Algebraic Number Theory I

Pete L. Clark

Contents

Introduction

These notes represent my first serious attempt at a first algebraic number theory course with an algebraic mindset: drawing on results of commutative algebra and field theory in order to work over an arbitrary Dedekind domain. I have drawn from several sources, but most of all from some wonderful notes of Drew Sutherland.

I taught a course, Math 8400, from these notes at the University of Georgia in Fall 2022. I thank the hardy students who took the course for their engagement with this approach, which is far from the simplest possible but seems to offer more conceptual insight.

CHAPTER 1

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 1.1 (Chinese Remainder Theorem). *Let $I_1, \ldots, I_r$ 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 1.1.

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 1.2. *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 1.3. *State and prove the analogue of Exercise 1.2 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 1.2. *An R-module M is Noetherian iff every submodule of M is finitely generated.*

EXERCISE 1.4. *Prove Proposition 1.2.*

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 1.3. *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 1.4 (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

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

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 1.5. *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]. □

4. Prime Avoidance

LEMMA 1.6 (Prime Avoidance). *Let R be a ring, and let $I_1, \ldots, I_n, J$ 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 1.5. *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 1.6. *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 1.7. *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 1.8. *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 1.7. *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* $\operatorname{Hom}(P, \cdot)$ *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 $M^\vee := \operatorname{Hom}_R(M, R)$; this is again an R-module.

Theorem 1.8. *For an R-module A, the following are equivalent:*

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

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

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

Proof. This is [**CA**, Thm. 7.32]. □

Exercise 1.9.

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**:

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

(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 1.10. *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 1.8: 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

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

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** $S \subset R$: this is a subset containing 1 and closed under multiplication: $SS \subset S$. 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 1.11. *Find a commutative ring R and a multiplicative subset $S \subset R$ 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 1.12. *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 1.13 (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 $\varphi(S) \subset T^{\times}$: 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

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

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

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

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

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

EXERCISE 1.14. *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 1.9. *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 1.10. *Let $S \subset R$ 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 1.11. *Let $S \subset R$ 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 $\mathfrak{q} \subset \mathfrak{p}$. 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 1.12. *Let R be a ring, let $S \subset R$ 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 1.15. *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 1.16 (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 1.6).*

8.2. Localization of Modules. Let $S \subset R$ 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 1.17. *Let* $S \subset R$ *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 1.18. *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 1.13. *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 1.19. *Show that containment of submodules is a local property: if N_1 and N_2 are submodules of an R-module M, then we have $N_1 \subseteq N_2$ if and only if $(N_1)_{\mathfrak{m}} \subseteq (N_2)_{\mathfrak{m}}$ for all $\mathfrak{m} \in \operatorname{MaxSpec} R$.*
(Hint: $N_1 \subsetneq N_2$ if and only if the inclusion map $N_1 \cap N_2 \to N_1$ is surjective.

Proposition 1.14. *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 1.15. *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 1.16. *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 1.13, 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 1.15 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 1.17. *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 1.20. *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 1.21. *Let R be a domain, and let $S \subset R$ 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) $S^{-1}(I : J) = (S^{-1}I : S^{-1}J)$.

Exercise 1.22. *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 1.23. *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 $I \in \operatorname{Frac}(R)$, so $\operatorname{Frac}(R)$ 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 $\operatorname{Frac} R$ 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 1.24. *Let R be a domain, and let J be an* invertible *fractional R-ideal. Show: for all $I \in \operatorname{Frac}(R)$ 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 $I \in \operatorname{Frac}(R)$, we put

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

Exercise 1.25. *Let R be a domain, and let $I \in \operatorname{Frac}(R)$. Show: $II^* \subseteq R$.*

Now we have a very important lemma:

Lemma 1.18. *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. This is [**CA**, Lemma 19.8]. (The proof is not at all difficult; I encourage you to read it.) □

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 1.15 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 1.19. *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 1.10) it has rank 1.

Furthermore:

Theorem 1.20. *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 1.20, every rank 1 projective R-module is isomorphic to a fractional ideal I. By Exercise 1.23 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 $\operatorname{Inv}(R)$ the group of invertible fractional R-ideals (this is the unit group of the commutative monoid $\operatorname{Frac}(R)$). The principal fractional R-ideals form a subgroup of $\operatorname{Inv}(R)$ that we denote $\operatorname{Prin}(R)$.

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

$$\operatorname{CaCl}(R) := \operatorname{Inv}(R)/\operatorname{Frac}(R).$$

But the point is that we have named the same group twice: we have just explained that the canonical map $\operatorname{CaCl}(R) \to \operatorname{Pic} R$ that associates to every invertible ideal class the isomorphism class of the underlying rank 1 projective module is an isomorphism, and by Theorem 1.20b) 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 $\operatorname{Cl}(R)$: see [**CA**, §19.4] for one possible definition. There is a canonical injective group homomorphism

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

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 nontriviality is no longer the sole obtruction to $\mathcal{O}$ being a PID.

10. Integral Extensions

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

Exercise 1.26. *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 1.21. *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 $A \subset C \subset B$ 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 1.22. *Let $A \subset B \subset C$ 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 $\{\alpha_i\beta_j\}_{1\leq i\leq m,\ 1\leq j\leq n}$ 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 1.23. *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 1.21 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 1.21, $A[\alpha_1]$ 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 1.22a), $A[\alpha_1, \alpha_2]$ 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 1.24. *Let $A \subset B$ 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 1.27. *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 1.25. *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 1.26. *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 1.27. *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 1.28 (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 1.29. *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 $\iota_*(I) \subset \iota_*(\mathfrak{m})$, 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 $\iota_*(\mathfrak{m}) \subset \mathcal{P} \subsetneq B$. 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 1.30 (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 1.30 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 1.30 later on: see Theorem 4.21.

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 1.30, $\mathbb{Z}_K$ 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 1.3 $\mathbb{Z}_K$ 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 1.29e), 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 1.30 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 $\mathbb{Z}[\sqrt{d}] \subset \mathbb{Z}_K$. 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 1.27b), 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 $\text{ord}_2(b) = -1$ 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 1.31. *Let d be a squarefree integer not equal to 0 or 1, and put $K = \mathbb{Q}(\sqrt{d})$. Then:*

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

CHAPTER 2

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 1.1 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 2.1 (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 2.2. *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) $\Longrightarrow$ (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 2.2 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 2.1. *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 2.2. *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 2.2 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 $v(x + y) \geq \max v(x), v(y)$.

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 2.3. *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 2.4. *Let K be a field, and let $v : K^\times \to \mathbb{Z}$ be a normalized discrete valuation on K. Put*

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

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 2.2, 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 2.3 (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 1.28, 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 2.4. *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 2.4 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 1.19).

Actually this is a characteristic property of Dedekind domains:

Theorem 2.5. *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 1.19. We just showed (i) $\implies$ (ii). For (iii) $\implies$ (i) see [**CA**, Thm. 20.1]. □

Theorem 2.6. *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 1.18): 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 2.5. *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 2.6. *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 2.7. *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 2.8. *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 2.7 (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 2.8. *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

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

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 2.9. *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 2.8b), 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 2.10. *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 2.9 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 $y_1, \ldots, y_r \in R$ usch that $I = \langle xy_1, \ldots, y_r \rangle_R$.

Exercise 2.9. *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 2.11 (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 2.10 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 2.12. *Let R be a Dedekind domain, and let M be a finitely generated R-module. Then:*

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

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

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 $M[\text{tors}]$ 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*

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

The proof of Theorem 2.12 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 2.9 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 1.15, 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 $S \subset R$, 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 2.13. *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 1.18). 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 2.13, 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 2.14. *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 2.14 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 2.15. *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**:

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

Exercise 2.10. *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 2.11. *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 2.12. *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 2.13. *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 2.10, 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 2.16.

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 2.14. *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 2.15. *Let R be a Dedekind domain, and let $I \subset J$ be fractional R-ideals. Show: J/I has finite length and*

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

Exercise 2.16. *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 3

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 2.13, every lattice Λ is finitely generated projective, and conversely every rank r projective module Λ is a lattice in $\Lambda \otimes_R K$.

Exercise 3.1. *Show: R-lattices in K are precisely fractional ideals of K.*

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

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

Exercise 3.2. *Let Λ_1, Λ_2 be R-lattices in V. Show: there is $d \in R^\bullet$ such that*

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

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

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 $g \cdot N := \{gn \mid n \in N\}$. 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 $\mathcal{E} := \langle x_1, \ldots, x_n \rangle$. This choice of basis allows us to identify $\mathrm{Aut}_K(V)$ with $\mathrm{GL}_n(K)$.

Proposition 3.1. *Let V be a finite-dimensional K-vector space with K-basis $e_1, \ldots, e_n$, and put $\mathcal{E} := \langle e_1, \ldots, e_n \rangle$.*

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 3.3. *Prove Proposition 3.1.*

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

Proposition 3.2. *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

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

Then the Steinitz class $\mathrm{St}(\Lambda)$ is $[I]$, the class of I, which is nontrivial, so by Corollary 2.15 the lattice Λ is not free. □

Let Λ be any R-lattice in the n-dimensional K-vector space V. By Theorem 2.12, 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 3.3. *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 3.4. *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 3.4. *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 $\mathfrak{d}_i := \mathfrak{a}_i \mathfrak{b}_i^{-1}$, 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 3.5.

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 3.6. *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 3.7. *Let Λ_1 and Λ_2 be R-lattices in the n-dimensional K-vector space V. Then Smith Normal Form (Theorem 3.4b) 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 3.5. *Let $\Lambda_1, \Lambda_2, \Lambda_3$ be R-lattices in the K-vector space V. Then:*

a)

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

b)

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

Exercise 3.8. *Prove Proposition 3.5.*

Proposition 3.6. *Let $M \in \operatorname{Aut}_K(V)$ and let Λ be an R-lattice in V. Then:*

$$\chi(\Lambda, M\Lambda) = (\det M).$$

Proof. Both sides can be computed locally, so we are reduced to the case in which R is a DVR. We may therefore assume that Λ is free: let $x_1, \ldots, x_n$ be an R-basis for Λ, which is also a K-basis for V, which we may use to represent M by a matrix in $\mathrm{GL}_n(K)$. One version of Smith Normal Form 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 $d_1, \ldots, d_n \in K^\times$. Choose $\alpha \in R^\bullet$ such that $\alpha d_i \in R^\bullet$ for all i. Then $\alpha M\Lambda$ is free with basis $\alpha d_1 x_1, \ldots, \alpha d_n x_n$, so $M/(\alpha M\Lambda) \cong \bigoplus_{i=1}^n R/dd_iR$. Therefore

$$\chi(\Lambda, \alpha M\Lambda) = ((\alpha d_1) \cdots (\alpha d_n)) = (\alpha^n)(d_1 \cdots d_n).$$

By definition of the Fröhlich inviarant, we have

$$\chi(\Lambda, M\lambda) = (\alpha^{-n})\chi(\Lambda, \alpha M\Lambda) = (d_1 \cdots d_n) = (\det M). \qquad \square$$

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*

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

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

$$\Lambda_{\mathfrak{p}} \coloneqq \Lambda \otimes_R R_{\mathfrak{p}},$$

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

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

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" $\{\Lambda_{\mathfrak{p}}\}_{\mathfrak{p} \in \operatorname{MaxSpec} R}$. The answer is: completely!

First of all, as a special case of Proposition 1.14 we have

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

This ensures that the mapping

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

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

When $n = 1$ and $\operatorname{MaxSpec} R$ 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 $\operatorname{supp} I$ we have $I_{\mathfrak{p}} = R_{\mathfrak{p}}$. Conversely, if for each $\mathfrak{p} \in \operatorname{MaxSpec} R$ we are given a 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 3.7 (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 $\Lambda(\mathfrak{p}) = \Lambda_{\mathfrak{p}}$. □

5. Lattices in a Quadratic Space

5.1. Bilinear Forms on a Vector Space. Let F 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

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

and

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

Because of this, we get induced mappings

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

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

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 $G(i, j) := \langle e_i, e_j \rangle$.

EXERCISE 3.9. *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 3.8. *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 3.10. *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:

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

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**).

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 3.9. *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, $G_e \in \operatorname{GL}_n(R)$.)*
   (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) $\Longrightarrow$ (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) $\Longrightarrow$ (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) $\Longleftrightarrow$ (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. □

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** δ of the bilinear module $(M, \langle \cdot, \cdot \rangle)$.

5.3. Quadratic Lattices. We now wish to expand the definition of quadratic lattice in two ways.

First let M be a finitely generated free R-module, which we view as an R-lattice in $V := M \otimes_R K$. Let $\langle \cdot, \cdot \rangle : V \times V \to K$ be a K-bilinear form. Then if we restrict $\langle \cdot, \rangle$ to M we do *not* necessarily get an R-bilinear form because we may not have $\langle M, M \rangle \subseteq M$. 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 quadratic spaces. A little thought shows that in this case, associated to any R-basis $e_1, \ldots, e_n$ of M 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 not necessarily free R-lattice Λ in V. Our task is to define the discriminant $\delta(M)$ as a fractional ideal anyway. If the bilinear form is degenerate, we put

$\delta(M) := 0$, so we may assume that it 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 $\mathfrak{p}^{\delta_{\mathfrak{p}}(M)}$ for some well-defined $\delta_{\mathfrak{p}}(M) \in \mathbb{Z}$. We then wish to define

$$\delta(M) := \prod_{\mathfrak{p} \in \operatorname{MaxSpec} R} \mathfrak{p}^{\delta_{\mathfrak{p}}(M)},$$

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 consider its Gram matrix G_e. Then only finitely many primes $\mathfrak{p}$ can divide any entry of the Gram matrix and the determinant of the Gram matrix, being a principal fractional ideal of R, is coprime to all but finitely many primes, which shows that $(M_{\mathfrak{p}}, \langle \cdot, \cdot \rangle)$ is perfect for all but finitely many primes $\mathfrak{p}$.

