For all ideals A, B, C of R, $A(B \cap C) = AB \cap AC$.
(vi) For all ideals A, B of R, $(A + B)(A \cap B) = AB$.
(vii) If A and C are ideals of R with C finitely generated and $A \subset C$, then there exists an ideal B of R such that $A = BC$.
(viii) For all ideals A, B, C of R with C finitely generated, we have

$$(A + B : C) = (A : C) + (B : C).$$

(ix) For all ideals A, B, C of R with C finitely generated, we have

$$(C : A \cap B) = (C : A) + (C : B).$$

(x) For all ideals A, B, C of R, $A \cap (B + C) = A \cap B + A \cap C$.

Proof. We will show: (i) $\iff$ (i′),
(i) $\iff$ (ii), (i) $\implies$ (iii) $\implies$ (iv) $\implies$ (v) $\implies$ (vi) $\implies$ (ii), (i) $\implies$ (vii) $\implies$ (iv), (iv) $\implies$ (viiii) $\implies$ (ii), (iv) $\implies$ (ix) $\implies$ (ii), and (iv) $\iff$ (x). This suffices!
(i) $\implies$ (i′) is immediate.
(i′) $\implies$ (i): We go by induction on the number of generators. A nonzero ideal with a single generator is principal, hence invertible. By assumption, every nonzero ideal generated by two elements is invertible. Hence we may assume that $n \geq 3$ and that every nonzero ideal of R generated by $n-1$ elements is invertible, and let $\mathfrak{c} = \langle c_1, \ldots, c_n \rangle$. We may assume $c_i \neq 0$ for all i. Put

$$\mathfrak{a} = \langle c_1, \ldots, c_{n-1} \rangle, \ \mathfrak{b} = \langle c_2, \ldots, c_n \rangle,$$
$$\mathfrak{d} = \langle c_1, c_n \rangle, \ \mathfrak{e} = c_1 \mathfrak{a}^{-1} \mathfrak{d}^{-1} + c_n \mathfrak{b}^{-1} \mathfrak{d}^{-1}.$$

Then

$$\begin{aligned} \mathfrak{ce} &= (\mathfrak{a} + \langle c_n \rangle) c_1 \mathfrak{a}^{-1} \mathfrak{d}^{-1} + (\langle c_1 \rangle + \mathfrak{b}) c_n \mathfrak{b}^{-1} \mathfrak{d}^{-1} \\ &= c_1 \mathfrak{d}^{-1} + c_1 c_n \mathfrak{a}^{-1} \mathfrak{d}^{-1} + c_1 c_n \mathfrak{b}^{-1} \mathfrak{d}^{-1} + c_n \mathfrak{d}^{-1} \\ &= c_1 \mathfrak{d}^{-1} (R + c_n \mathfrak{b}^{-1}) + c_n \mathfrak{d}^{-1} (R + c_1 \mathfrak{a}^{-1}). \end{aligned}$$

[67] Except for the zero ideal, of course.

Since $c_n\mathfrak{b}^{-1},\ c_1\mathfrak{a}^{-1} \subset R$, we get

$$\mathfrak{c}\mathfrak{e} = c_1\mathfrak{d}^{-1} + c_n\mathfrak{d}^{-1} = \langle c_1, c_n\rangle\mathfrak{d}^{-1} = R.$$

(iii) $\implies$ (iii′) is immediate. (iii′) $\implies$ (iii): if $\mathfrak{p} \in \operatorname{Spec} R$, let $\mathfrak{m}$ be a maximal ideal containing $\mathfrak{p}$. Then $R_{\mathfrak{p}}$ is an overring of $R_{\mathfrak{m}}$, and every overring of a valuation ring is a valuation ring.
(i) $\implies$ (ii) is immediate, since invertible ideals are cancellable.
(ii) $\implies$ (iii): First suppose that $\mathfrak{a}$ is a nonzero finitely generated ideal and $\mathfrak{b}, \mathfrak{c}$ are ideals of R with $\mathfrak{a}\mathfrak{b} \subset \mathfrak{a}\mathfrak{c}$. Then $\mathfrak{a}\mathfrak{c} = \mathfrak{a}\mathfrak{b} + \mathfrak{a}\mathfrak{c} = \mathfrak{a}(\mathfrak{b} + \mathfrak{c})$; cancelling $\mathfrak{a}$ gives $\mathfrak{c} = \mathfrak{b} + \mathfrak{c}$, so $\mathfrak{b} \subset \mathfrak{c}$. Now let $\mathfrak{p}$ be a prime ideal of R. By Exercise 17.6, it is enough to show that for any $\frac{a}{s}, \frac{b}{t} \in R_{\mathfrak{p}}$, we have either $(\frac{a}{s}) \subset (\frac{b}{t})$ or $(\frac{b}{t}) \subset (\frac{a}{s})$. Since $\frac{1}{s}, \frac{1}{t} \in R^\times$, it is equivalent to show that $(a) \subset (b)$ or $(b) \subset (a)$: for this we may clearly assume $a, b \neq 0$.

□

Theorem 21.2. *Let R be a domain.*
a) Suppose R is a GCD-domain. Then R is Prüfer iff it is Bézout.
b) A Prüfer UFD is a PID.

Proof. a) Since principal ideals are invertible, any Bézout domain is a Prüfer domain. Conversely, suppose R is a GCD-domain and a Prüfer domain. Let $x, y \in R^\bullet$ and let d be a GCD of x, y. Certainly we have $(d) \supset \langle x, y\rangle$. Thus $\iota : \langle x, y\rangle \hookrightarrow (d)$ is a homomorphism of R-modules which we want to show is an isomorphism. By the Local-Global Principle for Module Homomorphisms it is enough to show that for all $\mathfrak{p} \in \operatorname{Spec} R$, $\iota_{\mathfrak{p}}$ is an isomorphism of $R_{\mathfrak{p}}$-modules, i.e., $\langle x, y\rangle_{R_{\mathfrak{p}}} = \langle d\rangle_{\mathbb{R}_{\mathfrak{p}}}$. By Proposition 15.16, d is again the GCD of x and y in the valuation ring $R_{\mathfrak{p}}$ (equivalently, the valuation of d is the minimum of the valuations of x and y) so that the principal ideal $\langle x, y\rangle_{R_{\mathfrak{p}}}$ is generated by $\langle d\rangle_{R_{\mathfrak{p}}}$.
b) Suppose R is a Prüfer UFD. By part a) R is Bézout, and by Theorem 16.17 a Bézout UFD is a PID. □

Proposition 21.3. *For a Prüfer domain R, TFAE:*
(i) R is a Bézout domain.
(ii) $\operatorname{Pic}(R) = 0$.

Proof. In the Prüfer domain R, an ideal I is invertible iff it is finitely generated. So (i) and (ii) each assert that every finitely generated ideal is principal. □

Proposition 21.4. *A Prüfer domain is integrally closed.*

Proof. In Theorem 20.1 we showed that a domain in which all fractional R-ideals are invertible is integrally closed. In the proof we only used the invertbility of finitely generated fractional ideals, so the argument works in any Prüfer domain. □

Exercise 21.2: Prove Corollary 21.4 using the local nature of integral closure.

21.1.1. *A Chinese Remainder Theorem for Prüfer domains.*

Recall that we have a Chinese Remainder Theorem which is valid in any ring: Theorem 4.18. There is however another useful version of the Chinese Remainder Theorem which holds in a domain R iff R is a Prüfer domain.

Let R be a ring, let $I_1, \ldots, I_n$ be a finite sequence of ideals in R and let $x_1, \ldots, x_n$

be a finite sequence of elements in R. We may ask: when is there an element $x \in R$ such that $x \equiv x_i \pmod{I_i}$ for all i?

If we assume the ideals I_i are pairwise comaximal, then this holds in any ring by CRT (Theorem 4.18). But suppose we drop that condition. Then, if such an x exists, we have $x - x_i \in I_i$ for all i, hence for all i and j,

$$x_i - x_j = (x - x_j) - (x - x_i) \in I_i + I_j. \tag{40}$$

Thus we get a necessary condition (which, notice, is vacuous when the ideals are pairwise comaximal). Let us say that a ring has property **ECRT(n)** if for all ideals $I_1, \ldots, I_n$ and elements $x_1, \ldots, x_n$ satisfying (40), there exists $x \in R$ such that $x \equiv x_i \pmod{I_i}$ for all i. We say that R satisfies **ECRT** (Elementwise Chinese Remainder Theorem) if it satisfies ECRT(n) for all $n \in \mathbb{Z}^+$.

Exercise 21.3: Show that a PID satisfies property ECRT.

Lemma 21.5. *Any ring satisfies ECRT*(1) *and ECRT*(2).

Proof. ECRT(1) is trivial. As for ECRT(2): let I, J be ideals of R, let $x_1, x_2 \in R$, and suppose $x_1 - x_2 \in I + J$: there are $i \in I$, $j \in J$ such that $x_1 - x_2 = i + j$. Put $x = x_1 - i = x_2 + j$. Then $x \equiv x_1 \pmod{I}$ and $x \equiv x_2 \pmod{J}$. □

Theorem 21.6. *For a ring R, the following are equivalent:*
(i) ECRT holds in R.
(ii) ECRT(3) *holds in R.*
(iii) For all ideals A, B, C in R, $A + (B \cap C) = (A + B) \cap (A + C)$.
(iv) For all ideals A, B, C in R, $A \cap (B + C) = (A \cap B) + (A \cap C)$.

Proof. (i) $\implies$ (ii) is immediate.
(ii) $\implies$ (iii): The inclusion $A + (B \cap C) \subset (A + B) \cap (A + C)$ holds for ideals in any ring. Conversely, let $t \in (A + B) \cap (A + C)$. Then by ECRT(3) there is $x \in R$ satisfying all of the congruences

$$x \equiv 0 \pmod{A},$$
$$x \equiv t \pmod{B},$$
$$x \equiv t \pmod{C},$$

and thus $x \in A$, $x - t \in B \cap C$, so $t = x - (x - t) \in A + (B \cap C)$.
(iii) $\implies$ (iv): For A, B, C ideals of R, we we have

$$(A \cap B) + (A \cap C) = ((A \cap B) + A) \cap ((A \cap B) + C) = A \cap ((A \cap B) + C)$$

and

$$(A \cap B) + (A \cap C) = (A + (A \cap C)) \cap ((A \cap C) + B) = A \cap ((A \cap C) + B),$$

and thus

$$(A \cap B) + C = (A \cap C) + B.$$

It follows that

$$(A \cap B) + C = (A \cap B) + C + (A \cap C) + B = B + C$$

and thus

$$(A \cap B) + (A \cap C) = A \cap ((A \cap B) + C) = A \cap (B + C).$$

(iv) $\implies$ (iii): Assume (iv). Then for all ideals A, B, C of R,

$$(A+B)\cap(A+C) = (A+B)\cap A \ + \ (A+B)\cap C = A\cap(A+B) \ + \ C\cap(A+B)$$
$$= (A\cap A)+(A\cap B)+(A\cap C)+(B\cap C) = A+(A\cap B)+(A\cap C)+(B\cap C) = A+(B\cap C).$$

(iii) $\implies$ (i): We go by induction on n. Having established that ECRT(1) and ECRT(2) hold in any ring, we let $n \geq 2$, assume ECRT(n) and show ECRT($n+1$): let $x_1, \ldots, x_{n+1} \in R$ and $I_1, \ldots, I_{n+1}$ be ideals of R such that $x_i - x_j \in I_i + I_j$ for all $1 \leq i, j \leq n$. By ECRT(n), there is $y \in R$ with $y \equiv x_i \pmod{I}_i$ for $1 \leq i \leq n$. We CLAIM that $y - x_{n+1} \in I_{n+1} + \bigcap_{i=1}^n I_i$.

PROOF OF CLAIM: Since we have assumed (iii), we have by induction that

$$\mathfrak{a} + \bigcap_{i=1}^n \mathfrak{b}_i = \bigcap_{i=1}^n (\mathfrak{a} + \mathfrak{b}_i),$$

and in particular

$$I_{n+1} + \bigcap_{i=1}^n I_i = \bigcap_{i=1}^n (I_i + I_{n+1}).$$

Also, for all $1 \leq i \leq n$, we have

$$y - x_{n+1} = (y - x_i) + (x_i - x_{n+1}) \in I_i + I_i + I_{n+1} \in I_i + I_{n+1}$$

and thus indeed

$$y - x_{n+1} \in \bigcap_{i=1}^n (I_i + I_{n+1}) = I_{n+1} + \bigcap_{i=1}^n I_i.$$

Because of the claim and ECRT(2), there is $t \in R$ satisfying

$$t \equiv y \pmod{\bigcap_{i=1}^n I_i},$$

$$t \equiv x_{n+1} \pmod{I_{n+1}}.$$

Then for $1 \leq i \leq n$,

$$t - x_i = (t - y) + (y - x_i) \in I_i.$$

□

21.2. **Butts's Criterion for a Dedekind Domain.**

One of our first results on Dedekind domains was Theorem 20.4: in a Dedekind domain –defined as a Noetherian, integrally closed domain of dimension at most one – every nonzero ideal factors uniquely as a product of prime ideals. It was then natural to ask about the converse: if in a domain R every nonzero proper ideal is uniquely a product of prime ideals, must R be Dedekind? We proved a result of Matusita which is stronger than this: a domain in which every nonzero proper ideal is a product of prime ideals is necessarily a Dedekind domain: uniqueness of the product was not required.

In particular if all ideals factor into primes then all ideals factor uniquely into primes. Let's try to show this directly: suppose we have nonzero prime ideals $\mathfrak{p}_1, \ldots, \mathfrak{p}_r, \mathfrak{q}_1, \ldots, \mathfrak{q}_s$ in a domain such that

$$\mathfrak{p}_1 \cdots \mathfrak{p}_r = \mathfrak{q}_1 \cdots \mathfrak{q}_s.$$

Then $\mathfrak{p}_1 \supset \mathfrak{q}_1 \cdots \mathfrak{q}_s$, so by X.X, $\mathfrak{p}_1 \supset \mathfrak{q}_j$ for some j. It is natural to try to deduce $\mathfrak{p}_1 = \mathfrak{q}_j$ from this. This certainly holds if each $\mathfrak{q}_j$ is maximal, so we get the desired implication when R has dimension one. In general it seems that we have acquired nothing more than further respect for Matusita's Theorem, but the above idea will be used in the proof of the main result of this section.

