Algebraic Number Theory I

Pete L. Clark

Contents

CHAPTER 1

Introduction

Let us give some motivation for the main conceit of this text: that modern algebraic number theory ought to begin with the general study of Dedekind domains and their finite extensions and then specialize to the Dedekind domains that are of arithmetic interest.

Ancient number theory is the study of the integers $\mathbb{Z}$: primes, divisibility, and so forth. The Fundamental Theorem of Arithmetic is the assertion that every positive integer uniquely factors into a product of primes. Let us first reformulate this in terms of unique factorization domains (UFDs) and principal ideal domains (PIDs).

In this course, a "ring" means a ring that has a multiplicative identity, denoted by 1, and is commutative. For a ring R, we denote the set of nonzero elements by $R^\bullet$. More generally, if X is any set with a "zero element" and Y is a subset of X, by $Y^\bullet$ we mean $Y \setminus \{0\}$. For a ring R, we denote the group of units – i.e., elements $x \in R$ for which there is $y \in R$ with $xy = 1$ – by $R^\times$.

A **domain** is a nonzero ring without nonzero divisors of 0: that is, for $x, y \in R$ we have $xy = 0$ if and only if at least one of x and y is 0. Here "nonzero" means that we exclude the ring with a single element $0 = 1$.

EXERCISE 1.1. *For a nonzero ring R, show that the following are equivalent:*

(i) *R is a domain.*

(ii) *The set $R^\bullet$ of nonzero elements of R is a submonoid of the multiplicative monoid $(R, \cdot)$.*

(iii) *For all $x \in R^\bullet$, the map $x\bullet : R \to R$ given by $y \mapsto xy$ is injective.*

Every domain has a fraction field K: it is characterized as being a field K containing R with the property that every nonzero element of K of the form $\frac{x}{y}$ for $x, y \in R^\bullet$. Later we will have occasion to review the construction of the fraction field of a domain as a warmup to the more general concept of localization.

An **ideal** in a ring R is a subset I of R that is a subgroup of the additive group $(R, +)$ and such that for all $x \in R$ and $y \in I$ we have $xy \in I$. An ideal I of R is **prime** if $I \subsetneq R$ and for all $x, y \in R$, if $xy \in I$ then at least one of x, y lies in I. Equivalently, I is prime if and only if the quotient ring R/I is a domain. An ideal $\mathfrak{m}$ of R is called **maximal** if it is maximal among *proper* ideals of R: that is $\mathfrak{m} \subsetneq R$ and there is no ideal I of R with $\mathfrak{m} \subsetneq I \subsetneq R$. Equivalently, I is maximal if and only if the quotient ring $R/\mathfrak{m}$ is a field. A standard Zorn's Lemma argument shows that any proper ideal in a ring is contained in at least one maximal ideal.

For $x \in R$, we define

$$(x) \coloneqq \{ax \mid a \in R\}.$$

Then (x) is an ideal of R, called **principal**.

More generally, if $x_1, \ldots, x_n$ is any finite sequence of elements in R, then

$$\langle x_1, \ldots, x_n \rangle \coloneqq \{a_1 x_1 + \ldots + a_n x_n \mid a_1, \ldots, a_n \in R\}$$

is an ideal of R, called the **ideal generated by** $x_1, \ldots, x_n$. (It is indeed the unique minimal ideal containing $x_1, \ldots, x_n$ in the sense that if I is any ideal containing $x_1, \ldots, x_n$, then $I \supseteq \langle x_1, \ldots, x_n \rangle$.) More generally yet, for any subset S of R, the set $\langle S \rangle$ of finite R-linear combinations of elements of S is an ideal of R, called the **ideal generated by** S.

For ideals I, J of R, the product IJ is the ideal generated by all pairwise products xy with $x \in I$ and $y \in J$. More precisely it is the set of all finite sums $x_1 y_1 + \ldots + x_n y_n$ with $x_1, \ldots, x_n \in I$ and $y_1, \ldots, y_n \in J$.

EXERCISE 1.2. *Let R be a ring, and let $x, y \in R$ be such that $(x) = (y)$.*

a) *Suppose R is a domain. Show: there is a unit $u \in R^\times$ such that $y = ux$.*

b) *Find an example of a ring R and $x, y \in R$ such that there is no $u \in R^\times$ for which $y = ux$.*
(Examples are not so easy to come by. You may wish to consult `https://math.stackexchange.com/questions/355994`*.)*

We say that the ring R is **principal** or a **principal ideal ring** if every ideal of R is principal. A **principal ideal domain (PID)** is indeed a principal ideal ring that is also a domain.

EXERCISE 1.3.

a) *Show: the ring $\mathbb{Z}$ is a PID.*
(Suggestion: for a nonzero ideal I in $\mathbb{Z}$ we may choose $x \in I$ such that $|x|$ is minimal among all nonzero elements of I. Show: $I = (x)$.)

b) *Let k be a field. Show: the polynomial ring $k[t]$ is a PID.*
(Suggestion: for a nonzero ideal I in $k[t]$ we may choose $f \in I$ such that $\deg f$ is minimal among all nonzero elements of I. Show $I = (f)$.)

An **ascending chain** of ideals in a ring R is an infinite sequence of ideals

$$I_1 \subsetneq I_2 \subsetneq \ldots \subsetneq I_n \subsetneq \ldots.$$

We say that R satisfies the **ascending chain condition on principal ideals (ACCP)** if there is no ascending chain of principal ideals. We observe that any principal ideal ring satisfies ACCP: indeed, if we had an ascending chain

$$(a_1) \subsetneq (a_2) \subsetneq \ldots \subsetneq (a_n) \subsetneq \ldots$$

then the union

$$I \coloneqq \bigcup_{n \geq 1} (a_n)$$

is an ideal of R (indeed the union of any ascending chain of ideals in a ring is an ideal of the ring) that cannot be principal: if $I = (a)$ then we must have $a \in (a_N)$ for some $N \in \mathbb{Z}^+$ and then we have $(a_n) = (a)$ for all $n \geq N$.

An element x in a domain R is **irreducible** if x is neither 0 nor a unit and whenever we have $x = yz$ for $y, z \in R$ then one of y, z is a unit (indeed exactly one; if both were units, then x would be a unit). Notice that for positive elements of the ring $\mathbb{Z}$ this coincides with the classical deifnition of "prime number." However, this terminology obscures a key distinction. Namely, we say that $p \in R^\bullet$ is a **prime element** if (p) is a prime ideal. To spell this out, it means that for all $x, y \in R$, if $p \mid xy$, then $p \mid x$ or $p \mid y$. In any domain, prime elements are irreducible: if $p = xy$ then $p \mid x$ or $p \mid y$; if $p \mid x$ then there is $a \in R$ such that $x = ap$ and then $p = xy = apy$; cancelling p (as we may since R is a domain) gives $1 = ay$, so $y \in R^\times$. Symmetrically, if $p \mid y$ then $x \in R^\times$. The more interesting question is whether an irreducible element is necessarily prime: in the ring $\mathbb{Z}$, the assertion that an irreducible element ("prime number") is a prime eleement – i.e., if a prime number p divides xy then p divides x or p divides y – is called **Euclid's Lemma** and is the lion's share of the proof of the Fundamental Theorem of Arithmetic. Here is a generalization of this:

PROPOSITION 1.1. *In a PID, irreducible elements are prime.*

PROOF. Let p be an irreducible element of the PID R, and suppose that $p \mid xy$ and $p \nmid x$. Then

$$\langle p, x \rangle = \{ap + bx \mid a, b \in R\}$$

is an ideal of the PID R, so there is $u \in R$ such that $\langle p, x \rangle = (u)$. In particular u divides both p and x. But in any domain, a divisor of an irreducible element p is either a unit or a unit times p. If u were a unit times p, then u divides exactly what p divides, so u does not divide x: contradiction. So u is a unit, meaning $(u) = R$. Thus we have shown that there $a, b \in R$ such that $ap + bx = 1$. Multiplying by y we get

$$apy + bxy = y.$$

Since p divides both apy and bxy, p divides the left hand side, so $p \mid y$, as desired. □

A **unique factorization domain** is a domain R satisfying:
(UFD1) For every nonzero nonunit $a \in R$, there are irreducibles $b_1, \ldots, b_r$ such that $a = b_1 \cdots b_r$; and
(UFD2) If $b_1, \ldots, b_r, c_1, \ldots, c_s$ are irreducibles such that

$$b_1 \cdots b_r = c_1 \cdots c_s$$

then $r = s$, and there is a bijection $\sigma : \{1, \ldots, r\} \to \{1, \ldots, r\}$ such that for all $1 \leq i \leq r$ we have

$$(b_i) = (c_{\sigma(i)}).$$

In other words, a UFD is a domain in which every nonzero nonunit factors as a product of irreducibles and for which this factorization is as unique as makes sense in this contextd, namely up to reordering the irreducible elements and multiplying them by unit factors.

Here is another way of phrasing it that may be a bit more elegant: let us say that an atom of a domain R is an ideal that is generated by an irreducible element. Then R is a UFD if and only if every proper, nonzero principal ideal of R factors as a product of atoms, uniquely up to the order. Anyway, here is a characterization of UFDs that is often useful:

PROPOSITION 1.2. *A domain R is a UFD if and only if R satisfies the ascending chain condition on principal ideals and every irreducible element of R is pirme.*

EXERCISE 1.4. *Prove Proposition 1.2.*

THEOREM 1.3. *A PID is a UFD.*

PROOF. Indeed we showed that PIDs satisfy (ACCP) and that irreducible elements in PIDs are prime. □

There is a reason that one learns about PIDs in any first graduate course in algebra: they are a thoroughly pleasant class of rings. In particular, there is a wonderful structure theorem for finitely generated modules over a PID: every finitely generated module over a PID is a direct sum of *cyclic* modules and thus a direct sum of modules in which each summand is isomorphic either to R or to $R/(p^a)$ for some prime element p of R and some $a \in \mathbb{Z}^+$. However there are both number-theoretic and algebraic reasons to move beyond PIDs. On the number theory side, many natural Diophantine equations are best attacked by considering the arithmetic of certain "higher rings of integers" that need not be UFDs. Here are two examples:

• Let $N \in \mathbb{Z}^+$ be squarefree such that $N \equiv 1, 2 \pmod 4$. Suppose one wishes to consider the prime numbers p repesented by the quadratic form

$$q_N(x, y) := x^2 + Ny^2.$$

We say that q_N **represents** an integer n if there are $x, y \in \mathbb{Z}$ such that $q_N(x, y) = n$.

EXERCISE 1.5. *Let p be a prime that does not divide $-4N$. Show: if $q_N := x^2 + Ny^2$ represents p, then $\left(\frac{-N}{p}\right) = 1$, i.e., $-N$ is a nonzero square modulo p.*

Thus for instance, taking $N = 1$, we see that if an odd prime p is represented by $x^2 + y^2$, then -1 is a square modulo p; equivalently, $p \equiv 1 \pmod 4$ (this is the "First Supplement to the Quadratic Reciprocity Law" that one should learn in an undergraduate number theory course; let's assume it for now). The celebrated Two Squares Theorem of Fermat asserts that conversely every prime $p \equiv 1 \pmod 4$ is represented by x^2+y^2. This result is easy to prove if we know that the ring $\mathbb{Z}[\sqrt{-1}]$ is a UFD:

EXERCISE 1.6. *Suppose that the ring $\mathbb{Z}[\sqrt{-1}]$ is a UFD, and let $p \equiv 1 \pmod 4$.*

a) *Using the First Supplement to QR, show that there are $n, x \in \mathbb{Z}$ such that $np = x^2 + 1$.*

b) *Using the factorization $x^2 + 1 = (x + \sqrt{-1})(x - \sqrt{-1})$, show that p is not a prime element of $\mathbb{Z}[\sqrt{-1}]$.*

c) *Since $\mathbb{Z}[\sqrt{-1}]$ is a UFD, it follows that there are nonunits $\alpha, \beta \in \mathbb{Z}[\sqrt{-1}]$ such that $p = \alpha\beta$. Show that an element $\gamma = a + b\sqrt{-1}$ of $\mathbb{Z}[\sqrt{-1}]$ is a unit if and only if $a^2 + b^2 = 1$. Deduce that $|\alpha| = |\beta| = \sqrt{p}$ and that therefore p is represented by $x^2 + y^2$.*

EXERCISE 1.7. *Show: $\mathbb{Z}[\sqrt{-1}]$ and $\mathbb{Z}[\sqrt{-2}]$ are PIDs.*

On the other hand:

EXERCISE 1.8. *Let N be an integer such that $-N$ is not a square.*

a) *Let p be a prime number such that $-N$ is a square modulo p. Show: if $\mathbb{Z}[\sqrt{-N}]$ is a UFD, then there are $x, y \in \mathbb{Z}$ such that $x^2 + Ny^2 = p$.*

b) *Suppose $N \geq 3$. Observe that* there are no $x, y \in \mathbb{Z}$ *such that* $x^2+Ny^2 = 2$, *and deduce that* $\mathbb{Z}[\sqrt{-N}]$ *is* not *a UFD.*

Thus in addressing Diophantine equations via "higher integer rings," one must deal with the fact these rings need not be (and in certain regimes very much tend not to be) UFDs. Once one develops tools for dealing with more general rings, the story can continue: indeed, for the equation $x^2 + Ny^2 = p$ with $N \in \mathbb{Z}^+$, this story is the subject of an entire book [**Co**]. Here is one of the main results:

THEOREM 1.4. *For $N \in \mathbb{Z}^+$, let $\mathcal{S}_N$ be the set of prime numbers p represented by $x^2 + Ny^2$.*

a) *The relative density of $\mathcal{S}_N$ within the set of prime numbers is positive:*

$$\lim_{X\to\infty} \frac{\#\{p \in \mathcal{S}_N \mid p \leq X\}}{\#\{\text{primes } p \leq X\}} = \lim_{X\to\infty} \frac{\#\{p \in \mathcal{S}_N \mid p \leq X\}}{X/\log X} > 0.$$

b) *There is a finite commutative group $G_N := \operatorname{Pic} \mathbb{Z}[\sqrt{-N}]$ attached to the ring $\mathbb{Z}[\sqrt{-N}]$ such that the relative density of part a) is precisely $\frac{1}{2\#G_N}$.*

For another example, let $k \in \mathbb{Z}^+$ be such that $-k$ is not a square, and consider the **Mordell Equation**:

$$y^2 + k = x^3.$$

Then the left hand side factors over $\mathbb{Z}[\sqrt{-k}]$ as $(y + \sqrt{-k})(y - \sqrt{-k})$. Let us first suppose that $k = 1$, in which case we know that $\mathbb{Z}[\sqrt{-1}]$ is a PID hence a UFD. In any UFD we say that two nonzero elements are **coprime** if no nonunit divides both of them. One can show that if $y^2+1 = x^3$, then the elements $y+\sqrt{-1}$ and $y-\sqrt{-1}$ of $\mathbb{Z}[\sqrt{-1}]$ are coprime (cf. Exercise A.A). For $n \in \mathbb{Z}^{\geq 2}$ if we have coprime elements a, b of a UFD R such that $ab = z^n$ is an nth power, then there are $u_a, u_b \in R^\times$ and $A, B \in R$ such that $a = u_a A^n$ and $b = u_b B^n$. In $\mathbb{Z}[\sqrt{-1}]$ every unit is a cube, so if $y^2 + 1 = x^3$ then there are $\alpha, \beta \in \mathbb{Z}[\sqrt{-1}]$ such that

$$y + \sqrt{-1} = A^3 \text{ and } y - \sqrt{-1} = B^3.$$

This is a very strong condition, and it leads rather quickly to the fact that $(x, y) = (1, 0)$ (cf. Exercise B.B).

Suppose $k \in \mathbb{Z}^+$ is squarefree with $k \equiv 1, 2 \pmod 4$. Then it is not hard to show that if $y^2 + k = x^3$, then the ideal $\langle y + \sqrt{-k}, y - \sqrt{-k}\rangle$ of $\mathbb{Z}[\sqrt{-k}]$ is all of $\mathbb{Z}[\sqrt{-k}]$. Thus the elements $y \pm \sqrt{-k}$ are **comaximal**: $\langle y+\sqrt{-k}, y-\sqrt{-k}\rangle = \mathbb{Z}[\sqrt{-k}]$. More concretely, two elements a and b of a ring are comaximal if there are $c, d \in R$ such that $ac + bd = 1$. In a UFD if a, b are comaximal then they are certainly coprime: any element that divides both a and b must divide 1 so must be a unit. (In a general UFD being comaximal may be stronger: e.g. the polynomial ring $C[x, y]$ is a UFD and the elements x, y are coprime but not comaximal. But in a PID the two conditions coincide.)

Thus if $\mathbb{Z}[\sqrt{-k}]$ were a UFD we could run the above argument and, it turns out, use it to find all solutions to $y^2 + k = x^3$. However, as we have already seen, this only applies to $\mathbb{Z}[\sqrt{-1}]$ and $\mathbb{Z}[\sqrt{-2}]$. However, it turns out that in order to write each of $y \pm \sqrt{-k}$ as a unit times a cube, it suffices for $\mathbb{Z}[\sqrt{-k}]$ to have a weaker property: namely for any ideal I of $\mathbb{Z}[\sqrt{-k}]$, if I^3 is principal, then I is principal. We will see later that (with our conditions on k), the ring $\mathbb{Z}[\sqrt{-k}]$ is a Dedekind domain that has a finite **ideal class group** $\operatorname{Cl} \mathbb{Z}[\sqrt{-k}]$. For any $n \in \mathbb{Z}^+$ and any

Dedekind domain R, the condition that for all ideals I of R, if I^n is principal then I is principal is equivalent to the n-torsion subgroup $(\operatorname{Cl} R)[n]$ being trivial. Thus in the finite commutative group $\operatorname{Cl} \mathbb{Z}[\sqrt{-k}]$, the property that the cube of an ideal is principal implies that the ideal is principal holds if and only if the class number $\# \operatorname{Cl} \mathbb{Z}[\sqrt{-k}]$ is not divisible by 3. This condition holds for *many* integers k; conjecturally for a positive proportion.

Similarly, for $N \geq 3$ we have the famous **Fermat equation**

$$x^N + y^N = z^N.$$

Put $\zeta_N := e^{2\pi i/N}$. Then in $\mathbb{Z}[\zeta_N]$ we have $x^N + y^N = \prod_{i=0}^{-1}(x + \zeta^k y)$, so similarly one imagines that it would be helpful if $\mathbb{Z}[\zeta_N]$ were a UFD. If $N \equiv 2 \pmod 4$ then ζ_{2N} lies in the subgroup generated by ζ_N and -1, so $\mathbb{Z}[\zeta_{2N}] = \mathbb{Z}[\zeta_N]$. For $N \not\equiv 2 \pmod 4$ we have that $\mathbb{Z}[\zeta_N]$ is a UFD if and only if

$$N \in \{1, 3, 4, 5, 7, 8, 9, 11, 12, 13, 15, 16, 17, 19, 20,$$

$$21, 24, 25, 27, 28, 32, 33, 35, 36, 40, 44, 45, 48, 60, 84\}.$$

However, again the ring $\mathbb{Z}[\zeta_N]$ is a Dedekind domain with finite class group, and already in 1847 Kummer showed that if the class number of $\mathbb{Z}[\zeta_p]$ is not divisible by p – such primes are called **regular** and admit a more elementary characterization in terms of Bernoulli numbers – then the Fermat equation $x^p + y^p = z^p$ has no integer solutions with $xyz \neq 0$. (The details of this are significantly more complicated than for the Mordell Equation considered above.) Siegel conjectured that the relative asymptotic density of the set of regular primes is $e^{\frac{-1}{2}} \approx .6065$. In fact it is known that there are infinitely many irregular primes, not known that there are infinitely many regular primes, and – thanks to work of Wiles, Taylor and Ribet in the early 1990's – that for all $N \geq 3$ the Fermat Equation has no integer solutions with $xyz \neq 0$, but still: not bad for the 1847!

1. Introducing Dedekind Domains

As we hoped to indicate in the previous section, once we are given a PID we are just about maximally pleased, but the issue is that the condition of a domain to be a PID is in many respects too delicate. Moreover, in number theory one naturally wants to pass to certain "extensions" of the domain that one is given, but the class of PIDs does not behave at all well under this extension process.

Before we dial in on this, let us further clarify the connection between PIDs and UFDs. As we know, every PID is a UFD. The converse is certainly not true: a well-known result essentially going back to Gauss shows that if R is a UFD then so is the polynomial ring $R[t]$, so for instance since $\mathbb{C}[x]$ is a PID, the ring $\mathbb{C}[x, y] = (\mathbb{C}[x])[y]$ is a UFD, and it is easy to see that the ideal $\langle x, y\rangle$ is not prinicpal: x and y are not both multiples of any nonconstant polynomial. The criterion for when a UFD is a PID involves the concept of Krull dimension. A ring R is said to have finite Krull dimension if there is some $d \in \mathbb{N}$ such that for every ascending chain

$$\mathfrak{p}_0 \subsetneq \mathfrak{p}_1 \subsetneq \ldots \subsetneq \mathfrak{p}_n$$

of prime ideals of R, we have $n \leq d$, and in this case the least such d is called the **Krull dimension**. Alternately, for every prime ideal $\mathfrak{p}$ of R, the **height** of $\mathfrak{p}$ is the maximum of lengths of ascending chains of prime ideals terminating at $\mathfrak{p}$, assuming

this maximum exists; otherwise $\mathfrak{p}$ is said to have infinite height. Then the Krull dimension is the maximum of the heights of its prime ideals, again assuming this maximum exists.

In truth, although we wanted to give the general definitions of dimension and height, in our course we only need to look at rings of dimension 0 and 1. A ring has dimension 0 if there are no proper containments among prime ideals. Since in a domain the zero ideal is prime and evidently contained in every other prime ideal, a domain has dimension zero if and only if it is a field. Similarly, a domain has Krull dimension 1 if every nonzero prime ideal is maximal. Now here is the desired result.

THEOREM 1.5. *For a UFD R, the following are equivalent:*

(i) *R is a PID.*
(ii) *R has dimension at most 1.*

PROOF. (i) $\implies$ (ii): Let R be a PID that is not a field. Then every nonzero prime ideal of R is generated by a prime element p. For prime elements p and q, it is not possible to have $(p) \subsetneq (q)$: indeed, if $(p) \subseteq (q)$ then $p = aq$ for some $a \in R$; since p is prime it is irreducible, and thus $a \in R^\times$ and $(p) = (q)$. Thus there is no proper containment among nonzero ideals of R, so R has dimension 1.
(ii) $\implies$ (i): Since a field is a PID, we may assume that R is a one-dimensional UFD. Let $\mathfrak{p}$ be a nonzero prime ideal of R, and let $x \in \mathfrak{p}^\bullet$ be a nonzero element. Then x is a finite product of prime elements and $\mathfrak{p}$ is a prime ideal, so $\mathfrak{p}$ contains some prime element p: thus we have a containment of prime ideals $(0) \subsetneq (p) \subseteq \mathfrak{p}$, and because R has dimension 1 we must have $\mathfrak{p} = (p)$. That is, every nonzero prime ideal of R is principal; the zero ideal is also principal, so every prime ideal is principal. By a result of Cohen [**CA**, Thm. 4.32], this implies that R is a PID. □

Now we come to one of the key definitions, which is a generalization of the passage from $\mathbb{Z}$ to rings like $\mathbb{Z}[\sqrt{N}]$ and $\mathbb{Z}(\zeta_N)$. Let $R \subseteq T$ be an extension of rings. An element x of T is **integral over R** if there is a monic polynomial

$$p(t) = t^n + a_{n-1}t^{n-1} + \ldots + a_1 t + a_0 \in R[t]$$

such that $p(x) = 0$. Thus for instance the complex number $\sqrt{N}$ is integral over $\mathbb{Z}$ because it satisfies the monic polynomial equation $t^2 - N = 0$ and the complex number ζ_N is integral over $\mathbb{Z}$ because it satisfies the monic polynomial equation $t^N - 1 = 0$. We say that an extension of rings $R \subseteq T$ is an **integral extension** if every element of T is integral over R. When R is a field, any nozero polynomial equation can be rescaled to give a monic polynomial equation, so a field extension L/K is integral precisely when it is **algebraic**. It turns out that for any extension $R \subseteq T$ of rings, the set $I_T(R)$ of elements of T that are integral over R is a subing of T (clearly containing R; every $x \in R$ is a root of the polynomial $t - x$) that is caled the **integral closure of R in T**.

EXAMPLE 1.6.

a) *The integral closure of $\mathbb{Q}$ in $\mathbb{C}$ is $\overline{\mathbb{Q}}$, the field of all algebraic numbers. In general, the algebraic closure of a field in an algebraically closed extension field is algebraically closed.*

b) *The integral closure of $\mathbb{Z}$ in $\mathbb{C}$ is denoted $\overline{\mathbb{Z}}$ and is called the ring of all algebraic integers. All of the "higher rings of integers" we saw above are subrings of $\overline{\mathbb{Z}}$.*

c) *The integral closure of $\mathbb{Z}$ in $\mathbb{Q}$ is just $\mathbb{Z}$. Indeed, let $x = \frac{a}{b}$ be a nonzero rational number, written in lowest terms and that $p(x) = 0$ where*

$$p(t) = t^n + a_{n-1}t^{n-1} + \ldots + a_1 t + a_0 \in \mathbb{Z}[t].$$

Plugging in x and clearing denominators, we get

$$a^n + ba_{n-1}a^{n-1} + \ldots + b^{n-1}a_1 a + b^n a_0 = 0.$$

Bringing a^n to the other side we see that $b \mid a^n$. If b were not ± 1, then it would be divisible by some prime number p, and then $p \mid a^n$, hence $p \mid a$, and the fraction $\frac{a}{b}$ has both numerator and denominator divisible by p so is not in lowest terms, contradiction.

d) *The integral closure of $\mathbb{Z}$ in $\mathbb{Q}(\sqrt{-1})$ is $\mathbb{Z}[\sqrt{-1}]$. This is* not *obvious. It's clear that $\sqrt{-1}$ is integral over $\mathbb{Z}$ – it satisfies the polynomial $t^4 - 1$ – and since the set of elements that are integral over $\mathbb{Z}$ form a $\mathbb{Z}$-subalgebra, it follows that every element of $\mathbb{Z}[\sqrt{-1}]$ is integral over $\mathbb{Q}$, but we still need to show that no other elements of $\mathbb{Q}[\sqrt{-1}]$ are integral over $\mathbb{Z}$.*

e) *The integral closure of $\mathbb{Z}$ in $\mathbb{Q}(\sqrt{-5})$ is* not *$\mathbb{Z}[\sqrt{-5}]$. Indeed, it is clear that $\mathbb{Z}[\sqrt{-5}]$ is* an *integral extension of $\mathbb{Z}$, but how do we know that no other elements of $\mathbb{Q}(\sqrt{-5})$ is integral over $\mathbb{Z}$? In fact, the golden ratio*

$$\varphi := \frac{1 + \sqrt{5}}{2}$$

is integral over $\mathbb{Z}$, since it satisfies the polynomial $t^2 - t - 1$. Please first check that this is true and then remind yourself of the high school algebra needed to find this polynomial. This is an important cautionary tale: integral elements can "have denominators."

Let R be a domain with fraction field K. We say that R is **integrally closed** if its integral closure in K is R itself, i.e., every element of K that satisfies a monic polynomial equation with coefficients in R already lies in R.

PROPOSITION 1.7. *A UFD is integrally closed.*

EXERCISE 1.9. *Prove it.*
(Hint: the proof we gave that $\mathbb{Z}$ is integrally closed really works in any UFD.)

Wouldn't it be nice if after taking the integral closure we always got something integrally closed? Just because the terminology suggests something doesn't make it true,[1] and there is something to show here: essentially that being integral over an integral extension of a ring R is the same as being integral over R. It is indeed true that if $A \subseteq B \subseteq C$ are ring extensions, B is integral over A and C is integral over B, then C is integral over A [**CA**, Cor. 14.5], and indeed that implies the desired fact [**CA**, Cor. 14.11]:

THEOREM 1.8. *Let A be a domain with fraction field K, let L/K be any field extension, and let B be the integral closure of A in L. Then B is integrally closed.*

[1] At the end of [**CA**, Chapter 14] I discuss the concept of **complete integral closure** and **completely integrally closed domains**. It is unfortunately *not* the case that when one takes the complete integral closure, one necessarily gets something that is completely integrally closed!

PROOF. See [**CA**, Cor. 14.11]. □

We can now make the most important definition of classical algebraic number theory: let K be a number field; that is, a finite-degree field extension of $\mathbb{Q}$. Note that we are in characteristic 0, so the Primitive Element Theorem applies here: every K is of the form $\mathbb{Q}[t]/(f)$ for an irreducible polynomial $f \in \mathbb{Q}[t]$. We define the **ring of integers of** K to be the integral closure of $\mathbb{Z}$ in K and denote it $\mathbb{Z}_K$. Note that we have $\mathbb{Z}_K = K \cap \overline{\mathbb{Z}}$.

Okay, let me spoil things a bit, for clarity:

THEOREM 1.9.

a) *Let d be an integer that is squarefree, not a square, and congruent to 2 or 3 modulo 4. Then the ring of integers of $\mathbb{Q}(\sqrt{d})$ is $\mathbb{Z}[\sqrt{d}]$.*
b) *Let d be an integer that is squarefree, not a square and congruent to 1 modulo 4. Then the ring of integers of $\mathbb{Q}(\sqrt{d})$ is $\mathbb{Z}[\frac{\sqrt{d}+1}{2}]$.*
c) *Let $N \in \mathbb{Z}^+$. Then the ring of integers of $\mathbb{Q}(\zeta_N)$ is $\mathbb{Z}[\zeta_N]$.*

Thus the concept of integral closure is what is taking us from the PID $\mathbb{Z}$ to the sort of "higher rings of integers" that intervene (for instance!) when one is studying certain Diophantine equations. More precisely, some of the higher rings of integers we considered were proper subrings of $\mathbb{Z}_K$ with fraction field K that are not the full ring of integers $\mathbb{Z}_K$ of K. This is actually related to the failure of $\mathbb{Z}[\sqrt{-N}]$ to be a UFD for certain values of $N \geq 3$. Namely, if $N \equiv 3 \pmod 4$ then $-N \equiv 1 \pmod 4$, so the element $\frac{\sqrt{N}+1}{2} \in \mathbb{Q}(\sqrt{N})$ is integral over $\mathbb{Z}[\sqrt{-N}]$ but does not lie in $\mathbb{Z}[\sqrt{-N}]$, so $\mathbb{Z}[\sqrt{-N}]$ is not integrally closed and therefore cannot be a UFD. The word for this kind of subring is **nonmaximal order** and we will come back to it later. But if N is squarefree and congruent to 1 or 2 modulo 4 then $\mathbb{Z}[\sqrt{-N}] = \mathbb{Z}_{\mathbb{Q}(\sqrt{-N})}$ and still we saw that it is not a UFD, so being integrally closed is necessary but not sufficient for a domain to be a UFD.

Next I want to mention some important and general "spectral properties" of integral extensions. For a ring R, let $\operatorname{Spec} R$ be the set of prime ideals of R and let $\operatorname{MaxSpec} R$ be the set of maximal ideals of R. If $\iota : R \to T$ is a ring homomorphism and $\mathcal{P}$ is a prime ideal of T, it is easy to see that

$$\iota^*(\mathcal{P}) \coloneqq \iota^{-1}(\mathcal{P})$$

is always a prime ideal of R. In general though if $\mathcal{P}$ is maximal, then $\iota^{-1}(\mathcal{P})$ need not be maximal: e.g. take $\iota : \mathbb{Z} \hookrightarrow \mathbb{Q}$ be the natural inclusion map. Since $\mathbb{Q}$ is a field, the zero ideal (0) is maximal; its inverse image in $\mathbb{Z}$ is just the zero ideal (0) of $\mathbb{Z}$, which is prime but not maximal. However:

THEOREM 1.10. *Let $R \subseteq T$ be an integral extension of rings.*

a) *The map $\iota^* : \operatorname{Spec} T \to \operatorname{Spec} R$ by $\mathcal{P} \mapsto \mathcal{P} \cap R$ is surjective.*
b) *For $\mathcal{P} \in \operatorname{Spec} T$, the ideal $\mathcal{P}$ is maximal if and only if the ideal $\mathcal{P} \cap R$ is maximal.*
c) *R has finite Krull dimension if and only if T has finite Krull dimension, and if so the Krull dimension of R is equal to the Krull dimension of T.*

Since $\mathbb{Z}$ is a PID that is not a field, it has dimension 1, so by the previous theorem so does $\mathbb{Z}_K$ for any number field K. Thus $\mathbb{Z}_K$ is a one-dimensional integrally closed

domain. We are getting close to the definition of a Dedekind domain. To get a hint of what is missing, consider the ring $\overline{\mathbb{Z}}$ of all algebraic integers. For exactly the same reasons discussed above, this is also a one-dimensional integrally closed domain. However, I claim that not only do nonzero nonunit elements not *uniquely* factor into irreducibles in $\overline{\mathbb{Z}}$, they do not factor into irreducibles at all...because there are no irreducibles! Indeed, let x be any nonzero nonunit in $\overline{\mathbb{Z}}$. Then there is $y \in \overline{\mathbb{Q}}$ such that $y^2 = x$, and y satisfies the equation $t^2 - x = 0$, so $y \in \overline{\mathbb{Z}}$. y is certainly nonzero, and if it were a unit, then so would be $x = y^2$, so x is not irreducible.

This is striking evidence that the ring $\overline{\mathbb{Z}}$ is "too big" in a basic algebraic sense. We want to impose the single most important finiteness condition in commutative algebra: a ring R is **Noetherian** if all ideals of R are finitely generated.

EXERCISE 1.10. *Show: a ring R is Noetherian if and only if there are no ascending chains*

$$I_1 \subsetneq I_2 \subsetneq \ldots \subsetneq I_n \subsetneq$$

of ideals in R.

Earlier we worked a little bit to show that a principal ring satisfies the ascending chain condition on principal ideals (ACCP). With the preceding exercise, this is clear: in a principal ring every ideal is singly generated, hence finitely generated, hence principal rings are Noetherian, so there are no ascending chains of principal ideals, hence certainly no ascending chains of principal ideals.

EXERCISE 1.11. *A domain R is called **atomic** if every nonzero unit factors as a (finite!) product of irreducibles. (Notice that this is one of the two defining properties of a UFD).*

a) *Show: if R satisfies (ACCP), then R is atomic.*[2]
(Suggestion: whether an element x factors into irreducibles depends only on the principal ideal (x). If there are principal ideals without this property in an (ACCP) domain, there must be a maximal *such ideal...)*
b) *Deduce: the ring $\overline{\mathbb{Z}}$ is* not *Noetherian.*
c) *Exhibit an explicit ideal in $\overline{\mathbb{Z}}$ that is not finitely generated.*

We can now make the definition that begins modern algebraic number theory: a **Dedekind domain** is a Noetherian domain that is integrally closed and of Krull dimension at most one: nonzero prime ideals are maximal. This definition allows fields to be Dedekind domains...which is good, but for almost everything we are doing we are interested in Dedekind domains that are not fields: these are the integarlly closed Noetherian domains of dimension one.

Here is one thing that is clear from the definition:

PROPOSITION 1.11. *A PID is a Dedekind domain.*

PROOF. We may assume that R is a PID and not a field. As we saw, R is Noetherian and a one-dimensional UFD, hence a Noetherian, one-dimensional integrally closed domain. □

[2]The converse is not true, but this is by no means obvious. Rather it is a theorem of Grams: [**Gr74**].

Thus a Dedekind domain is a certain kind of generalization of a PID. In order to try to understand the relation, we next want to introduce a certain kind of specialization of a PID:

PROPOSITION 1.12. *For a domain R that is not a field, the following are equivalent:*

(i) *There is an element π such that every nonzero ideal of R is of the form (π^n) for a unique $n \in \mathbb{Z}^{\geq 0}$.*
(ii) *R is a local PID: that is, a PID with a unique maximal ideal.*

A ring satisfying these equivalent conditions is called a ***discrete valuation ring (DVR)****.*

PROOF. (i) $\implies$ (ii): We've assumed that all the ideals of R are principal...so R is a PID. And we've assumed that the nonzero ideals form a descending chain:

$$R = (\pi^0) \supsetneq (\pi^1) \supsetneq (\pi^2) \supsetneq \ldots \supsetneq (\pi^n) \supsetneq \ldots$$

so the unique maximal ideal is (π^1).
(ii) $\implies$ (i): To say that R is a local PID is to say that it has a unique prime element, up to units. Since every nonzero proper ideal in a PID is generated by a finite product of prime elements, every such ideal must be of the form (π^n) for some $n \in \mathbb{Z}^+$. □

Soon enough we will see that every Dedekind domain generates many examples of DVRs, but let us give some initial examples.

EXAMPLE 1.13.

a) *Let p be a prime. We denote by $\mathbb{Z}_{(p)}$ the subring of $\mathbb{Q}$ consisting of rational numbers $\frac{a}{b}$ with $a, b \in \mathbb{Z}$ and $p \nmid b$. In this ring, the units are the fractions in which (when written in lowest terms) p does not divide the numerator. The nonunits are therefore the elements divisible by p so form an ideal (p), and it is clear that every element in $\mathbb{Z}_{(p)}^\bullet$ can be written as a unit times a power of p. Now let I be any nonzero ideal of $\mathbb{Z}_{(p)}$; as above, every $x \in I^\bullet$ may be written as $u \cdot p^{(k(x)}$ with $u \in \mathbb{Z}_{(p)}^\times$ and $k(x) \in \mathbb{N}$. Let K be the minimum of $k(x)$ as x ranges over nonzero elements of I. Then $p^K \in I$ and every element of I is divisible by p^K, so $I = (p^k)$. It follows that $\mathbb{Z}_{(p)}$ is a DVR.*
b) *Let k be a field, and let $R \coloneqq k[[t]]$ be the ring of formal power series with coefficients in k: that is, elements are formal expressons $f = \sum_{n=0}^\infty a_n t^n$ with $a_n \in k$ for all $n \in \mathbb{N}$ and addition and multiplication are as in calculus. In this ring, the units are the elements with $a_0 \neq 0$. The nonunits are therefore the elements divisible by t, so form an ideal (t), and again it is clear that every element in $k[[t]]^\bullet$ can be written as a unit times a power of t. Arguing as in part a) we find that $k[[t]]$ is a DVR.*

EXERCISE 1.12. *Let k be a field, and let $k(t)$ be the field of rational functions in the indeterminate t – this is just the fraction field of the polynomial ring $k[t]$.*

a) *Let R_0 be the subring of $k(t)$ of rational functions of the form $\frac{f(t)}{g(t)}$ with $g(0) \neq 0$. Show: R_0 is a DVR with maximal ideal (t).*
b) *Let R_∞ be the subring of $k(t)$ of rational functions of the form $\frac{f(t)}{g(t)}$ with $g \neq 0$ and $\deg(f) \leq \deg(g)$. (Here we use the convention that the 0*

polynomial has degree $-\infty$.) Show: R_∞ is a DVR and find a generator of its maximal ideal.

Let R be a one-dimensional Noetherian domain that is local, with unique maximal ideal $\mathfrak{m}$. I claim that R is a Dedekind domain if and only if R is a PID. Indeed, there is a result in commutative algebra [**CA**, Thm. 17.8] that says many "nice" properties of a one-dimensional local Noetherian domain are equivalent, including: (i) R is a PID; (ii) $\mathfrak{m}$ is principal; (iii) R is integrally closed; and (iv) R is regular: $\dim_{R/\mathfrak{m}} \mathfrak{m}/\mathfrak{m}^2 = 1$. The coincidence of the last two conditions in particular is a miracle of dimension one: for any local Noetherian ring, being "regular" means that $\dim_{R/\mathfrak{m}} \mathfrak{m}/\mathfrak{m}^2 = \dim R$. Regularity is a "nonsingularity" condition of a geometric sort; it always implies integral closure ("normality"), which is a condition of a much more algebraic flavor. Starting in dimension 2, integally closed domains need *not* be regular, and this is a main source of the additional complication in the study of higher-dimensional algebraic varieties versus algebraic curves. Anyway, (i) $\iff$ (iv) establishes our claim that a local Dedekind domain is a PID.

So we have DVR $\implies$ PID $\implies$ Dedekind.

My contention is that PIDs sit somewhat awkwardly in the middle of these two classes of rings, which I will try to preliminarily explain in at least two ways. First, for any domain R with fraction field K, a **multiplicative subset** of R is a subset $S \subseteq R^\bullet$ that contains 1 and is closed under multiplication: $S \cdot S = S$. To such an S we can define a **localization** of R: a more principled and general definition will come later, but in this case $S^{-1}R$ is the subring of the fraction field K of R obtained by adjoining the inverses $\frac{1}{s}$ of the elmeents $s \in S$. (If we take $S := R^\bullet$ then we adjoin the inverses of all nonzero elements of R, so we get the fraction field. Thus we can think of localization as a sort of "partial ring of fractions" construction.) Localization is one of the fundamental operations in commutative algebra: it is equally as important as passing to quotient rings and in some ways complementary to it. Among fundamental operations in commutative algebra, localization is certainly the most benevolent.

EXERCISE 1.13. *Let R be a domain, and let $S \subseteq R^\bullet$ be a multiplicative subset. Recall $S^{-1}R := R[\frac{1}{s} \mid s \in S]$.*

a) *Show: if R is a PID, so is $S^{-1}R$.*
b) *Show: if R is a UFD, so is $S^{-1}R$.*

Also if R is a Dedekind domain, then so is every localization $S^{-1}R$. This is an example of the benevolence of localization: (i) the localization of a Noetherian ring is Noetherian; (ii) the localization of an integrally closed domain is integrally closed (and this is true because being integrally closed is in a certain sense a local property), and (iii) localization preserves or decreases Krull dimension. So if all of UFDs, PIDs and Dedekind domains behave well under localization, what's the issue?

There is a special kind of localization that is especially important: for an ideal I of a domain R, I looks like a multiplicative subset: it is certainly closed under multiplication. However, our definition of multiplicative subset excluded 0: we do not want 0 as a denominator. (The more general definition of localization in a ring

that is not a domain does allow the presence of 0, but if $0 \in S$ then in $S^{-1}R$ we have $0 = 1$: it is the zero ring.) However, the complement $R \setminus I$ is a multiplicative subset if and only if I is a prime ideal, so for a prime ideal $\mathfrak{p}$ of R, we denote by $R_{\mathfrak{p}}$ the localization at $S := R \setminus \mathfrak{p}$: that is, we allow every element of R lying *outside* of $\mathfrak{p}$ to serve as a denominator. It is part of the basic theory of localization that $R_{\mathfrak{p}}$ is a local ring of dimension equal to the height of $\mathfrak{p}$. So if R is a Dedekind domain then for any nonzero prime $\mathfrak{p}$ of R, the localization $R_{\mathfrak{p}}$ is a local Dedekind domain, hence a DVR. Again though exactly the same holds for any PID: so what?

Here's what:

THEOREM 1.14. *Let R be a Noetherian domain such that for every maximal ideal $\mathfrak{p}$ of R, the local domain $R_{\mathfrak{m}}$ is a DVR. Then R is a Dedekind domain.*

We will discuss this in more detail later: again it is a quick consequence of the benevolence of localization. The consequence is: a Noetherian domain is locally a PID if and only if it is a Dedekind domain. This means that (among Noetherian domains, which not asking too much) Dedekind domains are precisely the global analogues of DVRs. This suggests that certain results about Dedekind domains could be attacked by reduction to the case of DVRs, and we will see in the course that this is absolutely correct. It turns out though that being *locally a PID* is a more basic and robust property than being *globally a PID*: the latter is great when you have it but is most often too much to ask.

We now move on to the next and more important reason that Dedekind domains are a more robust class of rings than PIDs. As we saw in §1, though $\mathbb{Z}$ is a PID, the ring $\mathbb{Z}_K$ of integers in a number field may not be and in certain regimes will usually not be. In contrast, there is the following remarkable result:

THEOREM 1.15. *Let A be a Dedekind domain with fraction field K, let L/K be a finite degree field extension, and let B be the integral closure of A in L. Then B is a Dedekind domain.*

Theorem 1.15 immediately implies that the ring of integers $\mathbb{Z}_K$ of a number field is a Dedekind domain. Similarly, for any field k, the polynomial ring $k[t]$ is a PID, with fraction field $k(t)$. Let $L/k(t)$ be a finite degree field extension. Then the integral clsoure B of $k[t]$ in L is a Dedekind domain. In arithmetic geometry, one learns that $B = k[C^\circ]$ is the affine coordinate ring of a regular, integral affine algebraic curve C°/k and that conversely, for any regular integral affine curve C° over a field k with fraction field $k(C)$, there is $t \in k[C^\circ]$ such that B is the integral closure of $k[t]$ in $k(C)$. (You should think about how to prove this if and only if you know about affine and projective curves and the Riemann-Roch Theorem.) In contrast, whether there are infinitely many number fields K such that $\mathbb{Z}_K$ is a PID has been an open problem since Gauss's time.

In our course we will prove Theorem 1.15 under the additional hypothesis that L/K is *separable*, which is automatic in characteristic 0. Under that hypothesis, the arugment will also show that B is finitely generated as an A-module, which need not be true in the general case. From this it follows easily that if A is a PID and $[L : K] = n$, then B is free of rank n as an A-module, i.e., isomorphic to the direct sum of n copies of A. In the case $A = \mathbb{Z}$ this will show that the ring $\mathbb{Z}_K$ has

an **integral basis**: there are $\alpha_1, \ldots, \alpha_n \in \mathbb{Z}_K$ such that every element of $\mathbb{Z}_K$ can be written uniquely as a $\mathbb{Z}$-linear combination of $\alpha_1, \ldots, \alpha_n$.

In truth about half of our course will be concerned with the "ANTI square": A is a Dedekind domain with fraction field K, L is a finite degree separable field extension, and B is its integral closure in L. This is the context in which we will study splitting / inertness /ramification of prime ideals of A, the discriminant ideal and the different ideal. However, there are some results of classical algebraic number theory that hold for the rings $\mathbb{Z}_K$ that absolutely do not hold for arbitrary Dedekind domains, as we will now explain.

Let R be a Dedekind domain. Then, obviously, R may fail to be a PID precisely in that there may be ideals of R that are not principal. However, this failure of ideals to be principal can be made much more precise: as mentioned before, every Dedekind domain has a **class group** $\mathrm{Cl}\, R$. Here is a quick and dirty definition: we will give a better one later. For any domain R, let $\mathrm{Int}(R)$ be the set of nonzero ideals of R. On $\mathrm{Int}(R)$ we introduce an equivalence relation: $I \sim J$ if there are $x, y \in R^\bullet$ such that $(x)I = (y)J$. Let $C(R)$ be the quotient $\mathrm{Int}(R)/\sim$. It is not hard to see that the multiplication of ideals descends to a well-defined binary operation on $C(R)$ that makes it into a commutative monoid with identity element the class of $R = (1)$. It turns out that $C(R)$ is a group if and only if R is Dedekind: in simpler terms, in a Dedekind domain, for every nonzero ideal I there is a nonzero ideal J such that $IJ = (x)$ is principal, and then in $C(R)$ J becomes the inverse of I. This is one definition of $\mathrm{Cl}\, R$ for a Dedekind domain. Even this definition makes clear that R is a PID if and only if the class group is trivial.

THEOREM 1.16.

a) *For any number field K, the class group $\mathrm{Cl}\, \mathbb{Z}_K$ is finite.*
b) *Let $\mathbb{F}_q$ be a finite field, let $L/\mathbb{F}_q(t)$ be a finite degree field extension, and let B be the integral closure of $\mathbb{F}_q[t]$ in L. Then $\mathrm{Cl}\, B$ is finite.*

We will prove part a) in our course. Most approaches to part b) use some geometry: indeed, it is morally equivalent to the fact that an algebraic curve over a fintie field $\mathbb{F}_q$ has only finitely many $\mathbb{F}_q$-rational points. It is possible however to give an algebraic approach roughly in parallel with the number field case; if time permits, I will make some exercises about this.

On the other hand:

THEOREM 1.17 (Claborn [**Cl66**]). *Let G be a commutative group. Then there is a Dedekind domain R such that $\mathrm{Cl}\, R \cong G$.*

Thus Claborn's Theorem says that, up to isomorphism, any commtuative group whatsoever can serve as the ideal class group of a Dedekind domain. A second proof of Claborn's Theorem was given by Leedham-Green [**LG72**], whose argument showed that the Dedekind domain R can be taken to be the integral closure of a PID in a quadratic field extension. I gave a third proof of Claborn's Theorem [**Cl09**] (and Leedham-Green's refinement) using elliptic curves, following a 1976 paper of Rosen who had treated the case of countable groups.

Thus there is more to the number theory of $\mathbb{Z}_K$ than the algebra of Dedekind

domains. In the last portion of the course we will come back to earth and prove the remaining three fundamental finiteness theorems of number theory: the finiteness of the class group (mentioned above), Dirichlet's Theorem on the finite generation and structure of the unit group $\mathbb{Z}_K^\times$, and Hermite's Theorems on number fields with prescribed ramification.

CHAPTER 2

Some Background Algebra

In these notes all rings are commutative with 1. All modules are left modules.

In this first chapter we review some key definitions and results from commutative algebra. Sufficiently short and enlightening proofs will be given, but the text [**CA**] provides a common reference for all of this material.

1. Chinese Remainder Theorem

Two ideals I and J in a ring R are **comaximal** if no proper ideal of R contains both of them: equivalently, the ideal $I + J = R$. A set of ideals is called **pairwise comaximal** if any two distinct ideals in the set are comaximal.

THEOREM 2.1 (Chinese Remainder Theorem). *Let $I_1, \dots, I_r$ be pairwise comaximal ideals in a ring R. Then:*

a) *We have $I_1 \cdots I_r = \bigcap_{i=1}^r I_i$.*
b) *The natural map $\Phi : R \to \prod_{i=1}^r R/I_i$ is surjective, and thus – applying part a) – we get an isomorphism*

$$\Phi : R/(I_1 \cdots I_r) \xrightarrow{\sim} \prod_{i=1}^n R/I_I.$$

PROOF. This is [**CA**, Lemma 4.19 and Thm. 4.20]. □

2. Prime and Maximal Ideals; Krull Dimension

Recall that an ideal I of R is **prime** if $I \subsetneq R$ and:

$$\forall x, y \in R,\ xy \in I \iff x \in I \text{ or } y \in I.$$

Equivalently, I is prime if and only if R/I is a domain.

For a ring R, we denote by $\operatorname{Spec} R$ the set of prime ideals of R. It is partially ordered under inclusion. It also carries a natural topology, the **Zariski topology** [**CA**, Chapter13], but we will have no need of that in these notes. A **maximal ideal** is defined to be an ideal that is maximal among all *proper* ideals of R. An ideal I is maximal if and only if R/I is a field, so it follows that maximal ideals are prime and moreover the maximal ideals are the maximal elements of $\operatorname{Spec} R$. We denote the partially ordered set of maximal ideals as $\operatorname{MaxSpec} R$. Note though that $\operatorname{MaxSpec} R$ is in general much less interesting than $\operatorname{Spec} R$ *as a partially ordered set*: in $\operatorname{MaxSpec} R$ any two distinct elements are incomparable.

A standard Zorn's Lemma argument shows that every proper ideal is contained in at least one maximal ideal.

A ring R has **finite Krull dimension** if there is some number d such that for every finite chain of prime ideals $\mathfrak{p}_0 \subsetneq \mathfrak{p}_1 \subsetneq \ldots \subsetneq \mathfrak{p}_\ell$ we have $\ell \leq d$. In this case the maximal length of such a chain is called the **Krull dimension** of R and denoted by $\dim R$. If R does not have finite Krull dimension it is traditional to put $\dim R = \infty$.[1]

EXERCISE 2.1.

a) *Show that a field has Krull dimension* 0.
b) *Show that a finite ring has Krull dimension* 0.
c) *Show that* $\mathbb{Z}$ *has Krull dimension* 1.
d) *More generally, let* R *be a principal ideal domain (PID) that is not a field. Show:* $\dim R = 1$.

3. Chain Conditions

Let $(X, \leq)$ be a partially ordered set. We say X satisfies the **ascending chain condition (ACC)** if there is no infinite sequence $\{x_n\}_{n=1}^\infty$ of elements of X with $x_n < x_{n+1}$ for all $n \in \mathbb{Z}^+$.

In a partially ordered set $(X, \leq)$, a **maximal element** if an element $x \in X$ such that for no element x' in X do we have $x < x'$. Since X is only partially ordered, this is not as strong as saying that for all $x' \neq x$ we have $x' < x$: such an element would be called a **top element**.[2]

EXERCISE 2.2. *Show: a partially ordered set* $(X, \leq)$ *satisfies ACC if and only if for every nonempty subset has a maximal element.*

Although we already have a perfectly good name for this condition, it is helpful to give it another one: a partially ordered set is **Noetherian** if it satisfies ACC.

Working in this level of generality it is clear that we ought to make a second, "dual" definition. Namely, we say that a partially ordered subset satisfies the **descending chain condition (DCC)** if there is no infinite sequence $\{x_n\}_{n=1}^\infty$ of elements of X with $x_n > x_{n+1}$ for all $n \in \mathbb{Z}^+$.

EXERCISE 2.3. *State and prove the analogue of Exercise 2.2 for the* ***descending chain condition (DCC)****.*

Again we give a second name to this: a partially ordered set $(X, \leq)$ is **Artinian** if it satisfies (DCC).

For any partially ordered set $(X, \leq)$ we can define the *dual ordering* $\leq^*$ in which $x \leq^* y$ if and only if $y \leq x$. Evidently a partially ordered set is Noetherian if and only if its dual is Artinian, and a partially ordered set is Artinian if and only its dual is Noetherian, so at this level of generality we really have "the same concept."

[1] For a ring R, one could define the **cardinal Krull dimension** $\operatorname{carddim}(R)$ as the supremum of the set of cardinalities of totally ordered subsets of $\operatorname{Spec} R$: this is a cardinal number that may be infinite. This definition is made for instance in [**Cl17**]. We will certainly not need it here.

[2] Some people say "maximum element" where we say "top element." To me this seems terrible: we change an adjective to the corresponding noun and the meaning changes. As Serge Lang once said: the terminology should be functorial with respect to the ideas.

However, in practice the two concepts separate themselves, as we will now see.

Let R be a commutative ring, and let M be an R-module. The set of all R-submodules of M is a partially ordered set under inclusion. We say that M is a **Noetherian module** if this partially ordered set is Noetherian: i.e., if there are no infinite ascending chains of submodules.

PROPOSITION 2.2. *An R-module M is Noetherian iff every submodule of M is finitely generated.*

EXERCISE 2.4. *Prove Proposition 2.2.*

A ring R is **Noetherian** if R is a Noetherian R-module: in other words, if every ideal of R is finitely generated. A ring R is **Artinian** if R is an Artinian R-module.

PROPOSITION 2.3. *Let R be a ring.*

a) *R is Noetherian iff every finitely generated R-module is Noetherian.*
b) *R is Artinian iff every finitely generated R-module is Artinian.*

PROOF. This is [**CA**, Exc. 8.4]. (It looks a little weird to refer to an exercise as a proof, so let me note that the content here is [**CA**, Thm. 8.4] – which is proved in the notes! – from which this follows very quickly.) □

So far Noetherian and Artinian still look like "dual" conditions on a ring, but that is really not the case, as the following result shows.

THEOREM 2.4 (Akizuki-Hopkins). *For a ring R, the following are equivalent:*

(i) *R is Artinian.*
(ii) *R is Noetherian and $\dim R = 0$.*

PROOF. See [**CA**, Thm. 8.35]. □

Thus the class of Artinian rings is a tiny subclass of the class of all Noetherian rings.

A ring R is **local** if it has a unique maximal ideal.

It is clear that every finite ring is Artinian: indeed, a finite ring is has only finitely many ideals, and obviously finite sets are both Noetherian and Artinian. So for instance $\mathbb{Z}/N\mathbb{Z}$ is any Artinian ring. If we factor $N = p_1^{a_1} \cdots p_r^{a_r}$ then the ideals $(p_1^{a_1}), \ldots, (p_r^{a_r})$ of $\mathbb{Z}$ are pairwise comaximal, so the Chinese Remainder Theorem gives an isomorphism

$$\mathbb{Z}/N\mathbb{Z} \xrightarrow{\sim} \prod_{i=1}^{r} \mathbb{Z}/p_i^{a_i}\mathbb{Z}.$$

Each ring $\mathbb{Z}/p_i^{a_i}\mathbb{Z}$ is finite *local*, with maximal ideal generated by the class of p.

In fact this kind of CRT decomposition extends to all Artinian rings:

THEOREM 2.5. *Every Artinian ring is a finite product of local Artinian rings. Thus an Artinian ring has finitely many prime ideals, all of which are maximal.*

PROOF. This is [**CA**, Thm. 8.37]. □

EXERCISE 2.5. *Let R be an Artinian ring, with prime ideals $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$. Show that the following are equivalent:*

(i) *The ring R is finite.*
(ii) *For all $1 \leq i \leq r$, the field $R/\mathfrak{p}_i$ is finite.*

4. Prime Avoidance

LEMMA 2.6 (Prime Avoidance). *Let R be a ring, and let $I_1, \dots, I_n, J$ be ideals of R. Suppose that all but at most two*[3] *of the I_i's are prime ideals and that $J \subseteq \bigcup_{i=1}^{n} I_i$. Then $J \subseteq I_i$ for some i.*

PROOF. This is [**CA**, Lemma 8.51]. □

5. Annihilators

Let M be an R-module, and let $m \in M$. The **annihilator** of m is

$$\operatorname{ann}(m) \coloneqq \{x \in R \mid xm = 0\}.$$

This is an ideal of R. If R is a domain, we say an R-module M is **torsionfree** if for all $m \in M^\bullet \coloneqq M \setminus \{0\}$ we have $\operatorname{ann}(m) = 0$.

More generally, if S is any subset of M then we can define

$$\operatorname{ann}(S) \coloneqq \{x \in R \mid xm = 0 \ \forall x \in S\}.$$

In fact we have

$$\operatorname{ann}(S) = \bigcap_{m \in S} \operatorname{ann}(m),$$

so $\operatorname{ann}(S)$ is also an ideal of R.

EXERCISE 2.6. *Let M be an R-module, let $S \subseteq M$ be a subset, and let $\langle S \rangle_R$ denote the R-submodule generated by S. Show:*

$$\operatorname{ann} S = \operatorname{ann}\langle S \rangle_R.$$

The extreme case is $\operatorname{ann} M$, the set of elements $x \in R$ such that x acts on M as the zero endomorphism. A module M is called **faithful** if $\operatorname{ann} M = 0$.

EXERCISE 2.7. *Show that every R-module M is, in a canonical way, a faithful $R/\operatorname{ann}(M)$-module.*

An R-module M is **cyclic** if it can be generated by a single element.

EXERCISE 2.8. *Let M be a cyclic R-module. Show:*

$$M \cong R/\operatorname{ann}(M).$$

An R-module M is **simple** if it is not the zero module and it has no nonzero proper submodules.

EXERCISE 2.9. *Let M be a simple R-module. Show: there is a unique maximal ideal $\mathfrak{m}$ of R such that $M \cong R/\mathfrak{m}$.*

[3] That one or two of the ideals I_i are allowed not to be prime is what the proof gives. But I know of no application of this extra generality, and it seems easier to remember the result under the hypothesis that every I_i is a prime ideal.

6. Jordan-Hölder Series

Recall that a Jordan-Hölder series for a finite group is a finite chain of subgroups, each normal in the next, with simple successive quotients. The simple quotients are called **Jordan-Hölder factors**, and we count them with multiplicity. For instance, the Jordan-Hölder factors of $\mathbb{Z}/p_1^{a_1}\cdots p_r^{a_r}\mathbb{Z}$ are $\mathbb{Z}/p_1\mathbb{Z}, \ldots, \mathbb{Z}/p_r\mathbb{Z}$, with multiplicities $a_1, \ldots, a_r$.

Much the same holds for modules. A **Jordan-Hölder series** for an R-module M is a finite chain of R-submodules, each of whose successive quotients is a simple R-module. A module admits a Jordan-Hölder series iff it is both Noetherian and Artinian [**CA**, Thm. 8.14]. (Thus for instance a module over an Artinian ring admits a Jordan-Hölder series iff it is finitely generated.) Such modules are said to be of **finite length**. The Jordan-Hölder Theorem still holds here: in any two Jordan-Hölder series for the same finite length module, the same simple modules (up to isomorphism, of course) appear, with the same multiplicities. Again we call these the Jordan-Hölder factors. In particular the number of Jordan-Hölder factors – equivalently, the length of any Jordan-Hölder series – is an invariant of the module, which is called its **length**.

7. Projective Modules

THEOREM 2.7. *For an R-module P, the following are equivalent:*

(i) *There is an R-module Q such that $P \oplus Q$ is free.*
(ii) *If $\pi : M \to N$ is a surjection of R-modules and $\varphi : P \to N$ is an R-module map, then there is a "lift" of φ to $\Phi : P \to M$: that is, $\varphi = \pi \circ \Phi$.*
(iii) *The functor $\mathrm{Hom}(P, \cdot)$ is eaxct.*
(iv) *Each short exact sequence of R-modules terminating at P – that is:*

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

splits: there is an R-module map $\sigma : P \to M$ such that $q \circ \sigma = 1_P$. This gives an internal direct sum decomposition $M = N \oplus \sigma(P)$.

*A module satisfying these equivalent conditions is called **projective**.*

For an R-module M, we put $M^\vee := \mathrm{Hom}_R(M, R)$; this is again an R-module.

THEOREM 2.8. *For an R-module A, the following are equivalent:*

(i) *A is finitely generated projective.*
(ii) *For all R-modules B, the natural map*

$$\Phi : A^\vee \otimes_R B \to \mathrm{Hom}_R(A, B)$$

induced by $(f, b) \mapsto (a \mapsto f(a)b)$ is an isomorphism.

PROOF. This is [**CA**, Thm. 7.32]. □

EXERCISE 2.10.

a) *Show: if $M \cong R^n$ for some $n \in \mathbb{Z}^+$, then also $M^\vee \cong R^n$.*
b) *Show: if P is finitely generated projective, so is $P^\vee$.*

If R is a domain with fraction field K, then to a finitely generated projective module P we can attach a **rank**:

$$\mathrm{rk}(P) := \dim_K(P \otimes_R K).$$

(We *only* speak of the rank for finitely generated projective modules, so when we say "P has rank n" then it is understood that P is finitely generated.) If it helps you to hear this, we can think geometrically of P as a **vector bundle** on $\operatorname{Spec} R$ and the rank is, well, the rank of the vector bundle, i.e., the common dimension of the fibers. In particular we can think of rank 1 projective modules as line bundles.

EXERCISE 2.11. *Let R be a domain, and let I be a nonzero ideal of R.*

a) *Show: I is principal $\iff$ I is a free R-module $\iff$ $I \cong_R R$.*

b) *Show: if I is projective, then it has rank* 1.

Still in the case that R is a domain, it is easy to see that for two finitely generated projective modules P_1 and P_2 we have

$$\operatorname{rk}(P_1 \oplus P_2) = \operatorname{rk} P_1 + \operatorname{rk} P_2,\ \operatorname{rk}(P_1 \otimes_R P_1) = (\operatorname{rk} P_1)(\operatorname{rk} P_2).$$

Thus the tensor product of two rank one projective modules is another rank 1 projective module. Thus $\otimes_R$ gives a binary operation on isomorphism classes of rank one projective R-modules. Since $P \otimes_R R = P$, the free rank 1 R-module – i.e., R – gives an identity for this operation. If we believe the analogy between rank 1 projective modules and line bundles, we should expect that there are also inverses: i.e., for every rank one projective R-module P, there i rank 1 projective R-module P' such that $P \otimes_R P' \cong R$. f

I claim that $P^\vee$ serves this role: for any rank 1 projective R-module P, we have $P \otimes_R P^\vee \cong R$. To see this, the first step is to apply Theorem 2.8: we get

$$P^\vee \otimes_R P \cong \operatorname{Hom}_R(P, P) = \operatorname{End}_R(P).$$

It remains to show that if P is rank 1 projective, then $\operatorname{End}_R(P) \cong R$. This is true if R is free. We will deduce the general case using localization...as we now discuss.

8. Localization

8.1. Localization of Rings. The concept of localization of a commutative ring stems from the construction of the field of fractions of a domain. Namely we formally introduce ordered pairs (a, b) of elements of R with $b \in R^\bullet$, and we form the fraction field by imposing the equivalence relation

$$(a, b) \sim (c, d) \iff ad = bc$$

and checking that the familiar formulas for addition and multiplication of fractions

$$(a_1, b_1) + (a_2, b_2) \coloneqq \frac{a_1 b_2 + b_1 a_2}{b_1 b_2},\ (a_1, b_1) \cdot (a_2, b_2) \coloneqq \frac{a_1 a_2}{b_1 b_2}$$

are well-defined on equivalence classes. The ring F that we get is certainly a field, because when $a_1 \neq 0$, the inverse of (a_1, b_1) is (b_1, a_1). Moreover we have $R \hookrightarrow F$ via $a \mapsto (a, 1)$. Of course we write $\frac{a}{b}$ for the equivalence class of (a, b).

More generally, for a domain R it makes sense to invert some but not all elements of $R \setminus \{0\}$. To do this, we can just take any subset $B \setminus R^\bullet$ and form $R[\frac{1}{b} \mid b \in B]$, the subring of F generated by r and the inverses of elements of B. However, it is to our advantage to be a bit more careful: e.g. if $R = \mathbb{Z}$ and $B = \{2, 3\}$, then the subring $\mathbb{Z}[\frac{1}{2}, \frac{1}{3}]$ can be described more precisely as $\{\frac{a}{2^{b_1} 3^{b_2}} \mid a \in \mathbb{Z},\ b_1, b_2 \in \mathbb{N}\}$. Because the units in any ring form a group, if we invert 2 and invert 3 we must also invert $2^{b_1} 3^{b_2}$. This leads us to the idea of a **multiplicative subset** $S \subseteq R$: this

is a subset containing 1 and closed under multiplication: $SS \subseteq S$. If we start with such a set, then indeed

$$R\left[\frac{1}{s} \mid s \in S\right] = \left\{\frac{a}{s} \mid \ a \in R,\ s \in S\right\},$$

while if we start with an arbitrary subset $B \subseteq R^\bullet$ as above, then we can take S_B to be the submonoid of $R^\bullet$ generated by B – i.e., the set consisting of 1 and all finite products of elements of B – and then

$$R\left[\frac{1}{b} \mid b \in B\right] = R\left[\frac{1}{s} \mid s \in S_B\right] = \left\{\frac{a}{s} \mid s \in S\right\}.$$

If for an arbitrary ring R we performed this construction with S a multiplicative subset of *nonzerodivisors* of R – i.e., elements $r \in R$ with $\operatorname{ann} r = 0$ – then everything holds as above. In particular, if we take R° to be the set of nonzerodivisors of R, then this is the largest such multiplicatively closed subset, and the ring that we get in this way is called the **total fraction ring** of R. When we move on to inverting zero-divisors, things get one step more complicated: one would like to define $S^{-1}R$ as the set of ordered pairs (a, s) with $a \in R$ and $s \in S$, with

$$(a_1, s_1) \sim (a_2, s_2) \iff s_2 a_1 = s_1 a_2.$$

However it turns out that this need not be an equivalence relation!

Exercise 2.12. *Find a commutative ring R and a multiplicative subset $S \subseteq R$ such that the relation $\sim$ on $R \times S$ defined by $(a_1, s_1) \sim (a_2, s_2) \iff s_2 a_1 = s_1 a_2$ is* not *an equivalence relation.*

To fix this, we put

$$(a_1, s_1) \sim (a_2, s_2) \iff \exists s \in S \text{ such that } s s_2 a_1 = s s_1 a_2.$$

(If no element of S is a zero divisor, then $s s_2 a_1 = s s_1 a_2 \iff s_2 a_1 = s_1 a_2$, so this definition is equivalent to the old one.)

Exercise 2.13. *Let R be a ring, and let S be a multiplicative subset.*

a) *Define a relation $\sim$ on $R \times S$ as above:*

$$(a_1, s_1) \sim (a_2, s_2) \iff \exists s \in S \mid s s_2 a_1 = s s_1 a_2.$$

Show: this is an equivalence relation.

b) *Show: $+$ and $\cdot$ are well-defined on equivalence classes, which makes the set of equivalence classes into a commutative ring, denoted $S^{-1}R$.*

c) *Show: $S^{-1}R$ is the zero ring (i.e., with one element $0 = 1$) if and only if $0 \in S$.*
(Because of this, the case in which $0 \in S$ is often tacitly excluded.)

d) *Show: there is a ring homomorphism $\iota : R \to S^{-1}R$ defined by $a \mapsto \frac{a}{1} := [(a, 1)]$. Also show: the kernel of ι is the set of elements r of R whose annihilator meets S:* $\operatorname{ann}(r) \cap S \neq \varnothing$.

e) *Show: ι is surjective if and only if $S \subseteq R^\times$, in which case ι is an isomorphism.*

Exercise 2.14 (Universal Property of Localization). *Let S be a multiplicative subset of a ring R. Show that the homomorphism $\iota : R \to S^{-1}R$ is* universal *for homomorphisms $\varphi : R \to T$ in which $\varphi(S) \subseteq T^\times$: that is, for any such homomorphism, there is a unique homomorphism $\Phi : S^{-1}R \to T$ such that $\varphi = \Phi \circ \iota$.*

Localization at a prime ideal: Let I be an ideal of a ring R. Then I is a multiplicative subset...but not an interesting one: since $0 \in I$, the localization $I^{-1}R$ is the zero ring. Notice however that the complement $R \setminus I$ is a multiplicative subset if and only if I is a prime ideal. Thus for $\mathfrak{p} \in \operatorname{Spec} R$, we define **the localization of R at $\mathfrak{p}$** as

$$R_{\mathfrak{p}} \coloneqq (R \setminus \mathfrak{p})^{-1}R.$$

We claim that $R_{\mathfrak{p}}$ is a local ring. We will deduce this from some more general recalled spectral properties of the localization map $\iota : R \to S^{-1}R$.

For any ring homomorphism $f : A \to B$, we may use f to "push forward" ideals of A to get ideals of B: for an ideal I of A, we put

$$f_*(I) \coloneqq IB = \langle f(i) \mid i \in I \rangle_B.$$

We may also use f to "pull back" ideals of B to get ideals of A: for an ideal J of B, we put

$$f^*(J) \coloneqq f^{-1}(J) = \{x \in R \mid f(x) \in J\}.$$

EXERCISE 2.15. *If $f : A \to B$ is a ring homomorphism and $\mathfrak{p}$ is a prime ideal of B, show that $f^*(\mathfrak{p})$ is a prime ideal of A. Thus we get an induced map*

$$f^* : \operatorname{Spec} B \to \operatorname{Spec} A.$$

LEMMA 2.9. *Let $\iota : R \to S^{-1}R$ be a localization map. Let I be an ideal of R.*

a) *We have $\iota_*(I) = \left\{\frac{x}{s} \in S^{-1}R \mid x \in I \text{ and } s \in S\right\}$.*
b) *The following are equivalent:*
   (i) *We have $I \cap S = \varnothing$.*
   (ii) *We have $\iota_*(I) \subsetneq S^{-1}R$.*

PROOF. Part a) is [**CA**, Lemma 7.2]. Part b) is [**CA**, Lemma 7.4]. □

PROPOSITION 2.10. *Let $S \subseteq R$ be multiplicatively closed, and let $\iota : R \to S^{-1}R$ be the localization map. If J is an ideal of $S^{-1}R$, we have*

$$J = \iota_*\iota^* J.$$

PROOF. This is [**CA**, Prop. 7.3]. □

Thus using ι^*, we may view the set of ideals of $S^{-1}R$ as a subset of the ideals of R. It would be desirable to characterize the image of ι^*. Combining the last two results, we see that the only proper ideals of R lying in the image of ι^* are those that are disjoint from S. If we restrict to prime ideals, this turns out to the only condition:

PROPOSITION 2.11. *Let $S \subseteq R$ be multiplicatively closed, and let $\iota : R \to S^{-1}R$ be the localization map.*

a) *If $\mathfrak{p} \in SpecR$ is a prime ideal that is disjoint from S, then $\iota_*(\mathfrak{p})$ is a prime ideal of $S^{-1}R$. Moreover we have*

$$\iota^*(\iota_*\mathfrak{p}) = \mathfrak{p}.$$

b) *The maps ι_* and ι^* give mutually inverse bijections from $\operatorname{Spec} S^{-1}R$ to the set of prime ideals of R that are disjoint from S.*

PROOF. This is [**CA**, Prop. 7.5] and [**CA**, Cor. 7.6]. □

These considerations apply especially nicely to the case in which $S = R \setminus \mathfrak{p}$ for a prime ideal $\mathfrak{p}$ of R. In this case, $\operatorname{Spec} R_{\mathfrak{p}}$ consists of prime ideals $\mathfrak{q}$ of R that are disjoint from $R \setminus \mathfrak{p}$, i.e., such that $\mathfrak{q} \subseteq \mathfrak{p}$. Thus we find that $R_{\mathfrak{p}}$ is a local ring with unique maximal ideal $\mathfrak{p}R_{\mathfrak{p}}$ (often this is notationally shortened to just $\mathfrak{p}$). Overall, to any commutative ring R we have attached a family of local rings parametrized by the prime ideals of R. This is a useful construction, to say the least!

This example also shows that localization is "roughly dual" to taking quotients: that is, let is try to compare a localization map

$$\iota : R \to S^{-1}R$$

to a quotient map attached to an ideal I of R:

$$q : R \to R/I.$$

Quotient maps also have the "pull-push property" – for all ideals J of R/I we have $q_*(q_*J) = J$ [**CA**, §1.5]. Moreover, under ι^* the ideals of R/I correspond bijectively to the ideals of R that contain I. Thus whereas quotienting by an arbitrary ideal I "cuts off the lattice of ideals of R below I," making I the smallest element of the new lattice, localizing at a prime ideal $\mathfrak{p}$ "cuts off the lattice of prime ideals of R above $\mathfrak{p}$," making $\mathfrak{p}$ the largest element of the new lattice. The analogy is not perfect, but it seems close enough to be helpful.