As usual, it is 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 3.11. *With notation as above, show:*

a) *If the bilinear space is degenerate, then $\delta(x_1, \ldots, x_n) = 0$ for all $x_1, \ldots, x_n \in V$.*
b) *If the bilinear 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 3.10. *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*

$$\delta(M) = D.$$

Exercise 3.12. *Prove Proposition 3.10.*

6. Dual Lattices

Throughout this section, a K-**bilinear space** will mean a finite-dimensional K-vector space V equipped with a nondegnerate, symmetric K-bilinear pairing $\langle \cdot, \cdot \rangle$.

To an R-lattice Λ in a K-bilinear space we may attrach its **dual lattice**

$$\Lambda^* := \{x \in V \mid \langle x, \Lambda \rangle = 0\}.$$

Exercise 3.13. *Let M, N be R-lattices in V. Show: $M \subseteq N \implies N^* \subseteq M^*$.*

In what follows, for a field k, by a k**-bilinear space** we will mean a finite dimensional k-vector space V equipped with a nondegenerate k-bilinear pairing $\langle \cdot, \cdot \rangle$.

Theorem 3.11. *Let R be a Noetherian domain with fraction field K, and let $(V, \langle \cdot, \cdot \rangle)$ by a K-bilinear space. For each R-lattice Λ in V, we have that Λ^* is an R-lattice in V that is isomorphic as an R-module to $\Lambda^\vee$.*

Proof. Let $(e_1, \ldots, e_n)$ be a K-basis for V that lies in Λ. By Proposition 3.9, there is a unique K-basis $(e_1', \ldots, e_n')$ of V such that for all $1 \leq i, j \leq n$ we have $\langle e_i', e_j \rangle = \delta_{i,j}$.

Step 1: We show that $\langle \Lambda^* \rangle_k = V$. Choose a finite set S of R-module generators for Λ; express each in terms of the basis $(e_1, \ldots, e_n)$, and let d be the product of all denominators that appear. We claim that for all $1 \leq i \leq n$ that $de_i' \in \Lambda'$. Indeed, for $m \in S$, write $m = \sum_{j=1}^n m_j e_j$; then for all $1 \leq i \leq n$ we have

$$\langle de_i', m \rangle = d \sum_{j=1}^n m_j \langle e_i', e_j \rangle = dm_i \in R,$$

so $de_i' \in \Lambda *$. Thus Λ^* contains $(de_1', \ldots, de_n')$, which is a K-basis for V.
Step 2: We show that Λ^* is finitely generated. Let N be the free R-submodule of M with basis $(e_1, \ldots, e_n)$. Then N is a free R-lattice in V. For all $1 \leq i \leq n$ we have $e_i' \in N^*$. We claim that $(e_1', \ldots, e_n')$ is an R-basis for N^*. Since $e_1', \ldots, e_n'$ are K-linearly independent, they are R-linearly independent. For $x \in N^*$, if we write $x = \sum_{i=1}^n x_i e_i'$ then for all $1 \leq i \leq n$,

$$\langle x, e_i \rangle = x_i \in R,$$

so $x \in \langle e_1', \ldots, e_n' \rangle_R$.

So N^* is a free A-module of rank n. Since $N \subseteq \Lambda$ we have $\Lambda^* \subseteq N^*$. Since R is Noetherian and N^* is finitely generated, also Λ^* is finitely generated. Thus Λ^* is indeed an R-lattice in V.
Step 3: We show that $\Lambda^* \cong \Lambda^\vee$. Let

$$\varphi : \Lambda^* \to \Lambda^\vee, \ x \mapsto (m \mapsto \langle x, m \rangle).$$

This is a homomorphism of R-modules. 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 3.14. *Let R be a Noetherian domain with fraction field K. For $i = 1, 2$, let $(V_i, \langle \cdot, \cdot \rangle_i)$ be a K-bilinear 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 $\Lambda^* = \Lambda_1^* \oplus \Lambda_2^*$.*

Corollary 3.12. *Let R be a Noetherian domain with fraction field J, let V be a K-bilinear space, and let Λ be a* free *R-lattice in V, with basis $e_1, \ldots, e_n$. Then Λ^* has a unique R-basis $(e_1', \ldots, e_n')$ such that $\langle e_i', e_j \rangle = \delta_{i,j}$.*

Proof. In the proof of theorem 3.11 we may take $N = \Lambda$. Then we get that $\Lambda^* = N^*$ is free with basis $(e_1', \ldots, e_n')$ satisfying $\langle e_i', e_j \rangle = \delta_{i,j}$. The uniqueness is left to the reader. □

Lemma 3.13. *Let R be a Notherian domain with fraction field K, let $(V, \langle \cdot, \cdot \rangle)$ be a k-bilinear space, let Λ be an R-lattice in V, and let S be a multiplicative subset of R. Then $S^{-1}\Lambda$ and $S^{-1}\Lambda^*$ are $(S^{-1}R)$-lattices in V satisfying $(S^{-1}\Lambda)^* = S^{-1}\Lambda^*$.*

Proposition 3.14. *Let R be a Dedekind domain with fraction field K, let $(V, \langle \cdot, \cdot \rangle)$ be a symmetric K-bilinear space, and let Λ be an R-lattice in V. Then $\Lambda^{**} = \Lambda$.*

Proof. In a tautological way we have $\Lambda \subseteq \Lambda^{**}$. By Proposition 1.13 it therefore suffices to check the equality after replacing R by $R_{\mathfrak{p}}$ for each $\mathfrak{p} \in \operatorname{MaxSpec} R$. Then R is a PID so lattices are free: if $(e_1, \ldots, e_n)$ is a basis for Λ, then by Corollary 3.12 there is a unique basis $(e_1', \ldots, e_n')$ for Λ^* such that $\langle e_i', e_j \rangle = \delta_{i,j}$ for all i, j; applying this result again, there is a unique basis $(e_1'', \ldots, e_n'')$ for Λ^{**} such that $\langle e_i'', e_j' \rangle = \delta_{i,j}$ for all i, j. But the symmetry of the pairing and the uniqueness forces $e_i'' = e_i$ for all i and thus $\Lambda^{**} = \Lambda$. □

More generally, we could work in any Noetherian domain R and assume that our lattice Λ is projective. Then for all $\mathfrak{p} \in \operatorname{MaxSpec} R$, the $R_{\mathfrak{p}}$-lattice $\Lambda_{\mathfrak{p}}$ is free, so it follows from Lemma 3.13 that Λ^* is also projective. Then the proof of Proposition 3.14 goes through to show that $\Lambda^{**} = \Lambda$.

I believe that for any Noetherian domain R and R-lattice Λ in V, we should have $\Lambda^{**} = \Lambda$ if and only if Λ is *reflexive* (reflexive modules are defined in §4.4).

There is an important relation among the discriminant, the dual lattice and the Fröhlich invariant:

Corollary 3.15. *Let $\langle \cdot, \cdot \rangle$ be a nondegenerate symmetric K-bilinear form on V. Let Λ be an R-lattice in V, and let δ be the discriminant of Λ. Then*

$$\delta = \chi(\Lambda^*, \Lambda).$$

Proof. This equality of fractional ideals can be checked locally, so we may assume that R is a DVR and thus Λ is free with basis $(e_1, \ldots, e_n)$, say and then Λ^* has a unique basis $(e_1', \ldots, e_n')$ such that $\langle e_i', e_j \rangle = \delta_{i,j}$. Writing

$$e_j = \sum_{i=1}^{n} M_{i,j} e_i'$$

we get that $\Lambda = M\Lambda^*$, so by Proposition 3.6 we have $\chi(\Lambda^*, \Lambda) = (\det M)$. Moreover for all $1 \leq i, j \leq n$ we have

$$\langle e_i, e_j \rangle = \langle \sum_k M_{k,i} e_k', e_j \rangle = M_{j,i},$$

so $\delta = \det M^T = \det M$. □

Corollary 3.16. *Let $\langle \cdot, \cdot \rangle$ be a nondegenerate symmetric K-bilinear form on V, and let Λ_1, Λ_2 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 $y_i = P x_i$ 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

$$\delta_{\Lambda_2} = (\det P)^2 \delta_{\Lambda_1}. \tag{3}$$

Moreover we have $\Lambda_2 = P\Lambda_1$, so by Propositions 3.5 and 3.6 we have

$$\chi(\Lambda_1, \Lambda_2) = \chi(\Lambda_1, P\Lambda_1) = (\det P). \tag{4}$$

Combining (3) and (4) we get part a). Part b) follows: indeed $\mathfrak{a} = \chi(\Lambda_1, \Lambda_2)$, which is an integral ideal since $\Lambda_2 \subseteq \Lambda_1$. □

Exercise 3.15. *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 invariant of Λ. Show:*

$$[\delta] = \operatorname{St}(\Lambda)^2.$$

I want to end this section with some "fancy" remarks that are motivated by Exercise 3.15. 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 $\langle x, y \rangle \coloneqq \operatorname{Trace}(xy)$ 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 3.15 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 4

Algebraic Number Theory in Dedekind Domains

1. Etale Algebras

Exercise 4.1. *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 4.2. *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) *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.*
c) *Suppose k is algebraically closed. Show: f is separable if and only if it is a product of distinct linear factors.*
d) *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.*

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 4.1. *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 1.5 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. □

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 [**FT**, Cor. 7.3]. Does this monogenicity hold for separable k-algebras that are not fields? Let's see:

Exercise 4.3. *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 4.4. *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 4.5. *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 $I \subseteq \operatorname{Ker} \varphi$.*
(b) *Show: φ induces a surjective $\mathbb{F}_q$-algebra homomorphism $\mathbb{F}_q^{q^N} \to \mathbb{F}_q^r$.*
c) *Deduce: $q^N \geq r$. That is, A needs at least $\log_q(r)$ generators as an $\mathbb{F}_q$-algebra.*

Exercise 4.6. *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.*

Proposition 4.2. *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 $A_{/l} := A \otimes_k l$ 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 $A_{/l} = k[t]/(f) \otimes_k l = l[t]/(f)$. A polynomial f over a field is separable if and only if $\gcd(f, f') = 1$. Since f is separable, there are $a, b \in k[t]$ such that $af + bf' = 1$; evidently this same equation holds in $k[t]$, which shows the gcd condition still holds in the larger field, so $f \in l[t]$ is separable, so $f = f_1 \cdots f_r$ with f_i distinct monic irreducible polynomials, and then by the Chinese Remainder Theorem

$$A_{/l} = l[t]/(f) = l[t]/(f_1 \cdots f_r) \cong \prod_{i=1}^{r} k[t]/(f_i)$$

is a separable k-algebra. □

Theorem 4.3. *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, we have that $A_{/K} := A \otimes_k K$ is reduced.*

Proof.
(i) $\implies$ (ii): Since étale algebras are reduced, this follows from Proposition 4.2.
$\neg$ (i) $\implies$ $\neg$ (ii): Suppose that A is not an étale k-algebra. Being a commutative Artinain ring, k is a finite product of Artinian local rings, so we find that since A is not étale, either A is not reduced or it is a finite product $\prod_{i=1}^{r} l_i$ of finite degree field extensions, at least one of which is inseparable. Since $A \hookrightarrow A_{/K}$, if A is not reduced, neither is $A_{/K}$. So it suffices to show that if l/k is a finite degree inseparable field extension then $l \otimes_k K$ is not reduced. Since l/k is inseparable, there

is $x \in l$ with an inseparable minimal polynomial $f \in k[t]$. The minimal polynomial does not change upon base extension (Exercise 4.1), so the minimal polynomial of $x \in A_{/K}$ is inseparable, so $K[t]/(f) \cong K[x] \subseteq A_{/K}$ is not reduced, so $A_{/K}$ is not reduced. □

Corollary 4.4. *Let k be a field, and let $A_{/k}$ 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 4.5. *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 4.3 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 4.3.
(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 4.1 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 4.4. □

Let $A_{/k}$ be an étale algebra of dimension n. A field extension l/k **splits** A if $A_{/l} \cong l^n$. If K/k is separably closed, then $A_{/K}$ is is a finite product of finite degree separable field extensions of K, of which there are none but K itself, so $A_{/K} \cong K^n$ and thus K splits A.

If we write our étale algebra as $A = \prod_{i=1}^r l_i$, then a field etension l/k splits A if and only if it splits l_i for all i. We may then write $l_i = k[t]/(f_i)$ for a separable polynomial f, and then l splits l_i if and only if f splits into linear factors in l, so l is a splitting field for l_i if and only if it contains a Galois closure of l_i. Thus, all in all, if we view the l_i's as living in a common algebraic closure $\overline{k}$ of k (as we may, up to isomorphism) then the unique minimal extension l/k that splits A is the Galois closure of the compositum $l_1 \cdots l_r$. This is also the splitting field of the polynomial $f_1 \cdots f_r$ (which need not be separable, but as above can be chosen to be separable when k is infinite).