The deduction $\mathfrak{p}_1 \supset \mathfrak{q}_j \implies \mathfrak{p}_1 = \mathfrak{q}_j$ also holds if $\mathfrak{p}_1 = (p)$ and $\mathfrak{q}_j = (q)$ are both principal: for principal ideals, to contain is to divide, so we get $q = xp$, and then because prime elements are irreducible elements we have $x \in R^\times$ so $\mathfrak{p}_1 = \mathfrak{q}_j$.

Neither of the above steps works in general. By Proposition X.X, a Noetherian domain in which to contain is to divide is necessarily a Dedekind domain. Generalizing irreducible elements to ideals we get the condition on a nonzero proper ideal $\mathfrak{a}$ that $\mathfrak{a} = \mathfrak{bc}$ implies $\mathfrak{b} = R$ or $\mathfrak{c} = R$. We cannot call such an $\mathfrak{a}$ "irreducible" since that is already taken for a condition involving intersections of ideals, so following H. Butts we call such an ideal **unfactorable**. An ideal $\mathfrak{a}$ is **factorable** if it is not unfactorable, i.e., if there are proper ideals $\mathfrak{b}$ and $\mathfrak{c}$ such that $\mathfrak{a} = \mathfrak{bc}$.

Example: Let R be a valuation ring with valuation group $\mathbb{Q}$ and maximal ideal $\mathfrak{m}$. Then $\mathfrak{m} = \mathfrak{m} \cdot \mathfrak{m}$. Thus it is possible for a nonzero prime (even maximal) ideal to be factorable. This also shows that it is possible for an ideal to be a product of prime ideals in more than one way.

As usual in factorization theory, the ascending chain condition makes things nicer.

Exercise 21.4: Let R be a Noetherian domain.
a) Show that every nonzero ideal of R is a (finite, of course) product of unfactorable ideals. (Products over sets of cardinality 0 and 1 are allowed.)
b) Show that a nonzero prime ideal of R is unfactorable.

A domain in which each nonzero nonunit factors uniquely into a product of irreducible elements is, by definition, a UFD. So it is natural to ask in which domains each nonzero proper ideal factors uniquely into a product of unfactorable ideals. A theorem of H. Butts gives the answer.

Theorem 21.7. *(Butts* [But64]*) Let R be a domain in which each nonzero proper ideal factors uniquely as a product of unfactorable ideals. Then R is Dedekind.*

Proof. Step 1: Unique factorization into unfactorables implies: for ideals $\mathfrak{a}, \mathfrak{b}$, if $\mathfrak{ac} = \mathfrak{bc}$ then $\mathfrak{a} = \mathfrak{b}$. By Theorem 21.1, R is Prüfer.
Step 2: We will show that every nonzero prime ideal of R is invertible and apply Theorem 20.1. So let $\mathfrak{p}$ be a nonzero prime ideal, and let $p \in \mathfrak{p}^\bullet$. Let $(p) = \mathfrak{u}_1 \cdots \mathfrak{u}_r$ be the unique factorization of p into unfactorable ideals. Since (p) is invertible, so is each $\mathfrak{u}_i$; by Proposition 19.8, each $\mathfrak{u}_i$ is finitely generated. Let $x \in R \setminus \mathfrak{u}_i$. Then $U_i = \mathfrak{u}_i + \langle x \rangle$ is a finitely generated ideal in a Prüfer domain, hence invertible, so by Lemma 19.7 $\mathfrak{u}_i = U_i(\mathfrak{u}_i : U_i)$. Since u_i is unfactorable, either $U_i = R$ or $(\mathfrak{u}_i : U_i) = R$. If $(\mathfrak{u}_i : U_i) = R$ then $\mathfrak{u}_i = U_i$, contradiction. So $U_i = R$. Thus $\mathfrak{u}_i$ is maximal. Since $\mathfrak{p} \supset \mathfrak{u}_1 \cdots \mathfrak{u}_r$, we have $\mathfrak{p} = \mathfrak{u}_i$ for some i, so $\mathfrak{p}$ is invertible. □

21.3. **Modules over a Prüfer domain.**

Recall that a module is **semihereditary** if every finitely generated submodule is projective and that a ring R is **semihereditary** if the module R is semihereditary: i.e., every finitely generated ideal of R is projective.

Proposition 21.8. *A domain R is a semihereditary iff it is a Prüfer domain.*

Exercise 21.5: Prove Proposition 21.8.

Lemma 21.9. *Let R be a domain, and let M be a finitely generated torsionfree R-module. Then M is a submodule of a finitely generated free module.*

Proof. Since M is torsionfree, $M \hookrightarrow M \otimes_R K$, and $\iota : M \otimes_R K \cong K^n$ for some $n \in \mathbb{N}$. Since M is finitely generated, there exists $x \in R^\bullet$ such that the image of xM in $M \otimes_R K$ is contained in R^n, and thus $\iota \circ (x\bullet) : M \hookrightarrow R^n$. □

Theorem 21.10. *For an integral domain R, TFAE:*
(i) Every torsionfree R-module is flat.
(ii) Every finitely generated torsionfree R-module is projective.
(iii) R is a Prüfer domain.

Proof. (i) $\implies$ (ii): Let M be a finitely generated torsionfree R-module. By assumption M is flat, and since R is a domain, by Corollary 13.20 M is projective.
(ii) $\implies$ (iii): Finitely generated ideals are assumed projective, hence invertible.
(iii) $\implies$ (i): Let R be a Prüfer domain and M a torsionfree R-module. Then $M = \varinjlim_i M_i$ is the direct limit of its finitely generated submodules, hence a direct limit of finitely generated torsionfree modules M_i. By Lemma 21.9, each M_i is a finitely generated submodule of a free R-module. By Theorems 21.8 and 3.62, each M_i is projective, hence flat. Thus M is a direct limit of flat modules, hence is itself a flat module by Corollary 3.85. □

22. One Dimensional Noetherian Domains

22.1. Finite Quotient Domains.

For an ideal I in a ring R, we put $|I| = \#R/I$ (a possibly infinite cardinal).

R is a **finite quotient ring** if or every nonzero ideal I, R/I is finite.

Exercise 22.1: Show that every finite ring and every field is a finite quotient ring.

Exercise 22.2: Let R be a ring such that $R/(a)$ is finite for all $a \in R^\bullet$. Show that R is a finite quotient ring.

Lemma 22.1. *Let $0 \leq I \subset J$ be ideals in a finite quotient ring. Then:*
a) $|J| \mid |I|$.
b) We have $I = J \iff |I| = |J|$.

Exercise 22.3: Prove it.

Proposition 22.2. *Let R be a finite quotient ring which is not a field. Then:*
a) R is Noetherian.
b) We have $\dim R \leq 1$.
c) The following are equivalent:
(i) R is a domain.

(ii) $\dim R = 1$.
d) The following are equivalent:
(i) R is finite.
(ii) $\dim R = 0$.

Proof. a) Since for any nonzero ideal I, R/I is finite, we can say even more: the length of a chain of ideals starting with I is at most the number of prime divisors (counted with multiplicity) of $|I|$.
b) If $\mathfrak{p}$ is a nonzero prime ideal of R, then $R/\mathfrak{p}$ is a finite domain, hence a field, so $\mathfrak{p}$ is maximal. Thus $\dim R \leq 1$.
c) If R is a domain, then – since it is not a field – $\dim R \geq 1$. Combining with part b) we get $\dim R = 1$. Inversely, if R is not a domain, then (0) is not prime, so for every prime ideal $\mathfrak{p}$ of R, $R/\mathfrak{p}$ is finite, hence $\mathfrak{p}$ is maximal: $\dim R = 0$.
d) Clearly if R is finite then it has dimension 0. Conversely, if $\dim R = 0$ then by part a) R is Artinian. By XXX we may reduce to the case in which R is Artinian local with nilpotent maximal ideal: suppose e is the least positive integer such that $\mathfrak{m}^e = 0$. Since R is not a field, $e > 1$ and thus $R/\mathfrak{m}$ is a finite field. Then for all $i \in \mathbb{N}$, $\mathfrak{m}^i/\mathfrak{m}^{i+1}$ is a finitely generated module over the finite field $R/\mathfrak{m}$, so it's finite. Thus $\#R = \#R/\mathfrak{m}\#\mathfrak{m}/\mathfrak{m}^2 \cdots \#\mathfrak{m}^{e-1}/\mathfrak{m}^e < \infty$. □

Theorem 22.3. *(Samuel* [Sa71]*) Let R be any Noetherian ring, and $n \in \mathbb{Z}^+$. Then the set of ideals I of R with $|I| = n$ is finite.*

Proof. Since the number of isomorphism classes of rings of cardinality n is finite, it is enough to fix any ring S of cardinality n and show that the set $\{\mathfrak{b}_i\}_{i \in I}$ of ideals of R such that $R/\mathfrak{b}_i \cong S$ is finite.

Putting $\mathfrak{b} = \bigcap_{i \in I} \mathfrak{b}_i$, we have a monomorphism of rings

$$B := R/\mathfrak{b} \hookrightarrow \prod_{i \in I} R/\mathfrak{b}_i \cong S^I. \tag{41}$$

Let $\mathfrak{m}_1, \ldots, \mathfrak{m}_r$ be the maximal ideals of the (finite, hence Artinian) ring S, and for each $1 \leq j \leq r$, let q_j be the cardinality of the finite field $S/\mathfrak{m}_j$. Then $\mathfrak{m}_1 \cdots \mathfrak{m}_r = \bigcap_{j=1}^r \mathfrak{m}_j$ is the Jacobson radical which coincides with the nilradical, hence there exists $s \in \mathbb{Z}^+$ such that $(\mathfrak{m}_1 \cdots \mathfrak{m}_r)^s = 0$. Let $P(t) \in \mathbb{Z}[t]$ be the polynomial

$$P(t) = \prod_{j=1}^r (t^{q_j} - t)^s.$$

Then for any $x \in S$ and any $1 \leq j \leq r$, $x^{q_j} - x \in \mathfrak{m}_j$, so $P(x) = 0$. It follows that for all $X = (x_i) \in S^I$, $P(X) = (P(x_i)) = 0$. From (41) it follows that $P(x) = 0$ for all $x \in B$. Since the nonzero polynomial P has only finitely many roots in any domain, for each prime ideal $\mathfrak{p}$ of B, we conclude that $B/\mathfrak{p}$ is finite. Thus B is Noetherian of Krull dimension 0 hence is Artinian. But by the structure theory for Artinian rings, any Artinian ring with finite residue fields is actually finite. That is, $R/\mathfrak{b}$ is finite, so by the correspondence theorem there are only finitely many ideals of R containing $\mathfrak{b}$. In particular I is finite. □

Proposition 22.4. *Let I and J be nonzero ideals of the finite quotient domain R.*
a) If I and J are comaximal – i.e., $I + J = R$ – then $|IJ| = |I||J|$.
b) If I is invertible, then $|IJ| = |I||J|$.

Proof. Part a) follows immediately from the Chinese Remainder Theorem. As for part b), we claim that the norm can be computed locally: for each $\mathfrak{p} \in \Sigma_R$, let $|I|_{\mathfrak{p}}$ be the norm of the ideal $IR_{\mathfrak{p}}$ in the local finite norm domain $R_{\mathfrak{p}}$. Then

$$|I| = \prod_{\mathfrak{p}} |I|_{\mathfrak{p}}. \tag{42}$$

To see this, let $I = \bigcap_{i=1}^n \mathfrak{q}_i$ be a primary decomposition of I, with $\mathfrak{p}_i = \mathrm{rad}(\mathfrak{q}_i)$. It follows that $\{\mathfrak{q}_1, \ldots, \mathfrak{q}_n\}$ is a finite set of pairwise comaximal ideals, so the Chinese Remainder Theorem applies to give

$$R/I \cong \prod_{i=1}^n R/\mathfrak{q}_i.$$

Since $R/\mathfrak{q}_i$ is a local ring with maximal ideal corresponding to $\mathfrak{p}_i$, it follows that $|\mathfrak{q}_i| = |\mathfrak{q}_i R_{\mathfrak{p}_i}|$, establishing the claim.
Using the claim reduces us to the local case, so that we may assume the ideal $I = (xR)$ is principal. In this case the short exact sequence of R-modules

$$0 \to \frac{xR}{xJ} \to \frac{R}{xJ} \to \frac{R}{(x)J} \to 0$$

together with the isomorphism

$$\frac{R}{J} \stackrel{\cdot x}{\to} \frac{xR}{xJ}$$

does the job. □

Theorem 22.5. *(Butts-Wade) For a finite quotient domain R, TFAE:*
(i) R is a Dedekind domain.
(ii) For all nonzero ideals $\mathfrak{a}, \mathfrak{b}$ of R, $|\mathfrak{ab}| = |\mathfrak{a}||\mathfrak{b}|$.