There is also a useful compatibility between quotients and localization:

LEMMA 2.12. *Let R be a ring, let $S \subseteq R$ be a multiplicatively closed subset, and let I be an ideal of R. Let $q : R \to R/I$ be the quotient map, and put $\overline{S} \coloneqq q(S)$. Then there is a canonical isomorphism*

$$S^{-1}R/IS^{-1}R \cong \overline{S}^{-1}R/I.$$

PROOF. This is [**CA**, Lemma 7.7]. □

EXERCISE 2.16. *Let $\mathfrak{m}$ be a maximal ideal in a ring R.*

a) *Use the universal property of localization to show that the quotient map $q : R \to R/\mathfrak{m}$ factors through the localization map $\iota : R \to R_{\mathfrak{m}}$: i.e., there is a unique ring homomorphism $\alpha : R_{\mathfrak{m}} \to R/\mathfrak{m}$ such that $q = \alpha \circ \iota$.*

b) *Show: $\operatorname{Ker}(\alpha) = \mathfrak{m}R_{\mathfrak{m}}$. Deduce that α induces an isomorphism*

$$R_{\mathfrak{m}}/\mathfrak{m}R_{\mathfrak{m}} \xrightarrow{\sim} R/\mathfrak{m}.$$

c) *Show: For all $a \in \mathbb{Z}^+$ we have a canonical isomorphism*

$$R_{\mathfrak{m}}/(\mathfrak{m}R_{\mathfrak{m}})^a \xrightarrow{\sim} R/\mathfrak{m}^a.$$

EXERCISE 2.17 (Semilocalization). *Let $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ be prime ideals in a ring R, none containing any of the others. Let*

$$S \coloneqq \bigcap_{i=1}^{r} (R \setminus \mathfrak{p}_i).$$

a) *Show: S is a multiplicatively closed subset. We define the **semilocalization** of R at $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ as*

$$R_{\mathfrak{p}_1,\ldots,\mathfrak{p}_r} \coloneqq S^{-1}R.$$

b) *Show: under the identification of* $\operatorname{Spec} S^{-1}R$ *with the elements of* $\operatorname{Spec} R$ *that are disjoint from* S*, we have*

$$\operatorname{MaxSpec} R_{\mathfrak{p}_1,\ldots,\mathfrak{p}_r} = \{\mathfrak{p}_1, \ldots, \mathfrak{p}_r\}.$$

Suggestion: use ***Prime Avoidance*** *(Lemma 2.6).*

8.2. Localization of Modules. Let $S \subseteq R$ be a multiplicative subset. To an R-module M, we want to define an $S^{-1}R$-module $S^{-1}M$ and a homomorphism of R-modules $\iota_M : M \to S^{-1}M$. In order to define these maps, the minor complication is that there are *two* perfectly good contructions that present themselves:

• We observe that the localization construction makes sense on M just as well as on R: i.e., we take the quotient of $M \times S$ under the equivalence relation $(m_1, s_1) \sim (m_2, s_2)$ if there is $s \in S$ such that $ss_2m_1 = ss_1m_2$.

• Or we could put $S^{-1}M \coloneqq S^{-1}R \otimes_R M$.

In order to check that both of these constructions work, perhaps the cleanest approach is to identify the following desired properties of $S^{-1}M$ and ι_M: $S^{-1}M$ should be an R-module on which each element of s acts bijectively, and among all R-module maps $f : M \to N$ for which N is an R-module on which each element of S acts bijectively, $\iota_M : M \to S^{-1}M$ should be the *universal* such map: i.e., there should be a unique R-module homomorphism $F : S^{-1}M \to N$ such that $f = F \circ \iota_M$. As usual, this determines ι_M up to a unique isomorphism. So it suffices to check that *both* of the above constructions satisfy this universal mapping property. We leave this as an exercise.

Here is a closely related remark: an R-module M can be endowed with the structure of an $S^{-1}R$-module compatibly with its R-module structure if and only if each $s \in S$ acts bijectively on M, in which case this $S^{-1}R$-module structure is unique: indeed, we can and must define $\frac{x}{s}$ as $s^{-1} \circ x$ (where s^{-1} denotes the inverse of s as an endomorphism of M). Thus for instance a $\mathbb{Q}$-vector space is precisely a commutative group in which mutiplication by n is bijective for all $n \in \mathbb{Z} \setminus \{0\}$. By the way, this is also analogous to the case of quotients: for an ideal I of R, an R-module M can be given the compatible structure of an R/I-module if and only if each element of I acts on M as the zero endomorphism, in which case the compatible R/I-module structure is unique.

EXERCISE 2.18. *Let* $S \subseteq R$ *be a multiplicatively closed subset. Show: the kernel of* $\iota_M : M \to S^{-1}M$ *is the set of* $m \in M$ *such that* $\operatorname{ann}(m) \cap S \neq \varnothing$.

EXERCISE 2.19. *Let* R *be a domain, with fraction field* K*, and let* M *be an* R*-module.*

a) *Let* R *be a domain with fraction field* K*. Let* M *be an* R*-module. show:*

$$\operatorname{Ker}(M \to M \otimes K) = M[\text{tors}].$$

b) *Suppose that* M *is finitely generated. Show: the following are equivalent:*
(i) M *is torsionfree.*
(ii) M *embeds in a finitely generated free module.*

8.3. Local Properties.

PROPOSITION 2.13. *Let $f : M \to N$ be a homomorphism of R-modules. Then f is injective (resp. surjective, resp. bijective) if and only if $f_{\mathfrak{m}} : M_{\mathfrak{m}} \to N_{\mathfrak{m}}$ is injective (resp. surjective, resp. bijective) for all $\mathfrak{m} \in \operatorname{MaxSpec} R$.*

PROOF. This is [**CA**, Prop. 7.14]. □

EXERCISE 2.20. *Let R be a ring, M and R-module and let N_1, N_2 be R-submodules of M.*

a) *Show: $N_1 \subseteq N_2$ if and only if $(N_1)_{\mathfrak{m}} \subseteq (N_2)_{\mathfrak{m}}$ for all $\mathfrak{m} \in \operatorname{MaxSpec} R$. (Hint: $N_1 \subseteq N_1 \iff (N_1 + N_2)/N_2 = 0$.)*
b) *Show: $N_1 = N_2$ if and only if $(N_1)_{\mathfrak{m}} = (N_2)_{\mathfrak{m}}$ for all $\mathfrak{m} \in \operatorname{MaxSpec} R$.*

PROPOSITION 2.14. *Let R be a domain with fraction field K, let V be a finite-dimensional K-vector space, and let Λ be a finitely generated R-submodule of V. Then inside V we have*

$$\bigcap_{\mathfrak{m} \in \operatorname{MaxSpec} R} \Lambda_{\mathfrak{m}} = \Lambda.$$

PROOF. This is [**CA**, Thm. 7.16]. □

8.4. Localization and Projective Modules. One of the most important properties that is *not* local is being freeness of modules. This is highly relevant to us, because a nonzero ideal I in a domain R is principal if and only if it is free, in which case it is free of rank 1. We cannot check locally whether ideals are principal: as we will soon see, in any Dedekind domain that is not a PID, every ideal is locally free but not every ideal is free. However, what we can check locally is projectivity, at least with some fine print.

THEOREM 2.15. *Let R be a ring. Suppose that R is* either *Noetherian or a domain. Let M be a finitely generated R-module. The following are equivalent:*

(i) *M is projective.*
(ii) *M is locally free: $M_{\mathfrak{m}}$ is free for all $\mathfrak{m} \in \operatorname{MaxSpec} R$.*

PROOF. When R is Noetherian this follows from [**CA**, Thm. 7.29]. When R is a domain this follows from [**CA**, Cor. 13.36]. □

COROLLARY 2.16. *For a domain R and a rank 1 projective module P, we have $\operatorname{End}_R(P) \cong R$.*

PROOF. For any R-module M, we have a homomorphism of R-modules $f : R \to \operatorname{End}_R(M)$. By Proposition 2.13, we have that $f : P \to \operatorname{End}_R(P)$ is a bijection if and only if $f_{\mathfrak{m}} : R_{\mathfrak{m}} \to \operatorname{End}_R(P) \otimes R_{\mathfrak{m}} = \operatorname{End}_{R_{\mathfrak{m}}}(M_{\mathfrak{m}})$, so we are reduced to the case in which R is a local ring. But then by Theorem 2.15 we have that $M \cong R$, and as mentioned before we certainly have $\operatorname{End}_R(R) = R$. □

Thus we have shown that for a domain R, isomorphism classes of rank 1 projective R-modules form a group under $\otimes$. This group is called the **Picard group** of R and denoted $\operatorname{Pic} R$.

Digression: Over an arbitrary ring R, a finitely generated module M has a rank *function*: for $\mathfrak{p} \in \operatorname{Spec} R$, let $k_{\mathfrak{p}} := R_{\mathfrak{p}}/\mathfrak{p}R_{\mathfrak{p}}$. Then we put $\operatorname{rk}_{\mathfrak{p}}(M) := \dim_{k_{\mathfrak{p}}} M \otimes_R k_{\mathfrak{p}}$. This function is continuous, so is constant on the connected components of $\operatorname{Spec} R$.

If R is a domain then $\operatorname{Spec} R$ is connected, so we get a constant function, and evaluating at $\mathfrak{p} = (0)$ we get our previous definition of the rank. In general define a rank 1 projective module to be a finitely generated projective module whose rank function is constantly 1, and then once again $\operatorname{Pic} R$ is the group of isomorphism classes of rank 1 projective modules under $\otimes$.

In turn this is a special case of the Picard group of a locally ringed space.... However, since R is a domain we can give a more down-to-earth description of $\operatorname{Pic} R$ in terms of certain ideals of R. We do this next.

9. Fractional Ideals

Let R be a domain with fraction field K. A **fractional ideal** of R is a nonzero R-submodule I of K for which there is $a \in R^\bullet$ such that $aI \subseteq R$ (equivalently, $I \subseteq \frac{1}{a}R$). Then aI is a nonzero ideal of R, so a good way to think about a fractional ideal is as a (nonzero) ideal divided by a (nonzero) principal ideal.

REMARK 2.17. *One can extend the notion of "fractional R-ideal" to commutative rings with zero divisors. First one replaces the fraction field K with the "total fraction ring" of R, i.e., the localization at the set of all nonzerodivisors. Second, instead of nonzero ideals one works with ideals containing a* regular element*: that is, a nonzerodivisor. In principle this is the right level of generality. Maybe I will do this in a future version of these notes, but for now I will restrict to domains.*

EXERCISE 2.21. *Let R be a domain with fraction field K.*

a) *Show: every finitely generated R-submodule of K is a fractional R-ideal.*
b) *Show that the following are equivalent:*
   (i) *R is Noetherian.*
   (ii) *Every fractional R-ideal is a finitely generated R-submodule of K.*

We denote the set of all fractional R-ideals by $\operatorname{Frac}(R)$.

If I and J are fractional R-ideals, then all of following are also fractional R-ideals [**CA**, Thm. 19.1]:

- $I \cap J$.
- $I + J := \{x + y \in x \in I, y \in J\} = \langle I, J \rangle_R$.
- $IJ := \{\sum_{i=1}^n x_i y_j \mid x_i \in I,\ y_i \in J\}$.
- $(I : J) := \{x \in K \mid xJ \subseteq I\}$.

EXERCISE 2.22. *Let R be a domain, and let $S \subseteq R$ be a multiplicatively closed subset. Let I and J be fractional R-ideals. Show:*

a) $S^{-1}(I \cap J) = (S^{-1}I) \cap (S^{-1}J)$.
b) $S^{-1}(I + J) = S^{-1}I + S^{-1}J$.
c) $S^{-1}(IJ) = (S^{-1}I)(S^{-1}J)$.
d) *If J is finitely generated, then* $S^{-1}(I : J) = (S^{-1}I : S^{-1}J)$.

EXERCISE 2.23. *Let R be a domain, and let I and J be fractional R-ideals. Show that the map*

$$(I : J) \to \operatorname{Hom}_R(J, I),\ x \mapsto (y \mapsto xy)$$

is an isomorphism of R-modules.

EXERCISE 2.24. *Let R be a domain. For fractional R-ideals I and J, show that the following are equivalent:*

(i) *I and J are isomorphic as R-modules.*
(ii) *There is $x \in K^\times$ such that $J = (x)I$.*

Certainly we have $RI = R$ for all $I \in \mathrm{Frac}(R)$, so $\mathrm{Frac}(R)$ forms a commutative monoid under multiplication of ideals. A fractional ideal is **invertible** if it has an inverse in this monoid: i.e., if there is another fractional ideal I' such that $II' = R$. Thus $\mathrm{Frac}\, R$ is a group if and only if *every* fractional R-ideal is invertible. When does this happen? In the next chapter we will identify the class of domains for which this holds.

EXERCISE 2.25. *Let R be a domain, and let J be an* invertible *fractional R-ideal. Show: for all $I \in \mathrm{Frac}(R)$ we have*

$$(I : J) = IJ^{-1}.$$

This provides some intuition for the colon ideal construction: when J is invertible, $(I : J)$ is literally I divided by J. But – intriguingly – this definition makes sense even if J is not invertible. To follow up on this, for $I \in \mathrm{Frac}(R)$, we put

$$I^* := (R : I).$$

EXERCISE 2.26. *Let R be a domain, and let $I \in \mathrm{Frac}(R)$. Show: $II^* \subseteq R$.*

Now we have a very important lemma:

LEMMA 2.18. *Let R be a domain.*

a) *For a fractional R-ideal I, the following are equivalent:*
   (i) *I is invertible.*
   (ii) *We have $II^* = R$.*
b) *(**To contain is to divide**) If $I \subseteq J$ are fractional R-ideals with J invertible, then*
$$I = J(I : J).$$

PROOF. See [**CA**, Lemma 19.8]. (I encourage you to read the proof.) □

Let $\iota : II^* \hookrightarrow R$ be the inclusion map, an injection of R-modules. Whether ι is a bijection can be checked locally! It follows that invertibility of fractional ideals can also be checked locally. There is one kind of fractional ideal that is rather obviously invertible: namely, a fractional R-ideal is **principal** if it is monogenic as an R-module: that is $I = (a) := Ra$ for some $a \in K^\times$. Indeed, we have

$$(a)^{-1} = (a^{-1}).$$

So it follows that a fractional ideal is invertible if it is *locally principal*. Since a nonzero ideal in any domain is principal if and only if it is free if and only if it is free of rank 1 as an R-module, we deduce from Theorem 2.15 that a finitely generated fractional R-ideal is locally principal if and only if it is projective if and only if it is projective of rank 1.

So finitely generated projective fractional ideals are invertible. It turns out that the converse is also true, so we get:

THEOREM 2.19. *Let R be a domain, and let I be a fractional R-ideal. Then I is invertible if and only if I is finitely generated projective.*

PROOF. This is [**CA**, Thm. 19.11]. □

Thus over any domain, a fractional R-ideal is invertible if and only if it is finitely generated projective as an R-module, in which case (by Exercise 2.11) it has rank 1.

Furthermore:

THEOREM 2.20. *Let R be a domain, and let I and J be invertible fractional R-ideals.*

a) *Multiplication induces an isomorphism of R-modules $I \otimes_R J \xrightarrow{\sim} IJ$.*
b) *Let P be a rank 1 projective R-module. Then there is a fractional ideal I of R such that $M \cong_R I$.*

PROOF. Part a) is [**CA**, Thm. 19.14]. Part b) is [**CA**, Thm. 19.16]. □

By Theorem 2.20, every rank 1 projective R-module is isomorphic to a fractional ideal I. By Exercise 2.24 this ideal I is well-determined precisely up to multiplication by a principal fractional ideal, so the set of isomorphism classes of rank 1 projective modules gets identified with the set of invertible ideal *classes*. To make that last part more precise, we denote by $\mathrm{Inv}(R)$ the group of invertible fractional R-ideals (this is the unit group of the commutative monoid $\mathrm{Frac}(R)$). The principal fractional R-ideals form a subgroup of $\mathrm{Inv}(R)$ that we denote $\mathrm{Prin}(R)$.

Now (but not for long!) we define the **Cartier class group** as the quotient

$$\mathrm{CaCl}(R) \coloneqq \mathrm{Inv}(R)/\mathrm{Frac}(R).$$

But the point is that we have named the same group twice: we have just explained that the canonical map $\mathrm{CaCl}(R) \to \operatorname{Pic} R$ that associates to every invertible ideal class the isomorphism class of the underlying rank 1 projective module is an isomorphism, and by Theorem 2.20b) it is an isomorphism of groups.

This is an exciting result: the general trend in commutative algebra is to move from the study of rings to the study of ideals to the study of modules. But here we have managed to come back the other way: for any domain R, rank 1 projective R-modules can be completely understood in terms of invertible fractional R-ideals.

Aside: we spoke of the *Cartier* class group of R rather than just the class group. As you might surmise, there is another kind of class group. If R is a Noetherian integrally closed domain, then there is a **divisor class group** denoted $\mathrm{Cl}(R)$: see [**CA**, §19.4] for one possible definition. There is a canonical injective group homomorphism

$$\operatorname{Pic} R \hookrightarrow \mathrm{Cl}(R)$$

that can fail to be surjective: in algebraic geometry this corresponds to the fact that every Cartier (= locally principal) divisor is a Weil divisor, but not necessarily conversely. These two groups however do coincide whenever we have that $R_{\mathfrak{m}}$ is a UFD for all $\mathfrak{m} \in \operatorname{MaxSpec} R$. In turn this happens whenever R is a regular ring.

In our course we are only interested in *one-dimensional* Noetherian domains, in which case as mentioned before, integrally closed is the same as regular, so we

only have one kind of class group. Nevertheless the notion of a Weil divisor in a Dedekind domain is indeed a familiar and important one: it is a finite formal $\mathbb{Z}$-linear combination of height 1 (= maximal, here) prime ideals. Thus Weil divisors correspond to fractional ideals and "every Weil divisor is Cartier" is a fancy way of saying that all fractional ideals are invertible.

We will also be interested in one-dimensional Noetherian domains that are not integrally closed, especially in the case of non-maximal orders $\mathcal{O}$ in a number field. In this case the Picard group $\operatorname{Pic}\mathcal{O}$ is still meaningful and important, but its non-triviality is no longer the sole obtruction to $\mathcal{O}$ being a PID.

10. Integral Extensions

10.1. Basic Properties. Let $A \subseteq B$ be a ring extension. We may also write "let B/A be a ring extension."

EXERCISE 2.27. *Let B/A be a ring extension. Show: B is a faithful A-module.*

An element $\alpha \in B$ is **integral over A** if there are $a_0, \ldots, a_{n-1} \in A$ such that

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

In other words, $\alpha \in B$ is integral over A if there is a monic polynomial $P \in A[t]$ such that $P(\alpha) = 0$.

THEOREM 2.21. *Let B/A be a ring extension. For $\alpha \in B$, the following are equivalent:*

(i) *α is integral over A.*
(ii) *$A[\alpha]$ is a finitely generated A-module.*
(iii) *There is an intermediate ring $A \subseteq C \subseteq B$ such that $\alpha \in C$ and C is finitely generated as an A-module.*
(iv) *There is a faithful $A[\alpha]$-submodule of C that is finitely generated as an A-module.*

PROOF. This is [**CA**, Thm. 14.1]. □

We say a ring extension B/A is **integral** if every element of B is integral over A. Notice that a field extension is integral if and only if it is algebraic.

LEMMA 2.22. *Let $A \subseteq B \subseteq C$ be a tower of rings.*

a) *If B is a finitely generated A-module and C is a finitely generated B-module, then C is a finitely generated A-module: indeed, if $\{\beta_i\}_{i=1}^m$ generates B as an A-module and $\{\gamma_j\}_{j=1}^n$ generates C as a B-module, then $\{\alpha_i\beta_j\}_{1\le i\le m,\ 1\le j\le n}$ generates C as an A-module.*
b) *If B is integral over A and C is integral over B, then C is integral over A.*

PROOF. a) This is [**CA**, Lemma 14.4]. b) This is [**CA**, Lemma 14.3]. □

A good intuition for integral extensions B/A is that they are the ring extensions of A that are "locally finitely generated as A-modules." The following result shows that under integrality, the weaker finiteness condition of being finitely generated as an A-algebra is equivalent to the stronger finiteness condition of being finitely generated as an A-module.

COROLLARY 2.23. *Let B/A be a ring extension.*

a) *If B is finitely generated as an A-module, then B is integral over A.*
b) *If B is integral over A and finitely generated as an A-algebra, then it is finitely generated as an A-module.*

PROOF. (i) $\implies$ (ii): If B is finitely generated as an A-module, let $\alpha \in B$. Condition (iii) of Theorem 2.21 applies with $C = B$, so α is integral over A.
(ii) $\implies$ (i): Since B is finitely generated as an A-algebra, we may write $B = A[\alpha_1, \ldots, \alpha_n]$. Since α_1 is integral over A, by Theorem 2.21, $A[\alpha_1]$ is finitely generated as an A-module. Since α_2 is integral over A, it is also integral over $A[\alpha_1]$, so $A[\alpha_1, \alpha_2]$ is finitely generated as an $A[\alpha_1]$-module. By Lemma 2.22a), $A[\alpha_1, \alpha_2]$ is finitely generated as an A-module. Continuing in this manner, we get that $A[\alpha_1, \ldots, \alpha_n]$ is finitely generated as an A-module. □

10.2. Integral Extensions of Domains. If B/A is a ring extension, then the **integral closure of A in B** is the set of all elements of B that are integral over A. We will denote this by $I_B(A)$. It is a subring of B [**CA**, Cor. 14.6].

PROPOSITION 2.24. *Let $A \subseteq B$ be domains, let K be the fraction field of A and let L be the fraction field of B.*

a) *The fraction field of $I_B(A)$ is $I_L(K)$.*
b) *In particular, if L/K is an algebraic extension, then the fraction field of $I_B(A)$ is L.*

PROOF. a) This is [**CA**, Prop. 14.10]. b) If L/K is algebraic, then $I_L(K) = L$, so this follows from part a). □

EXERCISE 2.28. *Let A be a domain with fraction field K, let L/K be an algebraic field extension, and let B be the integral closure of A in L. Show: for all $\alpha \in L$, there is $a \in A^\bullet$ such that $a\alpha \in B$.*

The following result tells us that localization commutes with integral closure.

THEOREM 2.25. *Let B/A be an extension of domains, and let $S \subseteq A$ be a multiplicatively closed subset. Then*

$$I_{S^{-1}B}(S^{-1}A) = S^{-1}I_B(A).$$

PROOF. This is [**CA**, Thm. 14.9]. □

If B/A is a ring extension, **A is integrally closed in B** is $I_B(A) = A$: that is, if every element of B that is integral over A arleady lies in A. If A is a domain with fraction field K, we say that A is **integrally closed** if A is integrally closed in K.

PROPOSITION 2.26. *A unique factorization domain (UFD) is integrally closed.*

PROOF. Let A be a UFD with fraction field K, and let $\alpha \in K$ be integral over A, so there are $a_0, \ldots, a_{n-1} \in A$ such that

$$\alpha^n + a_{n-1}\alpha^{n-1} + \ldots + \alpha_1 x + \alpha_0 = 0.$$

Certainly we may assume that $x \neq 0$. Then, since R is a UFD, we may write $\alpha = \frac{r}{s}$ with $r, s \in A^\bullet$ and with $\gcd(r, s) = 1$. Substituting this in gives

$$\left(\frac{r}{s}\right)^n + a_{n-1}\left(\frac{r}{s}\right)^{n-1} + \ldots + a_1\left(\frac{r}{s}\right) + a_0 = 0,$$

and clearing denominators, we get

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

This shows that $s \mid r^n$. If s is not a unit of A it is divisible by some prime element p, and thus $p \mid r^n$ and then $p \mid r$, contradicting the coprimality of r and s. So $s \in R^\times$ and thus $\alpha = \frac{r}{s} \in A$. □

THEOREM 2.27. *Let A be a domain with fraction field K. Let L/K be a field extension, and let $\alpha \in L$ be integral over A. Let $P \in K[t]$ be the minimal polynomial of α.*

a) *We have $P(t) \in I_K(A)[t]$.*
b) *If A is integrally closed, then α is integral over A if and only if $P \in A[t]$.*

PROOF. This is [**CA**, Thm. 14.18]. □

THEOREM 2.28 (Local nature of integral closure). *For a domain R, the following are equivalent:*

(i) *R is integrally closed.*
(ii) *For all $\mathfrak{p} \in \operatorname{Spec} R$, the ring $R_\mathfrak{p}$ is integrally closed.*
(iii) *For all $\mathfrak{m} \in \operatorname{MaxSpec} R$, the ring $R_\mathfrak{m}$ is integrally closed.*

PROOF. This is [**CA**, Thm. 14.19]. □

10.3. Spectral Properties of Integral Extensions.

THEOREM 2.29. *Let $\iota : A \hookrightarrow B$ be an integral ring extension. Then:*

a) *The pullback map $\iota^* : \operatorname{Spec} B \to \operatorname{Spec} A$ is surjective.*
b) *If $I \subsetneq A$ is a proper ideal of A, then $\iota_*(I) \subsetneq B$ is a proper ideal of B.*
c) *For $\mathfrak{p} \in \operatorname{Spec} B$, we have that $\mathfrak{p}$ is maximal if and only if $\iota^*(\mathfrak{p})$ is maximal.*
d) *The pullback map $\iota^* : \operatorname{MaxSpec} B \to \operatorname{MaxSpec} A$ is surjective.*
e) *We have $\dim A = \dim B$.*

PROOF. a) This is [**CA**, Thm. 14.13].
b) By Zorn's Lemma, I is contained in a maximal ideal $\mathfrak{m}$ of R. Since $\iota_*(I) \subseteq \iota_*(\mathfrak{m})$, it suffices to show that $\iota_*(\mathfrak{m})$ is a proper ideal of B. By part a) there is a prime ideal $\mathcal{P}$ of B such that $\iota^*(\mathcal{P}) = \mathfrak{m}$. This means that $\mathcal{P} \cap A = \mathfrak{m}$, so $\mathcal{P}$ is an ideal of B containing $\mathfrak{m}$, so $\iota_*(\mathfrak{m}) \subseteq \mathcal{P} \subsetneq B$. c) This is [**CA**, Cor. 14.16].
d) Let $\mathfrak{m} \in \operatorname{MaxSpec} A$. By part a), there is $\mathcal{P} \in \operatorname{Spec} B$ such that $\iota^*(\mathcal{P}) = \mathfrak{m}$. By part c), $\mathcal{P}$ is maximal.
e) This is [**CA**, Cor. 14.17]. □

If B/A is an integral extension and $\mathfrak{p}$ is a prime ideal of A, then a prime ideal $\mathcal{P}$ of B is said to **lie over** $\mathfrak{p}$ if $\iota^*(\mathcal{P}) = \mathfrak{p}$, or in other words if $\mathcal{P} = \mathfrak{p}$.

10.4. Normalization Theorem.

THEOREM 2.30 (Normalization Theorem). *Let A be an integrally closed Noetherian domain with fraction field K, let L/K be a finite degree **separable** field extension, and let B be the integral closure of R in L. Then:*

a) *B is finitely generated as an A-module.*
b) *If A is a PID, then $B \cong_A A^{[L:K]}$.*

PROOF. This is [**CA**, Thm. 18.1]. □

The proof of Theorem 2.30 given in [**CA**] is a classic algebraic number theory argument: it involves traces, discriminants and so forth. We will give a (different, but not *that* different) proof of Theorem 2.30 later on: see Theorem 5.20.

10.5. The Ring of Integers of a Number Field. Let K be a number field, i.e., a finite degree extension of $\mathbb{Q}$, say of degree n. We denote by $\mathbb{Z}_K$ the integral closure of $\mathbb{Z}$ in K. By Theorem 2.30, $\mathbb{Z}_K$ a free $\mathbb{Z}$-module of rank n. Moreover $\mathbb{Z}_K$ is a Noetherian ring: indeed, since $\mathbb{Z}$ is Noetherian and $\mathbb{Z}_K$ is finitely generated as a $\mathbb{Z}$-module, by Proposition 2.3 $\mathbb{Z}_K$ is a Noetherian $\mathbb{Z}$-module. This means that $\mathbb{Z}_K$ satisfies (ACC) on $\mathbb{Z}$-submodules, so certainly it satisfies (ACC) on $\mathbb{Z}_K$-submodules. Finally, by Theorem 2.29e), we have that $\dim \mathbb{Z}_K = 1$. In the next chapter we will define a *Dedekind domain* to be a Noetherian, one-dimensional integrally closed domain; thus $\mathbb{Z}_K$ is a Dedekind domain.

The proof of Theorem 2.30 does not actually compute a $\mathbb{Z}$-basis for $\mathbb{Z}_K$. In general to do so is a nontrivial problem. We will present an algorithm for this later in the course. For now, we treat the case of $n = 2$:

Every quadratic number field is of the form $K = \mathbb{Q}(\sqrt{d})$ for a squarefree $d \in \mathbb{Z} \setminus \{0, 1\}$. We will compute $\mathbb{Z}_K$. First, we observe that $\sqrt{d} \in \mathbb{Z}_K$: indeed $\sqrt{d}$ satisfies the monic polynomial $t^2 - d \in \mathbb{Z}[t]$. It follows that $\mathbb{Z}[\sqrt{d}] \subseteq \mathbb{Z}_K$. Notice that $\mathbb{Z}[\sqrt{d}]$ is itself a free $\mathbb{Z}$-module generated by 1 and $\sqrt{d}$. So the only honest first guess is that $\mathbb{Z}_K = \mathbb{Z}[\sqrt{d}]$. It turns out that this may or may not be true, depending on d.

Indeed, an arbitrary element of K can be written as $\alpha = a + b\sqrt{d}$ with $a, b \in \mathbb{Q}$. Since $(\alpha - a)^2 = db^2$, we have found the minimal polynomial of α: it is

$$P(t) = t^2 - 2a\alpha + a^2 - db^2.$$

The ring $\mathbb{Z}$ is a PID, hence a UFD, hence integrally closed. So by Theorem 2.27b), we get that $\alpha \in \mathbb{Z}_K$ if and only if $P(t) \in \mathbb{Z}[t]$, hence if and only if $2a, a^2 - db^2 \in \mathbb{Z}$.

Suppose first that $a \in \mathbb{Z}$. Then we get that $db^2 \in \mathbb{Z}$. Since d is squarefree, this happens if and only if $b \in \mathbb{Z}$

Now suppose that $2a \in \mathbb{Z}$ but $a \notin \mathbb{Z}$, so that $a = \frac{c}{2}$ with c an odd integer. Then $a^2 - db^2 = \frac{c^2 - 4db^2}{4} \in \mathbb{Z}$, so there exists an integer e with $c^2 - 4db^2 = 4e$. Such an e exists only if $\mathrm{ord}_2(b) = -1$ and $d \equiv 1 \pmod 4$. We conclude that if $d \equiv 2, 3 \pmod 4$ $\mathbb{Z}_K = \mathbb{Z}[\sqrt{d}]$, whereas if $d \equiv 1 \pmod 4$, $\mathbb{Z}_K$ is the set of all $a + b\sqrt{d}$ where a, b are rational numbers which are either both integers or both half-integers. A little thought shows that this latter case can be written more cleanly as $\mathbb{Z}_K = \mathbb{Z}[\frac{1+\sqrt{d}}{2}]$.

In summary:

THEOREM 2.31. *Let d be a squarefree integer not equal to 0 or 1, and put $K = \mathbb{Q}(\sqrt{d})$. Then:*

$$\mathbb{Z}_K = \begin{cases} \mathbb{Z}[\sqrt{d}] & d \equiv 2, 3 \pmod 4 \\ \mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right] & d \equiv 1 \pmod 4. \end{cases}$$

11. The Dual Module

If R is a ring and M and N are R-modules, the set $\mathrm{Hom}_R(M,N)$ of R-module maps from M to N itself has the structure of an R-module: for $f_1, f_2 \in \mathrm{Hom}_R(M,N)$ and $a \in R$, we put

$$(af_1 + f_2) \coloneqq (m \mapsto af_1(m) + f_2(m).$$

Note that we are using here that R is commutative.

Exercise 2.29. *Let M, M_1, M_2, N, N_1, N_2 be R-modules. In the following exercise we state equalities; they are actually canonical isomorphisms that ist is your task to define.*

a) *Show:* $\mathrm{Hom}_R(R,N) = N$.
b) *Show:* $\mathrm{Hom}_R(M_1 \oplus M_2, N) = \mathrm{Hom}_R(M_1,N) \oplus \mathrm{Hom}_R(M_2,N)$.
c) *Show:* $\mathrm{Hom}_R(M, N_1 \oplus N_2) = \mathrm{Hom}_R(M,N_1) \oplus \mathrm{Hom}_R(M,N_2)$.
d) *An R-module map $\varphi : M_1 \to M_2$ induces an R-module map*

$$\varphi^* : \mathrm{Hom}_R(M_2,N) \to \mathrm{Hom}_R(M_1,N).$$

If φ is surjective, then φ^* is injective.
e) *An R-module map $\psi : N_1 \to N_2$ induces an R-module map*

$$\psi_* : \mathrm{Hom}_R(M,N_1) \to \mathrm{Hom}_R(M,N_2).$$

If ψ is injective, then ψ_* is injective.

Proposition 2.32. *If R is Noetherian and M and N are finitely generated, then $\mathrm{Hom}_R(M,N)$ is also finitely generated.*

Proof. Since M is finitely generated, there is $n \in \mathbb{Z}^+$ and a surjective R-module map $R^n \to M$, which by Exercise 2.30d) induces an injective R-module map $\mathrm{Hom}_R(M,N) \to \mathrm{Hom}_R(R^n,N)$. By Exercise 2.30 b) and a) we have $\mathrm{Hom}_R(R^n,N) = \mathrm{Hom}_R(R,N)^n = N^n$ is finitely generated. Since R is Noetherian, the submodule $\mathrm{Hom}_R(M,N)$ of N^n is also finitely generated. □

Exercise 2.30. *Let R be a ring, and let I be an ideal of R.*

a) *Show:* $\mathrm{Hom}_R(R/I,R) = \mathrm{ann}\, I$.
b) *Find an example of R and I such that* $\mathrm{ann}\, I$ *is not finitely generated.*

For a ring R and an R-module M, we put

$$M^\vee \coloneqq \mathrm{Hom}_R(M,R).$$

This is also an R-module, via $a \in R, f \in M^\vee \mapsto (x \in M \mapsto af(x))$. It follows from Exercise 2.30 that a map $\iota : M_1 \to M_2$ induces a map $\iota^\vee \coloneqq \iota^* : M_2^\vee \to M_1^\vee$ that is injective if ι is surjective. Moreover by Exercise 2.30 we have

$$(M_1 \oplus M_2)^\vee = M_1^\vee \oplus M_2^\vee.$$

By Proposition 2.32, when R is Noetherian and M is finitely generated, $M^\vee$ is also finitely generated. (Moreover, by Exercise 2.30, there is an ideal I in a ring R such that the dual $(R/I)^\vee$ of the cyclic module R/I is not finitely generated.)

There is a natural bilinear pairing

$$\langle \cdot, \cdot \rangle : M \times M^\vee \to R, \langle x, f \rangle \coloneqq f(x).$$

As a general rule, we should consider duals of infinitely generated modules only if we are interested in set-theoretic issues. Even for a vector space V over a field K, if $\dim V$ is infinite, then $\dim V^\vee > \dim V$ in the sense of cardinal arithmetic. Similar but wilder things can happen for infinitely generated modules over rings.

EXERCISE 2.31. *Let R be a ring, and let F be a finitely generated free R-module, with basis $e_1, \ldots, e_n$.*

a) *For $1 \leq i \leq n$, show that there is a unique $e_i^\vee \in F^\vee$ such that for all $1 \leq j \leq n$, we have*

$$e_i^\vee(e_j) = \delta(i,j) = \begin{cases} 1 & \text{if } i = j \\ 0 & \text{otherwise} \end{cases}.$$

b) *Show: $e^1, \ldots, e^n$ is a basis for $F^\vee$, called the **dual basis**.*

c) *Deduce: $F^\vee \cong F$.*

EXERCISE 2.32. *Let R be a ring, and let P be a finitely generated projective R-module. Show: $P^\vee$ is also finitely generated projective.*

For any R-module M we have a natural map

$$\iota_M : M \to M^{\vee\vee}, (x, f) \in M \times M^\vee \mapsto f(x) \in R.$$

We say that M is **torsionless** if ι_M is an injection and that M is **reflexive** if ι_M is an isomorphism.

LEMMA 2.33. *For an R-module M, the following are equivalent:*

(i) *M is torsionless.*

(ii) *There is a set I such that M is a submodule of $R^I := \prod_{i \in I} R$.*

PROOF. Suppose there is an R-module embedding $\iota : M \hookrightarrow R^I$ for some set I. For each $i \in I$, let $\pi_i : R^I \to R$ be projection onto the ith factor and let $\iota_i := \pi_i \circ \iota \in M^\vee$. For $x \in M^\bullet$, since ι is an injection there is $i \in I$ such that $\iota_i(x) \neq 0$. Thus M is torsionless. Conversely, if M is torsionless then the natural map $M \to R^{M^\vee}$ given by $x \mapsto (f(x))_{f \in M^\vee}$ is an injection. □

In particular, every submodule of a free module is torsionless.

LEMMA 2.34. *Let R be a Noetherian domain, and let M be a finitely generated R-module. The following are equivalent:*

(i) *M is torsionless.*

(ii) *M is torsionfree.*

(iii) *M is a submodule of a finitely generated free module.*

EXERCISE 2.33. *Show that the additive group $(\mathbb{Q}, +)$ of the rational numbers is a torsionfree $\mathbb{Z}$-module that is not torsionless.*

EXERCISE 2.34. *Let $G := \mathbb{Z}^{\mathbb{N}}$ be the direct* product *of countably infinitely many copies of the $\mathbb{Z}$. Show: G is a torsionless $\mathbb{Z}$-module that is not free.*

EXERCISE 2.35. a) *Show: a projective module is torsionless.*

b) *Show: a submodule of a torsionless module is torsionless.*

c) *Show: a finitely generated free module is reflexive.*

d) *Show: a finitely generated projective module is reflexive.*

12. Eisenstein's Criterion

Let A be a UFD with fraction field K. A nonzero polynomial $f = a_n t^n + \ldots + a_1 t + a_0 \in R[t]$ is **primitive** if for all $x \in A^\bullet$, if $x \mid a_i$ for all $0 \leq i \leq n$, then $x \in A^\times$. If A is a PID, a polynomial is primitive if and only if $\langle a_0, \ldots, a_n \rangle = A$, but in general the latter condition is stronger: e.g. in the UFD $A = \mathbb{C}[x, y]$, the polynomial $xt + y$ is primitive but its coefficients generate a maximal ideal $\langle x, y \rangle$.

The following is one of the results that goes under the name **Gauss's Lemma**: in [**CA**] it is derived as a corollary of another result that bears that name.

PROPOSITION 2.35. *Let A be a UFD with fraction field K, and let $f \in A[t]$ be a polynomial of positive degree.*

a) *The following are equivalent:*
   (i) *$f \in A[t]$ is irreducible.*
   (ii) *f is primitive and $f \in K[t]$ is irreducible.*

b) *The following are equivalent:*
   (i) *$f \in K[t]$ is reducible.*
   (ii) *There are $g, h \in A[t]$ such that $\deg(g), \deg(h) < \deg f$ and $f = gh$.*

PROOF. This is [**CA**, Cor. 15.25]. □

If A is a domain, $f = a_d t^d + \ldots + a_1 t + a_0 \in A[t]$ is a polynomial of positive degree and $\mathfrak{p} \in \operatorname{Spec} A$ is a prime ideal such that $a_0 \notin \mathfrak{p}^2$, for all $0 \leq i < d$ we have $a_i \in \mathfrak{p}$ and $a_d \notin \mathfrak{p}$, we say that f **is Eisenstein at** $\mathfrak{p}$.

THEOREM 2.36 (Schönnemann-Eisenstein Criterion). *Let A be a UFD with fraction field K and let*

$$f = a_d t^d + \ldots + a_1 t + a_0 \in A[t]$$

be a polynomial of positive degree. If there is $\mathfrak{p} \in \operatorname{Spec} A$ such that f is Eisenstein at $\mathfrak{p}$, then f is irreducible in $K[t]$.

PROOF. uppose to the contrary that $f \in K[t]$ is reducible. Then by Proposition 2.35 there are $g, h \in A[t]$ with $\deg(g), \deg(h) < \deg f$ and $gh = f$. Write

$$g = b_m t^m + \ldots + b_1 t + b_0 \text{ and } h = c_n t^n + \ldots + c_1 t + c_0 \text{ with} b_m c_n \neq 0.$$

Since $a_0 = b_0 c_0 \in \mathfrak{p} \setminus \mathfrak{p}^2$, t follows that exactly one of b_0 and c_0 lies in $\mathfrak{p}$: without loss of generality, we may suppose that $b_0 \notin \mathfrak{p}$ and $c_0 \in \mathfrak{p}$. Since $a_d = b_m c_n \notin \mathfrak{p}$, we have $c_n \notin \mathfrak{p}$. Let $0 < k \leq n < d$ be minimal such that $c_k \notin \mathfrak{p}$. 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, one of b_0 and c_k lies in $\mathfrak{p}$, which is a contradiction. □

For a domain A, a polynomial $f \in A[t]$ of positive degree and $\mathfrak{p} \in SpecA$, we say that f is **locally Eisenstein at** $\mathfrak{p}$ if $f \in A_{\mathfrak{p}}[t]$ is primitive and Eisenstein with respect to the maximal ideal $\mathfrak{p}A_{\mathfrak{p}}$ of the local ring $A_{\mathfrak{p}}$. Since the fraction field of $A_{\mathfrak{p}}$ if K, if f is locally Eisenstein at $\mathfrak{p}$, then Theorem 2.36 applies to show that $f \in K[t]$ is irreducible. The following exercise shows that in a PID, being Eisenstein at $\mathfrak{p}$ is the same as being locally Eisenstein at $\mathfrak{p}$.

EXERCISE 2.36. *Let A be a PID, and let $f \in A[t]$ be a polynomial of positive degree. Let $\mathfrak{p} \in \operatorname{MaxSpec} A$.*

a) *Show:* $f \in A[t]$ *is primitive if and only if* $f \in A_{\mathfrak{p}}[t]$ *is primitive for all* $\mathfrak{p} \in \operatorname{MaxSpec} A$.
b) *Let* $\mathfrak{p} \in \operatorname{MaxSpec} A$. *Show:* f *is Eisenstein at* $\mathfrak{p}$ *if and only if* $f \in A_{\mathfrak{p}}[t]$ *is Eisenstein at* $\mathfrak{p}A_{\mathfrak{p}}$.

CHAPTER 3

Dedekind Domains

1. PIDs and DVRs

Let R be a PID: a domain that is not a field and for which each ideal is principal. Let K be the fraction field of R.

Then R is certainly Noetherian: indeed, every ideal is generated by a single element. By Exercise 2.1 a PID has Krull dimension 1.

Moreover R is a unique factorization domain (UFD). This is a well-known undergraduate level result that can be established e.g. by first establishing that the gcd of any two elements can be expressed as a linear combination of those elements and then proving "Euclid's Lemma" that irreducible elements generate prime ideals. Here is a slightly more sophisticated approach:

THEOREM 3.1 (Kaplansky). *For a Noetherian domain R, the following are equivalent:*

(i) *R is a UFD.*
(ii) *Every height 1 prime of R is principal.*

PROOF. See [**CA**, Cor. 15.2]. □

The module theory of PIDs is also especially simple and pleasant.

THEOREM 3.2. *Let R be a PID. Let M be a finitely generated R-module, and let N be any R-module.*

a) *M is isomorphic to a direct sum of cyclic R-modules.*
b) *M is torsionfree if and only if M is free.*
c) *The following are equivalent:*
   (i) *N is free.*
   (ii) *N is projective.*
   (iii) *N is a submodule of a free module.*
d) *The following are equivalent:*
   (i) *N is torsionfree.*
   (ii) *N is flat.*

PROOF. a) This is [**CA**, Thm. 16.11]. b) This is [**CA**, Prop. 3.62].
c) Certainly (i) implies both (ii) and (iii). That (iii) $\implies$ (i) is part of [**CA**, Thm. 3.60]. Suppose N is projective. If N is finitely generated, then finitely generated projective implies finitely generated torsionfree implies finitely generated free, the latter by part b). It is a general result of Bass that over any Noetherian domain R (or more generally, any Noetherian ring R without nontrivial idempotents) that

every infinitely generated projective module is free [**CA**, Thm. 6.11].
d) This is [**CA**, Cor. 3.96]. □

For a module over any domain R we have
free $\implies$ projective $\implies$ flat $\implies$ torsionfree.

Theorem 3.2 says that all of these conditions coincide for *finitely generated* modules over a PID. For infinitely generated modules we still have that free = projective and flat = torsionfree, but these two classes remain distinct: e.g. the additive group of $(\mathbb{Q}, +)$ is a torsionfree but not free $\mathbb{Z}$-module. In fact:

EXERCISE 3.1. *Let R be a domain that is not a field, with fraction field K. Show: the R-module K is flat but not projective.*

The $\mathbb{Z}$-module $(\mathbb{Q}, +)$ is also not a direct sum of cyclic modules. In fact, by a result of Cohen-Kaplansky, the rings R over which *every* R-module is a direct sum of cyclic modules are precisely the principal *Artinian* rings.

All this is to say that PIDs are a truly wonderful class of rings. If you encounter a ring R "in real life", you would be delighted to learn that it is a PID, as this will make whatever you are trying to do with it much easier. The only catch is that it is usually difficult to *show* that a ring is a PID. (In a first course on the subject you learn about Euclidean rings, a subclass of Euclidean rings, and a good way to show that rings like $\mathbb{Z}$ and $k[t]$ for a field k are PIDs is to show that they are Euclidean. But this is highly unrepresentative: most of the time it is *even harder* to show that a ring is Euclidean.) As I will now try to explain, the class of PIDs is a "delicate" class of rings that is intermediate in size between two more "robust" classes: namely discrete valuation rings and Dedekind domains.

EXERCISE 3.2. *Let R be a PID, and let I be a nonzero fractional R-ideal. Show: there are distinct $\mathfrak{p}_1, \ldots, \mathfrak{p}_r \in \operatorname{MaxSpec} R$ and unique $a_1, \ldots, a_r \in \mathbb{Z}$ such that*

$$I = \mathfrak{p}_1^{a_1} \cdots \mathfrak{p}_r^{a_r}.$$

Let $\mathfrak{p} \in \operatorname{MaxSpec} R$. We use Exercise 3.2 to define a map $v_{\mathfrak{p}} : K^\times \to \mathbb{Z}$: namely, for each $x \in K^\times$ we factor the fractional ideal (x) into products of primes and define $v_{\mathfrak{p}}(x)$ to be the power of $\mathfrak{p}$ that appears.

For any field K, a map $v : K^\times \to \mathbb{Z}$ is a **discrete valuation** if:
(V0) There is $x \in K^\times$ such that $v(x) \neq 0$,
(V1) For all $x, y \in K^\times$, we have $v(xy) = v(x) + v(y)$, and
(V2) For all $x, y \in K^\times$ with $x + y \neq 0$, we have $v(x + y) \geq \min v(x), v(y)$.

We say that v is **normalized** if $v(K^\times) = \mathbb{Z}$. By (V0) and (V1), a discrete valuation is in particular a nontrivial group homomorphism $K^\times \to \mathbb{Z}$, so if it is not surjective then its image is of the form $e\mathbb{Z}$ for some $e \in \mathbb{Z}^+$. Then $\frac{1}{e}v$ is a normalized discrete valuation. So we don't miss out on much by restricting to normalized valuations.

In this context it is convenient to extend v to all of K by formally putting $v(0) = \infty$; i.e., some element that is larger than every integer.

EXERCISE 3.3. *Let R be a PID with fraction field K, and let $\mathfrak{p} \in \operatorname{MaxSpec} R$. Show: the map $v_{\mathfrak{p}}$ defined above is a normalized discrete valuation of K.*

EXERCISE 3.4. *Let K be a field, and let $v : K^\times \to \mathbb{Z}$ be a normalized discrete valuation on K. Put*

$$R \coloneqq \{x \in K^\times \mid v(x) \geq 0\} \cup \{0\}.$$

a) *Show that R is a domain with fraction field K.*
b) *Let π be an element of K with $v(\pi) = 1$. Show that R is a local PID with maximal ideal $\mathfrak{m} = (\pi)$.*

Let S be a multiplicatively closed subset of our PID R. Then the localization $S^{-1}R$ is a PID: indeed, for any localization map $\iota : R \to S^{-1}R$ and any ideal J of $S^{-1}R$ we have $J = \iota_* \iota^* J$, so every ideal in a localization comes by pushing forward an ideal of R. The pushforward of a principal ideal is principal.

Let's consider the special case in which we localize at a nonzero prime ideal $\mathfrak{p} = (\pi)$ of R. Then $R_\mathfrak{p} = (R \setminus \mathfrak{p})^{-1}R$ is a local PID. By Exercise 3.2, every nonzero fractional ideal of K is of the form (π^n) for a unique $n \in \mathbb{Z}$. Indeed $R_\mathfrak{p}$ is nothing else than the valuation ring attached to the discrete valuation $v_\mathfrak{p}$.

A **discrete valuation ring (DVR)** is a local PID. For a field K, it follows from our discussion that there is a bijective correspondence between DVRs with fraction field K and normalized discrete valuations on K. In fact, if R is a PID with fraction field K, then the discrete valuation rings $\tilde{R}$ with $R \subseteq \tilde{R} \subsetneq K$ are precisely $R_\mathfrak{p}$ for $\mathfrak{p} \in \operatorname{MaxSpec} R$.

In summary, a DVR is a local PID, so it is in particular an integrally closed Noetherian local domain of Krull dimension 1. It turns out though that all these other conditions *imply* that ideals are principal. In fact, among Noetherian local domains of Krull dimension 1, there are many equivalent "nice" conditions:

THEOREM 3.3 (DVR Recognition Theorem). *Let $(R, \mathfrak{m})$ be a one-dimensional Noetherian local domain. The following are equivalent:*

(i) *R is a PID.*
(ii) *R is a UFD.*
(iii) *R is integrally closed.*
(iv) *$\mathfrak{m}$ is principal.*
(v) *R is a* regular *local ring:* $\dim_{R/\mathfrak{m}} \mathfrak{m}/\mathfrak{m}^2 = 1$.

PROOF. This is [**CA**, Thm. 17.21]. □

For those who are geometrically minded, the last condition is probably the key one. We can view any one-dimensional Noetherian domain R as being a kind of "generalized affine curve" (or rather, as the ring of functions on such a curve, but there is a categorical equivalence here), and condition (v) at a maximal ideal $\mathfrak{p}$ of R is telling us that the curve is "nonsingular at $\mathfrak{p}$." Thus all the other conditions are necessary and sufficient for this nonsingularity in the one-dimensional case. In particular being integrally closed is what geometers call "normal." In general normality is weaker than nonsingularity but they coincide in dimension 1. It is an extremely important foundational fact that nonsingularity makes the maximal ideal principal *after localization*.

This result provdes all-important motivation for us: it allows us to see that while

PIDs are nice, in some sense the condition that ideals be "globally principal" is more than we need in order to deduce most of the other facts about PIDs of this section. Suppose instead that we consider the class of Noetherian domains R such that $R_{\mathfrak{m}}$ is a DVR for all $\mathfrak{m} \in \operatorname{MaxSpec} R$. Such a domain must be one-dimensional: since some $R_{\mathfrak{m}}$ is not a field, R is not a field, and if there were a maximal ideal $\mathfrak{m}$ of height at least 2, then $R_{\mathfrak{m}}$ would have dimension at least 2 so not be a DVR. But here is a key point: by Theorem 2.28, in order for each $R_{\mathfrak{m}}$ to be integrally closed, it is necessary and sufficient for R itself to be integrally closed. So we have shown:

THEOREM 3.4. *For a Noetherian domain R, the following are equivalent:*

(i) *R is one-dimensional and integrally closed.*
(ii) *For all $\mathfrak{m} \in \operatorname{MaxSpec} R$, the local ring $R_{\mathfrak{m}}$ is a DVR.*

2. Dedekind domains

Theorem 3.4 allows us to make the single most important definition of this text: a ring R is a **Dedekind domain** if it is an integrally closed Noetherian domain of Krull dimension 1.

Let R be a Dedekind domain, and let I be a fractional R-ideal. Then for all $\mathfrak{p} \in \operatorname{MaxSpec} R$ we have that $I_{\mathfrak{p}} := IR_{\mathfrak{p}}$ is a fractional $R_{\mathfrak{p}}$-ideal. Since $R_{\mathfrak{p}}$ is a DVR, necessarily $I_{\mathfrak{p}}$ is principal. Thus I is locally principal, hence projective, hence invertible (cf. Theorem 2.19).

Actually this is a characteristic property of Dedekind domains:

THEOREM 3.5. *Let R be a domain. The following are equivalent:*

(i) *R is a Dedekind domain.*
(ii) *Every ideal of R is a projective module.*[1]
(iii) *Every fractional ideal of R is invertible.*

PROOF. (ii) $\iff$ (iii) was 2.19. We just showed (i) $\implies$ (ii). For (iii) $\implies$ (i) see [**CA**, Thm. 20.1]. □

THEOREM 3.6. *Let R be a Dedekind domain, and let I be a nonzero, proper ideal of R. Then there are distinct $\mathfrak{p}_1, \ldots, \mathfrak{p}_r \in \operatorname{MaxSpec} R$ and $a_1, \ldots, a_r \in \mathbb{Z}^+$ such that $I = \mathfrak{p}_1^{a_1} \cdots \mathfrak{p}_r^{a_r}$.*

PROOF. Of course, if an ideal factors into a product of not necessarily distinct prime ideals, then just by grouping together instances of the same prime ideal we get a "standard form factorization" as in the statement of the theorem.

Let $\mathcal{S}$ be the set of nonzero, proper ideals of R that *do not* factor into products of primes, partially ordered under inclusion. We want to show that $\mathcal{S}$ is empty, so seeking a contradiction we assume that it is nonempty. Then because R is Noetherian there is a maximal element $I \in \mathcal{S}$. Then I is contained in some maximal ideal $\mathfrak{p}$ of R. We just saw that all nonzero ideals are invertible, so "to contain is to divide" (Lemma 2.18): we have $I = \mathfrak{p}J$ for some ideal J. Then $J := \mathfrak{p}^{-1}I$ strictly contains I (the ideal I is invertible too; alternately, in any Noetherian domain, the

[1] A module is called **hereditary** if every submodule is projective. (Seems like "hereditarily projective" would be better, no?) Thus Dedekind domains are precsiely the domains that are hereditary rings: all ideals are projective.

equality $I = \mathfrak{p}I$ would violate the Krull Intersection Theorem), so there are prime ideals $\mathfrak{q}_1, \ldots, \mathfrak{q}_s$ such that

$$\mathfrak{p}^{-1}I = \mathfrak{q}_1 \cdots \mathfrak{q}_s,$$

so

$$I = \mathfrak{p}\mathfrak{q}_1 \cdots \mathfrak{q}_s,$$

and I is a product of prime ideals after all: contradiction. □

EXERCISE 3.5. *Let R be a Dedekind domain.*

a) *Show that the factorization of an ideal into primes is* unique*: if we have not necessarily distinct prime ideals $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ and $\mathfrak{q}_1, \ldots, \mathfrak{q}_s$ such that*

$$\mathfrak{p}_1 \cdots \mathfrak{p}_r = \mathfrak{q}_1 \cdots \mathfrak{q}_s,$$

then there is a bijection $\sigma : \{1, \ldots, r\} \to \{1, \ldots, s\}$ such that for all $1 \leq i \leq r$ we have $\mathfrak{q}_{\sigma(i)} = \mathfrak{p}_i$.

b) *Let I be a fractional R-ideal. Show that there is a unique function $a : \operatorname{MaxSpec} R \to \mathbb{Z}$ such that $a(\mathfrak{p}) = 0$ for all but finitely many maximal ideals $\mathfrak{p}$ and $I = \prod_{\mathfrak{p} \in \operatorname{MaxSpec} R} \mathfrak{p}^{a(\mathfrak{p})}$. Show also that I is integral if and only if $a(\mathfrak{p}) \geq 0$ for all $\mathfrak{p} \in \operatorname{MaxSpec} R$.*

EXERCISE 3.6. *Let R be a Dedekind domain with fraction field K.*

a) *Let $\mathfrak{p} \in \operatorname{MaxSpec} R$. Define a function $v_{\mathfrak{p}} : K^\times \to \mathbb{Z}$ as follows: $v_{\mathfrak{p}}(x)$ is the power to which $\mathfrak{p}$ appears in the prime factorization of the fractional ideal (x). Show: $v_{\mathfrak{p}}$ is a normalized discrete valuation on K. Show that the corresponding valuation ring*

$$\{x \in K \mid v_{\mathfrak{p}}(x) \geq 0\} \cup \{0\}$$

is $R_{\mathfrak{p}}$.

b) *Show: $\bigcap_{\mathfrak{p} \in \operatorname{MaxSpec} R} R_{\mathfrak{p}} = R$.*

EXERCISE 3.7. *Let I, J be fractional ideals in a Dedekind domain R, and write*

$$I = \prod \mathfrak{p}^{a_{\mathfrak{p}}}, \ J = \prod \mathfrak{p}^{b_{\mathfrak{p}}}.$$

(Of course for all but finitely many $\mathfrak{p}$ we have $a_{\mathfrak{p}} = b_{\mathfrak{p}} = 0$.)

a) *Show: $I + J = \prod \mathfrak{p}^{\min a_{\mathfrak{p}}, b_{\mathfrak{p}}}$.*

b) *Show: $IJ = \prod_{\mathfrak{p}} \mathfrak{p}^{a_{\mathfrak{p}} + b_{\mathfrak{p}}}$.*

c) *Show: $I \cap J = \prod_{\mathfrak{p}} \mathfrak{p}^{\max a_{\mathfrak{p}}, b_{\mathfrak{p}}}$.*

EXERCISE 3.8. *Let I and J be fractional ideals in a Dedekind domain. We say that $I \mid J$ if $JI^{-1} \subseteq R$.*

a) *Show that the following are equivalent:*
   (i) *$I \mid J$.*
   (ii) *$J \subseteq I$.*
   (iii) *For all $\mathfrak{p} \in \operatorname{MaxSpec} R$ we have $v_{\mathfrak{p}}(I) \leq v_{\mathfrak{p}}(J)$.*

b) *Show that the set $\operatorname{Frac} R$ of fractional R-ideals, partially ordered by inclusion, is a lattice, with the least upper bound (or "join") of I and J being $I + J$ and the greatest lower bound (or "meet") of I and J being $I \cap J$.*

c) *Show: $IJ = (I \cap J)(I + J)$.*

Again it turns out that the factorization of ideals into primes characterizes Dedekind domains among all domains:

THEOREM 3.7 (Matusita, 1944). *Let R be a domain in which every nonzero, proper ideal is a product of prime ideals. Then R is a Dedekind domain.*

PROOF. This is [**CA**, Thm. 20.8]. □

3. Moving Lemma

For a fractional ideal I in a Dedekind domain, we define the **support** $\operatorname{supp} I$ to be the set of maximal ideals $\mathfrak{p}$ of R for which $v_{\mathfrak{p}}(I) \neq 0$: this is a finite set. We say that two fractional ideals I and J of R are **coprime** if their supports are disjoint: in other words, no maximal ideal $\mathfrak{p}$ appears with nonzero exponent in the factorization of both I and J.

LEMMA 3.8. *Let R be a Dedekind domain, and let $S = \{\mathfrak{p}_1, \ldots, \mathfrak{p}_n\}$ be a finite set of maximal ideals of R.*

a) *Let I be a fractional ideal of R. There is $x \in I$ such that*

$$\forall 1 \leq i \leq n,\ v_{\mathfrak{p}_i}(x) = v_{\mathfrak{p}_i}(I). \tag{1}$$

b) *[Moving Lemma] Let $\mathfrak{a}$ be a fractional ideal of R. Then there is an integral ideal $\mathfrak{b}$ of $\mathfrak{a}$ with support disjoint from S lying in the same class as $\mathfrak{a}$.*

PROOF. a) Step 1: Suppose that I is an integral ideal. We may write

$$I = \mathfrak{p}_1^{a_1} \cdots \mathfrak{p}_r^{a_r} \mathfrak{q}_1^{b_1} \cdots \mathfrak{q}_s^{b_s}$$

where the $\mathfrak{q}_j$'s are the maximal ideals containing I *other than* $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$ and $a_i \geq 0$ for all i and $b_j \geq 1$ for all j. By the Chinese Remainder Theorem, the diagonal ring homomorphism

$$R \to \prod_{i=1}^{r} R/\mathfrak{p}_i^{a_i+1} \times \prod_{j=1}^{s} R/\mathfrak{q}_j^{b_j+1}$$

is surjective. From this it follows that there is $x \in R$ such that

$$\forall i,\ x \in \mathfrak{p}_i^{a_i} \setminus \mathfrak{p}_i^{a_i+1} \text{ and } \forall j,\ x \in \mathfrak{q}_j^{b_j} \setminus \mathfrak{q}_j^{b_j+1}.$$

Equivalently, this element x satisfies

$$\forall i,\ v_{\mathfrak{p}_i}(x) = a_i = v_{\mathfrak{p}_i}(I) \text{ and } \forall j,\ v_{\mathfrak{q}_j}(x) = b_j = v_{\mathfrak{q}_j}(J).$$

This latter condition first of all ensures that x is an element of I and second of all gives (1).

Step 2: Now suppose that I is a fractional ideal; we may write $I = \frac{J}{b}$ for J an integral ideal and $b \in R^\bullet$. By part a), there is $x \in R^\bullet$ such that for every prime divisor $\mathfrak{p}$ of J we have $\operatorname{ord}_{\mathfrak{p}}(x) = \operatorname{ord}_{\mathfrak{p}}(J)$, which once again ensures that $x \in J$. Then the element $\frac{x}{b}$ does what we want: it lies in $\frac{J}{b} = I$ and

$$\forall i,\ v_{\mathfrak{p}_i}(\frac{x}{b}) = v_{\mathfrak{p}_i}(x) - v_{\mathfrak{p}_i}(b) = v_{\mathfrak{p}_i}(J) - v_{\mathfrak{p}_i}(b) = v_{\mathfrak{p}_i}(J).$$

b) Applying part a) with $I = \mathfrak{a}^{-1}$, there is $x \in \mathfrak{a}^{-1}$ such that for all $1 \leq i \leq\leq n$ we have $v_{\mathfrak{p}_i}(x) = v_{\mathfrak{p}_i}(\mathfrak{a}^{-1})$. Then the fractional ideal $\mathfrak{a}^{-1}x^{-1}$ has support prime to S and

$$\mathfrak{a}^{-1}x^{-1} \supseteq \mathfrak{a}^{-1}(\mathfrak{a}^{-1})^{-1} = R.$$

It follows that $x\mathfrak{a}$ has support prime to S and is contained in R. □

COROLLARY 3.9. *Let R be a Dedekind domain.*

a) *Exactly one of the following holds:*

(i) *R is a PID.*
(ii) *R has infinitely many nonprincipal prime ideals.*

b) *If R is semilocal – i.e.,* $\operatorname{MaxSpec} R$ *is finite – then R is a PID.*

PROOF. Let K be the fraction field of R.
a) Conditions (i) and (ii) are certainly mutually exclusive, so it suffices to assume that there is a finite subset $S \subseteq \operatorname{MaxSpec} R$ such that every $\mathfrak{p} \in (\operatorname{MaxSpec} R) \setminus S$ is principal and show that every fractional ideal of R is principal.

Let I be a fractional ideal of R. By Lemma 3.8b), there is $x \in K^\bullet$ such that the support of xI is disjoint from S. By assumption, this means that xI is of the form $\prod_{j=1}^s \mathfrak{q}_j^{b_i}$ with each $\mathfrak{q}_j$ a *principal* prime ideal and $b_i \in \mathbb{Z}$. But this means that $xI = (y)$ is principal, so $I = (\frac{y}{x})$ is principal.
b) This follows immediately from part a). □

Here are some further applications:

PROPOSITION 3.10. *Let I be a nonzero ideal in a Dedekind domain R. Then:*

a) *The ring R/I is a principal ring.*
b) *The ring R/I is Artinian. More precisely: if*

$$I = \mathfrak{p}_1^{a_1} \cdots \mathfrak{p}_r^{a_r},$$

then the ideals of R/I correspond bijectively to the ideals $\mathfrak{p}_1^{b_1} \cdots \mathfrak{p}_r^{b_r}$ of R with $0 \leq b_i \leq a_i$ for all $1 \leq i \leq r$. In particular, there are precisely $\prod_{i=1}^r (a_i + 1)$ ideals of R.

PROOF. a) The ring R/I is also a quotient of the semilocalization $R_{\mathfrak{p}_1,\ldots,\mathfrak{p}_r}$, which by Corollary 3.9 is a PID. Thus R/I is a quotient of a principal ring, hence principal.
b) This follows immediately from the fact that the ideals of R containing I are precisely $\mathfrak{p}_1^{b_1} \cdots \mathfrak{p}_r^{b_r}$ with $0 \leq b_i \leq a_i$ for all $1 \leq i \leq r$. □

For $r \in \mathbb{N}$, we say that a ring R has the **r-generation property** if every ideal of R can be generated by at most r elements. We say that a ring R has the **$(r+\epsilon)$-generation property** if for every nonzero ideal I of R and every nonzero element $x \in I$, then there are $y_1, \ldots, y_r \in R$ such that $I = \langle x, y_1, \ldots, y_r \rangle_R$.

EXERCISE 3.9. *Let $r \in \mathbb{Z}^{\geq 0}$. Suppose that a ring R has the r-generation property (resp. the $(r+\epsilon)$-generation property). Show: every localization $S^{-1}R$ of R has the r-generation property (resp. the $(r+\epsilon)$-generation property).*

THEOREM 3.11 (Asano-Jensen). *For a domain R, the following are equivalent:*

(i) *R is a Dedekind domain.*
(ii) *R has the $(1+\epsilon)$-generation property.*

PROOF. (i) $\implies$ (ii): let I be a nonzero ideal of R, and let $x \in I \setminus \{0\}$. We have a short exact sequence of R-modules

$$0 \to (x) \to I \to I/(x) \to 0.$$

By Proposition 3.10 the R-module $I/(x)$ is cyclic; let $\overline{y}$ be any generator, and lift it to $y \in I$. Then $I = \langle x, y \rangle$.
(ii) $\implies$ (ii) Suppose R has the $(1+\epsilon)$-generation property. In particular every ideal is finitely generated, so it is a Noetherian domain, so it suffices to show that for each nonzero $\mathfrak{p} \in \operatorname{Spec} R$ we have that the localization $R_{\mathfrak{p}}$ is a DVR. By the

preceding exercise, $R_{\mathfrak{p}}$ has the $(1+\epsilon)$-generation property. Let I be a nonzero, proper ideal of $R_{\mathfrak{p}}$. Then $\mathfrak{p}$ is generated by any nonzero element $x \in I\mathfrak{p}$ together with some other element $y \in \mathfrak{p}$, so

$$\mathfrak{p} = I\mathfrak{p} + yR_{\mathfrak{p}}.$$

It follows that $I + \mathfrak{p} = yR_{\mathfrak{p}} + \mathfrak{p}$, and by Nakayama's Lemma we have $I = bR_{\mathfrak{p}}$. So $R_{\mathfrak{p}}$ is a local PID, hence a DVR. □

4. Modules Over a Dedekind Domain

4.1. Structure Theory for Finitely Generated Modules.

THEOREM 3.12. *Let R be a Dedekind domain, and let M be a finitely generated R-module. Then:*

a) *$P \coloneqq M/M[\mathrm{tors}]$ is finitely generated projective, say of rank r.*
b) (i) *If $r = 0$, then $M = M[\mathrm{tors}]$.*
(ii) *If $r \geq 1$ then there is a nonzero ideal I of R such that*

$$M \cong M[\mathrm{tors}] \oplus P \cong M[\mathrm{tors}] \oplus R^{r-1} \oplus I.$$

c) *The class $[I]$ of I in $\operatorname{Pic} R$ is an isomorphism invariant of M. Thus for each $r \geq 1$, the set of isomorphism classes of rank r projective R-modules is in bijection with $\operatorname{Pic} R$.*
d) *If $M[\mathrm{tors}]$ is nontrivial, then there are $N, n_1, \ldots, n_N \in \mathbb{Z}^+$ and maximal ideals $\mathfrak{p}_1, \ldots, \mathfrak{p}_N$ of R such that*

$$M[\mathrm{tors}] \cong \bigoplus_{i=1}^{N} R/\mathfrak{p}_i^{n_i}.$$

The proof of Theorem 3.12 is not especially difficult, but it is a bit lengthy. Let us try to separate it out into steps:
Step 1: We show: each finitely generated torsion R-module is a direct sum of cyclic modules with prime power annihilator.
Step 2: We show: each finitely generated torsionfree R-module P is projective.
Step 3: We show: each rank n projective module P is isomorphic to a direct sum of rank 1 projective modules and thus to $\bigoplus_{i=1}^{n} I_i$ for nonzero ideals $I_1, \ldots, I_n$ of R.
Step 4: We show: for nonzero ideals I and J of R, we have $I \oplus J \cong IJ$.
Step 5: From Steps 3 and 4, it follows that if P is a rank n projective module then $P \cong R^{n-1} \oplus I$ for some nonzero ideal I of R. Finally, we show: the class of I in $\operatorname{Pic} R$ depends only on the isomorphism class of P.

Step 1: Let M be a finitely generated torsion R-module. If $M = \langle x_1, \ldots, x_n \rangle$ then $\operatorname{ann} M = \bigcap_{i=1}^{n} \operatorname{ann}(x_i) \supseteq \prod_{i=1}^{n} \operatorname{ann}(x_i) \supsetneq (0)$, since in any domain the product of nonzero ideals is nonzero. So we may write

$$\operatorname{ann} M = \mathfrak{p}_1^{a_1} \cdots \mathfrak{p}_r^{a_r}$$

and thus M is an $R/\mathfrak{p}_1^{a_1} \cdots \mathfrak{p}^{a_r}$ module. Since the homomorphism $R \to R/\mathfrak{p}_1^{a_1} \cdots \mathfrak{p}_r^{a_r}$ factors through the semilocalization $R_{\mathfrak{p}_1,\ldots,\mathfrak{p}_r}$, M is also an $R_{\mathfrak{p}_1,\ldots,\mathfrak{p}_r}$-module. Since $\operatorname{MaxSpec} R_{\mathfrak{p}_1,\ldots,\mathfrak{p}_r} = \{\mathfrak{p}_1, \ldots, \mathfrak{p}_r\}$ is finite, by Corolalry 3.9 we have that $R_{\mathfrak{p}_1,\ldots,\mathfrak{p}_r}$ is a PID. This allows us to completely reduce to the structure theory of finitely generated torsion modules over a PID: M is isomorphic to a direct sum of cyclic modules with prime power annihilator, i.e., to a direct sum of modules of the form

$R_{\mathfrak{p}_1,\ldots,\mathfrak{p}_r}/\mathfrak{p}_i^{a_i} \cong R/\mathfrak{p}_i^{a_i}$.

Step 2: Let P be a finitely generated torsionfree R-module. By Theorem 2.15, P is projective if and only if it is locally free: for all $\mathfrak{p} \in \operatorname{MaxSpec} R$ we have that $P_{\mathfrak{p}}$ is a free $R_{\mathfrak{p}}$-module. But this is easy: for any domain R and multiplicative subset $S \subseteq R$, if M is a finitely generated torsionfree R-module, then $M_S := M \otimes_R S^{-1}R$ is a finitely generated torsionfree $S^{-1}R$-module. So $P_{\mathfrak{p}}$ is a finitely generated torsionfree module over the local *PID* $R_{\mathfrak{p}}$...so $P_{\mathfrak{p}}$ is free.

Step 2 allows us to establish the following important fact:

PROPOSITION 3.13. *Let R be a Dedekind domain with fraction field K. For a finitely generated R-module M, the following are equivalent:*

(i) *M is projective.*
(ii) *There is a finite-dimensional K-vector space V and an injective R-module map $M \hookrightarrow V$.*

PROOF. (i) $\implies$ (ii): If M is projective, then it is torsionfree, so the map $M \hookrightarrow M \otimes_R K$ is injective (see Exercise 2.19). Take $V := M \otimes_R K$; then V is a finite-dimensional K-vector space, and we have an injection $M \hookrightarrow V$.
(ii) $\implies$ (i): Since V is a K-module, it is an R-module on which each nonzero element of R acts invertibly, hence a torsionfree R-module. Since we have an injective R-module map $M \hookrightarrow V$, we conclude that M is a finitely generated torsionfree R-module, hence projective by Step 2 above. □

Step 3: Let P be a finitely generated projective R-module of rank $r \geq 1$. Then $V := P \otimes_R K$ is an r-dimensional K-vector space. Let $\lambda : V \to K$ be a surjective K-linear map. Then $Q := \lambda(P)$ is a finitely generated R-submodule of K, hence projective by Proposition 3.13, and clearly of rank 1. Let $\mathcal{K}$ be the kernel of $\lambda|_P : P \to K$; then we have a short exact sequence of R-modules

$$0 \to \mathcal{K} \to P \to Q \to 0.$$

Because Q is projective, this sequence splits, and we have shown that $P \cong \mathcal{K} \oplus Q$. It follows that $\mathcal{K}$ is projective of rank $r-1$, so an evident inductive argument allows us to write P as a direct sum of r rank one projective modules.