Proposition 4.6. *Let A be an étale k-algebra, and let K/k be a field that splits A. Then we have an isomorphism of étale K-algebras*

$$A \otimes_k K \overset{\Sigma}{\to} K^{\mathrm{Hom}_k(A,K)}$$

given by

$$\Sigma : \beta \otimes 1 \mapsto (\sigma(\beta))_\sigma.$$

Proof. It is easy to reduce to the case in which $A = k[t]/(f)$ is a separable field extension. In K the polynomial f factors as $f = (t-\alpha_1)\cdots(t-\alpha_n)$ with distinct α_i. By standard field theory, $\mathrm{Hom}_k(A,K)$ is in natural bijection with the roots $\alpha_1, \ldots, \alpha_n$, via the map $t \mapsto \alpha_i$. We have natural isomorphisms

$$A \otimes_k K = K[t]/\prod_{i=1}^n (t-\alpha_i) = \prod_{i=1}^n K[t]/(t-\alpha_i) = \prod_{i=1}^n K$$

that map

$$x \otimes 1 \mapsto x \mapsto (\alpha_1, \ldots, \alpha_n) \mapsto (\sigma_1(x), \ldots, \sigma_n(x)).$$

Since $x \otimes 1$ genereates $A \otimes_k K$ as a K-algebra, it follows that for all $y \in A$ we have $y \otimes 1 \mapsto (\sigma(\beta))_\sigma$. □

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 4.7. *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 4.7. *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 4.8. *Prove Proposition 4.7.*

THEOREM 4.8. *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*

$$T_{A/k}(a) = \sum_{\sigma \in \operatorname{Hom}_k(A,K)} \sigma(a) \text{ and } N_{A/k}(a) = \prod_{\sigma \in \operatorname{Hom}_k(A,K)} \sigma(a).$$

PROOF. Let $n = \dim_k A$. Then the isomorphism $A_{/K} \to K^n$ of Proposition 4.6 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 4.9. *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 $T_{l/k}(a) = e \sum_{i=1}^{f} \alpha_i = -e a_{d-1}$.*
c) *We have $N_{l/k}(a) = \prod_{i=1}^{d} \alpha_i^e = (-1)^{de} a_0^e$.*

Proof. a) This is [**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. □

Here is a generalization of Theorem 4.8 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 [**FT**, §5.2].

Theorem 4.10. *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

$$N_{K/F}(\alpha) = (\prod_{i=1}^{n_s} \tau_i(\alpha))^{p^e} \tag{5}$$

and

$$\mathrm{Tr}_{K/F}(\alpha) = p^e \sum_{i=1}^{m} \tau_i(\alpha). \tag{6}$$

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 4.9 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 (5) and (6) follow immediately. □

Corollary 4.11. *Let R be an integrally closed domain with fraction field k, and let l/k be a finite degree field extension. If $a \in l$ is integral over R, then*

$$T_{l/k}(a),\ N_{l/k}(a) \in R.$$

Proof. This follows from Proposition 4.9 and [**CA**, Thm. 14.18]. □

Theorem 4.12 (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

Suppose that $A \subset B$ 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:

$$T(x,y) := \mathrm{Tr}(xy).$$

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 be content to refer to either one as the discriminant.)

First we consider the case in which A and B are both fields. In this case it is immediate from (6) that if K/F is inseparable then the trace map $\mathrm{Tr}_{K/F}$ vanishes identically. So let us assume that K/F is separable, and let $\sigma_1, \ldots, \sigma_n$ be the F-algebra embeddings of K into $\overline{F}$. Then by (6) for all $x \in K$,

$$\mathrm{Tr}_{K/F}(x) = \sum_{i=1}^{n} \sigma_i(x).$$

Let $\mathbf{x} = (x_1, \ldots, x_n) \in K^n$, and let $S(\mathbf{x}) \in M_n(\overline{F})$ be the matrix with

$$S(\mathbf{x})_{ij} = \sigma_i(x_j).$$

Then

$$(S(\mathbf{x})^T S(\mathbf{x}))_{ij} = \sum_{k=1}^{n} \sigma_k(x_i)\sigma_k(x_j) = \sum_{k=1}^{n} \sigma_k(x_i x_j) = \mathrm{Tr}_{K/F}(x_i x_j).$$

Thus, if we set

$$\delta(\mathbf{x}) := \det \mathrm{Tr}_{K/F}(x_i x_j)$$

then we have

$$\delta(\mathbf{x}) = (\det S(\mathbf{x}))^2. \tag{7}$$

Exercise 4.9. *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 clsoure of L/K.*

a) *Show: M contains $K(\sqrt{\delta_{L/K}})$.*
b) *Let Λ be any A-lattice in L. Show: M contains $K(\sqrt{\delta_\Lambda})$.*

3.1. The Trace Form of a Field Extension.

Theorem 4.13. *(Dedekind's Lemma on Linear Independence of Characters) Let M be a monoid and K a field. The set $X(M,K)$ of all monoid homomorphisms $M \to K^\times$ is linearly independent as a subset of the K-vector space K^M of all functions from M to K.*

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 $X(M,K)$ is linearly independent in K^M. We show this by induction on N. The base case, $N = 1$, is immediate: the only one element linearly dependent subset of K^M is the zero function, and elements of $X(M,K)$ are nonzero at all values of M. So suppose $N \geq 2$, that every $N-1$ element subset of $X(M,K)$ is linearly independent, and let $\chi_1, \ldots, \chi_N$ be distinct elements of $X(M,K)$. Let $\alpha_1, \ldots, \alpha_N \in K$ 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 $\alpha_1 = \cdots = \alpha_{N-1} = 0$. □

Theorem 4.14. *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 (6) 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 $\Delta(\mathbf{x}) = \det T(x_ix_j) \neq 0$. Seeking a contradiction we suppose $\Delta(\mathbf{x}) = 0$; then by (7), 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 4.13). □

EXERCISE 4.10. *Give a different proof of (iv) $\implies$ (i) in Theorem 4.14 using the Primitive Element Corollary and the Vandermonde determinant.*

EXERCISE 4.11. *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 $\Delta(\mathbf{x}) = \det \mathrm{Tr}_{K/F}(x_i x_j) = 0$.*

EXAMPLE 4.15 (Trace form of a quadratic field extension). *Let F be a field of characteristic different from 2, and let $K = F(\sqrt{D})$ be a quadratic field extension. We wish to explicitly compute the trace form. A natural choice of F-basis for K is $(1, \sqrt{D})$. The Gram matrix is then*

$$M = \left[\begin{array}{cc} \mathrm{Tr}(1) & \mathrm{Tr}(\sqrt{D}) \\ \mathrm{Tr}(\sqrt{D}) & \mathrm{Tr}(D) \end{array} \right] = \left[\begin{array}{cc} 2 & 0 \\ 0 & 2D \end{array} \right].$$

The corresponding quadratic form is $2x^2 + 2Dy^2$, of discriminant

$$4D = D \in K^\times / K^{\times 2}.$$

THEOREM 4.16. *Let $A_{/k}$ be a finite dimensional commutative k-algebra. The following are equivalent:*

(i) *The trace form associated to A is nondegenerate.*
(ii) *A is an étale k-algebra.*

PROOF. Step 1: Suppose A is not reduced. Then A is not étale. Also there is a nilpotent $x \in A^\bullet$. For all $y \in A$ the element xy is nilpotent, hence has trace zero, so x lies in the kernel of the trace form. Thus in this case neither (i) nor (ii) holds. Step 2: Suppose A is reduced, so $A = \prod_{i=1}^r l_i$ is a finite product of finite degree field extensions. The trace form on A decomposes as a direct product of the trace forms restricted to l_i. A finite product of bilinear spaces is nondegenerate if and only if each factor is nondegenerate, so we are reduced to showing that if l/k is a finite degree field extension, then the trace form is nondegenerate if and only if l/k is separable. In this case the result is [**FT**, Thm. 6.10]. □

EXERCISE 4.12. *Let k be a field, and let $A_{/k}$ 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*

$$A \supsetneq \mathfrak{p} \supsetneq \mathfrak{p}^2 \supsetneq \ldots \supsetneq \mathfrak{p}^{e-1} \supsetneq \mathfrak{p}^e = (0). \tag{11}$$

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 (11) gives a filtration of the finite-dimensional k-vector space A by subspaces invariant under the k-linear map $x\bullet$. If $W' \subseteq W \subset A$ 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 that multiplication by π^e induces an A-module isomorphism $A/\mathfrak{p} \rightarrow \mathfrak{p}^i/\mathfrak{p}^{i+1}$ that commutes with multiplication by x. Deduce that 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.*

4. Lattices and Pairings

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

$$M^\vee := \operatorname{Hom}_R(M, R).$$

This is also an R-module, via $a \in R, f \in M^\vee \mapsto (x \in M \mapsto af(x))$. This is an additive contravariant functor from the category of left R-modules to itself.

For any R-module M we have a natural map

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

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

Lemma 4.17. *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 $\pi_i : R^I \rightarrow R$ 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 $M \rightarrow R^{M^\vee}$ given by $x \mapsto (f(x))_{f \in M^\vee}$ is an injection. □

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

Lemma 4.18. *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 4.13. *Show that the additive group $(\mathbb{Q}, +)$ of the rational numbers is a torsionfree $\mathbb{Z}$-module that is not torsionless.*

Exercise 4.14. *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 4.15. 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.*

Let R be a Noetherian domain with fraction field k. For a fractional R-ideal I we have a canonical isomorphism from $(R : I)$ to $I^\vee$: if for $x \in k$ we have $xI \subset R$ then $x\cdot \in I^\vee$. Conversely, let $\lambda \in I^\vee$. The map λ extends uniquely to a k-linear map λ_k from k to itself: indeed, if $x \in k$, then $x = \frac{i}{r}$ with $i \in I$ and $r \in R^\bullet$ and then we must take

$$\lambda_k(x) = \frac{1}{r}\lambda(i).$$

It is easy to see that λ_k is a well-defined k-linear map. Then $\lambda_k : k \to k$ is given by multiplication by α for a unique $\alpha \in k$ and thus in $(R : I)$.

For any fractional R-ideal, we put $I^* := (R : I)$ and $\overline{I} := I^{**}$. In this case the canonical injection on the torsionless R-module I

$$\iota_I : I \hookrightarrow I^{\vee\vee}$$

is just the injection from I to

$$\overline{I} := (R : (R : I)).$$

Thus I is reflexive if and only if $I = \overline{I}$: such ideals are called **divisorial**. Because a fractional R-ideal is invertible if and only if it is projective and finitely generated projective modules are reflexive, we see that invertible ideals are divisorial.

Pairings: let M be an R-module, and let $\langle \cdot, \cdot \rangle : M \times M \to R$ be an R-bilinear map. This induces an R-linear map

$$\varphi : M \to M^\vee, \ x \mapsto (y \mapsto \langle x, y \rangle)).$$

We say that the pairing is **nondegenerate** if φ is injective and **perfect** if φ is an isomorphism. If M is finitely generated and R is a field, then nondegenerate and perfect are the same; in general they are not. For instance, if $R = M = \mathbb{Z}$ then every bilinear pairing $\mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$ is given by

$$\langle x, y \rangle = nxy$$

for some $n \in \mathbb{Z}$. Then the pairing is nondegenerate if and only if $n \neq 0$ and is perfect if and only if $n \in \{\pm 1\}$.

Proposition 4.19. *Let M be a free R-module of rank n, and let $\langle \cdot, \cdot \rangle : M \times M \to R$ be a perfect pairing. For each R-basis $(e_1, \ldots, r_n)$ of M there is a unique basis $(e_1', \ldots, e_n')$ of M such that*

$$\forall 1 \leq i, j \leq n, \ \langle e_i', e_j \rangle = \delta_{i,j} = \begin{cases} 1 & i = j \\ 0 & \textit{otherwise} \end{cases}.$$

Let R be a Noetherian domain with fraction field k, and let V be a finite-dimensional k-vector space. An **R-lattice in V** is a finitely generated R-submodule Λ of V that spans V as a k-vector space: equivalently, the natural map

$$\Lambda \otimes_R k \to V, \ x \otimes \alpha \mapsto \alpha x$$

is an isomorphism.

4.1. AKLB Applications.

Proposition 4.20. *Let R be a 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. Then:*

a) *Every element of L may be written as $\frac{s}{r}$ with $s \in S$ and $r \in R$.*
b) *Thus $\langle S \rangle_K = L$ and L is the fraction field of S.*

Proof. Let $\alpha \in L$. By scaling the minimal polynomial of α by an element of $R^\bullet$ we get a polynomial

$$f(t) = a_n t^n + \ldots + a_1 t + a_0 \in R[t]$$

such that $a_n \neq 0$ and $f(\alpha) = 0$. Thus

$$a_n^{n-1} f(\frac{\alpha}{a_n}) = t^n + a_{n-1}t^{n-1} + a_n a_{n-2} t^{n-2} + \ldots + a_n^{n-2} a_1 t + a_n^{n-1} a_0 \in R[t]$$

is monic and has $a_n\alpha$ as a root. So $a_n\alpha$ is integral over R, and thus $s := a_n\alpha$ lies in S, the integral closure of A in L and $\alpha = \frac{s}{a_n}$, establishing part a). It follows immediately that $\langle S \rangle_K = L$, and then the fraction field of S contains S and in particular contains R hence also contains the fraction field K of R. So the fraction field of S is L. □

Theorem 4.21 (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: $\langle x, y \rangle := T_{B/A}(xy)$. Let $x \in S$. By Corollary 4.11, 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 4.20 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

$$\Lambda := \langle e_1, \ldots, e_n \rangle_A$$

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.