Proof. (i) $\implies$ (ii): Apply Theorem 20.1 and Proposition 22.4.
(ii) $\implies$ (i): Step 1: By 22.2, R is Noetherian. So if we can show that **to contain is to divide**, Theorem X.X applies to show that R is Dedekind. Let $\mathfrak{a} \subset \mathfrak{b}$ be ideals of R. The divisibility trivially holds if $\mathfrak{a} = (0)$, so we may assume that $\mathfrak{a} \neq (0)$.
Step 2: Suppose that we can show that if $\mathfrak{b} = \mathfrak{a} + \langle b \rangle$ we have

$$\mathfrak{a} = \mathfrak{b}(\mathfrak{a} : \mathfrak{b}).$$

Then the general case follows: since R is Noetherian we may write $\mathfrak{b} = \mathfrak{a} + \langle b_1, \ldots, b_n \rangle$. For $1 \leq i \leq n$ put $\mathfrak{b}_i = \mathfrak{a} + \langle b_1, \ldots, b_i \rangle$. By Step 3,

$$\mathfrak{a} = \mathfrak{b}_1(\mathfrak{a} : \mathfrak{b}_1), \mathfrak{b}_1 = \mathfrak{b}_2(\mathfrak{b}_1 : \mathfrak{b}_2), \ldots, \mathfrak{b} = \mathfrak{b}_{n-1}(\mathfrak{b} : \mathfrak{b}_{n-1}),$$

and thus

$$\mathfrak{a} = (\mathfrak{a} : \mathfrak{b}_1)(\mathfrak{b}_1 : \mathfrak{b}_2) \cdots (\mathfrak{b}_{n-1} : \mathfrak{b})\mathfrak{b}.$$

Step 3: So suppose $\mathfrak{b} = \mathfrak{a} + \langle b \rangle$. Certainly $\mathfrak{b}(\mathfrak{a} : \mathfrak{b}) \subset \mathfrak{a}$. Since $(\mathfrak{a} : \mathfrak{b}) \supset \mathfrak{a}$, $(\mathfrak{a} : \mathfrak{b})$ and hence also $\mathfrak{b}(\mathfrak{a} : \mathfrak{b})$ is not zero, so the above containment gives

$$|\mathfrak{a}| \mid |\mathfrak{b}(\mathfrak{a} : \mathfrak{b})| = |\mathfrak{b}||(\mathfrak{a} : \mathfrak{b})|.$$

Since $\mathfrak{a} \subset \mathfrak{b}$, $k = \frac{|\mathfrak{a}|}{|\mathfrak{b}|} \in \mathbb{Z}^+$ and

$$\frac{|\mathfrak{a}|}{|\mathfrak{b}|} \mid |(\mathfrak{a} : \mathfrak{b})|.$$

So if we can show $|(\mathfrak{a} : \mathfrak{b})| \leq k$, then $|\mathfrak{a}| = |\mathfrak{b}||(\mathfrak{a} : \mathfrak{b})| = |\mathfrak{b}(\mathfrak{a} : \mathfrak{b})|$, and by Lemma 22.1, $\mathfrak{b}(\mathfrak{a} : \mathfrak{b}) = \mathfrak{a}$. Let $\{x_i\}_{i=1}^k$ be a set of coset representatives for $\mathfrak{a}$ in $\mathfrak{b}$, and let

$\{y_j\}_{j=1}^n$ be a set of coset representatives for $(\mathfrak{a} : \mathfrak{b})$ in R. We will define an injection from the first set to the second, which suffices to complete the proof. For $1 \leq i \leq n$, $by_i \in \mathfrak{b}$, so there is a unique $1 \leq i \leq k$ such that $by_j \in \mathfrak{a} + x_i$, and we define

$$\Phi : \{y_j\}_{j=1}^n \to \{x_i\}_{i=1}^k,\ y_j \mapsto x_i.$$

(If $y \in R$ is such that $y + (\mathfrak{a} : \mathfrak{b}) = y_j + (\mathfrak{a} : \mathfrak{b})$, then $b(y - y_j) \in \mathfrak{b}(\mathfrak{a} : \mathfrak{b}) \subset \mathfrak{a}$, so $by + \mathfrak{a} = by_j + \mathfrak{a}$: that is, the mapping is well-defined on cosets, independent of the chosen representatives. But that is not necessary for the argument to go through.) We check the injectivity: if $1 \leq u, v \leq n$ are such that $by_u, by_v \in \mathfrak{a} + x_j$, then $b(y_u - y_v) \in \mathfrak{a}$ so $y_u - y_v \in ((b) : \mathfrak{a}) = ((b) + \mathfrak{a}, \mathfrak{a}) = (\mathfrak{b}, \mathfrak{a})$, so $u = v$. □

Exercise 22.4: Let R be a finite quotient domain. By Theorem 22.3, for all $n \in \mathbb{Z}^+$, there are only finitely many ideals I with $N(I) \leq n$. We can therefore define a formal Dirichlet series

$$\zeta_R(s) = \sum_{I \supsetneq \{0\}} N(I)^{-s},$$

the **Dedekind zeta function** of R.
a) Show that $\zeta_{\mathbb{Z}}(s) = \sum_n \frac{1}{n^s} = \prod_p \frac{1}{1-p^{-s}} = \prod_p \zeta_{\mathbb{Z}_{(p)}}(s)$, where the products extend over all prime numbers p.
b) Let $R = \mathbb{F}_p[t]$. Show that $\zeta_R(s) = \frac{1}{1-p^{1-s}}$.
c) Suppose R is a Dedekind domain. Show that

$$\zeta_R(s) = \prod_{\mathfrak{p} \in \operatorname{MaxSpec} R} \zeta_{R_{\mathfrak{p}}}(s).$$

Exercise 22.5: Let $R = Z[t]/(t^2 + 3)$ (or, equivalently, $\mathbb{Z}[\sqrt{-3}]$). Let $\mathfrak{q} = (2)$.
a) Show that there is a unique ideal $\mathfrak{p}_2$ with $R/\mathfrak{p}_2 = \mathbb{Z}/2\mathbb{Z}$. Evidently $\mathfrak{p}_2$ is maximal.
b) Show that $r(\mathfrak{q}) = \mathfrak{p}_2$, and deduce that I is primary.
c) Show that $\mathfrak{q}$ is not a prime power, and indeed, cannot be expressed as a product of prime ideals.[68]

23. Structure of overrings

23.1. **Introducing overrings.**

Let R be an integral domain with fraction field K. Let Σ_R be the set of height one prime ideals of R. By an **overring** of R we mean a subring of K containing R, i.e., a ring T with $R \subset T \subset K$. (We allow equality.) This is standard terminology among commutative algebraists, but we warn that someone who has not heard it before will probably guess incorrectly at its meaning: one might well think that "T is an overring of R" would simply mean that "R is a subring of T".

[68] Suggestion: show that R is a ring with finite quotients, and use properties of the norm function $||I|| = \#R/I$.

23.2. **Overrings of Dedekind domains.**

In this section we will carefully study overrings of a Dedekind domain R. In particular, we will answer the following questions.

Question 5. *Let R be a Dedekind domain.*
a) Can we (in some sense) classify the overrings of R?
b) Under what conditions is every overring of R a localization?
c) Let T be an overring of R. What is the relationship between $\operatorname{Pic} T$ *and* $\operatorname{Pic} R$*?*

(In point of fact we can *ask* these questions for any domain R. But for a Dedekind domain we will obtain definitive, useful answers.)

As a warmup, suppose R is a PID. In this case every overring is indeed a localization: to see this it is enough to show that for all coprime $x, y \in R^\bullet$, $\frac{1}{y} \in R[\frac{x}{y}]$. But since x and y are coprime in the PID R, there are $a, b \in R$ such that $ax + by = 1$, and then $\frac{1}{y} = \frac{ax+by}{y} = a\left(\frac{x}{y}\right) + b \in R[\frac{x}{y}]$.

It follows that every overring of a PID is obtained by localizing at a multiplicative subset $S \subset R^\bullet$. Further, by uniqueness of factorization the saturated multiplicatively closed subsets of $R^\bullet$ are in bijection with subsets of Σ_R: in other words, an overring is entirely determined by the set of prime elements we invert, and inverting different sets of prime elements leads to distinct overrings. Further, since a localization of a PID is a again a PID, in this case we have $\operatorname{Pic} T = 0$ for all overrings.

Some of the above analysis generalizes to arbitrary Dedekind domains: we will show that for any Dedekind domain R the overrings of R correspond bijectively to subsets of Σ_R. More precisely, for any subset $W \subset \Sigma_R$ we define

$$R_W = \bigcap_{\mathfrak{p} \in W} R_{\mathfrak{p}}$$

and also

$$R^W = \bigcap_{\mathfrak{p} \in \Sigma_R \setminus W} R_{\mathfrak{p}}.$$

(Note that $R^W = R_{\Sigma_R \setminus W}$. So it is logically unnecessary to consider both R_W and R^W, but it will be notationally convenient to do so.) When $W = \{\mathfrak{p}\}$ consists of a single element, we we write $R^{\mathfrak{p}}$ for $R^{\{\mathfrak{p}\}}$. Let $\Phi : \Sigma_R \to \operatorname{Pic} R$ be the ideal class map, i.e., $\mathfrak{p} \mapsto [\mathfrak{p}]$. Then we will show that every overring of a Dedekind domain R is of the form R^W for a unique subset $W \subset \Sigma_R$ and that $\operatorname{Pic} R^W \cong \operatorname{Pic} R / \langle \Phi(W) \rangle$.

On the other hand, it is not generally true that an arbitrary overring of R arsies as a localization. However, O. Goldman gave a beautiful analysis of the situation: it turns out that a Noetherian domain R has the property that every overring is a localization iff R is a Dedekind domain and $\operatorname{Pic} R$ is a torsion group.

23.2.1. *Structure of overrings.* Let R be a Dedekind domain with fraction field K.

Lemma 23.1. *a) For all $\mathfrak{p} \in \Sigma_R$, there exists $f_{\mathfrak{p}} \in R^{\mathfrak{p}} \setminus R$.*
b) The mapping from subsets of Σ_R to overrings of R given by $W \mapsto R^W$ is injective.

Proof. a) Choose $x \in K \setminus R_{\mathfrak{p}}$, and let S be the finite set of maximal ideals $\mathfrak{q}$ distinct from $\mathfrak{p}$ such that $\operatorname{ord}_{\mathfrak{q}}(x) < 0$. For each $\mathfrak{q} \in S$, let $y_{\mathfrak{q}} \in \mathfrak{q} \setminus \mathfrak{p}$. Let

$N = \max_{\mathfrak{q} \in S} - \mathrm{ord}_{\mathfrak{q}}(x)$, and put $f_{\mathfrak{p}} = (\prod_{\mathfrak{q} \in S} y_{\mathfrak{q}})^N x$.
b) Suppose W_1 and W_2 are distinct subsets of Σ_R. After relabelling if necessary, we may assume that there exists $\mathfrak{p} \in W_2 \setminus W_1$. By part a), there exists $f_{\mathfrak{p}} \in R^{\mathfrak{p}} \setminus R$ and thus $f_{\mathfrak{p}} \in R^{W_1} \setminus R^{W_2}$. □

Proposition 23.2. *Let R be a Dedekind domain with fraction field K, and let T be an overring of R. Write $\iota : R \hookrightarrow T$ for the inclusion map.*
a) For every $\mathcal{P} \in \Sigma_T$, $T = R_{\mathcal{P} \cap R}$.
b) T is itself a Dedekind domain.
c) $\iota^* : \Sigma_T \hookrightarrow \Sigma_R$ is an injection.
d) For all $\mathcal{P} \in \Sigma_T$, $\iota_* \iota^* \mathcal{P} = \mathcal{P}$.
e) ι^* identifies Σ_T with the subset of $\mathfrak{p} \in \Sigma_R$ such that $\mathfrak{p}T \subsetneq T$.

Proof. a) Put $\mathfrak{p} = \mathcal{P} \cap R$. There exist $x, y \in R^\bullet$ such that $\frac{x}{y} \in \mathcal{P}$. Then $0 \neq x = y(\frac{x}{y}) \in \mathfrak{p}$, so $\mathfrak{p}$ is a nonzero prime ideal of R. Thus $T_{\mathfrak{P}}$ contains the DVR $R_{\mathfrak{p}}$ and is properly contained in its fraction field, so $T_{\mathcal{P}} = R_{\mathfrak{p}}$.
b) By the Krull-Akizuki Theorem, T is a Noetherian domain of Krull dimension one. By part a), the localization of T at every prime is a DVR. So T is integrally closed and is thus a Dedekind domain.
c) For distinct $\mathcal{P}_1, \mathcal{P}_2 \in \Sigma_T$, the localizations $T_{\mathcal{P}_1}$, $T_{\mathcal{P}_2}$ are distinct DVRs. But by part a), putting $\mathfrak{p}_i = \iota^*(\mathcal{P}_i)$, we have $R_{\mathfrak{p}_i} = T_{\mathcal{P}_i}$ for $i = 1, 2$, so $\mathfrak{p}_1 \neq \mathfrak{p}_2$.
d) Suppose $\mathfrak{p} = \iota^*(\mathcal{P})$. Then

$$(\iota_* \iota * \mathcal{P}) T_{\mathcal{P}} = \mathfrak{p} T_{\mathcal{P}} = \mathcal{P} T_{\mathcal{P}}.$$

By part c), $\iota * \iota^* \mathcal{P}$ is not divisible by any prime other than $\mathcal{P}$, so $\iota_* \mathfrak{p} = \mathcal{P}$.
e) This follows immediately and is stated separately for later use. □

Theorem 23.3. *For any overrring T of the Dedekind domain R, we have*

$$T = R_{\iota^*(\Sigma_T)}.$$

The proof (that I know) of this theorem requires the study overrings of more general Prüfer domains, to which we turn in the next section.

23.2.2. *When overrings are localizations.*

Lemma 23.4. *Let R be an integrally closed domain with fraction field K, and let T be an overring of R.*
a) The relative unit group $T^\times / R^\times$ is torsionfree.
b) Suppose that R is a Dedekind domain, $\mathfrak{p} \in \Sigma_R$ and $T = R^{\mathfrak{p}}$. TFAE:
(i) $T^\times / R^\times \cong \mathbb{Z}$.
(ii) $T^\times \supsetneq R^\times$.
(iii) $[\mathfrak{p}] \in \mathrm{Pic}(R)[\mathrm{tors}]$.
(iv) There exists $x \in R$ which is contained in $\mathfrak{p}$ and in no maximal ideal $\mathfrak{q} \neq \mathfrak{p}$.

Proof. a) Since R is integrally closed, all finite order elements of $K^\times$ (i.e., roots of unity in K) lie in R and *a fortiori* in T: $R^\times[\mathrm{tors}] = T^\times[\mathrm{tors}]$. On the other hand, let $x \in T^\times$ be of infinite order such that $x^n \in R^\times$ for some $n \in \mathbb{Z}^+$. Again integral closure of R implies $x \in R$, and then $x^n \in R^\times \implies x \in R^\times$.
b) (i) $\implies$ (ii) is clear.
(ii) $\implies$ (iii): Let $x \in K^\times$. Then $x \in T^\times$ iff $Rx = \mathfrak{p}^a$ for some $a \in \mathbb{Z}$, and $x \in R^\times$ iff $a = 0$. Therefore (ii) holds iff some power of $\mathfrak{p}$ is principal, which is to say that the class of $\mathfrak{p} \in \mathrm{Pic}\, R$ is torsion.