Step 4: The proof here is less conceptual, and for now we will just cite the result:

LEMMA 3.14. *Let $I_1, \ldots, I_n$ be fractional ideals in a 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. See [**CA**, Lemma 20.17]. □

Step 5: Finally, suppose that I and J are fractional ideals of a Dedekind domain R. We want to show that for all $n \geq 1$, if $R^n \oplus I \cong_R R^n \oplus J$, then I and J lie in the same ideal class (the converse is immediate). Using Lemma 3.14 we have

$$R^{n+1} \oplus R = R^{n+2} \cong (R^n \oplus I) \oplus I^{-1} \cong (R^n \oplus J) \oplus I^{-1} \cong R^{n+1} \oplus JI^{-1}.$$

This means that JI^{-1} is a rank 1 projective module that is **stably free**: after taking the direct sum with a finitely generated free module, it becomes isomorphic to a finitely generated free module. By [**CA**, Prop. 7.17] we conclude that JI^{-1} is free, i.e., principal, hence J and I lie in the same ideal class.

This completes the proof of the structure theorem for finitely generated modules over a Dedekind domain. To summarize: whereas a finitely generated module M over a PID is classified up to isomorphism by a finite sequence of ideals $(\mathfrak{a}_1, \ldots, \mathfrak{a}_r)$ – such that $M[\text{tors}] \cong \bigoplus_{i=1}^r R/\mathfrak{a}_i$ – together with a natural number $r(M)$, its **rank**, to classify a finitely generated module M over a Dedekind domain, one needs one further invariant: we may write $M/M[\text{tors}] \cong R^{r-1} \oplus I$, and then that invariant is the class of I in $\operatorname{Pic} R$. We call this the **Steinitz class** $\operatorname{St}(M)$ of M. In particular:

COROLLARY 3.15. *For a finitely generated module M over a Dedekind domain, the following are equivalent:*

(i) *M is free.*
(ii) *M is torsionfree with trivial Steinitz class:* $\operatorname{St}(M) = 0$.

4.2. The Characteristic Ideal. Let R be a ring, and let M be a finite length R-module. As discussed in Chapter 1, any two Jordan-Hölder series for M have the same associated finite multiset of simple modules, and any simple R-module is isomorphic to $R/\mathfrak{m}$ for a unique $\mathfrak{m} \in \operatorname{MaxSpec} R$, so the "invariant data on M" obtained by considering Jordan-Hölder series is precisely a finite multiset of maximal ideals $\mathfrak{m}_1, \ldots, \mathfrak{m}_r$ (it is convenient to write it as a finite sequence, with the understanding that the sequence is well-defined up to permutations of the terms). From this data we define the **characteristic ideal of M**:

$$\chi(M) \coloneqq \mathfrak{m}_1 \cdots \mathfrak{m}_r.$$

EXERCISE 3.10. *Let M be a finite length R-module.*

a) *Show: $\chi(M)$ annihilates M.*
b) *Deduce: M is an $R/\chi(M)$-module. Show by example that M need not be a faithful $R/\chi(M)$-module.*

EXERCISE 3.11. *Let $0 \to M_1 \to M_2 \to M_3 \to 0$ be a short exact sequence of R-modules.*

a) *Show: M_2 has finite length if and only if both M_1 and M_3 have finite length.*
b) *If M_2 has finite length, show: $\chi(M_2) = \chi(M_1)\chi(M_3)$.*

EXERCISE 3.12. *Let R be a domain, and let M be an R-module.*

a) *Suppose that M has finite length. Show: M is finitely generated torsion.*
b) *Find a domain R and a finitely generated torsion R-module M that does* not *have finite length.*

For the rest of this section we again assume that R is a Dedekind domain.

EXERCISE 3.13. *Let R be a Dedekind domain, and let M be an R-module.*

a) *Show: M has finite length if and only if M is finitely generated torsion.*
b) *Suppose M is finitely generated torsion. As we know, we may write*

$$M \cong \bigoplus_{i=1}^r R/I_i.$$

Show: $\chi(M) = I_1 \cdots I_r$.

How should we think of the characteristic ideal $\chi(M)$ of a finitely generated torsion R-module M? By Exercise 3.10, we know that $\chi(M) \subseteq \operatorname{ann} M$, but the inequality may be strict. Indeed, if we write $M \cong \bigoplus_{i=1}^r R/I_i$, then whereas $\chi(M) = I_1 \cdots I_r$, we have $\operatorname{ann} M = \operatorname{lcm} I_1 \cdots I_r$. It follows that every nonzero ideal of R is a characteristic ideal, and a nonzero ideal I of R is the characteristic ideal of a *unique* (up to isomorphism) module if and only if I is squarefree (a product of distinct primes).

To get a little more insight, let us consider two special cases:

EXAMPLE 3.16.

a) *Suppose $R = \mathbb{Z}$. Then a $\mathbb{Z}$-module M has finite length if and only if it is finite. When this occurs, we have $M \cong \prod_{i=1}^r \mathbb{Z}/n_i\mathbb{Z}$ and then $\chi(M)$ is the ideal generated by $n_1 \cdots n_r = \#M$. Thus one interpretation of $\chi(M)$ is a measure of the "size" of M. Like the cardinality of a finite $\mathbb{Z}$-module, the characteristic ideal is multiplicative on short exact sequences.*

b) *Let k be a field, let $R = k[t]$ be the univariate polynomial ring, and let M be an R-module. Then M is finitely generated torsion if and only if it is finite-dimensional as a k-vector space. Suppose that M is finitely generated torsion. After choosing a k-basis we may identify M with k^n for some $n \in \mathbb{Z}^+$, and the R-module structure is determined by the k-linear map $t\bullet$, which we may represent as a matrix $m \in M_n(k)$. The characteristic ideal $\chi(M)$ has a unique monic polynomial generator $P(t)$, which is nothing else than the characteristic polynomial $\det(t - m)$. (See e.g.* [**Cl-IS**, Thm. 9.2]*.) This should help to explain "characteristic ideal." That $\chi(M)$ annihilates M is a version of the Cayley-Hamilton Theorem.*[2]

This example should serve to show that in general $\chi(M)$ is measuring something more refined than the "size" of M, since in this case the k-dimension n sems to be a purer measure of the size of M. In general, the length $\ell(M)$ is also measuring its size (in a different way from the k-dimension). The following exercise formalizes the fact that $\chi(M)$ is "the universal additive (on short exact sequences) invariant of M.

EXERCISE 3.14. *Let R be a Dedekind domain. Show: mapping a finite length R-module to its characteristic ideal induces an isomorphism from the Grothendieck group of the category of finite length R-modules to the group* $\operatorname{Frac} R$.

EXERCISE 3.15. *Let R be a Dedekind domain, and let $I \subseteq J$ be fractional R-ideals. Show: J/I has finite length and*

$$\chi(J/I) = IJ^{-1}.$$

EXERCISE 3.16. *Show that over a Dedekind domain R, the characteristic ideal can be computed locally: let M be a finitely generated torsion R-module. For $\mathfrak{p} \in \operatorname{MaxSpec} R$, let $M_{\mathfrak{p}} := M \otimes_R R_{\mathfrak{p}}$.*

a) *Show: $M_{\mathfrak{p}}$ is a finitely generated torsion $R_{\mathfrak{p}}$-module.*

b) *Since $R_{\mathfrak{p}}$ is a DVR, we may write $\chi(M_{\mathfrak{p}})$ as $\mathfrak{p}^{a_{\mathfrak{p}}} R_{\mathfrak{p}}$ for some $a_{\mathfrak{p}} \geq 0$. Show: we have $a_{\mathfrak{p}} = 0$ for all but finitely many $\mathfrak{p} \in \operatorname{MaxSpec} R$, and*

$$\chi(M) = \prod_{\mathfrak{p} \in \operatorname{MaxSpec} R} \mathfrak{p}^{a_{\mathfrak{p}}}.$$

[2]One could argue that in this approach to Cayley-Hamilton, most of the content resides in showing the equivalence of our two descriptions of the characteristic polynomial.

CHAPTER 4

Quadratic Lattices over a Dedekind Domain

1. Lattices: Basic Definitions

Let R be a Dedekind domain with fraction field K, and let V be a finite-dimensional K-vector space. An **R-lattice in V** is a finite-dimensional R-submodule Λ of V that spans V as a K-vector space: the last condition is equivalent to the natural map $\Lambda \otimes_R K \to V$ being an isomorphism. By Proposition 3.13, every lattice Λ is finitely generated projective, and conversely every rank r projective module Λ is a lattice in $\Lambda \otimes_R K$.

EXERCISE 4.1. *Show: R-lattices in K are precisely fractional ideals of K.*

EXERCISE 4.2. *Let V be a finite-dimensional K-vector space, and let $\Lambda_1 \subseteq \Lambda_2$ be R-lattices in V. Let M be a subset of V such that $\Lambda_1 \subseteq M \subseteq \Lambda_2$. Show that the following are equivalent:*

(i) *M is an R-lattice in V.*
(ii) *M is an R-submodule of V.*

Our definition of lattice makes sense for any domain R, but for any domain R that is not Dedekind (and not a field) there will be nonprojective lattices: indeed, already in K itself, by the previous exercise. Over a more general domain, the theory of R-lattices in K-vector spaces does not get very far without some further assumptions on the underlying R-modules.

Let V be an n-dimensional K-vector space. Choose a K-basis $(e_1, \ldots, e_n)$ and let $\mathcal{E} := \langle e_1, \ldots, e_n \rangle_R$, a free R-lattice in V. We will call the lattice $\mathcal{E}$ **standard**.

This definition, I hope, feels slightly wrong: in what way is $\mathcal{E}$ actually distinguished from all other free lattices in V? It isn't, of course.[1] What is happening is a bit more subtle: to compare lattices with each other, it will help to compare to a fixed lattice...any fixed lattice. So we fixed one.

Now let Λ be any R-lattice in V. Because Λ spans V as a K-vector space, it contains some K-basis $\lambda_1, \ldots, \lambda_n$ of V, and then each e_i is a K-linear combination of the λ_i's. Clearing denominators, there is $d \in R^\bullet$ such that for all $1 \leq i \leq n$ we have that $de_1, \ldots, de_n$ is an R-linear combination of the λ_i's hence lies in Λ. On the other hand, let $x_1, \ldots, x_N$ generate Λ as an R-module. We may write each x_i as a K-linear combination of $e_1, \ldots, e_N$, and let D be the product of all the denominators of the coefficients in each of these combinations. Thus we have shown that there are $d, D \in R^\bullet$ such that

$$d\mathcal{E} \subseteq \Lambda \subseteq \frac{1}{D}\mathcal{E}. \tag{2}$$

[1] Moreover, the fact that $\mathcal{E}$ is free will not actually be used!

EXERCISE 4.3. *Let Λ_1, Λ_2 be R-lattices in V. Show: there is $d \in R^\bullet$ such that*

$$d\Lambda_1 \subseteq \Lambda_2 \subseteq \frac{1}{d}\Lambda_1.$$

2. Action of $\mathrm{Aut}_K(V)$ on Lattices

Again let V be a finite-dimensional K-vector space. The group $\mathrm{Aut}_K(V)$ of K-linear automorphisms acts on the set of R-lattices in V. This is by no means surprising: quite generally, if R is a ring and M is an R-module, then the group $\mathrm{Aut}_R(M)$ acts on the set $\mathrm{Sub}_R(M)$ of R-submodules of M, just by $g \cdot N \coloneqq \{gn \mid n \in N\}$. The map $g : N \to gN$ is an R-module isomorphism. Since V is moreover a K-module and K is the fraction field of R, every R-linear endomorphism of V is also a K-linear endomorphism, so $\mathrm{End}_R(V) = \mathrm{End}_K(V)$ and thus

$$\mathrm{Aut}_R(V) = \mathrm{End}_R(V)^\times = \mathrm{End}_K(V)^\times = \mathrm{Aut}_K(V).$$

Thus $\mathrm{Aut}_K(V)$ acts on all R-submodules of V, and the action takes each submodule to an isomorphic submodule, so finitely generated submodules get mapped to finitely generated submodules.

As above, we choose a K-basis $e_1, \ldots, e_n$ of K and consider the standard lattice $\mathcal{E} \coloneqq \langle x_1, \ldots, x_n \rangle$. This choice of basis allows us to identify $\mathrm{Aut}_K(V)$ with $\mathrm{GL}_n(K)$.

PROPOSITION 4.1. *Let V be a finite-dimensional K-vector space with K-basis $e_1, \ldots, e_n$, and put $\mathcal{E} \coloneqq \langle e_1, \ldots, e_n \rangle$.*

a) *The orbit of $\mathrm{GL}_n(K)$ on $\mathcal{E}$ is the set of all* free *R-lattices in V.*
b) *The stabilizer of $\mathcal{E}$ is $\mathrm{GL}_n(R)$.*
c) *It follows that the set of free R-lattices in K is isomorphic as a $\mathrm{GL}_n(K)$-set to $\mathrm{GL}_n(K)/\mathrm{GL}_n(R)$.*

EXERCISE 4.4. *Prove Proposition 4.1.*

This is a good description of the free R-lattices in V. What about the others? Here is an important observation

PROPOSITION 4.2. *Let V be a (nontrivial) finite-dimensional K-vector space. Then every R-lattice in V is free if and only if R is a PID.*

PROOF. Lattices are finitely generated torsionfree R-modules, so if R is a PID they are all free. Conversely, suppose that R is not a PID, so there is a nonprincipal ideal I. Choose a basis $e_1, \ldots, e_n$ for V, and consider the lattice

$$\Lambda \coloneqq Re_1 \oplus Re_2 \ldots \oplus Ie_n \cong R^{n-1} \oplus I.$$

Then the Steinitz class $\mathrm{St}(\Lambda)$ is $[I]$, the class of I, which is nontrivial, so by Corollary 3.15 the lattice Λ is not free. □

Let Λ be any R-lattice in the n-dimensional K-vector space V. By Theorem 3.12, there is an isomorphism

$$\varphi : \left(\bigoplus_{i=1}^{n-1} R \right) \oplus I \to \Lambda.$$

If we tensor with K we get an isomorphism

$$\varphi_K : K^n \to V.$$

Let $e_1, \ldots, e_n$ be the standard basis vectors for K^n, and let $v_1, \ldots, v_n$ be their images under φ. If $I = (\alpha)$ were principal, then $v_1, \ldots, v_{n-1}, \alpha v_n$ is a basis for Λ. If I is not principal, then Λ has no basis, but we still get something rather close: Λ is the direct sum of its submodules $Rv_1, \ldots, Rv_{n-1}$, Iv_n.

From this we can deduce the following:

COROLLARY 4.3. *Let V be a finite-dimensional K-vector space.*

a) *Let Λ_1 and Λ_2 be two R-lattices in V. Then Λ_1 and Λ_2 lie in the same $\mathrm{Aut}_K(V)$-orbit if and only if they have the same Steinitz class: $\mathrm{St}(\Lambda_1) = \mathrm{St}(\Lambda_2)$.*
b) *Thus the set of $\mathrm{Aut}_K(V)$-orbits on lattices in V is naturally in bijection with $\mathrm{Pic}\, R$.*

EXERCISE 4.5. *Let I be a fractional R-ideal, and let $n \geq 2$. Find the subgroup of $\mathrm{GL}_n(K)$ that stabilizes the R-lattice $R^{n-1} \oplus I$ in K^n.*

The above considerations also serve to motivate the following definition: if Λ is an R-lattice in an n-dimensional K-vector space, then a **pseudobasis** for Λ is a K-basis $x_1, \ldots, x_n$ for which there are fractional R-ideals $\mathfrak{a}_1, \ldots, \mathfrak{a}_n$ such that

$$\Lambda = \mathfrak{a}_1 x_1 \oplus \ldots \oplus \mathfrak{a}_n x_n.$$

Above we showed that every lattice has a pseudobasis of a very particular form. But if we take the more permissive approach, we get analogues of the Hermite and Smith normal forms:

THEOREM 4.4. *Let V be an n-dimensional K-vector space.*

a) *[Hermite Normal Form] Let $y_1, \ldots, y_n$ be a K-basis for V, and let Λ be an R-lattice in V. Then there are $x_1, \ldots, x_n \in V$ and fractional R-ideals $\mathfrak{a}_1, \ldots, \mathfrak{a}_n$ such that*

$$M = \mathfrak{a}_1 x_1 \oplus \ldots \oplus \mathfrak{a}_n x_n$$

and for all $1 \leq j \leq n$, we have $x_j \in \langle y_1, \ldots, y_j \rangle_K$.
b) *[Smith Normal Form] Let Λ_1 and Λ_2 be R-lattices in V. There is a K-basis $x_1, \ldots, x_n$ of V and fractional ideals $\mathfrak{a}_1, \ldots, \mathfrak{a}_n, \mathfrak{b}_1, \ldots, \mathfrak{b}_n$ such that*

$$\Lambda_1 = \mathfrak{a}_1 x_1 \oplus \ldots \oplus \mathfrak{a}_n x_n,$$

$$\Lambda_2 = \mathfrak{b}_1 x_1 \oplus \ldots \oplus \mathfrak{b}_n x_n.$$

If for all i we put $\mathfrak{d}_i \coloneqq \mathfrak{a}_i \mathfrak{b}_i^{-1}$, then we may further require that $\mathfrak{d}_1 \subseteq \ldots \subseteq \mathfrak{d}_n$, in which case the fractional ideals $\mathfrak{d}_1, \ldots, \mathfrak{d}_n$ are uniquely determined by Λ_1 and Λ_2.

PROOF. A future version of these notes will give a full proof. For now: a complete proof of part b) (Smith Normal Form) can be found in [**O'M**, §81D]. Given this, a complete proof of part a) (Hermite Normal Form) can be found in [**Ch96**]. Cohen's article also takes an algorithmic approach that is very useful e.g. in the case in which one wishes to do computations in number fields in the "relative case": i.e., when the bottom number field is not $\mathbb{Q}$. □

3. The Fröhlich Invariant

Now to a pair of R-lattices Λ_1, Λ_2 in V we will associate a fractional R-ideal $\chi(\Lambda_2, \Lambda_1)$. Suppose first that we have a containment $\Lambda_1 \subseteq \Lambda_2$ of R-lattices in V. Since $\Lambda_2 \subseteq d\Lambda_1$ for some $d \in R^\bullet$, the quotient Λ_2/Λ_1 is a finitely generated torsion R-module, hence it has a characteristic ideal $\chi(\Lambda_2/\Lambda_1)$.

In general we choose $\alpha \in R^\bullet$ such that $\alpha\Lambda_1 \subseteq \Lambda_2$; we put

$$\chi(\Lambda_2, \Lambda_1) := (\alpha)^{-n}\chi(\Lambda_2/\alpha\Lambda_1).$$

Exercise 4.6.

a) *Show that $\chi(\Lambda_2, \Lambda_1)$ is well-defined: it does not depend upon the choice of α used to scale Λ_1 inside Λ_2.*

(b) *If $\chi(\Lambda_2, \Lambda_1)$ is an integral R-ideal, does it follow that $\Lambda_1 \subseteq \Lambda_2$?*

Exercise 4.7. *Let I and J be fractional R-ideals, viewed as lattices in the one-dimensional R-vector space K. Show:*

$$\chi(I, J) = JI^{-1}.$$

(Comment: One might have expected it to come out to be IJ^{-1} instead. The inversion is however clearly present in the defintiion: e.g. if $I \in \operatorname{Int} R$, then $\chi(R, I) = \chi(R/I) = I = IR^{-1}$.)

Exercise 4.8. *Let Λ_1 and Λ_2 be R-lattices in the n-dimensional K-vector space V. Then Smith Normal Form (Theorem 4.4b) supplies us with a K-basis $x_1, \ldots, x_n$ and fractional ideals $\mathfrak{a}_1, \ldots, \mathfrak{a}_n, \mathfrak{b}_1, \ldots, \mathfrak{b}_n$ such that*

$$\Lambda_1 = \mathfrak{a}_1 x_1 \oplus \ldots \oplus \mathfrak{a}_n x_n,$$

$$\Lambda_2 = \mathfrak{b}_1 x_1 \oplus \ldots \oplus \mathfrak{b}_n x_n.$$

For $1 \leq i \leq n$, put $\mathfrak{d}_i := \mathfrak{a}_i\mathfrak{b}_i^{-1}$. Show:

$$\chi(\Lambda_2, \Lambda_1) = \mathfrak{d}_1 \cdots \mathfrak{d}_n.$$

Proposition 4.5. *Let $\Lambda_1, \Lambda_2, \Lambda_3$ be R-lattices in the n-dimensional K-vector space V. Then:*

a)
$$\chi(\Lambda_3, \Lambda_1) = \chi(\Lambda_3, \Lambda_2)\chi(\Lambda_2, \Lambda_1).$$

b)
$$\chi(\Lambda_2, \Lambda_1) = \chi(\Lambda_1, \Lambda_2)^{-1}.$$

c) *For $\alpha \in K^\times$, we have*
$$\chi(\Lambda_2, \alpha\Lambda_1) = (\alpha^n)\chi(\Lambda_2, \Lambda_1)$$
and
$$\chi(\alpha\Lambda_2, \Lambda_1) = (\alpha^{-n})\chi(\Lambda_2, \Lambda_1).$$

Exercise 4.9. *Prove Proposition 4.5.*

Proposition 4.6. *Let V be an n-dimensional K-vector space. Let $M \in \operatorname{Aut}_K(V)$ and let Λ be an R-lattice in V. Then:*

$$\chi(\Lambda, M\Lambda) = (\det M). \tag{3}$$

PROOF. Both sides of (3) can be computed locally, so we reduce to the case of R a DVR. We may therefore assume that Λ is free: let $x_1, \ldots, x_n$ be an R-basis for Λ. Then $x_1, \ldots, x_n$ is also a K-basis for V, which we may use to represent M by a matrix in $\mathrm{GL}_n(K)$. Now let $\alpha \in K^\times$. Under replacement of M by αM, both $(\det M)$ and $\chi(\Lambda, M\Lambda)$ scale by (α^n): the former is a well-known linear algebra fact and the latter is Proposition 4.5c). Thus the result holds for M if and only if it holds for αM, so by a suitable choice of α we may assume that $M \in M_n(R) \cap \mathrm{GL}_n(K)$: i.e., the entries of M lie in R and the determinant is nonzero.[2]

The classical version of Smith Normal Form – see e.g. [**C-L**, Thm. 5.3.10] – tells us that there are matrices $P, Q \in \mathrm{GL}_n(R)$ such that PMQ is diagonal. Since $\det P, \det Q \in R^\times$, we have $(\det PMQ) = (\det M)$. Moreover, since P and Q are bijective lienar maps we have $M\Lambda = PMQ\Lambda$. Thus we may assume that M is diagonal, say with diagonal entries $d_1, \ldots, d_n \in R^\bullet$. Then $M\Lambda$ is free with basis $d_1x_1, \ldots, d_nx_n$, so $M/(M\Lambda) \cong \bigoplus_{i=1}^n R/d_iR$. Moreover, since $M \in M_n(R)$ we have $M\Lambda \subseteq \Lambda$, so the Fröhlich invariant is the characteristic ideal of the quotient:

$$\chi(\Lambda, M\Lambda) = \chi(\Lambda/M\Lambda) = \chi(\bigoplus_{i=1}^n R/d_iR) = (d_1 \cdots d_n) = (\det M). \qquad \square$$

4. The Local-Global Principle

Again we have a Dedekind domain R with fraction field K, a finite-dimensional K-vector space V. After choosing a basis $e_1, \ldots, e_n$ of V, we get a *standard lattice*

$$\mathcal{E} := \langle e_1, \ldots, e_n \rangle_R.$$

Let Λ be a lattice in V. For any multiplicatively closed subset S of R, the localization $\Lambda := S^{-1}R$ is an $S^{-1}R$-lattice in V. For each $\mathfrak{p} \in \mathrm{MaxSpec}\, R$ we put

$$\Lambda_\mathfrak{p} := \Lambda \otimes_R R_\mathfrak{p},$$

an $R_\mathfrak{p}$-lattice in V. We have

$$\Lambda \subseteq \Lambda_\mathfrak{p} \subseteq V.$$

Each $\Lambda_\mathfrak{p}$ is a simpler object than Λ: since $R_\mathfrak{p}$ is a DVR, the $R_\mathfrak{p}$-module $\Lambda_\mathfrak{p}$ is free. So it is natural to ask to what exent we can study the "global" lattice Λ in terms of the "package of local lattices" $\{\Lambda_\mathfrak{p}\}_{\mathfrak{p} \in \mathrm{MaxSpec}\, R}$. The answer is: completely!

First of all, as a special case of Proposition 2.14 we have

$$\Lambda = \bigcap_{\mathfrak{p} \in \mathrm{MaxSpec}\, R} \Lambda_\mathfrak{p}.$$

This ensures that the mapping

$$\mathcal{L} : \Lambda \mapsto \{\Lambda_\mathfrak{p}\}_{\mathfrak{p} \in \mathrm{MaxSpec}\, R}$$

that sends a global lattice to its local package is injective. It remains to determine the image of $\mathcal{L}$.

When $n = 1$ and $\mathrm{MaxSpec}\, R$ is infinite, the map $\mathcal{L}$ is not surjective. Indeed, when $n = 1$ a lattice is a fractional ideal I, and for each $\mathfrak{p}$ outside the support $\mathrm{supp}\, I$ we have $I_\mathfrak{p} = R_\mathfrak{p}$. Conversely, if for each $\mathfrak{p} \in \mathrm{MaxSpec}\, R$ we are given a

[2] If R is a domain with fraction field K and $R \subsetneq K$, then $\mathrm{GL}_n(R) \subsetneq M_n(R) \cap \mathrm{GL}_n(K)$: the right hand side consists of matrices with entries in R whose determinant lies in $R^\bullet$, while the left hand side consists of matrices with entries in R whose determinant lies in $R^\times$.

fractional $R_\mathfrak{p}$-ideal $I(\mathfrak{p})$ in such a way that $I(\mathfrak{p}) = R_\mathfrak{p}$ for all but finitely many $\mathfrak{p} \in \operatorname{MaxSpec} R$, then there is a fractional R-ideal I such that

$$\forall \mathfrak{p} \in \operatorname{MaxSpec} R,\ IR_\mathfrak{p} = I(\mathfrak{p}).$$

Indeed, we may write $I(\mathfrak{p}) = (\mathfrak{p}R_\mathfrak{p})^{a_\mathfrak{p}}$ and our assumption is that $a_\mathfrak{p} = 0$ for all but finitely many $\mathfrak{p}$, so we may (and must!) take

$$I = \prod_{\mathfrak{p} \in \operatorname{MaxSpec} R} \mathfrak{p}^{a_\mathfrak{p}}.$$

In order to generalize this to $n \geq 2$ we use our standard lattice $\mathcal{E}$, as follows:

THEOREM 4.7 (Local-Global Principle for Lattices). *With notation as above, let $\{\Lambda(\mathfrak{p})\}_{\mathfrak{p} \in \operatorname{Spec} R}$ be a package of local lattices in V. The following are equivalent:*

(i) *For all but finitely many $\mathfrak{p} \in \operatorname{MaxSpec} R$ we have $\Lambda(\mathfrak{p}) = \mathcal{E}_\mathfrak{p}$.*
(ii) *There is an R-lattice Λ in V such that $\Lambda_\mathfrak{p} = \Lambda(\mathfrak{p})$ for all $\mathfrak{p} \in \operatorname{MaxSpec} R$.*

When these conditions hold, the lattice Λ is uniquely determined: it is $\bigcap_{\mathfrak{p} \in \operatorname{MaxSpec} R} \Lambda(\mathfrak{p})$.

PROOF. (ii) $\implies$ (i) For any R-lattice Λ we have $\Lambda_\mathfrak{p} = \mathcal{E}_\mathfrak{p}$ for all but finitely many $\mathfrak{p} \in \operatorname{MaxSpec} R$. Indeed, by 2 there are $d, D \in R^\bullet$ such that

$$d\mathcal{E} \subseteq \Lambda \subseteq \frac{1}{D}\mathcal{E}$$

from which it follows that $\Lambda_\mathfrak{p} = \mathcal{E}_\mathfrak{p}$ for all $\mathfrak{p}$ lying outside the support of (dD).
(i) $\implies$ (ii): Put $\Lambda := \bigcap_{\mathfrak{p} \in \operatorname{MaxSpec} R} \Lambda(\mathfrak{p})$. We first observe that there are $d, D \in R^\bullet$ such that

$$\forall \mathfrak{p} \in \operatorname{MaxSpec} R,\ d\mathcal{E}_\mathfrak{p} \subseteq \Lambda(\mathfrak{p}) \subseteq \frac{1}{D}\mathcal{E}_\mathfrak{p}.$$

For each $\mathfrak{p}$ we can certainly find $d_\mathfrak{p}$ and $D_\mathfrak{p}$ in $R^\bullet$ such

$$d_\mathfrak{p}\mathcal{E}_\mathfrak{p} \subseteq \Lambda(\mathfrak{p}) \subseteq \frac{1}{D_\mathfrak{p}}\mathcal{E}_\mathfrak{p}$$

and because of Condition (i) we can choose $d_\mathfrak{p} = D_\mathfrak{p} = 1$ for all but finitely many $\mathfrak{p}$. Then we may take $d = \prod_\mathfrak{p} d_\mathfrak{p}$ and $D = \prod_\mathfrak{p} D_\mathfrak{p}$. It follows that

$$d\mathcal{E} = \bigcap_\mathfrak{p} d\mathcal{E}_\mathfrak{p} = \bigcap_\mathfrak{p} \Lambda(\mathfrak{p}) \subseteq \bigcap_\mathfrak{p} \frac{1}{D}\mathcal{E}_\mathfrak{p} = \frac{1}{D}\mathcal{E}.$$

Thus $\Lambda = \bigcap \Lambda(\mathfrak{p})$ is an R-submodule of V that is intermediate between two R-lattices, so it is an R-lattice. Let $\mathfrak{p} \in \operatorname{MaxSpec} R$. Since $\Lambda(\mathfrak{p})$ is an $R_\mathfrak{p}$-module containing Λ, it also contains $\langle \Lambda \rangle_{R_\mathfrak{p}} = \Lambda_\mathfrak{p}$. Conversely, let $x \in \Lambda(\mathfrak{p})$. Then x lies in $d\mathcal{E}_\mathfrak{q}$ for all but finitely many $\mathfrak{q}$, so also lies in $\Lambda(\mathfrak{q})$ for all but a finite set $\mathfrak{q}_1, \ldots, \mathfrak{q}_r$ of prime ideals. There are elements $f_1, \ldots, f_r \in R^\bullet$, each prime to $\mathfrak{p}$ such that $x \in \frac{1}{f_i}\Lambda(\mathfrak{q}_i)$ for all i. (Indeed, by The Chinese Remainder Theorem, for each $1 \leq i \leq r$ there is an element $\pi_i \in R$ such that $v_{\mathfrak{q}_i}(\pi_i) = 1$ and $v_\mathfrak{p}(\pi_i) = 0$, and we may take f_i to be any sufficiently large power of π_i.) Then $f := f_1 \cdots f_r$ is prime to $\mathfrak{p}$ and $fx \in \bigcap_\mathfrak{q} \Lambda(\mathfrak{q}) = \Lambda$. It follows that $x \in \frac{1}{f}\Lambda \subseteq \Lambda_\mathfrak{p}$. Thus $\Lambda(\mathfrak{p}) = \Lambda_\mathfrak{p}$. $\square$

5. Lattices in a Quadratic Space

5.1. Bilinear Forms on a Vector Space. Let K be a field, and let V be a finite-dimensional K-vector space. A **bilinear pairing** on V is a map

$$\langle \cdot, \cdot \rangle : V \times V \to K$$

such that

$$\forall x, y, z \in V,\ \forall \alpha \in K,\ \langle \alpha x + y, z \rangle = \alpha \langle x, z \rangle + \langle y, z \rangle$$

and

$$\forall x, y, z \in V,\ \forall \alpha \in K,\ \langle x, \alpha y + z \rangle = \alpha \langle x, y \rangle + \langle x, z \rangle.$$

Because of this, we get induced mappings

$$\Phi_L : V \to V^\vee,\ F\Phi_L(x) \mapsto \langle x, \cdot \rangle : V \to K,$$

$$\Phi_R : V \to V^\vee,\ \Phi_R(x) \mapsto \langle \cdot, x \rangle : V \to K.$$

Because V is finite-dimensional, we have $V^\vee \cong_K V$, so Φ_L is injective if and only if it is surjective if and only if it is an isomorphism. When these equivalent conditions hold, we say that the bilinear form is **left-nondegenerate**. Similarly, we say that the bilinear form is **right-nondegenerate** if Φ_R is an isomorphism (equivalently, is injective, equivalenty, is surjective).

Let $e_1, \ldots, e_n$ be a K-basis for V. Using this basis we define the **Gram matrix** of $\langle \cdot, \cdot \rangle$: it is the matrix $G \in M_n(K)$ with (i, j) entry $G(i, j) \coloneqq \langle e_i, e_j \rangle$.

EXERCISE 4.10. *Using the basis $e_1, \ldots, e_n$ we identify V with K^n. Show: for all $v, w \in K^n$ we have*

$$\langle v, w \rangle = v^T G w.$$

Thus the Gram matrix of a bilinear form completely determines the bilinear form.

PROPOSITION 4.8. *With notation as above, the following are equivalent:*

(i) *The bilinear form $\langle \cdot, \cdot \rangle$ is left-nondegnerate.*
(ii) *The bilinear form $\langle \cdot, \cdot \rangle$ is right-nondegenerate.*
(iii) *The Gram matrix G is nonsingular:* $\det G \neq 0$.

PROOF. We will identify V with K^n using the basis $e_1, \ldots, e_n$.

Suppose first that G is singular, so there is $0 \neq w \in K^n$ such that $Gw = 0$. Then for all $v \in K^n$ we have

$$\langle v, w \rangle = v^T G w = v^T 0 = 0,$$

so w is a nonzero element of Φ_R and thus the bilinear form is right-degenerate. Also $\det G^T = \det G = 0$, so there is a nonzero $v \in K^n$ such that $G^T v = 0$, so

$$0 = (G^T v)^T = v^T G,$$

from which it follows that for all $w \in K^n$ we have

$$0 = v^T G w = \langle v, w \rangle,$$

so v is a nonzero element of Φ_L and the bilinear form is also left-degenerate.

Next suppose that G is nonsingular. Then for all nonzero $w \in K^n$ we have that Gw is nonzero; if i is a nonzero component of Gw then $\langle e_i, w \rangle = e_i^T (Gw) \neq 0$, so w does not lie in the kernel of Φ_R and thus the bilinear form is right-nondegenerate. And again, G^T is nonsingular, so for all nonzero $v \in K^n$ we have that $G^T v$ is nonzero, hence $v^T G = (G^T v)^T$ is nonzero; if j is a nonzero component of $v^T G$

then $\langle v, e_j \rangle \neq 0$, so v does not lie in the kernel of Φ_L and thus the bilinear form is left-nondegenerate. □

The proof shows that we can just say **nondegenerate** or **degenerate**; there is no need to distinguish between left and right. Synonyms here include **regular** and **nonsingular**.

EXERCISE 4.11. *Let K be a field. For $i = 1, 2$, let $(V_i, \langle \cdot, \cdot \rangle_i)$ be a bilinear form on a finite-dimensional K-vector space. Put*

$$V \coloneqq V_1 \oplus V_2,$$

and define

$$\langle \cdot, \cdot \rangle : V \times V \to K$$

by: for $x_1, y_1 \in V_1$ and $x_2, y_2 \in V_2$,

$$\langle (x_1, x_2), \langle (y_1, y_2) \rangle \coloneqq \langle x_1, y_1 \rangle_1 + \langle x_2, y_2 \rangle_2.$$

*We call V the **orthogonal direct sum** of the bilinear spaces V_1 and V_2.*[3]

a) *For $i = 1, 2$, let B_i be a K-basis for V_i. Viewing V_1 and V_2 as subspaces of V via $v_1 \mapsto (v_1, 0)$ and $v_2 \mapsto (0, v_2)$, $B \coloneqq B_1 \cup B_2$ is a K-basis for V. For $i = 1, 2$, let G_i be the Gram matrix for $\langle \cdot, \cdot \rangle_i$ with respect to the basis B_i. Show that the Gram matrix for $\langle \cdot, \rangle$ is the block diagonal matrix*

$$\begin{bmatrix} G_1 & 0 \\ 0 & G_2 \end{bmatrix}.$$

b) *Deduce: V is nondegenerate if and only if both V_1 and V_2 are.*

EXERCISE 4.12. *Show that for a bilinear form $\langle \cdot, \cdot \rangle$ on a finite-dimensional K-vector space V, the following are equivalent:*

(i) *The bilinear form is **symmetric**: for all $x, y \in V$ we have $\langle x, y \rangle = \langle y, x \rangle$.*
(ii) *The Gram matrix G is symmetric: $G^T = G$.*

If we have a nondegenerate bilinear form $\langle \cdot, \cdot \rangle$ on a finite-dimensional K-vector space V, then to a K-basis $e_1, \ldots, e_n$ we attach the **dual basis** $e^1, \ldots, e^n$ of V characterized by:

$$\forall 1 \leq i, j \leq n,\ \langle e_i, e^j \rangle = \delta(i, j) \coloneqq \begin{cases} 1 & i = j \\ 0 & \text{otherwise} \end{cases}.$$

One way to see the existence is to take $e^1, \ldots, e^n$ to be the images of the dual basis $e_1^\vee, \ldots, e_n^\vee$ of $V^\vee$ under the isomorphism $\Phi_R^{-1} : V^\vee \to V$. The uniqueness is immediate from the nondegeneracy.

Although we could continue to develop the theory of not-necessarily-symmetric bilinear forms, in all of our applications we will have a symmetric form, so let us impose that condition now. In this case there is an associated **quadratic form**

$$q : V \to K,\ q(x) \coloneqq \langle x, x \rangle.$$

When the characteristic of K is not 2, one can recover the bilinear form from the associated quadratic form q, so the two structures are equivalent. We don't actually need to discuss this, but just mention it because one often speaks of the structure $(V, \langle \cdot, \cdot \rangle)$ as a **quadratic space** (rather than as a **symmetric bilinear space**).

[3]Other common terminology: **orthogonal sum**.

5.2. Bilinear Forms on a Free Module. Now suppose that in place of a field K we take a commutative ring R, and in place of a finite-dimensional K-vector space we take a finitely generated *free* R-module M. Then some of the above discussion goes through verbatim: namely, the definition of an R-bilinear form $\langle \cdot, \cdot \rangle : M \times M \to R$ is a map that is R-linear in each variable for each fixed value of the other variable. And again, a choice of a basis $e_1, \ldots, e_n$ for M gives us a **Gram matrix**

$$G_e(i,j) \coloneqq \langle e_i, e_j \rangle.$$

Note that we have put a subscripted "e" on G to remember the dependence on the basis; this will be further discussed shortly.

However, the notion of degeneracy becomes more complicated here: if R is not a field, then an R-linear endomorphism of R^n can be injective without being surjective: e.g. take $R = \mathbb{Z}$; then multiplication by 2 on $\mathbb{Z}^n$ is injective but not surjective. It is still true that a surjective R-linear endomorphism must be an isomorphism [**CA**, Thm. 3.45]. So we need more careful terminology: we say that the pairing is **left-nondegenerate** (resp. **right-nondegnerate**) if the associated map $\Phi_L : M \to M^\vee$ (resp. $\Phi_R : M \to M^\vee$) is an injection. We say that the pairing is **left-perfect** (resp. **right-perfect**) if Φ_L (resp. Φ_R) is an isomorphism.

At least in the case where R is a domain, it is not so hard to sort this all out:

PROPOSITION 4.9. *Let R be a domain, let M be finitely generated, free R-module, and let $\langle \cdot, \cdot \rangle : M \times M \to R$ be a bilinear form. Let $e_1, \ldots, e_n$ be an R-basis for M.*

a) *The following are equivalent:*
   (i) *The pairing is left-nondegenerate: $\Phi_L : M \hookrightarrow M^\vee$.*
   (ii) *The pairing is right-nondegenerate: $\Phi_R : M \hookrightarrow M^\vee$.*
   (iii) *The Gram matrix G_e (with respect to $e_1, \ldots, e_n$) has nonzero determinant.*

b) *The following are equivalent:*
   (i) *The pairing is left-perfect: $\Phi_L : M \xrightarrow{\sim} M^\vee$.*
   (ii) *The pairing is right-perfect: $\Phi_R : M \xrightarrow{\sim} M^\vee$.*
   (iii) *We have $\det G_e \in R^\times$. (In other words, $G_e \in \mathrm{GL}_n(R)$.)*
   (iv) *There are elements $e^1, \ldots, e^n$ of M such that:*

$$\forall 1 \leq i, j \leq n,\ \langle e_i, e^j \rangle = \delta(i,j).$$

PROOF. a) The proof in the case where R is a field still works to show this.
b) (ii) $\iff$ (iv): Again, if Φ_R is an isomorphism then we take e^j to be $\Phi_R^{-1}(e_j^\vee)$. Conversely, if $e^1, \ldots, e^n$ satisfy (iv) and $\ell \in M^\vee$ is an R-linear functional, then

$$\forall x \in V,\ \ell(x) = \langle x, \ell(e_1)e^1 + \ldots + \ell(e_n)e^n \rangle.$$

(Indeed, both sides agree at $x = e_1, \ldots, e_n$, so they are equal.)
(iv) $\implies$ (iii): If (iv) holds, then let $H \in M_n(R)$ be the matrix with jth column e^j. Then one can check that H is the inverse of the Gram matrix G_e, so $\det G_e \in R^\times$.
(iii) $\implies$ (ii): Similarly, if $\det G_e \in R^\times$ then G_e is invertible; if H is its inverse, then we can take e^j to be the jth column of H.
(i) $\iff$ (ii): Similarly to the above, left-perfection holds if and only if G_e^T is invertible. The adjugate equation $G_e G_e^T = (\det G_e) I_n$ shows that this happens if and only if G_e is invertible if and only if right-perfection holds. $\square$

In particular we don't need to say left-perfect or right-perfect, so we won't: we will just say **perfect**. We may also say **unimodular**, referring to the fact that the determinant of the Gram matrix is a unit in R.

Our next order of business is to examine what happens to the Gram matrix when we change the basis: let $f_1, \ldots, f_n$ be another R-basis for M, and let $P \in \mathrm{GL}_n(R)$ be the change-of-basis matrix, i.e., the unique matrix such that $Pe_i = f_i$ for all $1 \leq i \leq n$. Let G_e be the Gram matrix for $e_1, \ldots, e_n$ and G_f be the Gram matrix for $f_1, \ldots, f_n$. Then:

$$\forall 1 \leq i, j \leq n,\ \langle f_i, f_j \rangle = \langle Pe_i, Pe_j \rangle = (Pe_i)^T G_e (Pe_j) = e_i^T P^T G_e P e_j.$$

This shows that

$$G_f = P^T G_e P.$$

Taking determinants, we get

$$\det G_f = \det(P^T G_e P) = \det(G_e)(\det P)^2.$$

Since $P \in \mathrm{GL}_n(R)$, we have $\det P \in R^\times$. This shows that the "determinant" of $\langle \cdot, \cdot \rangle$ is *not* well-defined – it depends on the choice of basis – but the class of the determinant in $R/R^{\times 2}$ is well-defined. We call this class the **discriminant** $\delta(M)$ of the bilinear module $(M, \langle \cdot, \cdot \rangle)$.

5.3. Bilinear Lattices. We now wish to expand the definition of a bilinear lattice in two ways.

First let Λ be a finitely generated free R-module, which we view as an R-lattice in $V \coloneqq \Lambda \otimes_R K$. Let $\langle \cdot, \cdot \rangle : V \times V \to K$ be a K-bilinear form. Then if we restrict $\langle \cdot, \rangle$ to Λ, we do *not* necessarily get an R-bilinear form because we may not have $\langle \Lambda, \Lambda \rangle \subseteq R$. If this occurs we say that the lattice is **integral** with respect to the bilinear form. But it can be natural and useful to consider the case of not necessarily integral lattices in bilinear spaces. A little thought shows that in this case, associated to any R-basis $e_1, \ldots, e_n$ of Λ we still have a Gram matrix G_e, which however now lies in $M_n(K)$ (and in $\mathrm{GL}_n(K)$ iff the bilinear form is nondegenerate). The above discussion about change of R-basis goes through verbatim. In particular, we still have a well-defined notion of **discriminant** here: the discriminant is 0 iff the bilinear form is degenerate; otherwise the discriminant is a well-defined element of $K^\times/R^\times$, so in particular defines a *principal fractional idea* δ.

Our final generalization is probably not surprising. Namely, suppose that we have a symmetric bilinear form $\langle \cdot, \cdot \rangle$ on a finite-dimensional K-vector space V and that we have a (projective, but) not necessarily free R-lattice Λ in V. Again we define Λ to be **integral** if $\langle \Lambda, \Lambda \rangle \subseteq R$. We say that Λ is **maximal** if it is integral and not strictly contained in any other integral lattice in V.

What is clear is:

Exercise 4.13. *Let $\langle \cdot, \cdot \rangle$ be a bilinear form an a finite-dimensional K-vector space V.*

a) *Show: being integral for $\langle \cdot, \cdot \rangle$ is a local property of lattices: Λ is R-integral if and only if $\Lambda_\mathfrak{p}$ is $R_\mathfrak{p}$-integral for all $\mathfrak{p} \in \mathrm{MaxSpec}\, R$.*

b) *Show: being maximal for $\langle \cdot, \cdot \rangle$ is a local property of lattices: Λ is maximal if and only if $\Lambda_\mathfrak{p}$ is maximal for all $\mathfrak{p} \in \mathrm{MaxSpec}\, R$.*

c) *Show: for any bilinear form $\langle \cdot, \cdot \rangle$ on a finite-dimensional K-vector space V, there is an integral R-lattice in V.*

We would naturally next like to show that every integral lattice in a bilinear space V is contained in a maximal lattice. It may at first seem that this is a standard Zorn's Lemma argument, but that is not quite true. Notice that if $R \subsetneq K$ then if we ignore the bilinear form there are no maximal R-lattices in V: if $\Lambda \in \mathcal{L}(V)$ and $D \in R^\bullet \setminus R^\times$ then $\Lambda \subsetneq \frac{1}{D}\Lambda$. The proof that every integral lattice in a nondegenerate K-space is contained in maximal lattice uses the next key concept that we now define, namely the discriminant.

Let Λ be an R-lattice in the bilinear space $(V, \langle \cdot, \cdot \rangle)$. If the bilinear form is degenerate, we put $\delta(\Lambda) := 0$; now we assume that the bilinear form is nondegenerate. Then, as always when we are working with fractional ideals in a Dedekind domain, we may proceed locally: let $\mathfrak{p} \in \operatorname{MaxSpec} R$, and look at the $R_\mathfrak{p}$-lattice $\Lambda_\mathfrak{p}$ in V. Since $R_\mathfrak{p}$ is a DVR, this is is a free lattice, so has a discriminant, which is a fractional $R_\mathfrak{p}$-ideal, which we may identify with $\mathfrak{p}^{\delta_\mathfrak{p}(\Lambda)}$ for some well-defined $\delta_\mathfrak{p}(\Lambda) \in \mathbb{Z}$. We then wish to define

$$\delta(\Lambda) := \prod_{\mathfrak{p} \in \operatorname{MaxSpec} R} \mathfrak{p}^{\delta_\mathfrak{p}(\Lambda)},$$

but there is one thing to check: that $\delta_\mathfrak{p}(M) = 0$ for all but finitely many $\mathfrak{p}$. We can see this as follows: take any K-basis $e_1, \ldots, e_n$ for V, and define $\mathcal{E}$ to be the "standard" lattice

$$\mathcal{E} := \langle e_1, \ldots, e_n \rangle.$$

Then there is a finite subset S of $\operatorname{MaxSpec} R$ such that for all $\mathfrak{p} \in \operatorname{MaxSpec} R \setminus S$, we have $\mathcal{E}_\mathfrak{p} = \Lambda_\mathfrak{p}$, so it suffices to show that $\delta(\mathcal{E}_\mathfrak{p}) = R_\mathfrak{p}$ for all but finitely many $\mathfrak{p} \in \operatorname{MaxSpec} R \setminus S$. For all such $\mathfrak{p}$, $\delta(\mathcal{E}_\mathfrak{p})$ is the determinant of the Gram matrix G_e with respect to the basis $e_1, \ldots, _n$. Since the bilinear form is nondegenerate we have $\det G_e \neq 0$, and it then follows that for all but finitely many $\mathfrak{p} \in \operatorname{MaxSpec} R \setminus S$ we have that $G_e \in \mathrm{GL}_n(R_\mathfrak{p})$, so $\delta(\mathcal{E}_\mathfrak{p}) = R_\mathfrak{p}$.

Exercise 4.14. *Let R be a Dedekind domain with fraction field K. For $i = 1, 2$, let V_i be a finite-dimensional K-vector space endowed with a bilinear form $\langle \cdot, \cdot \rangle_i$. Let $V := V_1 \oplus V_2$ be the orthogonal direct sum of the biilnear spaces V_1 and V_2 (cf. Exercise 4.11). For $i = 1, 2$, let Λ_i be an R-lattice in V_i.*

a) *Show: $\Lambda := \Lambda_1 \oplus \Lambda_2$ is an R-lattice in V.*
b) *Show: $\delta(\Lambda) = \delta(\Lambda_1)\delta(\Lambda_2)$.*

It is also possible to give a "global" definition of the discriminant. For this, we first observe that for any n-tuple of elements $x_1, \ldots, x_n$ in a symmetric K-bilinear space $(V, \langle \cdot, \cdot \rangle)$ we may define the discriminant

$$\delta(x_1, \ldots, x_n) := \det \langle x_i, x_j \rangle.$$

Exercise 4.15. *With notation as above, show:*

a) *If the space is degenerate, then $\delta(x_1, \ldots, x_n) = 0$ for all $x_1, \ldots, x_n \in V$.*
b) *If the space is nondegenerate, then for $x_1, \ldots, x_n$ in V, we have that $\delta(x_1, \ldots, x_n) \neq 0$ iff $x_1, \ldots, x_n$ is a K-basis for V.*

Now we can give our global definition of the discriminant:

PROPOSITION 4.10. *Let R be a Dedekind domain with fraction field K, let V be a finite-dimensional K-vector space equipped with a symmetric bilinear form $\langle \cdot, \cdot \rangle$, and let Λ be an R-lattice in K. Let D be the fractional R-ideal generated by $\delta(x_1, \ldots, x_n)$ as $x_1, \ldots, x_n$ ranges over all n-tuples of elements of Λ. Then*

$$\delta(\Lambda) = D.$$

EXERCISE 4.16. *Prove Proposition 4.10.*

EXERCISE 4.17. *Let $(V, \langle \cdot, \cdot \rangle)$ be a finite-dimensional K-vector space equipped with a nondegenerate bilinear form.*

a) *Show: if Λ is an integral lattice, then* $\operatorname{disc}(\Lambda)$ *is an integral ideal of R.*
b) *Let $\langle \cdot, \cdot \rangle$ be the standard inner product on K^2 (in other words, the "dot product"; in* other *words, the bilinear form whose Gram matrix is the identity). Suppose R is not a field, and let $d \in R^\bullet \setminus R^\times$. With $e_1 = (1, 0)$ and $e_2 = (0, 2)$, put*

$$\Lambda \coloneqq de_1 \oplus \frac{1}{d} e_2.$$

Show: Λ is not *integral, but* $\operatorname{disc} \Lambda = R$.

THEOREM 4.11. *Let $(V, \langle \cdot, \cdot \rangle)$ be a nondegenerate bilinear K-vector space, and let $\Lambda_1, \Lambda_2 \in \mathcal{L}(V)$ be two R-lattices in V. Then:*

a) *We have $\delta(\Lambda_1) = \delta(\Lambda_2)\chi(\Lambda_1, \Lambda_2)^2$.*
b) *If $\Lambda_2 \subseteq \Lambda_1$, then $\delta(\Lambda_2) = \delta(\Lambda_1)\mathfrak{a}^2$ for an ideal $\mathfrak{a}$ of R.*

PROOF. Once again both sides can be computed locally, so we may assume that R is a DVR, so Λ_1 and Λ_2 are free R-lattices. Let $x_1, \ldots, x_n$ be an R-basis for Λ_1 and $y_1, \ldots, y_n$ be an R-basis for Λ_2, and let $P \in \mathrm{GL}_n(K)$ be such that $y_i = Px_i$ for all i. Let G_1 be the Gram matrix for the basis $x_1, \ldots, x_n$ and let G_2 be the Gram matrix for the basis $y_1, \ldots, y_n$. Then $G_2 = P^T G_1 P$, so

$$\delta(\Lambda_2) = (\det P)^2 \delta(\Lambda_1). \tag{4}$$

Moreover we have $\Lambda_2 = P\Lambda_1$, so by Propositions 4.5 and 4.6 we have

$$\chi(\Lambda_1, \Lambda_2) = \chi(\Lambda_1, P\Lambda_1) = (\det P). \tag{5}$$

Combining (4) and (5) we get part a). Part b) follows: indeed $\mathfrak{a} = \chi(\Lambda_1, \Lambda_2)$, which is an integral ideal since $\Lambda_2 \subseteq \Lambda_1$. □

COROLLARY 4.12. *Maintain the notation of Theorem 4.11. Let Λ be an integral R-lattice in V. Then Λ is contained in a maximal R-lattice in V.*

PROOF. If $\Lambda_1 \subsetneq \Lambda_2$ is a proper containment of integral R-lattices in V, then Theorem 4.11b) gives a proper containment of integral R-ideals $\operatorname{disc} \Lambda_1 \subsetneq \operatorname{disc} \Lambda_2$. Thus the ascending chain condition on ideals of R (which holds: R is Noetherian!) implies the ascending chain condition holds on integral R-lattices in V. □

EXERCISE 4.18. *Let $(V, \langle \cdot, \cdot \rangle$ be a* degenerate *quadratic K-vector space. Show: there is an integral R-lattice in V that is* not *contained in any maximal R-lattice.*

EXERCISE 4.19. *Let $\langle \cdot, \cdot \rangle$ be a nondegenerate symmetric K-bilinear form on a finite-dimensional K-vector space V, let Λ be an R-lattice in V, and let $\delta \in \operatorname{Frac} R$ be the discriminant of Λ.*

a) *Let* $[\delta]$ *be the class of* δ *in* $\operatorname{Pic} R$*. Show that* $[\delta]$ *is a square: i.e., there is* $I \in \operatorname{Frac} R$ *such that* $[\delta] = [I]^2$*.*
b) *Let* $\operatorname{St}(\Lambda)$ *be the Steinitz class of* Λ*. Show:*

$$[\delta] = \operatorname{St}(\Lambda)^2.$$

EXERCISE 4.20 (Compability of Discriminants with Localization). *Let* R *be a Dedekind domain with fraction field* K*, and let* $S \subseteq R$ *be a multiplicatively closed subset. Let* $(V, \langle \cdot, \cdot \rangle)$ *be a bilinear* K*-space, and let* Λ *be an* R*-lattice in* V*, with discriminant* $\delta_\Lambda \in \operatorname{Frac} R$*. Then* $S^{-1}\Lambda$ *is an* $S^{-1}R$*-lattice in* V*, with discriminant* $\delta_{S^{-1}\Lambda} \in \operatorname{Frac} S^{-1}R$*. Let* $\iota : R \hookrightarrow S^{-1}R$ *be the localization map. For* $I \in \operatorname{Frac} R$*, we have that* $S^{-1}I \in \operatorname{Frac}(S^{-1}R)$*. Show:*

$$\delta_{S^{-1}\Lambda} = S^{-1}\delta_\Lambda.$$

6. Dual Lattices

Throughout this section: R is a Dedekind domain with fraction field K, and a **quadratic K-space** is a finite-dimensional K-vector space V equipped with a nondegenerate symmetric bilinear form $\langle \cdot, \cdot \rangle : V \times V \to K$.

To an R-lattice Λ in a K-bilinear space we may attrach its **dual lattice**

$$\Lambda^* \coloneqq \{x \in V \mid \langle x, \Lambda \rangle \subseteq R\}.$$

We will show shortly that Λ^* is actually an R-lattice in V, but first of all we observe that Λ^* is certainly an R-submodule of V.

EXERCISE 4.21. *Equip* K *itself with the bilinear form* $\langle x, y \rangle \coloneqq xy$*. Let* $I \in \operatorname{Frac} R$*. Show:* $I^* = I^{-1}$*.*

EXERCISE 4.22. *Let* $\Lambda, \Lambda_1, \Lambda_2 \in \mathcal{L}(V)$ *and let* $\alpha \in K^\times$*.*

a) *Show:* $(\alpha\Lambda)^* = \frac{1}{\alpha}\Lambda^*$*.*
b) *Show:* $\Lambda \subseteq \Lambda^{**}$*.*
c) *Show:* $\Lambda_1 \subseteq \Lambda_2 \implies \Lambda_2^* \subseteq \Lambda_1^*$*.*

PROPOSITION 4.13. *Let* $e_1, \ldots, e_n$ *be a* K*-basis for* V*, and put* $\mathcal{E} \coloneqq \langle e_1, \ldots, e_n \rangle$*. Let* $e'_1, \ldots, e'_n$ *be the unique elements of* V *such that for all* $1 \leq i, j \leq n$ *we have* $\langle e_i, e^j \rangle = \delta(i, j)$*. Then* $\mathcal{E}^* = \langle e^1 \ldots, e^n \rangle_R$ *is a free* R*-lattice.*

PROOF. As we know, the R-span of any K-basis of V is a free R-lattice, so it suffices to show that $\mathcal{E}^* = \langle e^1 \ldots, e^n \rangle$. Half of this is immediate: for all $1 \leq j \leq n$ we have $\langle \Lambda, e^j \rangle \in \langle \langle e_i, e^j \rangle \mid 1 \leq i \leq n \rangle_R = R$, so $\langle e^1, \ldots, e^n \rangle \subseteq \mathcal{E}^*$. Conversely, let $v \in \mathcal{E}^*$ and write $v = \sum_{j=1}^n \alpha_j e^j$ for $\alpha_1, \ldots, \alpha_n \in K$. For all $1 \leq i \leq n$ we have

$$\alpha_j = \langle e_i, \sum_{j=1}^n \alpha_j e^j \rangle = \langle e_i, v \rangle \in R,$$

so $v \in \langle e^1, \ldots, e^n \rangle_R$. □

THEOREM 4.14. *Let* Λ *be an* R*-lattice in* V*. Then* Λ^* *is an* R*-lattice in* V *that is isomorphic as an* R*-module to* $\Lambda^\vee \coloneqq \operatorname{Hom}_R(\Lambda, R)$*.*

PROOF. Step 1: We can choose free R-lattices $\mathcal{E}_1$ and $\mathcal{E}_2$ such that

$$\mathcal{E}_1 \subseteq \Lambda \subseteq \mathcal{E}_2.$$

By Exercise 4.22 we have

$$\mathcal{E}_2^* \subseteq \Lambda^* \subseteq \mathcal{E}_1^*.$$

By Proposition 4.13, both $\mathcal{E}_1^*$ and $\mathcal{E}_2^*$ are (free) R-lattices; since Λ^* is an R-submodule, by Exercise 4.2, also Λ^* is an R-lattice in V.
Step 2: We define a homomorphism of R-modules

$$\varphi : \Lambda^* \to \Lambda^\vee,\ x \mapsto (m \mapsto \langle x, m\rangle).$$

We claim that the R-module homomorphism

$$\psi : \Lambda^\vee \to V,\ f \mapsto \sum_{i=1}^n f(e_i)e_i'$$

is the inverse of φ. First we need to check that for all $f \in \Lambda^\vee$ we have $\psi(f) \in \Lambda^*$, so let $f \in \Lambda^\vee$ and let $m = \sum_{j=1}^m m_j e_j \in \Lambda$. Then

$$\langle \psi(f), m\rangle = \langle \sum_{i=1}^n f(e_i)e_i', \sum_{j=1}^m m_j e_j\rangle = f(m) \in R.$$

Now let $x = \sum_{i=1}^n x_i e_i' \in \Lambda^*$. Then

$$\psi(\varphi(x)) = \sum_{i=1}^n \varphi(x)(e_i)e_i' = \sum_{i=1}^n \langle x, e_i\rangle e_i' = \sum_{i=1}^n x_i e_i' = x.$$

If $f \in \Lambda^\vee$ and $m = \sum_{j=1}^n m_j e_j \in \Lambda$ then

$$\varphi(\psi(f))(m) = \varphi(\sum_{i=1}^n f(e_i)e_i')(m) = \sum_{i=1}^n \langle f(e_i)e_i', \sum_{j=1}^n m_j e_j\rangle = f(m). \qquad \square$$

EXERCISE 4.23. *Let Λ be a lattice in a quadratic K-space. Recalling that $\operatorname{St} M$ is the Steinitz class of a finitely generated R-module, show:*

$$\operatorname{St} \Lambda^* = (\operatorname{St} \Lambda)^{-1}.$$

EXERCISE 4.24. *For $i = 1, 2$, let $(V_i, \langle\cdot,\cdot\rangle_i)$ be a quadratic K-space.*

a) *Show: $\langle\cdot,\cdot\rangle_1 + \langle\cdot,\cdot\rangle_2$ defines a nondegenerate K-bilinear pairing on $V := V_1 \oplus V_2$.*
b) *For $i = 1, 2$, let Λ_i be an R-lattice in V_i. Show: $\Lambda := \Lambda_1 \oplus \Lambda_2$ is an R-lattice in V and $\Lambda^* = \Lambda_1^* \oplus \Lambda_2^*$.*

LEMMA 4.15. *Let $(V, \langle\cdot,\cdot\rangle)$ be a quadratic K-space, and let $\Lambda \in \mathcal{L}(V)$. Let S be a multiplicative subset of R. Then*

$$(S^{-1}\Lambda)^* = S^{-1}\Lambda^*.$$

EXERCISE 4.25. *Prove Lemma 4.15.*

PROPOSITION 4.16. *Let Λ be a lattice in the quadratic K-space $(V, \langle\cdot,\cdot\rangle)$. Then $\Lambda^{**} = \Lambda$.*

PROOF. By Exercise 4.22c) we have $\Lambda \subseteq \Lambda^{**}$. By Proposition 2.13 it suffices to check the equality after replacing R by $R_{\mathfrak{p}}$ for each $\mathfrak{p} \in \operatorname{MaxSpec} R$, so we reduce to the case in which Λ is free. In view of Proposition 4.13 this comes down to the (immediate!) fact that if $e_1, \ldots, e_n$ is a K-basis of V with dual basis $e^1, \ldots, e^n$, then the dual basis of $e^1, \ldots, e^n$ is $e_1, \ldots, e_n$. □

There is an important relation among the discriminant, the dual lattice and the Fröhlich invariant:

COROLLARY 4.17. *Let $(V, \langle \cdot, \cdot \rangle)$ be a quadratic K-space. If $\Lambda \in \mathcal{L}(V)$, then:*

$$\delta(\Lambda) = \chi(\Lambda^*, \Lambda).$$

PROOF. This equality of fractional ideals can be checked locally, so we may assume that R is a DVR. Then Λ is free with basis $(e_1, \ldots, e_n)$ and Λ^* is free with basis $(e^1, \ldots, e^n)$ such that $\langle e_i, e^j \rangle = \delta(i, j)$. Let us use $e^1, \ldots, e^n$ to identify V with K^n. We may then define a matrix $M = M(i, j) \in \mathrm{GL}_n(K)$ by

$$\forall 1 \leq i \leq n,\ e_i = \sum_{k=1}^{n} M(k, i) e^k$$

and then we have

$$\Lambda = M\Lambda^*,$$

so using Proposition 4.6 we get

$$\chi(\Lambda^*, \Lambda) = \chi(\Lambda^*, M\Lambda^*) = (\det M).$$

On the other hand, for all $1 \leq i, jgf \leq n$ we calculate

$$\langle e_i, e_j \rangle = \langle \sum_{k=1}^{n} M(k, i) e^k, e_j \rangle = M(j, i).$$

This shows that if G is the Gram matrix for Λ with respect to $e_1, \ldots, e_n$, then

$$G = M^T,$$

so

$$\chi(\Lambda^*, \Lambda) = (\det M) = (\det M^T) = (\det G) = \delta(\Lambda).$$ □

EXERCISE 4.26. *Let Λ be a lattice in the quadratic K-space $(V, \langle \cdot, \cdot \rangle)$.*

a) *Show: Λ is integral if and only if $\Lambda \subseteq \Lambda^*$.*
b) *Show: $\Lambda = \Lambda^*$ if and only if Λ is integral and $\operatorname{disc}(\Lambda) = R$.*
(Exercise 4.17 shows that the second condition does not imply the first.)

I want to end this chapter with some "fancy" remarks that are motivated by Exercise 4.19. In the next chapter we will introduce the *standard ANT1 setup*: we have a Dedekind domain A with fraction field K and a finite degree sparable field extension L/K, and we take B to the integral closure of A in L. Then the *trace form* (to be studied in detail) on B/A defines a nondegenerate quadratic form $\langle x, y \rangle := \operatorname{Trace}(xy)$ on L. Using this we can define the **discriminant** $\delta_{B/A}$ as the discriminant of the A-lattice B with respect to the trace form. In the classical case $A = \mathbb{Z}$, the discriminant is a principal ideal because $\mathbb{Z}$ is a PID. However, in general – even for a relative extension of number fields – the discriminant δ is a not necessarily principal integral A-ideal, and then Exercise 4.19 applies to show that

its class in $\operatorname{Pic} A$ is a square.

We will see later that B^* is a fractional B-ideal, whose inverse

$$\Delta_{B/A} \coloneqq (B^*)^{-1}$$

is an integral B-ideal, called the **different ideal**. As we will see, it is deeply related to ramification in the extension B/A. When K is a number field, it is a theorem of Hecke from circa 1923 [**He**, Satz 176, p. 261] that the class of the different ideal $\Delta_{B/A}$ in $\operatorname{Pic} B$ is a square. This deep result raises the question of whether the squareness $[\Delta_{B/A}]$ in $\operatorname{Pic} B$ holds in the standard ANT1 setup: i.e., for the integral closure of an arbitrary Dedekind domain in a finite degree separable field extension. The answer is negative, as was shown later by Fröhlich, Serre and Tate [**FST62**].

Their example is of an arithmetic geometric character, and indeed the paper [**FST62**] is a must-read for those interested in the arithmetic of algebraic curves. It is slightly over one page long. Let me say just a little bit about their construction with the hope of tempting you to read it: they show that for an perfect field k and any nice genus zero curve $C_{/k}$ without k-rational points and containing a closed point P of degree divisible by 4 — these hypotheses are satisfied e.g. for the conic

$$C_{/\mathbb{Q}} : X^2 + Y^2 + Z^2 = 0,$$

one can take B to the the affine coordinate ring $k[C \setminus \{P\}]$. By a version of the Noether Normalization Theorem [**CA**, Thm. 14.24], there is a k-subalgebra A of B that is isomorphic to $k[t]$ and such that B is finitely generated as an A-module. It follows that B is the integral closure of A in $L \coloneqq k(C)$. If Δ is the discriminant of B/A, then it is actually an easy consequence of the Differential Pullback Theorem [**AC**, Thm. 3.18] that Δ cannot be a square in $\operatorname{Pic} B$.

In the above construction there is a lot of latitude in the choice of k, but it will *not* work to choose k finite, since genus 0 curves over a finite field necessarily have k-rational points. The authors of [**FST62**] raise the question of whether Hecke's Theorem continues to hold when A is the affine coordinate ring of a nice affine curve over a finite field (this is well-known to be the closest function field analogue of the number field case). This was shown affirmatively by Armitage [**Ar67**], who also gives a new proof of Hecke's theorem in the number field case.

Some further algebraic number theory of differents, discriminants and Steinitz classes is given in [**Sc13**].

CHAPTER 5

Algebraic Number Theory in Dedekind Domains

1. Etale Algebras

Let k be a field. In this section, by a "k-algebra" we mean a commutative ring A that contains k as a subring and is finite-dimensional as a k-vector space.

EXERCISE 5.1. *Let k be a field, and let $f, g \in k[t]$ be polynomials, not both 0. By the **gcd** of f and g we mean the monic generator of the ideal $\langle f, g \rangle$. Let l/k be a field extension. Show that $\gcd(f, g)$ as computed in $k[t]$ is the same as $\gcd(f, g)$ as computed in $l[t]$.*

EXERCISE 5.2. *Let k be a field, and let $f \in k[t]$ be a nonzero polynomial. Let f' be its "formal" derivative. We say f is **separable** if $\gcd(f, f') = 1$.*

a) *Suppose $f \in k[t]$ is irreducible. Show: f is separable if and only if $f' \neq 0$.*
b) *Show: f is separable if and only if it is squarefree (there is no irreducible polynomial p such that $p^2 \mid f$) and every irreducible factor of f is separable.*
c) *Let l/k be a field extension. Show: if $f \in k[t]$, then f is separable if and only if f is separable when regarded as a polynomial over l.*
d) *Suppose k is algebraically closed. Show: f is separable if and only if it is a product of distinct linear factors.*
e) *Let K/k be an algebraically closed extension field. Show: f is separable if and only if f splits into distinct linear factors in K.*

Recall that an algebraic field extension l/k is **separable** if for all $x \in l$, the minimal polynomial of x over k is separable.[1] This holds if and only if every finite degree subextension of l/k is separable. A field k is **perfect** if every algebraic field extension l/k is separable. If k is a field of characteristic 0, then for every $f \in k[t]$ of positive degree, we have $\deg(f') = \deg(f) - 1$, so Exercise 5.2 implies that every irreducible polynomial in $k[t]$ is separable and thus every algebraic field extension is separable: thus fields of characteristic 0 are perfect. It turns out that in characteristic $p > 0$, a field k is perfect if and only if the Frobenius endomorphism

$$\mathrm{Fr} : k \to k, \ x \mapsto x^p$$

is surjective [**Cl-FT**, Prop. 5.3]. Half of the proof goes as follows: if there is $x \in k$ that is not a pth power in k, then the polynomial

$$f \coloneqq t^p - x \in k[t]$$

turns out to be irreducible [**Cl-FT**, Lemma 9.20]. Evidently we have $f' = 0$, so f is not separable, and thus $k(x^{1/p})/k$ is an inseparable degree p field extension.

[1] In more advanced field theory one defines separability of transcendental field extensions as well: see e.g. [**Cl-FT**, §12.4]. This concept is useful when studying algebraic curves, but it will not come up in this text.

Alternately, we observe that if $x^{1/p}$ is a pth root of x in an algebraic closure of k, then

$$f = t^p - x = (t - x^{1/p})^p,$$

so f has a single root of multiplicity p.

It is clear that the Frobenius map is surjective when k is finite or when k is algebraically closed, so these fields are perfect. The simplest example of an imperfect field is a rational function field $k(t)$, where k is any field of characteristic p. Then t is certainly not a pth power in $k(t)$: every $\frac{f}{g} \in k(t)^\bullet$ has a **degree** $\deg(f) - \deg(g) \in \mathbb{Z}$, and $\deg(xy) = \deg(x) + \deg(y)$, so $\deg(f^p) = p\deg(f)$. Since $\deg(t) = 1$ and 1 is not a multiple of p, the element t is not a pth power, and thus $k(t^{1/p})/k(t)$ is an inseparable field extension.

Let k be a field. An **étale k-algebra** is a finite dimensional commutative k-algebra l that is isomorphic to $\prod_{i=1}^r l_i$ where each l_i/k is a finite degree separable field extension. The **dimension** of an étale algebra is its dimension as a k-vector space.

LEMMA 5.1. *Let A be a finite-dimensional commutative k-algebra. The following are equivalent:*

(i) *A is reduced.*
(ii) *A is a finite product of finite degree field extensions of k.*

PROOF. (i) $\implies$ (ii): The descending chain condition holds on k-submodules of A, hence on A-submodules of A: A is Artinian. By Theorem 2.5 there are local Artinian rings $(\mathfrak{r}_i, \mathfrak{m}_i)_{i=1}^r$ such that $A = \prod_{i=1}^r \mathfrak{r}_i$. Since A is reduced, so is each $\mathfrak{r}_i$. Since $\mathfrak{m}_i$ is the nilradical of $\mathfrak{r}_i$ we have $\mathfrak{m}_i = 0$ for all i, and thus $\mathfrak{r}_i$ is a field.
(ii) $\implies$ (i): Fields are reduced, and any product of reduced rings is reduced. □

EXERCISE 5.3. *Show that for a field k, the following are equivalent:*

(i) *k is perfect.*
(ii) *A finite-dimensional commutative k-algebra A is étale if and only if it is reduced.*

We say that a k-algebra A is **monogenic** if there is $x \in A$ such that the k-subalgebra of A generated by x is A itself. Evidently a k-algebra is monogenic if and only if it is a quotient of $k[t]$. Recall that every finite degree separable field extension if monogenic: the Primitive Element Corollary [**Cl-FT**, Cor. 7.3]. Does this monogenicity hold for separable k-algebras that are not fields? Let's see:

EXERCISE 5.4. *Let k be a field, and let $l = k[\alpha]$ be a field extension of degree $2 \leq d < \aleph_0$. Let $\mathcal{G}$ be the set of generators of l as a k-algebra: that is, the set of $\beta \in l$ such that $k[\beta] = l$. Show: $\mathcal{G}$ is infinite if and only if k is infinite.*

EXERCISE 5.5. *Let k be an infinite field, and let $A = \prod_{i=1}^r l_i$ be an étale k-algebra. By the Primitive Element Theorem, for $1 \leq i \leq r$, there is a monic irreducible polynomial $f_i \in k[t]$ such that $k[t]/(f_i) \cong l_i$.*

a) *Suppose that the polynomials $f_1, \ldots, f_r$ are pairwise distinct. Show that $A \cong k[t]/(f_1 \cdots f_r)$ and thus A is monogenic.*
b) *Use the previous exercise to show that we can always choose the polynomials $f_1, \ldots, f_r$ to be pairwise distinct.*

EXERCISE 5.6. *Let q be a prime power, and let $A = \mathbb{F}_q^r$, viewed as an étale $\mathbb{F}_q$-algebra. Let $N \in \mathbb{Z}^+$, and suppose we have a surjective $\mathbb{F}_q$-algebra homomorphism*

$$\varphi : \mathbb{F}_q[t_1, \ldots, t_N] \to A.$$

a) *Let $I = \langle t_1^q - t_1, \ldots, t_N^q - t_N \rangle$. Show that $I \subseteq \operatorname{Ker} \varphi$, so φ induces a surjective $\mathbb{F}_q$-algebra homomorphism*

$$\varphi : \mathbb{F}_q[t_1, \ldots, t_N]/I \to A.$$

b) *A monomial $t_1^{a_1} \cdots t_N^{a_N}$ is **reduced** if $a_i < q$ for all $1 \leq i \leq N$. A polynomial $g \in \mathbb{F}_q[t_1, \ldots, t_N]$ if it is an $\mathbb{F}_q$-linear combination of reduced monomials. Show: the number of reduced polynomials is q^{q^N}.*

c) *Show: for all $f \in \mathbb{F}_q[t_1, \ldots, t_N]$ there is a reduced polynomial g such that $f - g \in I$. Deduce:*

$$\#\mathbb{F}_q[t_1, \ldots, t_N]/I \leq q^{q^N}.$$

d) *Deduce: $q^N \geq r$.*

EXERCISE 5.7.

a) *In the notation of Exercise 5.6, show that there is an $\mathbb{F}_q$-algebra isomorphism $\mathbb{F}_q[t_1, \ldots, t_N]/I \cong \mathbb{F}_q^{q^N}$.*

b) *Show: the minimal number of generators for $\mathbb{F}_q^r$ as an $\mathbb{F}_q$-algebra is $\lceil \log_q(r) \rceil$.*

EXERCISE 5.8. *For a field k, show that the following are equivalent:*

(i) *Every étale k-algebra is isomorphic to k^n for some $n \in \mathbb{Z}^+$.*

(ii) *The field k is separably closed.*

For a k-algebra A and a field extension l/k, we may "extend scalars" to get

$$A_l \coloneqq A \otimes_k l,$$

which is an l-algebra.