If I is a nonzero ideal of A, consider the **pushforward**

$$\iota_*(I) \coloneqq IB.$$

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 [**CA**, Thm. 14.19] the ring $B_{\mathfrak{p}} = (A \setminus \mathfrak{p})^{-1}B$ is the integral closure of $A_{\mathfrak{p}}$ in L. If $\mathfrak{p}B = B$, then $\mathfrak{p}B_{\mathfrak{p}} = B_{\mathfrak{p}}$, which contradicts [**CA**, Lemma 14.12].

Or better: by [**CA**, Thm. 14.13] there is a prime 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.

Standard properties of integral extensions tell us that the pullback maps

$$\iota^* : \operatorname{Spec} B \to \operatorname{Spec} A, \;\; \iota^* : \operatorname{MaxSpec} B \to \operatorname{MaxSpec} A$$

are both surjective.

Exercise 4.16. *Show:* $\iota_*(IJ) = \iota_*(I)\iota_*(J)$.

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 $\mathfrak{p}$ and is also denoted $e(\mathcal{P}_i|\mathfrak{p})$.

The ideals $\mathcal{P}_1, \ldots, \mathcal{P}_r$ of B are precisely the prime ideals of S that contain $\mathfrak{p}$. We claim that

$$(\iota^*)^{-1}\{\mathfrak{p}\} = \{\mathcal{P}_1, \ldots, \mathcal{P}_r\}.$$

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**

$$f_{\mathcal{P}} = f(\mathcal{P}|\mathfrak{p}) \coloneqq [S/\mathcal{P} : R/\mathfrak{p}].$$

Lemma 4.22. *Let A be a Dedekind domain with fraction field K, let $K \subset L \subset M$ 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.*[1] *Let $\mathfrak{r} \in \operatorname{MaxSpec} C$, let $\mathfrak{q} := \mathfrak{r} \cap B$ and let $\mathfrak{p} := \mathfrak{q} \cap A$. 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 4.17. *Prove Lemma 4.22.*

Lemma 4.23. *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 $S := R \setminus \mathfrak{p}$ and $R_\mathfrak{p} := S^{-1}R$. 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 4.24. *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 $\sum_{\mathcal{P}|\mathfrak{p}} e_\mathcal{P} f_\mathcal{P} = [L : K]$.*

Proof. Put $n := [L : K]$.
a) Let $S := A \setminus \mathfrak{p}$, and let $A_\mathfrak{p} := S^{-1}A$, $B_\mathfrak{p} := S^{-1}B$. Then

$$A_\mathfrak{p}/\mathfrak{p}A_\mathfrak{p} = S^{-1}A/(\mathfrak{p}S^{-1}A) \cong A/\mathfrak{p}$$

and

$$B_\mathfrak{p}/\mathfrak{p}B_\mathfrak{p} = (S^{-1}B)/(\mathfrak{p}S^{-1}B) \cong B/\mathfrak{p}B.$$

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 thus that 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

$$n = [L : K] = \dim_{A/\mathfrak{p}} B/\mathfrak{p}B = \sum_{i=1}^{g} \dim_{A/\mathfrak{p}} B/\mathcal{P}_i^{e_i}.$$

[1] It follows that C is finitely generated as an A-module.

Now consider

$$B \supseteq \mathcal{P}_i \supseteq \mathcal{P}_i^2 \supseteq \ldots \supseteq \mathcal{P}_i^{e_i}.$$

By Lemma 4.23, 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 4.24 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.
- 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 $\mathfrak{p}$.

EXAMPLE 4.25. *Let l/k be an inseparable field extension of finite degree n, let $A := k[t]$, a PID with fraction field $K = k(t)$. Let $L = l(t)$. The integral clousre of A in L is $B = l[t]$. Then an l-basis for k is a basis for B as an A-module. Let $\mathfrak{p} = (t)$. Then $\mathfrak{p}B = tB$ is still prime. We have $A/\mathfrak{p} = k$ and $B/\mathfrak{p}B = l$. So $\mathfrak{p}$ is ramified in L/K even though there is a unique prime of B lying over $\mathfrak{p}$.*

EXERCISE 4.18. *Show: if $\mathfrak{p}$ in A splits completely in B, then L/K is unramified over $\mathfrak{p}$.*

EXAMPLE 4.26. *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. Then for any $\mathfrak{p} \in \operatorname{Spec} R$ there is a unique prime of S lying over $\mathfrak{p}$, namely*

$$\operatorname{rad}(\mathfrak{p}B) := \{x \in B \mid x^n \in \mathfrak{p}B \textit{ for some } n \in \mathbb{Z}^+\}.$$

This is [**CA**, Lemma 14.20].

5. 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 4.19. *Show: for $x_1, \ldots, x_n$ we have $\delta(x_1, \ldots, x_n) \neq 0$ if and only if $x_1 \ldots, x_n$ are linearly independent over R.*

Since A is integrally closed, the quadratic lattice B is *integral*: $\langle B, B \rangle \subseteq A$. It follows that for any integral A-lattice Λ in B, for the discriminant δ_Λ of Λ (cf. §3.5) we have

$$\delta_\Lambda \in \operatorname{Int} A.$$

Especially, we define the **discriminant ideal** $\delta_{B/A}$ to be δ_B.

PROPOSITION 4.27. *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 (7). Part b) follows from part a) using the Vandermonde determinant. □

PROPOSITION 4.28. *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 4.29. *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 δ be the discriminant ideal of B/A. For $\mathfrak{p} \in \operatorname{MaxSpec} R$, 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 $B_{\mathfrak{p}} := B \otimes_A A_{\mathfrak{p}}$. Now A is a DVR and B 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 4.3 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. □

6. The Ideal Norm

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, so B is a Dedekind domain and finitely generated as an A-module. Let $\iota : A \hookrightarrow B$ be the inclusion map.

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 4.30. *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 4.31. *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

$$0 \to J_2/(J_1J_2) \to B/(J_1J_2) \to B/J_2 \to 0,$$

so $\chi_A(B/J_1J_2) = \chi_A(J_2/(J_1J_2))\chi_A(B/J_2)$. By Lemma 4.30 we know that $J_2/(J_1J_2)$ and B/J_1 are isomorphic B-modules, so certainly they are isomorphic A-modules. Thus $\chi_A(J_2/(J_1J_2) = \chi_A(B/J_1)$, 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

$$N(IJ^{-1}) := \frac{N(I)}{N(J)}. \tag{12}$$

Indeed, by Proposition 4.31, 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 $\chi_A(B/J)$.

Happily, (1) and (2) turn out to be the same. For notational simplicity, let us define the ideal norm of a fractional ideal via (12). Then:

Proposition 4.32. *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 4.33 (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. See [**CA**, Thm. 22.3]. $\square$

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 4.34. *If $[L : K] = n$, then for all $I \in \operatorname{Frac} A$ we have $N(\iota_*(I)) = I^n$.*

Proof. 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 4.24b), we get

$$N(\iota^*(\mathfrak{p}))) = \prod_{i=1}^{r} \mathfrak{p}^{e_{\mathcal{P}|\mathfrak{p}} f_{\mathcal{P}|\mathfrak{p}}} = \mathfrak{p}^{\sum_{i=1}^{r} e(\mathcal{P}|\mathfrak{p}) f(\mathcal{P}|\mathfrak{p})} = \mathfrak{p}^n. \qquad \square$$

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 4.35. *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 3.6 we have

$$\chi_A(B/(\beta B)) = (\det \beta \cdot) = N_{L/K}(\beta). \qquad \square$$

Proposition 4.35 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.N(

Theorem 4.36. *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 $I_{\mathfrak{p}} \subseteq N(J_{\mathfrak{p}})$. $\square$

7. Dedekind-Kummer and Monogenicity

7.1. Dedekind-Kummer Version 1.

Exercise 4.20. *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 4.21. *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 I and J be nonzero ideals of B. Suppose that $I \subseteq J$ and $N(I) = N(J)$. Show: $I = J$.*

THEOREM 4.37 (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 4.21.

So: we have

$$N(\prod_{i=1}^{r} \mathcal{P}_\rangle^{e_i}) = \mathfrak{p}^{\sum_{i=1}^{r} f(\mathcal{P}_i|\mathfrak{p}) e_i} = \mathfrak{p}^{\sum_{i=1}^{r} e_i \deg \overline{g_i}} = \mathfrak{p}^{\deg f} = \mathfrak{p}^n. \qquad \square.$$

Let us give some applications.

EXAMPLE 4.38. *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* $\underline{D}$ *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 4.22. *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 4.39. *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 4.40. *Let* $N \in \mathbb{Z}^{\geq 3}$*. Let* $\zeta_N = e^{2\pi i/N}$ *and put* $K := \mathbb{Q}(\zeta_N)$*, the* N*th cyclotomic field. By* [**FT**, Thm. 9.8]*, the minimal polynomial for* ζ_N *is* $\Phi_N(t)$*, the monic polynomial whose roots are the primitive* N*th 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* N*th 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* N*th 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 4.37 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.

Proposition 4.41. *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. Suppose that there is $\mathfrak{p} \in \operatorname{MaxSpec} R$ with the following properties:*

(i) *The residue field $A/\mathfrak{p}$ is finite, say of order q.*
(ii) *There are more than q prime ideals $\mathcal{P}$ of B such that $\mathcal{P}$ lies over $\mathfrak{p}$ and $f(\mathcal{P}|\mathfrak{p}) = 1$.*

Then B is not monogenic over A.

Proof. The idea is simple: seeking a contradiction, we suppose that $B = A[\alpha] \cong A[t]/(f)$ for an irreducible monic polynomial f. Applying Theorem 4.37 and hypotheses (i) and (ii), we will get a contradiction.

Indeed, let $\overline{f}$ be the image of f in the polynomial ring $(A/\mathfrak{p})[t]$. By Theorem 4.37, the primes $\mathcal{P}$ of B lying over $\mathfrak{p}$ are in bijection with the distinct irreducible factors $\overline{g}$ of $\overline{f}$ and moreover we have $f(\mathcal{P}|\mathfrak{p}) = \deg \overline{g}$. It follows then that the degree 1 primes lying over $\mathfrak{p}$ – i.e., the primes $\mathcal{P}$ with $f(\mathcal{P}|\mathfrak{p}) = 1$ – are in bijection with the distinct *linear* factors of $\overline{f}$. Because $A/\mathfrak{p}$ is finite of cardinality q, every such linear factor is of the form $t - \alpha$ for some $\alpha \in A/\mathfrak{p}$, so there are at most q such factors....contradicting (ii). □

If we apply Proposition 4.41 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 bound: 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.

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_1L_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 $K_{d_1,d_2} := \mathbb{Q}(\sqrt{d_1}, \sqrt{d_2})$ 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 4.22, 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

4.41, 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 $d_1 \equiv d_2 \equiv 1 \pmod 3$. 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 4.41, the Dedekind domain $\mathbb{Z}_{K_{d_1,d_2}}$ is not monogenic over $\mathbb{Z}$.

7.2. A Supplement to Dedekind-Kummer. The material of this section comes from [**Se:CL**, Ch. III].

PROPOSITION 4.42. *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 4.43. *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 $g := \sum_{n=2}^{\infty} b_n (t-a)^{n-2}$, 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 4.44. *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 $k := R/\mathfrak{p}$ and $l := S/\mathcal{P}$, so $f = [l : k]$. By Theorem 4.24 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 $\{x^i\pi^j\}_{0 \leq i < f,\ 0 \leq j < e}$ span S as an R-module.[2] 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 $0 \leq m < e$, 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 $1 \leq m < e$ the elements $x^i\pi^j$ with $0 \leq j < m$ 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

$$x - \sum_{i,j} r_{i,j} x^i \pi^i - \sum_{i=0}^{f-1} a_i x^i \pi^m \in \pi^{m+1} S.$$

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 4.43 there is $s \in S$ such that

$$g(x + \pi) = g(x) + \pi g'(x) + \pi^2 s.$$

[2] Since L/K is separable, S is free of rank n as an R-module. By [**CA**, Thm. 3.44], the claim implies that $\{x^i\pi^j\} - 0 \leq i < f,\ 0 \leq j < e$ in fact form an R-basis of 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 $\pi := g(x)$. By Step 1, the elements $\{x^i g(x)^j\}_{0 \leq i < f,\ 0 \leq j < e}$ span S over R. Thus $S = R[x]$. □

8. 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 4.21 we observed that B^* is an A-lattice in L and

$$B \subseteq B^*.$$

We make the following additional observation:

Lemma 4.45. *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 4.46. *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 4.47. *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 4.48. *We have*

$$\delta_{B/A} = N_{B/A}(\Delta_{B/A}).$$

Proof. Using Corollary 3.15 and Proposition 4.32, we get

$$\delta_{B/A} = \chi_A(B^*/B) = \chi_A(B/B^*)^{-1} = N(B^*)^{-1} = N((B^*)^{-1}) = N(\Delta_{B/A}). \quad \square$$

Lemma 4.49. *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 4.50 (Dedekind's Different Theorem). *Let $\mathcal{P} \in \operatorname{MaxSpec} B$ lie over $\mathfrak{p} \in \operatorname{MaxSpec} A$. Let $e = e(\mathcal{P}|\mathfrak{p})$. Then:*

a) *If $e \notin \mathfrak{p}$ and $(B/\mathcal{P})/(A/\mathfrak{p})$ is separable, then* $\operatorname{ord}_{\mathcal{P}}(\Delta_{B/A}) = e - 1$.
b) *If $e \in \mathfrak{p}$ or $(B/\mathcal{P})/(A/\mathfrak{p})$ is inseparable, then* $\operatorname{ord}_{\mathcal{P}}(\Delta_{B/A}) \geq e$.