(iii) $\implies$ (i): Let a be the least positive integer such that $\mathfrak{p}^a$ is principal. Thus $\mathfrak{p}^a = xR$ with x uniquely determined modulo $R^\times$. It follows that $T^\times$ is generated by $R^\times$ and x, so $T^\times/R^\times$ is a nontrivial cyclic group. By part a) it is also torsionfree so $T^\times/R^\times \cong \mathbb{Z}$.
(iii) $\implies$ (iv): If $\mathfrak{p}^a = xR$, then x lies in $\mathfrak{p}$ but in no other maximal ideal $\mathfrak{q}$.
(iv) $\implies$ (iii): If $a = v_\mathfrak{p}(x)$, then $a > 0$ and $xR = \mathfrak{p}^a$. □

Remark: Part (iv) of Lemma 23.4 was added following an observation of H. Knaf.

Theorem 23.5. *(Goldman* [Gol64]*) For a Dedekind domain R, TFAE:*
(i) $\operatorname{Pic} R$ *is a torsion group.*
(ii) Every overring of R is a localization.

Proof. (i) $\implies$ (ii): Let $\mathfrak{p} \in \Sigma_R$. By Lemma 23.1 $R^\mathfrak{p}$ is a proper overring of R, so by assumption $R^\mathfrak{p}$ is a localization of R and thus has a strictly larger unit group. By Lemma 23.4 this implies that $[\mathfrak{p}] \in \operatorname{Pic}(R)[\text{tors}]$. Since $\operatorname{Pic}(R)$ is generated by the classes of the nonzero prime ideals, it follows that $\operatorname{Pic} R$ is torsion.
(ii) $\implies$ (i): Let T be an overring of R, and put $S = R \cap T^\times$. We want to show that $T = S^{-1}R$. That $S^{-1}R \subset T$ is clear. Conversely, let $x \in T$, and write $xR = \mathfrak{a}\mathfrak{b}^{-1}$ with $\mathfrak{a}, \mathfrak{b}$ coprime integral ideals of R: $\mathfrak{a} + \mathfrak{b} = R$. Thus $\mathfrak{a}T + \mathfrak{b}T = T$ whereas $\mathfrak{a}T = x\mathfrak{b}T \subset \mathfrak{b}T$, so $\mathfrak{b}T = T$ and hence also $\mathfrak{b}^n T = T$ for all $n \in \mathbb{Z}^+$. Since $\operatorname{Pic} R$ is torsion, there exists $n \in \mathbb{Z}^+$ with $\mathfrak{b}^n = bR$. It follows that $bT = T$ and thus $b \in S$. Now $x\mathfrak{b} = \mathfrak{a} \subset R$, so $xb \in R$. Thus $x \in S^{-1}R$, and we conclude $T \subset S^{-1}R$. □

Corollary 23.6. *Suppose that W is a finite subset of Σ_R and that every $\mathfrak{p} \in W$ hsa finite order in* $\operatorname{Pic} R$*. Then there is $a \in R^\bullet$ such that $R^W = R[\frac{1}{a}]$.*

Exercise 23.1: Prove Corollary 23.6.

Exercise 23.2: Let $T = R^W$ be an overring of R such that $T = R[\frac{1}{a}]$ for some $a \in R^\bullet$.
s) Show that W is finite.
b) Must it be the case that every $\mathfrak{p} \in W$ has finite order in $\operatorname{Pic} R$?

23.2.3. *The Picard group of an overring.*

Theorem 23.7. *Let R be a Dedekind domain, $W \subset \Sigma_R$, let $R^W = \bigcap_{\mathfrak{p} \in \Sigma_R \setminus W} R_\mathfrak{p}$, and let $\operatorname{Frac}_W R = \bigoplus_{\mathfrak{p} \in W} \mathbb{Z}$ denote the subgroup of fractional R-ideals supported on W. There is a short exact sequence*

$$1 \to R^\times \to (R^W)^\times \xrightarrow{v} \operatorname{Frac}_W R \to \operatorname{Pic} R \xrightarrow{\iota_*} \operatorname{Pic} R^W \to 1.$$

Proof. The map $v : (R^W)^\times \to \operatorname{Frac}_W R$ is obtained by restricting the canonical map $K^\times \to \operatorname{Frac} R$ to $(R^W)^\times$: the fractional ideals so obtained have $\mathfrak{p}$-adic valuation 0 for all $\mathfrak{p} \in \operatorname{MaxSpec} R^W = \operatorname{MaxSpec} R \setminus W$: thus the image lands in $\operatorname{Frac}_W R$.
It is easy to see most of the exactness claims: certainly $R^\times \to (R^W)^\times$ is injective; further, for $x \in (R^W)^\times$, $v(x) = 0$ iff $v_\mathfrak{p}(x) = 0$ for all $\mathfrak{p} \in W \cup \operatorname{MaxSpec} R^W = \operatorname{MaxSpec} R$ iff $x \in R^\times$. If $I \in \operatorname{Frac}_W R$, then I is principal iff it has a generator $x \in K^\times$ with $v_\mathfrak{p}(x) = 0 \forall \mathfrak{p} \in \operatorname{MaxSpec} R \setminus W = \operatorname{MaxSpec} R^W$ iff $I = (x)$ for $x \in (R^W)^\times$. Exactness at $\operatorname{Pic} R$: Let $[I] \in \operatorname{Pic} R$ be such that $\iota_*([I]) = 1$: thus there is $x \in K^\times$ with $IR^W = xR^W$. Then $[I] = [x^{-1}I]$ and $x^{-1}I \in \operatorname{Frac}_W R$. Conversely, if $I \in \operatorname{Frac}_W R$, then $IR^W = R^W$. Finally, by Proposition 23.2 $\iota_* \circ \iota^* = 1_{\Sigma(S)}$, so every prime ideal of R^W is of the form $\iota_*(\mathfrak{p})$ for a prime ideal of R. This certainly implies that $\iota_* : \iota_* : \operatorname{Pic} R \to \operatorname{Pic} R^W$ is surjective. □

Exercise 23.3: We maintain the setup of Theorem 23.7.
a) Use Theorem 23.7 to give a new proof of Lemma 23.4.
a) Show that the relative unit group $(R^W)^\times/R^\times$ is free abelian. (This strengthens Lemma 23.4 when R is a Dedekind domain.)
b) Suppose $\operatorname{Pic} R$ is torsion. Show:

$$(R^W)^\times \cong R^\times \oplus \bigoplus_{\mathfrak{p} \in W} \mathbb{Z}.$$

c) Deduce the Hasse-Chevalley S-Unit Theorem from the Dirichlet Unit Theorem.
d) Suppose that K is a number field. Show that $K^\times$ is isomorphic to the product of a finite cyclic group with a free abelian group of countable rank.

23.2.4. *Repleteness in Dedekind domains.*

Let R be a Dedekind domain, and consider the map $\Phi : \Sigma_R \to \operatorname{Pic} R$ given by $\mathfrak{p} \mapsto [\mathfrak{p}]$. We say that R is **replete** if Φ is surjective, i.e., if every element of $\operatorname{Pic} R$ is of the form $[\mathfrak{p}]$ for some *prime* ideal $\mathfrak{p}$.

Example: Let R be an S-integer ring in a global field. It follows immediately from the **Chebotarev Density Theorem** that R is replete.

For our coming applications it is useful to consider a variant: we say that a Dedekind domain R is **weakly replete** if for every subgroup $H \subset \operatorname{Pic} R$, there is a subset $W_H \subset \Sigma_R$ such that $\langle \Phi(W_H) \rangle = H$. The point of this condition is that it allows a complete classification of the Picard groups of overrings of R. Indeed:

Proposition 23.8. *Let R be a weakly replete Dedekind domain. Then for any subgroup H of $\operatorname{Pic} R$, there is an overring T of R such that $\operatorname{Pic} T \cong (\operatorname{Pic} R)/H$.*

Proof. By definition of weakly replete, there exists a subset $W \subset \Sigma_R$ such that $\langle \Phi(W) \rangle = H$. By Theorem 23.7, $\operatorname{Pic} R^W \cong \operatorname{Pic} R/\langle \Phi(W) \rangle \cong (\operatorname{Pic} R)/H$. □

Proposition 23.9. *Let R be a Dedekind domain and R^W an overring of R.*
a) If R is replete, so is R^W.
b) If R is weakly replete, so is R^W.

Exercise 23.4: Prove Proposition 23.9.

A **repletion** of a Dedekind domain R is a replete Dedekind domain S together with an injective ring homomorphism $\iota : R \hookrightarrow S$, such that $\iota_* : \operatorname{Pic}(R) \xrightarrow{\sim} \operatorname{Pic}(S)$.

Theorem 23.10. *(Claborn) For a Dedekind domain R, let R^1 denote the localization of $R[t]$ at the multiplicative set generated by all monic polynomials. Then R^1 is Dedekind and the composite map $\iota : R \to R[t] \to R^1$ is a repletion.*

Proof. **COMPLETE ME!** □

Exercise 23.5: Use Proposition 23.8 and Theorem 23.10 to show: if for every cardinal κ, there is a Dedekind domain R with Picard group a free abelian group of rank κ, then for every commutative group G there is a Dedekind domain R with $\operatorname{Pic} R \cong G$.

23.3. **Elasticity in Replete Dedekind Domains.**

Let R be a domain and $x \in R^\bullet \setminus R^\times$. If for $n \in \mathbb{Z}^+$ there are (not necessarily distinct) irreducible elements $\alpha_1, \ldots, \alpha_n$ of R such that $x = \alpha_1 \cdots \alpha_n$, we say that x admits an irreducible factorization of **length** n.

A **half factorial domain** (or **HFD**) is an atomic domain in which for all $x \in R^\bullet \setminus R^\times$, any two irreducible factorizations of x have the same length.

Exercise 23.6: (Zaks) Show that $\mathbb{Z}[\sqrt{-3}]$ is a HFD which is not integrally closed.

For R an atomic domain and $x \in R^\bullet \setminus R^\times$, let $L(x)$ be the supremum of all lengths of irreducible factorizations of x and let $\ell(x)$ be the minimum of all lengths of irreducible factorizations of x. We define the **elasticity of x**, $\rho(x)$, as the ratio $\frac{L(x)}{\ell(x)}$. We also make the convention that for $x \in R^\times$, $\rho(x) = 1$. Finally we define the **elasticity of R** as $\rho(R) = \sup_{x \in R^\bullet} \rho(x)$.

An atomic domain is a HFD iff $\rho(R) = 1$. Thus $\rho(R)$ is a quantitative measure of how far an atomic domain is from being a HFD.

Let $(G, \cdot)$ be a commutative group. A finite sequence $g_1, \ldots, g_n$ of elements in G is **irreducible** if for all nonempty proper subsets $S \subset \{1, \ldots, n\}$, $\prod_{i \in S} g_i \neq 1$.

Lemma 23.11. *Let $(G, \cdot)$ be a commutative group, let $x_1, \ldots, x_n$ be an irreducible sequence in G, and let $x_{n+1} = \left(\prod_{i=1}^n x_i\right)^{-1}$. If $x_{n+1} \neq 1$, then $x_1, \ldots, x_n, x_{n+1}$ is an irreducible sequence.*

Proof. A nontrivial proper subsequence of $x_1, \ldots, x_{n+1}$ with trivial product must be of the form $x_{i_1}, \ldots, x_{i_k}, x_{n+1}$ for some nonempty proper subset $S = \{i_1, \ldots, i_k\}$ of $\{1, \ldots, n\}$. Put $S' = \{1, \ldots, n\} \setminus S$. Then $\prod_{i \in S'} x_i^{-1} = 1$, hence also $\prod_{i \in S'} x_i = 1$, contradicting the irreducibility of $x_1, \ldots, x_n$. □

Proposition 23.12. *Let R be a Dedekind domain, let $x \in R^\bullet \setminus R^\times$, and let*

$$(x) = \prod_{i=1}^r \mathfrak{p}_i$$

be the factorization of x into prime ideals.
a) (Carlitz-Valenza) The following are equivalent:
(i) For no nonempty proper subset $S \subset \{1, \ldots, r\}$ is $\prod_{i \in S} \mathfrak{p}_i$ is principal.
(ii) The element x is irreducible.
b) If $\mathfrak{p}$ is a prime ideal such that $\mathfrak{p}^r = (x)$ and $\mathfrak{p}^s$ is nonprincipal for all $1 \leq s < r$, then x is irreducible.
c) If no $\mathfrak{p}_i$ is principal, the length of any irreducible factorization of x is at most $\frac{r}{2}$.

Exercise 23.7: Prove Proposition 23.12.

For a commutative group $(G, \cdot)$ the **Davenport constant** $D(G)$ of G is the maximum length of an irreducible sequence in G, or ∞ if the lengths of irreducible sequences in G are unbounded.

Proposition 23.13. *Let R be a Dedekind domain, and let $x \in R^\bullet$ be irreducible. Write $(x) = \mathfrak{p}_1 \cdots \mathfrak{p}_r$. Then $r \leq D(\operatorname{Pic} R)$.*

Proof. By Proposition 23.12a), $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ is an irreducible sequence in $\operatorname{Pic} R$. □

Proposition 23.14.
a) If H is a subgroup of a commutative group G, then $D(H) \leq D(G)$.
b) If H is a quotient of a commutative group G, then $D(H) \leq D(G)$.
c) $D(G) \geq \exp G = \sup_{x \in G} \#\langle x \rangle$.
d) If G is infinite, $D(G) = \infty$.
e) If G is finite, then $D(G) \leq \#G$.
f) If G is finite cyclic, then $D(G) = \#G$.
g) We have

$$D(\bigoplus_{i=1}^r \mathbb{Z}/n_i\mathbb{Z}) \geq 1 + \sum_{i=1}^r (n_i - 1). \tag{43}$$

h) We have $D(G) = 1 \iff \#G = 1$ and $D(G) = 2 \iff \#G = 2$.