EXAMPLE 5.2. *We consider $\mathbb{C}$ as an $\mathbb{R}$-algebra. Then*

$$\mathbb{C}_{\mathbb{C}} = \mathbb{C} \otimes_{\mathbb{R}} \mathbb{C} = \mathbb{R}[t]/(t^2+1) \otimes_{\mathbb{R}} \mathbb{C} \cong \mathbb{C}[t]/(t^2+1)$$

$$\cong \mathbb{C}[t]/((t+\sqrt{-1})(t-\sqrt{-1})) \cong \mathbb{C}[t]/(t+\sqrt{-1}) \times \mathbb{C}[t]/(t-\sqrt{-1}) \cong \mathbb{C} \times \mathbb{C}.$$

Notice that $\mathbb{C}$ is a field but its scalar extension $\mathbb{C}_{\mathbb{C}}$ is not. However, $\mathbb{C}_{\mathbb{C}}$ is still an étale $\mathbb{C}$-algebra.

Example 5.2 suggests that the class of étale K-algebras behaves better under extension of scalars than the class of separable field extensions. This is true: our next major result is that for a k-algebra A and a field extension l/k, A is an étale k-algebra if and only if $A_{/l}$ is an étale l-algebra. If this is true, then we can check whether a k-algebra A is étale by extending scalars to the algebraic closure $\overline{k}$, where according to Exercise 5.3 it suffices to check whether $A_{\overline{k}}$ is reduced. In fact we will establish this consequence first and use it to prove that if $A_{/l}$ is étale then so is A.

PROPOSITION 5.3. *Let k be a field, let $A_{/k}$ be a k-algebra, and let l/k be a field extension. If A is an étale k-algebra, then $A_{/l} \coloneqq A \otimes_k l$ is an étale l-algebra.*

PROOF. A finite product of étale algebras is an étale algebra, so we may assume that A/k is a finite degree separable field extension. By the Primitive Element Corollary we have $A \cong k[t]/(f)$ for some monic separable polynomial f, and then

$$A_l \cong k[t]/(f) \otimes_k l \cong l[t]/(f).$$

By Exercise 5.2, the polynomial $f \in l[t]$ remains separable and factors as $f_1 \cdots f_r$ for distinct monic separable $f_1, \ldots, f_r$. The Chinese Remainder Theorem gives

$$A_l \cong l[t]/(f) \cong \prod_{i=1}^{r} l[t]/(f_i),$$

so A_l is a separable l-algebra. □

THEOREM 5.4. *Let k be a field, and let A be a finite-dimensional commutative k-algebra. The following are equivalent:*

(i) *A is an étale k-algebra.*
(ii) *For every algebraically closed field extension K/k, the ring $A_K = A \otimes_k K$ is reduced.*
(iii) *There is an algebraically closed field extension K/k such that the ring A_K is reduced.*

PROOF. (i) $\implies$ (ii): Suppose that A is étale, and let K/k be an algebraically closed field extenion. By Proposition 5.3 we have that $A_{/K}$ is étale, hence reduced.
(ii) $\implies$ (iii) is of course immediate.
(iii) $\implies$ (i): By contraposition, it suffices to show that if A is not étale and K/k is an algebraically closed field extension, then A_K is not rediuced. Since A is a commutative Artinian ring, it is a finite product of local Artinian k-algebras, so because A is not étale, either is A is not reduced or it is a finite product of finite degree field extensions, one of which is inseparable. We take the two cases in turn:
• Suppose A is not reduced. Since A is a subring of A_K, also A_K is not reduced.
• If $A = B \times C$ is a product of two k-algebras and B_K is not reduced, then also $A_K = B_K \times C_K$ is not reduced. So we may suppose that A/k is a finite degree inseparable field extension. Let $x \in A$ be an element with inseparable minimal polynomial, so $k(x)/k$ is a monogenic inseparable subalgebra of A. Then $k[x]_K$ is a subalgebra of A_K, so it is enough to show that $k[x]_K$ is not reduced. If $f \in k[t]$ is the minimal polynomial of x, then

$$k[x]_K \cong K[t]/(f).$$

By Exercise 5.2d), we may write $f = \prod_{i=1}^{r}(t-\alpha_i)^{e_i}$ with distinct $\alpha_1, \ldots, \alpha_r \in K$ and $e_1, \ldots, e_r \in \mathbb{Z}^+$ with $e_1 \geq 2$. By the Chinese Remainder Theorem, we have

$$K[t]/(f) \cong K[t]/(t-\alpha_1)^{e_1} \times K[t]/(\prod_{i=2}^{r}(t-\alpha_i)^{e_i}).$$

Then $t-\alpha_1$ is a nonzero nilpotent in $K[t]/(t-\alpha_1)^{e_1}$, so $K[t]/(f)$ is not reduced. □

COROLLARY 5.5. *Let k be a field, and let A be a finite-dimensional commutative k-algebra. Then:*

a) *If A is an étale k-algebra, then so is every k-subalgebra of A.*
b) *Let l/k be any field extension. If A_l is an étale k-algebra, then A is an étale k-algebra.*

PROOF. a) Let B be a k-subalgebra of A. If K is any algebraically closed field containing k, then A_K is reduced, hence so is its subring B_K, so B is an étale k-algebra.
b) Let K be an algebraically closed field extension of l. Since A_l is etale, A_K is reduced. Since K is also an algebraically closed field extension of k, we conclude that A is an étale k-algebra. □

THEOREM 5.6. *Let A be a finite-dimensional commutative k-algebra. Consider the following conditions:*

(i) *A is an étale k-algebra.*
(ii) *For all $\alpha \in A$, the minimal polynomial $f \in k[t]$ of α is separable.*
(iii) *For every field extension l/k, the l-algebra $A_l := A \otimes_k l$ is reduced.*
(iv) *For every field extension l/k, the l-algebra A_l is a product of fields.*
(v) *We have $A = k[t]/(f)$ for a separable polynomial $f \in k[t]$.*

Then:

a) *We have (v) $\implies$ (i) $\iff$ (ii) $\iff$ (iii) $\iff$ (iv).*
b) *If k is infinite, then (i) $\implies$ (v).*

PROOF. a) (v) $\implies$ (i): We may assume without loss of generality that f is monic. A monic separable polynomial f is a product of distinct irreducible monic separable polynomials: $f = g_1 \cdots g_r$. By the Chinese Remainder Theorem we have

$$A = k[t]/(f) \cong \prod_{i=1}^{r} k[t]/(g_i),$$

and each $k[t]/(g_i)$ is a separable field extension of k, so A is an étale k-algebra.
(i) $\iff$ (iii): If A is étale, then by Theorem 5.4 we have $A \otimes_k K$ is reduced for every algebraically closed field extension K. Because if l/k is a field extension with algebraic closure K we have $A \otimes_k l \hookrightarrow A \otimes_k K$, also $A \otimes_k l$ is reduced, so (iii) holds. The converse follows directly from Theorem 5.4.
(i) $\implies$ (ii): Suppose that for $1 \leq i \leq r$, we have a finite degree separable field extension l_i/k such that $A = \prod_{i=1}^{r} A_i$. Let $\alpha = (\alpha_1, \ldots, \alpha_r) \in A$. Since subextensions of separable field extensions are separable, for all $1 \leq i \leq r$ the minimal polynomial $f_i \in k[t]$ of α_i is separable. Then the minimal polynomial of α is the least common multiple of $f_1, \ldots, f_r$, and the least common multiple of finitely many separable polnomials is separable.
(ii) $\implies$ (iii): First, A must be reduced: the minimal polynomial of a nonzero nilpotent element is t^k for some $k \geq 2$, which is not separable. By Lemma 5.1 we therefore have $A \cong \prod_{i=1}^{r} l_i$ with each l_i/k a finite degree field extension. If for some $1 \leq i \leq r$ the field extension l_i/k is inseparable, let $\alpha_i \in l_i$ be an element with inseparable minimal polynomial $f_i \in k[t]$. The element $\alpha \in A$ with ith coordinate α_i and all other coordinates 0 has minimal polynomial f_i, so is inseparable.
b) This is Exercise 5.5. □

EXERCISE 5.9. *Let l/k be a finite degree separable field extension.*

a) *Show: if A is a reduced k-algebra, then $A_l = A \otimes_k l$ is also reduced. (Hint: for k-algebras A and B, we have $A \otimes_k B \cong B \otimes_k A$.)*
b) *Deduce: if $f \in k[t]$ is squarefree (i.e., is a product of mutually nonassociate irreducible factors), then $f \in l[t]$ is also squarefree.*

EXERCISE 5.10. *Let l/k be a finite degree field extension. If l/k is separable, then by Proposition 5.3 we have that $l \otimes_k l$ is étale and hence reduced. In this exercise we will show that if l/k is* inseparable *then $l \otimes_k l$ is not reduced.*

a) *By definition of inseparability, there is $\alpha \in l$ such that the minimal polynomial $f \in k[t]$ of α is inseparable. Show: if $k[\alpha] \otimes_k k[\alpha]$ is not reduced, then $l \otimes_k l$ is not reduced. So we may assume that $l = k[\alpha]$ is monogenic over k.*

b) *By part a), we have $l \otimes_k l \cong l[t]/(p))$, with $p \in k[t]$ the minimal polynomial of α. In $l[t]$ we may write*

$$f = (t - \alpha)g(t).$$

By taking derivatives, show: $g(\alpha) = 0$, and thus in $l[t]$ we may write

$$f = (t - \alpha)^e h(t)$$

with $e > 1$ and $h(\alpha) \neq 0$.

c) *Deduce: $l \otimes_k l$ is not reduced.*

d) *Suppose that l/k is an inseparable algebraic extension that is not necessarily of finite degree. Show: $l \otimes_k l$ is not reduced.*

Let A_k be an étale algebra of dimension n. A **splitting field** for A is a field extension l/k such that

$$A_l \cong l^n.$$

We also say that **l splits A** if l is a splitting field for A. It follows from Corollary 5.5 and Exercise 5.8 that a separably closed extension l/k is a splitting field for every étale k-algebra. Conversely, if a field extension l/k splits every étale k-algebra, then every irreducible separable polynomial $f \in k[t]$ has a root in l, so l contains a separable closure of k.

However, any given étale algebra A admits a splitting field that is a finite Galois extension of k. Indeed, let $\overline{k}$ be an algebraic closure of k; then $A \cong \prod_{i=1}^r l_i$ with each l_i a finite degree separable subextension of $\overline{k}/k$. Let l be a subextension of $\overline{k}/k$. Then l splits A if and only if l splits l_i for all $1 \leq i \leq r$. For all $1 \leq i \leq r$, we have $l_i \cong k[t]/(f_i)$ for an irreducible separable polynomial f_i, and then l splits l_i if and only if f_i splits into linear factors in l, so l splits l_i if and only if l contains the Galois closure of l_i/l. Thus all in all, the unique minimal subextension l of $\overline{k}/k$ that splits A is the Galois closure of the compositum $l_1 \cdots l_r$, which is the splitting field of the polynomial $f_1 \cdots f_r$.

EXERCISE 5.11. *Let L/K be a degree n field extension. Show that the following are equivalent:*

(i) *L/K is Galois.*

(ii) *L is a splitting field for l: that is, $L \otimes_K L \cong L^n$.*

PROPOSITION 5.7. *Let K be a field, let A be an étale K-algebra, and let L/K be a splitting field for A. Then we have an isomorphism of étale L-algebras*

$$A_L \stackrel{\Sigma}{\to} L^{\mathrm{Hom}_K(A,L)}$$

given by

$$\Sigma : \beta \otimes \gamma \mapsto (\gamma\sigma(\beta))_\sigma.$$

PROOF. It is easy to reduce to the case in which A/K is a separable field extension, say of degree n. Because A/K is separable and L is a splitting field for K, we have $\#\operatorname{Hom}_K(A,L) = n$. Let us order the elements as $\sigma_1, \ldots, \sigma_n$. Then we have a K-algebra map

$$A \hookrightarrow L^n,\ \beta \mapsto (\sigma_1(\beta), \ldots, \sigma_n(\beta)).$$

This map has a unique extension to an L-algebra map $A_L \to L^n$, which is (up to fixing an ordering on the elements of $\operatorname{Hom}_K(A,L)$, as we have) the map Σ. Because both A_L and L^n are n-dimensional vector spaces, in order to see that Σ is an isomorphism it suffices to show that it is injective.

Suppose that $\sum_j \beta_j \otimes \gamma_j$ lies in the kernel of Σ: that is,

$$\forall 1 \leq i \leq n,\ \sum_j \sigma_i(\beta_j)\gamma_j = 0.$$

We want to show that each $\gamma_j = 0$, so assume not: then the matrix $M \in M_n(L)$ with $M(i,j) = \sigma_i(\beta_j)$ is not invertible, hence neither its transpose: there are $\lambda_1, \ldots, \lambda_n \in L$, not all zero, such that

$$\forall 1 \leq j \leq n, \sum_i \lambda_i \sigma_i(\beta_j) = 0.$$

Let $\alpha_1, \ldots, \alpha_n$ be a K-basis for A. Every element $\beta \in A$ may be written as $\beta = \sum_{j=1}^n a_j \alpha_j$ with $a_1, \ldots, a_n \in K$, so we get

$$\sum_{i=1}^n \lambda_i \sigma_i(\beta) = \sum_{i=1}^n \lambda_i \sigma_i(\sum_{j=1}^n \beta_j \alpha_j) = \sum_{j=1}^n \beta_j \sum_{i=1}^n \lambda_i \sigma_i(\alpha_j) = 0,$$

contradicting Corollary 5.15. □

2. Norm and Trace

Let $A \subseteq B$ be an extension of commutative rings such that B is free and finitely generated as an A-module. Then for any $b \in B$, the map $b\cdot : B \to B$ is B-linear hence also A-linear. After choosing an A-basis $e_1, \ldots, e_n$ of B, we may represent this map by a matrix $m(b) \in M_n(A)$. In this way we can define a **trace map**

$$T_{B/A} : B \to A,\ b \mapsto \operatorname{tr} m(b) = \sum_{i=1}^n m(b)_{i,i}.$$

The trace is an A-linear functional on B, i.e., an A-valued A-linear map. We can also define the **norm map**

$$N_{B/A} : B \to A, b \mapsto \det m(b) \in A.$$

The norm map is mutiplicative, so it restricts to a group homomorphism

$$N_{B/A} : B^\times \to A^\times.$$

EXERCISE 5.12. *Let B_1, B_2 be two ring extensions of A that are each free and finitely generated as A-modules. Show that for all $b = (b_1, b_2) \in B_1 \times B_2$, we have*

$$T_{B_1 \times B_2/A}(b_1, b_2) = T_{B_1/A}(b_1) + T_{B_2/A}(b_2)$$

and

$$N_{B_1 \times B_2/A}(b_1, b_2) = N_{B_1/A}(b_1) N_{B_2/A}(b_2).$$

The following result shows the compatibility of the trace and norm with base change. The proof is almost immediate, but it is very important.

PROPOSITION 5.8. *Let $A \subseteq B$ be a ring extension such that B is free of finite rank n as an A-module, and let $\varphi : A \to A'$ be a ring homomorphism. Then $B' := B \otimes_A A'$ is free of rank n as an A'-module, and*

$$\forall b \in B,\ \varphi(T_{B/A}(b)) = T_{B'/A'}(b \otimes 1),\ \varphi(N_{B/A}(b)) = N_{B'/A}(b \otimes 1).$$

EXERCISE 5.13. *Prove Proposition 5.8.*

THEOREM 5.9. *Let k be a field, and let A_k be an étale k-algebra. Let K/k be a field extension that splits A. Then for all $a \in A$ we have*

$$T_{A/k}(a) = \sum_{\sigma \in \mathrm{Hom}_k(A,K)} \sigma(a) \text{ and } N_{A/k}(a) = \prod_{\sigma \in \mathrm{Hom}_k(A,K)} \sigma(a).$$

PROOF. Let $n = \dim_k A$. Then the isomorphism $A_K \to K^n$ of Proposition 5.7 maps $a \otimes 1$ to $(\sigma_1(a), \ldots, \sigma_n(a))$. The matrix of multiplication by $(\sigma_1(a), \ldots, \sigma_a(n))$ is just the diagonal matrix with entries $\sigma_1(a), \ldots, \sigma_n(a)$. It follows that

$$T_{A/k}(a) = T_{A_K/K}(a \otimes 1) = T_{K^n/K}(\sigma_1(a), \ldots, \sigma_n(a)) = \sum_{i=1}^n \sigma_i(a)$$

and

$$N_{A/k}(a) = N_{A_K/K}(a \otimes 1) = N_{K^n/K}(\sigma_1(a), \ldots, \sigma_n(a)) = \prod_{i=1}^n \sigma_i(a). \qquad \square$$

PROPOSITION 5.10. *Let l/k be a field extension of degree n, and let K/k be a field containing the normal closure of l/k. Let $a \in l^\times$ have minimal polynomial $f = \sum_{i=0}^d a_i t^i \in k[t]$ that splits in K as $f = \prod_{i=1}^d (t - \alpha_i)$ (since we do not assume that l/k is separable, the α_i's need not be distinct). Let $\chi \in k[t]$ be the characteristic polynomial of $a\cdot$ acting on l. Put*

$$e := [l : k(a)].$$

Then:

a) *We have $\chi(t) = f(t)^e$.*
b) *We have $T_{l/k}(a) = e \sum_{i=1}^d \alpha_i = -e a_{d-1}$.*
c) *We have $N_{l/k}(a) = \prod_{i=1}^d \alpha_i^e = (-1)^{de} a_0^e$.*

PROOF. a) This is [**Cl-FT**, Cor. 6.5].
b),c) From part a) it follows that the eigenvalues of $a\bullet$ are the roots of f, with each multiplicity multiplied by e, so $T_{l/k} = e \sum_{i=1}^f \alpha_i$ and $N_{l/k} = \prod_{i=1}^d \alpha_i^e$. By standard algebra on roots and coefficients of polynomials we have $\alpha_1 + \ldots + \alpha_d = -a_{d-1}$ – from which the second formula for the trace follows by multiplying by e – and $\alpha_1 \cdots \alpha_d = (-1)^d a_0$ – from which the second formula for the norm follows by raising to the eth power. $\square$

Here is a generalization of Theorem 5.9 to all finite degree field extensions. It makes use of the notions of *separable degree* and *inseparable degree* of a finite degree field extension K/F. For this, see [**Cl-FT**, §5.2].

THEOREM 5.11. *Let K/F be a field extension of degree $n < \infty$ and separable degree n_s. Put $p^e = \frac{n}{n_s} = [K:F]_i$. Let $\overline{K}$ be an algebraic closure of K. Let $\alpha \in K$ and let $f(t)$ be the characteristic polynomial of $\alpha\bullet \in \mathrm{End}_F(K)$. Let $\tau_1, \ldots, \tau_{n_s}$ be the distinct F-algebra embeddings of K into $\overline{K}$. Then*

$$f(t) = \prod_{i=1}^{n_s} (t - \tau_i(\alpha))^{p^e}.$$

It follows that

$$N_{K/F}(\alpha) = (\prod_{i=1}^{n_s} \tau_i(\alpha))^{p^e} \tag{6}$$

and

$$\mathrm{Tr}_{K/F}(\alpha) = p^e \sum_{i=1}^{m} \tau_i(\alpha). \tag{7}$$

PROOF. Put $L = F[\alpha]$. Let $d = [L:F]$ be the degree, let $d_s = [L:F]_s$ be the separable degree and let $d_i = [L:F]_i$ be the inseparable degree. Also let n_s be the separable degree of K/F. Let $\sigma_1, \ldots, \sigma_{d_s}$ be the distinct F-algebra homomorphisms from L into $\overline{F}$. For each $1 \leq i \leq d_s$, σ_i extends to $\frac{n_s}{d_s}$ F-algebra homomorphisms from K into $\overline{F}$. Let

$$f(t) = (\prod_{i=1}^{d_s} (t - \sigma_i(\alpha)))^{d_i}$$

be the minimal polynomial of α over F, and let $g(t)$ be the characteristic polynomial of $\alpha\bullet$ on K, so by Proposition 5.10 we have

$$g(t) = f(t)^{[K:L]} = (\prod_{i=1}^{d_s} (t - \sigma_i(\alpha))^{d_i \frac{n}{d}} = \left((\prod_{i=1}^{d_s} (t - \sigma_i(\alpha))^{\frac{n_s}{d_s}} \right)^{n_i}$$

$$= \left(\prod_{i=1}^{n_s} (t - \tau_i(\alpha)) \right)^{p^i}.$$

Equations (6) and (7) follow immediately. □

COROLLARY 5.12. *Let A be an integrally closed domain with fraction field K, and let L/K be a finite degree field extension. If $x \in L$ is integral over A, then*

$$T_{L/K}(x),\ N_{L/K}(x) \in A.$$

PROOF. This is immediate from Proposition 5.10 and Theorem 2.27. □

THEOREM 5.13 (Transitivity of Trace and Norm). *Let $A \subseteq B \subseteq C$ be commutative rings with B free and finitely generated over A and C free and finitely generated over B. Then C is free and finitely generated over A and*

$$T_{C/A} = T_{B/A} \circ T_{C/B} \text{ and } N_{C/A} = N_{B/A} \circ N_{C/B}.$$

PROOF. That C is free and finitely generated over A is an easy exercise. The rest of it is annoyingly more difficult than one might like: it should be in my field theory notes, but isn't yet. For now, please see [**B**, §III.9.4]. □

3. The Trace Form

3.1. Definition and First Examples. Suppose that $A \subseteq B$ is an extension of commutative rings with B free of rank N as an A-module. Using the trace, we define a symmetric A-bilinear form on B:

$$\langle x, y \rangle := \mathrm{Tr}(xy).$$

We define the **discriminant** $\delta_{B/A}$ as the discriminant of the trace form; again, this is well-defined up to the square of a unit in A, hence gives a well-defined principal ideal of A. We will allow some ambiguity in whether $\delta_{B/A}$ means a principal ideal or an element of $A/A^{\times 2}$. As a rule of thumb: when $A = \mathbb{Z}$, then $\mathbb{Z}/\mathbb{Z}^{\times 2} = \mathbb{Z}$, so we may and shall regard $\delta_{B/\mathbb{Z}}$ as an integer. Otherwise we will usually regard $\delta_{B/A}$ as a principal ideal.

Exercise 5.14. *Let A be a ring, let B_1 and B_2 be A-algebras that are free and finitely generated as A-modules, and put $B := B_1 \times A_2$, so B is also an A-algebra that is free and finitely generated as an A-module.*

a) *Show: if we embed B_1 in B via $x \mapsto (x, 0)$ and B_2 in B via $y \mapsto (0, y)$, the trace form $\langle \cdot, \cdot \rangle$ on B is the orthogonal direct sum (cf. Exercise 4.11) of the trace form $\langle \cdot, \cdot \rangle_1$ on B_1 and the trace form $\langle \cdot, \cdot \rangle_2$ on B_2.*

b) *Show: we may choose A-bases for B_1, B_2 and A in such a way that the Gram matrix G for $\langle \cdot, \cdot \rangle$ is the "matrix direct sum" $\begin{bmatrix} G_1 & 0 \\ 0 & G_2 \end{bmatrix}$, where G_i is the Gram matrix for the trace form on B_i.*

c) *Deduce:*

$$\delta_{B/A} = \delta_{B_1/A} \delta_{B_2/A}.$$

In particular, the trace pairing on B is nondegenerate (resp. perfect) if the trace pairings on both B_1 and B_2 are nondegenerate (resp. perfect).

The following exercise is a refresher on quadratic field extensions, including the characteristic 2 case.

Exercise 5.15. *Let L/K be a quadratic field extension.*

a) *Suppose that K does* not *have characteristic 2. Show: there is $\alpha \in L$ with minimal polynomial $t^2 - D$ for some $D \in K^\times \setminus K^{\times 2}$, and thus $L = K[\sqrt{D}]$ and L/K is separable. Conversely, for all $D \in K^\times \setminus K^{\times 2}$, show: $t^2 - D$ is irreducible and $K[t]/(t^2 - D)$ is a separable quadratic field extension.*

b) *Suppose that K has characteristic 2 and L/K is* not *separable. Show: there is $\alpha \in L$ with minimal polynomial $t^2 - D$ for some $D \in K^\times \setminus K^{\times 2}$ and thus $L = K[\sqrt{D}]$. (Suggestion: in characteristic $p > 0$, an irreducible polynomial $f \in K[t]$ is inseparable if and only if it is of the form $f = g(t^p)$ for some $g \in K[t]$.) Conversely, for all $D \in K^\times \setminus K^{\times 2}$, show that $t^2 - D$ is an ireducible polynomial and $K[t]/(t^2 - D)$ is an inseparable quadratic field extension.*

c) *Suppose that K has characteristic 2 and L/K is separable. Show: there is $\alpha \in L$ with minimal polynomial $t^2 + t + c$ for some $c \in K$. Conversely, if $c \in K$ is not of the form $x^2 + x$ for any $x \in K$, show that $t^2 + t + c$ is irreducible and $K[t]/(t^2 + t + c)/K$ is a separable quadratic field extension.*

Exercise 5.16. *Let A be a ring, let $D \in A$, and put $B := A[t]/(t^2 - D)$. (Thus, when A is a domain and D is not a square in the fraction field of A, we*

have $B \coloneqq A[\sqrt{D}]$.) Then B is an A-algebra that is free and finitely generated as an A-module with basis given by (the images in B of) 1 and t.

a) *Let $a_0, a_1 \in A$, so $\alpha \coloneqq a_0 + a_1 t$ is an arbitrary element of B. Show that the matrix of multiplication by α with respect to the basis $1, t$ is $\begin{bmatrix} a_0 & a_1 D \\ a_1 & a_0 \end{bmatrix}$. Deduce:*

$$T_{B/A}(\alpha) = 2a_0 \text{ and } N_{B/A}(\alpha) = a_0^2 - Da_1^2.$$

b) *Show: the Gram matrix of the trace form on B/A with respect to the basis $1, t$ is $\begin{bmatrix} 2 & 0 \\ 0 & 2D \end{bmatrix}$ and thus the discriminant of B/A is $4D \pmod{A^{\times 2}}$.*

c) *Deduce: in characteristic different from 2, the trace form on a quadratic field extension is nondegenerate, while if L/K is an inseparable quadratic extension in characteristic 2, the trace map $T_{L/K}$ is identically 0.*

EXERCISE 5.17. *Let A be a ring of characteristic 2, let $c \in A$, and put $B \coloneqq A[t]/(t^2 + t + c)$. Then B is an A-algebra that is free and finitely generated as an A-module with basis given by (the images in B of) 1 and t.*

a) *Let $a_0, a_1 \in A$, so $\alpha \coloneqq a_0 + a_1 t$ is an arbitrary element of B. Show that the matrix of multiplication by α with respect to the basis $1, t$ is $\begin{bmatrix} a_0 & a_1 D \\ a_1 v & a_0 + a_1 \end{bmatrix}$. Deduce:*

$$T_{B/A}(\alpha) = a_1 \text{ and } N_{B/A}(\alpha) = a_0^2 + a_0 a_1 + c a_1^2.$$

b) *Show: the Gram matrix of the trace form on B/A with respect to the basis $1, t$ is $\begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix}$ and thus the discriminant of B/A is $1 \pmod{A^{\times 2}}$.*

c) *Deduce: the trace form on a separable quadratic field extension in characteristic 2 is nondegenerate.*

EXERCISE 5.18. *Let A be a ring. We consider the A-algebra A^n, which is certainly free and finitely generated as an A-module.*

a) *We work with the standard basis $e = (e_1, \ldots, e_n)$ of A^n. Show: the matrix of multiplication by $x \coloneqq (x_1, \ldots, x_n)$ on A^n is the diagonal matrix $\operatorname{diag}(x_1, \ldots, x_n)$. Deduce:*

$$T_{A^n/A}(x) = x_1 + \ldots + x_n \text{ and } N_{A^n/A}(x) = x_1 \cdots x_n.$$

b) *Show: the Gram matrix G_e for the trace form on A^n/A with respect to the basis e is the identity matrix I_n. In other words, the trace form $\langle \cdot, \cdot \rangle$ on A^n/A is the standard dot product.*

EXERCISE 5.19. *Let $A_{/\mathbb{R}}$ be an étale algebra, so $A \cong \mathbb{R}^r \times \mathbb{C}^s$ for some $r, s \geq 0$.*

a) *Show: there is an $\mathbb{R}$-basis for A with respect to which the Gram matrix for the trace form is is diagonal, with $r + s$ diagonal entries $+1$ and s diagonal entries -1.*

b) *Deduce: $\delta_{A/\mathbb{R}} = (-1)^s \in \mathbb{R}^\times / \mathbb{R}^{\times 2}$.*

EXERCISE 5.20. *Let R be a ring, let $B, C \in R$, and let*

$$A \coloneqq R[t]/(t^3 + Bt + C).$$

Notice that A is free of rank 3 as an R-module, with basis given by the classes of $1, t, t^2$ in A.

a) *Show: the Gram matrix for the trace form on A with respect to the above basis is*
$$\begin{bmatrix} 3 & 0 & -2B \\ 0 & -2B & -3C \\ -2B & -3C & 2B^2 \end{bmatrix}.$$
b) *Deduce: $\delta_{A/R} = -4B^3 - 27C^2 \pmod{R^{\times 2}}$.*
c) *Suppose $R = \mathbb{R}$. Show: $\delta_{A/R}$ is positive, zero, or negative acording to whether the cubic $t^3 + Bt + C$ has three, two or one real roots.*

Having computed discriminants of all étale $\mathbb{R}$-algebras, the next simplest case is probably that of a finite field $\mathbb{F}_q$. If q is even, then every étale $\mathbb{F}_q$-algebra has square discriminant because every element of $\mathbb{F}_q^\times$ is a square. So the interesting case is when q is odd, in which case $[\mathbb{F}_q^\times : \mathbb{F}_q^{\times 2}] = 2$ and we just need to determine whether the discriminant is a square or not, and we immediately reduce to the question: for $d \in \mathbb{Z}^+$, when is $\delta_{\mathbb{F}_{q^d}/\mathbb{F}_q}$ a square? The answer is triially yes when $d = 1$ and is no when $d = 2$ by Exercise 5.16. Unfortunately Exercise **??** is less immediately helpful, as we first need to choose B and C so that $t^3 + Bt + C$ is irreducible and then we need to determine whether $-4B^3 - 27C^2$ is a square in $\mathbb{F}_q^\times$, but compuations will suggest that the discriminant is always a square in this case. We will take up this question again later in this section.

3.2. The Trace Form of a Field Extension.

THEOREM 5.14. *(Dedekind's Lemma on Linear Independence of Characters) Let M be a monoid and L a field. The set $X(M, L)$ of all monoid homomorphisms $M \to L^\times$ is linearly independent as a subset of the L-vector space L^M of all functions from M to L.*

PROOF. By definition, a subset of a vector space is linearly independent iff every nonempty finite subset is linearly independent. So it's enough to show that for all $N \in \mathbb{Z}^+$, every N-element subset of $X(M, L)$ is linearly independent in L^M. We show this by induction on N. The base case, $N = 1$, is immediate: the only one element linearly dependent subset of L^M is the zero function, and elements of $X(M, L)$ are nonzero at all values of M. So suppose $N \geq 2$, that every $N - 1$ element subset of $X(M, L)$ is linearly independent, and let $\chi_1, \ldots, \chi_N$ be distinct elements of $X(M, L)$. Let $\alpha_1, \ldots, \alpha_N \in L$ be such that for all $x \in M$, we have

$$\alpha_1\chi_1(x) + \ldots + \alpha_N\chi_N(x) = 0. \tag{8}$$

Our goal is to show that $\alpha_1 = \ldots = \alpha_N = 0$. Since $\chi_1 \neq \chi_N$, there is $m \in M$ such that $\chi_1(m) \neq \chi_N(m)$. Substituting mx for x in (8), we get that for all $x \in M$,

$$\alpha_1\chi_1(m)\chi_1(x) + \alpha_2\chi_2(m)\chi_2(x) + \ldots + \alpha_N\chi_N(m)\chi_N(x) = 0. \tag{9}$$

Multiplying (9) by $\chi_1(m)^{-1}$ and subtracting this from (8), we get

$$\forall x \in M,\ \alpha_2\left(\frac{\chi_2(m)}{\chi_1(m)} - 1\right)\chi_2(x) + \ldots + \alpha_N\left(\frac{\chi_N(m)}{\chi_1(m)} - 1\right)\chi_N(x) = 0. \tag{10}$$

By induction, $\chi_2, \ldots, \chi_N$ are linearly independent, so $\alpha_N\left(\frac{\chi_N(m)}{\chi_1(m)} - 1\right) = 0$ and thus $\alpha_N = 0$. Thus (8) gives a linear dependence relation among the $N - 1$ characters $\chi_1, \ldots, \chi_{N-1}$, so by induction $\alpha_1 = \cdots = \alpha_{N-1} = 0$. □

COROLLARY 5.15. *Let K/F and L/F be field extensions. Let $\sigma_1, \ldots, \sigma_n : K \to L$ be distinct F-algebra emdeddings. Then in the L vector space L^K of all maps from K to L, the maps $\sigma_1, \ldots, \sigma_n$ are linearly independent.*

PROOF. We apply Theorem 5.14 with $M := K^\times$ and get that the restrictions of $\sigma_1, \ldots, \sigma_n$ to $K^\times$ are linearly independent as maps from $K^\times$ to L, which immediately implies that they are linearly independent as maps from K to L. □

THEOREM 5.16. *Let K/F be a field extension of finite degree n. The following are equivalent:*

(i) *The trace form $T : K \times K \to F$ is nondegenerate.*
(ii) *There exists some $x \in K$ such that $\mathrm{Tr}(x) \neq 0$.*
(iii) *The trace function $\mathrm{Tr} : K \to F$ is surjective.*
(iv) *The extension K/F is separable.*

PROOF. (i) $\implies$ (ii): This is immediate.
(ii) $\implies$ (iii): Since $\mathrm{Tr} : K \to F$ is F-linear and nonzero, it must be surjective.
(iii) $\implies$ (iv): It follows from (7) that $\mathrm{Tr}_{K/F} \equiv 0$ when K/F is not separable.
(iv) $\implies$ (i): Let $\mathbf{x} = (x_1, \ldots, x_n) \in K^n$ be any basis for K/F. We must show that $\Delta(\mathbf{x}) = \det T(x_i x_j) \neq 0$. Seeking a contradiction we suppose $\Delta(\mathbf{x}) = 0$; then by (11), we have $\det(\sigma_i(x_j)) = 0$, and this means that there are $\alpha_1, \ldots, \alpha_n \in \overline{F}$, not all 0, such that

$$\sum_{i=1}^{n} \alpha_i \sigma_i(x_j) = 0 \ \forall j.$$

Since this holds for all elements of a basis of K/F, we deduce

$$\forall x \in K, \ \sum_{i=1}^{n} \alpha_i \sigma_i(x) = 0,$$

contradicting Dedekind's Lemma (Theorem 5.14). □

EXERCISE 5.21. *Give a different proof of (iv) $\implies$ (i) in Theorem 5.16 using the Primitive Element Corollary and the Vandermonde determinant.*

EXERCISE 5.22. *Let K/F be a degree n field extension, and let $\mathbf{x} = (x_1, \ldots, x_n) \in K^n$ be linearly* dependent *over F. Show that $\Delta(\mathbf{x}) = \det \mathrm{Tr}_{K/F}(x_i x_j) = 0$.*

3.3. The Trace Form on an Étale K-Algebra.

THEOREM 5.17. *Let A be a finite dimensional commutative K-algebra. The following are equivalent:*

(i) *A is an étale K-algebra.*
(ii) *The trace form $\langle \cdot, \cdot \rangle : A \times A \to K$ is nondegenerate.*
(iii) *$\delta_{A/K} \neq (0)$.*

PROOF. A bilinear space over a field is nondegenerate if and only if its discriminant is nonzero, so (ii) $\iff$ (iii).
Step 1: Suppose $A \cong \prod_{i=1}^{r} l_i$ is a finite product of finite degree field extensions l_i/k. By Exercise 5.14 we have

$$\delta_{A/k} = \prod_{i=1}^{r} \delta_{l_i/k},$$

and by Theorem 5.16 for each $1 \leq i \leq r$ we have $\delta_{l_i/k} \neq (0)$ if and only if l_i/k is separable. Thus in this case we have that $\delta_{A/k} \neq 0$ if and only if each l_i/k is separable. This shows that (i) $\implies$ (iii).
Step 2: Suppose A is *not* an étale k-algebra. Then either A is isomorphic to a finite product of finite degree field extensions at least one of which is inseparable – in which case Step 1 shows that $\delta_{A/k} = (0)$ – or A is not reduced: there is $x \in A^\bullet$ and $n \in \mathbb{Z}^+$ such that $x^n = 0$. Then for all $y \in A$ we have $(xy)^n = x^n y^n = 0$.[2] After choosing a k-basis for A, this means that xy is represented by a nilpotent matrix, so all its eigenvalues are 0, so its trace is 0. Thus $\langle x, y \rangle = 0$ for all $y \in A$ and the trace form on A is degenerate. □

Now let A/K be an étale K-algebra, and let L/K be a splitting field for K: e.g. we may take $L = \overline{K}$ to be an algebraic closure of K. Let $n = \dim_K A$, and let $\sigma_1, \ldots, \sigma_n : A \to L$ be the K-algebra maps from A to L. By Propoposition 5.7, the map $A \to L^n$ by $x \mapsto (\sigma_1(x), \ldots, \sigma_n(x))$ extends uniquely to an L-algebra isomorphism $A_L \to L^n$. For all $x \in A$, we have

$$T_{A/K}(x) = T_{A_L/L}(x \otimes 1) = T_{L^n/L}(\sigma(x \otimes 1)) = \sum_{i=1}^n \sigma_i(x).$$

Now let $\mathbf{x} = (x_1, \ldots, x_n) \in A^n$, and let $S(\mathbf{x}) \in M_n(L)$ be the matrix with

$$S(\mathbf{x})_{ij} = \sigma_i(x_j).$$

Then

$$(S(\mathbf{x})^T S(\mathbf{x}))_{ij} = \sum_{k=1}^n \sigma_k(x_i)\sigma_k(x_j) = \sum_{k=1}^n \sigma_k(x_i x_j) = \mathrm{Tr}_{A/K}(x_i x_j).$$

In particular, if $\mathbf{x}$ is a K-basis for A and $G_{\mathbf{x}}$ is the Gram matrix for the trace form on A/K with respect to $\mathbf{x}$, then we have

$$G_{\mathbf{x}} = S(\mathbf{x})^T S(\mathbf{x}),$$

so if we set

$$\delta(\mathbf{x}) \coloneqq \det G_{\mathbf{x}},$$

then we have

$$\delta(\mathbf{x}) = (\det S(\mathbf{x}))^2. \tag{11}$$

Exercise 5.23. *Let A be a Dedekind domain with fraction field K, let L/K be a finite degree separable extension, and let B be the integral closure of A in L. Let M/K be the Galois closure of L/K.*

a) *Show: M contains $K(\sqrt{\delta_{L/K}})$. Deduce: if $[L : K]$ is odd, then $\delta_{L/K} \in K^{\times 2}$ if and only if L/K is Galois.*
b) *Let Λ be any A-lattice in L. Show: M contains $K(\sqrt{\delta_\Lambda})$.*

Let $R \coloneqq \mathbb{Z}[a_0, \ldots, a_{n-1}]$; here $a_0, \ldots, a_{n-1}$ are independent indeterminates, so A is a UFD (CITE). Consider the polynomial

$$f \coloneqq t^n + a_{n-1}t^{n-1} + \ldots + a_1 t + a_0 \in R[t].$$

[2]Note that we are using the commutativity of A here: for matrices $m_1, m_2 \in M_n(k)$, if m_1 and m_2 are both nilpotent, then $m_1 m_2$ need not be...unless m_1 and m_2 commute, in which case the above one line computation shows that $m_1 m_2$ is nilpotent.

Then f is irreducible (in both $R[t]$ and $K[t]$): indeed, it is a primitive polynomial over a UFD, so reducibility would imply that it is a product of two polynomials of degree smaller than n, but such a factorization would imply a similar factorization for every monic degree n polynomial $g \in \mathbb{Z}[t]$, which is clearly impossible. Put

$$A_f := R[t]/(f),$$

which is free of rank n as an R-algebra. Since $R^\times = \mathbb{Z}^\times = \{\pm 1\}$, we have $R^{\times 2} = \{1\}$, so the discriminant

$$\delta(f) := \delta_{A_f/R}$$

is a well-defined element of R. We will obtain a useful formula for $\delta(f)$. Over an algebraic closure $\overline{K}$ of the fraction field K of R, we may factor

$$f(t) = \prod_{i=1}^n (t - \alpha_i).$$

Put $\alpha := \alpha_1$, $L := K(\alpha)$ and $M := K(\alpha_1, \ldots, \alpha_n)$, so M is the splitting field of $f \in K[t]$. Under the isomorphism $A_f \to R[\alpha]$ obtained by mapping t to α, the R-basis $1, t, \ldots, t^{n-1}$ maps to the power basis $\mathbf{x} = (1, \alpha, \ldots, \alpha^{n-1})$ of $R[\alpha]$. We may choose the K-algebra embeddings $\{\sigma_i : L \hookrightarrow M\}_{i=1}^n$ such that $\alpha_i = \sigma_i(\alpha)$ for all $1 \leq i \leq n$. Then as above, if we put $S(\mathbf{x})_{ij} = \sigma_i(\alpha^j) = \alpha_i^j$, then

$$\delta(f) = \delta(\mathbf{x}) = (\det S(\mathbf{x}))^2.$$

The matrix $S(\mathbf{x})$ is Vandermonde, so its determinant is

$$\mathfrak{s} = \mathfrak{s}(\alpha_1, \ldots, \alpha_n) := \prod_{1 \leq i < j \leq n} (\alpha_j - \alpha_i), \tag{12}$$

so altogether we find:

$$\delta(f) = \prod_{1 \leq i \neq j \leq n} (\alpha_i - \alpha_j).$$

This means that $\prod_{1 \leq i \neq j \leq n} (\alpha_i - \alpha_j)$ is of the form $P_n(a_0, \ldots, a_{n-1}) \in \mathbb{Z}[a_0, \ldots, a_{n-1}]$. For instance, we have

$$P_1(a_0) = 1,\ P_2(a_0, a_1) = a_1^2 - 4a_0,\ P_3(a_0, a_1, a_2) = a_2^2 a_1^2 - 4a_1^3 - 4a_2^3 a_0 - 27a_0^2 + 18 a_0 a_1 a_2.$$

Now for any ring R and any monic

$$f := t^n + a_{n-1} t^{n-1} + \ldots + a_1 t + a_0 \in R[t],$$

we may define

$$\delta(f) := P_n(a_1, \ldots, a_{n-1}) \in R.$$

For elements $\alpha_1, \ldots, \alpha_n$ of a domain R, we define the **semidiscriminant** $\mathfrak{s}(\alpha_1, \ldots, \alpha_n)$ using (12), so $\delta(f) = \mathfrak{s}^2$. If we start with a monic degree n polynomial over a domain R, the semi-discriminant is defined using an ordering of the roots $\alpha_1, \ldots, \alpha_n$ (which we view as lying in the splitting field M of f) so it is natural to ask whether the semidiscriminant is an invariant of f itself. The symmetric group S_n acts on M^n by permutation of coordinates, and for $\alpha = (\alpha_1, \ldots, \alpha_n) \in M^n$, we have

$$\mathfrak{s}(\sigma(\alpha)) = \operatorname{sgn}(\sigma) \mathfrak{s}(\alpha),$$

where $\operatorname{sgn}(\sigma) \in \{\pm 1\}$ is the sign of the permutation σ. If we assume that f is separable – that is, $\alpha_1, \ldots, \alpha_n$ are distinct; otherwise $\delta(f) = \mathfrak{s}(\alpha) = 0$ – then we have $\mathfrak{s}(\sigma(\alpha)) = \mathfrak{s}(\alpha)$ if and only if σ lies in the alternating group A_n, so if $n \geq 2$ the answer is that $\pm \mathfrak{s}(\alpha)$ depends only on f.

PROPOSITION 5.18. *Let K be a field of characteristic different from 2, let $f \in K[t]$ be a monic separable degree n polynomial with irreducible factorization $p_1 \cdots p_r$ and roots $\alpha_1, \ldots, \alpha_n$ in its splitting field M. Suppose that $G := \mathrm{Aut}(M/K)$ is cyclic. Then $\delta(f) \in K^{\times 2}$ if and only if $n + r$ is even.*

PROOF. Let σ be a generator of the finite cyclic group G. We may view G as acting faithfully on $\{\alpha_1, \ldots, \alpha_n\}$, and its orbits are in bijection with the irreducible factors $p_1, \ldots, p_r$. Then σ must cyclically permute the roots of each p_i, so it has cyclic type $(\deg p_1, \ldots, \deg p_r)$ and thus sign $(-1)^{\sum_{i=1}^r (\deg p_i)-1} = (-1)^{n+r}$. □

EXERCISE 5.24. *Use Proposition 5.18 to give another proof of Exercise 5.19b).*

EXERCISE 5.25. *Let q be an odd prime power and let $n \in \mathbb{Z}^+$. Use Proposition 5.18 to show that $\delta_{\mathbb{F}_q^n/\mathbb{F}_q} \in \mathbb{F}_q^{\times 2}$ if and only if n is odd.*

3.4. The Trace Form on an Artinian Principal K-Algebra.

EXERCISE 5.26. *Let k be a field, and let A be a finite dimensional commutative k-algebra. In this exercise we will determine when the trace map $T : A \to k$ is identically 0 in the case when A is a **principal ideal ring**.*

a) *Show: we can write $A = \prod_{i=1}^r A_i$ with each A_i a local, Artinian principal ring: there is a principal maximal ideal $\mathfrak{p} = (\pi)$; if e is the least positive integer such that $\pi^e = 0$ then all the ideals of A are*

$$A \supsetneq \mathfrak{p} \supsetneq \mathfrak{p}^2 \supsetneq \ldots \supsetneq \mathfrak{p}^{e-1} \supsetneq \mathfrak{p}^e = (0). \tag{13}$$

b) *For $x \in A = \prod_{i=1}^r A_i$, write $x = (x_1, \ldots, x_r)$. Show: $T(x) = \sum_{i=1}^r T_{A_i/k}(x_i)$. Thus $T : A \to k$ is the zero map if and only if each $T_i = T_{A_i/k}$ is the zero map, so we may assume that A is local.*

c) *Let $x \in A$. Since each $\mathfrak{p}^e$ is an A-submodule, it is in particular a k-subspace of A, so (13) gives a filtration of the finite-dimensional k-vector space A by subspaces invariant under the k-linear map $x\bullet$. If $W' \subseteq W \subseteq A$ are subspaces such that $x(W') \subseteq W'$ and $x(W) \subseteq W$, then $x\bullet$ gives a well-defined k-linear map on the quotient W/W'; we denote its trace by $T(x|W/W')$. Show:*

$$T(x) = \sum_{i=0}^{e-1} T(x|\mathfrak{p}_i/\mathfrak{p}_{i+1}).$$

d) *Let $0 \leq i \leq e-1$. Show: multiplication by π^e induces an A-module isomorphism $A/\mathfrak{p} \to \mathfrak{p}^i/\mathfrak{p}^{i+1}$ that commutes with multiplication by x. Deduce: for all $0 \leq i \leq e-1$ we have $T(x|\mathfrak{p}_i/\mathfrak{p}_{i+1}) = T(x|A/\mathfrak{p})$ and thus*

$$T(x) = eT(x|A/\mathfrak{p}).$$

e) *Conclude that the trace form on a local principal Artinian k-algebra $(A, \mathfrak{p})$ is identically 0 if and only if $A/\mathfrak{p}$ is an inseparable field extension of k or e is divisible by the characteristic of k.*

3.5. AKLB Applications.

PROPOSITION 5.19. *Let A be a domain with fraction field K, let L/K be a finite degree field extension, and let B be the integral closure of A in L. Then:*

a) *Every element of L may be written as $\frac{b}{a}$ with $b \in B$ and $a \in A^\bullet$.*

b) *Thus $\langle B \rangle_K = L$ and L is the fraction field of B.*

PROOF. Let $\alpha \in L$. By scaling the minimal polynomial of α by an element of $A^\bullet$ we get a polynomial

$$f(t) = a_n t^n + \ldots + a_1 t + a_0 \in A[t]$$

such that $a_n \neq 0$ and $f(\alpha) = 0$. Thus

$$a_n^{n-1} f(\frac{\alpha}{a_n}) = t^n + a_{n-1}t^{n-1} + a_n a_{n-2} t^{n-2} + \ldots + a_n^{n-2} a_1 t + a_n^{n-1} a_0 \in A[t]$$

is monic and has $a_n\alpha$ as a root. So $a_n\alpha$ is integral over A, and thus $s \coloneqq a_n\alpha$ lies in B, the integral closure of A in L and $\alpha = \frac{s}{a_n}$, establishing part a). It follows immediately that $\langle B \rangle_K = L$, and then the fraction field of B contains A hence also contains its fraction field K. So the fraction field of B is L. □

THEOREM 5.20 (Normalization Theorem). *Let A be an integrally closed Noetherian domain with fraction field K, let L/K be a finite degree **separable** field extension, and let B be the integral closure of A in L. Then:*

a) *B is an A-lattice in L. In particular, B is finitely generated as an A-module.*
b) *We have that A is a Dedekind domain if and only if B is a Dedekind domain.*

PROOF. Step 1: We write $\langle \cdot, \cdot \rangle$ for the trace pairing on B: $\langle x, y \rangle \coloneqq T_{B/A}(xy)$. Let $x \in S$. By Corollary 5.12, for all $y \in B$ we have $\langle x, y \rangle = T_{B/A}(xy) \in A$, which shows that

$$B \subseteq B^*.$$

Step 2: By Proposition 5.19 we know that B spans L as a K-vector space, so B contains a K-basis $(e_1, \ldots, d_n)$ of L. So

$$\Lambda \coloneqq \langle e_1, \ldots, e_n \rangle_A$$

is an A-lattice in L and $\Lambda \subseteq B$. It follows that

$$B \subseteq B^* \subseteq \Lambda^*.$$

Since Λ^* is a (free) R-lattice in L, it is finitely generated as an A-module. Since A is Noetherian, the submodule B is also finitely generated. Thus B is an A-lattice in L. This completes the proof of part a).
Step 3: Since B is a finitely generated module over the Noetherian ring A, the A-module B is Noetherian: every submodule is finitely generated. Let I be an ideal of B. Then I is an B-submodule of B, hence also an A-submodule of B, so I is finitely generated as an A-module, hence also finitely generated as an B-module, i.e., finitely generated as an ideal. Thus B is Noetherian. It is integrally closed by [**CA**, Cor. 14.11] (which states that the integral closure of a domain in any field extension is integrally closed.) Since B/A is an integral extension, we have $\dim A = \dim B$ [**CA**, Cor. 14.17]. Thus B is a Dedekind domain if and only if $\dim B = 1$ if and only if $\dim A = 1$ if and only if A is a Dedekind domain. □

Splitting of primes: suppose that A is a Dedekind domain with fraction field K, L/K is a finite degree field extension, and B is the integral closure of A in L. We **assume** that B is finitely generated as an A-module, which we just saw happens when L/K is separable. Let $\iota : A \hookrightarrow B$ denote the inclusion map.

THEOREM 5.21. *Let R be a Dedekind domain with fraction field K, let L/K be a separable field extension, and let $\alpha \in L$ be such that $[L : K(\alpha)]$ is* not *divisible by the characteristic of K.*[3] *The following are equivalent:*

(i) *The element α is integral over R.*
(ii) *For all $i \in \mathbb{Z}^+$ we have $\mathrm{Tr}_{L/K}(\alpha^i) \in R$.*

PROOF. If α is integral over R then so is α^i for all $i \in \mathbb{Z}^+$. So (i) $\implies$ (ii) is a special case of Corollary 5.12.
(ii) $\implies$ (i): Suppose that we have $\mathrm{Tr}_{L/K}(\alpha^i) \in R$ for all $i \in \mathbb{Z}^+$. Put

$$d := [L : K(\alpha)].$$

By hypothesis, $d \in R^\bullet$. By Theorem 5.13 we have

$$\mathrm{Tr}_{L/K}(\alpha^i) = \mathrm{Tr}_{K(\alpha)/K}(\mathrm{Tr}_{L/K(\alpha)}(\alpha^i i)) = d\,\mathrm{Tr}_{K(\alpha)/K}(\alpha^i). \tag{14}$$

Put $n := [K(\alpha) : K]$, so $d, d\alpha, \ldots, d\alpha^{n-1}$ is a K-basis for $K(\alpha)$. Thus

$$\Lambda := \langle d, d\alpha, \ldots, d\alpha^{n-1} \rangle$$

is a (free) R-lattice in $K(\alpha)$, which we view as a quadratic K-space under the trace form. Using (14) we get

$$R[\alpha] \subseteq \Lambda^*.$$

Since Λ^* is an R-lattice in $K(\alpha)$, hence a finitely generated R-module, and R is Noetherian, it follows that $R[\alpha]$ is a finitely generated R-module, which by Theorem 2.21 means α is integral over R. □

REMARK 5.22. *In Theorem 5.21, the hypothesis that the characteristic of K does not divide $[L : K(\alpha)]$ may look like an artifact of the proof. On the contrary, it is actually necessary for the result to hold. Indeed, suppose that K has characteristic $p > 0$, and let L/K be a separable extension of degree divisible by p, and take $\alpha \in K \setminus R$, so $p \mid [L : K] = [L : K(\alpha)]$. For all $i \in \mathbb{Z}^+$ we have*

$$\mathrm{Tr}_{L/K}(\alpha^i) = [L : K]\alpha^i = 0.$$

COROLLARY 5.23. *Let R be a Dedekind domain with fraction field K, let L/K be a finite degree separable field extension, and use the trace form on L/K to view L as a quadratic K-space. Suppose:*

$$\mathrm{char}(K) \nmid [L : K].$$

Then the integral closure S of R in L is the unique maximal R-lattice in L.

If I is a nonzero ideal of A, consider the **pushforward**

$$\iota_*(I) := IB.$$

We claim that just because ι is an integral ring extension, if I is a proper ideal of A then $\iota_*(I)$ is a proper ideal of B. Indeed, since I is proper there is a maximal ideal $\mathfrak{p}$ of A containing I, and $\iota_*(I) \subseteq \iota_*(\mathfrak{p})$, so it suffices to show that $\iota_*(\mathfrak{p})$ is proper. By Theorem 2.29d), there is a maximal ideal $\mathcal{P}$ of B such that $\iota^*(\mathcal{P}) = \mathfrak{p}$. Then $\iota_*\mathfrak{p} = \langle \mathfrak{p} \rangle_B \subseteq \langle \mathcal{P} \rangle_B = \mathcal{P}$, so is proper.

EXERCISE 5.27. *Let $\iota : A \hookrightarrow B$ be an integral extension of domains, and let $\mathfrak{p}$ be a maximal ideal of A. Show:*

$$\iota^*\iota_*\mathfrak{p} = \mathfrak{p}.$$

[3]Notice that this indivisbility hypothesis is vacuous in characteristic 0.

Now suppose that A is a Dedekind domain, hence so is B. Because the pushforward is multiplicative, we may focus on the case of pushing forward a prime ideal. For $\mathfrak{p} \in \operatorname{MaxSpec} A$, write

$$\mathfrak{p}S = \mathcal{P}_1^{e_1} \cdots \mathcal{P}_r^{e_r}.$$

The exponent e_i is called the **ramification index** of $\mathcal{P}_i$ over $\mathfrak{p}$; we denote it by $e(\mathcal{P}_i|\mathfrak{p})$. When the "downstairs prime" $\mathfrak{p}$ is undertood, we may also write $e_{\mathcal{P}_i}$.

The ideals $\mathcal{P}_1, \ldots, \mathcal{P}_r$ are precisely the prime ideals of B that contain $\mathfrak{p}$. We claim:

$$(\iota^*)^{-1}\{\mathfrak{p}\} = \{\mathcal{P}_1, \ldots, \mathcal{P}_r\}.$$

First, if $\mathcal{P} \in \operatorname{MaxSpec} B$ is such that $\mathcal{P} \cap A = \mathfrak{p}$, then $\mathcal{P}$ contains $\mathfrak{p}$, so $\mathcal{P} = \mathcal{P}_i$ for some i. Conversely, for $1 \leq i \leq r$ we have that $\mathcal{P}_i \cap A$ is a maximal ideal of A that contains $\mathfrak{p}$, so $\mathcal{P}_i \cap A = \mathfrak{p}$.

If $\mathcal{P}$ lies over $\mathfrak{p}$ then the kernel of the composite map $A \hookrightarrow B \to B/\mathcal{P}$ is $\mathcal{P} \cap A = \mathfrak{p}$, so we get an induced injection

$$A/\mathfrak{p} \hookrightarrow B/\mathcal{P}.$$

Since $\mathfrak{p}$ and $\mathcal{P}$ are both maximal ideals, this is a field homomorphism. Since B is finitely generated as an A-module, certainly $B/\mathcal{P}$ is finitely generated as an $A/\mathfrak{p}$ vector space (the images of any set of generators will still generate). We define the **residual degree**

$$f_{\mathcal{P}} = f(\mathcal{P}|\mathfrak{p}) \coloneqq [B/\mathcal{P} : A/\mathfrak{p}].$$

LEMMA 5.24. *Let A be a Dedekind domain with fraction field K, let $K \subseteq L \subseteq M$ be a tower of finite degree field extensions, let B be the integral closure of A in L and let C be the integral closure of A in M. We **suppose** that B is finitely generated as an A-module and C is finitely generated as a B-module.*[4] *Let $\mathfrak{r} \in \operatorname{MaxSpec} C$, let $\mathfrak{q} \coloneqq \mathfrak{r} \cap B$ and let $\mathfrak{p} \coloneqq \mathfrak{q} \cap A$. Then:*

$$e(\mathfrak{r}|\mathfrak{p}) = e(\mathfrak{r}|\mathfrak{q})e(\mathfrak{q}|\mathfrak{p}) \text{ and } f(\mathfrak{r}|\mathfrak{p}) = f(\mathfrak{r}|\mathfrak{q})f(\mathfrak{q}|\mathfrak{p}).$$

EXERCISE 5.28. *Prove Lemma 5.24.*

LEMMA 5.25. *Let R be a Dedekind domain, $\mathfrak{p} \in \operatorname{MaxSpec} R$ and $e \in \mathbb{Z}^+$. Then*

$$\dim_{R/\mathfrak{p}} \mathfrak{p}^e/\mathfrak{p}^{e+1} = 1.$$

PROOF. Let $S \coloneqq R \setminus \mathfrak{p}$ and $R_{\mathfrak{p}} \coloneqq S^{-1}R$. Then $R/\mathfrak{p} = R_{\mathfrak{p}}/\mathfrak{p}R_{\mathfrak{p}}$ and $\mathfrak{p}^e/\mathfrak{p}^{e+1} = (\mathfrak{p}R_{\mathfrak{p}})^e/(\mathfrak{p}R_{\mathfrak{p}})^{e+1}$. So we may replace R with $R_{\mathfrak{p}}$ and thereby assume that R is a DVR, hence a PID. If $\mathfrak{p} = (\pi)$, then multiplication by π^e gives an R-module isomorphism from $R/\mathfrak{p}$ to $\mathfrak{p}^e/\mathfrak{p}^{e+1}$. □

THEOREM 5.26. *Let A be a Dedekind domain with fraction field K, let L/K be a finite degree field extension, let B be the integral closure of A in L, and **assume** that B is finitely generated as an R-module. Let $\mathfrak{p} \in \operatorname{MaxSpec} R$.*

a) *We have $\dim_{R/\mathfrak{p}} B/\mathfrak{p}B = [L : K]$.*
b) *We have $\sum_{\mathcal{P}|\mathfrak{p}} e_{\mathcal{P}} f_{\mathcal{P}} = [L : K]$.*

[4]It follows that C is finitely generated as an A-module.

PROOF. Put $n := [L : K]$.
a) Let $S := A \setminus \mathfrak{p}$, and let $A_{\mathfrak{p}} := S^{-1}A$, $B_{\mathfrak{p}} := S^{-1}B$. By Lemma 2.12 we get canonical isomorphisms

$$A_{\mathfrak{p}}/\mathfrak{p}A_{\mathfrak{p}} \xrightarrow{\sim} A/\mathfrak{p} \text{ and } B_{\mathfrak{p}}/\mathfrak{p}B_{\mathfrak{p}} \xrightarrow{\sim} B/\mathfrak{p}B$$

which we will regard as equalities. Thus if the result holds for $A_{\mathfrak{p}}$ and $B_{\mathfrak{p}}$ then it holds for A and B, so we may assume that A is a PID and B is a free A-module of rank n. Then as A-modules we have

$$\mathfrak{p}B \cong \mathfrak{p}A^n = (\mathfrak{p}A)^n,$$

so

$$B/\mathfrak{p}B \cong (A/\mathfrak{p}A)^n,$$

giving the result.
b) As in part a), we may assume that A is a DVR and thus B is a semilocal Dedekind domain, hence a PID. Write

$$\mathfrak{p}B = \mathcal{P}_1^{e_1} \cdots \mathcal{P}_g^{e_g}.$$

By the Chinese Remainder Theorem we have

$$B/\mathfrak{p}B = B/\prod_{i=1}^{g} \mathcal{P}_i^{e_i} \cong \prod_{i=1}^{g} B/\mathcal{P}_i^{e_i}.$$

By part a) we have

$$n = [L : K] = \dim_{A/\mathfrak{p}} B/\mathfrak{p}B = \sum_{i=1}^{g} \dim_{A/\mathfrak{p}} B/\mathcal{P}_i^{e_i}.$$

Now consider

$$B \supseteq \mathcal{P}_i \supseteq \mathcal{P}_i^2 \supseteq \ldots \supseteq \mathcal{P}_i^{e_i}.$$

By Lemma 5.25, each successive quotient $\mathcal{P}_i^a/\mathcal{P}_i^{a+1}$ is a one-dimensional $B/\mathcal{P}_i$-vector space, hence an $f_{\mathcal{P}_i}$-dimensional $A/\mathfrak{p}$-vector space. It follows that

$$\dim_{A/\mathfrak{p}} B/\mathcal{P}_i^{e_i} = e_i f_{\mathcal{P}_i}$$

so

$$n = \sum_{i=1}^{g} e_i f_{\mathcal{P}_i}. \qquad \square$$

Under the hypotheses of Theorem 5.26 let us introduce some further terminology:

- We say L/K is **totally ramified** at $\mathcal{P}$ if $e_{\mathcal{P}} = [L : K]$.
- We say L/K is **unramified** at $\mathcal{P}$ if $e_{\mathcal{P}} = 1$ and $(B/\mathcal{P})/(A/\mathfrak{p})$ is separable; otherwise we say that L/K is **ramified** at $\mathcal{P}$.
- We say L/K is **unramified over** $\mathfrak{p}$ if every $\mathcal{P}$ lying over $\mathfrak{p}$ is unramified. This holds if and only if $B/\mathfrak{p}B$ is an étale $A/\mathfrak{p}$-algebra.
- We say $\mathfrak{p}$ is **inert** in L if L/K is unramified over $\mathfrak{p}$ and $\mathfrak{p}B$ is a prime ideal.
- We say $\mathfrak{p}$ **splits completely** in L if there are $[L : K]$ primes of B lying over $\mathfrak{p}$.

Notice that L/K is both unramified at $\mathcal{P}$ and totally ramified at $\mathcal{P}$ if and only if $L = K$ (a trivial case).

EXERCISE 5.29. *Show: if $\mathfrak{p}$ in A splits completely in B, then L/K is unramified over $\mathfrak{p}$.*

EXAMPLE 5.27. *Let A be a domain with fraction field K, let L/K be a purely inseparable algebraic extension (possibly of infinite degree), and let B be the integral closure of A in L. For $\mathfrak{p} \in \operatorname{Spec} R$, there is a unique prime of S lying over $\mathfrak{p}$, namely*

$$\operatorname{rad}(\mathfrak{p}B) := \{x \in B \mid x^n \in \mathfrak{p}B \text{ for some } n \in \mathbb{Z}^+\}.$$

This is [**CA**, Lemma 14.20].

4. The Discriminant

Let A be a Dedekind domain with fraction field K, let L/K be a finite degree separable field extension, and let B be the integral closure of A in L. Let $\langle \cdot, \cdot \rangle$ be the trace form for L/K: that is, for $x, y \in L$, we put

$$\langle x, y \rangle := T(xy) \in K.$$

For $x_1, \ldots, x_n \in L$, we put

$$\delta(x_1, \ldots, x_n) := \det \langle x_i, x_j \rangle.$$

EXERCISE 5.30. *Show: for $x_1, \ldots, x_n \in L$ we have $\delta(x_1, \ldots, x_n) \neq 0$ if and only if $x_1 \ldots, x_n$ are linearly independent over K.*

Since A is integrally closed, the quadratic lattice B is *integral*: $\langle B, B \rangle \subseteq A$. Thus for any integral A-lattice Λ in B, for the discriminant δ_Λ of Λ (cf. §4.5) we have

$$\delta_\Lambda \in \operatorname{Int} A.$$

Especially, we define the **discriminant ideal** $\delta_{B/A}$ to be δ_B.

PROPOSITION 5.28. *Let L/K be a separable field extension of degree n, and let $\mathcal{K}/K$ be a field extension containing a Galois closure of L: equivalently, for which there are distinct elements $\sigma_1, \ldots, \sigma_n \in \operatorname{Hom}_K(L, \mathcal{K})$.*

a) *For $a_1, \ldots, a_n \in L$ we have*

$$\delta(a_1, \ldots, a_n) = \left(\det \sigma_i(a_j)\right)^2.$$

b) *For $x \in L$ we have*

$$\delta(1, x, x^2, \ldots, x^{n-1}) = \prod_{1 \leq i < j \leq n} \left(\sigma_i(x) - \sigma_j(x)\right)^2.$$

PROOF. Part a) essentially repeats (11). Part b) follows from part a) using the Vandermonde determinant. □

PROPOSITION 5.29. *Let $S \subseteq A$ be a multiplicative subset. Then*

$$S^{-1}\delta_{B/A} = \delta_{S^{-1}B/S^{-1}A}.$$

PROOF. If $x_1, \ldots, x_n \in B$ then $\delta(x_1, \ldots, x_n)$ is an element of both $\delta_{B/A}$ and of $\delta_{S^{-1}B/S^{-1}A}$. Thus

$$S^{-1}\delta_{B/A} = \langle \delta(x_1, \ldots, x_n) \mid x_1, \ldots, x_n \in B \rangle_{S^{-1}A} \subseteq \delta_{S^{-1}B/S^{-1}A}.$$

Conversely, if $y_1, \ldots, y_n \in S^{-1}B$ then there is $s \in S$ such that $sy_i \in B$ for all i. Then

$$\delta(y_1, \ldots, y_n) = s^{-2n}\delta(sy_1, \ldots, sy_n) \in S^{-1}\delta_{B/A},$$

so $\delta_{S^{-1}B/S^{-1}A} \subseteq S^{-1}\delta_{B/A}$. □

THEOREM 5.30. *Let A be a Dedekind domain with fraction field K, let L/K be a finite degree field extension, and let B be the integral closure of A in L. We **suppose** that B is finitely generated as an A-module (by Theorem 5.20, this holds if L/K is separable, the case of most interest to us). Let δ be the discriminant ideal of B/A. For $\mathfrak{p} \in \operatorname{MaxSpec} A$, the following are equivalent:*

(i) *The prime $\mathfrak{p}$ ramifies in L.*
(ii) *We have $\mathfrak{p} \mid \delta$.*

PROOF. Both conditions are local on A: that is, we may replace A with $A_{\mathfrak{p}}$ and B with $B_{\mathfrak{p}} := B \otimes_A A_{\mathfrak{p}}$, with the usual pleasant consequence: A is a DVR and B is a semilocal PID that is a free A-module. Because of the compatibility of the trace form with base change, we have that $\mathfrak{p} \mid \delta$ if and only if the trace form on the $A/\mathfrak{p}$-algebra $B/\mathfrak{p}B$ has discriminant 0. Let us put $k(\mathfrak{p}) := A/\mathfrak{p}$. Since $k(\mathfrak{p})$ is a field, by Theorem 5.4 the discrminant of $B/\mathfrak{p}B$ is 0 if and only if $B/\mathfrak{p}B$ is *not* an étale $k(\mathfrak{p})$-algebra. We may factor

$$\mathfrak{p}B = \mathcal{P}_1^{e_1} \cdots \mathcal{P}_r^{e_r},$$

and then

$$B/\mathfrak{p}B \cong B/\prod_{i=1}^r B/\mathcal{P}_i^{e_i} \cong \prod_{i=1}^r B/\mathcal{P}_i^{e_i}.$$

A finite product of k-algebras is étale if and only if each factor is étale. For $B/\mathcal{P}_i^{e_i}$ to be étale, it must be reduced, which holds iff $e_i = 1$. The $B/\mathcal{P}_i$ is an étale $k(\mathfrak{p})$-algebra if and only if the extension is separable. Thus $\mathfrak{p} \nmid \delta$ if and only if each ramification index equals 1 and each residual extension $(B/\mathcal{P}_i)/k(\mathfrak{p})$ is separable, which is precisely the definition for $\mathfrak{p}$ to be unramified in L. □

This has the following very important consequence:

COROLLARY 5.31. *Maintain the hypotheses of Theorem 5.30. Then:*

(i) *If L/K is separable, then only finitely many $\mathfrak{p} \in \operatorname{MaxSpec} A$ ramify in L.*
(ii) *If L/K is inseparable, then* every *$\mathfrak{p} \in \operatorname{MaxSpec} A$ ramifies in L.*

PROOF. By Theorem 5.16 and the compatbility of the discriminant with respect to the localization map map $A \hookrightarrow K$ (Exercise 4.20), we have that δ is a nonzero ideal of A if and only if L/K is separable. A nonzero ideal in the Dedekind domain A is divisible by – equivalently, contained in – only finitely many $\mathfrak{p} \in \operatorname{MaxSpec} A$, whereas the zero ideal is divisible by – equivalently, contained in – every $\mathfrak{p} \in \operatorname{MaxSpec} A$. □

The next three exercises share the following setup:
• l/k is a degree n field extension;
• $A := k[t]$, a PID with fraction field $l(t)$;
• $L := k(t)$;
• B is the integral closure of A in L.

EXERCISE 5.31. *Show: $B = l[t]$. Deduce: B is a finitely generated A-module. (Suggestion: it is enough to show that $l[t]$ is an integral extension of $k[t]$ that is integrally closed and has fraction field L.)*

EXERCISE 5.32. *With notation as above, suppose that l/k is separable.*

a) *Show: $\delta_{B/A}$ is generated by an element of $A^\times$. Deduce: every $\mathfrak{p} \in \operatorname{MaxSpec} A$ is uramified in B.*

b) *Show again that every* $\mathfrak{p} \in \operatorname{MaxSpec} A$ *is unramified in* B *by working directly with* $\mathfrak{p}B$.