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:

$$\mathcal{P}^{e-1} \mid \Delta_{B/A} \tag{13}$$

and

$$\mathcal{P}^{e} \mid \Delta_{B/A} \iff e \in \mathfrak{p} \text{ or } (B/(\mathcal{P}))/(A/\mathfrak{p}) \text{ is inseparable.} \tag{14}$$

Step 1: We will show (13). For this, write

$$\mathfrak{p}B = \mathcal{P}^{e-1}\mathfrak{a}.$$

Since by definition $e = \operatorname{ord}_{\mathcal{P}}(\mathfrak{p}B)$, we still have $\mathcal{P} \mid \mathfrak{a}$. By Lemma 4.49 it suffices to show that $\operatorname{Tr}_{L/K}(\mathcal{P}^{-(e-1)}) \subseteq A$. Since

$$\mathcal{P}^{-(e-1)} = \frac{1}{p}\mathfrak{a},$$

we have $\operatorname{Tr}_{L/K}(\mathcal{P}^{-(e-1)}) \subseteq A$ if and only if

$$\operatorname{Tr}_{L/K}(\mathfrak{a}) \subseteq pA.$$

Let $\alpha \in \mathfrak{a}$. Then $\operatorname{Tr}_{L/K}(\alpha) = \operatorname{Tr}_{B/A}(\alpha)$ and

$$\operatorname{Tr}_{B/A}(\alpha) \pmod{(p)} = \operatorname{Tr}_{(B/pB)/A/(p)}(\overline{\alpha}).$$

Since $\mathfrak{p}B = pB$ and $\mathfrak{a}$ are divisible by the same prime ideals of B, they have the same radical: $\operatorname{rad}(pB) = \operatorname{rad}(\mathfrak{a})$. 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 (14). 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 $\operatorname{Tr}(\mathfrak{b}) \subseteq pA$ if and only if:

$$\forall \beta \in \mathfrak{b},\ \operatorname{Tr}_{(B/pB)/A/pA}(\overline{\beta}) = 0.$$

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 $\operatorname{Tr}_{X/(A/pA)}(x)$.

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 4.12 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 4.51. *Let $\mathcal{P} \in \operatorname{MaxSpec} B$ lie over $\mathfrak{p} \in \operatorname{MaxSpec} A$. 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 4.52. *The argument that a) $\implies$ b) in Corollary 4.51 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 4.51 in his notes.*

Corollary 4.53. *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*

$$v_p(\delta_K) \geq n - \sum_{i=1}^{g} f_i. \tag{15}$$

b) *Equality holds in (15) 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 4.50, 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 4.50, 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 4.54. *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 4.23. *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*

$$\sum_{i=1}^n \frac{\alpha_i^k}{f'(\alpha_i)} \frac{f(t)}{t-\alpha_i} = t^k. \tag{16}$$

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 (16).)*

Theorem 4.55. *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* $\Lambda := A[\alpha]$. *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 4.23, 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

$$\begin{gathered} c_{n-1}(\alpha) = 1, \\ c_{n-2}(\alpha) = a_{n-1} + \alpha, \\ c_{n-3}(\alpha) = a_{n-2} + a_{n-1}\alpha + \alpha^2, \\ \vdots \\ c_1(\alpha) = a_2 + a_3\alpha + \ldots + a_{n-2}\alpha^{n-2}, \\ c_0(\alpha) = a_1 + a_2\alpha + \ldots + \alpha^{n-1}. \end{gathered}$$

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

$$\Lambda^* = \frac{1}{f'(\alpha)} \langle c_0(\alpha), \ldots, c_{n-1}(\alpha) \rangle_A = \frac{1}{f'(\alpha)} \langle 1, \alpha, \ldots, \alpha^{n-1} \rangle_A = \frac{1}{f'(\alpha)} \Lambda. \qquad \square$$

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 4.55 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 4.24. *Let A be a domain, let $f \in A[t]$ be a monic polynomial, and let $B := A[t]/(f)$. Let $\Omega_{B/A}$ be the module of Kähler differentials (see* [**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:*

$$\operatorname{ann} \Omega_{B/A} = \Delta_{B/A}. \tag{17}$$

In fact (17) 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.

9. Prime Decomposition in a Galois Extension

9.1. 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 4.21, B is an integrally closed Noetherian domain that is finitely generated as an A-module, and moreover $\dim B = \dim A$.

Let $G = \operatorname{Aut}(L/K)$ be the Galois group of L/K. For a subring X of L, we put

$$X^G := \{x \in X \mid \forall \sigma \in G,\ \sigma(x) = x\}.$$

It is immediate that if Xvis a subring of L, then X^G is a subring of K. Which subring we get is not so immediately clear, except in one case: by basic Galois theory, we have $L^G = K$.

Proposition 4.56. *With notation as above, we have $B^G = A$.*

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 4.25. *Let B be a domain, and let G be a finite group acting effectively on B by ring automorphisms. Let L be the fraction field of B and let K be the fraction field of A.*

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* $\operatorname{Aut}(L/K) = G$.
b) *Show that there is a unique extension of G to an action on 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* $\operatorname{Aut}(L(t)/K(t)) = G$.
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 4.57. *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 $\mathcal{P} \in \operatorname{Spec} B$ 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 $\operatorname{Spec} B$ and this action stabilizes each fiber of the map $\iota^* : \operatorname{Spec} B \to \operatorname{Spec} B^G$.
b) *Let $\mathfrak{p} \in \operatorname{Spec} B^G$. 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

$$N_G(x) \in \mathcal{P}_1 \cap B^G = \mathfrak{p} \subseteq \mathcal{P}_{\in}.$$

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

$$\mathcal{P}_1 \subset \bigcup_{\sigma \in G} \sigma(\mathcal{P}_2).$$

By part a) and Prime Avoidance (Lemma 1.6) 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 4.26. *Prove Proposition 4.57a).*

9.2. Galois Symmetry. We now intersect with the standard setup of this chapter: namely, suppose that A is a Dedekind domain with fraction field K, that L/K is a *Galois* extension of finite degree n, with $G = \operatorname{Aut}(L/K)$, and B is the integral closure of A in L. Then all of the previous results apply: in particular, for any $\mathfrak{p} \in \operatorname{MaxSpec} A$, 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 4.57 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 $\operatorname{Frac} B$. The following result analyzes this action.

Proposition 4.58. *For $I \in \operatorname{Frac} B$, 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 $\mathfrak{p} \in \operatorname{MaxSpec} A$, if $\mathcal{P}_1, \mathcal{P}_2 \in \operatorname{MaxSpec} B$ 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

$$I = \prod_{\mathcal{P}|\mathfrak{p}} \prod_{\mathfrak{p} \in \operatorname{MaxSpec} A} \mathcal{P}^{v_{\mathcal{P}}(I)}.$$

For $\mathfrak{p} \in \operatorname{MaxSpec} A$, 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 4.58 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).

Corollary 4.59. *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 4.27. *Let $I \in \operatorname{Frac} B$. As explained above, condition (iii) of Proposition 4.58 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 $e_{\mathfrak{p}}$.)*

9.3. 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**

$$D(\mathcal{P}|\mathfrak{p}) := \{\sigma \in L \mid \sigma(\mathcal{P}) = \mathcal{P}\}.$$

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 4.59 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

$$k(\mathfrak{p}) := A/\mathfrak{p}$$

for the residue field at $\mathfrak{p}$ and

$$l(\mathcal{P}) := B/\mathcal{P}$$

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 $D := D(\mathcal{P}/\mathfrak{p})$ 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 $\mathfrak{p}_D := \mathcal{P} \cap A_D$, so $\mathcal{P} \mid \mathfrak{p}_D \mid \mathfrak{p}$. On the one hand, $D = \operatorname{Aut}(L/L^D)$ acts transitively on the set of primes of B lying over $\mathfrak{p}_D$, but 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 two statements 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.

Exercise 4.28. *With notation as above, 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:*

$$D(\mathcal{P}|\mathfrak{p}_M) = D(\mathcal{P}|\mathfrak{p}) \cap \operatorname{Aut}(L/M).$$

b) *Show: $L^{D(\mathcal{P}|\mathfrak{p}_M)} = L^D M$.*

Exercise 4.29. *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 $\mathfrak{p}_M := \mathcal{P} \cap M$. 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.)

Corollary 4.60. *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^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 $F \subseteq L^s$.*

(ii) *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 4.29, 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 $G = \operatorname{Aut}(L/K)$, 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 4.61. *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 $\mathfrak{p} \in \operatorname{MaxSpec} A$ 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 4.61. 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 4.62. *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 $\mathfrak{p} \in \operatorname{MaxSpec} A$, 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 4.61 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

$$\mathfrak{r} : D(\mathcal{P}/\mathfrak{p}) \to \operatorname{Aut}(l(\mathcal{P})/k(\mathfrak{p})) :$$

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 4.30. *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 4.63. *With notation as above, suppose that for $\mathfrak{p} \in \operatorname{MaxSpec} A$ the residue field $k(\mathfrak{p}) := A/\mathfrak{p}$ is perfect. Let $\mathcal{P} \in \operatorname{MaxSpec} B$ lie over $\mathfrak{p}$, and put $l(\mathcal{P}) := B/\mathcal{P}$. Then:*

a) *The extension $l(\mathcal{P})/k(\mathfrak{p})$ is finite Galois (of degree $f_{\mathfrak{p}}$).*
b) *The reduction map $\mathfrak{r} : \operatorname{Aut}(L/K) \to \operatorname{Aut}(l(\mathcal{P})/l(\mathfrak{p}))$ is surjective.*
c) *We have $\# I(\mathcal{P}/\mathfrak{p}) = \# \operatorname{Ker} \mathfrak{r} = e_{\mathfrak{p}}$.*

Proof. a) Let us abbreviate $D := D(\mathcal{P}/\mathfrak{p})$ and $I := I(\mathcal{P}/\mathfrak{p})$. Let A_D be the integral closure of A in L^D, and let $\mathfrak{p}_D := \mathcal{P} \cap L^D$. Let's further put

$$e_D := e(\mathcal{P}|\mathfrak{p}_D),\ f_D := f(\mathcal{P}/\mathfrak{p}_D).$$

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 $\mathfrak{r}(\sigma)(\overline{x})$ 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 $\mathrm{Aut}(l(\mathcal{P})/k(\mathfrak{p}))$ is of the form $\mathfrak{r}(\sigma)$ for some $\sigma \in D$. Thus $\mathfrak{r}$ is surjective.
c) We know that $\mathfrak{r} : D \rightarrow \mathrm{Aut}(l(\mathcal{P})/k(\mathfrak{p})$ is surjective with kernel $I(\mathcal{P}/\mathfrak{p})$, so

$$\#I(\mathcal{P}/\mathfrak{p}) = \frac{\#D}{\#\,\mathrm{Aut}(l(\mathcal{P})/k(\mathfrak{p}))} = \frac{e_{\mathfrak{p}}f_{\mathfrak{p}}}{f_{\mathfrak{p}}} = e_{\mathfrak{p}}. \qquad \square$$

For L/K a finite Galois extension with $G = \mathrm{Aut}(L/K)$ and $\mathcal{P} \in \mathrm{MaxSpec}\,B$ lying over $\mathfrak{p} \in \mathrm{MaxSpec}\,A$, using the inertia group we can refine our above filtration of subfields to:

$$K \overset{r}{\subset} L^{D(\mathcal{P}|\mathfrak{p})} \overset{f}{\subset} L^{I(\mathcal{P}|\mathfrak{p})} \overset{e}{\subset} L.$$

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 4.31. *Let L/K be finite Galois, and 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:*

$$I(\mathcal{P}|\mathfrak{p}_M) = I(\mathcal{P}|\mathfrak{p}) \cap \mathrm{Aut}(L/M).$$

b) *Show: $L^{I(\mathcal{P}|\mathfrak{p}_M)} = L^D M$.*

Exercise 4.32. *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 $\mathfrak{p}_M := \mathcal{P} \cap A_M$. 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 4.64. *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 $\mathfrak{p} \in \mathrm{MaxSpec}\,A$.*

(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^s/K.*

Exercise 4.33. *Prove Corollary 4.64.*

Theorem 4.65. *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 $\mathfrak{p} \in \operatorname{MaxSpec} A$ be a prime that is unramified in A_i for all i. Then $\mathfrak{p}$ is unramified in B.