Proof. a) If H is a subgroup of G, then any irreducible sequence in H is an irreducible sequence in G.
b) If $q : G \to H$ is a surjective homomorphism and $x_1, \ldots, x_n$ is irreducible in H, then choosing any lift $\tilde{x_i}$ of x_i to G yields an irreducible sequence $\tilde{x}_1, \ldots, \tilde{x}_n$.
c) If $x \in G$ and $n \in \mathbb{Z}^+$ is less than or equal to the order of x, then $x, x, \ldots, x$ (n times) is an irreducible sequence in G of length n.
d) By part c), we may assume G is infinite and of finite exponent. Then for some prime p, $G[p]$ is infinite, and by part a) it suffices to show that $D(G[p]) = \infty$. But $G[p]$ is an infinite-dimensional vector space over the field $\mathbb{F}_p$: let $\{e_i\}_{i=1}^\infty$ be an infinite $\mathbb{F}_p$-linearly independent subset of $G[p]$. Then for all $n \in \mathbb{Z}^+$ the sequence $e_1, \ldots, e_n$ is irreducible.
e) Suppose $\#G = n$, and let $g_1, \ldots, g_{n+1}$ be a sequence in G. For $1 \leq i \leq n$, let $P_i = g_1 \cdots g_i$. By the Pigeonhole Principle there is $1 \leq i < j \leq n+1$ such that $P_i = P_j$, and thus $g_{i+1} \cdots g_j = 1$.
f) Since $\exp \mathbb{Z}/n\mathbb{Z} = \#\mathbb{Z}/n\mathbb{Z} = n$, this follows from parts c) and e).
g) Let $G = \bigoplus_{i=1}^r \mathbb{Z}/n_i\mathbb{Z}$,[69] and let $d(G) = 1 + \sum_{i=1}^k (n_i - 1)$. There is an "obvious" irreducible sequence $x_1, \ldots, x_{d(G)-1}$: for $1 \leq i \leq k$, let e_i be the element of G with ith coordinate 1 and other coordinates 0. Take $e_1, \ldots, e_1$ ($n_1 - 1$ times), $e_2, \ldots, e_2$ ($n_2 - 1$ times),....,$e_k, \ldots, e_k$ ($n_k - 1$ times). The sum of these elements is $(n_1 - 1, \ldots, n_k - 1) \neq 0$, so by Lemma 23.11 taking $x_{d(G)} = -\sum_{i=1}^{d(G)-1} x_i$, we get an irreducible sequence of length $d(G)$.
h) Left to the reader as an easy exercise in applying some of the above parts. □

Theorem 23.15. *Let R be a Dedekind domain.*
a) We have $\rho(R) \leq \max(\frac{D(\operatorname{Pic} R)}{2}, 1)$.
b) If R is replete, then $\rho(R) = \max(\frac{D(\operatorname{Pic} R)}{2}, 1)$.

Proof. For $x \in R^\bullet \setminus R^\times$, let $P(x)$ be the number of prime ideals (with multiplicity) in the factorization of (x).
Step 0: Of course if $\operatorname{Pic} R$ is trivial then $D(\operatorname{Pic} R) = 1$, $\rho(R) = 1$ and the result holds in this case. Henceforth we assume $\operatorname{Pic} R$ is nontrivial and thus $D(\operatorname{Pic} R) \geq 2$,

[69] Here we are considering G as an additive group.

and our task is to show that $\rho(R) \leq \frac{D(\operatorname{Pic} R)}{2}$, with equality if R is replete.
Step 1: Let $x \in R^\bullet \setminus R^\times$. Consider two irreducible factorizations

$$x = \alpha_1 \cdots \alpha_m = \beta_1 \cdots \beta_n$$

of x with $m \geq n$. Let k be the number of principal prime ideals in the prime ideal factorization of (x). Then $k = n \iff k = m \implies \rho(x) = 1$. Henceforth we assume $k < \min(m,n)$ (since $\operatorname{Pic} R$ is nontrivial, there is at least one such x). We may further assume that $\alpha_1, \ldots, \alpha_k$ (resp. $\beta_1, \ldots, \beta_k$) are prime elements and $\alpha_{k+1}, \ldots, \alpha_m$ (resp. $\beta_{k+1}, \ldots, \beta_n$) are not; dividing through by these prime elements and correcting by a unit if necessary, we may write

$$x' = \alpha_{k+1} \cdots \alpha_m = \beta_{k+1} \cdots \beta_n.$$

Since for $k+1 \leq i \leq m$, α_i is irreducible but not prime, $P(\alpha_i) \geq 2$ and thus

$$2(m-k) \leq P(\alpha_{k+1} \cdots \alpha_m) = P(x').$$

On the other hand, by Proposition 23.13 we have

$$P(x') = P(\beta_{k+1} \cdots \beta_n) \leq (n-k) D(\operatorname{Pic} R).$$

Combining these inequalities gives

$$\frac{m}{n} \leq \frac{m-k}{n-k} \leq \frac{D(\operatorname{Pic} R)}{2}.$$

It follows that $\rho(x) \leq \frac{D(\operatorname{Pic} R)}{2}$ and thus $\rho(R) \leq \frac{D(\operatorname{Pic} R)}{2}$, establishing part a).
Step 2: Suppose R is replete.
Step 2a: Suppose first that $\operatorname{Pic} R$ is finite and put $D = D(\operatorname{Pic} R)$. By repleteness, choose prime ideals $\mathfrak{p}_1, \ldots, \mathfrak{p}_D$ whose classes form an irreducible sequence in $\operatorname{Pic} R$. For $1 \leq i \leq D$, let $\mathfrak{q}_i$ be a prime ideal with $[\mathfrak{q}_i] = [\mathfrak{p}_i]^{-1}$. For $1 \leq i \leq D$, let c_i be such that $(c_i) = \mathfrak{p}_i \mathfrak{q}_i$; using Lemma 23.11 there are $d_1, d_2 \in R$ such that $(d_1) = \mathfrak{p}_1 \cdots \mathfrak{p}_D$ and $(d_2) = \mathfrak{q}_1 \cdots \mathfrak{q}_D$ and

$$c_1 \cdots c_D = d_1 d_2.$$

By Proposition 23.12, $c_1, \ldots, c_D, d_1, d_2$ are all irreducible, and thus $\rho(R) \geq \frac{D}{2}$.
Step 2b: If $\operatorname{Pic} R$ is infinite, then $D(\operatorname{Pic} R) = \infty$ and from this, repleteness and Lemma 23.11, for all $D \in \mathbb{Z}^+$ there are prime ideals $\mathfrak{p}_1, \ldots, \mathfrak{p}_D$ whose classes form an irreducible sequence in $\operatorname{Pic} R$ and such that $\mathfrak{p}_1 \cdots \mathfrak{p}_D$ is principal. The argument of Step 2a now shows $\rho(R) \geq \frac{D}{2}$. Since this holds for all $D \in \mathbb{Z}^+$, $\rho(R) = \infty$. □

Remark: When $\operatorname{Pic} R$ is finite, Theorem 23.15 is due to W. Narkiewicz [Nar95].

Remark: The condition that R be replete is essential in Theorem 23.15. For instance, A. Zaks has shown that for every finitely generated commutative group G, there is a half factorial Dedekind domain R with $\operatorname{Pic} R \cong G$ [Zak76]. Whether any commutative group can occur, up to isomorphism, as the Picard group of a half factorial Dedekind domain is an open problem.

Corollary 23.16. *a) A replete Dedekind domain R is a HFD iff $\#\operatorname{Pic} R \leq 2$.*
b) (Carlitz [Ca60]*) Let K be a number field. Then its ring of integers $\mathbb{Z}_K$ is a HFD iff the class number of K – i.e., $\#\operatorname{Pic} \mathbb{Z}_K$ – is either 1 or 2.*
c) (Valenza [Va90]*) Let K be a number field. Then*

$$\rho(\mathbb{Z}_K) = \max\left(\frac{D(\operatorname{Pic} \mathbb{Z}_K)}{2}, 1\right).$$

d) A replete Dedekind domain has infinite elasticity iff it has infinite Picard group.

Exercise 23.8: Prove Corollary 23.16.

Remark: Later we will show that every commutative group arises, up to isomorphism, as the Picard group of a Dedekind domain. Combining this with Theorems 23.10 and 23.15 we see that the possible elasticities for replete Dedekind domains are precisely $\frac{n}{2}$ for any integer $n \geq 2$ and ∞.

We end this section by giving a little more information on the Davenport constant: let G be a finite commutative group, so that there is a unique sequence of positive integers $n_1, \ldots, n_r$ with $n_r \mid n_{r-1} \mid \ldots \mid n_1 > 1$ such that $G \cong \bigoplus_{i=1}^r \mathbb{Z}/n_i\mathbb{Z}$. We put $d(G) = 1 + \sum_{i=1}^k (n_i - 1)$, so that (43) reads more succinctly as

$$D(G) \geq d(G). \tag{44}$$

J.E. Olson conjectured that equality holds in (43) for all finite commutative groups G [Ol69a]. He proved that the conjecture holds for p-groups [Ol69a] and also when $r \leq 2$ [Ol69b]. However, it was shown by P. van Emde Boas and D. Kruyswijk that (for instance) $D(G) > d(G)$ for $G = \mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ [EBK69]. Whether $D(G) = d(G)$ for all groups with $r = 3$ is still an open problem. In particular the exact value of $D(G)$ is unknown for most finite commutative groups.

23.4. **Overrings of Prüfer Domains.**

Theorem 23.17. *Let R be an integral domain with fraction field K, and let T be an overring of R. TFAE:*
(i) For every prime ideal $\mathfrak{p}$ of R, either $\mathfrak{p}T = T$ or $T \subset R_{\mathfrak{p}}$.
(ii) For every $x, y \in K^\times$ with $\frac{x}{y} \in T$, $((y) : (x))T = T$.
(iii) T is a flat R-algebra.

Proof. **COMPLETE ME!** □

Proposition 23.18. *Let R be an integral domain with fraction field K and consider rings $R \subset T \subset T' \subset K$.*
a) If T' is flat over R, then T' is flat over T.
b) If T' is flat over T and T is flat over R, then T' is flat over R.

Proof. a) Suppose T' is flat over R. Let $a, b \in T$ be such that $\frac{a}{b} \in T'$. Write $a = \frac{c}{s}$, $b = \frac{d}{s}$ with $c, d, s \in R$. Then $\frac{c}{d} \in T'$, so by Theorem 23.17, $((d) : (c))T' = T'$. Hence $1 = t_1u_1 + \ldots + t_ku_k$ for some $t_i \in T'$ and $u_i \in R$ with $u_ic \in (d)$ for all i. Then there is $z_i \in R$ such that $u_ic = dz_i$, so $u_ia = z_i\frac{d}{s} = z_ib \in Tb$ for all i. So $(Tb : Ta)T' = T'$. Applying Theorem 23.17 again, we get that T' is flat over T.
b) This holds for any $R_1 \subset R_2 \subset R_3$, since $M \otimes_{R_1} R_3 \cong (M \otimes_{R_1} R_2) \otimes_{R_2} R_3$. □

Proposition 23.19. *For an overring T of an integral domain R, TFAE:*
(i) T is flat over R.
(ii) For all $\mathfrak{p} \in \operatorname{MaxSpec} T$, $T_{\mathfrak{p}} = R_{\mathfrak{p} \cap R}$.
(iii) $T = \bigcap_{\mathfrak{p} \in \operatorname{MaxSpec} T} R_{\mathfrak{p}}$.

Proof. **COMPLETE ME!** □

Proposition 23.20. *Let T be an overring of a domain R which is both integral and flat over R. Then $R = T$.*

Proof. Let $x, y \in R$ be such that $\frac{x}{y} \in T$. Then by Theorem 23.17, $((y) : (x))T = T$. Let $\mathfrak{p} \in \operatorname{MaxSpec} R$. By Theorem 14.13, there exists a prime (in fact maximal by Corollary 14.16, but this is not needed here) ideal $\mathcal{P}$ of T lying over $\mathfrak{p}$. Since $\mathfrak{p}T \subset \mathcal{P}$, we have $\mathfrak{p}T \subsetneq T$. Therefore $((y) : (x))$ is not contained in any maximal ideal of R, so $((y) : (x)) = R$. It follows that $x \in (y)$, i.e., $x = ay$ for some $a \in R$, so that $\frac{x}{y} \in R$. Thus $R = T$. □

Theorem 23.21. *For an integral domain R, TFAE:*
(i) R is a Prüfer domain.
(ii) Every overring of R is a flat R-module.

Proof. (i) $\implies$ (ii): An overring is a torsionfree R-module, so this follows immediately from Theorem 21.10.
(ii) $\implies$ (i): Let $\mathfrak{p}$ be a maximal ideal of R. By Proposition 23.18, every overring of $R_{\mathfrak{p}}$ is flat. Let $a, b \in R_{\mathfrak{p}}$, and suppose that $aR_{\mathfrak{p}} \not\subset bR_{\mathfrak{p}}$. Then $(bR_{\mathfrak{p}} : aR_{\mathfrak{p}}) \neq R_{\mathfrak{p}}$; since $R_{\mathfrak{p}}$ is local, this implies $(bR_{\mathfrak{p}} : aR_{\mathfrak{p}}) \subset \mathfrak{p}R_{\mathfrak{p}}$. Now consider the ring $R_{\mathfrak{p}}[\frac{a}{b}]$. This is an overring of $R_{\mathfrak{p}}$, hence flat. Since $\frac{a}{b} \in R_{\mathfrak{p}}[\frac{a}{b}]$ we have by Theorem 23.17

$$(bR_{\mathfrak{p}} : aR_{\mathfrak{p}})R_{\mathfrak{p}}[\frac{a}{b}] = R_{\mathfrak{p}}[\frac{a}{b}].$$

Thus there exist elements $x_1, \ldots, x_n \in (bR_{\mathfrak{p}} : aR_{\mathfrak{p}}$ and $b_1, \ldots, b_n \in R_{\mathfrak{p}}[\frac{a}{b}]$ such that $x_1 b_1 + \ldots + x_n b_n = 1$. ... **COMPLETE ME!** □

Corollary 23.22. *Every overring of a Prüfer domain is a Prüfer domain.*

Proof. Let R be a Prüfer domain and T be an overring of R. Then every overring T' of T is in particular an overring of R, so T' is flat over R. By Proposition 23.18a), T' is also flat over T. Therefore every overring of T is flat over T, so by Theorem 23.21, T is a Prüfer domain. □

Corollary 23.23. *For a Noetherian domain R, TFAE:*
(i) Every overring of R is a localization.
(ii) R is a Dedekind domain and $\operatorname{Pic} R$ *is a torsion group.*

Exercise 23.9: Prove Corollary 23.23.

Finally we give a result which generalizes the (as yet unproven) Theorem 23.3. Namely, for R a domain, let W be a subset of $\operatorname{MaxSpec} R$ and put

$$R_W = \bigcap_{\mathfrak{p} \in W} R_{\mathfrak{p}}.$$

Theorem 23.24. *Let R be a Prüfer domain, T an overring of R, and put*

$$W = \{\mathfrak{p} \in \operatorname{MaxSpec}(R) \mid \mathfrak{p}T \subsetneq T\}.$$

Then $T = R_W$.