EXERCISE 5.33. *With notation as above, suppose that* l/k *is inseparable.*

a) *Show:* $\delta_{B/A} = (0)$. *Deduce: every* $\mathfrak{p} \in \operatorname{MaxSpec} A$ *is unramified in* B.
b) *Let* $\mathfrak{p} = \langle t \rangle$. *Show:* $\mathcal{P} = \mathfrak{p}B$ *is a prime ideal, so* $e(\mathcal{P}|\mathfrak{p}) = 1$. *Compute* $k(\mathfrak{p}) := A/\mathfrak{p}$ *and* $l(\mathcal{P}) := B/\mathcal{P}$ *and show that* $l(\mathcal{P})/k(\mathfrak{p})$ *is inseparable.*
c) *Show: there is* $\mathfrak{p} \in \operatorname{MaxSpec} A$ *and a prime ideal* $\mathcal{P}$ *of* B *lying over* $\mathfrak{p}$ *such that* $e(\mathcal{P}|\mathfrak{p}) > 1$.
(Suggestion: There is $\alpha \in l$ *such that the minimal polynomial* $f \in k[t]$ *of* α *is inseparable. Take* $\mathfrak{p} = \langle f \rangle$ *and use Exercise 5.10.)*

EXAMPLE 5.32. *Let* k *be a field of characteristic* $p > 0$. *Put* $A := k[t]$, *a PID with fraction field* $K := k(t)$. *Let* $L := k(t^{1/p})$. *Then* L/K *is inseparable of degree* p. *Let* B *be the integral closure of* A *in* L. *We claim that* $B = k[t^{1/p}]$: *on the one hand,* $t^{1/p}$ *is certainly integral over* A, *so* $k[t^{1/p}] \subseteq B$. *On the other hand,* $k[t^{1/p}]$ *is isomorphic to* $k[t]$, *hence a PID, hence is integrally closed and has fraction field* L, *so any element of* L *that is integral over* A *would also be integral over* $k[t^{1/p}]$ *and hence have to lie in* $k[t^{1/p}]$.

Let $\mathfrak{p} \in \operatorname{MaxSpec} A$. *Then* $\mathfrak{p} = \langle f \rangle$ *for a monic irreducible polynomial*

$$f = t^n + a_{n-1}t^{n-1} + \ldots + a_0 \in k[t].$$

By Example 5.27, the ideal $\mathfrak{p}B$ *is a prime power. More explicitly,* $\mathfrak{p}B$ *is the principal ideal of* $k[t^{1/p}]$ *generated by* $f(t)$. *If we make the "change of variable"* $s := t^{1/p}$, *then* $\mathfrak{p}B$ *is the principal ideal of* $k[s]$ *generated by*

$$f(t) = f(s^p) = s^{np} + a_{n-1}s^{(n-1)p)} + \ldots + a_1 s^p + a_0.$$

Then $f(s^p)' = 0$, *so* $f(s^p)$ *is not separable.*
Case 1: *Suppose* k *is perfect. Then* $f(s^p)' = 0$ *means that* $f(s^p)$ *cannot be irreducible. More explicitly we have*

$$f(s^p) = (s^n + a_{n-1}^{1/p}s^{n-1} + \ldots + a_1^{1/p}s + a_0^{1/p})^p = g(s)^p,$$

where $g(s) = s^n + a_{n-1}^{1/p}s^{n-1} + \ldots + a_1^{1/p}s + a_0^{1/p}$. *Because* k *is perfect, the* p*th power map is a field automorphism of* k, *which induces a ring automorphism of* $k[t]$, *and under this automorphism* $g(s)$ *maps to the irreducible polynomial* $f(s)$, *so* $g(s)$ *is also irreducible. Thus* $\mathcal{P} := \langle g(s) \rangle \in \operatorname{MaxSpec} B$ *and*

$$\mathfrak{p}B = \mathcal{P}^p.$$

In particular we have $e(\mathcal{P}/\mathfrak{p}) = p$.
Case 2*: Suppose* k *is imperfect: there is* $\alpha \in k \setminus k^p$. *By* [**Cl-FT**, Lemma 9.20] *we have that for all* $n \in \mathbb{Z}^+$, *the polynomial* $t^{p^n} - \alpha \in k[t]$ *is irreducible. Let us take*

$$f(t) := t^p - \alpha,$$

so $\mathfrak{p}B = \langle g(s) \rangle$, *where*

$$g(s) = (s^p)^p - \alpha = s^{p^2} - \alpha.$$

In this case, if we put

$$k(\mathfrak{p}) := A/\mathfrak{p} \text{ and } l(\mathcal{P}) := B/\mathcal{P},$$

then $k(\mathfrak{p}) = k(\alpha^{1/p})$ *and* $l(\mathcal{P}) = k(\alpha^{1/p^2})$, *so* $l(\mathcal{P})/k(\mathcal{P})$ *is an inseparable field extension of degree* p.

5. The Ideal Norm

Let A be a Dedekind domain with fraction field K, let L/K be a degree n field extension, and let B be the integral closure of A in L, so B is a Dedekind domain. We will assume that B is finitely generated as an A-module, which once again will be the case if L/K is separable.

As for any inclusion $\iota : A \hookrightarrow B$ of domains, we have a group homomorphism $\iota_* : \operatorname{Frac} A \to \operatorname{Frac} B$ defined by

$$\iota_*(I) \coloneqq BI = I \otimes_A B.$$

We will now define a group homomorphism

$$N : \operatorname{Frac} B \to \operatorname{Frac} A$$

in the other direction. Because $\operatorname{Frac} B$ is a free $\mathbb{Z}$-module with basis $\operatorname{MaxSpec} B$, we may freely define $N(\mathcal{P})$ for all $\mathcal{P} \in \operatorname{MaxSpec} B$ and this extends to a unique group homomorphism. The most obvious such map is probably the one that sends $\mathcal{P}$ to the unique prime $\mathfrak{p}$ of A that lies below it. However, we will make a different choice (and explain why!).

Let J be a nonzero integral ideal of B. We claim that B/J is a finitely generated torsion A-module. Indeed, if $J = \mathcal{P}_1 \cdots \mathcal{P}_r$ for not necessarily distinct $\mathcal{P}_j \in \operatorname{MaxSpec} B$, then

$$J \cap A \supseteq (\mathcal{P}_1 \cap A) \cdots (\mathcal{P}_r \cap A),$$

which is a nonzero ideal of A, so B/J is a finitely generated $A/(J \cap A)$-module, hence a finitely generated torsion A-module. Therefore we may take the characteristic ideal of B/J *as an A-module*, which we write as $\chi_A(B/J)$. By definition, this is the **ideal norm** of J:

$$N(J) \coloneqq \chi_A(B/J).$$

It is sometimes convenient for bookkeeping to also define the norm of the zero ideal: as you surely suspected, we will put

$$N((0)) \coloneqq (0).$$

LEMMA 5.33. *For any nonzero ideals I and J in a Dedekind domain A, we have $I/(IJ) \cong_A A/J$.*

PROOF. Both sides are A/J-modules, so if we factor $J = \mathfrak{p}_1^{a_1} \cdots \mathfrak{p}_r^{a_r}$, they are also modules over the semilocalization $A_{\mathfrak{p}_1,\ldots,\mathfrak{p}_r}$. Thus we may assume that A is a PID, and in this case the result is easy: if $I = (\alpha)$ then multiplication by α gives an isomorphism from A/J to $I/(IJ)$. □

PROPOSITION 5.34. *For any nonzero ideals J_1, J_2 of B, we have*

$$N(J_1 J_2) = N(J_1) N(J_2).$$

PROOF. We have a short exact sequence of finite length A-modules

$$0 \to J_2/(J_1 J_2) \to B/(J_1 J_2) \to B/J_2 \to 0,$$

so $\chi_A(B/J_1 J_2) = \chi_A(J_2/(J_1 J_2))\chi_A(B/J_2)$. By Lemma 5.33 we know that $J_2/(J_1 J_2)$ and B/J_1 are isomorphic B-modules, so certainly they are isomorphic A-modules. Thus $\chi_A(J_2/(J_1 J_2) = \chi_A(B/J_1)$, and the result follows. □

So far we have defined the ideal norm as a map from integral B-ideals to integral A-ideals. We want to extend this to a map

$$N : \operatorname{Frac} B \to \operatorname{Frac} A.$$

There are two very reasonable ways to do this:
(1) For nonzero integral ideals I, J of B, we put

$$N(IJ^{-1}) := \frac{N(I)}{N(J)}. \tag{15}$$

Indeed, by Proposition 5.34, the ideal norm on integral ideals is a homomorphism from the monoid $\operatorname{Int} B$ of nonzero integral ideals of B under multiplication to the monoid $\operatorname{Int} A$ of nonzero integral ideals of A. For a Dedekind domain A, the monoid $\operatorname{Int} A$ of nonzero A-ideals under multiplication is the free commutative monoid on $\operatorname{MaxSpec} A$ and $\operatorname{Frac} A$ is its group completion, the free commutative group on $\operatorname{MaxSpec} A$. From this it follows easily that there is a unique way to extend any monoid homomorphism $\operatorname{Int} B \to \operatorname{Int} A$ to a group homomorphism $\operatorname{Frac} B \to \operatorname{Frac} A$: namely, as we did above.

(2) For a fractional ideal J of B, we may view B and J as A-lattices in the K-vector space L and take their Fröhlich invariant $\chi_A(B, J)$. (Here we write the subscripted A because B and J are also B-lattices in the one-dimensional L-vector space L, but $\chi_B(B, J) = J$ is not what we want.)

Happily, (1) and (2) turn out to be the same. For notational simplicity, let us define the ideal norm of a fractional ideal via (15). Then:

PROPOSITION 5.35. *Let $J \in \operatorname{Frac} B$. Then $N(J) = \chi_A(B, J)$.*

PROOF. This is the definition of $N(J)$ for integral ideals J. If J is a fractional B-ideal, let $\alpha \in A^\bullet$ be such that $I := \alpha J \subseteq B$, so $J = I(\alpha)^{-1}$. We observe that $N((\alpha)) = (\alpha)^n$: indeed, by localizing we can reduce to the case that A is a PID and then if $e_1, \ldots, e_n$ is an A-basis for B, then $\alpha e_1, \ldots, \alpha e_n$ is an A-basis for αB, so $B/\alpha B \cong \bigoplus_{i=1}^n A/(\alpha)$. Then we have

$$\chi_A(B, J) = (\alpha)^{-n}\chi(B/\alpha J) = N(\alpha B)^{-1}N(\alpha J) = \frac{N(I)}{N(\alpha B)}. \qquad \square$$

Let us introduce a different notion of an ideal norm. If R is a ring and I is an ideal such that R/I is finite, we put

$$||I|| := \#R/I.$$

When $A = \mathbb{Z}$ there is a close realtionship between these two norms. In this case $B = \mathbb{Z}_L$ is the ring of integers of the number field L. Since the characteristic ideal of a finite length $\mathbb{Z}$-module M is the principal ideal generated by $\#M$, we find:

$$\forall J \in \operatorname{Int} \mathbb{Z}_L,\ N(J) = ||J||.$$

The latter ideal norm $||J||$ – when it is different from $N(J)$ – will make only very sporadic appearances in these notes (e.g. in our discussion of the Chebotarev Density Theorem in the function field case). But while we are here, let us record one result about it.

THEOREM 5.36 (Samuel [**Sa71**]). *Let R be a Noetherian ring, and let $n \in \mathbb{Z}^+$. The set of ideals I of R with $||I|| = n$ is finite.*

PROOF. For $n \in \mathbb{Z}^+$, the number of isomorphism classes of rings of cardinality n is finite, so 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

$$B := R/\mathfrak{b} \hookrightarrow \prod_{i \in I} R/\mathfrak{b}_i \cong S^I. \tag{16}$$

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 $1 \leq j \leq r$, we have $x^{q_j} - x \in \mathfrak{m}_j$, so $P(x) = 0$. It follows that for all $X = (x_i) \in S^I$, $P(X) = (P(x_i)) = 0$. From (16) 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. By Exercise 2.5, an Artinian ring with finite residue fields is actually finite. That is, $R/\mathfrak{b}$ is finite, so there are only finitely many ideals of R containing $\mathfrak{b}$. In particular I is finite. □

Now let us compute the ideal norm more concretely. As above, multiplicativity reduces us to the case of $N(\mathcal{P})$ for $\mathcal{P} \in \operatorname{MaxSpec} B$. In this case, $\mathfrak{p} := \mathcal{P} \cap A$ is a prime ideal of A, so $B/\mathcal{P}$ is a finite-dimensional $A/\mathfrak{p}$-vector space, so

$$\chi(B/\mathcal{P}) = \mathfrak{p}^{\dim_{A/\mathfrak{p}} B/\mathcal{P}} = \mathfrak{p}^{f_{\mathcal{P}|\mathfrak{p}}}.$$

COROLLARY 5.37. *Let $n := [L : K]$.*

a) *For all $I \in \operatorname{Frac} A$ we have $N(\iota_*(I)) = I^n$.*

b) *The pushforward map $\iota_* : \operatorname{Frac} A \to \operatorname{Frac} B$ is injective.*

PROOF. a) Both sides of $N(\iota_*(I)) = I^n$ are multiplicative in I, so it is enough to consider the case of a prime ideal $\mathfrak{p}$ of A. Then $\iota_*(\mathfrak{p}) = \mathcal{P}_1^{e_1} \cdots \mathcal{P}_r^{e_r}$. Fo each $1 \leq i \leq r$ we have $N(\mathcal{P}) = \mathfrak{p}^{f(\mathcal{P}|\mathfrak{p})}$, so using Theorem 5.26b), we get

$$N(\iota^*(\mathfrak{p}))) = \prod_{i=1}^r \mathfrak{p}^{e_{\mathcal{P}|\mathfrak{p}} f_{\mathcal{P}|\mathfrak{p}}} = \mathfrak{p}^{\sum_{i=1}^r e(\mathcal{P}|\mathfrak{p}) f(\mathcal{P}|\mathfrak{p})} = \mathfrak{p}^n.$$

b) By part a), the composition $N \circ \iota_*$ on $\operatorname{Frac} A$ is $I \mapsto I^n$, which is injective since as a $\mathbb{Z}$-module $\operatorname{Frac} A$ is free, hence torsionfree. Therefore ι_* is also injective. □

We now give still another interpretation of the ideal norm in terms of the norm $N_{L/K}$ of the field extension L/K. First:

PROPOSITION 5.38. *Let $\beta \in L$. Then $N((\beta)) = N_{L/K}(\beta)$.*

PROOF. We have $N((\beta)) = \chi_A(B/(\beta B))$. Since βB is the image of the lattice B under the linear transformation $\beta\cdot$, by Proposition 4.6 we have

$$\chi_A(B/(\beta B)) = (\det \beta\cdot) = N_{L/K}(\beta).$$ □

Proposition 5.38 shows in particular that using the notation N for the ideal norm is not as "overloaded" as it first appeared.

If A is a DVR, then B is a PID, so every fractional ideal is principal. In general, like any ideal in a Dedekind domain, the ideal norm can be computed locally, and this leads to the following result.

THEOREM 5.39. *Let $J \in \operatorname{Frac} B$. Then*

$$N(J) = \langle N_{L/K}(\beta) \mid \beta \in J \rangle_A.$$

PROOF. Let I be the A-module generated by $N_{L/K}(\beta)$ for $\beta \in J$, so we want to show that $I = N(J)$. If we write $I = \prod_{\mathfrak{p}} \mathfrak{p}^{a_\mathfrak{p}}$ and $N(J) = \prod_{\mathfrak{p}} \mathfrak{p}^{b_\mathfrak{p}}$ then we want to show that $a_\mathfrak{p} = b_\mathfrak{p}$ for all $\mathfrak{p}$ or, equivalently, that for all $\mathfrak{p} \in \operatorname{MaxSpec} A$ we have $I_\mathfrak{p} = N(J)_\mathfrak{p}$ as ideals of $A_\mathfrak{p}$. Note that

$$I_\mathfrak{p} = \langle N_{L/K}(\beta) \mid \beta \in J \rangle_{A_\mathfrak{p}} = \langle N_{L/K}(\beta) \mid \beta \in J_\mathfrak{p} \rangle_{A_\mathfrak{p}}$$

and $N(J)_\mathfrak{p} = N(J_\mathfrak{p})$. Since $B_\mathfrak{p}$ is a PID, $J_\mathfrak{p}$ is principal, say, $J_\mathfrak{p} = (\pi_\mathfrak{p})$, and then $N(J_\mathfrak{p}) = \langle N_{L/K}\pi_\mathfrak{p} \rangle_{A_\mathfrak{p}}$, which shows that $N(J_\mathfrak{p}) \subseteq I_\mathfrak{p}$. On the other hand, every $\beta \in J_\mathfrak{p}$ is therefore of the form $\pi_\mathfrak{p}\gamma_\mathfrak{p}$ for some $\gamma_\mathfrak{p} \in B_\mathfrak{p}$, and thus $N_{L/K}(\beta) = N_{L/K}(\pi_\mathfrak{p})N_{L/K}(\gamma_\mathfrak{p}) \in \langle N_{L/K}(\pi_\mathfrak{p}) \rangle_{A_\mathfrak{p}} = N(J)_\mathfrak{p}$, so $I_\mathfrak{p} \subseteq N(J_\mathfrak{p})$. □

6. Dedekind-Kummer and Monogenicity

6.1. Dedekind-Kummer Version 1.

EXERCISE 5.34. *Let R be a Dedekind domain with fraction field K, let V be a finite-dimensional K-vector space. Let $\Lambda_1, \Lambda_2, \Lambda_3$ be three lattices in V. Suppose:*

(i) *We have $\Lambda_2 \subseteq \Lambda_3$.*
(ii) *We have $\chi(\Lambda_1, \Lambda_2) = \chi(\Lambda_1, \Lambda_3)$.*

Then $\Lambda_2 = \Lambda_3$.

EXERCISE 5.35. *Let A be a Dedekind domain with fraction field K, let L/K be a finite degree field extension, and let B be the integral closure of A in L, which we assume is finitely generated as an A-module. Let I and J be nonzero ideals of B. Suppose that $I \subseteq J$ and $N(I) = N(J)$. Show: $I = J$.*

THEOREM 5.40 (Dedekind-Kummer, Take 1). *Let A be a Dedekind domain with fraction field K, let L/K be a degree n separable field extension, and let B be the integral closure of A in L. **We suppose** that there is $\alpha \in B$ such that $B = A[\alpha]$. Let $f \in A[t]$ be the minimal polynomial of α. Then: for $\mathfrak{p} \in \operatorname{MaxSpec} A$, let*

$$\overline{f} = \prod_{i=1}^{r} \overline{g_i}^{e_i}$$

be the factorization of the image $\overline{f}$ of f in $A/\mathfrak{p}[t]$. For $1 \leq i \leq r$, let g_i be any lift of $\overline{g_i}$ to a monic polynomial in $A[t]$, and put

$$\mathcal{P}_i := \langle \mathfrak{p}, g_i(\alpha) \rangle.$$

Then each $\mathcal{P}_i$ is a maximal ideal of B, we have

$$\mathfrak{p}B = \prod_{i=1}^{r} \mathcal{P}_i^{e_i}$$

and we have $B/\mathcal{P}_i \cong A[t]/\overline{g_i}$. In particular, we have $f(\mathcal{P}_i|\mathfrak{p}_i) = \deg(\overline{g_i})$.

PROOF. Step 1: Since $B = A[\alpha] \cong A[t]/(f)$, we have

$$B/\mathcal{P}_i = A[\alpha]/\langle \mathfrak{p}, g_i(\alpha) \cong A[t]/\langle f, \mathfrak{p}, g_i\rangle \cong (A/\mathfrak{p})[t]/\langle \overline{f}, \overline{g_i}\rangle \cong (A/\mathfrak{p})[t]/(\overline{g_i}).$$

Now $\mathfrak{p}$ is a maximal ideal of A, so $A/\mathfrak{p}$ is a field, so $(A/\mathfrak{p})[t]$ is a PID and thus the irreducible polynomial $\overline{g_i}$ generates a maximal ideal in it. This shows that $\mathcal{P}_i$ is a maximal ideal of B, and evidently it contains $\mathfrak{p}$. Moreover it is clear that the residual degree $f(\mathcal{P}_i|\mathfrak{p}) = [(A/\mathfrak{p})[t]/(\overline{g_i}) : A/\mathfrak{p}] = \deg \overline{g_i}$.
Step 2: We claim that $\mathfrak{p}B$ divides $\prod_{i=1}^r \mathcal{P}_i^{e_i}$. Indeed, we have

$$\prod_{i=1}^r \mathcal{P}_i^{e_i} = \prod_{i=1}^r \langle \mathfrak{p}, g_i(\alpha)\rangle^{e_i} = \prod_{i=1}^r (\mathfrak{p}B + (g_i(\alpha))^{e_i}.$$

When we multiply out this product, it is clear that every term is divisible by $\mathfrak{p}$, except possibly for the term in which $\mathfrak{p}$ does not appear, but this latter term is

$$\prod_{i=1}^r (g_i(\alpha)^{e_i}) \equiv (f(\alpha)) \equiv 0 \pmod{\mathfrak{p}B}.$$

Step 3: We now know that $\mathfrak{p}B \supset \prod_{i=1}^r \mathcal{P}_i^{e_i}$. To show equality it suffices to show that $N(\prod_{i=1}^r \mathcal{P}_i^{e_i}) = \mathfrak{p}^n$, since then $N(\prod_{i=1}^r \mathcal{P}_i^{e_i}) = \mathfrak{p}^n = N(\mathfrak{p}B)$, so $\mathfrak{p}B = \prod_{i=1}^r \mathcal{P}_i^{e_i}$ by Exercise 5.35.

So: we have

$$N(\prod_{i=1}^r \mathcal{P}_i^{e_i}) = \mathfrak{p}^{\sum_{i=1}^r f(\mathcal{P}_i|\mathfrak{p})e_i} = \mathfrak{p}^{\sum_{i=1}^r e_i \deg \overline{g_i}} = \mathfrak{p}^{\deg f} = \mathfrak{p}^n. \qquad \square.$$

Let us give some applications.

EXAMPLE 5.41. *Let $D \in \mathbb{Z}^\bullet$ be a squarefree integer that is not a square, and let $K = \mathbb{Q}(\sqrt{D})$.*

a) *Suppose $D \equiv 2, 3 \pmod 4$. Then $\mathbb{Z}_K = \mathbb{Z}[\sqrt{D}]$, and the discriminant is $\Delta = 4D$. The minimal polynomial of $\sqrt{D}$ is $f(t) = t^2 - D$. Let $p \in \mathbb{Z}$ be a prime number. By Dedekind-Kummer:*
• If Δ is a nonzero square modulo p, then let $u \in (\mathbb{Z}/p\mathbb{Z})^2$ by such that $u^2 = \Delta$. Then f factors mod p as $(t+u)(t-u)$. By Dedekind-Kummer, (p) splits in $\mathbb{Z}_K$ into two primes $\mathcal{P}_1 = \langle p, \sqrt{D} + u\rangle$, $\mathcal{P}_2 = \langle p, \sqrt{D} - u\rangle$.
• If Δ is not a square modulo p, then $t^2 - D$ remains irreducible modulo p, so p is inert in $\mathbb{Z}_K$. Notice that Dedekind-Kummer says that the ideal over p is generated by p and $\sqrt{D}^2 - D$, but of course the latter element is 0, so the ideal is generated by p: that's what inert means.
• If $p \mid \Delta$, then f factors modulo p as t^2. The unique prime $\mathcal{P}$ of $\mathbb{Z}_K$ over (p) is $\mathcal{P} := \langle p, \sqrt{D}\rangle$.

b) *Suppose $D \equiv 1 \pmod 4$. Then $\mathbb{Z}_K = \mathbb{Z}[\alpha]$ where $\alpha = \frac{1+\sqrt{D}}{2}$, and the discriminant is $\Delta = D$. The minimal polynomial of α is $f(t) = t^2 + t + \frac{1-D}{4}$. Let p be an **odd** prime number. Since the discriminant of this polynomial is D, this goes much the same as in the previous part:*
• If D is a nonzero square modulo p, then (p) splits into $\mathcal{P}_1 = \langle p, t + u$ and $\mathcal{P}_2 = \langle p, t - u\rangle$, where u is a root of $t^2 + t + \frac{1-D}{4}$ modulo p.
• If D is not a square modulo p, then (p) is inert in $\mathbb{Z}_K$.
• If $p \mid D$, then let $r \in \mathbb{Z}$ be such that modulo p we have $t^2 + t + \frac{1-D}{4} = (t-r)^2$. Then $(p) = \mathcal{P}^2$, where $\mathcal{P} = \langle p, \alpha - r\rangle$.

EXERCISE 5.36. *Let $D \neq 1$ be a squarefree integer such that $D \equiv 1 \pmod 4$, and let $K = \mathbb{Q}(\sqrt{D})$. Show:*

a) *If $D \equiv 1 \pmod 8$, then 2 splits in $\mathbb{Z}_K$.*
b) *If $D \equiv 5 \pmod 8$, then 2 is inert in $\mathbb{Z}_K$.*

EXAMPLE 5.42. *Let A be a PID with fraction field K, let L/K be a separable quadratic field extension, and let B be the integral closure of A in L. I claim that B/A is a free A-module (necessarily of rank 1): if not, there is $x \in B \setminus A$ and $a \in A^\bullet$ such that $ax \in A$. But then $x \in \frac{1}{a}A \subseteq K$ and also is integral over A; since A is integrally closed, we get $x \in A$, a contradiction. Let α be the lift of a generator of B/A to A. Then $B = A[\alpha]$, so B is monogenic. Let $f(t) = t^2 + bt + c \in A[t]$ be the minimal polynomial for α, and let $\Delta = b^2 - 4c$. Let $\mathfrak{p} = (p) \in \operatorname{MaxSpec} A$. Then if Δ is a nonzero square in $A/(p)$, then (p) splits in B, if Δ is not a square in $A/(p)$, then (p) is inert in B, and if $p \mid \Delta$ then p ramifies in B.*

EXAMPLE 5.43. *Let $N \in \mathbb{Z}^{\geq 3}$. Let $\zeta_N = e^{2\pi i/N}$ and put $K \coloneqq \mathbb{Q}(\zeta_N)$, the Nth cyclotomic field. By* [**Cl-FT**, Thm. 9.8]*, the minimal polynomial for ζ_N is $\Phi_N(t)$, the monic polynomial whose roots are the primitive Nth roots of unity. We will use the fact that $\mathbb{Z}_K = \mathbb{Z}[\zeta_N]$. Thus the factorization of a prime ideal (p) of $\mathbb{Z}$ corresponds to the factorization of Φ_N modulo p. In particular:*

- *Suppose $p \equiv 1 \pmod N$. Then $N \mid (p-1)$, so the cyclic group $\mathbb{F}_p^\times$ has an element of order N, or in the other words, the fiinite field $\mathbb{F}_p$ contains a primitive Nth root of unity, so $\Phi_N(t)$ splits completely modulo p and thus (p) splits in $\mathbb{Z}_K$.*
- *Conversely, let $p \nmid N$. Then $\Phi_N(t)$ is separable in $\mathbb{F}_p$. If it splits completely, then the primitive Nth roots of unity live in $\mathbb{F}_p$, so $N \mid p-1$, so $p \equiv 1 \pmod N$. Thus a prime p splits completely in $\mathbb{Z}_K$ iff $p \equiv 1 \pmod N$.*
- *If $p \mid N$, there is no primitive pth root of unity in $\mathbb{F}_p$, hence no primitive Nth root of unity in $\mathbb{F}_p$. Thus $\Phi_n(t)$ is* not *separable in $\mathbb{F}_p[t]$, so p ramifies in $\mathbb{Z}_K$.*

The obvious limitation in Theorem 5.40 is the assumption that $B = A[\alpha]$ for some $\alpha \in B$: when this holds for a ring extension B/A, we say that B is **monogenic** over A. One might at first think that this monogenicity is automatic: after all, it is for a finite separable field extension L/K, as part of the Primitive Element Theorem. But such an extension B/A of Dedekind domains need not be monogenic, even when A is a PID. The following result allows for the production of a large class of counterexamples.

THEOREM 5.44. *Let A be a Dedekind domain with fraction field K, let L/K be a finite degree field extension, and let B be the integral closure of A in L. Let $\mathfrak{p} \in \operatorname{MaxSpec} A$ be such that $A/\mathfrak{p}$ has order q. Suppose that there are $\alpha_1, \ldots, \alpha_m \in B$ such that $B = A[\alpha_1, \ldots, \alpha_m]$, and let r be the number of prime ideals $\mathcal{P}$ of B lying over $\mathfrak{p}$ of degree 1: $f(\mathcal{P}|\mathfrak{p}) = 1$. Then:*

$$m \geq \log_q(r).$$

PROOF. Put $\mathbb{F}_q \coloneqq A/\mathfrak{p}$, a finite field of order q. Since $B = A[\alpha_1, \ldots, \alpha_m]$, we have a surjective A-algebra homomorphism

$$A[t_1, \ldots, t_m] \to B.$$

Tensoring to $A/\mathfrak{p}$ (or noting that the composite map $A[t_1, \ldots, t_m] \to B \to B/\mathfrak{p}B$ factors through $A/\mathfrak{p}[t_1, \ldots, t_m]$) we get a surjective $\mathbb{F}_q$-algebra homomorphism

$$\mathbb{F}_q[t_1, \ldots, t_m] \to B/\mathfrak{p}B. \tag{17}$$

In turn, we may write $\mathfrak{p}B = \mathcal{P}_1^{e_1} \cdots \mathcal{P}_r^{e_r} J$ with the $\mathcal{P}_i$'s degree 1 primes and $\gcd(\mathcal{P}_1 \cdots \mathcal{P}_r, J) = 1$. We then get surjective $\mathbb{F}_q$-algebra maps

$$B/\mathfrak{p}B \xrightarrow{\sim} \prod_{i=1}^{r} B/\mathcal{P}_i^{e_I} \times B/J \to \prod_{i=1}^{r} B/\mathcal{P}_i = \mathbb{F}_q^r. \tag{18}$$

Composing (17) and (18) we get a surjective $\mathbb{F}_q$-algebra homomorphism

$$\mathbb{F}_q[t_1, \ldots, t_m] \to \mathbb{F}_q^r.$$

Since $\mathbb{F}_q^r$ has r maximal ideals, each with residue field $\mathbb{F}_q$, it follows that $\mathbb{F}_q[t_1, \ldots, t_m]$ has at least r maximal ideals with residue field $\mathbb{F}_q$. But by [**CA**, Lemma 11.2], for any field K, there is a bijection from K^m to the set of maximal ideals of $K[t_1, \ldots, t_m]$ with residue field K given by

$$(x_1, \ldots, x_m) \mapsto \langle t_1 - x_1, \ldots, t_m - x_m \rangle.$$

So $\mathbb{F}_q[t_1, \ldots, t_m]$ has precisely q^m maximal ideals with residue field $\mathbb{F}_q$, and it follows that $q^m \geq r$ and thus $\log_q m \geq r$. □

If we apply Theorem 5.44 with $A = \mathbb{Z}$, we find: if K is a number field of degree n and p is a prime number such that $\mathbb{Z}_K$ has more than p degree 1 primes lying over p, then $\mathbb{Z}_K$ is not monogenic. The number of degree 1 primes is certainly at most n, so in order for this strategy to succeed we need $n \geq p + 1 \geq 3$.

Using the methods of Number Theory II one can prove that such examples abound: e.g. for any prime p and $n, r \in \mathbb{Z}^+$ such that $1 \leq r \leq n$, there is a degree n number field K for which $\mathbb{Z}_K$ has precisely r degree 1 primes lying over (p), so if $r > p$ then $\mathbb{Z}_K$ is not monogenic. In particular, for all $n \geq 2$ there is a number field K of degree n in which 2 splits completely, so there are n degree 1 primes of $\mathbb{Z}_K$ lying over (2), and by Theorem 5.44, the $\mathbb{Z}$-algebra $\mathbb{Z}_K$ requires $\lceil \log_2 n \rceil$ generators. Remarkably, this bound is sharp: Pleasants has shown that for each number field K of degree $n \geq 2$, $\mathbb{Z}_K$ can be generated as a $\mathbb{Z}$-algebra by $\lceil \log_2 n \rceil$ generators [**Pl74**]. In fact he gives more precise results on the minimal number of generators of $\mathbb{Z}_K$ as a $\mathbb{Z}$-algebra and also the minimal number of generators of $\mathbb{Z}_L$ as a $\mathbb{Z}_K$-algebra for an extension of number fields L/K from which this bound is a consequence.

To give "Number Theory I" examples we will borrow from the following fact that will be covered later on: let A be a Dedekind domain with fraction field K, let L_1 and L_2 be finite degree separable field extensions inside an algebraic closure $\overline{K}$ of K, and let L be the compositum $L_1 L_2$. For $i = 1, 2$ let B_i be the integral clousre of A in L_i, and let B be the integral closure of A in L. Suppose $\mathfrak{p} \in \operatorname{MaxSpec} A$ splits completely in both B_1 and in B_2. Then $\mathfrak{p}$ splits completely in B.

We can apply this to show that various biquadratic number fields $K_{d_1,d_2} \coloneqq \mathbb{Q}(\sqrt{d_1}, \sqrt{d_2})$ are not monogenic. First suppose that d_1 and d_2 are distinct squarefree integers, each different from 1, such that $d_1 \equiv d_2 \equiv 1 \pmod 8$. By Exercise 5.36, 2 splits in both $\mathbb{Q}(\sqrt{d_1})$ and $\mathbb{Q}(\sqrt{d_2})$, so by the above observation, 2 splits completely in K_{d_1,d_2}. Thus $\mathbb{Z}_{K_{d_1,d_2}}$ has $4 > 2$ degree 1 primes lying over (2), so by Proposition 5.44, the Dedekind domain $\mathbb{Z}_{K_{d_1,d_2}}$ is not monogenic over $\mathbb{Z}$.

Now replace the congruence condition $d_1 \equiv d_2 \equiv 1 \pmod 8$ by $d_1 \equiv d_2 \equiv 1$

(mod 3). Then 3 splits in both $\mathbb{Q}(\sqrt{d_1})$ and $\mathbb{Q}(\sqrt{d_2})$, so 3 splits completely in K_{d_1,d_2}. Thus $\mathbb{Z}_{K_{d_1,d_2}}$ has $4 > 3$ degree 1 primes lying over (3), so by Proposition 5.44, the Dedekind domain $\mathbb{Z}_{K_{d_1,d_2}}$ is not monogenic over $\mathbb{Z}$.

EXERCISE 5.37. *Let $f := t^3 - t^2 - 2t - 8 \in \mathbb{Q}[t]$.*

a) *Show: f is irreducible. Let $\alpha \in \mathbb{C}$ be a root of f, and put $K := \mathbb{Q}[\alpha]$, so $K/\mathbb{Q}$ is a cubic number field.*
b) *Put $\mathcal{O} := \mathbb{Z}[\alpha]$. Show: $\Delta_{\mathcal{O}} = -2^2 \cdot 503$. (Note: 503 is prime!)*
c) *Show: $\beta := \frac{\alpha+\alpha^2}{2} \in \mathbb{Z}_K$. Conclude: $\mathbb{Z}_K = \mathbb{Z}[\alpha, \beta]$ and $\Delta_{\mathbb{Z}_K} = -503$.*
d) *For $x \in \mathbb{Z}_K^\bullet$, we write $N(x)$ for the positive generator of $N((x))$, the norm of the principal ideal (x). Recall that this is on the one hand $|N_{K/\mathbb{Q}}(x)|$ and on the other hand is $\#\mathbb{Z}_K/(\alpha)$. Show: $N(\alpha) = 8$ and $N(\alpha - 1) = 10$. Use this to show that 2 splits completely in $\mathbb{Z}_K$.*
e) *Show: $\mathbb{Z}_K$ is* not *monogenic.*

6.2. Supplements to Dedekind-Kummer. The material of this section comes from [**Se:CL**, Ch. III].

PROPOSITION 5.45. *Let R be a DVR with maximal ideal $\mathfrak{m}$ and residue field k. Let $f \in R[t]$ be monic of positive degree, and put*

$$S := R[t]/(f).$$

Then S is a semi-local ring, and its maximal ideals are obtained as follows: let $\overline{f}$ be the image of f in $k[t]$, and factor it: $\overline{f} = p_1^{e_1} \cdots p_r^{e_r}$ with $p_1, \ldots, p_r \in k[t]$ distinct monic irreducible polynomials. For each $1 \leq i \leq r$, choose $g_i \in R[t]$ that lifts p_i (i.e., so that the reduction of g_i modulo $\mathfrak{m}$ is p_i). For $1 \leq i \leq r$, put

$$\mathcal{P}_i := \langle \mathfrak{m}, g_i \rangle.$$

Then $\operatorname{MaxSpec} S = \{\mathcal{P}_1, \ldots, \mathcal{P}_r\}$.

PROOF. For $1 \leq i \leq r$, we have

$$S/\mathcal{P}_i = R[t]/\langle \mathfrak{m}, f, g_i \rangle = k[t]/(p_i)$$

is a (finite degree) field extension of k, so $\mathcal{P}_i$ is a maximal ideal of S. The ideals $\mathcal{P}_1, \ldots, \mathcal{P}_g$ are precisely the maximal ideals of S that contain $\mathfrak{m}S$. We claim that these are all the maximal ideals of S. To see this, let $\mathcal{P}$ be any maximal ideal of S. If $\mathcal{P}$ did not contain $\mathfrak{m}S$, then we would have $\mathcal{P} + \mathfrak{m}S = S$; since S is finitely generated as a module over the local ring $(R, \mathfrak{m})$, Nakayama's Lemma implies $\mathcal{P} = S$, a contradiction. □

LEMMA 5.46. *Let R be a commutative ring, let $f \in R[t]$, and let $a \in R$. There is a unique $g \in R[t]$ such that*

$$f(t) = f(a) + f'(a)(t - a) + (t - a)^2 g(t).$$

PROOF. By the universal property of polynomial rings, there is a unique R-algebra homomorphism $\Psi : R[t] \to R[t]$ that maps t to $t - a$. Clearly the unique homomorphism that maps t to $t + a$ is its inverse, so Ψ is an isomorphism. In particular, it is an R-module isomorphism, so it carries the R-basis $\{t^n \mid n \in \mathbb{N}\}$ to the R-basis $\{(t - a)^n \mid n \in \mathbb{N}\}$. Thus there unique $\{b_n\}_{n=0}^\infty$ in R, all but finitely of which are zero, such that

$$f = \sum_{n=0}^\infty b_n (t - a)^n = b_0 + b_1(t - a) + (t - a)^2 \sum_{n=2}^\infty b_n (t - a)^{n-2}.$$

Evaluating at a we find $b_0 = f(a)$. Differentiating and then evaluating at a we find that $b_1 = f'(a)$. Taking $g \coloneqq \sum_{n=2}^{\infty} b_n (t-a)^{n-2}$, we get

$$f(t) = f(a) + f'(a)(t-a) + (t-a)^2 g(t).$$

The polynomial g has to be unique, for if another polynomial h worked in its place we would have $(t-a)^2(g(t)-h(t)) = 0$, but the monic polynomial $(t-a)^2$ is not a zero divisor in $R[t]$. □

Let R be a Dedekind domain with fraction field K, let L/K be a finite degree field extension, and let S be the integral closure of R in L. We say that S/R is **monogenic** if there is $\alpha \in S$ such that $S = R[\alpha]$. (In particular this implies that S is finitely generated as an R-module, which is always true if L/K is separable but need not hold in general.) In a "global" context, monogenicity is a sensitive issue: it is far from guaranteed that e.g. the ring of integers of a number field is monogenic over $\mathbb{Z}$. (In this classical context, instead of monogenicty one often speaks in terms of the existence of a **power basis**.) However, in the local context monogenicity is much easier: the following result shows in particular that if R is a complete discrete valuation ring with perfect residue field then S/R is monogenic for every finite degree separable field extension L/K. In particular, the ring of integers of every p-adic field is monogenic over $\mathbb{Z}_p$.

THEOREM 5.47. *Let R be a DVR with fraction field K. Let L/K be a separable finite degree field extension, and let S be the integral closure of R in L. We assume:*

(i) *S is a DVR; and*
(ii) *the residual extension l/k is separable.*

Then S is monogenic over R.

PROOF. Let $\mathfrak{p}$ be the maximal ideal of R and $\mathcal{P}$ be the maximal ideal of S, and let π be a uniformizer of S. Let $e = e(L/K)$, so $\mathfrak{p}S = (\pi^e)$. Let $k \coloneqq R/\mathfrak{p}$ and $l \coloneqq S/\mathcal{P}$, so $f = [l : k]$. By Theorem 5.26 we have $ef = [L : K]$. Since l/k is assumed separable, by the Primitive Element Theorem there is $\overline{x} \in l$ such that $l = k[\overline{x}]$. Let x be a lift of $\overline{x}$ to S.

Step 1: We claim that $\{x^i \pi^j\}_{0 \le i < f,\ 0 \le j < e}$ span S as an R-module.[5] By Nakayama's Lemma it is enough to show that their images in $S/\mathfrak{p}S$ span it as an R-module. Since $\mathfrak{p}S = \pi^e S$, it is enough to show that for all $0 \le m < e$, if the elements span $S/\pi^m S$ then they span $S/\pi^{m+1}S$. For $m = 0$, we have $S/\pi S = l$, so certainly the elements $1, x, \ldots, x^{f-1}$ span. Inductively we assume that for $1 \le m < e$ the elements $x^i \pi^j$ with $0 \le j < m$ span $S/\pi^m S$, and let $x \in S$. Then by assumption there are $r_{i,j} \in R$ and $y \in S$ such that

$$x - \sum_{i,j} r_{i,j} x^i \pi^j = \pi^m y.$$

There are $a_0, \ldots, a_{f-1} \in R$ such that $y - \sum_i a_i x^i \in \pi S$. Thus

$$x - \sum_{i,j} r_{i,j} x^i \pi^i - \sum_{i=0}^{f-1} a_i x^i \pi^m \in \pi^{m+1} S.$$

[5]Since L/K is separable, S is free of rank n as an R-module. By [**CA**, Thm. 3.44], the claim implies that $\{x^i \pi^j\} - 0 \le i < f,\ 0 \le j < e$ in fact form an R-basis of S.

Step 2: We claim that we may choose x such that there is $g \in R[t]$ monic of degree f such that $g(x)$ is a uniformizer of S.
Proof: Start first with $g \in R[t]$ monic that reduces to the minimal polynomial of $\overline{x}$ over k. Let w be the normalized valuation on L, so $w(g(x)) \geq 1$. If $w(g(x)) = 1$, we have found our g. Otherwise $w(g(x)) \geq 2$. Let π be a uniformizer for L. By Lemma 5.46 there is $s \in S$ such that

$$g(x + \pi) = g(x) + \pi g'(x) + \pi^2 s.$$

Since l/k is separable, we have $\overline{g}'(\overline{x}) \neq 0$, so $w(\pi g'(x)) = 1$ and thus $w(g(x+\pi)) = 1$. Thus $x + \pi$ is an acceptable choice of x.
Step 3: Choose x as in Step 2 and put $\pi \coloneqq g(x)$. By Step 1, the elements $\{x^i g(x)^j\}_{0 \leq i < f,\ 0 \leq j < e}$ span S over R. Thus $S = R[x]$. □

THEOREM 5.48. *Let A be a Dedekind domain with fraction field K, let L/K be a degree n separable field extension, let B be the integral closure of A in L. Let $\alpha \in B$ be such that $L = K[\alpha]$, let $f \in A[t]$ be the minimal polynomial of α, and put*

$$\mathcal{O} \coloneqq A[\alpha].$$

Suppose there is $\mathfrak{p} \in \operatorname{MaxSpec} A$ such that f is locally Eisenstein at $\mathfrak{p}$. Then $\mathcal{O}$ is maximal at $\mathfrak{p}$: we have $\mathcal{O}_\mathfrak{p} = B_\mathfrak{p}$, or equvialently that $\mathfrak{p} \nmid \chi_A(B/\mathcal{O})$.

PROOF. We may replace A with $A_\mathfrak{p}$ and therefore assume: A is a DVR with maximal ideal $\mathfrak{p} = (\pi)$, f is Eisenstein at $\mathfrak{p}$ and show that $\mathcal{O} = B$. Assume not: then there is $\xi \in B \setminus \mathcal{O}$ such that $\pi\xi \in \mathcal{O}$. There are $b_0, \ldots, b_{n-1} \in A$, not all divisible by π, such that

$$\pi\xi = b_{n-1}\alpha^{n-1} + \ldots + b_1\alpha + b_0 \in \mathcal{O}.$$

Let $0 \leq j \leq n-1$ be the minimal index such that $b_j \notin \pi A$. Then

$$\eta \coloneqq \xi - \left(\frac{b_0}{\pi} + \frac{b_1}{\pi}\alpha + \ldots + \frac{b_{j-1}}{\pi}\alpha^{j-1}\right)$$

$$= \frac{b_j}{\pi}\alpha^j + \frac{b_{j+1}}{\pi}\alpha^{j+1} + \ldots + \frac{b_{n-1}}{\pi}\alpha^{n-1} \in B.$$

Then for all $0 \leq j \leq n-1$ we have

$$\frac{b_j}{\pi}\alpha^{n-1} + \frac{\alpha^n}{\pi}\left(b_{j+1} + b_{j+2}\alpha + \ldots + b_{n-1}\alpha^{n-j-2}\right) \in B.$$

Because f is Eisenstein at $\mathfrak{p} = (\pi)$, we have that

$$\frac{\alpha^n}{\pi} = -\left(\frac{a_{n-1}}{\pi}\alpha^{n-1} + \ldots + \frac{a_0}{\pi}\right) \in B,$$

and it follows that

$$\frac{b_j}{\pi}\alpha^{n-1} \in B.$$

But we have

$$N_{L/K}(\frac{b_j}{\pi}\alpha^{n-1}) = \frac{b_j^n N_{L/K}(\alpha)^{n-1}}{\pi^n} = \frac{(-1)^n b_j^n a_0^{n-1}}{\pi^n},$$

which does not lie in A because $\pi \nmid b_j$ and $\pi^2 \nmid a_0$, contradicting Corollary 5.12. □

EXERCISE 5.38. *Let $a \in \mathbb{Z}^+$ and let $n \in \mathbb{Z}^+$. Suppose the polynomial $t^n - a \in \mathbb{Q}[t]$ is irreducible. (By* [**Cl-FT**, Thm. 9.21]*, when $4 \nmid n$, this holds if for all primes $p \mid n$ we have $a \notin \mathbb{Q}^{\times p}$: that is, for no prime p dividing n is a a pth power in $\mathbb{Q}$; if $4 \mid n$, if we add the condition that $-4a \notin \mathbb{Q}^{\times 4}$, then $t^n - a$ is irreducible.) Let α be a root of $t^n - a$ in $\mathbb{C}$, and let $K := \mathbb{Q}[\alpha]$.*

a) *Show: $\delta_{\mathbb{Z}[\alpha]/\mathbb{Z}} = (-1)^{\frac{(n+2)(n-1)}{2}} n^n a^{n-1}$. Deduce: for a prime number p, if $p \nmid na$, then $\mathbb{Z}[\alpha]$ is maximal at p and p is unramified in $\mathbb{Z}_K$.*

b) *Show: if $p \nmid na$, then $\mathbb{Z}/p\mathbb{Z}[t]/(t^n - a)$ is an étale $\mathbb{Z}/p\mathbb{Z}$-algebra. Once again deduce: for a prime number p, if $p \nmid na$, then $\mathbb{Z}[\alpha]$ is maximal at p and p is unramified in $\mathbb{Z}_K$.*

c) *Let p be a prime. Suppose $p \mid a$ and $p^2 \nmid a$. Show: $\mathbb{Z}[\alpha]$ is maximal at p.*

d) *Suppose: all $p \mid n$, we have $a \notin \mathbb{Q}^{\times p}$; if $4 \mid n$, also suppose $-4a \notin \mathbb{Q}^{\times 4}$. Suppose moreover that $a \mid n$, a is squarefree, and for all primes p we have $p \mid a \iff p \mid n$. (In other words, a is squarefree and n is obtained from a by multiplying by primes $p \mid a$ and possibly by -1.) Show:*

$$\mathbb{Z}_K = \mathbb{Z}[\alpha].$$

EXERCISE 5.39. *For $n \in \mathbb{Z}^+$, let $\Phi_n(t) \in \mathbb{C}[t]$ be the unique monic separable polynomial whose roots are the primitive nth roots of unity. Then $\Phi_n(t) \in \mathbb{Z}[t]$* [**Cl-FT**, Prop. 9.6] *and Φ_n has degree $\varphi(n)$ (Euler's totient function). As Gauss showed, $\Phi_n(t) \in \mathbb{Q}[t]$ is irreducible* [**Cl-FT**, Thm. 9.8]*. Put*

$$\zeta_n := e^{2\pi i/n},$$

*a root of $\Phi_n(t)$. The **nth cyclotomic field** is*

$$\mathbb{Q}(\zeta_n) \cong \mathbb{Q}[t]/(\Phi_n).$$

An important basic result is that $\mathbb{Z}_{\mathbb{Q}(\zeta_n)} = \mathbb{Z}[\zeta_n]$. In this exercise we will prove this when $n = p^a$ is a prime power; later we will deduce the general case from this. From now on we put

$$\zeta := \zeta_{p^a} = e^{2\pi i/p^a}.$$

a) *Show: there is $N \in \mathbb{Z}^{\geq 0}$ and $\epsilon \in \{\pm 1\}$ such that $\delta_{\mathbb{Z}[\zeta]/\mathbb{Z}} = \epsilon p^N$.*
(Hint: It is equivalent to show that for all primes $\ell \neq p$, the $\mathbb{Z}/\ell\mathbb{Z}$-algebra $\mathbb{Z}/\ell\mathbb{Z}[t]/(\Phi_{p^a})$ is étale. For this, notice that $\Phi_{p^a}(t) \mid t^{p^a} - 1$, while for any $n \in \mathbb{Z}^+$, if K is a field of characteristic not dividing n, then $t^n - 1 \in K[t]$ is a separable polynomial.)

b) *We claim that $\Phi_{p^a}(t+1)$ is Eisenstein at p. To see this:*
   (i) *Show: The image of $\Phi_{p^a}(t) \in \mathbb{Z}/p\mathbb{Z}[t]$ is $t^{\varphi(p^a)}$.*
   (ii) *Show: $\Phi_{p^a}(1) = p$.*

c) *Show: $\mathbb{Z}_{\mathbb{Q}(\zeta)} = \mathbb{Z}[\zeta]$ and (with notation as in part a)) $\delta(\mathbb{Q}(\zeta) = \epsilon p^N$.*

7. The Different

Throughout this section we will maintain the following setup: let A be a Dedekind domain with fraction field K, let L/K be a finite degree **separable** field extension, and let B be the integral closure of A in L.

During the proof of Theorem 5.20 we observed that B^* is an A-lattice in L and

$$B \subseteq B^*.$$

We make the following additional observation:

LEMMA 5.49. *B^* is a fractional B-ideal.*

PROOF. It is enough to check that $BB^* \subseteq B^*$: for then B^* is a B-submodule of L that is finitely generated as an A-module, hence certainly finitely generated as a B-module, and thus it is a fractional B-ideal.

Let $x \in B$ and $y \in B^*$. We need to check that for all $z \in B$, $T_{L/K}(xyz) \in A$. Now $T_{L/K}(xyz) = T_{L/K}((zx)y) \in A$ since $zx \in B$ and $y \in B^*$. □

Since B^* is a fractional B-ideal containing B, when we factor it as $\prod \mathfrak{p}_i^{a_i}$ all the nonzero exponents are negative. Therefore its inverse is a proper B-ideal: we call it the **different of S over R**:

$$\Delta_{B/A} := (B^*)^{-1}.$$

PROPOSITION 5.50. *Let A be a Dedekind domain with fraction field K, let $K \subseteq L \subseteq M$ be a tower of finite degree field extensions, let B be the integral closure of A in L and let C be the integral closure of A in M (C is also the integral closure of B in M). Then we have*

$$\Delta_{C/A} = \Delta_{B/A}\Delta_{C/B}.$$

PROOF. See [**N**, pp. 195-196]. □

PROPOSITION 5.51. *Let $S \subseteq A$ be a multiplicative subset. Then we have*

$$S^{-1}\Delta_{B/A} = \Delta_{S^{-1}B/S^{-1}A}.$$

PROOF. Both inverses and duals are compatible with localization. □

THEOREM 5.52. *We have*

$$\delta_{B/A} = N_{B/A}(\Delta_{B/A}).$$

PROOF. Using Corollary 4.17 and Proposition 5.35, we get

$$\delta_{B/A} = \chi_A(B^*/B) = \chi_A(B/B^*)^{-1} = N(B^*)^{-1} = N((B^*)^{-1}) = N(\Delta_{B/A}).$$ □

LEMMA 5.53. *For a nonzero ideal I of B, we have $I \mid \Delta_{B/A}$ if and only if $Tr_{L/K}(I^{-1}) \subseteq A$.*

PROOF. We have $I \mid \Delta_{B/A}$ if and only if $I \supseteq \Delta_{B/A}$ if and only if $I^{-1} \subseteq B^*$. if and only if $\mathrm{Tr}_{L/K}(I^{-1}) = \mathrm{Tr}_{L/K}(I^{-1}B) \subseteq A$. □

THEOREM 5.54 (Dedekind's Different Theorem). *Let $\mathcal{P} \in \mathrm{MaxSpec}\, B$ lie over $\mathfrak{p} \in \mathrm{MaxSpec}\, A$. Let $e = e(\mathcal{P}|\mathfrak{p})$. Then:*

a) *If $e \notin \mathfrak{p}$ and $(B/\mathcal{P})/(A/\mathfrak{p})$ is separable, then $\mathrm{ord}_{\mathcal{P}}(\Delta_{B/A}) = e - 1$.*
b) *If $e \in \mathfrak{p}$ or $(B/\mathcal{P})/(A/\mathfrak{p})$ is inseparable, then $\mathrm{ord}_{\mathcal{P}}(\Delta_{B/A}) \geq e$.*

PROOF. We may localize and thus assume that A is a DVR. Write $\mathfrak{p} = (p)$. We observe that to establish a) and b) it suffices to show:

$$\mathcal{P}^{e-1} \mid \Delta_{B/A} \tag{19}$$

and

$$\mathcal{P}^{e} \mid \Delta_{B/A} \iff e \in \mathfrak{p} \text{ or } (B/(\mathcal{P}))/(A/\mathfrak{p}) \text{ is inseparable.} \tag{20}$$

Step 1: We will show (19). For this, write

$$\mathfrak{p}B = \mathcal{P}^{e-1}\mathfrak{a}.$$

Since by definition $e = \mathrm{ord}_{\mathcal{P}}(\mathfrak{p}B)$, we still have $\mathcal{P} \mid \mathfrak{a}$. By Lemma 5.53 it suffices to show that $\mathrm{Tr}_{L/K}(\mathcal{P}^{-(e-1)}) \subseteq A$. Since

$$\mathcal{P}^{-(e-1)} = \frac{1}{p}\mathfrak{a},$$

we have $\mathrm{Tr}_{L/K}(\mathcal{P}^{-(e-1)}) \subseteq A$ if and only if

$$\mathrm{Tr}_{L/K}(\mathfrak{a}) \subseteq pA.$$

Let $\alpha \in \mathfrak{a}$. Then $\mathrm{Tr}_{L/K}(\alpha) = \mathrm{Tr}_{B/A}(\alpha)$ and

$$\mathrm{Tr}_{B/A}(\alpha) \pmod{(p)} = \mathrm{Tr}_{(B/pB)/A/(p)}(\overline{\alpha}).$$

Since $\mathfrak{p}B = pB$ and $\mathfrak{a}$ are divisible by the same prime ideals of B, they have the same radical: $\mathrm{rad}(pB) = \mathrm{rad}(\mathfrak{a})$. It follows that there is $N \in \mathbb{Z}^+$ such that $\alpha^N \in pB$, so $\overline{\alpha}$ is a nilpotent element of B/pB, so its trace is 0.

Step 2: We will show (20). Write $\mathfrak{p} = \mathcal{P}^e\mathfrak{b}$, so $\mathcal{P} \nmid \mathfrak{b}$. As above, we have that $\mathcal{P}^e \mid \Delta_{B/A}$ if and only if $\mathrm{Tr}(\mathfrak{b}) \subseteq pA$ if and only if:

$$\forall \beta \in \mathfrak{b},\ \mathrm{Tr}_{(B/pB)/A/pA}(\overline{\beta}) = 0.$$

In what follows, all our traces will have bottom ring the field A/pA, so if X is a finite-dimensional commutative A/pA-algebra and $x \in X$, we will simplify the notation by writing $T_X(x)$ instead of $\mathrm{Tr}_{X/(A/pA)}(x)$.

Since the ideals $\mathcal{P}^e$ and $\mathfrak{b}$ are coprime, the Chinese Remainder Theorem gives $B/pB \cong B/\mathcal{P}^e \times B/\mathfrak{b}$ and thus for all $x = (x_1, x_2) \in B/pB = B/\mathcal{P}^e \times B/\mathfrak{b}$ we have

$$T_{B/pB}(x) = T_{B/\mathcal{P}^e}(x_1) + T_{B/\mathfrak{b}}(x_2).$$

Of course if $x \in \mathfrak{b}$ and we write $\overline{x} = (x_1, x_2)$, then $x_2 = 0$. It follows that for all $x \in \mathfrak{b}$ we have

$$T_{B/pB}(\overline{x}) = T_{B/\mathcal{P}^e}(x_1) = T_{B/\mathcal{P}^e}(\overline{x}).$$

Moreover, for all $y \in B$, there is $x \in B$ such that $\begin{cases} x \equiv y \pmod{\mathcal{P}^e} \\ x \equiv 0 \pmod{\mathfrak{b}} \end{cases}$, so

$$T_{B/\mathcal{P}^e}(\overline{y}) = T_{B/\mathcal{P}^e}(\overline{x}) = T_{B/pB}(\overline{x}).$$

Thus we conclude that

$$T_{B/\pi}(\mathfrak{b}) = 0 \iff T_{B/\mathcal{P}^e}(B/\mathcal{P}^e) = 0.$$

Now $B/\mathcal{P}^e$ is a local principal Artinian $A/\mathfrak{p}$-algebra, so by Exercise 5.26 its trace map is identically 0 if and only if the residue extension $(B/\mathcal{P})/(A/\mathfrak{p})$ is inseparable or e is divisible by the characteristic of $A/\mathfrak{p}$; the latter holds if and only if $e \in \mathfrak{p}$. □

COROLLARY 5.55. *Let $\mathcal{P} \in \mathrm{MaxSpec}\, B$ lie over $\mathfrak{p} \in \mathrm{MaxSpec}\, A$. Then:*

a) *We have that $\mathcal{P}$ ramifies if and only if $\mathcal{P} \mid \Delta_{B/A}$.*
b) *We have that $\mathfrak{p}$ ramifies if and only if $\mathfrak{p} \mid \delta_{B/A}$.*

PROOF. Part a) follows from Dedekind's Different Theorem. As for part b), because $N_{B/A}(\Delta_{B/A}) = \delta_{B/A}$, the primes of A that divide $\delta_{B/A}$ are precisely the primes $\mathfrak{p}$ that lie under a prime $\mathcal{P}$ of B that divides $\Delta_{B/A}$, which by part a) are precisely the primes of A lying under ramified primes of B, which are (by definition!) precisely the ramified primes of A. □

REMARK 5.56. *The argument that a) $\implies$ b) in Corollary 5.55 can be reversed to show that b) $\implies$ a) if we moreover assume that $\mathcal{P}$ is the only prime of B that lies over A. This does not seem like an especially helpful remark, but actually it is: in Number Theory II one introduces completions, and then it is easy to check that just as the different is compatible with localization, it is also compatible with completion, so one can assume that A is a* ***complete*** *DVR. This forces B to also be a (complete) DVR: i.e., there is only one prime lying over $\mathfrak{p}$. This is the way Sutherland proves Corollary 5.55 in his notes.*

COROLLARY 5.57. *Let A be a Dedekind domain with fraction field K, let L/K be a degree n separable field extension, and let B be the integral closure of A in L. Let $\mathfrak{p} \in \operatorname{MaxSpec} A$, and write*

$$\mathfrak{p}B = \mathcal{P}_1^{e_1} \cdots \mathcal{P}_r^{e_r}, \ f_i = f(\mathcal{P}_i|p).$$

Then:

a) *We have*

$$v_p(\delta_K) \geq n - \sum_{i=1}^{g} f_i. \tag{21}$$

b) *Equality holds in (21) if and only if $\mathfrak{p} \nmid e_1 \cdots e_r$ and each residue extension $(B/\mathcal{P}_i)/(A/\mathfrak{p})$ is separable.*

PROOF. By Theorem 5.54, we have $\mathcal{P}_1^{e_1-1} \cdots \mathcal{P}_r^{e_r-1} \mid \Delta_K$. The discriminant is the norm of the different, so we find that $\delta_{B/A}$ is divisible by

$$\mathfrak{p}^{f_1(e_1-1)+\ldots f_r(e_r-1)} = p^{\sum_{i=1}^r e_i f_i - \sum_{i=1}^r f_i} = \mathfrak{p}^{n-\sum_{i=1}^r f_i}.$$

Moreover, according to Theorem 5.54, we get no further p-divisibility if and only if no ramification index is divisible by $\mathfrak{p}$ and every residual extension is separable. □

Dedekind's Different Theorem is a very useful tool in computational number theory. Here is an example due to K. Conrad:

EXAMPLE 5.58. *Let $K = \mathbb{Q}(\sqrt[3]{2})$. There is an obvious $\mathbb{Z}$-order in K, namely $\mathcal{O} = \mathbb{Z}(\sqrt[3]{2})$. We will show that $\mathcal{O} = \mathbb{Z}_K$. Since $\mathcal{O} \cong \mathbb{Z}[t]/(t^3 - 2)$, the dicriminant of $\mathcal{O}$ is $\operatorname{Res}(f, f') = -108 = -4 \cdot 27$. We will show that $|\delta_{\mathbb{Z}_K}| = 108$: then $\mathcal{O} = \mathbb{Z}_K$.*

Since $\delta_{\mathbb{Z}_K} \mid 108$, the only primes that could ramifiy in K are 2 and 3. In fact 2 and 3 are each totally ramified in K:

$$(2) = (\sqrt[3]{2})^3.$$

To see that 3 is totally ramified, put

$$\alpha := \sqrt[3]{2} + 1, \ u := \sqrt[3]{4} + \sqrt[3]{2} + 1.$$

Since $u(\sqrt[3]{2} - 1) = 1$, $u \in \mathcal{O}^\times$. Moreover

$$\alpha^3 = 3(\alpha^2 - \alpha + 1) = 3(\sqrt[3]{4} + \sqrt[3]{2} + 1),$$

so $(\alpha)^3 = 3$. By Dedekind's Different Theorem, the unique prime of K lying over 2 contributes a factor of 2^2 to δ_K and the unique prime of K lying over 3 contributes at least a factor of 3^3 to δ_K, so δ_K is divisible by 108.

EXERCISE 5.40. *Let K be a field, let $f \in K[t]$ be a monic separable polynomial, with roots $\alpha_1, \ldots, \alpha_n$ in an algebraic closure of K.*

a) *Show:* $\sum_{i=1}^n \frac{1}{f'(\alpha_i)} = \frac{f(t)}{t-\alpha_i} = 1$.
(Suggestion: The left hand side is a polynomial of degree at most n. Show that it evaluates to 1 at α_i for $1 \leq i \leq n$.)

b) *Similarly, show: for all $0 \leq k \leq n-1$, we have*

$$\sum_{i=1}^n \frac{\alpha_i^k}{f'(\alpha_i)} \frac{f(t)}{t-\alpha_i} = t^k. \tag{22}$$

c) *Write*

$$f(t) = (t-\alpha)(c_{n-1}(\alpha)t^{n-1} + \ldots + c_1(\alpha)t + c_0(\alpha)) \in \overline{K}[t].$$

Show: for all $0 \leq i, j \leq n-1$ we have

$$\sum_{i=1}^n \frac{\alpha_i^k}{f'(\alpha_i)} c_j(\alpha_i) = \delta_{j,k}.$$

(Suggestion: equate the coefficients of t^j in the LHS and RHS of (22).)

THEOREM 5.59. *Let R be a Dedekind domain with fraction field K, and let $L = K(\alpha)$ be a finite degree separable field extension. Let $f \in K[t]$ be the minimal polynomial of α. Write*

$$f = (t-\alpha)(c_{n-1}(\alpha)t^{n-1} + \ldots + c_1(\alpha)t + c_0(\alpha)) \in L[t].$$

a) *The dual basis to the basis $(1, \ldots, \alpha^{n-1})$ of L is $(\frac{c_0(\alpha)}{f'(\alpha)}, \frac{c_1(\alpha)}{f'(\alpha)}, \ldots, \frac{c_{n-1}(\alpha)}{f'(\alpha)})$.*

b) *Suppose α is integral over R and put $\Lambda \coloneqq A[\alpha]$. Then*

$$\Lambda^* = \frac{1}{f'(\alpha)}\Lambda.$$

PROOF. Step 1: Write $f(t) = a_n t^n + \ldots + a_{n-1}t + a_0 \in K[t]$; we have $a_n = 1$. Then

$$\frac{f(t)}{t-\alpha} = \frac{f(t)-f(\alpha)}{t-\alpha} = \sum_{i=1}^n \frac{t^i - \alpha^i}{t-\alpha}$$

$$= \sum_{i=1}^n \sum_{j=0}^{n-1} a_i \alpha^{i-1-j} t^j$$

$$= \sum_{j=0}^{n-1} \left(\sum_{i=j+1}^n a_i \alpha^{i-1-j} \right) t^j.$$

It follows that

$$c_j(\alpha) = \sum_{i=j+1}^n a_i \alpha^{i-1-j}$$

and in particular that $c_j(\alpha)$ is a polynomial in α with coefficients in K.
Step 2: Let the roots of αin an algebraic closure of F be $\alpha_1 = \alpha, \alpha_2, \ldots, \alpha_n$. By Exercise 5.40, for $0 \leq j, k \leq n-1$ we have

$$Tr_{L/K}(\frac{\alpha^k c_j(\alpha)}{f'(\alpha)} = \sum_{i=1}^n \frac{\alpha_i^k}{f'(\alpha_i)} c_j(\alpha_i) = \delta_{j,k},$$

so the dual basis to $(1, \alpha, \ldots, \alpha^{n-1})$ is $(\frac{c_0(\alpha)}{f'(\alpha)}, \frac{c_1(\alpha)}{f'(\alpha)}, \ldots, \frac{c_{n-1}(\alpha)}{f'(\alpha)})$.
Step 3: Suppose that α is integral over A, so the coefficients a_i of the minimal

polynomial f lie in R. Using the fact that $a_n = 1$, our formula for $c_j(\alpha)$ gives a system of equations

$$c_{n-1}(\alpha) = 1,$$
$$c_{n-2}(\alpha) = a_{n-1} + \alpha,$$
$$c_{n-3}(\alpha) = a_{n-2} + a_{n-1}\alpha + \alpha^2,$$
$$\vdots$$
$$c_1(\alpha) = a_2 + a_3\alpha + \ldots + a_{n-2}\alpha^{n-2},$$
$$c_0(\alpha) = a_1 + a_2\alpha + \ldots + \alpha^{n-1}.$$

The equations imply that each $c_i(\alpha)$ lies in $A[\alpha]$, the A-submodule of L spanned by the powers of α. But their particular form implies that each power of α lies in $\langle c_0(\alpha), \ldots, c_{n-1}(\alpha)\rangle_A$. So

$$\Lambda^* = \frac{1}{f'(\alpha)}\langle c_0(\alpha), \ldots, c_{n-1}(\alpha)\rangle_A = \frac{1}{f'(\alpha)}\langle 1, \alpha, \ldots, \alpha^{n-1}\rangle_A = \frac{1}{f'(\alpha)}\Lambda. \qquad \square$$

COROLLARY 5.60. *Let A be a Dedekind domain with fraction field K, let L/K be a finite degree separable field extension, let B be the integral closure of A in L, and let $\alpha \in B$ be such that $L = K(\alpha)$, and let $f \in A[t]$ be the minimal polynomial of α. Let $\delta \coloneqq \delta_{A[\alpha]/A}$, a nonzero principal ideal of A. Then we have*

$$\delta = (N_{L/K}(f'(\alpha))). \tag{23}$$

EXERCISE 5.41. *Prove Corollary 5.60.*
(Suggestion: combine Theorem 5.59b), Proposition 4.6 and Proposition 5.38.)

The different ideal can be computed by passing to the completion of A at each $\mathfrak{p} \in \operatorname{MaxSpec} A$. In Number Theory II we will see that if $(A, \mathfrak{p})$ is a complete DVR with fraction field K, L/K is a finite degree separable extension, B is the integral closure of A in L, then B is a complete DVR with maximal ideal $\mathcal{P}$, say. Then if the residual extension $(B/\mathcal{P})/(A/\mathfrak{p})$ is separable then B is monogenic as an A-algebra. Thus Theorem 5.59 can in principle always be used to compute the different of an extension B/A so long as the residue fields of A are perfect.

EXERCISE 5.42. *Let A be a domain, let $f \in A[t]$ be a monic polynomial, and let $B \coloneqq A[t]/(f)$. Let $\Omega_{B/A}$ be the module of Kähler differentials (see* [**Cl-FT**, §13.2]*): this is a B-module equipped with a* universal *A-derivation $d : B \to \Omega_{B/A}$.*

a) *Show: the map $1 \mapsto dt$ induces a B-module isomorphism*

$$B/(f'(t))B \xrightarrow{\sim} \Omega_{B/A}.$$

b) *Suppose that A and B are Dedekind domains. Show:*

$$\operatorname{ann} \Omega_{B/A} = \Delta_{B/A}. \tag{24}$$

In fact (24) holds whenever A is a Dedekind domain with fraction field K and B is its integral closure in a finite degree separable field extension [**N**, Prop. III.2.7]. This provides a hint as to why the different ideal $\Delta_{B/A}$ appears when one studies ramification of coverings of algebraic curves.

8. Prime Decomposition in a Galois Extension

8.1. Invariants under a Galois Extension. Let A be an integrally closed Noetherian domain with fraction field K, let L/K be a separable field extension of finite degree N, and let B be the integral closure of A in L. By Theorem 5.20, B is an integrally closed Noetherian domain that is finitely generated as an A-module, and moreover $\dim B = \dim A$.

Now we suppose that L/K is Galois, and let $G = \mathrm{Aut}(L/K)$ be its Galois group. For a subring B of L, we put

$$B^G := \{x \in B \mid \forall \sigma \in G,\ \sigma(x) = x\}.$$

Notice that if $B = L$, then by basic Galois theory we have $L^G = K$.

PROPOSITION 5.61. *Let A be an integrally closed domain with fraction field K, let L/K be a finite Galois field extension with $\mathrm{Aut}(L/K) = G$. Then $B^G = A$.*

PROOF. It is clear that $A = A^G \subseteq B^G \subseteq L^G = K$. Since B/A is an integral extension, also B^G/A is integral. So if $x \in B^G$ then x is an element of K that is integral over A, hence $x \in A$ since A is integrally closed. □

EXERCISE 5.43. *Let B be a domain, and let G be a finite group acting effectively on B by ring automorphisms. Let K be the fraction field of B^G, and let L be the fraction field of B.*

a) *Show that the action of G on B extends uniquely to an action of G on L. Show also that L/K is a finite Galois extension with $\mathrm{Aut}(L/K) = G$.*
b) *Show that there is a unique extension of the G-action to the rational function field $L(t)$ such that each element of G fixes t. Show also that $L(t)/K(t)$ is a finite Galois extension with $\mathrm{Aut}(L(t)/K(t)) = G$.*
c) *For $x \in B$, consider the polynomial $\Phi_x := \prod_{\sigma \in G}(t - \sigma x)$. Show that*

$$\Phi_x = N_{L(t)/K(t)}(t - x),$$

so

$$\Phi_x \in (B[t])^G = B^G[t].$$

Deduce that B/B^G is an integral extension.
d) *Show: if B is integrally closed, so is B^G.*

PROPOSITION 5.62. *Let G be a finite group acting effectively by automorphisms on a ring B, with invariant ring B^G. Let $\iota : B^G \hookrightarrow B$.*

a) *If $\mathcal{P} \in \mathrm{Spec}\, B$ and $\sigma \in G$, then $\sigma(\mathcal{P}) := \{\sigma(x) \mid x \in \mathcal{P}\}$ is a prime ideal of R. Moreover if $\mathfrak{p} := \iota^*(\mathcal{P}) = \mathcal{P} \cap B^G$, then also $\iota^*(\sigma(\mathcal{P})) = \mathfrak{p}$.*
   That is: G acts on $\mathrm{Spec}\, B$ and this action stabilizes each fiber of the map $\iota^* : \mathrm{Spec}\, B \to \mathrm{Spec}\, B^G$.
b) *Let $\mathfrak{p} \in \mathrm{Spec}\, B^G$. Then the G-action on the fiber $(\iota^*)^{-1}(\mathfrak{p})$ is transitive.*

PROOF. a) We leave this as an exercise.
b) Let $\mathcal{P}_1$ and $\mathcal{P}_2$ be two prime ideals of B lying over the prime ideal $\mathfrak{p}$ of B^G. For $x \in B$, we put $N_G(x) := \prod_{\sigma \in G} \sigma(x) \in B^G$. If $x \in \mathcal{P}_1$, then

$$N_G(x) \in \mathcal{P}_1 \cap B^G = \mathfrak{p} \subseteq \mathcal{P}_2.$$

Since $\mathcal{P}_2$ is a prime ideal containing $N_G(x)$, there is at least one $\sigma \in G$ such that $\sigma(x) \in \mathcal{P}_2$, so it follows that

$$\mathcal{P}_1 \subseteq \bigcup_{\sigma \in G} \sigma(\mathcal{P}_2).$$

By part a) and Prime Avoidance (Lemma 2.6) it follows that there is $\sigma \in G$ such that $\mathcal{P}_1 \subseteq \sigma(\mathcal{P}_2)$. Since B/B^G is integral, there are no proper containments of prime ideals of B lying over the same prime ideal of B^G [**CA**, Cor. 14.15], so $\mathcal{P}_1 = \sigma(\mathcal{P}_2)$. □

EXERCISE 5.44. *Prove Proposition 5.62a).*

8.2. Galois Symmetry. We now intersect with our standard setup: suppose that A is a Dedekind domain with fraction field K, that L/K is a *Galois* extension of finite degree n, with $G = \mathrm{Aut}(L/K)$, and B is the integral closure of A in L. Then all of the previous results apply: in particular, for any $\mathfrak{p} \in \mathrm{MaxSpec}\, A$, the Galois group G acts transitively on the set of primes of B lying over $\mathfrak{p}$.