Exercise 4.34. *Prove Theorem 4.65.*

Corollary 4.66. *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.*

9.4. 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 4.63, 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 4.35. *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 $k(\mathfrak{p}) := A/\mathfrak{p}$ 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, $\operatorname{Aut}(l(\mathcal{P})/k(\mathfrak{p})$ 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 4.36. *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 $\sigma \in G = \operatorname{Aut}(L/k)$.*

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.*

9.5. 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 4.67. *Suppose that L/K is normal, and put $G = \operatorname{Aut}(L/K)$. Let $\mathfrak{p} \in \operatorname{MaxSpec} R$. Then G acts transitively on $\operatorname{MaxSpec} S/\mathfrak{p}S$, 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 $x \in L$,

$$N_{L/K}(x) = \left(\prod_{\sigma \in G} \sigma(x)\right)^{p^a}. \tag{18}$$

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

$$N_{L/K}(x) = x\left(x^{p^a-1} \cdot \prod_{1 \neq \sigma \in G} \sigma(x)\right) \in \mathcal{P}_2 \cap R = \mathfrak{p}.$$

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 $N_{L/K}(x) \in \mathfrak{p} \subset \mathcal{P}_1$ but by (18) is a product of elements none of which are in $\mathcal{P}_1$, contradicting the primality of $\mathcal{P}_1$. □

EXERCISE 4.37. *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 4.67 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 4.38. *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.)*

10. Hensel's Different Theorem

Theorem 4.68 (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:*

$$v_{\mathcal{P}}(\Delta_{B/A}) \leq e - 1 + v_{\mathcal{P}}(e) \tag{19}$$

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 4.50a) 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 4.68, 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 4.44, 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 4.55 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 $s = v_{\mathcal{P}}(f'(\alpha)) = 0 = e - 1$.[3] By Corollary 4.64 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 4.46 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

$$\begin{aligned} v_{\mathcal{P}}(i a_i \alpha^{i-1}) &= v_{\mathcal{P}}(i_+ v_{\mathcal{P}}(a_i) + (i-1) v_{\mathcal{P}}(\alpha) \\ &= e\left(v_{\mathfrak{p}}(i) + v_{\mathfrak{p}}(a_i)\right) + (i-1) \equiv i - 1 \pmod{e}, \end{aligned}$$

[3] We knew this already from Theorem 4.50, but this is a different argument from the one given above.

so all of these valuations are distinct. It follows that

$$s = v_{\mathcal{P}}(f'(\alpha)) = \min_{1 \leq e} v_{\mathcal{P}}(ia_i\alpha^{i-1}) \leq v_{\mathcal{P}}(e\alpha^{e-1}) = e - 1 + v_{\mathcal{P}}(e). \qquad \Box$$

11. 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 $\tau_{\mathfrak{p}} \subset \mathrm{Gal}(L/K)$.

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 $T \subset \Sigma_R$. 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.

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 4.39. *Let $T \subset \Sigma_R$.*

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** $T \subset G$ will be a subset which is invariant under conjugation: for all $\sigma \in G$, $\sigma T \sigma^{-1} = S$.

EXERCISE 4.40. *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.

11.1. The Chebotarev Density Theorem.

THEOREM 4.69. *(Chebotarev, 1922) Let S/R be a Galois extension of global rings, with $G =$ $\mathrm{Gal}(L/K)$. Let $X \subset G$ be a normal subset, and consider the* ***Chebotarev set*** *$T_X \subset \Sigma_R$ 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 4.41. *Suppose that you know Chebotarev Density when $T \subset G$ is a single conjugacy class. Deduce the general case.*

Corollary 4.70. *For any separable extension S/R of local rings with $[L : K] = n$, the density of the set $\mathcal{S}$ of primes $\mathfrak{p}$ of R which split completely in S is $\frac{1}{\# \operatorname{Gal}(M/K)}$, where M is the Galois closure of L/K. In particular we have*

$$\frac{1}{n!} \leq \delta(S) \leq \frac{1}{n}.$$

Exercise 4.42. *Prove Corollary 4.70.*

Corollary 4.71. *(Equidistribution of Frobenius elements in the abelian case) With notation as above, suppose that $G = \operatorname{Gal}(L/K)$ 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 4.70 and 4.71 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 $\frac{1}{n}$.[4]

Example 4.72. *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 4.73. *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 $\operatorname{Gal}(L/K) = (\mathbb{Z}/n\mathbb{Z})^\times$, 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 4.74. *(Dirichlet's Theorem) For $n \in \mathbb{Z}^+$ and any a with $\gcd(a, n) = 1$, the set of primes p which are congruent to $a \pmod n$ has density $\frac{1}{\varphi(n)}$.*

Exercise 4.43. *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.*[5]

[4] This special case was proved much earlier by Frobenius: see below.

[5] This is proved in [**Br86**]. The generalization to polynomials over any global ring is proved in [**GSS05**].

11.2. Some further remarks.

Theorem 4.69 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 4.70.

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 4.69: 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 4.69 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 5

Geometry of Numbers

1. Geometry of Numbers

1.1. Convex subsets of Euclidean space. 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 5.1. *A bounded subset Ω of $\mathbb{R}^N$ can have at most one center.*

We will mostly be interested in properties of subsets of $\mathbb{R}^N$ that are isometry invariants. In particular it will usually be no loss of generality to assume that $0 \in \Omega$. So 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 5.2. *Let Ω be a nonempty subset of $\mathbb{R}$. Show: Ω is convex if and only if Ω is an interval.*

Exercise 5.3.

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 5.4. *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 $S \subset \mathbb{R}^N$, 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, we call $\operatorname{Conv} S$ an **n-simplex**.

Exercise 5.5. *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 5.6. *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 5.7. *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 5.1. *A bounded convex subset $\Omega \subseteq \mathbb{R}^N$ is Jordan measurable (hence Lebesgue measurable).*

Proof. See e.g. [**Sz97**]. □

1.2. Lattices in Euclidean Space. Let V be a finite-dimensional $\mathbb{R}$-vector space. A **lattice** Λ in V is the $\mathbb{Z}$-span of an $\mathbb{R}$-basis of V. Thus if $\dim V = N$ we have $\Lambda \cong_{\mathbb{Z}} \mathbb{Z}^N$.

Earlier in our course we studied lattices in a finite-dimensional K-vector space, where K is the fraction field of a Dedekind domain R. When $R = \mathbb{Z}$, a lattice in a finite-dimensional $\mathbb{Q}$-vector space V is indeed just the $\mathbb{Z}$-span of a $\mathbb{Q}$-basis of V. (Because $\mathbb{Z}$ is a PID, $\mathbb{Z}$-lattices must be free.) Thus our definition of lattices over *real* vector spaces is as close as it could possibly by to our definition: indeed, we just replaced $\mathbb{Q}$ by $\mathbb{R}$. However, this change of course causes some, um, changes. Since $\mathbb{R}$ has infinite dimension as a $\mathbb{Q}$-vector space, there are infinite subsets of $\mathbb{R}^N$ that are $\mathbb{Q}$-linearly independent but not $\mathbb{R}$-linearly independent, and it follows that V contains subgroups isomorphic to $\mathbb{Z}^n$ for all $n \in \mathbb{Z}^+$. Thus, whereas in an N-dimensional $\mathbb{Q}$-vector space, every subgroup isomorphic to $\mathbb{Z}^N$ is a $\mathbb{Q}$-latice, when $N \geq 2$ this does not hold in an N-dimensional $\mathbb{R}$-vector space: the problem is precisely that the subgroup Λ could lie in a proper $\mathbb{R}$-subspace.

For the following discussion we may as well choose an $\mathbb{R}$-basis of V and thereby identify V with $\mathbb{R}^N$.

For a subgroup Λ of $\mathbb{R}^N$ such that $\Lambda \cong_{\mathbb{Z}} \mathbb{Z}^N$, the extra condition on Λ to be a lattice is topological: we claim that it is necessary and sufficient for Λ to be discrete: that is, for all $x \in \Lambda$ there is $\delta > 0$ such that the open δ-ball $B^\circ(x, \delta)$ centered at x contains no point of $\Lambda \setminus \{x\}$. One direction of this is pretty clear: we can start with the fact that the standard lattice $\mathbb{Z}^N$ in $\mathbb{R}^N$ is a discrete subgroup. Moreover, since $\mathrm{GL}(\mathbb{R}^N) = \mathrm{GL}_N(\mathbb{R})$ acts $\mathbb{R}$-linearly on $\mathbb{R}^N$, it acts on subgroups of $(\mathbb{R}^N, +)$ and it sends lattices to lattices: indeed, for $m \in \mathrm{GL}_N(\mathbb{R})$ if Λ is the $\mathbb{Z}$-module spanned by the $\mathbb{R}$-basis $v_1, \ldots, v_N$ of $\mathbb{R}^N$, then $m\Lambda$ is the $\mathbb{Z}$-module spanned by the $\mathbb{R}$-basis $mv_1, \ldots, mv_N$ of $\mathbb{R}^N$. By the way, this action is clearly transitive because $\mathrm{GL}_N(\mathbb{R})$ acts simply transitively on *ordered* $\mathbb{R}$-bases of $\mathbb{R}^N$, and the stabilizer of $\mathbb{Z}^N$ is $\mathrm{GL}_N(\mathbb{Z})$, so the set of all lattices in $\mathbb{R}^N$ can be identified with the coset space

$$\mathrm{GL}_N(\mathbb{R}) / \mathrm{GL}_N(\mathbb{Z}).$$

This in particular gives it the structure of a locally compact topological space. In this topology, two lattices Λ_1 and Λ_2 are "close together" if we can choose ordered $v_1, \ldots, v_N$ for Λ_1 and $w_1, \ldots, w_N$ for Λ_2 such that for all $1 \leq i \leq N$, the vectors v_i and w_i are "close together."

Anyway, a homeomorphism of topological spaces takes discrete subspaces to discrete subspaces, so this shows that every lattice in $\mathbb{R}^N$ is a discrete subgroup. The converse takes a little more work. We will work a bit more generally. First:

Lemma 5.2. *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 5.3. *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 5.2, 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

$$\mathcal{P} := \left\{ \sum_{i=1}^{r} x_i e_i \mid x_i \in [0,1] \right\}$$

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

$$x_j := jx - \sum_{i=1}^{r} \lfloor j\lambda_i \rfloor e_i.$$

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

$$\operatorname{Covol} \Lambda := |\det M_v|.$$

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

$$|\det M_w| = |\det M_v|.$$

So the covolume of a lattice in $\mathbb{R}^N$ is well-defined. However, we should also not neglect to explain why we are calling it a "covolume"! In general, if a group G acts on a topological space X by homeomorphisms, we have the notion of a **fundamental region** for the action of G. Strictly speaking, this should be a subset $R \subseteq X$ containing precisely one element from each G-orbit. We cannot doubt that fundamental regions exist in great abundance: they correspond to sections $\iota : G\backslash X \to X$ of the orbit map $q : X \to G\backslash X$. (This means that $q \circ \iota = 1_{G\backslash X}$.) Indeed, given any section ι its image $\iota(G\backslash X)$ is a fundamental region, and if R is a fundamental region then ι sends a G-orbit to the unique element of R lying in that orbit.

However, this definition of the fundamental region makes no use of the topology on X. In practice, it is much more enlightening and useful to choose fundamental regions with nice topological properties. For instance, consider $(\mathbb{Z}^N, +)$ acting on $\mathbb{R}^N$ by translation. Then $R := [0, 1)^N$ is a fundamental region. This is topologically *okay*, but I would rather it be either open or closed, which will cause us to loosen our definition of fundamental region slightly. Let us say that a family $\{Y_i\}_{i \in I}$ of subsets of a topological space X is a **tiling** of X if:

(T1) $\bigcup_{i \in I} \overline{Y_i} = X$, and
(T2) For all $i \neq j$, we have $Y_i^\circ \cap Y_j^\circ = \varnothing$.

As an example, let $I = \mathbb{Z}^N$ and for $i = (i_1, \ldots, i_N) \in \mathbb{Z}^N$, put

$$Y_i := \prod_{n=1}^{N} [i_n, i_n + 1].$$

This gives a tiling of $\mathbb{R}^N$ by "closed unit cubes," each of which is a translate of $Y_0 = [0,1]^N$ by an element of $\mathbb{Z}^N$. Going back to our general setup of a group G acting on a space X, let us change our mind slightly and say that a subset $Y \subseteq X$ is a **fundamental region** if $\{gY\}_{g \in G}$ is a tiling of X. Thus X is the union of the translates of $\overline{Y}$ under G but the union doesn't have to be disjoint: we allow $g_1 Y$ and $g_2 Y$ to intersect along their boundaries. In this context, we find that $[0,1]^N$ is a closed fundamental region for the action of $\mathbb{Z}^N$ on $\mathbb{R}^N$. In general, if Y is a closed fundamental region for the action of G on X, then

$$q|_Y : Y \to G \backslash X$$

is a continuous surjection. So for instance, if we have a compact fundamental region Y, then the quotient space $G \backslash X$ is compact.

In our situation we also have a measure on $\mathbb{R}^N$ – Lebesgue measure – that is translation invariant, an thus every subgroup of $\mathbb{R}^N$ acts on $\mathbb{R}^N$ by measure-preserving automorphisms. There is some general theorem here involving a topological space X equipped with a Borel measure μ and a group G acting on X by measure-preserving automorphisms. Then – perhaps under some additional hypotheses – there should exist a measurable fundamental region, and any two measurable fundamental regions will have the same measure. We can then define the measure of $G \backslash X$ to be the measure of any measurable fundamental region. But let us not digress to nail this down precsiely: we will be using only a very special case.