Proof. **COMPLETE ME!** □

23.5. **Kaplansky's Theorem (III).**

Theorem 23.25. *(Kaplansky* [K]*) Let R be a Dedekind domain with fraction field K, and let $\overline{K}$ be an algebraic closure of K. Suppose that for every finite extension L/K, the Picard group of the integral closure R_L of R in L is a torsion abelian group. Then the integral closure S of R in $\overline{K}$ is a Bézout domain.*

Proof. Let $I = \langle a_1, \ldots, a_n \rangle$ be a finitely generated ideal of S. Then $L = K[a_1, \ldots, a_n]$ is a finite extension of K. Let R_L be the integral closure of R in L, and let $I_L = \langle a_1, \ldots, a_n \rangle_{R_L}$. By hypothesis, there exists $k \in \mathbb{Z}^+$ and $b \in R_L$ such that $I_L^k = bR_L$. Let c be a kth root of b in S and let $M = L[c]$. Thus in the Dedekind domain R_M we have $(I_L R_M)^k = (c^k)$, and from unique factorization of ideals we deduce $I_L R_M = cR_M$. Thus $I = I_L R_M S = cR_M S = cS$ is principal. □

Recall the basic fact of algebraic number theory that for any number field K, the Picard group of $\mathbb{Z}_K$ is finite. This shows that the ring $R = \mathbb{Z}$ satisfies the hypotheses of Theorem 23.25. We deduce that the ring of all algebraic integers $\overline{\mathbb{Z}}$ is a Bézout domain: Theorem 5.1.

Exercise 23.10: Adapt the proof of Theorem 23.25 to show that the Picard group of the ring of integers of the maximal solvable extension $\mathbb{Q}^{\mathrm{solv}}$ of $\mathbb{Q}$ is trivial.

Exercise 23.11: State a function field analogue of Theorem 5.1 and deduce it as a special case of Theorem 23.25.

We quote without proof two more recent results on Picard groups of integer rings of infinite algebraic extensions of $\mathbb{Q}$.

Theorem 23.26. *(Brumer* [Bru81]*) Let $\mathbb{Q}^{\mathrm{cyc}} = \bigcup_{n \in \mathbb{Z}^+} \mathbb{Q}(\zeta_n)$ be the field obtained by adjoining to $\mathbb{Q}$ all roots of unity, and let $\mathbb{Z}^{\mathrm{cyc}}$ be its ring of integers, i.e., the integral closure of $\mathbb{Z}$ in $\mathbb{Q}^{\mathrm{cyc}}$. Then*

$$\operatorname{Pic} \mathbb{Z}^{\mathrm{cyc}} \cong \bigoplus_{i=1}^{\infty} \mathbb{Q}/\mathbb{Z}.$$

Theorem 23.27. *(Kurihara* [Ku99]*) Let $\mathbb{Q}^{\mathrm{cyc}+} = \bigcup_{n \in \mathbb{Z}^+} \mathbb{Q}(\zeta_n + \zeta_n^{-1})$ be the maximal real subfield of $\mathbb{Q}^{\mathrm{cyc}}$, and let $\mathbb{Z}^{\mathrm{cyc}+}$ be its ring of integers, i.e., the integral closure of $\mathbb{Z}$ in $\mathbb{Q}^{\mathrm{cyc}+}$. Then*

$$\operatorname{Pic} \mathbb{Z}^{\mathrm{cyc}+} = 0.$$

23.6. **Every commutative group is a class group.**

To any ring R we attached a commutative group, the Picard group $\operatorname{Pic} R$. In fact the construction is functorial: a homomorphism $\varphi : R \to R'$ of domains induces a homomorphism $\varphi_* : \operatorname{Pic} R \to \operatorname{Pic} S$ of Picard groups. Explicitly, if M is a rank one projective R-module, then $M \otimes_R R'$ is a rank one projective R'-module. In general when one is given a functor it is natural to ask about its image. Here we are asking the following

Question 6. *Which commutative groups occur (up to isomorphism) as the Picard group of a commutative ring?*

We have also defined the divisor class group $\operatorname{Cl} R$ of a domain, so we may also ask:

Question 7. *Which commutative groups occur (up to isomorphism) as the divisor class group of an integral domain?*

It would be interesting to know at what point algebraists began serious consideration of the above questions. I have not discussed the history of $\operatorname{Pic} R$ and $\operatorname{Cl} R$ in part because I am not sufficiently knowledgeable to do so, but their study was

surely informed by two classical cases: the ideal class group of (the ring of integers of) a number field, and the Picard group of line bundles on an (affine or projective) complex algebraic variety. The groups that arise in these classical cases are very restricted: the class group of a number field is a finite abelian group, and the Picard group of a complex algebraic variety is an extension of a complex torus by a finitely generated abelian group. As far as I know the literature contains nothing beyond this until the dramatic full solution.

Theorem 23.28. *(Claborn* [Clb66]*) For every commutative group G, there is a Dedekind domain R with* $\operatorname{Pic} R = \operatorname{Cl} R \cong G$.

Even after developing several hundred pages of commutative algebra, Claborn's proof still requires some technical tools that we lack. Especially, Claborn first constructs a *Krull domain* R with $\operatorname{Cl} R \cong G$ and then by an approximation process constructs a Dedekind domain with the same class group. But we have not yet discussed Krull domains in these notes.

A more elementary – but still quite ingenious and intricate – proof was given later by C.R. Leedham-Green [Lee72]. Leedham-Green constructs the requisite R as the integral closure of a PID in a separable quadratic field extension.

Several years after that M. Rosen took a more naturally geometric approach, inspired by the Picard groups of varieties which appear in algebraic geometry. Especially, his approach uses some elliptic curve theory.

Let k be a field of characteristic zero. Fix elements $A, B \in K$ such that $4A^3 + 27B^2 \neq 0$, and let $k[E] = k[x,y]/(y^2 - x^3 - Ax - B)$. The ring R is precisely the affine coordinate ring of the elliptic curve

$$E : y^2 = x^3 + Ax + B.$$

Proposition 23.29. *The ring $k[E]$ is a Dedekind domain.*

We denote the fraction field of $k[E]$ by $k(E)$, also called the **function field** of $E_{/k}$.

The overrings of R are all of the form $R^W = \bigcap_{\mathfrak{p} \in \Sigma_R \setminus W} R_{\mathfrak{p}}$ for $W \subset \operatorname{MaxSpec} R$, and by the Krull-Akizuki Theorem each R^W is a Dedekind domain. By definition, a Dedekind domain which arises in this way – i.e., as an overring of the standard affine ring of an elliptic curve over a field of characteristic zero – is called an **elliptic Dedekind domain**. We refer to k as the **ground field** of R.

Exercise 23.12: a) Let k be a countable field, and let R be an elliptic Dedekind domain with ground field k. Show that $\operatorname{Pic} R$ is a countable abelian group.
b) More generally, show that if R is an elliptic Dedekind domain with ground field k, then $\#\operatorname{Pic} R \leq \max \aleph_0, \#k$.

Conversely:

Theorem 23.30. *(Rosen* [Ros76]*) For every countable abelian group G, there exists an elliptic Dedekind domain R with ground field an algebraic extension of $\mathbb{Q}$ and such that* $\operatorname{Pic} R \cong G$.

In 2008 I built on this work of Rosen to prove the following result [Clk09].

Theorem 23.31. *For any commutative group G, there is an elliptic Dedekind domain R such that:*
(i) R is the integral closure of a PID in a separable quadratic field extension, and
(ii) $\operatorname{Pic} R \cong G$.

Thus Theorem 23.31 implies the results of Claborn and Leedham-Green. On the other hand, Exercise 23.12 shows that the absolute algebraicity (or even the countability!) of the ground field k achieved in Rosen's construction cannot be maintained for uncountable Picard groups. Indeed our argument goes to the other extreme: we construct the ground field k as a transfinitely iterated function field.

Our argument will require some tenets of elliptic curve theory, especially the notion of the **rational endomorphism ring** $\operatorname{End}_K E$ of an elliptic curve $E_{/K}$. A K-rational endomorphism of an elliptic curve is a morphism $\varphi : E \to E$ defined over K which carries the neutral point O of E to itself.

Proposition 23.32. *Let k be a field and $E_{/k}$ an elliptic curve.*
a) The additive group of $\operatorname{End}_k(E)$ *is isomorphic to $\mathbb{Z}^{a(E)}$ for $a(E) \in \{1, 2, 4\}$.*
b) There is a short exact sequence

$$0 \to E(k) \to E(k(E)) \to \operatorname{End}_K(E) \to 0.$$

Since $\operatorname{End}_k(E)$ *is free abelian, we have $E(k(E)) \cong E(k) \bigoplus \mathbb{Z}^{a(E)}$.*
c) There is a canonical isomorphism $E(k) \cong \operatorname{Pic} k[E]$.

Proof. a) See [Si86, Cor. III.9.4].
b) $E(k(E))$ is the group of rational maps from the nonsingular curve E to the complete variety E under pointwise addition. Every rational map from a nonsingular curve to a complete variety is everywhere defined, so $E(k(E))$ is the group of morphisms $E \to E$ under pointwise addition. The constant morphisms form a subgroup isomorphic to $E(k)$, and every map $E \to E$ differs by a unique constant from a map of elliptic curves $(E, O) \to (E, O)$, i.e., an endomorphism of E.
c) By Riemann-Roch, $\Psi_1 : E(k) \to \operatorname{Pic}^0 E$ by $P \in E(k) \mapsto [[P] - [O]]$ is an isomorphism [Si86, Prop. III.3.4]. Moreover, $\Psi_2 : \operatorname{Pic}^0(E) \to \operatorname{Pic} k[E]$ given by $\sum_P n_P[P] \mapsto \sum_{P \neq O} n_P[P]$ is an isomorphism. Thus $\Psi_2 \circ \Psi_1 : E(k) \xrightarrow{\sim} \operatorname{Pic} k[E]$. □

Now fix a field k, and let $(E_0)/k$ be any elliptic curve.[70] Define $K_0 = k$, and $K_{n+1} = K_n(E_{/K_n})$. Then Proposition 23.32 gives

$$E(K_n) \cong E(k) \oplus \bigoplus_{i=1}^{n} \mathbb{Z}^{a(E)}.$$

Lemma 23.33. *Let K be a field, $(K_i)_{i \in I}$ a directed system of field extensions of K, and $E_{/K}$ an elliptic curve. There is a canonical isomorphism*

$$\lim_I E(K_i) = E(\lim_I K_i).$$

[70] In the paper [Clk09] I took the specific choice $(E_0)_{/\mathbb{Q}} : y^2 + y = x^3 - 49x - 86$, mostly for sentimental reasons. This curve has the property that $E_0(\mathbb{Q}) = 0$ [Ko89, Theorem H] and nonintegral j-invariant $\frac{2^{12}3^3}{37}$, so $\operatorname{End}_{\mathbb{Q}} E = \mathbb{Z}$. But in fact the construction can be made to work starting with any elliptic curve, and we have decided to phrase it this way here.

Exercise 23.13: Prove Lemma 23.33.

Now let o be an ordinal number. We define the field K_o by transfinite induction: $K_0 = k$, for an ordinal $o' < o$, $K_{o'+1} = K_{o'}(E_{/K_{o'}})$, and for a limit ordinal o, $K_o = \lim_{o'<o} K_{o'}$. By the Continuity Lemma, we have $E(K_o) = \lim_{o' \in o} E(K_{o'})$.

Lemma 23.34. *Let $a \in \mathbb{Z}^+$. For an abelian group A, the following are equivalent:*
(i) A is free abelian of rank $a \cdot \kappa$ for some cardinal κ.
(ii) A has a well-ordered ascending series with all factors $A_{s+1}/A_s \cong \mathbb{Z}^a$.

Exercise 23.14: Prove Lemma 23.34.
(Suggestion: use the Transfinite Dévissage Lemma.)

Corollary 23.35. *We have $E(K_o)/E(k) \cong \bigoplus_{o' \in o} \mathbb{Z}^{a(E)}$.*

Exercise 23.15: Prove Corollary 23.35.

One can put together the results derived so far together with Exercise 22.2 to get a proof of Theorem 23.28. However, to prove Theorem 23.31 we need to circumvent the appeal to Theorem 23.10. This is handled as follows.

Theorem 23.36. *Let $E_{/k}$ be an elliptic curve with equation $y^2 = P(x) = x^3 + Ax + B$. a) The affine ring $k[E]$ is weakly replete.*
b) If k is algebraically closed, $k[E]$ is not replete.
c) Suppose k does not have characteristic 2 and $k[E]$ is not replete. Then for all $x \in k$, there exists $y \in k$ with $y^2 = P(x)$.

Proof. Each point $P \neq O$ on $E(k)$ a prime ideal in the standard affine ring $k[E]$; according to the isomorphism of Proposition 23.32c), every nontrivial element of $\mathrm{Pic}(k[E])$ arises in this way. This proves part a). Part b) is similar: if k is algebraically closed, then by Hilbert's Nullstellensatz every prime ideal of $k[E]$ corresponds to a k-valued point $P \neq O$ on $E(k)$, which under Proposition 23.32c) corresponds to a nontrivial element of the class group. Therefore the trivial class is not represented by any prime ideal. Under the hypotheses of part c), there exists an $x \in k$ such that the points $(x, \pm\sqrt{P(x)})$ form a Galois conjugate pair. Therefore the divisor $(x, \sqrt{P(x)}) + (x, -\sqrt{P(x)})$ represents a closed point on the curve C^o, in other words a nonzero prime ideal of $k[E]$. But the corresponding point on $E(k)$ is $(x, \sqrt{P(x)}) + (x, -\sqrt{P(x)}) = O$. □

Finally we prove Theorem 23.31(i). Let G be an abelian group, and write it as F/H where F is a free abelian group of infinite rank. As above let k be any field of characteristic zero and $E_{/k}$ any elliptic curve. By Corollary 23.35, for all sufficiently large ordinals o, there is a surjection $E(K_0) \to F$ and thus also a surjection $E(K_o) \to G$. By Proposition 23.32c), there is a subgroup H of $K_o[E]$ such that $(\mathrm{Pic}\, K_o[E])/H \cong G$. By Proposition 18.1a) and Proposition 23.8, there is an overring T of $K_o[E]$ such that $\mathrm{Pic}\, T \cong G$, establishing Theorem 23.31(i).