The presence of this transitive group action both simplifies and deepens our discussion of how prime ideals of A decompose in B. Indeed, let $\mathcal{P}_1$ and $\mathcal{P}_2$ be two maximal ideals of B lying over the same maximal ideal $\mathfrak{p}$ of A. By Proposition 5.62 there is $\sigma \in G$ such that $\sigma(\mathcal{P}_1) = \mathcal{P}_2$. Then σ induces a field isomorphism

$$\sigma : B/\mathcal{P}_1 \xrightarrow{\sim} \sigma(B)/\sigma(\mathcal{P}_1) = B/\mathcal{P}_2.$$

In fact, because G acts trivially on A, this is not just a field isomorphism but an $A/\mathfrak{p}$-algebra isomorphism. It follows that

$$f(\mathcal{P}_1|\mathfrak{p}) = [B/\mathcal{P}_1 : A/\mathfrak{p}] = [B/\mathcal{P}_2 : A/\mathfrak{p}] = f(\mathcal{P}_2|\mathfrak{p}).$$

The Galois group G also acts on $\mathrm{Frac}\, B$. The following result analyzes this action.

PROPOSITION 5.63. *Let A be a Dedekind domain with fraction field K, let L/K be a finite Galois extension with $G \coloneqq \mathrm{Aut}(L/K)$, and let B be the integral closure of A in L. For $I \in \mathrm{Frac}\, B$, consider the following three conditions:*

(i) *There is a fractional ideal $\mathfrak{a}$ of A such that $\mathfrak{a}B = I$.*
(ii) *For all $\sigma \in G$ we have $\sigma(I) = I$.*
(iii) *For all $\mathfrak{p} \in \mathrm{MaxSpec}\, A$, if $\mathcal{P}_1, \mathcal{P}_2 \in \mathrm{MaxSpec}\, B$ both lie over $\mathfrak{p}$, then $v_{\mathcal{P}_1}(I) = v_{\mathcal{P}_2}(I)$.*

Then: (i) $\implies$ (ii) $\iff$ (iii).

PROOF. (i) $\implies$ (ii): If $\mathfrak{a}B = I$, then I is the B-module generated by the subset $\mathfrak{a}$, so for all $\sigma \in G$, $\sigma(I)$ is the B-module generated by the subset $\sigma(\mathfrak{a})$. But since $\mathfrak{a} \subseteq K$ we have $\sigma(\mathfrak{a}) = \mathfrak{a}$, so $\sigma(I) = I$.
(ii) $\iff$ (iii): We have

$$I = \prod_{\mathfrak{p} \in \mathrm{MaxSpec}\, A} \prod_{\mathcal{P}|\mathfrak{p}} \mathcal{P}^{v_{\mathcal{P}}(I)}.$$

For $\mathfrak{p} \in \mathrm{MaxSpec}\, A$, since G permutes $\{\mathcal{P} \mid \mathfrak{p}\}$, if I has the same valuation at every such $\mathcal{P}$, then $\sigma(I) = I$. Conversely, since the action on $\{\mathcal{P} \mid \mathfrak{p}\}$ is transitive, if there were $\mathcal{P}_1$ and $\mathcal{P}_2$ both lying over $\mathfrak{p}$ such that $v_{\mathcal{P}_1}(I) \neq v_{\mathcal{P}_2}(I)$, then there is $\sigma \in G$ such that $\sigma(\mathcal{P}_1) = \mathcal{P}_2$, and then

$$v_{\mathcal{P}_2}(\sigma(I)) = v_{\mathcal{P}_1}(I) \neq v_{\mathcal{P}_2}(I),$$

so $\sigma(I) \neq I$. □

Condition (i) is indeed generally stronger than the other two conditions: indeed, suppose $\mathfrak{p} \in \operatorname{MaxSpec} A$ is totally ramified in B: $\mathfrak{p}A = \mathcal{P}^e$ is a prime power with $e \geq 2$. Then $\mathcal{P} = \mathcal{P}^G$ but $\mathcal{P}$ is not pushed forward from A.

From Proposition 5.63 we deduce: if $\mathcal{P}_1, \mathcal{P}_2 \in \operatorname{MaxSpec} B$ both lie over $\mathfrak{p} \in \operatorname{MaxSpec} A$, then

$$e(\mathcal{P}_1|\mathfrak{p}) = e(\mathcal{P}_2|\mathfrak{p}).$$

Indeed, condition (i) applies to $\mathfrak{p}B$, and hence so does condition (iii).

EXERCISE 5.45. *With notation as above, let $J \in \operatorname{Frac} B$.*

a) *Show: there is a unique $I \in \operatorname{Frac} A$ such that $\iota_*(I) = \prod_{\sigma \in G} \sigma(J)$.*

b) *Show that $I = N(J)$, i.e., I is the ideal norm of J. Thus we have:*

$$\prod_{\sigma \in G} \sigma(J) = N(J)B. \tag{25}$$

COROLLARY 5.64. *With notation as above, let $\mathfrak{p} \in \operatorname{MaxSpec} A$, and let $\mathcal{P}_1, \ldots, \mathcal{P}_g$ be the primess of B lying over $\mathfrak{p}$. Then we may write $e_{\mathfrak{p}}$ for the common value $e(\mathcal{P}_i|\mathfrak{p})$ for all i and $f_{\mathfrak{p}}$ for the common value $f(\mathcal{P}_i|\mathfrak{p})$ for all i, and then we have*

$$\mathfrak{p}B = (\mathcal{P}_1 \cdots \mathcal{P}_r)^e_{\mathfrak{p}}$$

and

$$e_{\mathfrak{p}} f_{\mathfrak{p}} g = [L : K].$$

EXERCISE 5.46. *Let $I \in \operatorname{Frac} B$. As explained above, condition (iii) of Proposition 5.63 is not enough to ensure that $I = \mathfrak{a}B$ for some $\mathfrak{a} \in \operatorname{Frac} A$. However, there is a similar, but stronger, condition that is necessary and sufficient to ensure that $I = \mathfrak{a}B$. Find it and prove it. (Hint: use the ramification indices $e_{\mathfrak{p}}$.)*

EXERCISE 5.47. *Suppose L/K is a quadratic Galois with $\operatorname{Aut}(L/K) = \langle \sigma \rangle$, and let $J \in \operatorname{Frac} B$ be such that $\sigma(J) = J$. Show: there is $I \in \operatorname{Frac} A$ and a subset $\mathcal{S}$ of ramified primes of B – that is, for all $\mathcal{P} \in \mathcal{S}$, we have $e_{\mathcal{P} \cap A} = 2$ – such that*

$$J = IB \cdot \prod_{\mathcal{P} \in \mathcal{S}} \mathcal{P}.$$

8.3. Decomposition and Inertia Groups and Fields. We maintain our running assumptions:we have a Dedekind domain A with fraction field K, a degree n Galois extension L/K with $G = \operatorname{Aut}(L/K)$, and B is the integral closure of A in L.

Let $\mathfrak{p} \in \operatorname{MaxSpec} A$, and let $\mathcal{P} \in \operatorname{MaxSpec} B$ lie over $\mathfrak{p}$. We define the **decomposition group**

$$D(\mathcal{P}|\mathfrak{p}) \coloneqq \{\sigma \in L \mid \sigma(\mathcal{P}) = \mathcal{P}\}.$$

As we know, G acts transitively on the fiber $\{\mathcal{P} \mid \mathfrak{p}\}$. Recall that whenever a group G acts on a set X, if $x \in X$ and $g \in G$, if Stab_x is the stabilizer of x, then we have

$$\operatorname{Stab}_{gx} = g \operatorname{Stab}_x g^{-1}.$$

In particular, if G acts transitively on X then the various point stabilizers precisely yield a full, single conjugacy class of subgroups.

So this happens here: when we switch from one prime lying over $\mathfrak{p}$ to a different prime lying over $\mathfrak{p}$, the decomposition group changes to a conjugate subgroup, and

all conjugates of any one decomposition group do arise this way. The most favorable case is that in which the extension L/K is **abelian** – i.e., G is commutative. Then conjugation is trivial, so the decomposition group depends only on the downstairs prime $\mathfrak{p}$, and in this case will be denoted by $D(\mathfrak{p})$.

It follows from Corollary 5.64 and the Orbit-Stabilizer Theorem that

$$\#D(\mathcal{P}|\mathfrak{p}) = e_{\mathfrak{p}} f_{\mathfrak{p}}.$$

To ease the notation in what follows, let us write

$$k(\mathfrak{p}) \coloneqq A/\mathfrak{p}$$

for the residue field at $\mathfrak{p}$ and

$$l(\mathcal{P}) \coloneqq B/\mathcal{P}$$

for the residue field at $\mathcal{P}$. Thus $l(\mathcal{P})/k(\mathfrak{p})$ is a field extension of finite degree $f(\mathcal{P}|\mathfrak{p})$.

Using the decomposition group $D \coloneqq D(\mathcal{P}|\mathfrak{p})$, we can break up L/K into the tower of fields $L/L^{D(\mathcal{P}|\mathfrak{p})}/K$. Let A_D be the integral closure of A in L^D. Let $\mathfrak{p}_D \coloneqq \mathcal{P} \cap A_D$, so $\mathcal{P} \mid \mathfrak{p}_D \mid \mathfrak{p}$. On the one hand, $D = \mathrm{Aut}(L/L^D)$ acts transitively on the set of primes of B lying over $\mathfrak{p}_D$. On the other hand, by definition D acts trivially on the set of primes of B lying over $\mathfrak{p}$, so it certainly acts trivially on the smaller set of primes of B lying over $\mathfrak{p}_D$. Taking these together, we find that $\mathcal{P}$ is the only prime of B lying over $\mathfrak{p}_D$, so $e(\mathcal{P}|\mathfrak{p}_D)f(\mathcal{P}|\mathfrak{p}_D) = \#D = e_{\mathfrak{p}} f_{\mathfrak{p}}$, and thus

$$e(\mathfrak{p}_D|\mathfrak{p}) = f(\mathfrak{p}_D|\mathfrak{p}) = 1.$$

If D is normal in G, then L^D/K is Galois: in this case $\mathfrak{p}$ splits completely in L^D. The general case is a bit more complicated, and it is addressed in our next result.

Exercise 5.48. *With notation as above, let M be a subextension of L/K. Let $\mathcal{P} \in \mathrm{MaxSpec}\, B$ lie over $\mathfrak{p}_M \in \mathrm{MaxSpec}\, A_M$, which lies over $\mathfrak{p} \in \mathrm{MaxSpec}\, A$.*

a) *Show:*
$$D(\mathcal{P}|\mathfrak{p}_M) = D(\mathcal{P}|\mathfrak{p}) \cap \mathrm{Aut}(L/M).$$
b) *Show: $L^{D(\mathcal{P}|\mathfrak{p}_M)} = L^D M$.*

Exercise 5.49. *With notation as above, let M be a subextension of L/K, let A_M be the integral closure of A in M, and let $\mathfrak{p}_M \coloneqq \mathcal{P} \cap M$. Show that the following are equivalent:*

(i) *We have $M \subseteq L^{D(\mathcal{P}|\mathfrak{p})}$.*
(ii) *we have $e(\mathfrak{p}_M/\mathfrak{p}) = f(\mathfrak{p}_M/\mathfrak{p}) = 1$.*

(Hint for (ii) $\implies$ (i): use part b) of the previous Exercise.)

Theorem 5.65. *Let A be a Dedekind domain with fraction field K, let L/K be a finite degree separable field extension, and let B be the integral closure of A in L. Let $\mathfrak{p} \in \mathrm{MaxSpec}\, A$.*

a) *There is a unique subextension L^s of L/K with the following property: for a subextension F of L/K, the prime $\mathfrak{p}$ splits completely in F if and only if $F \subseteq L^s$.*
b) *If L/K is Galois, then so is L^s/K.*

PROOF. a) Let M be the Galois closure of L/K, let B_M be the integral closure of A in M, and suppose that

$$\mathfrak{p}B_N = \mathcal{P}_1^{e_1} \cdots \mathcal{P}_r^{e_r}.$$

If F is a subextension of M/K, let A_F be the integral closure of A in F. For $1 \leq i \leq r$, put $\mathfrak{q}_i := \mathcal{P}_i \cap A_F$. Then $\mathfrak{p}$ splits completely in F if and only if we have $e(\mathfrak{q}_i|\mathfrak{p})f(\mathfrak{q}_i|\mathfrak{p}) = 1$ for all i. By Exercise 5.49, this holds if and only if $F \subseteq \bigcap_{i=1}^r M^{D(\mathcal{P}_i|\mathfrak{p})}$. Thus we may take

$$L^s := L \cap \bigcap_{i=1}^s M^{D(\mathcal{P}_i|\mathfrak{p})}.$$

b) If L/K is Galois, then $M = L$ and $L^s = \bigcap_{i=1}^s L^{D(\mathcal{P}_i|\mathfrak{p})} = L^{\langle D(\mathcal{P}_i|\mathfrak{p})\rangle}$. Since the $D(\mathcal{P}_i|\mathfrak{p})$ form a full conjugacy class of subgroups of $G = \mathrm{Aut}(L/K)$, the subgroup $\langle D(\mathcal{P}_i|\mathfrak{p})\rangle$ is the precisely the least normal subgroup generatated by any one of the decomposition groups $D(\mathcal{P}_i|\mathfrak{p})$. In particular it is normal, so its fixed field L^s is Galois over K. □

THEOREM 5.66. *Let A be a Dedekind domain with fraction field K. Let K^{sep} be a separable closure of K, and let $K_1, \ldots, K_r$ be subextensions of K^{sep}/K, each with finite degree over K, and put*

$$L := K_1 \cdots K_r.$$

For $1 \leq i \leq r$, let A_i be the integral closure of A in K_i and let B be the integral closure of A in L. Let $\mathfrak{p} \in \mathrm{MaxSpec}\, A$ be a prime that splits completely in A_i for all i. Then $\mathfrak{p}$ splits completely in B.

PROOF. Let L^s be the subextension of L/K given by Corollary 5.66. For $1 \leq i \leq r$, since $\mathfrak{p}$ splits in A_i, we have $K_i \subseteq L^s$. Therefore $L = K_1 \cdots K_r$ is also contained in L^s, so $\mathfrak{p}$ splits completely in B. □

COROLLARY 5.67. *Let A be a Dedekind domain with fraction field K, let L/K be a finite degree separable extension, with Galois closure M. For a prime $\mathfrak{p} \in \mathrm{MaxSpec}\, A$, the following are equivalent:*

(i) *$\mathfrak{p}$ splits completely in L.*
(ii) *$\mathfrak{p}$ splits completely in M.*

PROOF. (i) $\implies$ (ii): The Galois closure M of L/K is the compositum of the finitely many distinct fields $\sigma(L)$ as σ runs through embeddings of L into an algebraic (or, if you like, separable algebraic) closure of K. So Theorem 5.66 applies. (ii) $\implies$ (i): This is immediate from the multiplicativity of ramification degrees and inertial indices in towers. □

Next we turn to a naturally defined "reduction" homomorphism

$$\mathfrak{r} : D(\mathcal{P}|\mathfrak{p}) \to \mathrm{Aut}(l(\mathcal{P})/k(\mathfrak{p})) :$$

indeed, for $\sigma \in D(\mathcal{P}|\mathfrak{p})$, we have $\sigma(\mathcal{P}) = P$ and thus σ induces an automorphism

$$\mathfrak{r}(\sigma) : B/\mathcal{P} \to \sigma(B)/\sigma(\mathcal{P}) = B/\mathcal{P}.$$

Let us give a name to the kernel of this homomorphism: we call this the **inertia group** $I(\mathcal{P}|\mathfrak{p})$. That is:

$$I(\mathcal{P}|\mathfrak{p}) := \{\sigma \in D(\mathcal{P}|\mathfrak{p}) \mid \sigma \text{ acts trivially on } B/\mathcal{P}\}.$$

EXERCISE 5.50. *Show that $I(\mathcal{P}|\mathfrak{p})$ is also the set of $\sigma \in G$ such that for all $x \in B$ we have $\sigma(x) - x \in \mathcal{P}$.*

In order to make progress we want to throw in one more assumption: namely that the residue field $k(\mathfrak{p}) = A/\mathfrak{p}$ is perfect. By definition, this means that every finite extension is separable, so in particular the extension $l(\mathcal{P})/k(\mathfrak{p})$ is separable. Every field of characteristic 0 is perfect, as is every finite field. The latter is the more important observation for us, since classical algebraic number theory takes place in the case $A = \mathbb{Z}$, in which case the residue fields are just $\mathbb{Z}/p\mathbb{Z}$.

THEOREM 5.68. *With notation as above, suppose that for $\mathfrak{p} \in \operatorname{MaxSpec} A$ the residue field $k(\mathfrak{p}) \coloneqq A/\mathfrak{p}$ is perfect. Let $\mathcal{P} \in \operatorname{MaxSpec} B$ lie over $\mathfrak{p}$, and put $l(\mathcal{P}) \coloneqq B/\mathcal{P}$. Then:*

a) *The extension $l(\mathcal{P})/k(\mathfrak{p})$ is finite Galois (of degree $f_{\mathfrak{p}}$).*
b) *The reduction map $\mathfrak{r} : D(\mathcal{P}|\mathfrak{p}) \to \operatorname{Aut}(l(\mathcal{P})/l(\mathfrak{p})$ is surjective.*
c) *We have $\#I(\mathcal{P}|\mathfrak{p}) = \#\operatorname{Ker}\mathfrak{r} = e_{\mathfrak{p}}$.*

PROOF. a) Let us abbreviate $D \coloneqq D(\mathcal{P}|\mathfrak{p})$ and $I \coloneqq I(\mathcal{P}|\mathfrak{p})$. Let A_D be the integral closure of A in L^D, and let $\mathfrak{p}_D \coloneqq \mathcal{P} \cap L^D$. Let's further put

$$e_D \coloneqq e(\mathcal{P}|\mathfrak{p}_D),\ f_D \coloneqq f(\mathcal{P}|\mathfrak{p}_D).$$

As seen above, we have $e(\mathfrak{p}_D|\mathfrak{p}) = f(\mathfrak{p}_D|\mathfrak{p}) = 1$. The latter gives us $A_D/\mathfrak{p}_D = A/\mathfrak{p}$.

Because $l(\mathcal{P})/k(\mathfrak{p})$ is a finite degree separable extension, it has a primitive element: say $l(\mathcal{P}) = k(\mathfrak{p})[\overline{\alpha}]$. Lift $\overline{\alpha}$ to an element $\alpha \in B$, and let $f \in L^D[t]$ be the minimal polynomial for α. Because α is integral over A it is also integral over A_D, so in fact $f \in A_D[t]$. Because L/L^D is Galois, the polynomial f splits in L and every root of f is of the form $\sigma(\alpha)$ for some $\alpha \in D$. Now let $\overline{f}$ be the image of f in $A_D/\mathfrak{p}_D[t] = A/\mathfrak{p}[t]$. It follows that the roots of $\overline{f}$ are all of the form $\mathfrak{r}(\sigma)(\overline{\alpha})$ for some $\sigma \in D$. All of these roots lie in $l(\mathcal{P})$, so $l(\mathcal{P})$ is the splitting field of the polynomial $\overline{f} \in k(\mathfrak{p})$ and therefore is a normal extension of $k(\mathfrak{p})$, hence a Galois extension of $k(\mathfrak{p})$ since we assumed that $k(\mathfrak{p})$ was perfect.
b) Since every conjugate of $\overline{\alpha}$ over $k(\mathfrak{p})$ is of the form $\mathfrak{r}(\sigma)(\overline{\alpha})$, every element of $\operatorname{Aut}(l(\mathcal{P})/k(\mathfrak{p}))$ is of the form $\mathfrak{r}(\sigma)$ for some $\sigma \in D$. Thus $\mathfrak{r}$ is surjective.
c) We know that $\mathfrak{r} : D \to \operatorname{Aut}(l(\mathcal{P})/k(\mathfrak{p})$ is surjective with kernel $I(\mathcal{P}|\mathfrak{p})$, so

$$\#I(\mathcal{P}|\mathfrak{p}) = \frac{\#D}{\#\operatorname{Aut}(l(\mathcal{P})/k(\mathfrak{p}))} = \frac{e_{\mathfrak{p}} f_{\mathfrak{p}}}{f_{\mathfrak{p}}} = e_{\mathfrak{p}}. \qquad \square$$

For L/K a finite Galois extension with $G = \operatorname{Aut}(L/K)$ and $\mathcal{P} \in \operatorname{MaxSpec} B$ lying over $\mathfrak{p} \in \operatorname{MaxSpec} A$, using the inertia group we can refine our filtration of subfields:

$$K \overset{r}{\subseteq} L^{D(\mathcal{P}|\mathfrak{p})} \overset{f}{\subseteq} L^{I(\mathcal{P}|\mathfrak{p})} \overset{e}{\subseteq} L.$$

We have a parallel to much of the above discussion when we replace the decomposition subgroup $D(\mathcal{P}|\mathfrak{p})$ by the inertia subgroup $I(\mathcal{P}|\mathfrak{p})$ and the condition $e(\mathcal{P}|\mathfrak{p})f(\mathcal{P}|\mathfrak{p}) = 1$ with the condition $e(\mathcal{P}|\mathfrak{p}) = 1$. We leave the proofs as exercises.

EXERCISE 5.51. *Let L/K be finite Galois, and let M be a subextension of L/K. Let $\mathcal{P} \in \operatorname{MaxSpec} B$ lie over $\mathfrak{p}_M \in \operatorname{MaxSpec} A_M$, which lies over $\mathfrak{p} \in \operatorname{MaxSpec} A$.*

a *Show:*

$$I(\mathcal{P}|\mathfrak{p}_M) = I(\mathcal{P}|\mathfrak{p}) \cap \operatorname{Aut}(L/M).$$

b) *Show: $L^{I(\mathcal{P}|\mathfrak{p}_M)} = L^{D(\mathcal{P}|\mathfrak{p})}M$.*

EXERCISE 5.52. *Let L/K be finite Galois, let M be a subextension of L/K, let A_M be the integral closure of A in M, and put $\mathfrak{p}_M \coloneqq \mathcal{P} \cap A_M$. Show that the following are equivalent:*

(i) *We have $M \subseteq L^{I(\mathcal{P}|\mathfrak{p})}$.*
(ii) *We have $e(\mathfrak{p}_M|\mathfrak{p}) = 1$.*

COROLLARY 5.69. *Let A be a Dedekind domain with fraction field K, let L/K be a finite degree separable field extension, and let B be the integral closure of A in L. Let $\mathfrak{p} \in \operatorname{MaxSpec} A$.*

(i) *There is a unique subextension L^i of L/K with the following property: for a subextension F of L/K, the prime $\mathfrak{p}$ is unramified in F if and only if $F \subseteq L^i$.*
(ii) *If L/K is Galois, then so is L^i/K.*

EXERCISE 5.53. *Prove Corollary 5.69.*

THEOREM 5.70. *Let A be a Dedekind domain with fraction field K. Let K^{sep} be a separable closure of K, and let $K_1, \ldots, K_r$ be subextensions of K^{sep}/K, each with finite degree over K, and put*

$$L \coloneqq K_1 \cdots K_r.$$

For $1 \leq i \leq r$, let A_i be the integral closure of A in K_i, and let B be the integral closure of A in L. Let $\mathfrak{p} \in \operatorname{MaxSpec} A$ be a prime that is unramified in A_i for all i. Then $\mathfrak{p}$ is unramified in B.

EXERCISE 5.54. *Prove Theorem 5.70.*

COROLLARY 5.71. *Let A be a Dedekind domain with fraction field K, let L/K be a finite degree separable field extension, with Galois closure M. For a prime $\mathfrak{p} \in \operatorname{MaxSpec} A$, the following are equivalent:*

(i) *$\mathfrak{p}$ is unramified in L.*
(ii) *$\mathfrak{p}$ is unramified in M.*

8.4. Frobenius Elements. We maintain the standard setup of this section: suppose A is a Dedekind domain with fraction field K, L/K is a finite Galois extension with $G = \operatorname{Aut}(L/K)$, and B is the integral closure of A in L. To this we now add the hypotheses that for $\mathfrak{p} \in \operatorname{MaxSpec} A$ the residue field $k(\mathfrak{p}) = A/\mathfrak{p}$ is finite, say of cardinality $q = p^a$.

Let $\mathcal{P} \in \operatorname{MaxSpec} B$ lie over A. Our hypothesis gives us a complete description of $D(\mathcal{P}|\mathfrak{p})/I(\mathcal{P}|\mathfrak{p})$. By Theorem 5.68, the reduction map induces an isomorphism from $D(\mathcal{P}|\mathfrak{p})/I(\mathcal{P}|\mathfrak{p})$ to $\operatorname{Aut}(l(\mathcal{P})/k(\mathfrak{p})$, where once again we put $l(\mathcal{P}) = B/\mathcal{P}$. Since $k(\mathfrak{p})$ is finite of cardinality q, $l(\mathcal{P})$ must be finite of cardinality $q^{f_\mathfrak{p}}$, and it follows that $\operatorname{Aut}(l(\mathcal{P})/k(\mathfrak{p}))$ is cyclic of order f.

This already implies some Galois-theoretic restrictions on how primes of A can decompose in B:

EXERCISE 5.55. *Let A be a Dedekind domain with fraction field K, let L/K be a degree n Galois extension with Galois group G, and let $\mathfrak{p} \in \operatorname{MaxSpec} A$.*

a) *Suppose that:*
   (i) *The residue field $k(\mathfrak{p}) \coloneqq A/\mathfrak{p}$ is finite.*

(ii) *The prime $\mathfrak{p}$ is inert in B: i.e., $\mathfrak{p}B$ is a prime ideal of B. Show: G is cyclic.*

b) *Find infinitely many number fields K that are Galois over $\mathbb{Q}$ and such that no prime (p) of $\mathbb{Z}$ is inert in $\mathbb{Z}_K$.*

We continue with the above dicsussion. Beyond being cyclic, $\mathrm{Aut}(l(\mathcal{P})/k(\mathfrak{p})$ has a canonical generator, namely the q-power Frobenius map $F_q : x \mapsto x^q$. We define a **Frobenius element** $\tau_{\mathcal{P}|\mathfrak{p}}$ to be an element of $D(\mathcal{P}|\mathfrak{p})$ that maps under $\mathfrak{r}$ to this canonical generator F_q. In general, $\tau_{\mathcal{P}|\mathfrak{p}}$ is well-defined up to an element of the inertia group $I(\mathcal{P}|\mathfrak{p})$, so when $\mathfrak{p}$ is unramified in B – as we will henceforth assume – we get a uniquely defined Frobenius element $\tau_{\mathcal{P}|\mathfrak{p}}$.

EXERCISE 5.56. *With notation as above, suppose $\mathfrak{p}$ is unramified in L/K, let $\mathcal{P}$ be a prime of B lying over $\mathfrak{p}$, and let $\sigma \in G = \mathrm{Aut}(L/k)$.*

a) *Show:*
$$\tau_{\sigma(\mathcal{P})|\mathfrak{p}} = \sigma\tau_{\mathcal{P}|\mathfrak{p}}\sigma^{-1}.$$

b) *Deduce that the set $\{\tau_{\mathcal{P}|\mathfrak{p}} \mid \mathcal{P}$ lies over $\mathfrak{p}\}$ of Frobenius elements attached to the set of primes of B lying over $\mathfrak{p}$ fill out a full conjugacy class in G.*

EXERCISE 5.57. *Let $n \geq 3$, let $K := \mathbb{Q}$, and let $L := \mathbb{Q}(\zeta_n)$ be the nth cyclotomic field. Then L/K is Galois, with $G = \mathrm{Aut}(L/K)$ canonically isomorphic to $(\mathbb{Z}/n\mathbb{Z})^\times$. Later (Theorem 7.6) we will prove that if p ramifies in $\mathbb{Z}_L$ then $p \mid n$, so for each $p \nmid n$ we have a Frobenius element[6] $\tau_p \in (\mathbb{Z}/n\mathbb{Z})^\times$.*

a) *Show: for $p \nmid n$ we have $\tau_p = p \pmod N$.*

b) *Let c denote complex conjugation, viewed as an element of G. Show: $c = -1 \pmod p$.*

8.5. Supplement on Inseparable Extensions. Some of the above holds when the degree n field extension L/K is normal but not separable. With the lack of separability, we still have that B is a Dedekind domain but it need not be the case that B is finitely generated as an A-module. But the results we discuss here do not require B to be finitely generated as an A-module.

PROPOSITION 5.72. *Suppose that L/K is normal, and put $G = \mathrm{Aut}(L/K)$. Let $\mathfrak{p} \in \mathrm{MaxSpec}\, R$. Then G acts transitively on $\mathrm{MaxSpec}\, S/\mathfrak{p}S$, i.e., on the set of maximal ideals of S lying over $\mathfrak{p}$.*

PROOF. Let p^a be the inseparable degree of L/K, so for $x \in L$,

$$N_{L/K}(x) = \left(\prod_{\sigma \in G} \sigma(x)\right)^{p^a}. \tag{26}$$

Suppose to the contrary that there are maximal ideals $\mathcal{P}_1 \neq \mathcal{P}_2$ lying over $\mathfrak{p}$ such that for all $\sigma \in G$, $\mathcal{P}_2 \neq \sigma\mathcal{P}_1$. By the Chinese Remainder Theorem, there is $x \in S$ such that

$$x \in \mathcal{P}_2,$$
$$\forall \sigma \in G,\ x \equiv 1 \in \sigma(\mathcal{P}_1).$$

Then

$$N_{L/K}(x) = x\left(x^{p^a-1} \cdot \prod_{1 \neq \sigma \in G} \sigma(x)\right) \in \mathcal{P}_2 \cap R = \mathfrak{p}.$$

[6]We get an element rather than a conjugacy class because G is commutative.

On the other hand, for all $\sigma \in G$, $x \notin \sigma\mathcal{P}_1$; equivalently $\sigma^{-1}x \notin \mathcal{P}_1$, and as σ runs through all elements of G so does σ^{-1}, so for all $\sigma \in G$, $\sigma(x) \notin \mathcal{P}_1$. Thus $N_{L/K}(x) \in \mathfrak{p} \subseteq \mathcal{P}_1$ but by (26) is a product of elements none of which are in $\mathcal{P}_1$, contradicting the primality of $\mathcal{P}_1$. □

EXERCISE 5.58. *Let A be an integrally closed domain with fraction field K, let L/K be a degree n* ***purely inseparable*** *field extension, and let B be the integral closure of A in L.*

a) *Deduce from Proposition 5.72 that the natural map* $\operatorname{MaxSpec} B \to \operatorname{MaxSpec} A$ *is a bijection.*

b) *Show directly the following stronger result: let A be a domain with fraction field K, L/K a purely separable algebraic extension (possibly of infinite degree), B the integral closure of A in L, and $\mathfrak{p} \in \operatorname{Spec} A$. Then* $\operatorname{rad}(\mathfrak{p}A)$ *is the unique prime ideal of B lying over $\mathfrak{p}$.*

EXERCISE 5.59. *Suppose that A is a Dedekind domain with fraction field K, that L/K is an* arbitrary *finite degree field extension, and that B is the integral closure of A in L. Show that the natural map* $\operatorname{Spec} B \to \operatorname{Spec} B$ *has finite fibers: for all $\mathfrak{p} \in \operatorname{Spec} A$,* $\operatorname{Spec} B/\mathfrak{p}B$ *is finite. (Suggestion: localize to reduce to the case in which $\mathfrak{p}$ is maximal. Then reduce to the case in which L/K is normal by passing to the normal closure.)*

9. Hensel's Different Theorem

THEOREM 5.73 (Hensel). *Let $\mathcal{P} \in \operatorname{MaxSpec} B$ lie over $\mathfrak{p} \in \operatorname{MaxSpec} A$. We put: $k := A/\mathfrak{p}$, $l := B/\mathcal{P}$, $e := e(\mathcal{P}|\mathfrak{p})$. Suppose that l/k is separable. Then:*

$$v_{\mathcal{P}}(\Delta_{B/A}) \leq e - 1 + v_{\mathcal{P}}(e) \tag{27}$$

Notice that in the hypothesis of Hensel's Theorem, if $\mathcal{P}/\mathfrak{p}$ is tamely ramified then the upper bound is $v_{\mathcal{P}}(\Delta_{B/A}) \leq e-1$. In fact, by Theorem 5.54a) we have equality in this case. Thus the new content of Hensel's Theorem is an upper bound on $v_{\mathcal{P}}(\Delta_{B/A})$ in the presence of wild ramification (and a separable residual extension).

We will give the proof of Theorem 5.73, but our proof will use some results from Number Theory II [**NTII**]. You will probably wish to wait to read this proof until they are familiar with the theory of completions of discretely valued fields.

PROOF. We will use the fact that $\Delta_{B/A}$ can be computed after completion: if $B_{\mathcal{P}}$ is the completion of B with respect to the $\mathcal{P}$-adic valuation and $A_{\mathfrak{p}}$ is the completion of A with respect to the $\mathfrak{p}$-adic valuation, then [**N**, Prop. III.2.2(iii)]

$$\Delta_{B/A} \otimes_B B_{\mathcal{P}} = \Delta_{B_{\mathcal{P}}/A_{\mathfrak{p}}}.$$

To ease the notation, we simply assume that A and B are complete DVRs. By Theorem 5.47, we get that B is monogenic over A: say $B = A[\alpha]$. Let

$$f = t^N + \sum_{i=0}^{n-1} a_i t^i = \sum_{i=0}^{n} a_i t^i \in A[t]$$

be the minimal polynomial of α. By Theorem 5.59 we have

$$s = v_{\mathcal{P}}(f'(\alpha)).$$

Suppose first that L/K is unramified. By Dedekind-Kummer, the polynomial $\overline{f} \in k[t]$ is separable, so $\overline{f}'(\alpha) \neq 0$ and thus $s = v_{\mathcal{P}}(f'(\alpha)) = 0 = e - 1$.[7] By Corollary 5.69 there is a unique maximal unramified subextension L' of L/K. Let B' be the integral closure of A in L', let $\mathcal{P}'$ be the unique prime of B' lying over $\mathfrak{p}$, and let $l' := B'/\mathcal{P}'$. We claim that L/L' is totally ramified over $\mathcal{P}'$. If not, then l/l' is a proper, finite degree separable field extension. As argued in [**NTII**, §2.2] using Hensel's Lemma, this gives an unramified subextension M of L/L' such that $[M : L'] = [l : l'] > 1$, contradicting the fact that L' was the maximal unramified subextension of L/K. Using this and Proposition 5.50 we reduce to the case in which L/K is totally ramified over $\mathfrak{p}$. Then by [**NTII**, Thm. 2.11], if $\alpha = \Pi$ is a uniformizing element for $\mathcal{P}$ then $B = A[\Pi]$ and the minimal polynomial f of α is is *Eisenstein* at $\mathfrak{p}$: we have $a_0 \in \mathfrak{p} \setminus \mathfrak{p}^2$ and $a_i \in \mathfrak{p}$ for all $1 \leq i \leq N-1$. Thus

$$f'(\alpha) = \sum_{i=1}^{e} i a_i \alpha^{i-1}.$$

For $1 \leq i \leq e$ we have

$$v_{\mathcal{P}}(i a_i \alpha^{i-1}) = v_{\mathcal{P}}(i_+ v_{\mathcal{P}}(a_i) + (i-1) v_{\mathcal{P}}(\alpha)$$

$$= e\,(v_{\mathfrak{p}}(i) + v_{\mathfrak{p}}(a_i)) + (i-1) \equiv i - 1 \pmod{e},$$

so all of these valuations are distinct. It follows that

$$s = v_{\mathcal{P}}(f'(\alpha)) = \min_{1 \leq e} v_{\mathcal{P}}(i a_i \alpha^{i-1}) \leq v_{\mathcal{P}}(e \alpha^{e-1}) = e - 1 + v_{\mathcal{P}}(e). \qquad \square$$

10. The Chebotarev Density Theorem

Let k be either $\mathbb{Q}$ or $\mathbb{F}_p(t)$; $\mathfrak{o} = \mathbb{Z}$ or $\mathbb{F}_p[t]$. Let K/k be a finite separable extension and L/K be a finite Galois extension. Let R be the integral closure of $\mathfrak{o}$ in K, S the integral closure of $\mathfrak{o}$ in S. We further write Σ_R (resp. Σ_S) for the set of nonzero prime ideals of R (resp. of S). For brevity, we summarize this situation by saying that S/R is a **Galois extension of global rings**.

Notice that R and S are Dedekind rings with finite quotients, so all of the material of the previous section applies: especially, for any prime $\mathfrak{p}$ in R not dividing $\Delta(S/R)$, we have a Frobenius conjugacy class $\tau_{\mathfrak{p}} \subseteq \mathrm{Gal}(L/K)$.

We also have (just!) one more thing: we have a norm map on the nonzero integral ideals of R, with the property that there are only finitely many ideals of norm less than or equal to any given number.

Let $T \subseteq \Sigma_R$. We say that T **has a natural density** if

$$\lim_{x \to \infty} \frac{\#\{I \in T \mid N(I) \leq x\}}{\#\{I \in \Sigma_R \mid N(I) \leq x\}}$$

exists; if so we define its natural density $\delta(T) \in [0,1]$ to be the above limit.

[7] We knew this already from Theorem 5.54, but this is a different argument from the one given above.

We say that T **has a Dirichlet density** if

$$\lim_{s \to 1^+} \frac{\sum_{\mathfrak{p} \in \mathcal{T}} N(\mathfrak{p})^{-s}}{\sum_{\mathfrak{p} \in \Sigma_R} N(\mathfrak{p})^{-s}}$$

exists; if so we define its Dirichlet density $\delta_D(T) \in [0,1]$ to be the above limit.

EXERCISE 5.60. *Let $T \subseteq \Sigma_R$.*

a) *Show that if T has a natural density, then it has a Dirichlet density and $\delta_D(T) = \delta(T)$.*

b) *Exhibit a T which has a Dirichlet density but no natural density.*

For any group G, a **normal subset** $T \subseteq G$ will be a subset which is invariant under conjugation: for all $\sigma \in G$, $\sigma T \sigma^{-1} = S$.

EXERCISE 5.61. *Show that a subset T of G is normal iff it is a disjoint union of conjugacy classes.*

Notice that if G is abelian, then all subsets are normal.

10.1. The Chebotarev Density Theorem.

THEOREM 5.74. *(Chebotarev, 1922) Let S/R be a Galois extension of global rings, with $G = \mathrm{Gal}(L/K)$. Let $X \subseteq G$ be a normal subset, and consider the* ***Chebotarev set*** *$T_X \subseteq \Sigma_R$ of prime ideals $\mathfrak{p}$ which are unramified in S and such that the Frobenius conjugacy class $\tau_{\mathfrak{p}}$ is contained in X.*

a) *The set T_X has Dirichlet density $\frac{\#X}{\#G}$.*

b) *If $\mathrm{char}\, K = 0$, then T_X has natural density $\frac{\#X}{\#G}$.*

EXERCISE 5.62. *Suppose that you know Chebotarev Density when $T \subseteq G$ is a single conjugacy class. Deduce the general case.*

COROLLARY 5.75. *For any separable extension S/R of global rings with $[L : K] = n$, the density of the set $\mathcal{S}$ of primes $\mathfrak{p}$ of R which split completely in S is $\frac{1}{\#\,\mathrm{Gal}(M/K)}$, where M is the Galois closure of L/K. In particular we have*

$$\frac{1}{n!} \leq \delta(S) \leq \frac{1}{n}.$$

EXERCISE 5.63. *Prove Corollary 5.75.*

COROLLARY 5.76. *(Equidistribution of Frobenius elements in the abelian case) With notation as above, suppose that $G = \mathrm{Gal}(L/K)$ is commutative. Then for any $\sigma \in G$, the set of unramified primes $\mathfrak{p}$ such that $\tau_{\mathfrak{p}} = \sigma$ has density $\frac{1}{\#G}$.*

The "intersection" of Corollaries 5.75 and 5.76 is important in of itself: that in an abelian extension L/K of degree n, the set of unramified primes $\mathfrak{p}$ of R for which $\tau_{\mathfrak{p}} = 1$ – i.e., which split completely in L – has density $\frac{1}{n}$.[8]

EXERCISE 5.64. *Let L/K be an extension of number fields. Corollary 5.75 shows that the density of primes $\mathfrak{p} \in \mathrm{MaxSpec}\, \mathbb{Z}_K$ that split completely in $\mathbb{Z}_L$ is positive (and computes it). It is remarkable how much easier it is to show that infinitely many primes split completely in $\mathbb{Z}_L$. We follow an argument of Poonen on MathOverflow* [**Po10**].

[8]This special case was proved much earlier by Frobenius: see below.

a) *Explain why it suffices to show in any finite degree Galois extension $K/\mathbb{Q}$, there are infinitely many prime numbers p that split completely in $\mathbb{Z}_K$.*
b) *Choose $\alpha \in \mathbb{Z}_K$ such that $K = \mathbb{Q}[\alpha]$, and let $f \in \mathbb{Z}[t]$ be the minimal polynomial of α. Let p be a prime number that does not divide the discriminant of f. Show: p splits completely in $\mathbb{Z}_K$ if and only if there is $n \in \mathbb{Z}$ such that $p \mid f(n)$.*
c) *Fill in the details of the following argument to show that for any nonconstant polynomial $f \in \mathbb{Z}[t]$, there are infintiely many prime numbers p such that $p \mid f(n)$ for some $n \in \mathbb{Z}$.*

We may assume that $f(0) \neq 0$, let $p_1, \ldots, p_k$ be the prime divisors of $f(0)$ ($k = 0$ is possible), and let $q_1, \ldots, q_\ell$ be any other prime numbers. For $1 \leq i \leq k$, let a_i be the p-adic valuation of $f(0)$, and for $N \in \mathbb{Z}^+$, put

$$x_N := f(Np_1^{a_1+1} \cdots p_k^{a_k+1} q_1 \cdots q_\ell).$$

Show: for all but finitely many values of N, the integer x_N is divisible by a prime different from any of $p_1, \ldots, p_k, q_1, \ldots, q_\ell$.

EXAMPLE 5.77. *Let L/K be a quadratic extension. Then the set of ramified primes is finite, and the set of primes which split completely and the set of inert primes both have density $\frac{1}{2}$. Applying this in particular to $K = \mathbb{Q}$, $L = \mathbb{Q}(\sqrt{D})$, this gives: for $(p, 4D) = 1$, the set of primes p such that $(\frac{D}{p}) = 1$ and the set such that $(\frac{D}{p}) = -1$ each have density $\frac{1}{2}$.*

EXAMPLE 5.78. *Let $K = \mathbb{Q}$ and $L = \mathbb{Q}(\zeta_n)$, where ζ_n is (still) a primitive nth root of unity. The well-known irreducibility of the cyclotomic polynomials easily implies that $\mathrm{Gal}(L/K) = (\mathbb{Z}/n\mathbb{Z})^\times$, the isomorphism being given by $a \pmod n \mapsto (\zeta_n \mapsto \zeta_n^a)$. Recall that every prime not dividing n is unramified. So for p with $\gcd(p, n) = 1$, there is a well-defined Frobenius element τ_p in G; it is a great exercise to check that under the above isomorphism τ_p is precisely the class of p in $(\mathbb{Z}/n\mathbb{Z})^\times$. Thus in this very special case we recover the following seminal result:*

THEOREM 5.79. *(Dirichlet's Theorem) For $n \in \mathbb{Z}^+$ and any a with $\gcd(a, n) = 1$, the set of primes p that are congruent to $a \pmod n$ has density $\frac{1}{\varphi(n)}$.*

EXERCISE 5.65. *Let $P(t) \in \mathbb{Z}[t]$ be a monic polynomial of positive degree d. For a prime number ℓ, let $\tilde{P}_\ell \in \mathbb{F}_\ell[t]$ denote the obvious (coefficientwise) modulo ℓ reduction of P.*

a) *If P is reducible over $\mathbb{Z}[t]$, then for all ℓ, $\tilde{P}_\ell$ is reducible over $\mathbb{F}_\ell[t]$. Thus, applying the contrapositive, we get a sufficient condition for irreducibility of P: it suffices for $\tilde{P}_\ell$ to be reducible for some ℓ.*
b) *Suppose that the degree d is a **prime number**. Show a (much more interesting) converse: the set of primes ℓ such that $\tilde{P}_\ell(t)$ is irreducible has positive density.*
c) *Find an irreducible quartic (i.e., $d = 4$) polynomial all of whose mod ℓ reductions are reducible.*
d) *Show that a polynomial as in part c) exists for all composite degrees d.*[9]

[9]This is proved in [**Br86**]. The generalization to polynomials over any global ring is proved in [**GSS05**].

10.2. Some further remarks.

Theorem 5.74 was conjectured by Frobenius in 1896. He was able to prove a substantial special case: in the **Frobenius Density Theorem** the subset T must be invariant under conjugation and also have the property that if $\sigma \in T$, so is every other generator of the cyclic subgroup generated by σ, i.e., for all i prime to the order of σ, $\sigma^i \in T$. Note that when G is a symmetric group (which is what the Galois group of an extension of global fields will be "with probability 1") the first condition implies the second, since σ^i has the same cycle type as σ. Also Frobenius' theorem applies in the case in which T is a normal sub**group** of G; in particular it applies to $T = \{e\}$, giving Corollary 5.75.

Nikolai Grigorevich Chebotarev was born in 1896 and died in 1947. He proved the density theorem in summer of 1922, having just turned 26, while being physically occupied with rather menial labor (e.g., bringing buckets of cabbages to the market for his mother to sell) in the city of Odessa. He was not able to defend his dissertation (on the density theorem) until 1927.

Strictly speaking what Chebotarev proved was weaker than Theorem 5.74: he proved the result when K is a number field and for the Dirichlet density $\delta_D(T_X)$. The generalization to natural density in the number field case is a significant piece of analytic number theory. Even in the special case of Dirichlet's Theorem (proved in the case of Dirichlet density by....Dirichlet), the version for natural density was not proven until much later by de la Vallée Poussin. Apparently the replacement of Dirichlet density by natural density in the full-fledged Chebotarev Theorem was first done by Hecke (and is sufficiently difficult not to be found in any of the standard texts that I have consulted). It should be noted that in the vast majority of cases the real import of the Density Theorem is to show that the set of primes in question is infinite, and for this it certainly doesn't matter which density is used.

The proof in the function field case – $\operatorname{char} K > 0$ – is not dramatically different, and in some ways it is simpler. It seems to have first been proven by Reichardt in 1936. The argument is similar to Chebotarev's and in some ways simpler.

However, in the function field case it is not always true that the *natural* density $\delta(T_X)$ exists! It turns out that $\delta_D(T_X)$ exists when the extension L/K has trivial constant field extension – i.e., if the algebraic closure of $\mathbb{F}_p$ in K is algebraically closed in L – but there are counterexamples in the general case. This was pointed out to me by Melanie Matchett Wood on 6/19/13, correcting an error in the way Theorem 5.74 had originally been stated (in spring 2008). Wood also suggests the reference [**Ba08**] for more information on this phenomenon.

There are **effective** versions of the Chebotarev Density Theorem, i.e., one can give an explicit upper bound on the norm of the least unramified prime $\mathfrak{p}$ whose Frobenius conjugacy class lies in the normal subset T of $\operatorname{Gal}(L/K)$. I have had occasion to look at such estimates: as one might imagine, the estimates depend on all the quantities in question (especially, the discriminant $\Delta(S/R)$) in a somewhat complicated way. What is unconditionally known is somewhat disappointingly weaker than what should be true: if one is willing to assume the Generalized Riemann Hypothesis (GRH) then there are bounds which are a full logarithm better than the unconditional bounds.

CHAPTER 6

Geometry of Numbers

1. Geometry of Numbers

1.1. Convex subsets of $\mathbb{R}^N$. Let $N \in \mathbb{Z}^+$, and let Ω be a subset of $\mathbb{R}^N$. A point $p \in \mathbb{R}^N$ is a **center** for Ω if for all $x \in \Omega$, the reflection of x through p also lies in Ω.

EXERCISE 6.1. *A bounded subset Ω of $\mathbb{R}^N$ can have at most one center.*

We define a subset Ω to be **centrally symmetric** if 0 is a center for Ω: that is, for all $x \in \mathbb{R}^N$ we have $x \in \Omega \iff -x \in \Omega$.

A subset Ω of $\mathbb{R}^N$ is **convex** if for all $P, Q \in \mathbb{R}^N$, if $P, Q \in \Omega$ then the entire line segment from P to Q is contained in Ω: precisely, for all $\lambda \in [0,1]$ we have $(1-\lambda)P + \lambda Q \in \Omega$.

Here are some "undergraduate level facts" about convexity (indeed, most of these results were either proved or assigned as exercises in the undergraduate real analysis course I taught in Fall 2022):

EXERCISE 6.2. *Let Ω be a nonempty subset of $\mathbb{R}$. Show: Ω is convex if and only if Ω is an interval.*

EXERCISE 6.3.

a) *Let $\{\Omega_i\}_{i \in I}$ be a family of convex subsets of $\mathbb{R}^N$ indexed by a nonempty set I. Show: $\bigcap_{i \in I} \Omega_i$ is always convex, but if $\#I \geq 2$ then $\bigcup_{i \in I} \Omega_i$ need not be.*

b) *Let $\Omega_1 \subseteq \Omega_2 \subseteq \ldots \subseteq \Omega_n \subseteq \ldots$ be an ascending chain of convex subsets of $\mathbb{R}^N$. Show: $\bigcup_{n=1}^{\infty} \Omega_n$ is convex.*

c) *Let $\Omega_1 \subseteq \mathbb{R}^{N_1}$ and $\omega_2 \subseteq \mathbb{R}^{N_2}$ be convex subsets. Show that the Cartesian product $\Omega_1 \times \Omega_2 \subseteq \mathbb{R}^{N_1+N_2}$ is convex.*

EXERCISE 6.4. *Show: open and closed balls in $\mathbb{R}^N$ are convex.*

And here are some results about convexity that are just a little deeper than the ones above. First we need the notion of a **convex combination**: if $x_1, \ldots, x_n$ are vectors in $\mathbb{R}^N$, then a **convex combination** of $x_1, \ldots, x_n$ is a linear combination

$$\lambda_1 x_1 + \ldots + \lambda_n x_n$$

satisfying the extra conditions

$$\lambda_1, \ldots, \lambda_n \geq 0, \ \lambda_1 + \ldots + \lambda_n = 1.$$

For a subset $S \subseteq \mathbb{R}^N$, we define $\operatorname{Conv} S$ to be the set of convex combinations of $x_1, \ldots, x_n$, where we range over all finite sequences of elements of S. Notice that

if $S = \{x, y\}$ then $\operatorname{Conv} S$ is the line segment from x to y. A nonempty subset $S \subseteq \mathbb{R}^N$ is **affinely independent** if for each $x_0 \in S$, the set $\{x - x_0 \mid x \in S \setminus \{0\}\}$ is linearly independent. Actually, it suffices to require this condition for any one $x_0 \in S$: this means that after S is translated back to the origin, its set of nonzero elements is linearly independent. Evidently if $S \subseteq \mathbb{R}^N$ is affinely independent, then $\#S \leq N + 1$. If S is an affinely independent set with cardinality $n + 1$, we call $\operatorname{Conv} S$ an **n-simplex**.

EXERCISE 6.5. *Let $S \subseteq \mathbb{R}^N$.*

a) *Show that there is a unique subset $\mathcal{C}(S)$ of $\mathbb{R}^N$ with the properties that: $\mathcal{C}(S) \supseteq S$, $\mathcal{C}(S)$ is convex, and for all convex subsets $\Omega \supseteq S$ we have $\Omega \supseteq \mathcal{C}(S)$.*
b) *Show that $\mathcal{C}(S) = \operatorname{Conv} S$.*

*This subset is called the **convex hull** of S.*

EXERCISE 6.6. *Let (X, τ) be a topological space. For a subset $Y \subseteq X$ we denote by Y° the interior of Y, i.e., the largest open subset contained in Y; and we denote by $\overline{Y}$ the closure of Y, i.e., the smallest closed subset containing Y. A subset Y is **regular-open** if $Y = (\overline{Y})^\circ$. A subset Y is **regular-closed** if $Y = \overline{Y^\circ}$.*

a) *Show: evey regular-open subset of a topological space is open. Exhibit a subset Y of $\mathbb{R}$ that is open but not regular-open.*
b) *Show: every regular-closed subset of a topological space is closed. Exhibit a subset Z of $\mathbb{R}$ that is closed but not regular-closed.*
c) *Show: if $\Omega \subseteq \mathbb{R}^N$ is convex, then $\Omega^\circ = (\overline{\Omega})^\circ$. Deduce: an open convex set is regular-open.*
d) *Show: if $\Omega \subseteq \mathbb{R}^N$ is convex, then $\overline{\Omega} = \overline{\Omega^\circ}$. Deduce: a closed convex set is regular-closed.*

EXERCISE 6.7. *Let Ω be a subset of $\mathbb{R}^N$. Show that the following are equivalent:*

(i) *Ω is convex.*
(ii) *Ω° is convex.*
(iii) *$\overline{\Omega}$ is convex.*

A bounded subset $\Omega \subseteq \mathbb{R}^N$ is **Jordan measurable** if its characteristic function

$$\mathbf{1}_\Omega : \mathbb{R}^N \to \mathbb{R} \text{ by } x \mapsto \begin{cases} 1 & x \in \Omega \\ 0 & x \notin \Omega \end{cases}$$

is Riemann integrable. Yes, I said Riemann! Because Riemann integrable functions are Lebesgue integrable, a bounded Jordan measurable subset is certainly also Lebesgue measurable, but being Jordan measurable is strictly stronger: indeed, Lebesgue's Criterion[1] says that the bounded function $\mathbf{1}_\Omega$ is Riemann integrable if and only if its discontinuities form a set of Lebesgue measure zero. It is easy to see that $\mathbf{1}_\Omega$ is discontinuous precisely on the boundary $\partial\Omega$ of Ω, so....a bounded set is Jordan measurable if and only if its boundary has Lebesgue measure zero.

Here is a basic fact:

[1]My colleague Roy Smith showed me where this result appears in Riemann's work, so I don't know why it is not named after Riemann....but it isn't.

THEOREM 6.1. *A bounded convex subset $\Omega \subseteq \mathbb{R}^N$ is Jordan measurable (hence Lebesgue measurable).*

PROOF. See e.g. [**Sz97**]. □

1.2. Lattices in $\mathbb{R}^N$. Let $N \in \mathbb{Z}^+$. A **lattice** Λ in $\mathbb{R}^N$ is the $\mathbb{Z}$-span of an $\mathbb{R}$-basis of $\mathbb{R}^N$.

Let $\mathcal{L}(\mathbb{R}^N)$ be the set of lattices in $\mathbb{R}^N$. If $\Lambda \in \mathcal{L}(\mathbb{R}^N)$ and $M \in \mathrm{GL}_N(\mathbb{R})$, then

$$M\Lambda := \{Mx \mid x \in \Lambda\}$$

also lies in $\mathcal{L}(\mathbb{R}^N)$: indeed, if Λ is the $\mathbb{Z}$-span of the $\mathbb{R}$-basis $x_1, \ldots, x_N$ then $M\Lambda$ is the $\mathbb{Z}$-span of the $\mathbb{R}$-basis $Mx_1, \ldots, Mx_N$. The space $\mathcal{L}(\mathbb{R}^N)$ can be topologized as a quotient space of $\mathrm{GL}_N(\mathbb{R})$, as explored in the following exercise.

EXERCISE 6.8.

a) *Show:* $\mathrm{GL}_N(\mathbb{R})$ *acts transitively on* $\mathcal{L}(\mathbb{R}^N)$ *and that the stabilizer of* $\mathbb{Z}^N$ *is* $\mathrm{GL}_N(\mathbb{Z})$. *Deduce an isomorphism of* $\mathrm{GL}_N(\mathbb{R})$*-sets*

$$\iota : \mathcal{L}(\mathbb{R}^N) \xrightarrow{\sim} \mathrm{GL}_N(\mathbb{R})/\mathrm{GL}_N(\mathbb{Z}).$$

b) $\mathrm{GL}_N(\mathbb{R})$ *is a topological space – indeed, a Lie group whose underlying* $\mathbb{R}$*-manifold has dimension* N^2 *– and this allows us to endow* $\mathcal{L}(\mathbb{R}^N)$ *with a topology, the quotient topology with respect to the map*

$$q : \mathrm{GL}_N(\mathbb{R}) \to \mathcal{L}(\mathbb{R}^N),\ M \mapsto M\mathbb{Z}^N.$$

(This is really the quotient topology on $\mathrm{GL}_N(\mathbb{R})/\mathrm{GL}_N(\mathbb{Z})$ *"transported" via the bijection* ι*.) Show:* q *is a covering map. Deduce:* $\mathcal{L}(\mathbb{R}^N)$ *is a Hausdorff, second-countable* $\mathbb{R}$*-manifold of dimension* N^2*.*

c) *Show: if* $\Lambda \in \mathcal{L}(\mathbb{R})$*, then* $\Lambda = \langle\lambda\rangle$ *for a unique* $\lambda \in \mathbb{R}^{>0}$*. Deduce:* $\mathcal{L}(\mathbb{R})$ *is homeomorphic to* $\mathbb{R}^{>0}$*.*

d) *Let* $\{\Lambda_n\}_{n=1}^{\infty}$ *be a sequence in* $\mathcal{L}(\mathbb{R}^N)$ *and let* $\Lambda \in \mathcal{L}(\mathbb{R}^N)$*. Show:* $\Lambda_n \to \Lambda$ *if and only if for all* $n \in \mathbb{Z}^+$ *there is an ordered* $\mathbb{Z}$*-basis* $\mathbf{x}_n$ *of* Λ_n *and an ordered* $\mathbb{Z}$*-basis* $\mathbf{x}$ *of* Λ *such that, as vectors in* $\mathbb{R}^{Nn}$ *we have* $\mathbf{x}_n \to \mathbf{x}$*.*
(Hint: if $\pi : Y \to X$ *is a covering map and* $x_n \to x$ *is a convergent sequence in* X*, then for any lift* $\tilde{x}$ *of* x *to* Y*, one can lift each* x_n *to* $\widetilde{x_n}$ *such that* $\widetilde{x_n} \to x_n$*: indeed, after choosing* $\tilde{x}$*, for all sufficiently large* n *the desired lift* $\widetilde{x_n}$ *of* x_n *is unique.)*

For a Dedekind domain A with fraction field K, in Chapter 4 we studied A-lattices in a finite-dimensional K-vector space. Taking $A = \mathbb{Z}$, we have the notion of a $\mathbb{Z}$-lattice Λ in $\mathbb{Q}^N$: because $\mathbb{Z}$ is a PID, Λ is necessarily the $\mathbb{Z}$-span of a $\mathbb{Q}$-basis $x_1, \ldots, x_N$ for $\mathbb{Q}^N$. If L/K is a field extension, V is a K-vector space and S is a subset of V, then S is K-linearly independent if and only if S is L-linearly independent in $V_L := V \otimes_K L$; it follows that $x_1, \ldots, x_N$ are also $\mathbb{R}$-linearly independent hence form an $\mathbb{R}$-basis for $\mathbb{R}^N$. That is, Λ is also an $\mathbb{R}$-lattice in $\mathbb{R}^N$, so we get:

$$\mathcal{L}(\mathbb{Q}^N) \subseteq \mathcal{L}(\mathbb{R}^N).$$

It is easy to see that $\mathcal{L}(\mathbb{Q}^N)$ is a countable dense subset of $\mathcal{L}(\mathbb{R}^N)$.

Thus our new notion of lattice is evidently related to our old notion of lattice, but there are still some differences. Here is one:

EXERCISE 6.9. *Let Λ be a subgroup of $\mathbb{Q}^N$. Show: Λ is a $\mathbb{Z}$-lattice in $\mathbb{Q}^N$ if and only if $\Lambda \cong \mathbb{Z}^N$.*

It is clear that if $\Lambda \in \mathcal{L}(\mathbb{R}^N)$, then $\Lambda \cong_{\mathbb{Z}} \mathbb{Z}^N$. The converse holds when $N = 1$, just because any nonzero element of $\mathbb{R}$ is an $\mathbb{R}$-basis for $\mathbb{R}$. However the converse fails for $N \geq 2$: since $\mathbb{R}$ is an infinite-dimensional $\mathbb{Q}$-vector space for all $N \geq 1$ there is an injective group homomorphism $\mathbb{Z}^N \hookrightarrow \mathbb{R}$. Viewing $\mathbb{R}$ as a subset of $\mathbb{R}^N$ via $x \mapsto (x, 0, \ldots, 0)$, we see that for all $N \geq 2$ we get an injective homomorphism $\iota : Z^N \to \mathbb{R}^N$ such that $\dim \langle \iota(\mathbb{Z}^N) \rangle_{\mathbb{R}} = 1$.

Let $\Lambda \subseteq \mathbb{R}^N$ be a subgroup such that $\Lambda \cong \mathbb{Z}^N$. We claim that Λ is a lattice in $\mathbb{R}^N$ if and only if Λ is discrete. One direction of this is clear: indeed, if $M \in \mathrm{GL}_N(\mathbb{R})$, then $M\cdot : \mathbb{R}^N \to \mathbb{R}^N$ is an isomorphism of topological groups (i.e., a group isomorphism and a homeomorphism) so it carries discrete subgroups to discrete subgroups. Clearly $\mathbb{Z}^N$ is a discrete subgroup of $\mathbb{R}^N$, so also $M\mathbb{Z}^N$ is a discrete subgroup of $\mathbb{R}^N$, and every lattice in $\mathbb{R}^N$ is of this form.
The converse takes more work. We will give a complete proof, but let me mention that this result is not needed for any of our number-theoretic applications so can safely be skipped if desired. We will work a bit more generally. First:

LEMMA 6.2. *Let G be a Hausdorff topological group, and let H be a locally compact subgroup of G. Then:*

a) *The subgroup H is closed in G.*
b) *In particular: if H is discrete, then H is closed in G.*

PROOF. a) Let K be a compact neighborhood of the identity element e in H. Let U be an open neighborhood of e in G such that $U \cap H \subseteq K$. Let x lie in the closure $\overline{H}$ of H. Then there is a neighborhood V of x in G such that $V^{-1}V \subseteq U$, and thus

$$(V \cap H)^{-1}(V \cap H) \subseteq U \cap H \subseteq K.$$

Since $x \in \overline{H}$, we have that $V \cap H$ is nonempty. Choose $y \in V \cap H$; then $V \cap H \subseteq yK$. For every neighborhood W of x, also $W \cap V$ is a neighborhood of x, so $W \cap V \cap H$ nonempty; it follows that $x \in \overline{V \cap H}$. Since yK is a compact subset of the Hausdorff space H, it is closed, an thus

$$x \in \overline{V \cap H} \subseteq \overline{yK} = YK \subseteq H.$$

It follows that H is closed.
b) This is immediate from part a): discrete groups are locally compact. □

For a subgroup $G \subseteq \mathbb{R}^N$, we define the **real rank** $\mathfrak{r}(G)$ to be the maximal size of an $\mathbb{R}$-linearly independent subset of G, so $0 \leq \mathfrak{r}(G) \leq N$. This is a reasonable definition for us to make at this point because, as we saw, if $\Lambda \subseteq \mathbb{R}^N$ is a subgroup that is isomorphic to $\mathbb{Z}^N$, then Λ is a lattice precisely when $\mathfrak{r}(\Lambda) = N$. Now:

THEOREM 6.3. *Let G be a discrete subgroup of $(\mathbb{R}^N, +)$, of real rank r. Then there are $\mathbb{R}$-linearly independent elements $v_1, \ldots, v_r \in \mathbb{R}^N$ forming a $\mathbb{Z}$-basis for G.*

PROOF. By Lemma 6.2, we know that G is closed. Evidently we have $r = 0 \iff G = \{0\}$, so we may assume that $1 \leq r \leq N$.

By definition of the real rank, there are $e_1, \ldots, e_r \in G$ that are $\mathbb{R}$-linearly

independent. Let

$$\mathcal{P} \coloneqq \left\{ \sum_{i=1}^{r} x_i e_i \mid x_i \in [0,1] \right\}$$

be the corresponding paralleletope. Then $G \cap \mathcal{P}$ is closed, discrete and compact, hence finite. Let $x \in G$. Since r is the real rank of G, there are $\lambda_1, \ldots, \lambda_r \in \mathbb{R}$ such that

$$x = \sum_{i=1}^{r} \lambda_i e_i.$$

For $j \in \mathbb{Z}$, put

$$x_j \coloneqq jx - \sum_{i=1}^{r} \lfloor j\lambda_i \rfloor e_i.$$

Thus

$$x_j = \sum_{i=1}^{r} \left(j\lambda_i - \lfloor j\lambda_i \rfloor \right) e_i,$$

so $x_j \in G \cap \mathcal{P}$. Since $x = x_1 + \sum_{i=1}^{r} \lfloor \lambda_i \rfloor e_i$, we see that G is generated as a $\mathbb{Z}$-module by $G \cap \mathcal{P}$, hence is finitely generated. Moreover, since $G \cap \mathcal{P}$ is finite and $\mathbb{Z}$ is infinite, there are distinct $j, k \in \mathbb{Z}$ such that $x_j = x_k$. Then

$$\forall 1 \leq i \leq r,\ (j-k)\lambda_i = \lfloor j\lambda_i \rfloor - \lfloor k\lambda_i \rfloor,$$

so $\lambda_i \in \mathbb{Q}$ for all i. Thus G is generated as a $\mathbb{Z}$-module by a finite number of $\mathbb{Q}$-linear combinations of the e_i's. Let d be a common denominator for the coefficients of this finite generating set, so

$$dG \subseteq \langle e_1, \ldots, e_r \rangle_{\mathbb{Z}}.$$

This shows that the free rank of dG is at most r, but the free rank of dG is equal to the free rank of G, so the free rank of G is at most r. Conversely, since $e_1, \ldots, e_r$ are $\mathbb{R}$-linearly independent they are certainly $\mathbb{Z}$-linearly independent, so G is free of rank r. Let $v_1, \ldots, v_r$ be any $\mathbb{Z}$-basis for G. Since the $\mathbb{R}$-span of $v_1, \ldots, v_r$ contains the $\mathbb{R}$-linearly indendent set $e_1, \ldots, e_r$,t he elements $v_1, \ldots, v_r$ must also be $\mathbb{R}$-linearly independent. □

A lattice Λ in $\mathbb{R}^N$ has a **covolume** $\operatorname{Covol} \Lambda \in \mathbb{R}^{>0}$: if $v_1, \ldots, v_N$ is a $\mathbb{Z}$-basis for Λ, let $M_v \in \mathrm{GL}_N(\mathbb{R})$ be the matrix whose columns are $v_1, \ldots, v_N$; then we put

$$\operatorname{Covol} \Lambda \coloneqq |\det M_v|.$$

We should check that this is independent of the chosen $\mathbb{Z}$-basis, but this is easy: if $w_1, \ldots, w_N$ is another $\mathbb{Z}$-basis of Λ, let A be the matrix representing the linear automorphism of $\mathbb{R}^N$ that carries v_i to w_i for all $1 \leq i \leq N$. Then, if $M_w \in \mathrm{GL}_N(\mathbb{R})$ is the matrix with columns $w_1, \ldots, w_N$, we have

$$M_w = AM_v.$$

Moreover the jth column of A gives the coefficients in the unique expression of w_j as an $\mathbb{R}$-linear combination of $v_1, \ldots, v_N$; but w_j is a $\mathbb{Z}$-linear combnation of $v_1, \ldots, v_N$, so $A \in M_N(\mathbb{Z})$. The same argument with the v's and w's reversed shows that $A^{-1} \in M_N(\mathbb{Z})$, so $A \in \mathrm{GL}_N(\mathbb{Z})$ and thus $\det A \in \mathbb{Z}^\times = \{\pm 1\}$, so

$$|\det M_w| = |\det M_v|.$$

EXERCISE 6.10. *Let $\Lambda \in \mathcal{L}(\mathbb{R}^N)$ and $M \in \mathrm{GL}_N(\mathbb{R})$. Show:*

$$\mathrm{Covol}(M\Lambda) = |\det M| \,\mathrm{Covol}(\Lambda).$$

EXERCISE 6.11.

a) *Let $\Lambda_n \to \Lambda$ be a convergent sequence in $\mathcal{L}(\mathbb{R}^N)$. Show:* $\mathrm{Covol}\,\Lambda_n \to \mathrm{Covol}\,\Lambda$.

b) *Show: for no $N \in \mathbb{Z}^+$ is $\mathcal{L}(\mathbb{R}^N)$ compact.*
(Suggestion: because $\mathcal{L}(\mathbb{R}^N)$ is metrizable, it is equivalent to find a sequence of lattices with no convergent subsequence.)

There are some unanswered questions about $\mathrm{Covol}\,\Lambda$: e.g. why "volume" and why "co"? Let us give a geometric interpretation: multiplication by M_v gives the linear automorphism of $\mathbb{R}^N$ that carries the standard basis $(e_1, \ldots, e_N)$ to the basis $(v_1, \ldots, v_N)$. Therefore M_v maps the unit cube $C_N := [0,1]^N$ to the **paralleletope**

$$\mathcal{P}_v := \{x_1 v_1 + \ldots + x_N v_N \mid x_1, \ldots, x_N \in [0,1]\}.$$

A standard interpretation of the determinant of $M \in \mathrm{GL}_N(\mathbb{R})$ is that it is the change in "signed volume" effected by the linear transformation $M\cdot$, so that

$$|\det M_v| = \mathrm{Vol}(\mathcal{P}_v).$$

(Here we denote the Lebesgue measure on $\mathbb{R}^N$ by Vol.) More generally, if $X \subset \mathbb{R}^N$ is any bounded Lebesgue-measurable set and $M \in \mathrm{GL}_N(\mathbb{R})$, then

$$\mathrm{Vol}(MX) = |\det M| \,\mathrm{Vol}(X). \tag{28}$$

Thus, if we put $\Lambda_v := \langle v_1, \ldots, v_N \rangle_{\mathbb{Z}}$, we find:

$$\mathrm{Covol}\,\Lambda_v = \mathrm{Vol}(\mathcal{P}_v).$$

This is a special case of something quite general, which we now briefly sketch out. Suppose a group G acts on a set X. A **fundamental region** for the action of G is a subset $R \subset X$ that contains exactly one element of each G-orbit on X. Thus fundamental regions correspond to sections of the quotient map

$$X \to G\backslash X$$

and thereby exist in great abundance. For the natural action of Λ_v on $\mathbb{R}^N$, the paralleletope $\mathcal{P}_v$ is *almost* a fundamental region, but it is slightly too large: rather

$$\mathcal{R}_v := \{x_1 v_1 + \ldots + x_N v_N \mid x_1, \ldots, x_N \in [0,1)\}$$

is a fundamental region. Notice that $\mathcal{R}_v$ is neither open nor closed but its closure is $\mathcal{P}_v$ and we have $\mathrm{Vol}(\mathcal{R}_v) = \mathrm{Vol}(\mathcal{P}_v)$.

Suppose now that our G-set X is a topological space equipped with a Borel measure μ and that G acts on X by measure-preserving homeomorphisms. Under some further reasonable hypotheses – which we need not digress to specify – both of the following will hold: (i) there is a measurable fundamental region R for the action of G; and (ii) any two measurable fundamental regions for the action of G have the same measure. Then we can define $\mu(G\backslash X)$ to be the measure of any fundamental region. This is what is happening in the context of Λ_x acting on $\mathbb{R}^N$: the Lebesgue measure on $\mathbb{R}^N$ induces a measure on the quotient space $\mathbb{R}^N/\Lambda_x$ (which is homeomorphic to an N-dimensional torus, i.e., to $(S^1)^N$) inherits a measure, whose total mass is $\mathrm{Covol}\,\Lambda_x$.

Notice that $\operatorname{Covol}\Lambda$ is *not* the measure of Λ: Λ is countable so has measure zero. It is rather the measure of any fundamental paralleletope for Λ, which we can think of as measuring "the space between the points of Λ." In particular, a lattice with large covlume has sparsely spaced vectors, while a lattice with small covolume has densely spaced vectors. In particular:

EXERCISE 6.12. *Let $\Lambda_1 \subseteq \Lambda_2$ be two latices in $\mathbb{R}^N$. Show:*

$$\operatorname{Covol}\Lambda_1 = [\Lambda_2 : \Lambda_1] \operatorname{Covol}\Lambda_2.$$

In fact, if we have lattices $\Lambda_1 \subseteq \Lambda_2$ in $\mathbb{R}^N$ and one of Λ_1 and Λ_2 is contained in $\mathbb{Q}^N$ then so is the other, and in this case Exercise 6.12 is a quick consequence of Proposition 4.6. It is actually possible to deduce the general case of Exercise 6.12 from this using an approximation by rational lattices...though I don't claim this is the easiest way to proceed.

Finally, we remark that different fundamental parallelepipeds for the same lattice all have the same size (volume = measure) but have very different shapes. Indeed, any bounded subset of $\mathbb{R}^N$ contains only finitely many points of Λ hence only finitely many bases for Λ, hence only finitely many fundamental parallelepipeds for Λ. Thus e.g. the fundamental parallelograms for $\mathbb{Z}^2$ in $\mathbb{R}^2$ can be put into a sequence, and as the terms of this sequence increase the parallelograms get longer (their diameters tend to ∞) and thinner (all their areas are $\frac{1}{2}$).

The following exercises introduces a version of the Fröhlich invariant for certain pairs of lattices in $\mathbb{R}^N$.