Indeed, if we have a lattice Λ in $\mathbb{R}^N$, then to any $\mathbb{Z}$-basis $v_1, \ldots, v_N$ of Λ we can attach a **fundamental parallelopiped**

$$P_v := \{x_1 v_1 + \ldots + x_N v_N \mid x_1, \ldots, x_N \in [0,1]\}.$$

Then P_v is a compact, convex fundamental region for Λ. Moreover, the volume (i.e., Lebesgue measure) of P_v is the covolume of Λ: indeed that $|\det M_v|$ is the volume of P_v is a standard interpretation of the determinant in linear algebra: or if you like, it is the linear case of the change of variables formula in multivariable calculus.vvThe reason we call this the *co*volume of Λ is that it is, first of all, certainly not the measure of Λ (Λ is countable so has measure zero) but of "the region between points of Λ." Indeed, $\operatorname{Covol} \Lambda$ bears an inverse relationship to the size of Λ:

Exercise 5.8. *Let $\Lambda_1 \subseteq \Lambda_2$ be two latices in $\mathbb{R}^N$. Show:*

$$\operatorname{Covol} \Lambda_1 = [\Lambda_2 : \Lambda_1] \operatorname{Covol} \Lambda_2.$$

Finally, we remark that different fundamental parallelopipeds 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 parallelopipeds 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 $\frac{1}{2}$).

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 5.9. *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.

One more fact about convex sets and volumes: let $M \in \mathrm{GL}_N(\mathbb{R})$; we identify M with the corresponding linear function $x \in \mathbb{R}^N \mapsto Mx$. Then it is a basic property of Lebesgue measure that for *any* measurable subset $S \subseteq \mathbb{R}^N$, the set $M(S) := \{M(s) \mid s \in S\}$ is measurable, and moreover we have

$$\operatorname{Vol}(M(S)) = |\det M| \operatorname{Vol}(S).$$

In particular, for $\alpha \in \mathbb{R}^{>0}$, we may define the **dilate of S by α** to be

$$\alpha S := \{\alpha s \mid s \in S\}.$$

Then $\alpha S = M_\alpha(S)$ where M_α is the diagonal matrix with all diagonal entries equal to α, so

$$\operatorname{Vol}(\alpha S) = |\det M_\alpha(S)| \operatorname{Vol}(S) = \alpha^N \operatorname{Vol}(S).$$

Moreover, for a lattice Λ in $\mathbb{R}^N$ and $M \in \mathrm{GL}_N(\mathbb{R})$ we have

$$\operatorname{Covol}(M(\Lambda)) = |\det M| \operatorname{Covol}\Lambda.$$

This follows (for instance) from the previous observation applied to a fundamental parallelopiped for Λ.

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 [**?**, 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

$$\frac{\mathrm{Vol}(M\Omega)}{\mathrm{Covol}(M\Lambda)} = \frac{|\det M| \,\mathrm{Vol}(\Omega)}{|\det M| \,\mathrm{Covol}(\Lambda)} = \frac{\mathrm{Vol}(\Omega)}{\mathrm{Covol}(\Lambda)},$$

so the ratio $\frac{\mathrm{Vol}(\Omega)}{\mathrm{Covol}(\Lambda)}$ 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 $\mathrm{Vol}\,\Omega > V_N$ we have $\Omega \cap (\mathbb{Z}^N)^\bullet \neq \varnothing$, then for all convex bodies Ω and lattices Λ with $\frac{\mathrm{Vol}(\Omega)}{\mathrm{Covol}(\Lambda)} > V_N$ we may choose $M \in \mathrm{GL}_N(\mathbb{R})$ such that $M\Lambda = \ Z^N$ and then

$$2^N < \frac{\mathrm{Vol}(\Omega)}{\mathrm{Covol}(\Lambda)} = \frac{\mathrm{Vol}(M(\Omega))}{\mathrm{Covol}(\mathbb{Z}^N)} = \mathrm{Vol}(M(\Omega)),$$

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 5.4. *(Minkowski's Convex Body Theorem) Let $\Omega \subset \mathbb{R}^N$ be a convex body, and let $\Lambda \subset \mathbb{R}^N$ be a lattice.*

a) *If* $\mathrm{Vol}\,\Omega > 2^N \,\mathrm{Covol}\,\Lambda$*, then* $\Omega \cap \Lambda^\bullet \neq \varnothing$.

b) *If Ω is compact and* $\mathrm{Vol}\,\Omega = 2^N \,\mathrm{Covol}\,\Lambda$*, 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 $\mathrm{Vol}\,\Omega \leq 1$.

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 $P := P_1 - P_2 \in (\mathbb{Z}^N)^\bullet$. 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 5.10. *Prove Theorem 5.4b).*
(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.)

2. The Additive Embedding

2.1. Basic Setup.

Let $K/\mathbb{Q}$ be a number field of degree N. Thus K is an N-dimensional $\mathbb{Q}$-vector space, so we may consider $\mathbb{Z}$-lattices in K, e.g. $\mathbb{Z}_K$. In the previous section we were studying $\mathbb{Z}$-lattices in finite-dimensional $\mathbb{R}$-vector spaces. Well, to any nontrivial $\mathbb{Q}$-vector space V we can attach an $\mathbb{R}$-vector space:

$$V_{\mathbb{R}} \coloneqq V \otimes_{\mathbb{Q}} \mathbb{R}.$$

If V was finite-dimensional, then every $\mathbb{Z}$-lattice in V is also a $\mathbb{Z}$-lattice in $V_{\mathbb{R}}$. (There are countably many $\mathbb{Z}$-lattices in V and uncountably many $\mathbb{Z}$-lattices in $\mathbb{R}$, so certainly most $\mathbb{Z}$-lattices in $V_{\mathbb{R}}$ are not contained in V.) Thus we may consider $K_{\mathbb{R}} \coloneqq K \otimes_{\mathbb{Q}} \mathbb{R}$ and thereby realize, e.g., $\mathbb{Z}_K$ as a $\mathbb{Z}$-lattice in $K_{\mathbb{R}}$.

This is indeed *most* of the idea of the additive embedding: $\mathbb{Z}$-lattices and $\mathbb{Z}$-orders in K may be realized as $\mathbb{Z}$-lattices in a real vector space, so Geometry of Numbers methods may be fruitfully brought to bear. But there is one more piece: $K_{\mathbb{R}}$ is isomorphic to $\mathbb{R}^N$, but not equal to it. So it is not clear how to define the covolume of a $\mathbb{Z}$-lattice in $K_{\mathbb{R}}$. From an abstract perspective, the extra ingredient necessary is a Haar measure on $K_{/\mathbb{R}}$, i.e., a translation invariant Borel measure. These are unique up to scaling, so the problem can be thought of as needeing to specify one lattice as "standard" and decreeing its covolume to be 1. (This suggests possibly taking $\mathbb{Z}_K$ as the standard lattice, but this is *not* what we want to do: then its covolume would be 1, whereas for what we actually do we will find that knowing $\operatorname{Covol} \mathbb{Z}_K$ is equivalent to knowing δ_K.) Alternately, if we choose an isomorphism $\iota : \mathbb{R}^N \to K_{\mathbb{R}}$ then the have chosen a basis $v_1, \ldots, v_N$ for $K_{\mathbb{R}}$ (the image of the standard basis of $\mathbb{R}^N$u under ι). We could then "transport the Lebesgue measure" from $\mathbb{R}^N$ to $K_{\mathbb{R}}$ under this isomorphism or just realize that this transport of structure means that the lattice $\Lambda_0 \coloneqq \langle v_1, \ldots, v_N \rangle_{\mathbb{Z}}$ gets covolume 1.

The correct thing to do involves the use of the N field embeddings $\sigma_i : K \hookrightarrow \mathbb{C}$. Recall that for any degree N separable field extension K/F and any field extension L/K that contains a splitting field for K/F, there are precisely N F-algebra embeddings $\sigma_i : K \hookrightarrow L$: indeed, by the Primitive Element Theorem we have $K = F[\alpha]$, and the minimal polynomial $f \in F[T]$ of α is separable of degree N, so $\operatorname{Hom}_F(K, L)$ is in natural bijection with the set of distinct roots of f in L, of which we have N because we assumed that L is a splitting field for K/F.

A number field K is **totally real** if $\mathbb{R}$ contains a splitting field for $K/\mathbb{Q}$: in other words, writing $K = \mathbb{Q}[\alpha]$, the minimal polynomial of α splits into distinct linear factors over $\mathbb{R}$ (or, in the less careful language that is more commonly used, f has only real roots). In the terminology of §4.1, this means that $\mathbb{R}$ is a splitting field for the étale $\mathbb{Q}$-algebra K, so writing out these N embeddings $\sigma_1, \ldots, \sigma_N : K \hookrightarrow \mathbb{R}$ in some order, Proposition 4.6 provides us with a canonical isomorphism of $\mathbb{R}$-algebras

$$\sigma : K_{\mathbb{R}} \to \mathbb{R}^N, \ x \otimes 1 \mapsto (\sigma_1(x), \ldots, \sigma_N(x)).$$

But now we can see a connection with the discriminant: let $\mathbf{x} = (x_1, \ldots, x_N) \in K^N$. As we did, in Chapter 4, we may take the discriminant of this N-tuple:

$$\delta(\mathbf{x}) = \det \operatorname{Tr}_{K/F}(x_i x_j),$$

and by (7) this is equal to $(\det S(\mathbf{x}))^2$, where $S(\mathbf{x})$ is the $N \times N$ matrix with entries in $\overline{\mathbb{Q}}$ with (i,j) entry equal to $\sigma_i(x_j)$. Thus:

Proposition 5.5. *Let K be a totally real number field of degree N, with distinct $\mathbb{Q}$-algebra embeddings $\sigma_1, \ldots, \sigma_N : K \to \mathbb{R}$. Let $x_1, \ldots, x_N \in K$ be $\mathbb{Z}$-linearly independent, and put*

$$\Lambda_{\mathbf{x}} := \langle x_1, \ldots, x_N \rangle_{\mathbb{Z}}.$$

Then:

a) *$\sigma(\Lambda_{\mathbf{x}})$ is a lattice in $\mathbb{R}^N$.*
b) *We have $\delta_{\Lambda_{\mathbf{x}}} \in \mathbb{Z}^+$.*
c) *We have*

$$\operatorname{Covol} \sigma(\Lambda_{\mathbf{x}}) = \sqrt{\delta_{\Lambda_{\mathbf{x}}}}.$$

Proof. To simplify notation, we will not distinguish between $\Lambda_{\mathbf{x}} \subseteq K$ and its isomorphic image $\sigma(\Lambda_{\mathbf{x}}) \subseteq \mathbb{R}^N$.
a),c) The jth column of the matrix $S(\mathbf{x})$ is $(\sigma_1(x_j), \ldots, \sigma_N(x_j)) = \sigma(x_j)$, the jth basis element of $\Lambda_{\mathbf{x}}$. We are about to write down a formula for $(\det S(\mathbf{x}))^2$ that will show that $\det S(\mathbf{x})$ is nonzero, and thus $S(\mathbf{x})$ is nonsingular and $\Lambda_{\mathbf{x}}$ will be a lattice, with $\operatorname{Covol} \Lambda_{\mathbf{x}} = \det S(\mathbf{x})$. Indeed we have

$$\operatorname{disc} \Lambda_{\mathbf{x}} = (\det S(\mathbf{x}))^2 = \left(\operatorname{Covol} \Lambda_{\mathbf{x}}\right)^2. \tag{20}$$

b) Equation (20) shows that $\Lambda_{\mathbf{x}}$ is the square of a real number, so $\Lambda_{\mathbf{x}} \in \mathbb{Z}^+$. □

This is a very striking result: the discriminant of a lattice in a number field has a geometric meaning. We now want to extend this from totally real number fields to arbitrary number fields. To see how to do this, look back at $K_{\mathbb{R}}$. If $K = \mathbb{Q}[\alpha]$ and $f \in \mathbb{Q}[t]$ is the minimal polynomial for α, then

$$K_{\mathbb{R}} \cong \mathbb{Q}[t]/(f) \otimes_{\mathbb{Q}} \mathbb{R} = \mathbb{R}[t]/(f).$$

Now, because $\mathbb{C}$ is algebraically closed, an irreducible polynomial $g \in \mathbb{R}[t]$ must have degree 1 or 2. So we may write

$$f = g_1 \cdots g_r h_1 \cdots h_s \in \mathbb{R}[t]$$

for distinct monic irreducibles $g_1, \ldots, g_r, h_1, \ldots, h_s$ with $\deg g_i = 1$ for all $1 \leq i \leq r$ and $\deg h_j = 2$ for all $1 \leq j \leq s$. The Chinese Remainder Theorem then gives

$$K_{\mathbb{R}} \cong \prod_{i=1}^{r} \mathbb{R}[t]/(h_i) \times \prod_{i=1}^{s} \mathbb{R}[t]/(h_j) \cong \mathbb{R}^r \times \mathbb{C}^s.$$

We now want to give a specific embedding $\sigma : K \hookrightarrow \mathbb{R}^r \times \mathbb{C}^s$. The field $\mathbb{C}$ is algebraically closed so certainly contains a splitting field for $K/\mathbb{R}$, so we have precisely N field embeddings $\sigma_i : K \hookrightarrow \mathbb{C}$. For $1 \leq i \leq N$, we have $\sigma_i(K) \subseteq \mathbb{R}$ if and only if $\sigma_i(\alpha) \in \mathbb{R}$. Because we can identify $\sigma_1(\alpha), \ldots, \sigma_N(\alpha)$ with the roots of f in $\mathbb{C}$, it follows that the number of embeddings σ_i such that $\sigma_i(K) \subseteq \mathbb{R}$ is r, the number of real roots of f. We call these embeddings **real** and the others **complex**. Moreveover, we get an action of $\operatorname{Aut}(\mathbb{C}/\mathbb{R}) = \{1, c\}$ on the set $\operatorname{Hom}_{\mathbb{Q}}(K, \mathbb{C})$: complex conjugation sends σ_i to $\overline{\sigma_i} = c \circ \sigma_i$. Evidently the fixed points under this action are precisely the real embeddings, so the complex embeddings come in complex conjugate pairs, s counts the number of *pairs* and $r + 2s = N$.