As for the second part: let σ be the automorphism of the function field $k(E)$ induced by $(x, y) \mapsto (x, -y)$, and notice that σ corresponds to inversion $P \mapsto -P$ on $E(k) = \mathrm{Pic}(k[E])$. Let $S = R^\sigma$ be the subring of R consisting of all functions which are fixed by σ. Then $k[E]^\sigma = k[x]$ is a PID, and S is an overring of $k[x]$, hence also a PID. More precisely, S is the overring of all functions on the projective

line which are regular away from the point at infinity and the x-coordinates of all the elements in H (note that since H is a subgroup, it is stable under inversion). Finally, to see that R is the integral closure of S in the separable quadratic field extension $k(E)/k(x)$, it suffices to establish the following simple result.

Lemma 23.37. *Let L/K be a finite Galois extension of fields, and S a Dedekind domain with fraction field L. Suppose that for all $\sigma \in \mathrm{Gal}(L/K)$, $\sigma(S) = S$. Then S is the integral closure of $R := S \cap K$ in L.*

Proof. Since S is integrally closed, it certainly contains the integral closure of R in L. Conversely, for any $x \in S$, $P(t) = \prod_{\sigma \in \mathrm{Gal}(L/K)}(t - \sigma(x))$ is a monic polynomial with coefficients in $(S \cap K)[t]$ satisfied by x. □

This completes the proof of Theorem 23.31.

References

[AB59] M. Auslander and D.A. Buchsbaum, *Unique factorization in regular local rings.* Proc. Nat. Acad. Sci. U.S.A. 45 (1959), 733-734.

[Ad62] J.F. Adams, *Vector fields on spheres.* Ann. of Math. (2) 75 (1962), 603-632.

[AHRT] J. Adámek, H. Herrlich, J. Rosický and W. Tholen, *Injective hulls are not natural.* Algebra Universalis 48 (2002), 379-388.

[Al99] N. Alon, *Combinatorial Nullstellensatz.* Recent trends in combinatorics (Mátraháza, 1995). Combin. Probab. Comput. 8 (1999), 7-29.

[An00] D.D. Anderson, *GCD domains, Gauss' lemma, and contents of polynomials.* Non-Noetherian commutative ring theory, 1-31, Math. Appl., 520, Kluwer Acad. Publ., Dordrecht, 2000.

[AR97] D.D. Anderson and M. Roitman, *A characterization of cancellation ideals.* Proc. Amer. Math. Soc. 125 (1997), 2853-2854.

[AP82] J.K. Arason and A. Pfister, *Quadratische Formen über affinen Algebren und ein algebraischer Beweis des Satzes von Borsuk-Ulam.* (German) J. Reine Angew. Math. 331 (1982), 181-184.

[Ar27] E. Artin, *Zur Theorie der hyperkomplexen Zahlen.* Abh. Hamburg, 5 (1927), 251-260.

[AT51] E. Artin and J.T. Tate, *A note on finite ring extensions.* J. Math. Soc. Japan 3 (1951), 74-77.

[At89] M.F. Atiyah, *K-theory.* Notes by D. W. Anderson. Second edition. Advanced Book Classics. Addison-Wesley Publishing Company, Redwood City, CA, 1989.

[AM] M.F. Atiyah and I.G. Macdonald, *Introduction to commutative algebra.* Addison-Wesley Publishing Co., Reading Mass.-London-Don Mills, Ont. 1969.

[Bae40] R. Baer, *Abelian groups that are direct summands of every containing abelian group.* Bull. Amer. Math. Soc. 46 (1940), 800-806.

[Bas59] H. Bass, *Global dimension of rings*, Ph.D. Thesis, University of Chicago, 1959.

[Bas63] H. Bass, *Big projective modules are free.* Illinois J. Math. 7 1963 24-31.

[Bau62] G. Baumslag, *On abelian hopfian groups. I.* Math. Z. 78 1962 5354.

[Bau63] G. Baumslag, *Hopficity and abelian groups.* 1963 Topics in Abelian Groups (Proc. Sympos., New Mexico State Univ., 1962) pp. 331-335 Scott, Foresman and Co., Chicago, Ill.

[BCR] J.Bochnak, M. Coste and M.-F. Roy, *Real algebraic geometry.* Ergebnisse der Mathematik und ihrer Grenzgebiete (3) 36. Springer-Verlag, Berlin, 1998.

[Be] D.J. Benson, *Polynomial invariants of finite groups* London Mathematical Society Lecture Note Series, 190. Cambridge University Press, Cambridge, 1993.

[Bk70] R. Bkouche, *Pureté, mollesse et paracompacité.* C. R. Acad. Sci. Paris Sér. A-B 270 (1970), A1653-A1655.

[Bor50] S. Borofsky, *Factorization of polynomials.* Amer. Math. Monthly 57 (1950), 317–320.

[BM58] R. Bott and J. Milnor, *On the parallelizability of the spheres.* Bull. Amer. Math. Soc. 64 (1958), 87-89.

[B] N. Bourbaki, *Commutative algebra. Chapters 1-7*. Translated from the French. Reprint of the 1989 English translation. Elements of Mathematics (Berlin). Springer-Verlag, Berlin, 1998.

[Bou78] A. Bouvier, *Le groupe des classes de l'algbre affine d'une forme quadratique*. Publ. Dép. Math. (Lyon) 15 (1978), no. 3, 53–62.

[BMRH] J.W. Brewer, P.R. Montgomery, E.A. Rutter and W.J. Heinzer, *Krull dimension of polynomial rings*. Conference on Commutative Algebra (Univ. Kansas, Lawrence, Kan., 1972), pp. 2645. Lecture Notes in Math., Vol. 311, Springer, Berlin, 1973.

[Bro02] G. Brookfield, *The length of Noetherian modules*. Comm. Algebra 30 (2002), 3177-3204.

[Bru81] A. Brumer, *The class group of all cyclotomic integers*. J. Pure Appl. Algebra 20 (1981), no. 2, 107-111.

[Buc61] D.A. Buchsbaum, *Some remarks on factorization in power series rings*. J. Math. Mech. 10 1961 749–753.

[But64] H.S. Butts, *Unique factorization of ideals into nonfactorable ideals*. Proc. Amer. Math. Soc. 15 (1964), 21.

[BW66] H.S. Butts and L.I. Wade, *Two criteria for Dedekind domains*. Amer. Math. Monthly 73 (1966), 14–21.

[Ca60] L. Carlitz, *A Characterization of Algebraic Number Fields with Class Number Two*. Proc. AMS 11 (1960), 391–392.

[Cd-SF] K. Conrad, *Stably Free Modules*. Notes available at `http://www.math.uconn.edu/~kconrad/blurbs/linmultialg/stablyfree.pdf`

[CDVM13] L.F. Cáceres Duque and J.A. Vélez-Marulanda, *On the Infinitude of Prime Elmeents*. Rev. Colombiana Mat. 47 (2013), 167–179.

[CE] H. Cartan and S. Eilenberg, *Homological algebra*. Princeton University Press, Princeton, N. J., 1956.

[CE59] E.D. Cashwell and C.J. Everett, *The ring of number-theoretic functions*. Pacific J. Math. 9 (1959) 975–985.

[Clb66] L.E. Claborn, *Every abelian group is a class group*. Pacific J. Math. 18 (1966), 219-222.

[Clk09] P.L. Clark, *Elliptic Dedekind domains revisited*. Enseignement Math. 55 (2009), 213–225.

[Clk12] P.L. Clark, *A Note on Euclidean Order Types*. Preprint, `www.math.uga.edu/~pete/OrdinalInvariant.pdf`.

[Coh68] P.M. Cohn, *Bézout rings and their subrings*. Proc. Cambridge Philos. Soc. 64 (1968), 251–264.

[Coh73] P.M. Cohn, *Unique factorization domains*. Amer. Math. Monthly 80 (1973), 1–18.

[Coh50] I.S. Cohen, *Commutative rings with restricted minimum conditions*. Duke Math. J. 17, (1950), 27-42.

[CK46] I.S. Cohen and I. Kaplansky, *Rings with a finite number of primes. I.* Trans. Amer. Math. Soc. 60 (1946), 468-477.

[CK51] I.S. Cohen and I. Kaplansky, *Rings for which every module is a direct sum of cyclic modules.* Math. Z. 54 (1951), 97-101.

[CS46] I.S. Cohen and A. Seidenberg, *Prime ideals and integral dependence*. Bull. Amer. Math. Soc. 52 (1946), 252-261.

[Cor64] A.L.S. Corner, *On a conjecture of Pierce concerning direct decompositions of Abelian groups*. 1964 Proc. Colloq. Abelian Groups (Tihany, 1963) pp. 43-48 Akadémiai Kiadó, Budapest.

[Cox11] D.A. Cox, *Why Eisenstein proved the Eisenstein criterion and why Schönemann discovered it first*. Amer. Math. Monthly 118 (2011), 3-21.

[Da09] C.S. Dalawat, *Wilson's theorem*. J. Théor. Nombres Bordeaux 21 (2009), 517-521.

[De71] R. Dedekind. . .

[DM71] F. DeMeyer and E. Ingraham, *Separable algebras over commutative rings*. Lecture Notes in Mathematics, Vol. 181 Springer-Verlag, Berlin-New York 1971.

[Ea68] P.M. Eakin, Jr. *The converse to a well known theorem on Noetherian rings*. Math. Ann. 177 (1968), 278-282.

[EBK69] P. van Emde Boas and D. Kruyswijk, *A combinatorial problem on finite abelian groups, III*, Report ZW- 1969-008, Math. Centre, Amsterdam, 1969.

[Ec00] O. Echi, *A topological characterization of the Goldman prime spectrum of a commutative ring*. Comm. Algebra 28 (2000), 2329-2337.

[ES53] B. Eckmann and A. Schopf, *Über injektive Moduln*. Arch. Math. (Basel) 4 (1953), 75-78.

[Eis] D. Eisenbud, *Commutative algebra. With a view toward algebraic geometry*. Graduate Texts in Mathematics, 150. Springer-Verlag, New York, 1995.

[Ei50] F. Eisenstein, *Über die Irredicibilität une einige andere Eigenschaften der Gleichung von welche der Theilung der ganzen Lemniscate abhängt*. J. Reine Angew. Math. 39 (1950), 160-179.

[FT] *Field Theory*, notes by P.L. Clark, available at `http://www.math.uga.edu/~pete/FieldTheory.pdf`

[FR70] R.L. Finney and J.J. Rotman, *Paracompactness of locally compact Hausdorff spaces*. Michigan Math. J. 17 (1970), 359-361.

[FW67] C. Faith and E.A. Walker, *Direct-sum representations of injective modules*. J. Algebra 5 (1967), 203-221.

[Fl71] C.R. Fletcher, *Euclidean rings*. J. London Math. Soc. 4 (1971), 79-82.

[For73] E. Formanek, *Faithful Noetherian modules*. Proc. Amer. Math. Soc. 41 (1973), 381-383.

[Fos73] R.M. Fossum, *The divisor class group of a Krull domain*. Ergebnisse der Mathematik und ihrer Grenzgebiete, Band 74. Springer-Verlag, New York-Heidelberg, 1973.

[Fu59] L. Fuchs, *The existence of indecomposable abelian groups of arbitrary power*. Acta Math. Acad. Sci. Hungar. 10 (1959) 453-457.

[Fu74] L. Fuchs, *Indecomposable abelian groups of measurable cardinalities*. Symposia Mathematica, Vol. XIII (Convegno di Gruppi Abeliani, INDAM, Rome, 1972), pp. 233244. Academic Press, London, 1974.

[Ga71] T.E. Gantner, *A Regular Space on which every Continuous Real-Valued Function is Constant*. Amer. Math. Monthly 78 (1971), 52–53.

[Ge91] R. Germundsson, *Basic Results on Ideals and Varieties in Finite Fields*. Technical report, Department of Electrical Engineering, Lïnkoping University, 1991.

[GJ76] L. Gillman and M. Jerison, *Rings of continuous functions*. Reprint of the 1960 edition. Graduate Texts in Mathematics, No. 43. Springer-Verlag, New York-Heidelberg, 1976.

[Gol51] O. Goldman, *Hilbert rings and the Hilbert Nullstellensatz*. Math. Z. 54 (1951). 136-140.

[Gol64] O. Goldman, *On a special class of Dedekind domains*. Topology 3 (1964) suppl. 1, 113-118.

[Gov65] V.E. Govorov, *On flat modules*. (Russian) Sibirsk. Mat. Ž. 6 (1965), 300-304.

[Gr74] A. Grams, *Atomic rings and the ascending chain condition for principal ideals*. Proc. Cambridge Philos. Soc. 75 (1974), 321–329.

[Gu73] T.H. Gulliksen, *A theory of length for Noetherian modules*. J. Pure Appl. Algebra 3 (1973), 159-170.

[Hai94] B. Haible, *Gauss' Lemma without Primes*, preprint, 1994.

[Has28] H. Hasse, *Über eindeutige Zerlegung in Primelemente oder in Primhauptideale in Integrittsbereichen*. J. reine Angew. Math. 159 (1928), 3–12.

[Hel40] O. Helmer, *Divisibility properties of integral functions*. Duke Math. J. 6 (1940), 345-356.

[Hei70] W. Heinzer, *Quotient overrings of an integral domain*. Mathematika 17 (1970), 139–148.

[Hei74] R.C. Heitmann, *PID's with specified residue fields*. Duke Math. J. 41 (1974), 565-582.

[Hes06] G. Hessenberg, *Grundbegriffe der Mengenlehre*. Göttingen, 1906.

[Hi90] D. Hilbert, *Ueber die Theorie der algebraischen Formen*. Mathl Annalen 36 (1890), 473-534.

[Ho69] M. Hochster, *Prime ideal structure in commutative rings*. Trans. Amer. Math. Soc. 142 (1969), 43–60.

[Hi75] J.-J. Hiblot, *Des anneaux euclidiens dont le plus petit algorithme n'est pas à valeurs finies*. C. R. Acad. Sci. Paris Sér. A-B 281 (1975), no. 12, Ai, A411–A414.