EXERCISE 6.13. *Let $\Lambda_1, \Lambda_2 \in \mathcal{L}(\mathbb{R}^N)$.*

a) *Show that the following are equivalent:*
   (i) *$\Lambda_1 \cap \Lambda_2$ has finite index in both Λ_1 and Λ_2.*
   (ii) *There is $n \in \mathbb{Z}^+$ such that $n\Lambda_1 \subseteq \Lambda_2 \subseteq \frac{1}{n}\Lambda_1$.*
   (iii) *Λ_1 and Λ_2 span the same $\mathbb{Q}$-subspace of $\mathbb{R}^N$.*
   *When these conditions hold, we say that Λ_1 and Λ_2 are **commensurable**. In this case we define a **generalized index** $[\Lambda_2 : \Lambda_1]$ as follows: we chooose $n \in \mathbb{Z}^+$ such that $n\Lambda_1 \subseteq \Lambda_2$ and put*

$$[\Lambda_2 : \Lambda_1] \coloneqq n^{-N}[\Lambda_2 : n\Lambda_1],$$

   where on the right hand side we have the usual group-theoretic index.
b) *Show that the generalized index of commensurable lattices is well-defined.*
c) *Show: if $\Lambda_1 \subseteq \Lambda_2$, then the generalized index coincides with the index.*
d) *Show:* $\operatorname{Covol}\Lambda_1 = [\Lambda_2 : \Lambda_1] \operatorname{Covol}\Lambda_2$.

1.3. Minkowski's Convex Body Theorem. We define a **convex body** to be a subset $\Omega \subseteq \mathbb{R}^N$ that is nonempty, convex, centrally symmetric and bounded. Some people also require a convex body to have nonempty interior. The following exercise gives some perspective on this:

EXERCISE 6.14. *Let $\Omega \subseteq \mathbb{R}^N$ be convex. Show that the following are equivalent:*
(i) *Ω is "flat," i.e., is contained in some hyperplane H of $\mathbb{R}^N$.*
(ii) $\operatorname{Vol}\Omega = 0$.
(iii) *Ω has empty interior.*

Thus requiring a convex body to have nonempty interior is the same as requiring it to have positive volume. We will soon see why we don't need to require this.

Geometry of Numbers starts when we consider a convex body $\Omega \subseteq \mathbb{R}^N$ and a lattice $\Lambda \subseteq \mathbb{R}^N$ together: consider $\Omega \cap \Lambda$. What can we say about this set?

Well, first of all it is nonempty. Indeed, since Ω is nonempty, it contains some point x; since Ω is centrally symmetric, it also contains $-x$, and since Ω is convex it contains $\frac{1}{2}(x) + \frac{1}{2}(-x) = 0$.

Let $\Lambda^\bullet := \Lambda \setminus \{0\}$. Could $\Lambda^\bullet \cap \Omega$ be empty?

Yes, of course. The set $\Lambda^\bullet$ is closed, so the distance from a point of $\Lambda^\bullet$ to 0 assumes a minimum value [**GT**, Thm. 2.114], which we actually call the **minimum** $m(\Lambda)$ of the lattice Λ. So $B^\circ(0, m(\Lambda))$, the open ball centered at the origin with radius $m(\Lambda)$, does not meet $\Lambda^\bullet$ (i.e, the intersection is empty). Of course if R is sufficiently large, then $B^\circ(0, R)$ does meet $\Lambda^\bullet$. The key question is: in order for $\Omega \cap \Lambda^\bullet$ to be nonempty, is it sufficient for $\operatorname{Vol}\Omega$ to be sufficiently large with respect to $\operatorname{Covol}\Lambda$?

As with many problems in the geometry of numbers, there is a useful *linear equivariance*. That is, let $M \in \mathrm{GL}_N(\mathbb{R})$. Certainly Ω meets $\Lambda^\bullet$ if and only if $M(\Omega)$ meets $M(\Lambda)$. Moreover we have nd for all $M \in \mathrm{GL}_N(\mathbb{R})$, we have

$$\frac{\operatorname{Vol}(M\Omega)}{\operatorname{Covol}(M\Lambda)} = \frac{|\det M| \operatorname{Vol}(\Omega)}{|\det M| \operatorname{Covol}(\Lambda)} = \frac{\operatorname{Vol}(\Omega)}{\operatorname{Covol}(\Lambda)},$$

so the ratio $\frac{\operatorname{Vol}(\Omega)}{\operatorname{Covol}(\Lambda)}$ is invariant under linear changes of variable. Because of this, if there is some number V_N such that for all convex bodies Ω with $\operatorname{Vol}\Omega > V_N$ we have $\Omega \cap (\mathbb{Z}^N)^\bullet \neq \varnothing$, then for all convex bodies Ω and lattices Λ with $\frac{\operatorname{Vol}(\Omega)}{\operatorname{Covol}(\Lambda)} > V_N$ we may choose $M \in \mathrm{GL}_N(\mathbb{R})$ such that $M\Lambda = Z^N$ and then

$$2^N < \frac{\operatorname{Vol}(\Omega)}{\operatorname{Covol}(\Lambda)} = \frac{\operatorname{Vol}(M(\Omega))}{\operatorname{Covol}(\mathbb{Z}^N)} = \operatorname{Vol}(M(\Omega)),$$

so $M(\Omega)$ meets $\mathbb{Z}^N = M(\Lambda)$ and thus Ω meets Λ. Since $\Omega = (-1, 1)^N$ has volume 2^N and doesn't meet $(\mathbb{Z}^N)^\bullet$ we must have $V_N \geq 2^N$. And now we are ready for the theorem:

THEOREM 6.4. *(Minkowski's Convex Body Theorem) Let $\Omega \subseteq \mathbb{R}^N$ be a convex body, and let $\Lambda \subseteq \mathbb{R}^N$ be a lattice.*

a) *If $\operatorname{Vol}\Omega > 2^N \operatorname{Covol}\Lambda$, then $\Omega \cap \Lambda^\bullet \neq \varnothing$.*
b) *If Ω is compact and $\operatorname{Vol}\Omega = 2^N \operatorname{Covol}\Lambda$, then $\Omega \cap \Lambda^\bullet \neq \varnothing$.*

PROOF. a) Step 1: We prove **Blichfeldt's Lemma**: if $\Omega \subseteq \mathbb{R}^N$ is **packable** — for all $x \neq y \in \mathbb{Z}^N$, $(x + \Omega) \cap (y + \Omega) = \varnothing$ — and measurable, then $\operatorname{Vol}\Omega \leq 1$.

To see this: for $x = (x_1, \ldots, x_N) \in \mathbb{Z}^N$, put

$$\Omega_x := \Omega \cap \prod_{i=1}^N [x_i, x_i + 1).$$

Thus $\Omega = \coprod_{x \in \mathbb{Z}^N} \Omega_x$, so $\mathrm{Vol}(\Omega) = \sum_{x \in \mathbb{Z}^N} \mathrm{Vol}(\Omega_x)$. Since Ω is packable, the family $\{-x + \Omega_x\}_{x \in \mathbb{Z}^N}$ is pairwise disjoint, so

$$\mathrm{Vol}(\coprod_{x \in \mathbb{Z}^N} (-x + \Omega_x)) = \sum_{x \in \mathbb{Z}^N} \mathrm{Vol}(-x + \Omega_x) = \sum_{x \in \mathbb{Z}^N} \mathrm{Vol}(\Omega_x) = \mathrm{Vol}(\Omega).$$

On the other hand, for all $x \in \mathbb{Z}^N$, we have $-x + \Omega_x \subseteq [0,1)^N$, so

$$\mathrm{Vol}(\Omega) = \mathrm{Vol}(\coprod_{x \in \mathbb{Z}^N} (-x + \Omega_x)) \leq \mathrm{Vol}[0,1)^N = 1.$$

Step 2: As explained above, it suffices to treat the case in which $\Lambda = \mathbb{Z}^N$ and that $\mathrm{Vol}\,\Omega > 2^N$. In fact, applying the linear transformation $x \mapsto \frac{x}{2}$, which changes volumes by a factor of 2^{-N}, it also suffices to treat the case in which $\Lambda = (1/2\mathbb{Z})^N$ and $\mathrm{Vol}\,\Omega > 1$. Thus Blichfeldt's Lemma tells us that Ω is *not* packable, which means there are $P_1, P_2 \in \Omega$ and $x \neq y \in \mathbb{Z}^N$ such that $x + P_1 = y + P_2$; thus $P \coloneqq P_1 - P_2 \in (\mathbb{Z}^N)^\bullet$. As argued above, since Ω is convex and centrally symmetric, we also have $P_2 \in \Omega$ and then $\frac{1}{2}P_1 - \frac{1}{2}P_2$ is a nonzero element of $\Omega \cap (1/2\mathbb{Z})^N$.
b) We leave this as an exercise. □

Exercise 6.15. *Prove Theorem 6.4b).*
(Suggestion: By part a), for all $\epsilon > 0$, the dilate $(1+\epsilon)\Omega$ contains an element of $\Lambda^\bullet$. Argue that there must in fact be a fixed element $P \in (\mathbb{Z}^N)^\bullet$ that lies in $(1+\epsilon)\Omega$ for all $\epsilon > 0$, and make a limiting argument using the fact that Ω is closed.)

1.4. A Slightly More Abstract Approach. Our discussion of both convex subsets and of lattices was with respect to subsets of $\mathbb{R}^N$. In this section we discuss the prospect of doing this in a finite-dimensional $\mathbb{R}$-vector space instead.

First of all, in any $\mathbb{R}$-vector space V (even if it is infinte-dimensional) one can define convex subsets in exactly the same way. The results of §6.1.1 that do not refer to topology ,measure or integration carry over verbatim in this context. We are however interested in the case where V is a finite-dimensional $\mathbb{R}$-vector space, say of dimension $N \in \mathbb{Z}^+$. Such a space is of course isomorphic to $\mathbb{R}^N$ but not canonically so: if $\iota : V \to \mathbb{R}^N$ is one such isomorphism, then the general such isomorphism is of the form $(M\cdot) \circ \iota$ for $M \in \mathrm{GL}_N(\mathbb{R})$. Because $M\cdot$ is a homeomorphism of $\mathbb{R}^N$, the vector space V has a canonical topology obtained from transporting the topology on $\mathbb{R}^N$ via any isomorphism ι. Moreover, because $M\cdot$ is a Lipschitz function, the notions of Lebesgue measurability and of measure zero carry over to V.[2] Thus in fact all of §6.1.1 goes through with $\mathbb{R}^N$ replaced by an abstract finite-dimensional $\mathbb{R}$-vector space V.

If V is an N-dimensional $\mathbb{R}$-vector space, then we can still define a lattice in V as the $\mathbb{Z}$-span of an $\mathbb{R}$-basis. The set $\mathrm{GL}(V)$ of all invertible $\mathbb{R}$-linear maps acts on the set $\mathcal{L}(V)$ of lattices in V as above, and again the action is transitive. After choosing one "standard lattice" Λ_0, we find that

$$\mathcal{L}(V) \cong \mathrm{GL}(V)/\mathrm{Aut}(\Lambda_0).$$

[2]See e.g. https://math.stackexchange.com/questions/1504487/a-lipschitz-transform-maps-measurable-set-to-measurable

Again this puts a topology on $\mathcal{L}(V)$. What we *do not* have in this context is a notion of volume or covolume. We can get a measure on V by transporting Lebesgue measure using an isomorphism $\iota : V \to \mathbb{R}^N$: that is, for $X \subseteq V$,

$$\mu_\iota(X) \coloneqq \mathrm{Vol}(\iota(X)).$$

However, for $M \in \mathrm{GL}_N(\mathbb{R})$, using (28) we find that

$$\mu_{(M\cdot)\circ\iota} = |\det M|\mu_\iota.$$

Let $\mathrm{SL}_N^{\pm}(\mathbb{R})$ be the subgroup of $\mathrm{GL}_N(\mathbb{R})$ consisting of matrices of determinant ± 1. (The notation is because $\mathrm{SL}_N(\mathbb{R})$ is an index 2 subgroup of $\mathrm{SL}_N^{\pm}(\mathbb{R})$.) A **unimodular structure** on V is an $\mathrm{SL}_N^{\pm}(\mathbb{R})$-orbit of isomorphisms $\iota : V \to \mathbb{R}^N$. Thus a unimodular structure on V gives us a well-defined volume.

Now let $\langle \cdot, \cdot \rangle : V \times V \to \mathbb{R}$ be an inner product, by which we mean an $\mathbb{R}$-bilinear form that is **positive definite**:

$$\forall x \in V^\bullet,\ \langle x, x \rangle > 0.$$

Given an inner product, we can choose an orthonormal basis $v_1, \ldots, v_N$ of V, that is an $\mathbb{R}$-basis whose Gram matrix is the identity. (Start with any basis, and perform the Gram-Schmidt process.) This gives us an isomorphism $\iota_v : V \to \mathbb{R}^N$ determined by $v_i \mapsto e_i$ that satisfies:

$$\forall x, y \in V,\ \iota_v(x) \cdot \iota_v(y) = \langle x, y \rangle.$$

(Indeed, by bilinearity it is enough to check this when $x = v_i$ and $y = v_j$, and this is immediate.) Now let $w_1, \ldots, w_N$ be any other orthonormal basis of V, and let $P \in \mathrm{GL}(V)$ be the linear map that carries each v_i to w_i, so

$$\iota_v = \iota_w \circ P.$$

Moreover, for the same reason as above, we have

$$\forall x, y \in V, \langle Px, Py \rangle = \langle x, y \rangle.$$

Thus the map $\iota_v \circ P \circ \iota_v^{-1}$ preserves the standard inner product of $\mathbb{R}^N$, meaning that it is represented by an orthogonal matrix, meaning

$$\det P = \det(\iota_v \circ P \circ \iota_v^{-1}) \in \{\pm 1\}.$$

Thus an inner product on V induces a unimodular structure on V and thereby gives us a well-defined volume.

Now let Λ be a lattice in $(V, \langle \cdot, \cdot \rangle)$, with $\mathbb{Z}$-basis $x = (x_1, \ldots, x_N)$. We define the Gram matrix

$$G_x(i, j) \coloneqq \langle x_i, x_j \rangle.$$

Let $v = (v_1, \ldots, v_N)$ be an orthonormal basis for V, and let $\iota_v : V \to \mathbb{R}^N$ be, as above, the isomorphism that carries each v_i to e_i. Because we have $\langle x, y \rangle = \iota_v(x) \cdot \iota_v(y)$ for all $x, y \in V$, the (i, j)-entry of G_x is equal to $\iota_v(x_i) \cdot \iota_v(x_j)$. Thus if $M_{\iota_v(x)}$ is the matrix with columns $\iota_v(x_1), \ldots, \iota_v(x_N)$, we have

$$G_x = M_{\iota_v(x)}^T M_{\iota_v(x)},$$

so

$$\det G_x = (\det M_{\iota_v(x)})^2 = (\mathrm{Covol}\, \iota_v(\Lambda))^2.$$

The point of our previous discussion is that we can write $\operatorname{Covol}\Lambda$ for $\operatorname{Covol}\iota(\Lambda)$, because our Lebesgue measure Vol on $(V, \langle\cdot,\cdot\rangle)$ does not depend upon the choice of v. We conclude:

PROPOSITION 6.5. *Let Λ be a lattice in the inner product space $(V, \langle\cdot,\cdot\rangle)$. Let G be a Gram matrix for Λ (with respect to some $\mathbb{Z}$-basis of Λ). Then we have:*

$$\operatorname{Covol}\Lambda = \sqrt{\det G}.$$

Finally, we comment that notwithstanding the fact that Minkowksi's Convex Body Theorem refers to both a volume and a covolume, it holds essentially verbatim in any finite-dimensional $\mathbb{R}$-vector space V, even witout an inner product. This is because, as comes out in the proof, the hypothesis is really that the *ratio* $\frac{\operatorname{Vol}\Omega}{\operatorname{Covol}\Lambda} > 2^N$.

Finally, suppose $(V, \langle\cdot,\cdot\rangle)$ is a quadratic $\mathbb{Q}$-space: recall that this means that V is a finite-dimensional $\mathbb{Q}$-vector space and $\langle\cdot,\cdot\rangle$ is a nondegenerate symmetric bilinear form. Then $\langle\cdot,\cdot\rangle$ uniquely extends to an $\mathbb{R}$-bilinear form on $V_{\mathbb{R}} \coloneqq V \otimes_{\mathbb{Q}} \mathbb{R}$ and indeed, if $v = (v_1, \ldots, v_N)$ is any $\mathbb{Q}$-basis for V, then $v \otimes 1 = (v_1 \otimes 1, \ldots, v_N \otimes 1)$ is an $\mathbb{R}$-basis for $V_{\mathbb{R}}$ and we have an equality of Gram matrices $G_v = G_{v\otimes 1}$. However, $\langle\cdot,\cdot\rangle$ need not be an inner product: that requires the additional condition that $\langle x, x\rangle > 0$ for all nonzero $x \in V_{\mathbb{R}}$. Some standard linear algebra / rudiments of quadratic forms theory shows that positive definiteness is equivalent to all the eigenvalues o the Gram matrix being positive (recall that being a smmetric real matrix, G_v has all real eigenvalues) which is in turn equivalent to $\langle x, x\rangle > 0$ for all nonzero $x \in V$, so we can speak of positive definite quadratic $\mathbb{Q}$-spaces as well. If $(V, \langle\cdot,\cdot\rangle)$ is a positive definite quadratic $\mathbb{Q}$-space, then we can speak of rational lattices in $V_{\mathbb{R}}$. In particular, any two rational lattices are commensurable.

2. The Additive Embedding

2.1. Basic Setup.

Let $K/\mathbb{Q}$ be a number field of degree N. Because $K/\mathbb{Q}$ is separable and $\mathbb{C}/\mathbb{Q}$ is algebraically closed, there are preicsely N $\mathbb{Q}$-algebra embeddings $\sigma : K \hookrightarrow \mathbb{C}$. We say that such a σ is **real** if $\sigma(K) \subset \mathbb{R}$; otherwise we say that σ is **complex**. For any embedding σ, its complex conjugate $\overline{\sigma}$ defined by $x \mapsto \overline{\sigma(x)}$ is also an embedding. Clearly $\sigma = \overline{\sigma}$ if and only if σ is real, so complex embeddings come in conjugate pairs. (When we speak of a conjugate pair of embeddings, we will always mean complex embeddings: $\overline{\sigma} = \sigma$ does not count as a conjugate pair.)

We also say that $\alpha \in K$ is **primitive** if $\mathbb{Q} = K[\alpha]$.

EXERCISE 6.16. *Let $K_1, \ldots, m$ and $L_1, \ldots, L_n$ be fields. Suppose the rings $\prod_{i=1}^m K_i$ and $\prod_{j=1}^n L_j$ are isomorphic. Show: there is a bijection $s : \{1, \ldots, m\} \to \{1, \ldots, n\}$ such that for all $1 \le i \le m$, $K_i \cong L_{s(i)}$.*
(Suggestion: if $\iota : A \to B$ is an isomorphism of rings, then $\mathfrak{m} \mapsto \iota(\mathfrak{m})$ is a bijection from $\operatorname{MaxSpec} A$ to $\operatorname{MaxSpec} B$, and for all $\mathfrak{m} \in \operatorname{MaxSpec} A$, $\iota : A/\mathfrak{m} \cong B/\iota(\mathfrak{m})$. What are the maximal ideals and residue fields of $\prod_{i=1}^m K_i$?)

PROPOSITION 6.6. *Let $K/\mathbb{Q}$ be a degree N number field. The following are equivalent:*

(i) *Every embedding $\sigma : K \hookrightarrow \mathbb{C}$ is real.*

(ii) *Let $\alpha \in K$ be any primitive element, and let $f \in \mathbb{Q}[t]$ be the minimal polynomial of α. Then f splits into linear factors in $\mathbb{R}[t]$.*
(iii) *There is a primitive element $\alpha \in K$ whose minimal polynomial $f \in \mathbb{Q}[t]$ splits into linear factors in $\mathbb{R}$.*
(iv) *$\mathbb{R}$ is a splitting field for the étale $\mathbb{Q}$-algebra K.*

*When these equivalent conditions hold, we say that K is **totally real**.*

PROOF. (i) $\implies$ (ii): We go by contrapositive: suppose that there is a primitive element $\alpha \in K$ for which the minimal polynomial $f \in \mathbb{Q}$ does not split into linear factors over $\mathbb{R}$. Since $f \in \mathbb{R}[t]$ is separable, it thus factors as $f = gh$ wth $\gcd(g, h) = 1$ and h irreducible quadratic. Then there are preicsely two $\mathbb{R}$-algebra isomorphisms $\alpha_1, \alpha_2 : \mathbb{R}[t]/(g) \to \mathbb{C}$, such that $\alpha_2 = \overline{\alpha_1}$. For $i = 1, 2$, we define $\sigma_i : K \hookrightarrow \mathbb{C}$ as the composite

$$K \hookrightarrow K \otimes_{\mathbb{Q}} R \xrightarrow{\sim} \mathbb{R}[t]/(f) \to \mathbb{R}[t]/(g) \xrightarrow{\alpha_i} \mathbb{C}.$$

Then $\sigma_1(\alpha)$ and $\sigma_2(\alpha)$ are the two (distinct!) roots of g in $\mathbb{C}$, which are complex conjugates of each other, so σ_1 and σ_2 form a conjugate pair and thus are not real.
(ii) $\implies$ (iii) is immediate, from the Primitive Element Theorem.
(iii) $\implies$ (iv) $\implies$ (ii): Let $\alpha \in K$ be any primitive element, with minimal polynomial $f \in \mathbb{Q}[t]$, so f is monic, separable and irreducible. In $\mathbb{R}[t]$ the polynomial f factors as $l_1 \cdots l_r \cdot q_1 \cdots q_s$ where the l_i's are distinct monic linear polynomials and the q_j's are distinct monic irreducible quadratics, so the Chinese Remainder Theorem gives

$$K \otimes_{\mathbb{Q}} \mathbb{R} \cong \mathbb{R}[t]/(f) \cong \prod_{i=1}^{r} \mathbb{R}[t]/(l_i) \times \prod_{j=1}^{s} \mathbb{R}[t]/(q_j) \cong \mathbb{R}^r \times \mathbb{C}^s.$$

If (iii) holds, then for some f we get $r = N$ and $s = 0$, so $K \otimes_{\mathbb{Q}} \mathbb{R} \cong \mathbb{R}^N$ and thus $\mathbb{R}$ is a splitting field. If (iv) holds, then let f be the minimal polynomial of any primitive element of K; if factors in $\mathbb{R}$ into r linear polynomials and s irreducible quadratics, we have $\mathbb{R}^N \cong K \otimes_{\mathbb{Q}} \mathbb{R} \cong \mathbb{R}^r \times \mathbb{C}^s$, and by Exercise 6.16 we get $r = N$ and $s = 0$, so f splits into linear factors over $\mathbb{R}$.
(iii) $\implies$ (i): If the minimal polynomial of some primitive element α of K factors over $\mathbb{R}$ into $\prod_{i=1}^{N}(t - \alpha_i)$ then for all $1 \leq i \leq n$ there is a unique $\mathbb{Q}$-algebra embedding $\sigma_i : K \hookrightarrow \mathbb{R}$ such that $\sigma_i(\alpha) = \alpha_i$. This gives N real embeddings $\sigma : K \hookrightarrow \mathbb{C}$, which is all the embeddings, so every embedding is real. □

A number field K is **real** if it has at least one real embedding; otherwise it is **totally complex**.

EXERCISE 6.17. *Let $K/\mathbb{Q}$ be a finite Galois extension. Show: K is either totally real or totally complex.*

Our goal is to define, for any number field K of degree N, a $\mathbb{Q}$-algebra embedding

$$\sigma : K \hookrightarrow \mathbb{R}^N$$

such that $\sigma(I)$ is a lattice in $\mathbb{R}^N$ for every fractional $\mathbb{Z}_K$-ideal $I \subset K$ and such that $\delta(K)$ is closely related to $\operatorname{Covol} \mathbb{Z}_K$. Because every $I \in \operatorname{Frac} \mathbb{Z}_K$ is a $\mathbb{Z}$-lattice in the $\mathbb{Q}$-vector space K, from the perspective of our previous section, it is natural to consider $V \coloneqq K \otimes_{\mathbb{Q}} \mathbb{R}$. Then every $\mathbb{Z}$-lattice in K can naturally be viewed as a "rational" lattice in V, which is not $\mathbb{R}^N$ but is an N-dimensional $\mathbb{R}$-vector space.

The perspective of §6.1.4 now becomes pertinent: we do not have a canonical measure Vol on V but we will get one if we can endow V with an inner product.

The most obvious candiate for an inner product is the trace form $\langle \cdot, \cdot \rangle$ on the $\mathbb{R}$-algebra V. As mentioned in §6.1.4, what needs to be checked is whether $\langle \cdot, \cdot \rangle$ is positive definite. The answer is:

PROPOSITION 6.7. *The trace form on $K \otimes_{\mathbb{Q}} \mathbb{R}$ is positive definite if and only if K is totally real.*

PROOF. If K is totally real, then $K \otimes_{\mathbb{Q}} \mathbb{R} \cong \mathbb{R}^N$. Isomorphic algebras have isometric trace forms, and for the standard basis $e = (e_1, \ldots, e_N)$, we have $T(e_i e_j) = T(\delta(i,j)e_i) = \delta(i,j)$, so the Gram matrix G_e is the identity, i.e., the trace form is the standard dot product on $\mathbb{R}^N$, which is positive definite.
If K is not totally real, then we may write $K \otimes_{\mathbb{Q}} \mathbb{R}$ as $\mathbb{C} \times A$ for an étale $\mathbb{R}$-algebra A, and then the trace form on $K \otimes_{\mathbb{Q}} \mathbb{R}$ is the orthogonal direct sum of the trace forms on $\mathbb{C}$ and on A in the sense of Exercise 4.11. In particular, for all $x \in \mathbb{C}$ the trace of x is the trace of $(x, 0) \in K \otimes_{\mathbb{Q}} \mathbb{R}$. For $x = a + bi \in \mathbb{C}$, we have $T(x) = 2x$, so $\langle i, i \rangle = T(i^2) = -2$, showing that the trace form on $\mathbb{C}$ is not positive definite hence neither is the trace form on $K \otimes_{\mathbb{Q}} \mathbb{R}$. □

EXERCISE 6.18. *Suppose K is a degree N number field with r real embeddings and s conjugate pairs of complex embeddings. Show: there is an $\mathbb{R}$-basis $v = (v_1, \ldots, v_N)$ for which the Gram matrix G_v of the trace form on $K \otimes_{\mathbb{Q}} \mathbb{R}$ is the diagonal matrix with $r + s$ diagonal entries 1 and s diagonal entries -1.*

Now let $K/\mathbb{Q}$ be a totally real number field of degree N, with embeddings $\sigma_1, \ldots, \sigma_N : K \hookrightarrow \mathbb{R}$. We define the **additive embedding**

$$\sigma : K \hookrightarrow \mathbb{R}^N, x \mapsto (\sigma_1(x), \ldots, \sigma_N(x)).$$

The map σ has a unique extension to an $\mathbb{R}$-linear map $\Sigma : K \otimes_{\mathbb{Q}} \mathbb{R} \to \mathbb{R}^N$ which is the isomorphism of Proposition 5.7. This any $\mathbb{Z}$-lattice Λ in K is also a $\mathbb{Z}$-lattice in $K \otimes_{\mathbb{Q}} \mathbb{R}$, so $\sigma(\Lambda)$ is a lattice in $\mathbb{R}^N$. More concretely, let $\mathbf{x} = (x_1, \ldots, x_N)$ be an ordered $\mathbb{Q}$-basis for K, and let $\Lambda_{\mathbf{x}} \coloneqq \langle x_1, \ldots, x_N \rangle_{\mathbb{Z}}$ be the $\mathbb{Z}$-lattice in K that it spans. If we define

$$S(\mathbf{x}) \in \mathrm{GL}_N(\mathbb{R}) \text{ by } \sigma_i(x_j),$$

then the columns of $S(\mathbf{x})$ are the basis vectors $\sigma(x_1), \ldots, \sigma(x_N)$ of $\sigma(\Lambda_x)$, so

$$\mathrm{Covol}(\sigma(\Lambda_{\mathbf{x}})) = |\det S(\mathbf{x})|.$$

On the other hand, by (11) the Gram matrix for the trace form on $K/\mathbb{Q}$ with respect to the basis $\mathbf{x}$ is

$$G_{\mathbf{x}} = S(\mathbf{x})^T S(\mathbf{x}),$$

so we find:

$$(\mathrm{Covol}\, \Lambda_{\mathbf{x}})^2 = |\det S(\mathbf{x})|^2 = \det G_{\mathbf{x}} =: \delta_{\Lambda_{\mathbf{x}}}. \tag{29}$$

In fact we don't need the embedding σ to prove this: since K is totally real, the trace form $\langle \cdot, \cdot \rangle$ on $K \otimes_{\mathbb{Q}} \mathbb{R}$ makes it an inner product space, and then (29) is just Proposition 6.5. But the use of σ is entirely reasonable: the additive embedding σ is the restriction of the $\mathbb{R}$-algebra isomorphism $\Sigma : K \otimes_{\mathbb{Q}} \mathbb{R} \to \mathbb{R}^N$, and this algebra isomorphism induces an isomorphism from the inner product space $(K \otimes_{\mathbb{Q}} \mathbb{R}, \langle \cdot, \cdot \rangle)$ to $\mathbb{R}^N$ endowed with the standard dot product, so all we are doing is adjusting by a convenient isomorphism.

Now let $K/\mathbb{Q}$ be any degree N number field, with r real embeddings and s conjugate pairs of complex embeddings. We still wish to define an additive embedding $\sigma : K \hookrightarrow \mathbb{R}^N$. If we let $f \in \mathbb{Q}[t]$ be the minimal polynomial of a primitive element α of K, and factor $f \in \mathbb{R}[t]$ as $l_1(t)\cdots l_r(t)q_1(t)\cdots q_s(t)$ with the l_i's monic lineaer and the q_j's monic irreducible quadratic, then as above we have a canonical $\mathbb{R}$-algebra isomorphism

$$\Pi : K \otimes_{\mathbb{Q}} \mathbb{R} \xrightarrow{\sim} \mathbb{R}[t]/(f) \xrightarrow{\sim} \prod_{i=1}^{r} \mathbb{R}[t]/(l_i) \times \prod_{j=1}^{s} \mathbb{R}[t]/(q_j) = \mathbb{R}^r \times \prod_{j=1}^{s} \mathbb{R}[t]/(q_j).$$

For $1 \leq i \leq r+s$, let π_i be Π restricted to K followed by projection onto the ith factor. Then the maps $\pi_1, \ldots, \pi_r : K \hookrightarrow \mathbb{R}$ are precisely the real embeddings of K. Now let $r+1 \leq i \leq r+s$ and consider

$$\pi_i : K \to \mathbb{R}[t]/(q_{i-r}).$$

The $\mathbb{R}$-algebra $\mathbb{R}[t]/(q_{i-r})$ is isomorphic to $\mathbb{C}$ but in two different ways, each isomorphism being the other followed by complex conjugation. If for each such i we choose one of these two isomomorphisms $\iota_i : \mathbb{R}[t]/(q_{i-r}) \to \mathbb{C}$, then the maps $\{\iota_i \circ \pi_i : K \to \mathbb{C}\}_{r+1 \leq i \leq s}$ give s complex embeddings of K that represent precisely one of each conjguate pair of complex embeddings. Thus we get an $\mathbb{R}$-algebra isomorphism

$$\Sigma \coloneqq (1_{\mathbb{R}^r} \times (\iota_1, \ldots, \iota_s)) \circ \Pi : K \otimes_{\mathbb{R}} \to \mathbb{R}^r \times \mathbb{C}^s$$

whose restriction to K takes the form

$$\sigma = (\sigma_1, \ldots, \sigma_r, \sigma_{r+1}, \sigma_{r+3}, \ldots, \sigma_{r+2s-1}) : K \to \mathbb{R}^r \times \mathbb{C}^s$$

where $\sigma_1, \ldots, \sigma_r : K \hookrightarrow \mathbb{R}$ are the real embeddings of K and we have ordered the complex embeddings $\sigma_{r+1}, \ldots, \sigma_{2s}$ so that $\sigma_{r+2} = \overline{\sigma_{r+1}}, \ldots, \sigma_{r+2s} = \overline{\sigma_{r+2s-1}}$.

This is *almost* the additive embedding we want, except that we want it to land in $\mathbb{R}^N$ rather than $\mathbb{R}^r \times \mathbb{C}^s$. For this there is something obvious to try, although it is not so obvious how it will work out: namely, we may of course identify $\mathbb{C}$ as an $\mathbb{R}$-vector space with $\mathbb{R}^2$ via $z \mapsto (\Re(z), \Im(z))$. Doing this, we get our additive embedding

$$\sigma : K \hookrightarrow \mathbb{R}^N.$$

The issue of course is that $\mathbb{C}$ is not isomorphic to $\mathbb{R}^2$ as an $\mathbb{R}$-*algebra*, so if Λ is a $\mathbb{Z}$-lattice in K, it is no longer "abstractly clear" that the discriminant δ_Λ in our number-theoretic sense (i.e., with respect to the trace form on $K/\mathbb{Q}$) is equal to the discriminant of $\sigma(\Lambda)$ as a lattice in $\mathbb{R}^N$. In fact when $s \geq 1$ these two discriminants are not equal...but luckily, they are very closely related, as we will now see.

Example 6.8. *Let $D < 0$ be squarefree such that $D \equiv 2, 3 \pmod 4$, put $K \coloneqq \mathbb{Q}(\sqrt{D})$, so $\mathbb{Z}_K = \mathbb{Z}[\sqrt{D}]$ and $\delta_{\mathbb{Z}_K} = 4D$. There are two complex embeddings $\sigma_1, \sigma_2 : K \hookrightarrow \mathbb{C}$; we may view σ_1 as being inclusion and σ_2 as being complex conjugation. Once we identify $\mathbb{C}$ and $\mathbb{R}^2$ in the usual manner, we find that $\sigma(\mathbb{Z}_K)$ is the lattice with basis e_1 and $\sqrt{|D|}e_2$, so its covolume is $\sqrt{D}$. Its Gram matrix is $G \coloneqq \begin{bmatrix} 1 & 0 \\ 0 & |D| \end{bmatrix}$, with determinant $|D| = -D$. Thus in this case we have*

$$\delta_{\mathbb{Z}_K} = -4(\operatorname{Covol} \sigma(\mathbb{Z}_K))^2. \tag{30}$$

EXERCISE 6.19. *Let $D < 0$ be squarefree with $D \equiv 1 \pmod 4$. Show: (30) again holds.*

It turns out that some errant factors of -4 are the worst of it. Let $\Lambda_{\mathbf{x}}$ be the $\mathbb{Z}$-lattce in K spanned by the $\mathbb{Q}$-basis $\mathbf{x} = (x_1, \ldots, x_N)$ of K. Again we order the embeddings $\sigma_1, \ldots, \sigma_N : K \hookrightarrow \mathbb{C}$ so that the first r of them are real and then complex conjugate pairs are written consecutively. Since $\mathbb{C}$ is a splitting field for K, we can again use (11) to compute $\delta_{\Lambda_{\mathbf{x}}}$: if $S(\mathbf{x}) \in \mathrm{GL}_N(\mathbb{C})$ is the matrix with (i,j)-entry $\sigma_i(x_j)$, then

$$\delta_{\Lambda_{\mathbf{x}}} = (\det S(\mathbf{x}))^2.$$

On the other hand, $\operatorname{Covol} \Lambda_{\mathbf{x}}$ is $|\det T(\mathbf{x})|$, were $T(\mathbf{x})$ is the matrix whose jth column is

$$(\sigma_1(x_j), \ldots, \sigma_r(x_j), \Re(\sigma_{r+1}(x_j)), \Im(\sigma_{r+1}(x_j)), \ldots, \Re(\sigma_{r+2s-1}(x_j)), \Im(\sigma_{r+2s-1}(x_j))).$$

Then we have:

LEMMA 6.9. *With notation as above,*

$$\det T(\mathbf{x}) = \left(\frac{\sqrt{-1}}{2}\right)^s \det S(\mathbf{x}).$$

PROOF. Each of first r rows of $T(\mathbf{x})$ is the same as the corresponding row of $S(\mathbf{x})$; the remaining rows correspond to conjugate pairs of complex embeddings, and where in $S(\mathbf{x})$ we have $\sigma_i(x_j)$ and $\overline{\sigma_i(x_j)}$, in $T(\mathbf{x})$ we have $\Re(\sigma_i(x_j))$ and $\Im(\sigma_i(x_j))$. If we call the two rows of the first matrix R_1 and R_2 and the two rows of the second matrix R_3 and R_4, then we have

$$R_3 = \frac{R_1 + R_2}{2}, \ R_4 = \frac{R_1 - R_2}{2\sqrt{-1}}.$$

Thus we can get from the first two rows the second two rows by row operations, which changes the determinant by a factor of $\frac{i}{2}$. This occurs s times in all, so

$$\det T(\mathbf{x}) = \left(\frac{i}{2}\right)^s \det S(\mathbf{x}). \qquad \square$$

We deduce:

THEOREM 6.10. *Let $\sigma : K \hookrightarrow \mathbb{R}^N$ be the additive embedding as defined above, and let Λ be a $\mathbb{Z}$-lattice in K. Then:*

$$\delta_\Lambda = (-4)^s (\operatorname{Covol} \sigma(\Lambda))^2.$$

PROOF. Using Lemma 6.9, we have

$$\delta_\Lambda = (\det S(\mathbf{x}))^2 = ((-2i)^s \det T(\mathbf{x}))^2 = (-4)^s (\det T(\mathbf{x}))^2 = (-4)^s \operatorname{Covol}(\Lambda)^2. \ \square$$

As an interesting byproduct of our approach, we deduce a result of Brill. Recall the **signum** (or sign) function

$$\operatorname{sgn} : \mathbb{R} \to \mathbb{R}, x \mapsto \begin{cases} 1 & x > 0 \\ 0 & x = 0 \\ -1 & x < 0 \end{cases}.$$

Then immediately from Theorem 6.10 we get:

THEOREM 6.11. *Let K be a number field of degree N, with s complex conjugate pairs of complex embeddings. Then:*

$$\operatorname{sgn}(\delta_K) = (-1)^s.$$

If we wanted to, we could set things up so as not to get the factor of 4^s. As we saw, it came from our identification of $\mathbb{R}^r \times \mathbb{C}^s$ with $\mathbb{R}^{r+2s}$. If intead we took the Haar measure on each factor $\mathbb{C}$ to be *twice* the standard Lebesgue measure, then this factor would disappear. This convention is sometimes taken: see e.g. [**Clxx**].

2.2. A Standard Volume Calculation.

PROPOSITION 6.12. *Let $r, s \in \mathbb{N}$, $n = r + 2s$, $t \in \mathbb{R}$, and let*

$$B_t = \{(y_1, \ldots, y_r, z_1, \ldots, z_s) \in \mathbb{R}^r \times \mathbb{C}^s \mid \sum_{i=1}^{r} |y_i| + 2\sum_{j=1}^{s} |z_j| \leq t\}.$$

Then for all $t \geq 0$, we have that B_t is a compact, convex body and

$$\operatorname{Vol} B_t = 2^r \left(\frac{\pi}{2}\right)^s \frac{t^n}{n!}.$$

EXERCISE 6.20. *Prove Proposition 6.12. (Cf.* [**S**, pp. 66-67]*.)*

2.3. Finiteness of the Ideal Class Monoid.

For a number field K of degree $N = r + 2s$, we define the **Minkowski constant**

$$M(K) = \left(\frac{4}{\pi}\right)^s \frac{N!}{N^N} |\delta_K|^{\frac{1}{2}}.$$

THEOREM 6.13. *Let $\mathfrak{a}$ be a nonzero integral ideal of $\mathbb{Z}_K$. Then $\mathfrak{a}$ contains a nonzero element x such that*

$$|N_{K/\mathbb{Q}}(x)| \leq M(K) N(\mathfrak{a}).$$

PROOF. Let $\sigma : K \to \mathbb{R}^r \times \mathbb{C}^s$ be the canonical embedding. Let $t \in \mathbb{R}^{>0}$, and as in Proposition 6.12 put

$$B_t = \{(y_1, \ldots, y_r, z_1, \ldots, z_s) \in \mathbb{R}^r \times \mathbb{C}^s \mid \sum_{i=1}^{r} |y_i| + 2\sum_{j=1}^{s} |z_j| \leq t\}.$$

B_t is a compact, convex body (Proposition 6.12). Choose t such that

$$2^r \left(\frac{\pi}{2}\right)^s \frac{t^N}{N!} = \operatorname{Vol} B_t = 2^N \operatorname{Covol} \mathfrak{a} = 2^N 2^{-s} \sqrt{|\delta_K|} N(\mathfrak{a}),$$

i.e., such that

$$t^N = 2^{N-r} \pi^{-s} N! \sqrt{|\delta_K|} N(\mathfrak{a}).$$

By Minkowski's Convex Body Theorem, there is $x \in \mathfrak{a}^\bullet$ such that $\sigma(x) \in B_t$, so

$$|N_{K/\mathbb{Q}}(x)| = \prod_{i=1}^{r} |\sigma_i(x)| \prod_{j=r+1}^{r+s} |\sigma_j(x)|^2 \leq \left(\frac{1}{N}\sum_{i=1}^{r} |\sigma_i(x)| + \frac{2}{N}\sum_{j=r+1}^{r+s} |\sigma_j(x)|\right)^N \leq \frac{t^N}{N^N}$$

$$= \left(\frac{4}{\pi}\right)^s \frac{N!}{N^N} \sqrt{|\delta_K|} N(\mathfrak{a}) = M(K) N(\mathfrak{a});$$

the first inequality uses the AGM Inequality and the second the definition of B_t. □

LEMMA 6.14. *Let K be a number field of degree N, and let $r \in \mathbb{Z}^+$. Then*

$$\#\{\mathfrak{a} \in \operatorname{Frac} \mathbb{Z}_K \mid \mathfrak{a} \supset \mathbb{Z}_K,\ [\mathfrak{a} : \mathbb{Z}_K] = r\} \leq 2^{r^N} < \infty.$$

PROOF. If $\mathfrak{a} \supset \mathbb{Z}_K$ and $[\mathfrak{a} : \mathbb{Z}_K] = r$, then $r\mathfrak{a} \subseteq \mathbb{Z}_K$ and thus

$$\mathbb{Z}_K \subseteq \mathfrak{a} \subseteq \frac{1}{r}\mathbb{Z}_K.$$

Since $\frac{\frac{1}{r}\mathbb{Z}_K}{\mathbb{Z}_K} \cong (\mathbb{Z}/r\mathbb{Z})^n$, there are at most as many choices of $\mathfrak{a}$ as there are subsets of an r^n-element set (of course this is a ridiculously crude upper bound). □

COROLLARY 6.15. *Let K be a number field. Then $\operatorname{Pic} \mathbb{Z}_K$ is finite.*

PROOF. By Lemma 6.14 the set of fractional $\mathbb{Z}_K$-ideals containing $\mathbb{Z}_K$ with index at most $M(K)$ is finite: let us call these fractional ideals $I_1, \ldots, I_c$. Let $\mathfrak{a} \in \operatorname{Frac} \mathbb{Z}_K$. By Theorem 6.13, there is $\alpha \in \mathfrak{a}^\bullet$ such that

$$[\mathbb{Z}_K : \alpha\mathbb{Z}_K] = |N_{K/\mathbb{Q}}(\alpha)| \leq M(K)N(\mathfrak{a}) = M(K)[\mathbb{Z}_K : \mathfrak{a}],$$

and thus we have

$$\left[\frac{1}{\alpha}\mathfrak{a} : \mathbb{Z}_K\right] = [\mathfrak{a} : \alpha\mathbb{Z}_K] = \frac{[\mathbb{Z}_K : \alpha\mathbb{Z}_K]}{[\mathbb{Z}_K : \mathfrak{a}]} \leq M(K).$$

It follows that there is some $1 \leq i \leq c$ such that $\frac{1}{\alpha}\mathfrak{a} = I_i$ and thus $\mathfrak{a} = \alpha I_i$. It follows that $\#\operatorname{Pic} \mathbb{Z}_K \leq c$. □

EXERCISE 6.21. *Let K be a number field. Show: $\operatorname{Pic} \mathbb{Z}_K$ is generated by classes of $I \in \operatorname{Int} \mathbb{Z}_K$ such that $N(I) \leq M_K$.*

Although we only recorded that $\operatorname{Pic} \mathbb{Z}_K$ is finite, the proof gives an explicit (though not very good) upper bound on $\#\operatorname{Pic} \mathbb{Z}_K$ in terms of n, r, s and $|\delta_K|$.

Next we observe that in the above argument, we never inverted any nonprincipal ideal, so we have not used that we were working in the Dedekind domain $\mathbb{Z}_K$ in any crucial way. So in fact we can prove a more general finiteness result: let $\mathcal{O} \subseteq \mathbb{Z}_K$ be any $\mathbb{Z}$-order in K: i.e., a $\mathbb{Z}$-lattice in K that is a subring.

For any domain R with fraction field K, we define the **ideal class monoid** $\operatorname{ICM}(R)$: we introduce an equivalence relation $\sim$ on $\operatorname{Frac} R$: $\mathfrak{a} \sim \mathfrak{b}$ if there are $\alpha, \beta \in K^\times$ such that $\alpha\mathfrak{a} = \beta\mathfrak{b}$. (The fact that principal fractional ideals are invertible makes this relation transitive.) Then $\operatorname{ICM}(R)$ is the set of equivalence classes. It is easy to see that if $\mathfrak{a}_1 \sim \mathfrak{b}_1$ and $\mathfrak{a}_2 \sim \mathfrak{b}_2$ then $\mathfrak{a}_1\mathfrak{a}_2 \sim \mathfrak{b}_1\mathfrak{b}_2$, so the multiplication of fractional ideals descends to a binary operation on equivalence classes that makes $\operatorname{ICM}(R)$ into a commutative monoid. Moreover, by definition of a fractional ideal, every nonzero fractional ideal is equivalent to a nonzero integral ideal, so $\operatorname{ICM}(R)$ may also be viewed as equivalence classes of nonzero integral ideals. Finally, we have:

$$\operatorname{ICM}(R)^\times = \operatorname{Pic}(R).$$

That is, the group of invertible elements is precisely the Picard group.

Now let $\mathcal{O}$ be a $\mathbb{Z}$-order in K: that is, a $\mathbb{Z}$-lattice in K that is also a subring. Since $\mathcal{O}$ is finitely generated over $\mathbb{Z}$, every element is integral over $\mathbb{Z}$, so $\mathcal{O} \subseteq \mathbb{Z}_K$, with finite index.

The following exercise is essentially asking you to revisit everything that we have done in this section and realize that we could have worked a bit more generally, in particular with ideals of $\mathcal{O}$.

EXERCISE 6.22. *Let $\mathcal{O}$ be an order in K, and put $f := [\mathbb{Z}_K : \mathcal{O}]$. Let $\mathfrak{a}$ be a nonzero $\mathcal{O}$-ideal.*

a) *Show: $\sigma(\mathfrak{a})$ is a lattice in $\mathbb{R}^N$ of covolume $2^{-s} f \sqrt{|\delta_K|}[\mathcal{O} : \mathfrak{a}]$.*

b) *Show: there is $x \in \mathfrak{a}^\bullet$ such that*

$$|N_{K/\mathbb{Q}}(x)| \leq f[\mathcal{O} : \mathfrak{a}]M(K).$$

c) *Show:* $\mathrm{ICM}(\mathcal{O})$ *is finite. Thus also* $\mathrm{Pic}(\mathcal{O})$ *is finite.*

When we study nonmaximal orders more deeply[3] we will learn that in fact the natural map $\operatorname{Pic}\mathcal{O} \to \operatorname{Pic}\mathbb{Z}_K$ given by pushing forward fractional ideals is a surjection, so $\#\operatorname{Pic}\mathbb{Z}_K \mid \#\operatorname{Pic}\mathcal{O}$, and moreover there is a nice formula for $\frac{\#\operatorname{Pic}\mathcal{O}}{\#\operatorname{Pic}\mathbb{Z}_K}$. In other words, $\operatorname{Pic}\mathcal{O}$ is rather well-understood in terms of $\operatorname{Pic}\mathbb{Z}_K$, so proving the finiteness of $\operatorname{Pic}\mathcal{O}$ is not much of an additional contribution. However we showed that the set of classes of *not necessarily invertible* $\mathcal{O}$-ideals is still finite. This is interesting! In general, $\mathrm{ICM}(\mathcal{O})$ is much less well understood than $\operatorname{Pic}\mathcal{O}$.

3. Discriminant Bounds and Hermite's Theorem

THEOREM 6.16. *(Minkowski) Let K be a number field of degree $N \geq 2$ with s complex places.*

a) *We have*

$$|\delta_K| \geq \left(\frac{\pi}{4}\right)^{2s} \frac{N^{2N}}{(N!)^2} \geq \frac{\pi}{3}\left(\frac{3\pi}{4}\right)^{N-1}.$$

b) *We have $|\delta_K| > 1$. That is, at least one prime p ramifies in K.*

PROOF. a) Applying Theorem 6.13 with $\mathfrak{a} = \mathbb{Z}_K$, we get: there is $x \in \mathbb{Z}_K^\bullet$ such that

$$|N_{K/\mathbb{Q}}(x)| \leq M(K).$$

Because $|N_{K/\mathbb{Q}}(x)| = \#\mathbb{Z}_K/(x)$, certainly $1 \leq |N_{K/\mathbb{Q}}(x)|$, and we deduce

$$1 \leq M(K) = \left(\frac{4}{\pi}\right)^s \frac{N!}{N^N}|\delta_K|^{\frac{1}{2}}.$$

Thus

$$|\delta_K| \geq \left(\frac{\pi}{4}\right)^{2s} \frac{N^{2N}}{(N!)^2} \geq \left(\frac{\pi}{4}\right)^{N} \frac{N^{2N}}{(N!)^2} =: a_N.$$

We have

$$a_2 = \frac{\pi^2}{4},$$

and the binomial theorem gives

$$\frac{a_{N+1}}{a_N} = \frac{\pi}{4}\left(1 + \frac{1}{N}\right)^{2N} \geq \frac{3\pi}{4}.$$

Thus for $N \geq 2$,

$$|\delta_K| \geq \frac{\pi^2}{4}\left(\frac{3\pi}{4}\right)^{N-2} = \frac{\pi}{3}\left(\frac{3\pi}{4}\right)^{N-1}.$$

[3]Unfortunately this does not take place in the current draft! But see [**N**, §1.12].

b) If $N \geq 2$, then $|\delta_K| \geq \frac{\pi}{3} \cdot \frac{3\pi}{4} = \frac{\pi^2}{4} > 1$. □

EXERCISE 6.23. *Let K be a number field with r real embeddings, s pairs of complex embeddings and degree N.*

a) *Use Theorem 6.16a) to show:*
   (i) *If $(r,s) = (2,0)$, then $\delta_K \geq 4$. There is no such K with $\delta_K = 4$, but there is with $\delta_K = 5$.*
   (ii) *If $(r,s) = (0,1)$, then $\delta_K = -3$. There is such a K with $\delta_K = -3$.*
   (iii) *If $(r,s) = (3,0)$, then $\delta_K \geq 21$.*
   (iv) *If $(r,s) = (1,1)$, then $\delta_K \leq -13$.*
   (v) *If $N \geq 4$, then $|\delta_K| \geq 44$.*

b) *Show: if $d \in \{\pm 1, \pm 2, 3, 4, 6, 7, 9, 10, 11, -12\}$, then there is no number field with discriminant d.*

Later we will show that for any number field K we have $\delta_K \equiv 0, 1 \pmod 4$ (Theorem 7.3). In view of this, the most interesting parts of Exercise 6.23b) are that 4, 9 and -12 are not discriminants of number fields.

EXERCISE 6.24. *Show that the cubic field $K := \mathbb{Q}[t]/(t^3 - t^2 - 1)$ has discriminant -23.*

The LMFDB contains the complete list of all cubic number fields K with $|\delta_K| \leq 3,375,000$. For instance there are nine cubic fields with $|\delta_K| \leq 100$:

(i) $\mathbb{Q}[t]/(t^3 - t^2 - 1)$, with $\delta_K = -23$;
(ii) $\mathbb{Q}[t]/(t^3 + t - 1)$, with $\delta_K = -31$;
(iii) $\mathbb{Q}[t]/(t^3 - t^2 + t + 1)$, with $\delta_K = -44$;
(iv) $\mathbb{Q}[t]/(t^3 - t^2 - 2t + 1)$, with $\delta_K = 49$;
(v) $\mathbb{Q}[t]/(t^3 + 2t - 1)$, with $\delta_K = -59$;
(vi) $\mathbb{Q}[t]/(t^3 - 2t - 2)$, with $\delta_K = -76$;
(vii) $\mathbb{Q}[t]/(t^3 - 3t - 1)$, with $\delta_K = 81$;
(viii) $\mathbb{Q}[t]/(t^3 - t^2 + t - 2)$, with $\delta_K = 83$;
(ix) $\mathbb{Q}[t]/(t^3 - t^2 + 2t + 1)$, with $\delta_K = -87$.

EXERCISE 6.25. *The LMFDB contains complete tables of number fields of small degree and small discriminants: see* `http://www.lmfdb.org/NumberField/Completeness`. *In particular, it contains tables of all number fields K of degree $3 \leq n \leq 7$ and all degree 8 number fields that are not totally real with $|\delta_K| \leq 10^6$.*

a) *Show: if K is a totally real number field of degree 8 then $|\delta_K| \geq 173,141$ and if K is a number field of degree at least 9 then $|\delta_K| \geq 165,029$.*
b) *Thus the LMFDB tables allow the complete determination of all $d \in \mathbb{Z}$ with $|d| \leq 165,028$ such that d is the discriminant of some number field. What is this list of d?*

Our next theorem is of the form: "there are only finitely many number fields such that..." Since so far for us a number field is just a finite degree field extension of $\mathbb{Q}$, there is a shallow set-theoretic problem here. For instance, consider the number fields $\mathbb{Q}[x]/(x^2+1)$ and $\mathbb{Q}[x]/(x^2 - 2x + 2)$. The first field is isomorphic to $\mathbb{Q}[i]$ and the second field is isomorphic to $\mathbb{Q}[1+i]$; but $\mathbb{Q}[1+i] = \mathbb{Q}[i]$, so the two fields $\mathbb{Q}[x]/(x^2+1)$ and $\mathbb{Q}[x]/(x^2-2x+2)$ are isomorphic. But are they *equal*? The answer is no, but the question is not so great either. It would be better not to

distinguish between isomorphic number fields.

However there is another approach that is often better still. Let $\overline{\mathbb{Q}}$ be the algebraic closure of $\mathbb{Q}$ that lives inside $\mathbb{C}$: that is, the integral closure of $\mathbb{Q}$ in $\mathbb{C}$. We can then think of number fields as being the subfields of $\overline{\mathbb{Q}}$ that have finite degree over $\mathbb{Q}$. Every abstract number field K can be embedded inside $\overline{\mathbb{Q}}$: indeed, we know that the number of such embeddings is $N = [K : \mathbb{Q}]$. The field $K/\mathbb{Q}$ is Galois if and only if for any two embeddings $\sigma_i, \sigma_j : K \hookrightarrow \overline{\mathbb{Q}}$ we have $\sigma_i(K) = \sigma_j(K)$. In general, these isomorphic but possibly distinct subfields of $\overline{\mathbb{Q}}$ are called the **conjugates** of $\sigma_1(K)$ over $\mathbb{Q}$. So an abstract number field may have multiple isomorphic copies inside $\overline{\mathbb{Q}}$, but at most $[K : \mathbb{Q}]$ so certainly *finitely many*. Therefore any statement about finiteness of a class of number fields means the same thing if we count isomorphism classes as it does if we count subfields of $\overline{\mathbb{Q}}$. We will always interpret finiteness statements in these equivalent ways.

THEOREM 6.17 (Hermite I). *For all $d \in \mathbb{Z}$, there are only finitely many number fields with discriminant d.*

PROOF. By Theorem 6.16, it suffices to show that for any fixed $r, s \in \mathbb{N}$, there are only finitely many number fields with r real places, s complex places, degree $N = r + 2s$ and discriminant d. We may, and shall, assume that $N \geq 2$. Let K be such a number field.

Let $B \subseteq \mathbb{R}^r \times \mathbb{C}^s$ be as defined as follows:
• If $r > 0$, $B = (y_1, \ldots, y_r, z_1, \ldots, z_s) \in \mathbb{R}^N$ such that $|y_1| \leq 2^{N-1} \left(\frac{\pi}{2}\right)^{-s} \sqrt{|d|}$, $|y_i| \leq \frac{1}{2}$ for $2 \leq i \leq r$, and $|z_j| \leq \frac{1}{2}$ for $1 \leq j \leq s$.
• if $r = 0$, $B = (y_1, \ldots, y_r, z_1, \ldots, z_s) \in \mathbb{R}^N$ such that $|z_1 - \overline{z_1}| \leq 2^N \left(\frac{\pi}{2}\right)^{1-s} \sqrt{|d|}$, $|z_1 + \overline{z_1}| \leq \frac{1}{2}$ and $|z_j| \leq \frac{1}{2}$ for $2 \leq j \leq s$.

We leave it as an exercise to show that B is a compact, convex body, and

$$\operatorname{Vol} B = 2^{N-s}\sqrt{|d|}.$$

By Theorem 6.10, the lattice $\sigma(\mathbb{Z}_K)$ has covolume

$$2^{-s}\sqrt{|d|},$$

so – what luck! – we have $\operatorname{Vol} B = 2^N \operatorname{Covol} \sigma(\mathbb{Z}_K)$. Thus Minkowski's Convex Body Theorem applies to give us $x \in \mathbb{Z}_K^\bullet$ such that $\sigma(x) \in B$.

We claim x is a primitive element of K, i.e., that $K = \mathbb{Q}[x]$. Suppose first that $r > 0$, so $|\sigma_i(x)| \leq \frac{1}{2}$ for all $i \geq 2$. Since

$$|N_{K/\mathbb{Q}}(x)| = \prod_{i=1}^{N} |\sigma_i(x)| \in \mathbb{Z}^+,$$

we must have $|\sigma_1(x)| > 1$. Thus we have $\sigma_1(x) \neq \sigma_i(x)$ for all $i \geq 2$, and it follows that x is a primitive element for K. (Cf. [**Cl-FT**, Thm. 5.5].) Similarly, if $r = 0$, then $|\sigma_1(x)| = |\overline{\sigma_1(x)}| \geq 1$. Moreover one of the defining conditions for B gives $|\Re(\sigma_1(x))| \leq \frac{1}{4}$, so it follows that $\sigma_1(x)$ is not real. Thus again we have $\sigma_1(x) \neq \sigma_i(x)$ for all ≥ 2, so x is a primitive element for K.

Let $f = \prod_{i=1}^n (t - \sigma_i(x)) \in \mathbb{Z}[t]$ be the minimal polynomial for x. The inequalities defining B show that all the conjugates $\sigma_i(x)$ are bounded, hence coefficients of the minimal polynomial of x, being elementary symmetric functions in the $\sigma_i(x)$'s,

are also bounded, and this gives finitely many choices for x and thus finitely many choices for K. □

EXERCISE 6.26. *Let A be a Dedekind domain with fraction field K, let L/K be a degree N separable field extension, and let B be the integral closure of A in L. Let $\mathfrak{p} \in \operatorname{MaxSpec} A$ and let $\mathcal{P} \in \operatorname{MaxSpec} B$ lying over $\mathfrak{p}$. Let e be the ramification index of $\mathcal{P}/\mathfrak{p}$. Let $v_{\mathfrak{p}}$ be the $\mathfrak{p}$-adic valuation on K and let $v_{\mathcal{P}}$ be the $\mathcal{P}$-adic valuation on L. Show:*

$$\forall x \in K^\times,\ v_{\mathcal{P}}(x) = e v_{\mathfrak{p}}(x).$$

LEMMA 6.18. *Let $K/\mathbb{Q}$ be a number field of degree $N \geq 2$. For each prime number p, we have*

$$v_p(\delta_K) \leq N\lfloor \log_p N \rfloor + N - 1 \leq N\lfloor \log_2 N \rfloor + N - 1.$$

PROOF. We have

$$v_p(\delta_K) = v_p(N_{K/\mathbb{Q}}(\Delta_{K/\mathbb{Q}})) = \sum_{\mathcal{P}|p} f_{\mathcal{P}} v_{\mathcal{P}}(\Delta_K).$$

Since $e_{\mathcal{P}} \leq N$ we have $v_p(e_{\mathcal{P}}) \leq \lfloor \log_p N \rfloor$, so by Exercise 6.26 we have

$$v_{\mathcal{P}}(e_{\mathcal{P}}) \leq e_{\mathcal{P}} \lfloor \log_p N \rfloor.$$

Using this together with (27), we get

$$v_{\mathcal{P}}(\Delta_K) \leq e_{\mathcal{P}} - 1 + v_{\mathcal{P}}(e_{\mathcal{P}}) = e_{\mathcal{P}} - 1 + e_{\mathcal{P}} v_p(e_{\mathcal{P}}) \leq e_{\mathcal{P}} - 1 + e_{\mathcal{P}} \lfloor \log_p N \rfloor,$$

so

$$v_p(\delta_K) = \sum_{\mathcal{P}|p} f_{\mathcal{P}} v_{\mathcal{P}}(\Delta_K) \leq \sum_{\mathcal{P}|p} f_{\mathcal{P}} \left(e_{\mathcal{P}} - 1 + e_{\mathcal{P}} \lfloor \log_p N \rfloor \right)$$

$$= N + N\lfloor \log_p N \rfloor - \sum_{\mathcal{P}|p} f_{\mathcal{P}} \leq N\lfloor \log_p N \rfloor + N - 1. \qquad \square.$$

THEOREM 6.19 (Hermite's Theorem II). *Let S be a finite set of prime numbers, and let $N \in \mathbb{Z}^+$. Then there are only finitely many number fields K of degree N that are unramified outside S.*

PROOF. Let $p_1 < \ldots < p_r$ be the primes of S. If K is a degree N number field that is unramified outside of S then $|\delta_K| = p_1^{a_1} \cdots p_r^{a_r}$ for some $a_1, \ldots, a_r \in \mathbb{Z}^{\geq 0}$. By Lemma 6.18 the exponents $a_1, \ldots, a_r$ are bounded in terms of N, so there are only finitely many possibilities for δ_K, and by Hermite's Theorem I there are only finitely many number fields with any given discriminant. □

4. The Dirichlet Unit Theorem

Let K be a number field. For $x \in K$, we will abbreviate $N_{K/\mathbb{Q}}(x)$ to $N(x)$.

We wish to study the structure of the unit group $\mathbb{Z}_K^\times$.

LEMMA 6.20. *For $x \in \mathbb{Z}_K$, the following are equivalent:*

(i) *We have $x \in \mathbb{Z}_K^\times$.*
(ii) *We have $|N(x)| = 1$.*

PROOF. If $x \in \mathbb{Z}_K^\times$, there is $y \in \mathbb{Z}_K^\times$ such that $xy = 1$, and then

$$|N(x)||N(y)| = |N(xy)| = |N(1)| = 1.$$

Since $|N(x)|, |N(y)| \in \mathbb{Z}^+$, this forces $|N(x)| = 1$. Conversely, if $|N(x)| = 1$, the minimal polynomial of x over $\mathbb{Q}$ is $x^n + a_{n-1}x^{n-1} + \ldots + a_1 x \pm 1 = 0$ (cf. Proposition 5.10a)), so $x \cdot (x^{n-1} + a_{n-1}x^{n-2} + \ldots + a_1) = \pm 1$, so $x \in \mathbb{Z}_K^\times$. □

EXERCISE 6.27. *Let K be a number field, and let $\zeta \in K$ be a root of unity: that is, $\zeta^n = 1$ for some $n \in \mathbb{Z}^+$. Show: $\zeta \in \mathbb{Z}_K^\times$.*

THEOREM 6.21 (Dirichlet Unit Theorem). *Let K be a number field of degree $n = r + 2s$. Then $\mathbb{Z}_K^\times$ is a finitely generated abelian group, with free rank $r + s - 1$ and torsion subgroup the group $\mu(K)$ of roots of unity in K, which is finite.*

PROOF. Let $\sigma_1, \ldots, \sigma_r : K \hookrightarrow \mathbb{R}$ be the real embeddings, and let $\sigma_{r+1}, \ldots, \sigma_{r+s} : K \hookrightarrow \mathbb{C}$ be complex embeddings, no two of which are complex conjugate. We define the **multiplicative embedding**, a homomorphism $L : \mathbb{Z}_K \setminus \{0\} \to \mathbb{R}^{r+s}$, by

$$L : x \mapsto (\log|\sigma_1(x)|, \ldots, \log|\sigma_{r+s}(x)|).$$

Step 1: We claim that for any compact subset $B \subseteq \mathbb{R}^{r+s}$, its preimage

$$B' := L^{-1}(B)$$

is finite. Because B is bounded, there is $\alpha > 1$ such that:

$$\forall x \in B',\ \forall 1 \le i \le r+s,\ |\sigma_i(x)| \le \alpha.$$

It follows that the coefficients of the characteristic polynomial of an element $x \in B'$ are bounded; since these coefficients lie in $\mathbb{Z}$, there are therefore only finitely many such polynomials and hence only finitely many elements of B'.
Step 2: It follows from Step 1 that $L^{-1}(0) = \operatorname{Ker} L$ is finite. In particular, each element of $\operatorname{Ker} L$ has finite order, i.e., is a root of unity. Conversely, since L is a homomorphism of $\mathbb{Z}$-modules, we have

$$L(\mathbb{Z}_K^\times[\text{tors}]) \subseteq \mathbb{R}^{r+s}[\text{tors}] = \{0\}.$$

So $\mathbb{Z}_K^\times[\text{tors}]$ —- i.e., the set of roots of unity in K — lies in $L^{-1}(0)$.
Step 3: It follows from Step 1 that $L(\mathbb{Z}_K^\times)$ is a discrete subgroup of $\mathbb{R}^{r+s}$, hence free abelian of rank at most $r + s$. Moreover, for $x \in \mathbb{Z}_K^\times$, by Lemma 6.20 we have

$$\pm 1 = N(x) = \prod_{i=1}^{n} \sigma_i(x) = \prod_{i=1}^{r} \sigma_i(x) \prod_{j=r+1}^{r+s} \sigma_j(x)\overline{\sigma_j(x)},$$

hence $L(x)$ lies in the hyperplane

$$W : \sum_{i=1}^{r} y_i + 2 \sum_{j=r+1}^{r+s} y_j = 0.$$

Thus

$$L(\mathbb{Z}_K^\times) \subseteq W \cong \mathbb{R}^{r+s-1},$$

so in fact $L(\mathbb{Z}_K^\times)$ is free abelian of rank at most $r + s - 1$.
Step 4: The last, most delicate part of the argument, is to show that $L(\mathbb{Z}_K^\times)$ has rank $r + s - 1$. We show this by a duality argument: for any nonzero linear form $f : W \to \mathbb{R}$, we claim there exists $u \in \mathbb{Z}_K^\times$ such that $f(L(u)) \neq 0$. From this it

follows that $\langle L(\mathbb{Z}_K^\times)\rangle_\mathbb{R} = W$, so $L(\mathbb{Z}_K^\times) \cong \mathbb{Z}^{r+s-1}$.

Put $M \coloneqq r+s-1$. The map

$$\pi : W \to \mathbb{R}^M,\ (y_1, \dots, y_{r+s}) \mapsto (y_1, \dots, y_{r+s-1})$$

is an $\mathbb{R}$-linear isomorphism, so for any $y = (y_1, \dots, y_{M+1}) \in W$, we may write

$$f(y) = c_1 y_1 + \ldots + c_M y_M,\ c_i \in \mathbb{R}.$$

Fix a real number $\alpha \geq 2^N \left(\frac{1}{2\pi}\right)^s \sqrt{|\delta_K|}$. For any $\lambda = (\lambda_1, \dots, \lambda_M)$ with $\lambda_i > 0$ for all i, choose $\lambda_{M+1} > 0$ such that

$$\prod_{i=1}^{r} \lambda_i \prod_{j=r+1}^{r+s} \lambda_j^2 = \alpha.$$

In $\mathbb{R}^r \times \mathbb{C}^s$, the set B of elements $(y_1, \dots, y_r, z_1, \dots, z_s)$ with $|y_i| \leq \lambda_i$ and $|z_j| \leq \lambda_{r+j}$ is a compact, symmetric convex set of volume

$$\prod_{i=1}^{r} 2\lambda_i \prod_{j=r+1}^{r+s} \pi\lambda_j^2 = 2^r \pi^s \alpha \geq 2^{N-s}\sqrt{|\delta_K|}.$$

By Minkowski's Convex Body Theorem and Theorem 6.10 there is $x_\lambda \in \mathbb{Z}_K^\bullet$ such that $\sigma(x_\lambda) \in B$. Thus

$$1 \leq |N(x_\lambda)| = \prod_{i=1}^{N} |\sigma_i(x_\lambda)| \leq \prod_{i=1}^{r} \lambda_i \prod_{j=r+1}^{r+s} \lambda_j^2 = \alpha.$$

Moreover, for all $1 \leq i \leq M$, we have

$$|\sigma_i(x_\lambda)| = |N(x_\lambda)| \prod_{j \neq i} |\sigma_j(x_\lambda)|^{-1} \geq \prod_{j \neq i} \lambda_j^{-1} = \lambda_i \alpha^{-1}$$

so

$$\lambda_i \alpha^{-1} \leq |\sigma_i(x_\lambda)| \leq \lambda_i,$$

hence

$$0 \leq \log \lambda_i - \log |\sigma_i(x_\lambda)| \leq \log \alpha.$$

Applying the linear form f we get

$$\left| f(L(x_\lambda)) - \sum_{i=1}^{M} c_i \log \lambda_i \right| \leq \left(\sum_{i=1}^{M} |c_i| \right) \log \alpha =: \gamma,$$

say. Let $\beta > \gamma$ be a constant, and for each $h \in \mathbb{Z}^+$, choose positive real numbers $\lambda_{1,h}, \dots, \lambda_{M,h}$ such that $\sum_{i=1}^{M} c_i \log \lambda_{i,h} = 2\beta h$. Put $\lambda(h) = (\lambda_{1,h}, \dots, \lambda_{M,h})$ and let $x_h = x_{\lambda(h)}$ be the corresponding element of $\mathbb{Z}_K^\bullet$. Then $|f(L(x_h)) - 2\beta h| < \beta$, so

$$(2h-1)\beta < f(L(x_h)) < (2h+1)\beta.$$

It follows that the $f(L(x_h))$ are all distinct. But since $|N(x_h)| \leq \alpha$, there are only finitely many principal ideals $x_h \mathbb{Z}_K$, so there exists $h \neq h'$ with $(x_h) = (x_{h'})$ and thus $x_h = u x_{h'}$ with $u \in \mathbb{Z}_K^\times$. Thus $f(L(u)) = f(L(x_h)) - f(L(x_{h'})) \neq 0$. □

Exercise 6.28. *Let K be a number field of degree $N \geq 2$. Let $\mu_K \coloneqq K^\times[\text{tors}]$ be the group of roots of unity in K. By Theorem 6.21, we know that μ_K is finite.*

a) *Show: the group μ_K is cyclic.*
b) *Put $m \coloneqq \#\mu_K$. Show: $\varphi(m) \leq N$.*
(Hint: use that the cyclotomic polynomial $\Phi_m(t) \in \mathbb{Q}[t]$ is irreducible.)

c) *Show: if* $N = 2$*, then* $m \in \{1, 2, 4, 6\}$ *and that all of these possibilities occur for imaginary quadratic fields.*

d) *Show: there is an absolute constant* C *such that for all* $N \geq 3$ *we have* $m \leq C \log \log N$*.*

CHAPTER 7

Some Classical Number Theory

1. Stickelberger's Theorem on the Discriminant

Let A be a Dedekind domain with fraction field K, let L/K be a degree n separable field extension, and choose $\alpha \in L$ such that $L = K(\alpha)$. Put $\mathcal{O} \coloneqq A[\alpha]$.

LEMMA 7.1. *We have*

$$\Delta(1, \alpha, \ldots, \alpha^{n-1}) = \prod_{1 \le i < j \le n} (\alpha_i - \alpha_j)^2 .$$

EXERCISE 7.1. *Prove Lemma 7.1.*

The siginificance of this is that if $f \in K[t]$ is the minimal polynomial for α, then $\prod_{1 \le i < j \le n} (\alpha_i - \alpha_j)^2 = \Delta(f)$ is the discriminant of the polynomial f, say by definition. It is then a piece of classical algebra that $\Delta(f)$ can also be computed as the resultant $\mathrm{Res}(f, f')$ of f and f'. This makes the computation of the discriminant of a monogenic order $A[\alpha]$ very straightforward (especially for a computer).

PROPOSITION 7.2. *Let A be an integrally closed domain with fraction field K, let $f \in K[t]$ be a separable monic polynomial, with splitting field L. Then there is $P \in A$ such that $\Delta(f) \equiv P^2 \pmod{4A}$.*

PROOF. Write $f = \prod_{i=1}^{n} (t - \alpha_i)$ with $\alpha_i \in L$. Consider the quantity

$$P \coloneqq \prod_{1 \le i < j \le n} (\alpha_i + \alpha_j).$$

Then: P lies in L, is integral over A, and is invariant under $\mathrm{Aut}(L/K)$, so $P \in A$. Now consider the quantity E

$$E \coloneqq \Delta(f) - P^2.$$

If K has characteristic 2 then $\Delta(f) = P^2$ is a square in A. Otherwise $\frac{E}{4}$ is an element of K that is integral over A, so $E \in 4A$ and thus $\Delta(f) \equiv P^2 \pmod{4A}$. □

THEOREM 7.3 (Stickelberger). *Let K be a number field, and let $\mathcal{O}$ be any $\mathbb{Z}$-order in K. Then $\delta(\mathcal{O}) \equiv 0, 1 \pmod 4$.*

PROOF. Step 0: It is enough to show that $\delta_K \coloneqq \Delta(\mathbb{Z}_K) \equiv 0, 1 \pmod 4$; then for any $\mathbb{Z}$-order $\mathcal{O}$ in K we have

$$\delta(\mathcal{O}) = [\mathbb{Z}_K : \mathcal{O}]^2 \delta_K \equiv [\mathbb{Z}_K : \mathcal{O}]^2 \delta_K \pmod 4 \equiv 0, 1 \pmod 4.$$

Step 1: Suppose that $2 \mid \delta_K$. Then there is a prime ideal $\mathfrak{p}$ of $\mathbb{Z}_K$ such that $e \coloneqq e(\mathfrak{p}|(2)) \ge 2$. Then by Theorem 5.54b) we have $v_{\mathfrak{p}}(\Delta_{\mathbb{Z}_K/Z}) \ge e - 1$, with equality if and only if $2 \nmid e$, from which it follows that $v_{\mathfrak{p}}(\Delta_{\mathbb{Z}_K}/\mathbb{Z}) \ge 2$ and thus that δ_K is divisible by $||\mathfrak{p}^2|| = 2^{2f(\mathfrak{p}|2)}$, hence by 4.