[Hi77] J.-J. Hiblot, *Correction à une note sur les anneaux euclidiens: "Des anneaux euclidiens dont le plus petit algorithme n'est pas à valeurs finies" (C. R. Acad. Sci. Paris Sér. A-B 281 (1975), no. 12, A411–A414)*. C. R. Acad. Sci. Paris S er. A-B 284 (1977), no. 15, A847-A849.

[Hö01] O. Hölder, *Die Axiome der Quantitat und die Lehre vom Mass*. Ber. Verh. Sachs. Ges. Wiss. Leipzig, Math.-Phys. Cl. 53 (1901), 1-64.
[Ho79] W. Hodges, *Krull implies Zorn*. J. London Math. Soc. (2) 19 (1979), 285-287.
[Hun68] T.W. Hungerford, *On the structure of principal ideal rings*. Pacific J. Math. 25 (1968), 543–547.
[Hus66] D. Husemöller, *Fibre bundles*. McGraw-Hill Book Co., New York-London-Sydney 1966.
[J1] N. Jacobson, *Basic algebra. I*. Second edition. W. H. Freeman and Company, New York, 1985.
[J2] N. Jacobson, *Basic algebra. II*. Second edition. W. H. Freeman and Company, New York, 1989.
[Jo00] P. Jothilingam, *Cohen's theorem and Eakin-Nagata theorem revisited*. Comm. Algebra 28 (2000), 4861-4866.
[Ka52] I. Kaplansky, *Modules over Dedekind rings and valuation rings*. Trans. Amer. Math. Soc. 72 (1952), 327–340.
[Ka58] I. Kaplansky, *Projective modules*. Ann. of Math. 68 (1958), 372-377.
[K] I. Kaplansky, *Commutative rings*. Allyn and Bacon, Inc., Boston, Mass. 1970.
[Ka] M. Karoubi, *K-theory. An introduction*. Reprint of the 1978 edition. With a new postface by the author and a list of errata. Classics in Mathematics. Springer-Verlag, Berlin, 2008.
[Kh03] D. Khurana, *On GCD and LCM in domains a conjecture of Gauss*. Resonance 8 (2003), 72–79.
[KM99] G. Kemper and G. Malle, *Invariant fields of finite irreducible reflection groups*. Math. Ann. 315 (1999), 569–586.
[Ko89] V. Kolyvagin, *On the Mordell-Weil and Shafarevich-Tate groups for Weil elliptic curves*, Math. USSR-Izv. 33 (1989), 473–499.
[Kr31] W. Krull, *Allgemeine Bewertungstheorie*. J. Reine Angew. Math. 167 (1931), 160-196.
[Kr37] W. Krull, *Beiträge zur Arithmetik kommutativer Integritätsbereiche, III, zum Dimensionsbegriff der Idealtheorie*, Mat. Zeit 42 (1937), 745–766.
[Kr51] W. Krull, *Jacobsonsche Ringe, Hilbertscher Nullstellensatz Dimensionen theorie*. Math. Z. 54 (1951), 354-387.
[Ku99] M. Kurihara, *On the ideal class groups of the maximal real subfields of number fields with all roots of unity*. J. Eur. Math. Soc. (JEMS) 1 (1999), 35-49.
[La87] D. Laksov, *Radicals and Hilbert Nullstellensatz for not necessarily algebraically closed fields*. Enseign. Math. (2) 33 (1987), 323-338.
[Lam99] T.Y. Lam, *Lectures on modules and rings*. Graduate Texts in Mathematics, 189. Springer-Verlag, New York, 1999.
[Lam05] T.Y. Lam, *Introduction to quadratic forms over fields*. Graduate Studies in Mathematics, 67. American Mathematical Society, Providence, RI, 2005.
[Lam06] T.Y. Lam, *Serre's problem on projective modules*. Springer Monographs in Mathematics. Springer-Verlag, Berlin, 2006.
[LR08] T.Y. Lam and M.L. Reyes, *A prime ideal principle in commutative algebra*. J. Algebra 319 (2008), 3006-3027.
[La53] S. Lang, *The theory of real places*. Ann. of Math. (2) 57 (1953), 378-391.
[Lan02] S. Lang, *Algebra*. Revised third edition. Graduate Texts in Mathematics, 211. Springer-Verlag, New York, 2002.
[LM] M.D. Larsen and P.J. McCarthy, *Multiplicative theory of ideals*. Pure and Applied Mathematics, Vol. 43. Academic Press, New York-London, 1971.
[Las05] E. Lasker, *Zur Theorie der Moduln und Ideale*. Math. Ann. 60 (1905), 19-116.
[Laz64] D. Lazard, *Sur les modules plats*. C. R. Acad. Sci. Paris 258 (1964), 6313-6316.
[Lee72] C.R. Leedham-Green, *The class group of Dedekind domains*. Trans. Amer. Math. Soc. 163 (1972), 493–500.
[Lev43] F.W. Levi, *Contributions to the theory of ordered groups*. Proc. Indian Acad. Sci., Sect. A. 17 (1943), 199-201.
[Les67] L. Lesieur, *Divers aspects de la théorie des idéaux d'un anneau commutatif*. Enseignement Math. 13 (1967), 75-87.
[Li33] F.A Lindemann, *The Unique Factorization of a Positive Integer*. Quart. J. Math. 4, 319-320, 1933.

[Mal48] A.I. Malcev, *On the embedding of group algebras in division algebras (Russian)*, Dokl. Akad. Nauk. SSSR 60 (1948), 1499–1501.

[Man58] H.B. Mann, *On integral bases*. Proc. Amer. Math. Soc. 9 (1958), 167–172.

[Mar71] C.F. Martin, *Unique factorization of arithmetic functions*. Aequationes Math. 7 (1971), 211.

[M] H. Matsumura, *Commutative ring theory*. Translated from the Japanese by M. Reid. Second edition. Cambridge Studies in Advanced Mathematics, 8. Cambridge University Press, Cambridge, 1989.

[Ma44] K. Matusita, *Über ein bewertungstheoretisches Axiomensystem für die Dedekind-Noethersche Idealtheorie*. Jap. J. Math. 19 (1944), 97–110.

[McC76] J. McCabe, *A Note on Zariski's Lemma*. Amer. Math. Monthly 83 (1976), 560–561.

[Mi] J.W. Milnor, *Topology from the differentiable viewpoint*. Based on notes by David W. Weaver. The University Press of Virginia, Charlottesville, Va. 1965.

[Mo49] T. Motzkin, *The Euclidean algorithm*. Bull. Amer. Math. Soc. 55 (1949), 1142-1146.

[Nag57] M. Nagata, *A remark on the unique factorization theorem*. J. Math. Soc. Japan 9 (1957), 143–145.

[Nag68] M. Nagata, *A type of subrings of a noetherian ring*. J. Math. Kyoto Univ. 8 (1968), 465-467.

[Nag78] M. Nagata, *On Euclid algorithm. C. P. Ramanujama tribute*, pp. 175–186, Tata Inst. Fund. Res. Studies in Math., 8, Springer, Berlin-New York, 1978.

[Nag85] M. Nagata, *Some remarks on Euclid rings*. J. Math. Kyoto Univ. 25 (1985), 421-422.

[Nag05] A.R. Naghipour, *A simple proof of Cohen's theorem.* Amer. Math. Monthly 112 (2005), 825-826.

[Nak53] N. Nakano, *Idealtheorie in einem speziellen unendlichen algebraischen Zahlkörper*. J. Sci. Hiroshima Univ. Ser. A. 16: 425-439.

[Nar95] W. Narkiewicz, *A Note on Elasticity of Factorizations*. J. Number Theory 51 (1995), 46–47.

[Neum49] B.H. Neumann, *On ordered division rings*. Trans. Amer. Math. Soc. 66 (1949), 202–252.

[Neus07] M.D. Neusel, *Invariant theory*. Student Mathematical Library, 36. American Mathematical Society, Providence, RI, 2007.

[No21] E. Noether, *Idealtheorie in Ringberereichen*. Math. Ann. 83 (1921), 24–66.

[No26] E. Noether, *Der Endlichkeitsatz der Invarianten endlicher linearer Gruppen der Charakteristik p*. Nachr. Ges. Wiss. Gttingen: 2835.

[NT] P.L. Clark, *Number Theory: A Contemporary Introduction*. `http://www.math.uga.edu/∼pete/4400FULL.pdf`

[O74] T. Ogoma, *On a problem of Fossum*. Proc. Japan Acad. 50 (1974), 266–267.

[Ol69a] J.E. Olson, *A combinatorial problem on finite Abelian groups. I.* J. Number Theory 1 (1969), 8-10.

[Ol69b] J.E. Olson, *A combinatorial problem on finite Abelian groups. II.* J. Number Theory 1 (1969), 195-199.

[Pa59] Z. Papp, *On algebraically closed modules*. Publ. Math. Debrecen 6 (1959), 311-327.

[Pe04] H. Perdry, *An elementary proof of Krull's intersection theorem.* Amer. Math. Monthly 111 (2004), 356-357.

[P] A. Pfister, *Quadratic forms with applications to algebraic geometry and topology*. London Mathematical Society Lecture Note Series, 217. Cambridge University Press, Cambridge, 1995.

[Que96] C.S. Queen, *Factorial domains*. Proc. Amer. Math. Soc. 124 (1996), no. 1, 11–16.

[Qui76] D. Quillen, *Projective modules over polynomial rings*. Invent. Math. 36 (1976), 167-171.

[Ra30] J.L. Rabinowitsch, *Zum Hilbertschen Nullstellensatz*. Math. Ann. 102 (1930), 520.

[R] M. Reid, *Undergraduate commutative algebra*. London Mathematical Society Student Texts, 29. Cambridge University Press, Cambridge, 1995.

[Rob67] A. Robinson, *Non-standard theory of Dedekind rings*. Nederl. Akad. Wetensch. Proc. Ser. A 70=Indag. Math. 29 (1967), 444–452.

[Roi93] M. Roitman, *Polynomial extensions of atomic domains*. J. Pure Appl. Algebra 87 (1993), 187-199.

[Ros76] M. Rosen, *Elliptic curves and Dedekind domains*. Proc. Amer. Math. Soc. 57 (1976), 197–201.

[Rot] J.J. Rotman, *An introduction to homological algebra*. Second edition. Universitext. Springer, New York, 2009.

[Rü33] W. Rückert, *Zum Eliminationsproblem der Potenzreihenideale*, Math. Ann. 107 (1933), 259–281.

[Ru87] W. Rudin, *Real and complex analysis*. Third edition. McGraw-Hill Book Co., New York, 1987.

[Sa61] P. Samuel, *On unique factorization domains*. Illinois J. Math. 5 (1961), 1–17.

[Sa64] P. Samuel, *Lectures on unique factorization domains*. Notes by M. Pavaman Murthy. Tata Institute of Fundamental Research Lectures on Mathematics, No. 30 Tata Institute of Fundamental Research, Bombay 1964.

[Sa68] P. Samuel, *Unique factorization*. Amer. Math. Monthly 75 (1968), 945–952.

[Sa71] P. Samuel, *About Euclidean rings*. J. Algebra 19 (1971), 282-301.

[S] W. Scharlau, *Quadratic and Hermitian forms*. Grundlehren der Mathematischen Wissenschaften 270. Springer-Verlag, Berlin, 1985.

[Sc45] T. Schönemann, *Grundzüge einer allgemeinen Theorie der höhern Congruenzen, deren Modul eine reelle Primzahl ist*. J. Reine Angew. Math. 31 (1845) 269-325.

[Sc46] T. Schönemann, *Von denjenigen Moduln, welche Potenzen von Primzahlen sind*. J. Reine Angew. Math. 32 (1846), 93-105.

[Se56] A. Seidenberg, *Some remarks on Hilbert's Nullstellensatz*. Arch. Math. (Basel) 7 (1956), 235-240.

[Si86] J. Silverman, *The Arithmetic of Elliptic Curves*, Graduate Texts in Mathematics 106, Springer Verlag, 1986.

[ST42] A.H. Stone and J.W. Tukey, *Generalized "sandwich" theorems*. Duke Math. J. 9 (1942), 356-359.

[Su11] B. Sury, *Uncountably Generated Ideals of Functions*. College Math. Journal 42 (2011), 404–406.

[Su76] A.A. Suslin, *Projective modules over polynomial rings are free*. Dokl. Akad. Nauk SSSR 229 (1976), 1063-1066.

[Sw62] R.G. Swan, *Vector bundles and projective modules*. Trans. Amer. Math. Soc. 105 (1962), 264-277.

[Sw69] R.G. Swan, *Invariant rational functions and a problem of Steenrod*. Invent. Math. 7 (1969), 148-158.

[Te72] G. Terjanian, *Dimension arithmétique d'un corps*. J. Algebra 22 (1972), 517-545.

[Tr88] H.F. Trotter, *An overlooked example of nonunique factorization*. Amer. Math. Monthly 95 (1988), no. 4, 339–342.

[Va90] R.J. Valenza, *Elasticity of factorizations in number fields*. J. Number Theory 36 (1990), 212–218.

[vdW39] B.L. van der Waerden, *Einftihrung in die algebraische Geometrie*, Berlin, 1939.

[Wa] R.B. Warfield, Jr., *Rings whose modules have nice decompositions*. Math. Z. 125 (1972) 187-192.

[Wed07] J.H.M. Wedderburn, *On Hypercomplex Numbers*. Proc. of the London Math. Soc. 6 (1907), 77118.

[W] C.A. Weibel, *An introduction to homological algebra*. Cambridge Studies in Advanced Mathematics, 38. Cambridge University Press, Cambridge, 1994.

[Wel80] R.O. Wells Jr., *Differential analysis on complex manifolds*. Second edition. Graduate Texts in Mathematics, 65. Springer-Verlag, New York-Berlin, 1980.

[Zak76] A. Zaks, *Half factorial domains*. Bull. Amer. Math. Soc. 82 (1976), 721-723.

[Zar47] O. Zariski, *A new proof of Hilbert's Nullstellensatz*. Bull. Amer. Math. Soc. 53 (1947), 362-368.

[Zas69] H. Zassenhaus, *On Hensel factorization. I*. J. Number Theory 1 (1969), 291–311.

[Ze34] E. Zermelo, *Elementare Betrachtungen zur Theorie der Primzahlen*. Nachr. Gesellsch. Wissensch. Gttingen 1, 43-46, 1934.