Step 2: Suppose $2 \nmid \delta_K$. If δ_K is a square, then δ_K is a square modulo 4 and thus $\delta_K \equiv 1 \pmod 4$, so we may assume that $\mathbb{Q}(\sqrt{\delta_K}) \supsetneq \mathbb{Q}$ is a proper quadratic field extension. If M is the Galois closure of $K/\mathbb{Q}$, then by Exercise 5.23 we have $\sqrt{\delta_K} \in M$. Since δ_K is odd, the prime 2 is unramified in K, hence also in the Galois closure L (Corollary 5.71), hence also in $\mathbb{Q}(\sqrt{\delta_K})$, so $\delta_K \equiv 1 \pmod 4$. □

EXERCISE 7.2. *Let $d \in \mathbb{Z} \setminus \{0, 1\}$ be such that $d \equiv 0, 1 \pmod 4$.*

a) *Show: there is an order $\mathcal{O}$ in a quadratic number field such that $\delta_{\mathcal{O}} = d$.*
b) *Show: if $\mathcal{O}_1$ and $\mathcal{O}_2$ are two orders in quadratic number fields, then $\mathcal{O}_1 \cong \mathcal{O}_2$ as rings if and only if $\delta_{\mathcal{O}_1} = \delta_{\mathcal{O}_2}$.*

While we are discussing Stickelberger's work:

THEOREM 7.4 (Pellet-Stickelberger). *Let K be a number field of degree n, and let $f \in \mathbb{Z}[t]$ be a polynomial such that $\mathbb{Q}[t]/(f) \cong K$. (Thus f is the minimal polynomial of an algebraic integer α such that $K = \mathbb{Q}[\alpha]$.) Let p be an odd prime that does not divide $\delta(f)$, and let r be the number of maximal ideals of $\mathbb{Z}_K$ lying over p. Then*

$$\left(\frac{\delta_K}{p}\right) = (-1)^{n+r}.$$

PROOF. The hypothesis $p \nmid \delta(f)$ means that the order $\mathbb{Z}[\alpha]$ is maximal at p and $\mathbb{Z}_K$ is unramified at p, so

$$\mathbb{Z}_K/p\mathbb{Z}_K = \mathbb{Z}[\alpha]/p\mathbb{Z}[\alpha] \cong \mathbb{Z}/p\mathbb{Z}[t]/(f)$$

is an étale $\mathbb{Z}/p\mathbb{Z}$-algebra, and by Dedekind-Kummer the polynomial $f \in \mathbb{Z}/p\mathbb{Z}[t]$ has r irreducible factors. By Proposition 5.18, we get that $\delta_K \pmod p = \delta(f) \pmod p$ is a square if and only if $n + r$ is even, which is the desired result. □

Stickelberger's work went a bit deeper than Theorem 7.4. First of all, the result holds verbatim for all odd primes p that do not ramify in K: this generalization is straightforward from the perspective of Number Theory II, since one can work over the complete DVR $\mathbb{Z}_p$ for which unramifiedness implies monogenicity. Second, the result applies also to $p = 2$ when p is unramified in K, provided one uses the Kronecker symbol $\left(\frac{\delta_K}{2}\right)$ – which is 1 if and only if 2 is split in $\mathbb{Q}(\sqrt{\delta_K})$, hence (using that $\delta_K \equiv 1 \pmod 4$ by Stickelberger's Theorem!) if and only if $\delta_K \equiv 1 \pmod 8$.

2. Coprime Number Fields

The following is a basic piece of multilinear algebra that unfortunately may not be very familiar:

EXERCISE 7.3. *Let R be a ring, let $n_1, n_2 \in \mathbb{Z}^+$, and for $i = 1, 2$, let V_i be a free, finitely generated R-module of rank n_i. Then $V := V_1 \otimes_R V_2$ is a free, finitely generated R-module of rank $n_1 n_2$. For $i = 1, 2$, let $A_i \in \operatorname{End}_R V_i$, so $A := A_1 \otimes A_2 \in \operatorname{End}_R V$. Show:*

$$\det A = (\det A_1)^{n_2} (\det A_2)^{n_1}.$$

Suggestion: see `https://math.stackexchange.com/questions/1316594`*, where several answers are sketched. The one I found most immediately appealing first observes that one can reduce to the case of $R = \mathbb{C}$ and then to the case where A_1*

is diagonalizable with eigenvalues $\alpha_1, \ldots, \alpha_{n_1}$ and A_2 is diagonalizable with eigenvalues $\beta_1, \ldots, \beta_{n_2}$, and it is enough to show that $A_1 \otimes A_2$ is diagonalizable with eigenvalues $\{\alpha_1\beta_j\}_{1 \le i \le n_1,\ 1 \le j \le n_2}$...which is actually easy.

THEOREM 7.5. *For $i = 1, 2$, let $K_i/\mathbb{Q}$ be a finite Galois extension of degree n_i, let δ_i be the discriminant of $\mathbb{Z}_{K_i}/\mathbb{Z}$, le $\alpha_1, \ldots, \alpha_{n_1}$ be a $\mathbb{Z}$-basis for $\mathbb{Z}_{K_1}$ and let $\beta_1, \ldots, \beta_{n_2}$ be a $\mathbb{Z}$-basis for $\mathbb{Z}_{K_2}$. Put*

$$L \coloneqq K_1K_2.$$

We suppose that:

(i) $K_1 \cap K_2 = \mathbb{Q}$*; and*
(ii) $\gcd(\delta_1, \delta_2) = 1$.

Then:

a) *The set $\{\alpha_i\beta_j\}_{1 \le i \le n_1, 1 \le j \le n_2}$ is a $\mathbb{Z}$-basis for $\mathbb{Z}_L$.*
b) *The discriminant of $\mathbb{Z}_L$ is $\delta_1^{n_2}\delta_2^{n_1}$.*

PROOF. Step 0: Since $K_1/\mathbb{Q}$ and $K_2/\mathbb{Q}$ are both Galois, by [**Cl-FT**, Prop. 12.11] the hypothesis $K_1 \cap K_2 = \mathbb{Q}$ is equivalent to the linear disjointness of K_1 and K_2 over $\mathbb{Q}$: that is, the natural $\mathbb{Q}$-algebra map $K_1 \otimes_{\mathbb{Q}} K_2 \to K_1K_2 = L$ is an injection, hence a $\mathbb{Q}$-algebra isomorphism, since both sides are $\mathbb{Q}$-vector spaces of dimension n_1n_2. It follows that $\{\alpha_1\beta_j\}_{1 \le i \le n_1, 1 \le j \le n_2}$ is a $\mathbb{Q}$-basis for L. Moreover we have

$$\mathrm{Aut}(L/\mathbb{Q}) = \mathrm{Aut}(L/K_1) \times \mathrm{Aut}(L/K_2).$$

Indeed, if we put $G \coloneqq \mathrm{Aut}(L/\mathbb{Q})$ and for $i = 1, 2$ put $H_i \coloneqq \mathrm{Aut}(L/K_i)$ then $\#G = n_1n_2$, H_1 is a normal subgroup of G of order n_2, H_2 is a normal subgroup of G of order n_1, $H_1 \cap H_2$ consists of elements of G that pointwise fix both L_1 and L_2, so $H_1 \cap H_2 = \{e\}$, and $L^{\langle H_1, H_2\rangle} = L^{H_1} \cap L^{H_2} = K_1 \cap K_2 = \mathbb{Q}$, so $\langle H_1, H_2\rangle = G$.
Step 1: Let $x \in \mathbb{Z}_L$, so we may write

$$x = \sum_{i,j} a_{ij}\alpha_i\beta_j \text{ with } a_{ij} \in \mathbb{Q},$$

and our task is to show that for all i, j we have $a_{ij} \in \mathbb{Z}$. For $1 \le j \le n_1$, put

$$b_j \coloneqq \sum_{i=1}^{n_1} a_{ij}\alpha_i \in K_1.$$

Write out the elements of H_1 as $\tau_1, \ldots, \tau_{n_2}$, so for all $1 \le k \le n_2$ we have

$$\tau_k(x) = \sum_{j=1}^{n_2} \tau_k(b_j\beta_j) = \sum_{j=1}^{n_2} b_j\tau_k(\beta_j).$$

This shows that if A is the matrix with (i, j) entry $\tau_i(\beta_j)$, $\tau(x)$ is the column vector $(\tau_1(x), \ldots, \tau_{n_1}(x))^T$ and b is the column vector $(b_1, \ldots, b_{n_1})^T$, then we have the matrix equation

$$\tau(x) = Ab. \tag{31}$$

Multiplying both sides of (31) on the left by $\mathrm{adj}(A)$, we get

$$\mathrm{adj}(A)\tau(x) = \det(A)b. \tag{32}$$

Both $\mathrm{adj}(A)$ and $\tau(x)$ have entries in $\mathbb{Z}_L$, so (32) implies that we have $\det(A)b_j \in \mathbb{Z}_L$ for all $1 \leq j \leq n_2$. By (11) we have that $\delta_2 = \det(A)^2$, so for all $1 \leq j \leq n_2$ we have

$$\delta_2 b_j \in \mathbb{Z}_L \cap K_1 = \mathbb{Z}_{K_1},$$

and since

$$\delta_2 b_j = \sum_{i=1}^{n_1} \delta_2 a_{ij} \alpha_i,$$

it follows that for all i, j we have $\delta_2 a_{ij} \in \mathbb{Z}$. The same argument applies with K_1 and K_2 interchanged, giving $\delta_1 a_{ij} \in \mathbb{Z}$. Since $\gcd(\delta_1, \delta_2) = 1$, we deduce $a_{ij} \in \mathbb{Z}$ for all i and j, completing the proof of part a).
Step 2: Let $\delta \coloneqq \delta_L$. By (11) again, we have $\delta = (\det B)^2$, where $B \in M_{n_1 n_2}(L)$ is the matrix with (i, j, k, l) entry $\sigma_i \tau_j(\alpha_k \beta_l)$. This means $B = C \otimes D$ is the Kronecker product of the matrix $C \in M_{n_1}(L)$ with (i, k) entry $\sigma_i(\alpha_k)$ and the matrix $D \in M_{n_2}(L)$ with (j, l) entry $\tau_j(\beta_l)$. By Exercise 7.3 we have

$$\delta = (\det B)^2 = (\det C \otimes D)^2 = ((\det C)^{n_2} (\det D)^{n_1})^2 = \delta_1^{n_2} \delta_2^{n_1}. \qquad \square$$

EXERCISE 7.4. *Let $n_1, n_2 \in \mathbb{Z}^+$ with $\gcd(n_1, n_2) = 1$.*

a) *Let K be a field containing for $i = 1, 2$ a primitive n_ith root of unity ζ_{n_i}. Show: the subgroup of $K^\times$ generated by ζ_{n_1} and ζ_{n_2} has order $n_1 n_2$ and thus contains a primitive $(n_1 n_2)$th root of unity $\zeta_{n_1 n_2}$.*

b) *Let K be a field with characteristic does not divide $n_1 n_2$. For $i = 1, 2$, let ζ_{n_i} be a primitive (n_i)th root of unity in an algebraic closure of K, and let $\zeta_{n_1 n_2}$ be a primitive $(n_1 n_2)$th root of unity in an algebraic closure of K. Show:*

$$K(\zeta_{n_1}) K(\zeta_{n_2}) = K(\zeta_{n_1 n_2}).$$

THEOREM 7.6. *Let $n \in \mathbb{Z}^+$, let $\zeta_n \coloneqq e^{2\pi i/n}$, and put*

$$K_n \coloneqq \mathbb{Q}(\zeta_n),$$

the nth cyclotomic field.

a) *For a prime number p, if $p \mid \delta(K)$, then $p \mid n$.*

b) *We have $\mathbb{Z}_{K_n} = \mathbb{Z}[\zeta_n]$.*

PROOF. Recalll that for all $n \in \mathbb{Z}^+$, the extension $K_n/\mathbb{Q}$ is Galois – for any two roots of Φ_n in $\mathbb{C}$, one is a power of the other, so K_n is the splitting field of Φ_n.
Step 1: Let $n_1, n_2 \in \mathbb{Z}^+$ be such that $\gcd(n_1, n_2) = 1$. Suppose that for $i = 1, 2$ we know that $\mathbb{Z}_{K_{n_i}} = \mathbb{Z}[\zeta_{n_i}]$ and that if a prime p ramifies in $\mathbb{Z}_{K_i}$ then $p \mid n_i$. For $i = 1, 2$, let $\delta_i \coloneqq \delta(\mathbb{Z}_{K_{n_i}})$, and let $\delta \coloneqq \delta(\mathbb{Z}_{K_{n_1 n_2}})$. Then by our assumptions we have $\gcd(\delta_1, \delta_2) = 1$. Moreover, by Exercise 7.4 we have

$$K_{n_1} K_{n_2} = \mathbb{Q}(\zeta_{n_1} \zeta_{n_2}) = \mathbb{Q}(\zeta_{n_1 n_2}) = K_{n_1 n_2}.$$

Applying Theorem 7.5 with $K_i = K_{n_i}$ for $i = 1, 2$, we get that

$$\mathbb{Z}_{K_{n_1 n_2}} = \mathbb{Z}[\zeta_{n_1}^i \zeta_{n_2}^j \mid 0 \leq i < \varphi(n_1),\ 0 \leq j \leq \varphi(n_2)] = \mathbb{Z}[\zeta_{n_1 n_2}]$$

and

$$\delta = \delta_1^{\varphi(n_2)} \delta_2^{\varphi(n_1)}.$$

Step 2: We prove the result by induction on the number r of distinct prime divisors of n. The base case $r = 1$ – i.e., $n = p^a$ – is Exercise 5.39. Now suppose that $r \geq 2$, that the result holds for all positive integers with fewer than r distinct

prime divisors, and let $n = p_1^{a_1} \cdots p_r^{a_r}$. Applying Step 1 with $n_1 = p_1^{a_1} \cdots p_{r-1}^{a_{r-1}}$ and $n_2 = p_r^{a_r}$ gives the result for n. □

EXERCISE 7.5. *Let $n \geq 3$. Determine all primes that ramify in $\mathbb{Q}(\zeta_n)$. (In view of Theorem 7.6a), the natural first guess is that p ramifies if and only if $p \mid n$. But since for odd n we have $\mathbb{Q}(\zeta_n) = \mathbb{Q}(\zeta_{2n})$, this cannot be quite right.)*

3. Quadratic Number Fields

3.1. The norm map.

PROPOSITION 7.7. *Let K be a number field of signature (r, s). Let $N : K \to \mathbb{Q}$ be the norm map. then $N(K) \subseteq \mathbb{R}^{\geq 0}$ if and only if $r = 0$.*

PROOF. Let $K_{\mathbb{R}} := K \otimes_{\mathbb{Q}} \mathbb{R}$. As we know, there is an $\mathbb{R}$-algebra isomorphism $\iota : K_{\mathbb{R}} \to \mathbb{R}^r \times \mathbb{C}^s$; for $\mathbf{y} \in K_{\mathbb{R}}$ we have $N(\mathbf{y}) = N(\iota(\mathbf{y}))$, and for $\mathbf{x} = (y_1, \ldots, y_r, z_1, \ldots, z_s) \in \mathbb{R}^r \times \mathbb{C}^s$ we have

$$N(\mathbf{x}) = y_1 \cdots y_r |z_1|^2 \cdots |z_s|^2.$$

This shows that $N(K_{\mathbb{R}}) \subseteq \mathbb{R}^{\geq 0}$ if and only if $r = 0$. So if $r = 0$, then $N(K) \subseteq \mathbb{R}^{\geq 0}$.

Now suppose that $r \geq 1$. Our expression for the norm map on $\mathbb{R}^\times \times \mathbb{C}^s$ shows that it is a continuous function (indeed, with respect to any $\mathbb{R}$-basis for $K_{\mathbb{R}}$, the norm map is a homogeneous polynomial function of degree $n = r + 2s$). Since K is dense in $K_{\mathbb{R}}$, if we had $N(x) \geq 0$ for all $x \in K$ then it would follow that $N(\mathbf{y}) \geq 0$ for all $\mathbf{y} \in K_{\mathbb{R}}$, which we just saw is not the case. □

Because every element of K is of the form $\frac{\alpha}{N}$ for $\alpha \in \mathbb{Z}_K$ and $N \in \mathbb{Z}^+$, it is immediate from Proposition 7.7 that there is $\alpha \in \mathbb{Z}_K$ of negative norm if and only if $r \geq 1$.

Suppose now that $r \geq 1$, and let $\sigma_1, \ldots, \sigma_r : K \hookrightarrow \mathbb{R}$ be the real embeddings of K. We define a map

$$\mathfrak{s} : K^\times \to \{\pm 1\}^r$$

by mapping $x \in K^\times$ to $(\mathrm{sgn}(\sigma_1(x)), \ldots, \mathrm{sgn}(\sigma_r(x))$; to be sure, for $y \in R^\times$, we put $\mathrm{sgn}(y) = 1$ if y is positive and -1 if y is negative. The proof of Proposition 7.7 shows that the map $(\sigma_1, \ldots, \sigma_r)$ embeds $K^\times$ as a dense subgroup of $(\mathbb{R}^\times)^r$, from which it follows that the map $\mathfrak{s}$ is surjective. However, a more interesting invariant comes from restricting $\mathfrak{s}$ to the unit group $\mathbb{Z}_K^\times$. This map factors through a homomorphism

$$\mathfrak{s} : \mathbb{Z}_K^\times / \mathbb{Z}_K^{\times 2} \to \{\pm 1\}^r.$$

The Dirichlet Unit Theorem implies that $\mathbb{Z}_K^\times / \mathbb{Z}_K^{\times 2}$ is cyclic of order 2^{r+s}. We define the **unit-sign group**

$$\mathfrak{u}_K := \mathfrak{s}(\mathbb{Z}_K^\times / \mathbb{Z}_K^{\times 2}).$$

Then $\mathfrak{u}_K \cong (\mathbb{Z}/2\mathbb{Z})^{u(K)}$. Clearly $\mathfrak{s}(1) \neq \mathfrak{s}(-1)$: 1 is positive with respect to every real embedding and -1 is negative with respect to every real embedding, so:

$$1 \leq u(K) \leq r.$$

We will see later that already for real quadratic fields, we can have either $u(K) = 1$ or $u(K) = 2$ and that this is a fundamental dichotomy in their arithmetic.

Now let $D \in \mathbb{Z}^\bullet$ be squarefree and not a square, and let $K := \mathbb{Q}(\sqrt{D})$. Let σ be the nontrivial field automorphism of K. Then for all $\alpha \in K$ we have $N(\alpha) = \alpha\sigma(\alpha)$,

but we can be even more explicit than this.

First suppose that $D \equiv 2, 3 \pmod 4$, so $\mathbb{Z}_K$ (resp. K) is the $\mathbb{Z}$-module (resp. $\mathbb{Q}$-vector space) spanned by 1 and $\sqrt{D}$. Then

$$\forall x, y \in K,\ N(x + y\sqrt{D}) = (x + y\sqrt{D})(x - y\sqrt{D}) = x^2 - Dy^2.$$

This certainly confirms Proposition 7.7 in this case: there are elements of $\mathbb{Z}_K$ of negative norm if and only if $D > 0$.

Next suppose that $D \equiv 1 \pmod 4$, so $\mathbb{Z}_K$ (resp. K) is the $\mathbb{Z}$-module (resp. $\mathbb{Q}$-vector space) spanned by 1 and $\frac{1+\sqrt{D}}{2}$. Then:

$$\forall x, y \in K,\ N(x+y(\frac{1+\sqrt{D}}{2})) = (x+y(\frac{1+\sqrt{D}}{2}))((x+y(\frac{1-\sqrt{D}}{2})) = x^2+xy+\left(\frac{1-D}{4}\right)y^2.$$

This time it is slightly less immediate that the norm takes negative values if and only if $D > 0$, but this would follow e.g. from completing the square.

Exercise 7.6. *Let $K = \mathbb{Q}(\sqrt{D})$ be a quadratic field, with D a squarefree integer that is not a square. Show: if $\alpha \in \mathbb{Z}_K$, then $N(\alpha)$ is a square in $\mathbb{Z}/D\mathbb{Z}$.*

3.2. Imaginary Quadratic Fields. Suppose now that $K = \mathbb{Q}(\sqrt{D})$ with $D < 0$ squarefree. The Dirichlet Unit Theorem implies that $\mathbb{Z}_K^\times$ is finite...but this is overkill. By Lemma 6.20 and Proposition 7.7, for $\alpha \in \mathbb{Z}_K$ we have $\alpha \in \mathbb{Z}_K^\times$ if and only if $N(\alpha) = 1$. Thus to find the units in $\mathbb{Z}_K$ we need to find all $x, y \in \mathbb{Z}$ such that $x^2 - Dy^2 = 1$ if $D \equiv 2, 3 \pmod 4$ or such that $x^2 + xy + \left(\frac{1-D}{4}\right)y^2 = 1$ if $D \equiv 1 \pmod 4$.

Exercise 7.7. *With notation as above, show:*
- *If $D = -3$, then $\mathbb{Z}_K^\times$ is cyclic of order 6.*
- *If $D = -4$, then $\mathbb{Z}_K^\times$ is cyclic of order 4.*
- *If $D < -4$, then $\mathbb{Z}_K^\times$ is cyclic of order 2.*

There is however another approach: for any $R > 0$, the set of $\mathbf{x} \in K_\mathbb{R} = \mathbb{C}$ such that $N(\mathbf{x}) \leq R$ is the set of points lying on or inside an ellipse in the complex plane, hence compact, hence has finite intersection with any $\mathbb{Z}$-lattice in $\mathbb{C}$, so $\mathbb{Z}_K^\times$ is finite, so is the set of Nth roots of unity for some $N \in \mathbb{Z}^+$. Indeed, because ± 1 are units we must have that N is even. If $N \geq 4$, then K contains $\mathbb{Q}(\zeta_N)$, so

$$2 \leq \varphi(N) = [\mathbb{Q}(\zeta_N) : \mathbb{Q}] \mid [K : \mathbb{Q}] = 2$$

and thus $\varphi(N) = 2$, which implies $N \in \{4, 6\}$. If $N = 4$ then K contains $\mathbb{Q}(\zeta_4)$ then since the latter number field also has degree 2 we have $K = \mathbb{Q}(\zeta_4)$, i.e., $D = -1$; similarly, if $N = 6$ then $K = \mathbb{Q}(\zeta_6)$; i.e., $D = -3$.

3.3. Real Quadratic Fields. Let $K = \mathbb{Q}(\sqrt{D})$ be a real quadratic field; for a given K, D is unique if we require it to be positive a positive squarefree integer that is not a square. We regard K as a subfield of $\mathbb{R}$. Let σ be the nontrivial element of $\mathrm{Aut}(K/\mathbb{Q})$.

In this case the Dirichlet Unit Theorem applies to show that there is an isomorphism

$$\iota : \mathbb{Z}_K^\times \to \mathbb{Z} \times \{\pm 1\}.$$

The group $K^\bullet$ is equipped with two natural involutions: the first is $u \mapsto -u$ and the second is $u \mapsto u^{-1}$. (So far the same can be said about the unit group of any ring.)

These two involutions commute with each other – $-u^{-1} = (-u)^{-1}$ – so overall we get an action of $U \coloneqq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ on $\mathbb{Z}_K^\times$. The U-orbit of 1 is $\{\pm 1\}$, of size 2; every other orbit has size 4. Indeed, the U-orbit of any unit $u \notin \{\pm 1\}$ consists of one element in each of the four intervals $(-\infty, -1)$, $(-1, 0)$, $(0, 1)$ and $(1, \infty)$ on the real line.

EXERCISE 7.8. *Let $\alpha = x + y\sqrt{D} \in \mathbb{Z}_K^\times$ (here x, y lie in $\mathbb{Q}$). Show that the U-orbit of α is*

$$\{x + y\sqrt{D}, x - y\sqrt{D}, -x + y\sqrt{D}, -x - y\sqrt{D}\}.$$

By precomposing the isomorphism ι by multiplication by -1 on $\mathbb{Z}_K^\times$ if necessary, we may assume that $\iota^{-1}(0, 1)$ is positive; and then by postcomposing with the isomorphism $(n, \epsilon) \mapsto (-n, \epsilon)$ on $\mathbb{Z} \times \{\pm 1\}$ if necessary, we may assume that $\epsilon \coloneqq \iota^{-1}(0, 1)$ is greater than 1. Then every element of $\mathbb{Z}_K^\times$ that is greater than one is of the form ϵ^n for a unique $n \in \mathbb{Z}^+$. We call ϵ the **fundamental unit** of K. By Exercise 7.8, we have $\epsilon = a + b\sqrt{D}$ with $a, b > 0$.

PROPOSITION 7.8. *The fundamental unit $\epsilon = a + b\sqrt{D}$ has the following property: for any unit $\eta = c + d\sqrt{D} > 1$, we have $a \leq c$, with equality if and only if $\epsilon = \eta$.*

PROOF. For $n \in \mathbb{Z}^+$, we may write

$$\epsilon^n = a_n + b_n\sqrt{D},$$

and it suffices to show that the sequence $\{a_n\}_{n=1}^\infty$ of rational numbers is strictly increasing. We have

$$\epsilon^{n+1} = \epsilon^n \epsilon = (a + b\sqrt{D})(a_n + b_n\sqrt{D}) = (aa_n + Dbb_n) + (ab_n + a_n b)\sqrt{D}.$$

If $D \equiv 2, 3 \pmod 4$ then a, a_n, b, b_n are all positive integers, so it is clear that $aa_n + Dbb_n > a_n$. When $D \equiv 1 \pmod 4$ then a, a_n, b, b_n are all positive integers or positive half-integers, so the same argument works when $a \geq 1$. The remaining case is $a = \frac{1}{2}$, and then

$$N(\epsilon) = \frac{1}{4} - Db^2 = \pm 1,$$

which implies $D = 5$ and $b = \frac{1}{2}$. The element

$$\epsilon \coloneqq \frac{1 + \sqrt{5}}{2}$$

is an element of $\mathbb{Z}_K$ and satisfes $N(\epsilon) = -1$, so is a unit. Since for any unit $\eta > 1$ we have $c, d \geq \frac{1}{2}$, clearly $\alpha \leq \eta$, so α is the fundamental unit of $\mathbb{Q}(\sqrt{5})$. Moreover we check that $a_2 = \frac{3}{2}$, so the fundamental unit is the unique entry with minimal rational part among units greater than 1. This ends the proof...except that above we claimed that $\{a_n\}_{n=1}^\infty$ is strictly increasing, which we haven't shown if $D = 5$. Because

$$\sigma(\epsilon)^n = a_n - b_n\sqrt{D},$$

we find:

$$\forall n \in \mathbb{Z}^+,\ a_n = \frac{\left(\frac{1+\sqrt{5}}{2}\right)^n + \left(\frac{1-\sqrt{5}}{2}\right)^n}{2},$$

from it which it follows that for all $n \geq 2$, a_n is the unique nearest half-integer to $\frac{1}{2}\left(\frac{1+\sqrt{5}}{2}\right)^n$, which is easily seen to be strictly increasing. □

EXAMPLE 7.9. *We list the fundamental units ϵ_D for some real quadratic fields $\mathbb{Q}(\sqrt{D})$:*

a) *We have $\epsilon_2 = 1 + \sqrt{2}$, with $N(\epsilon_2) = -1$.*
b) *We have $\epsilon_3 = 2 + \sqrt{3}$, with $N(\epsilon_3) = 1$.*
c) *As seen above, we have $\epsilon_5 = \frac{1+\sqrt{5}}{2}$, with $N(\epsilon_5) = -1$.*
d) *We have $\epsilon_6 = 5 + 2\sqrt{6}$, with $N(\epsilon_6) = 1$.*
e) *We have $\epsilon_7 = 8 + 3\sqrt{7}$, with $N(\epsilon_7) = 1$.*
f) *We have $\epsilon_{10} = 3 + \sqrt{10}$, with $N(\epsilon_{10}) = -1$.*
g) *We have $\epsilon_{11} = 10 + 3\sqrt{11}$, with $N(\epsilon_{11}) = 1$.*

Already we see a basic dichotomy: the fundamental unit ϵ_D could have norm 1 – in which case every unit of $\mathbb{Z}_K$ has norm 1 – or the fundamental unit could have norm -1. Recall we defined for a number field with a real embedding the **unit sign group** $\mathfrak{u}_K$ which is the collection of possible "total signs" of units under all the real embeddings; for a real quadratic field we have $r = 2$ and thus $\mathfrak{u}_K$ has order 2 or order 4. Indeed it has order 4 if and only if $N(\epsilon_D) = -1$: indeed, if this holds, then ϵ_D has different signs with respect to the two real embeddings (or, more concretely, if $\epsilon_D = a + b\sqrt{D}$, then $a - b\sqrt{D} < 0$), whereas if $N(\epsilon_D) = 1$ then all units have norm 1 and thus have the same sign with respect to the two real embeddings.

EXERCISE 7.9. *Let D be a positive squarefree integer that is not a square.*

a) *Show: the fundamental unit of $\mathbb{Q}(\sqrt{D})$ has norm -1 if and only if there is $u \in \mathbb{Z}[\sqrt{D}]^\times$ with $u = 1$, as follows:*
   (i) *Suppose $D \equiv 1 \pmod 8$. Show: $\mathbb{Z}[\frac{1+\sqrt{D}}{2}]^\times = \mathbb{Z}[\sqrt{D}]^\times$.*
   (ii) *Suppose $D \equiv 5 \pmod 8$. Show: if $u \in \mathbb{Z}[\frac{1+\sqrt{D}}{2}]^\times$, then $u^3 \in \mathbb{Z}[\sqrt{D}]^\times$.*
b) *Deduce: the fundamental unit of $\mathbb{Q}(\sqrt{D})$ has norm -1 if and only if the **negative Pell equation** $x^2 - Dy^2 = -1$ has an integral solution.*

The sequence of positive integers D for which the negative Pell equation $x^2 - Dy^2 = -1$ has an integral solution has an entry on the Online Encyclopedia of Integer Sequences: see `\https://oeis.org/A031396`. In particular, the set of such D in the interval $[1, 300]$ is

$$\{1, 2, 5, 10, 13, 17, 26, 29, 37, 41, 50, 53, 58, 61, 65, 73, 74, 82, 85, 89, 97, 101, 106, 109...$$

$$...113, 122, 125, 130, 137, 145, 149, 157, 170, 173, 181, 185, 193, 197, 202, 218, 226...$$

$$229, 233, 241, 250, 257, 265, 269, 274, 277, 281, 290, 293, 298\}.$$

From this data, one can see some apparent patterns: first, every prime $p \equiv 1 \pmod 4$ (in the given range) appears on this list; and second, no integer (in the given range) that is divisible by a prime $p \equiv 3 \pmod 4$ appears on this list. These facts are not so hard to prove:

PROPOSITION 7.10. *Let $D \in \mathbb{Z}^+$ be squarefree and not a square, let $K = \mathbb{Q}(\sqrt{D})$ and let ϵ_D be the fundamental unit of K.*

a) *Suppose that $D = p$ is a prime number such that $p \equiv 1 \pmod 4$. Then $N(\epsilon_D) = -1$.*
b) *Suppose that is divisible by a prime $p \equiv 3 \pmod 4$. Then $N(\epsilon_D) = 1$.*

PROOF. a) By Exercise 7.9, it is enough to find integers x, y such that $x^2 - py^2 = -1$. That exercise also shows that the index of the unit group in the nonmaximal order $\mathbb{Z}[\sqrt{D}]^\times$ in the unit group $\mathbb{Z}_K^\times$ is either 1 or 3, which gives us the classical result that the Pell equation $x^2 - py^2 = 1$ has an integral solution with $x, y \in \mathbb{Z}^+$. Since $p \equiv 1 \pmod 4$, any such solution has x odd and y even. We are going to make a classical descent argument: among such solutions to the Pell equation, choose one, (x_0, y_0), such that y_0 is minimal. Since

$$x_0^2 - 1 = (x_0 + 1)(x_0 - 1) = py^2$$

and $\gcd(x_0 + 1, x_0 - 1) = 2$, at least one of $x_0 - 1$ and $x_0 + 1$ is divisible by $2p$. In the former case, we have

$$\frac{x_0 + 1}{2} \cdot \frac{x_0 - 1}{2p} = (\frac{y}{2})^2$$

so we have a product of coprime integers being a square, so both are squares: we get $uv \in \mathbb{Z}$ such that

$$x_0 - 1 = 2pu^2 \text{ and } x_0 + 1 = 2v^2.$$

Then

$$v^2 - pu^2 = \frac{1}{2}((x_0 + 1) - (x_0 - 1)) = 1.$$

Since

$$py_0^2 = (x_0 - 1)(x_0 + 1) = 2pu^2(x_0 + 1),$$

we have

$$2u^2(x_0 + 1) = y_0^2$$

and thus $|u| < y_0$, so $|v|^2 - p|u|^2 = 1$ is a solution to the Pell equation that is smaller than the minimal solution, a contradiction. Thus we must be in the latter case: $X_0 + 1$ is divisible by $2p$, so

$$\frac{x_0 + 1}{2p} \cdot \frac{x_0 - 1}{2} = (\frac{y}{2})^2,$$

which as above implies that there are $u, v \in \mathbb{Z}$ such that

$$\frac{x_0 + 1}{2p} = u^2 \text{ and } \frac{x_0 - 1}{2} = v^2,$$

and then we have

$$v^2 = pu^2 = \frac{1}{2}((x_0 - 1) - (x_0 + 1)) = -1,$$

so we have a solution to the negative Pell equation.
b) By Exercise 7.6, we have that $N(\epsilon)$ is a square modulo D, hence also modulo p, but if $p \equiv 3 \pmod 4$ then -1 is not a square modulo p. □

Proposition 7.10 of course only determines the sign of $N(\epsilon_D)$ in certain cases. For instance, for a prime $p \equiv 1 \pmod 4$, it is often the case that $N(\epsilon_{2p}) = -1$ but not always, e.g. not for $p = 17$. Similarly, if $p \equiv q \equiv 1 \pmod 4$ are primes, then it is often the case that $N(\epsilon_{pq}) = -1$ but not always, e.g. not for $p = 5$ and $q = 41$. Some further results like Proposition 7.10 are known, but in general case the best we can say is that $N(\epsilon_D) = 1$ if and only if the period length of the c*nt*n**d fr*ct**n expansion of $\sqrt{d}$ is even. We will not discuss such matters here, but the reader may see e.g. [**D**, p. 96] for further details.

3.4. The 2-torsion subgroup of the class group of a quadratic field. For a quadratic field $K = \mathbb{Q}(\sqrt{D})$, let $G = \langle\sigma\rangle = \mathrm{Aut}(K/Q)$. We will compute $(\mathrm{Cl}\, K)[2]$, the 2-torsion subgroup of the ideal class group of K. Being a finite group of exponent 2, we have $(\mathrm{Cl}\, K)[2] \cong (\mathbb{Z}/2\mathbb{Z})^R$ for some $R \in \mathbb{N}$, so it is equivalent to determine its size. This theorem is due to Gauss, who established it via his theory of binary quadratic forms. We will give a treatment using the metods of algebraic number theory that those who are in the know will recognize as employing some rudiments of group cohomology...but we will neither assume nor explicitly use any group cohomology whatsoever.

Before beginning our exposition of the proof, we establish the following basic result that we will use in due course.

PROPOSITION 7.11. *Let $K = \mathbb{Q}(\sqrt{D})$ be a quadratic number field.*

a) *For $\alpha \in K^\times$, the following are equivalent:*
   (i) *There is $\beta \in K^\times$ such that $\alpha = \frac{\beta}{\sigma(\beta)}$.*
   (ii) *We have $N(\alpha) = 1$.*
   Moreover, when these equivalent conditions hold, β is unique precisely up to multiplication by an element of $\mathbb{Q}^\bullet$.

b) *For $\mathfrak{a} \in \mathrm{Frac}\, \mathbb{Z}_K$, the following are equivalent:*
   (i) *There is some $\mathfrak{b} \in \mathrm{Frac}\, \mathbb{Z}_K$ such that $\mathfrak{a} = \mathfrak{b}(\sigma(\mathfrak{b}))^{-1}$.*
   (ii) *We have $N(\mathfrak{a}) = 1$.*
   Moreover, when these equivalent conditions hold, we may take $\mathfrak{b} \in \mathrm{Int}\, \mathbb{Z}_K$.

PROOF. a) (i) $\implies$ (ii): Since $N(\beta) = N(\sigma(\beta))$, this direction is immediate.
(ii) $\implies$ (i): Suppose $N(\alpha) = 1$. If $\alpha = -1$, then we may take $\beta \coloneqq \sqrt{D}$. Otherwise we take $\beta \coloneqq 1 + \alpha$:

$$\frac{\beta}{\sigma(\beta)} = \frac{1+\alpha}{1+\sigma(\alpha)} = \frac{\alpha(1+\alpha)}{\alpha(1+\sigma(\alpha))} = \frac{\alpha(1+\alpha)}{\alpha+1} = \alpha.$$

Having found one β such that $\alpha = \frac{\beta}{\sigma(\beta)}$, now let $\gamma \in K^\bullet$. Then $\frac{\gamma\beta}{\sigma(\gamma\beta)} = \frac{\gamma}{\sigma(\gamma)}\alpha$, which is equal to α if and only if $\sigma(\gamma) = \gamma$ if and only if $\gamma \in \mathbb{Q}^\bullet$.
b) (i) $\implies$ (ii): Since $N(\mathfrak{a}) = N(\sigma(\mathfrak{a}))$, this direction is again immediate
(ii) $\implies$ (i): Suppose $N(\mathfrak{a}) = 1$. We may uniquely write $\mathfrak{a} = \mathfrak{b}\mathfrak{c}^{-1}$ for $\mathfrak{b}, \mathfrak{c} \in \mathrm{Int}\, \mathbb{Z}_K$ coprime. Thus $N(\mathfrak{b}) = N(\mathfrak{c})$. Let p be a prime dividing $N(\mathfrak{b})$. If p ramifies or is inert, then there is a unique $\mathfrak{p} \in \mathrm{MaxSpec}\, \mathbb{Z}_K$ lying over (p), so both $\mathfrak{b}$ and $\mathfrak{c}$ must be divisible by $\mathfrak{p}$, a contradiction. Therefore every prime $p \mid N(\mathfrak{b})$ is split. If $p\mathbb{Z}_K = \mathfrak{p}_1\mathfrak{p}_2$ and $\mathrm{ord}_p(N(\mathfrak{b})) = a$, then either $v_{\mathfrak{p}_1}(\mathfrak{b}) = a$ and $v_{\mathfrak{p}_2}(\mathfrak{b}) = 0$ or $v_{\mathfrak{p}_1}(\mathfrak{b}) = 0$ and $v_{\mathfrak{p}_2}(\mathfrak{b}) = a$: a is equal to the number of primes over p that divide $\mathfrak{b}$, with multiplicity, and $\mathfrak{b}$ cannot be divisible by both $\mathfrak{p}_1$ and $\mathfrak{p}_2$ because then $\mathfrak{c}$ must be divisible by either $\mathfrak{p}_1$ or $\mathfrak{p}_2$ and would then not be coprime with $\mathfrak{p}_1$. Therefore, after interchanging $\mathfrak{p}_1$ and $\mathfrak{p}_2$ if necessary we have

$$v_{\mathfrak{p}_1}(\mathfrak{b}) = a,\ v_{\mathfrak{p}_2}(\mathfrak{b}) = 0,\ v_{\mathfrak{p}_1}(\mathfrak{c}) = 0,\ v_{\mathfrak{p}_2}(\mathfrak{c}) = a.$$

Since $\mathfrak{p}_2 = \sigma(\mathfrak{p}_1)$, it follows that $\mathfrak{c} = \sigma(\mathfrak{b})$, completing the proof of part b). □

Our argument beings by noticing that the action of G on $K^\times$ induces an action on the group $\mathrm{Frac}\, \mathbb{Z}_K$ of fractional $\mathbb{Z}_K$-ideals that stabilizes its subgroup $\mathrm{Prin}\, \mathbb{Z}_K$ of principal fractional $\mathbb{Z}_K$-ideals, so therefore also G acts on the quotient $\mathrm{Cl}\, K$. For any commutative group A on which a group G acts via group automorphisms, we

have the subgroup A^G of G-invariant elements: i.e., the set of $a \in A$ such that $ga = a$ for all $g \in G$.

In our case, for $\mathfrak{a} \in \operatorname{Frac} \mathbb{Z}_K$, by (26) we have

$$\mathfrak{a}\sigma(\mathfrak{a}) = N(\mathfrak{a})\mathbb{Z}_K,$$

where $N(\mathfrak{a}) \in \operatorname{Frac} \mathbb{Z}$ is the ideal norm of $\mathfrak{a}$. Taking ideal classes, we find that

$$[\mathfrak{a}]\sigma([\mathfrak{a}]) = 1.$$

That is, σ acts by inversion on $\operatorname{Cl} K$. It follows that

$$(\operatorname{Cl} K)^G = (\operatorname{Cl} K)[2].$$

Thus we will compute $(\operatorname{Cl} K)[2]$ by computing the group $(\operatorname{Cl} K)^G$ of G-invariant ideal classes. It turns out to be easy to compute a variant of this group: if $\mathfrak{a} \in (\operatorname{Frac} \mathbb{Z}_K)^G$ – i.e., $\sigma(\mathfrak{a}) = \mathfrak{a}$ – then $\sigma[\mathfrak{a}] = [\sigma(\mathfrak{a})] = [\mathfrak{a}]$, so $[\mathfrak{a}] \in (\operatorname{Cl} K)^G$. But it is not clear whether the converse is true: if $\mathfrak{a} \in (\operatorname{Frac} \mathbb{Z}_K)^G$, then $\sigma(\mathfrak{a})$ lies in the same class as $\mathfrak{a}$, and the question is whether there is some $a \in K^\times$ such that $\sigma(a\mathfrak{a}) = a\mathfrak{a}$. The group of classes of G-invariant fracional ideals is the subgroup

$$\begin{aligned}(\operatorname{Frac} \mathbb{Z}_K)^G \operatorname{Prin} \mathbb{Z}_K / \operatorname{Prin} \mathbb{Z}_K &\cong (\operatorname{Frac} \mathbb{Z}_K)^G / ((\operatorname{Frac} \mathbb{Z}_K)^G \cap \operatorname{Prin} \mathbb{Z}_K) \\ &= (\operatorname{Frac} \mathbb{Z}_K)^G / (\operatorname{Prin} \mathbb{Z}_K)^G\end{aligned}$$

of $(\operatorname{Cl} K)^G$. To ease the notation, let us put

$$A_K \coloneqq \operatorname{Frac} \mathbb{Z}_K \text{ and } B_K \coloneqq \operatorname{Prin} \mathbb{Z}_K$$

so $(A_K/B_K)^G$ is the group of G-invariant ideal classes and A_K^G/B_K^G is its subgroup of classes of G-invariant ideals. If we also put

$$B_{\mathbb{Z}} = \operatorname{Prin} \mathbb{Z} = \operatorname{Frac} Z = A_{\mathbb{Z}},$$

then $B_{\mathbb{Z}}$ lies in the kernel of $A_K^G \to A_K^G/B_K^G$, so we get an exact sequence

$$1 \to B_K^G/B_{\mathbb{Z}} \to A_K^G/B_{\mathbb{Z}} \to A_K^G/B_K^G \to 1.$$

In fact we know the group $A_K^G/B_{\mathbb{Z}}$: as a special case of Exercise 5.47, if $\mathfrak{a}$ is a G-invariant fractional $\mathbb{Z}_K$-ideal then there is $a \in \mathbb{Q}^\bullet$ and distinct ramified primes $\mathfrak{p}_1, \ldots, \mathfrak{p}_s$ of $\mathbb{Z}_K$ such that $\mathfrak{a} = a\mathfrak{p}_1 \cdots \mathfrak{p}_s$. It follows that every element of $A_K^G/B_{\mathbb{Z}}$ is represented by a squarefree product of ramified primes. If $\mathfrak{a}, \mathfrak{b} \in A_K^G$ are such that $\mathfrak{a} = a\mathfrak{b}$ for some $a \in \mathbb{Q}^\bullet$, then $N(\mathfrak{a})N((a))N(\mathfrak{b}) = a^2N(\mathfrak{b})$, so $N(\mathfrak{a})$ and $N(\mathfrak{b})$ represent the same squareclass in $\mathbb{Q}$, but the norm of a squarefree product of ramified primes is the squarefree product of the rational primes lying below each ramified prime, so no two distinct such products lie in the same rational square class. Finally, for each ramified prime $\mathfrak{p}$ we have $\mathfrak{p}^2 = (p)$ for a rational prime p, so $A_K^G/B_{\mathbb{Z}}$ is a 2-torsion commutative group. We conclude:

PROPOSITION 7.12. *Let r be the number of ramified primes in K. Then:*

$$A_K^G/B_{\mathbb{Z}} \cong (\mathbb{Z}/2\mathbb{Z})^r.$$

Thus also $B_K^G/B_{\mathbb{Z}}$ is a 2-torsion group; the next step is to compute its order. For this we need just a little more notation: we put

$$\mathcal{U} \coloneqq \mathbb{Z}_K^\times,$$

$$\mathcal{U}^+ \coloneqq \{\alpha \in \mathcal{U} \mid N(\alpha) = 1\}$$

and

$$\mathcal{U}^{1-\sigma} \coloneqq \{\frac{\alpha}{\sigma(\alpha)} \mid \alpha \in \mathcal{U}\}.$$

Since for all $x \in K^\times$ we have $N(x) = N(\alpha(x))$, we have

$$\mathcal{U}^{1-\sigma} \subseteq \mathcal{U}^+ \subseteq \mathcal{U}.$$

The following result explains the relevance of these subgroups:

PROPOSITION 7.13. *We have an exact sequence*

$$1 \to \mathcal{U}^{1-\sigma} \to \mathcal{U}^+ \to B_K^G/B_{\mathbb{Z}} \to 1.$$

PROOF. We define a homomorphism

$$\lambda : \mathcal{U}^+ \to (\operatorname{Prin} \mathbb{Z}_K)^G/(\operatorname{Prin} \mathbb{Z})$$

as follows: by Proposition 7.11a), there is $\beta \in K^\times$ such that $\alpha = \frac{\beta}{\sigma(\beta)}$, and β is uniquely determined precisely up to multiplication by an elment of $\mathbb{Q}^\bullet$. Since $\alpha \in \mathbb{Z}_K^\times$ we have $\beta\mathbb{Z}_K = \sigma(\beta)\mathbb{Z}_K$, so β generates a G-invariant principal fractional $\mathbb{Z}_K$-ideal; and since β is uniquely determined up to multiplication by an element of $\mathbb{Q}^\bullet$, we may define $\lambda(\alpha)$ to be $\beta\mathbb{Z}_K$ modulo $\operatorname{Prin}\mathbb{Z}$. If α lies in $\mathcal{U}^{1-\sigma}$, then we may take β to be a unit in $\mathbb{Z}_K$ so $\beta\mathbb{Z}_K = (1)$. Conversely, if $\lambda(\alpha) \in \operatorname{Prin}\mathbb{Z}$ then $\beta = r\alpha$ for $r \in \mathbb{Q}^\bullet$ and $\gamma \in \mathcal{U}$, so $\alpha = \frac{\beta}{\sigma(\beta)} = \frac{\gamma}{\sigma(\gamma)} \in \mathcal{U}^{1-\sigma}$, so $\operatorname{Ker}\lambda = \mathcal{U}^{1-\sigma}$.

The surjectivity of λ is immediate: to say that an element $b\mathbb{Z}_K$ of $\operatorname{Prin}\mathbb{Z}_K$ is G-invariant is to say that $\sigma(b)\mathbb{Z}_K = b\mathbb{Z}_K$, so $\alpha := \frac{b}{\sigma(b)}$ lies in $\mathcal{U}$ and thus also in $\mathcal{U}^+$ since $N(b) = N(\sigma(b))$. □

Thus we've reduced the computation of B_K^G/A_K^G to determining the index of $\mathcal{U}^{1-\sigma}$ in $\mathcal{U}^+$, which is quite elementary:

PROPOSITION 7.14. *With notation as above, we have*

$$\mathcal{U}^+/\mathcal{U}^{1-\sigma} \cong \begin{cases} \mathbb{Z}/2\mathbb{Z} & \text{if } D < 0, \\ (\mathbb{Z}/2\mathbb{Z})^2 & \text{if } D > 0 \text{ and } N(\epsilon_D) = 1, \\ \mathbb{Z}/2\mathbb{Z} & \text{if } D > 0 \text{ and } N(\epsilon_D) = -1 \end{cases}.$$

PROOF.

• Suppose that $D < 0$. Because every $\alpha \in \mathcal{U}$ has norm 1, for all $\alpha \in \mathcal{U}$ we have $\sigma(\alpha) = \alpha^{-1}$, so for all $\alpha \in U$ we have $\frac{\alpha}{\sigma(\alpha)} = \alpha^2$ and thus $\mathcal{U}^{1-\sigma} = \mathbb{Z}_K^{\times 2}$. It follows that

$$\mathcal{U}^+/\mathcal{U}^{1-\sigma} \cong \mathbb{Z}_K^\times/\mathbb{Z}_K^{\times 2},$$

and since $\mathbb{Z}_K^\times$ is cyclic of even order we have $\mathbb{Z}_K^\times/\mathbb{Z}_K^{\times 2} \cong \mathbb{Z}/2\mathbb{Z}$.

• Suppose that $D > 0$ and $N(\epsilon_D) = 1$. Then every unit in $\mathbb{Z}_K$ has norm 1, so as above we get $\mathcal{U}^{1-\sigma} = \mathbb{Z}_K^\times$ so $\mathcal{U}^+/\mathcal{U}^{1-\sigma} \cong \mathbb{Z}_K^\times/\mathbb{Z}_K^{\times 2}$. Because $\mathbb{Z}_K^\times \cong \mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, this time its quotient modulo squares is isomorphic to $(\mathbb{Z}/2\mathbb{Z})^2$.

• Suppose that $D > 0$ and $N(\epsilon_D) = -1$. This time $\mathcal{U}^+$ has index 2 in $\mathcal{U}$ so is the subgroup $\langle \epsilon_D^2, -1\rangle$. For $n \in \mathbb{Z}$ we compute

$$\frac{\pm\epsilon_D^n}{\sigma(\pm\epsilon_D^n)} = \frac{\epsilon_D^n}{(-\epsilon_D^{-1})^n} = (-1)^n\epsilon_D^{2n}.$$

Thus $\mathcal{U}^{1-\sigma} = \langle -\epsilon_D^2, \epsilon_D^4\rangle$, which indeed has index 2 in $\langle \epsilon_D^2, -1\rangle$ since -1 does not lie in the first group and adjoining it to the first group we get the second group. □

Combining Propositions 7.12, 7.13 and 7.14, we get:

PROPOSITION 7.15. *Let r be the number of ramified primes in the quadratic field $\mathbb{Q}(\sqrt{D})$, and let B_K^G/A_K^G be the group of classes of G-invariant ideals. Then:*

a) *If $D < 0$, then $B_K^G/A_K^G \cong (\mathbb{Z}/2\mathbb{Z})^{r-1}$.*
b) *If $D > 0$ and $N(\epsilon_D) = -1$, then $B_K^G/A_K^G \cong (\mathbb{Z}/\mathbb{Z})^{r-1}$.*
c) *If $D > 0$ and $N(\epsilon_D) = 1$, then $B_K^G/A_K^G \cong (\mathbb{Z}/2\mathbb{Z})^{r-2}$.*

Finally, we address the discrepancy between the group $(\operatorname{Cl} K)[2] = (A_K/B_K)^G$ of G-invariant ideal classes and its subgroup A_K^G/B_K^G of classes of G-invariant ideals. First we will show that in the cases addressed in parts a) and b) of Proposition 7.15 these two groups are the same, so Proposition 7.15 computes $(\operatorname{Cl} K)[2]$. The case of part c) turns out be more complicated and more interesting.

Let $\mathfrak{a} \in (B_K/A_K)^G$, so there is some $a \in K^\bullet$ such that

$$\mathfrak{a}\sigma(\mathfrak{a})^{-1} = a\mathbb{Z}_K.$$

Applying σ, we get

$$\sigma(\mathfrak{a})\mathfrak{a}^{-1} = \sigma(a)\mathbb{Z}_K.$$

Multiplying these last two equations gives

$$\mathbb{Z}_K = N(a)\mathbb{Z}_K,$$

so $N(a) \in \mathbb{Q}^\bullet \cap \mathbb{Z}_K^\times = \mathbb{Z}^\times = \{\pm 1\}$.
Case 1: Suppose that $-1 \notin N(K^\times)$: this certainly occurs when $D < 0$ and may or may not occur when $D > 0$: more on this shortly. Then $N(a) = 1$, so by Proposition 7.11a) there is $b \in K^\times$ such that $a = \frac{b}{\sigma(b)}$; replacing b with $b' := \sigma(b)$ we get $a = \frac{\sigma(b')}{b'}$, so

$$\mathfrak{a}\sigma(\mathfrak{a})^{-1}\frac{\sigma(b')}{b'}\mathbb{Z}_K$$

or

$$\sigma(b'\mathfrak{a}) = b'\mathfrak{a},$$

showing that $[\mathfrak{a}] \in A_K^K/B_K^G$. Henceforth we may assume $D > 0$.
Case 2: Suppose $N(\epsilon_D) = -1$. If $N(a) = 1$, proceeding as above shows $[\mathfrak{a}] \in A_K^G/B_K^G$. If $N(a) = -1$, then also

$$\mathfrak{a}\sigma(\mathfrak{a})^{-1} = a\epsilon_D\mathbb{Z}_K,$$

and now $N(a\epsilon_D) = 1$, so replacing a with $a' := a\epsilon_D$ and arguing as above we get $[\mathfrak{a}] \in A_K^G/B_K^G$.
Case 3: Finally we suppose that -1 is the norm of an element of K but not of an element of $\mathbb{Z}_K^\times$. In this case the argument of Case 2 fails in a way that will allow us to define a homomorphism

$$\eta : (A_K/B_K)^G \to \{\pm 1\}$$

whose kernel is A_K^G/B_K^G. Indeed, given $[\mathfrak{a}] \in (A_K/B_K)^G$, as above there is $a \in K^\times$, well-defined up to multiplication by a unit of $\mathbb{Z}_K$, such that

$$\mathfrak{a}\sigma(\mathfrak{a})^{-1} = a\mathbb{Z}_K.$$

Since this time all units have norm 1, it follows that $N(a) \in \{\pm 1\}$ is well-defined. Indeed this is an invariant of $[\mathfrak{a}]$ and not just of $\mathfrak{a}$, since if we multiply $\mathfrak{a}$ by $x \in K^\times$ then a gets replaced by $a\frac{x}{\sigma(x)}$, which has the same norm as a. Thus we may define $\eta([\mathfrak{a}]) := N(a)$. This argument shows that if $N(a) = -1$, then $[\mathfrak{a}]$ has no G-invariant

representative, whereas as we saw above, if $N(a) = 1$, it does. It is immediate that η is a homomorphism, so we get an exact sequence

$$1 \to A_K^G/B_K^G \to (A_K/B_K)^G \stackrel{\eta}{\to} \{\pm 1\}.$$

The remaining question is whether η is surjective. We claim that it always is, which will complete the computation of $(A_K/B_K)^G = (\mathrm{Cl}\, K)[2]$ in this final case. To see this, we use some undergraduate number theory in a rather surprising way. The element -1 is a norm from K if and only if there are $x, y \in \mathbb{Q}$ such that $x^2 - Dy^2 = -1$. (This is because $1, \sqrt{D}$ is a $\mathbb{Q}$-basis for K in all cases, even when it is not a $\mathbb{Z}$-basis for $\mathbb{Z}_K$.) Clearly denominators, we get a nonzero integer solution (X, Y, Z) to

$$X^2 - DY^2 + Z^2 = 0. \tag{33}$$

Conversely, because D is not a square in $\mathbb{Q}$, a nonzero integer solution to (33) must have $Z \neq 0$ and thus yields a rational soluton to $x^2 - Dy^2 = -1$. A very old theorem of Legendre tells when a diagonalized conic $aX^2 + bY^2 + cZ^2 = 0$ has nonzero integer solutions: see e.g. [**Cl-NT**, Thm. 18.4]. Applied to (33), we get that -1 is a norm from K if and only if -1 is a square modulo D, which since D is squarefree is equivalent to -1 being a square modulo every odd prime divisor of D, which is equivalent (by results referred to and proved in Chapter 1) to D being divisible by no prime $p \equiv 3 \pmod 4$ which is at last equivalent to D being a sum of two integer squares: there are $a, b \in \mathbb{Z}^+$ such that

$$D = a^2 + b^2;$$

since D is squarefree, we may and shall assume that a is odd, which ensures $\gcd(a, 2b) = 1$. In the dramatic conclusion, we will use this representation to build an explicit element of c of $(A_K/B_K)^G$ with $\eta(c) = 1$. Indeed, we take

$$\mathfrak{a} := \langle a, b + \sqrt{D}\rangle.$$

Since

$$N(b + \sqrt{D}) - (b + \sqrt{D})(b - \sqrt{D}) = b^2 - D = -a^2,$$

we have

$$\begin{aligned}\mathfrak{a}^2 &= \langle a^2, ab + a\sqrt{D}, b^2 + D + 2b\sqrt{D}\rangle \\ &= \langle a^2, ab + a\sqrt{D}, 2b^2 + 2b\sqrt{D}\rangle = \langle a^2, a(b + \sqrt{D}), 2b(b + \sqrt{D})\rangle \\ &= \langle a^2, b + \sqrt{D}\rangle = \langle b + \sqrt{D}\rangle,\end{aligned}$$

so $\mathfrak{a}^2$ is principal – and thus $[\mathfrak{a}] \in (A_K/B_K)^G$ of norm a^2, so

$$\mathfrak{a}\sigma(\mathfrak{a}) = N(\mathfrak{a}) = a$$

and thus

$$\mathfrak{a}\sigma(\mathfrak{a})^{-1} = \mathfrak{a}^2/N(\mathfrak{a}) = \frac{b + \sqrt{D}}{a}\mathbb{Z}_K.$$

Since $N(\frac{b+\sqrt{D}}{a}) = -1$, we find that $\eta([\mathfrak{a}]) = -1$.

Finally, we can state and prove our main result:

THEOREM 7.16. *Let $K = \mathbb{Q}(\sqrt{D})$ be a quadratic field with r ramified primes.*

a) *If $D < 0$, then $(\mathrm{Cl}\, K)[2] \cong (\mathbb{Z}/2\mathbb{Z})^{r-1}$.*

b) *If $D > 0$ and D is not divisible by any prime $p \equiv 3 \pmod 4$, then $(\mathrm{Cl}\, K)[2] \cong (\mathbb{Z}/2\mathbb{Z})^{r-1}$.*

c) *If $D > 0$ and D is divisible by some prime $p \equiv 3 \pmod 4$, then* $(\mathrm{Cl}\, K)[2] \cong (\mathbb{Z}/2\mathbb{Z})^{r-2}$.

PROOF. a) Suppose $D < 0$. By our argument above and Proposition 7.15 we have

$$(\mathrm{Cl}\, K)[2] \cong A_K^G/B_K^G \cong (\mathbb{Z}/2\mathbb{Z})^{r-1}.$$

b) Suppose that $D > 0$ and D is not divisible by any prime $p \equiv 3 \pmod 4$. By our above discussion, -1 is a norm from $K^\times$.

• Suppose $N(\epsilon_D) = -1$. By our argument above and Proposition 7.15 we have

$$(\mathrm{Cl}\, K)[2] \cong A_K^G/B_K^G \cong (\mathbb{Z}/2\mathbb{Z})^{r-1}.$$

• Suppose $N(\epsilon_D) = 1$. By our argument above and Proposition 7.15 we have that $A_K^G/B_K^G \cong (\mathbb{Z}/2\mathbb{Z})^{r-2}$ and $\#G = 2\#(A_K^G/B_K^G)$, so

$$(\mathrm{Cl}\, K)[2] \cong (\mathbb{Z}/2\mathbb{Z})^{r-1}.$$

c) Suppose $D > 0$ and D is divisible by some prime $p \equiv 3 \pmod 4$. Then -1 is not a norm from K, so certainly $N(\epsilon_D) = 1$, and then by our argument above and Proposition 7.15 we have

$$(\mathrm{Cl}\, K)[2] \cong A_K^G/B_K^G \cong (\mathbb{Z}/2\mathbb{Z})^{r-2}. \qquad \square$$

Theorem 7.16 is more often covered in the easiser imaginary quadratic case: Cox for instance covers his early on in his lovely book [**Co**, Prop. 3.11] using the language of quadratic forms and even gives the generalization to nonmaximal imaginary quadratic orders. This result is extremely dear to me because of its applications to complex multiplication of elliptic curves.

In contrast, the real quadratic case of this result is strangely hard to find in texts: when searching the literature, I found many assertions that "Gauss's genus theory allows us one to compute $(\mathrm{Cl}\, K)[2]$ for any quadratic field K," but the only textbook I know that states and proves this result is a recent one of F. Lemmermeyer [**Le**]. My exposition here largely follows [**Le**, Ch. 9]. Theorem 7.16 is a manifestly equivalent restatement of [**Le**, Thm. 9.10]: Lemmermeyer's description of $\#(\mathrm{Cl}\, K)[2]$ is 2^{r-2} makes reference to $N(\epsilon_D)$ and whether D is a sum of two squares, but this must be a matter of taste.

It is curious that while the proof of Theorem 7.16 in the real quadratic case makes such critical use of the sign of the norm of the fundamental unit, in the end the final result does not depend on this. This makes one wonder whether this division into cases is really necessary. In fact there is a closely related result that is easier and in some sense more natural: when $D > 0$, rather than considering the ideal class group A_K/B_K, one can consider the **narrow class group** $\mathrm{Cl}_\infty K := A_K/C_K$, where C_K are principal fractional ideals that can be generated by totally positive elements: i.e.,elements that are positive in both real embeddings. As above, one finds that $(\mathrm{Cl}_\infty K)[2] = (A_K/C_K)^G$ are the G-invariant narrow classes. Then one has the following result:[1]

THEOREM 7.17. *Let K be a real qudaratic field with r ramified primes. Then*

$$(\mathrm{Cl}_\infty K)[2] \cong (\mathbb{Z}/2\mathbb{Z})^{r-1}.$$

[1]I suspect that it is Theorem 7.17 rather than Theorem 7.16 that appears (in the guise of a result on binary quadratic forms) in Gauss's *Disquisitiones Arithmeticae*, but it would be better for me to check than to speculate on this.

EXERCISE 7.10. *Modify the proof of Theorem 7.16 to prove Theorem 7.17. Show in particular that in all cases we have* $A_K^G/C_K^G = (A_K/C_K)^G$*, so the situation is actually simpler here.*

In lieu of solving Exercise 7.10, the reader may wish to consult the text of Fröhlich and Taylor: Theorem 7.17 appears therein as [**FT**, Thm. V.39], and the proof is along similar (though not identical) lines to the proof we've given of Theorem 7.16.

It is easy to see how the narrow class group relates to the class group:

EXERCISE 7.11. *Let* $K = \mathbb{Q}(\sqrt{D})$ *be a real quadratic field. There is a canonical surjective group homomorphism*

$$q : \mathrm{Cl}_\infty K \to \mathrm{Cl}\, K.$$

a) *Show: if* $N(\epsilon_D) = -1$*, then* q *is an isomorphism, and deduce Theorem 7.16 from Theorem 7.17 in this case.*
b) *Show: if* $N(\epsilon_D) = 1$*, then* $\mathrm{Ker}\, q$ *has order* 2*.*

However, the relationship between the 2-torsion subgroups of $\mathrm{Cl}_\infty K$ and $\mathrm{Cl}\, K$ is not as simple. Surprisingly, the text of Fröhlich and Taylor (who are two very distinguished algebraic number theorists) stumbles on this point: [**FT**, Cor. 1, p. 181] asserts that $\#(\mathrm{Cl}_\infty K)[2] = \#(\mathrm{Cl}\, K)[2]$ when $N(\epsilon_D) = -1$ and that $\#(\mathrm{Cl}_\infty K)[2] = 2\#(\mathrm{Cl}\, K)[2]$ when $N(\epsilon_D) = 1$. The first assertion is immediate from Exercise 7.11, but comparing the statements of Theorems 7.16 and 7.17 shows that the second assertion is not always true.

EXAMPLE 7.18. *Let* $D = 205 = 5 \cdot 41$*, and let* $K = \mathbb{Q}(\sqrt{D})$*, so* $r = 2$*. As reported above via* `\https://oeis.org/A031396`*, we have* $N(\epsilon_D) = 1$*. Theorems 7.16 and 7.17 give*

$$(\mathrm{Cl}\, K)[2] \cong \mathbb{Z}/2\mathbb{Z} \cong (\mathrm{Cl}_\infty K)[2].$$

MAGMA computes class groups and narrow class groups and gives

$$(\mathrm{Cl}_\infty K) \cong \mathbb{Z}/4\mathbb{Z} \text{ and } \mathrm{Cl}\, K \cong \mathbb{Z}/2\mathbb{Z},$$

so indeed the class group has half the size of the narrow class group in this case, but that does not hold on the 2*-torsion subgroups.*

Bibliography

[AC] P.L. Clark, *Algebraic Curves: An Algebraic Approach*. http://alpha.math.uga.edu/~pete/8320_2020.pdf

[AM69] M.F. Atiyah and I.G. Macdonald, *Introduction to commutative algebra*. Addison-Wesley Publishing Co., Reading, Mass.-London-Don Mills, Ont. 1969.

[Ar67] J.V. Armitage, *On a theorem of Hecke in number fields and function fields.* Invent. Math. 2 (1967), 238–246.

[B] N. Bourbaki, *Algebra I*.

[Ba08] C. Ballot, *Competing prime asymptotic densities in $\mathbb{F}_q[x]$: a discussion*. L'enseignment Mathématique 54 (2008), 303–328.

[Br86] R. Brandl, *Integer polynomials that are reducible modulo all primes.* Amer. Math. Monthly 93 (1986), 286–288.

[CA] P.L. Clark, *Commutative Algebra*. http://math.uga.edu/~pete/integral.pdf.

[Ch96] H. Cohen, *Hermite and Smith normal form algorithms over Dedekind domains.* Math. Comp. 65 (1996), 1681—1699.

[Cl-FT] P.L. Clark, *Field Theory*. http://math.uga.edu/~pete/FieldTheory.pdf

[Cl-IS] P.L. Clark, *Invariant Subspaces.* alpha.math.uga.edu/~pete/invariant_subspaces.pdf

[C-L] A. Chambert-Loir, *(Mostly) commutative algebra*. Universitext. Springer, Cham, 2021.

[Cl-NT] P.L. Clark, *Number Theory: A Contemporary Introduction*. http://alpha.math.uga.edu/~pete/4400FULL.pdf

[Cl66] L.E. Claborn, Every commutative group is a class group. Pacific J. Math. 18 (1966), 219–222.

[Cl09] P.L. Clark, *Elliptic Dedekind domains revisited.* Enseign. Math. (2) 55 (2009), 213–225.

[Cl17] P.L. Clark, *The cardinal Krull dimension of a ring of holomorphic functions.* Expo. Math. 35 (2017), 350–356.

[Clxx] P.L. Clark, *Abstract Geometry of Numbers: Linear Forms*. http://alpha.math.uga.edu/~pete/GoN_Linear_Forms.pdf

[Co] D.A. Cox, *Primes of the form $x^2 + ny^2$. Fermat, class field theory and complex multiplication*. A Wiley-Interscience Publication. John Wiley & Sons, Inc., New York, 1989.

[CS46] I.S. Cohen and A. Seidenberg, *Prime ideals and integral dependence*. Bull. Amer. Math. Soc. 52 (1946), 252–261.

[D] H. Davenport, *The higher arithmetic. An introduction to the theory of numbers*. Eighth edition. With editing and additional material by James H. Davenport. Cambridge University Press, Cambridge, 2008.

[DeS93] B. de Smit, *Algebraic numbers with integral power traces.* J. Number Theory 45 (1993), 112–116.

[FL96] A. Fuchs and G. Letta, *Le problème du premier chiffre décimal pour les nombres premiers*. The Foata Festschrift. Electron. J. Combin. 3 (1996), no. 2, Research Paper 25, approx. 7 pp.

[FST62] A. Fröhlich, J.-P. Serre and J. Tate, *A different with an odd class.* J. Reine Angew. Math. 209 (1962), 6–7.

[FT] A. Fröhlich and M.J. Taylor, *Algebraic number theory*. Cambridge Studies in Advanced Mathematics, 27. Cambridge University Press, Cambridge, 1993.

[Gr74] A. Grams, *Atomic rings and the ascending chain condition for principal ideals*. Proc. Cambridge Philos. Soc. 75 (1974), 321–329.

[GSS05] R. Guralnick, M.M. Schacher and J. Sonn, *Irreducible polynomials which are locally reducible everywhere.* Proc. Amer. Math. Soc. 133 (2005), 3171–3177.

[GT] P.L. Clark, *General Topology*. `http://alpha.math.uga.edu/~pete/pointset.pdf`

[Ha28] H. Hasse, *Über eindeutige Zerlegung in Primelemente oder in Primhauptideale in Integrittsbereichen*. J. reine Angew. Math. 159, 3-12, 1928.

[He] E. HEcke, *Vorlesungen über die Theorie der algebraischen Zahlen* Second edition of the 1923 original, with an index. Chelsea Publishing Co., Bronx, N.Y., 1970.

[He34] H. Heilbronn, *On the Class Number in Imaginary Quadratic Fields.* Quart. J. Math. Oxford Ser. 25 (1934), 150–160.

[L] S. Lang, *Algebra*. Revised third edition. Graduate Texts in Mathematics, 211. Springer-Verlag, New York, 2002.

[Le] F. Lemmermeyer, Lemmermeyer, *Quadratic number fields.* Translated from the 2017 German original. Springer Undergraduate Mathematics Series. Springer, Cham, 2021.

[LG72] C.R. Leedham-Green, *The class group of Dedekind domains.* Trans. Amer. Math. Soc. 163 (1972), 493–500.

[LM72] K.B. Levitz and J.L. Mott, *Rings with finite norm property*. Canad. J. Math. 24 (1972), 557–565.

[Ma58] H.B. Mann, *On integral bases.* Proc. Amer. Math. Soc. 9 (1958), 167–172.

[N] J. Neukirch, *Algebraic number theory.* Translated from the 1992 German original and with a note by Norbert Schappacher. With a foreword by G. Harder. Grundlehren der mathematischen Wissenschaften 322. Springer-Verlag, Berlin, 1999.

[Na53] N. Nakano, *Idealtheorie in einem speziellen unendlichen algebraischen Zahlkŕper*. J. Sci. Hiroshima Univ. Ser. A. 16 (1953), 425–439.

[NT0] P.L. Clark, *Number Theory: A Contemporary Introduction.* `http://alpha.math.uga.edu/~pete/4400FULL.pdf`

[NTII] P.L. Clark, *Number Theory II: Valuations, Local Fields and Adeles.* `alpha.math.uga.edu/~pete/8410FULL.pdf`

[O'M] T. O. O'Meara, *Introduction to quadratic forms.* Reprint of the 1973 edition. Classics in Mathematics. Springer-Verlag, Berlin, 2000.

[Pl74] P.A.B. Pleasants, *The number of generators of the integers of a number field.* Mathematika 21 (1974), 160–167.

[Po10] B. Poonen, http://mathoverflow.net/q/15221

[S] P. Samuel, *Algebraic theory of numbers.* Translated from the French by Allan J. Silberger Houghton Mifflin Co., Boston, Mass. 1970.

[Sa71] P. Samuel, *About Euclidean rings.* J. Algebra 19 (1971), 282–301.

[Sc13] P. Schmid, *Differents, discriminants and Steinitz classes.* Bull. Lond. Math. Soc. 45 (2013), 318—328.

[Se:CL] J.-P. Serre, *Local fields*. Translated from the French by Marvin Jay Greenberg. Graduate Texts in Mathematics, 67. Springer-Verlag, New York-Berlin, 1979.

[SL96] P. Stevenhagen and H.W. Lenstra, Jr., *Chebotarëv and his density theorem*. Math. Intelligencer 18 (1996), 26–37.

[St-ANT] P. Stevenhagen, *Number Rings*. Course notes available at `http://websites.math.leidenuniv.nl/algebra/ant.pdf`.

[Sz97] L. Szabó, *A simple proof for the Jordan measurability of convex sets.* Elem. Math. 52 (1997), 84–86.

[Su] A.V. Sutherland, *Number Theory I.* `https://ocw.mit.edu/courses/18-785-number-theory-i-fall-2021/pages/lecture-notes/`

[Tr88] H.F. Trotter, *An overlooked example of nonunique factorization.* Amer. Math. Monthly 95 (1988), no. 4, 339–342.

[ZS] O. Zariski and P. Samuel, *Commutative Algebra: Volume I*. Graduate Texts in Mathematics #28, Springer-Verlag.