It will be helpful to order the embeddings as follows: $\sigma_1, \ldots, \sigma_r : K \hookrightarrow \mathbb{R}$ are the real embeddings (in some order) and then the last $2s$ embeddings are ordered so that $\sigma_{r+2} = \overline{\sigma_{r+1}}$ and so forth: i.e., we put the complex conjugate pairs next to each other in the list. Having done that we define our **additive embedding**

$$\sigma : K \hookrightarrow \mathbb{R}^r \times \mathbb{C}^s, \sigma(x) = (\sigma_1(x), \ldots, \sigma_r(x), \sigma_{r+1}(x), \sigma_{r+3}(x), \ldots, \sigma_{r+2s-1}(x)).$$

Once again, if $\mathbf{x} = (x_1, \ldots, x_N) \in K^N$ is an N-tuple such that $x_1, \ldots, x_N$ are $\mathbb{Z}$-linearly independent, we can consider

$$\Lambda_{\mathbf{x}} \coloneqq \sigma(\langle x_1, \ldots, x_N \rangle_{\mathbb{Z}}) = \langle \sigma(x_1), \ldots, \sigma(x_N) \rangle_{\mathbb{Z}} \subseteq \mathbb{R}^r \times \mathbb{C}^s.$$

We want to show that $\Lambda_{\mathbf{x}}$ is a lattice in $\mathbb{R}^r \times \mathbb{C}^s$ and compute its covolume. As in the case $s = 0$ that we did above, it suffices to do the second thing: getting a finite covolume will tell us that $\Lambda_{\mathbf{x}}$ is a lattice. When $s \geq 1$ we need to think just a little bit about what covolumes mean in $\mathbb{R}^r \times \mathbb{C}^s$. One simple answer is to just identify $\mathbb{C}$ with $\mathbb{R}^2$ via $z \mapsto (\Re(z), \Im(z))$, which tells us how to identify $\mathbb{R}^r \times \mathbb{C}^s$ with $\mathbb{R}^N$. This works, but just to warn you, it results in a *slightly* annoying factor in the formula:

EXAMPLE 5.6. *Suppose $K = \mathbb{Q}(\sqrt{-1})$. Let $\Lambda = \mathbb{Z}_K$ be the lattice in K spanned by 1 and $\sqrt{-1}$. In this case we may take $\sigma_1 : K \hookrightarrow \mathbb{C}$ to be the identity map and σ_2 to be complex conjugation. In this case our additive embedding*

$$\sigma : K \hookrightarrow \mathbb{C}$$

is just the inclusion map. When we identify $\mathbb{C}$ with $\mathbb{R}^2$ as suggested above, we find that $\sigma(\mathbb{Z}_K) = \mathbb{Z} \oplus \mathbb{Z}$ inside $\mathbb{R}^2$. Evidently then the covolume of $\sigma(\mathbb{Z}_K)$ is 1, whereas $\delta_{\mathbb{Z}_K} = -4$. This is slightly odd*: in the totally real case, the discriminant was the square of the covolume, but here the disrimaint is* ***twice*** *the square of the covolume.*

Now we are fully prepared for the general case:

THEOREM 5.7. *Let K be a degree N number field with r real embeddings and s pairs of complex embeddings. Let $x_1, \ldots, x_N \in K$ be $\mathbb{Z}$-linearly independent; put*

$$\Lambda_{\mathbf{x}} \coloneqq \langle x_1, \ldots, x_N \rangle_{\mathbb{Z}}.$$

Then:

a) *$\sigma(\Lambda_{\mathbf{x}})$ is a lattice in $\mathbb{R}^r \times \mathbb{C}^s$.*
b) *Identify $\mathbb{R}^r \times \mathbb{C}^s$ with $\mathbb{R}^{r+2s}$ using $z \mapsto (\Re z, \Im z)$ for each complex component, we have*[2]

$$\operatorname{Covol} \sigma(\Lambda_{\mathbf{x}}) = 2^{-s} |\det S(\mathbf{x})|$$

and thus

$$|\delta_{\Lambda_{\mathbf{x}}}| = 4^s (\operatorname{Covol} \Lambda_{\mathbf{x}})^2. \tag{21}$$

PROOF. Again, we will not distinguish notationally between the $\mathbb{Z}$-lattice $\Lambda_{\mathbf{x}}$ in K and the $\mathbb{Z}$-lattice $\sigma(\Lambda_{\mathbf{x}})$ in $\mathbb{R}^r \times \mathbb{C}^s$.
Let $T(\mathbf{x}) \in M_{N,N}(\mathbb{C})$ be the matrix whose jth column is

$$\sigma(x_j) = (\sigma_1(x_j), \ldots, \sigma_r(x_j), \Re\sigma_{r+1}(x_j), \Im\sigma_{r+1}(x_j), \ldots, \Re\sigma_{r+s}(x_j), \Im\sigma_{r+s}(x_j)).$$

Then $\Lambda_{\mathbf{x}}$ is a lattice if and only if $T(\mathbf{x})$ is nonsingular, and if so its covolume is $|\det T(\mathbf{x})|$. Since by (7) we have $\det S(\mathbf{x})^2 = \delta_{\Lambda_{\mathbf{x}}}$, the crux of the matter is to

[2] In the expression $|\det S(\mathbf{x})|$, $\det S(\mathbf{x})$ is a complex number, and we have taken its absolute value in the usual sense.

compute $\det T(\mathbf{x})$ in terms of $\det S(\mathbf{x})$. These matrices are very closely related: 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

$$\det T(\mathbf{x}) = \left(\frac{i}{2}\right)^s \det S(\mathbf{x}).$$

Because $\det S(\mathbf{x}) \neq 0$, this shows that $\Lambda_{\mathbf{x}}$ is a lattice. Moreover, we have

$$|\delta_{\Lambda_{\mathbf{x}}}| = |\det S(\mathbf{x})^2| = 4^s(\det|T(\mathbf{x})|)^2 = 4^s \operatorname{Covol} \Lambda_{\mathbf{x}}^2. \qquad \square$$

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 5.8. *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 5.11. *Prove Proposition 5.8. (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**

$$M(K) = \left(\frac{4}{\pi}\right)^s \frac{n!}{n^n} |d(K)|^{\frac{1}{2}}.$$

THEOREM 5.9. *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 5.8 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 5.8). Choose t such that

$$2^r \left(\frac{\pi}{2}\right)^s \frac{t^n}{n!} = \operatorname{Vol} B_t = 2^n \operatorname{Covol} \mathfrak{a} = 2^n 2^{-s} \sqrt{|d(K)|} N(\mathfrak{a}),$$

i.e., such that

$$t^n = 2^{n-r}\pi^{-s}n!\sqrt{|d(K)|}N(\mathfrak{a}).$$

By Minkowski's Convex Body Theorem, there is $x \in \mathfrak{a}^\bullet$ such that $\sigma(x) \in B_t$, so

$$|N_{K/\mathbb{Q}}(x)| = \prod_{i=1}^{r}|\sigma_i(x)| \prod_{j=r+1}^{r+s}|\sigma_j(x)|^2 \leq \left(\frac{1}{n}\sum_{i=1}^{r}|\sigma_i(x)| + \frac{2}{n}\sum_{j=r+1}^{r+s}|\sigma_j(x)|\right)^n \leq \frac{t^n}{n^n}$$

$$= \left(\frac{4}{\pi}\right)^s \frac{n!}{n^n}\sqrt{|d(K)|}N(\mathfrak{a}) = M(K)N(\mathfrak{a});$$

the first inequality uses the AGM Inequality and the second the definition of B_t. □

Exercise 5.12. *Show: B_t is a compact, convex body.*

Lemma 5.10. *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 $r\mathfrak{a} \subset \mathbb{Z}_K$ and thus

$$\mathbb{Z}_K \subset \mathfrak{a} \subset \frac{1}{r}\mathbb{Z}_K.$$

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 5.11. *Let K be a number field. Then $\operatorname{Pic}\mathbb{Z}_K$ is finite.*

Proof. By Lemma 5.10 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 3, 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 $\#\operatorname{Pic}\mathbb{Z}_K \leq c$. □

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 $\mathcal{O} \subset \mathbb{Z}_K$ 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 5.13. *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:* $\operatorname{ICM}(\mathcal{O})$ *is finite. Thus also* $\operatorname{Pic}(\mathcal{O})$ *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, $\operatorname{ICM}(\mathcal{O})$ is much less well understood than $\operatorname{Pic}\mathcal{O}$.

3. Discriminant Bounds and Hermite's Theorem

Theorem 5.12. *(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) *In particular $|\delta(K)| > 1$.*

Proof. a) Applying Theorem 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

$$|\delta_K| \geq \left(\frac{\pi}{4}\right)^{2s} \frac{n^{2n}}{(n!)^2} \geq \left(\frac{\pi}{4}\right)^{n} \frac{n^{2n}}{(n!)^2} =: a_n.$$

[3] Unfortunately this does not take place in the current draft! But see [**N**, §1.12].

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 $n \geq 2$,

$$|\delta(K)| \geq \frac{\pi^2}{4}\left(\frac{3\pi}{4}\right)^{n-2} = \frac{\pi}{3}\left(\frac{3\pi}{4}\right)^{n-1}.$$

b) If $n \geq 2$, $|\delta(K)| \geq \frac{\pi}{3}\cdot\frac{3\pi}{4} = \frac{\pi^2}{4} > 1$. □

Remark 5.13. *Actually the proof shows that $|\delta_K| > 2$ for all $n \geq 2$. But this is only interesting if we don't know Stickelberger's Theorem: $\delta_K \equiv 0, 1 \pmod 4$. We* will *prove this later on: Theorem 6.5.*

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 5.14 (Hermite I). *For all $d \in \mathbb{Z}$, there are only finitely many number fields with discriminant d.*

Proof. By Theorem 5.12, 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 $B \subset \mathbb{R}^r \times \mathbb{C}^s$ 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 5.7, 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. [**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 5.14. *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:*

$$\forall x \in K^{\times},\ v_{\mathcal{P}}(x) = ev_{\mathfrak{p}}(x).$$

Lemma 5.15. *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 5.14 we have

$$v_{\mathcal{P}}(e_{\mathcal{P}}) \leq e_{\mathcal{P}}\lfloor \log_p N\rfloor.$$

Using this together with (19), 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 5.16 (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 5.15 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 5.17. *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 4.9a)), 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 5.15. *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 5.18 (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 $B \subset \mathbb{R}^{r+s}$, its preimage

$$B' := L^{-1}(B)$$

is finite. Because B is bounded, there is $\alpha > 1$ such that:

$$\forall x \in B',\ \forall 1 \leq i \leq r + s,\ |\sigma_i(x)| \leq \alpha.$$

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 5.17 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

$$L(\mathbb{Z}_K^\times) \subset W \cong \mathbb{R}^{r+s-1},$$

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 $M := r+s-1$. The map

$$\pi : W \to \mathbb{R}^M,\ (y_1, \ldots, y_{r+s}) \mapsto (y_1, \ldots, y_{r+s-1})$$

is an $\mathbb{R}$-linear isomorphism, so for any $y = (y_1, \ldots, y_{M+1}) \in W$, 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 $\lambda = (\lambda_1, \ldots, \lambda_M)$ 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 $(y_1, \ldots, y_r, z_1, \ldots, z_s)$ 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 5.7 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 $\lambda_{1,h}, \ldots, \lambda_{M,h}$ such that $\sum_{i=1}^{M} c_i \log \lambda_{i,h} = 2\beta h$. Put $\lambda(h) = (\lambda_{1,h}, \ldots, \lambda_{M,h})$ 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 5.16. *Let K be a number field of degree $N \geq 2$. Let $\mu_K := K^{\times}[\mathrm{tors}]$ be the group of roots of unity in K. By Theorem 5.18, we know that μ_K is finite.*

a) *Show: the group μ_K is cyclic.*

b) *Put $m := \#\mu_K$. 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 6

Some Classical Number Theory

1. Brill's Theorem on the Discriminant

Recall the **signum** (or sign) function

$$\mathrm{sgn} : \mathbb{R} \to \mathbb{R}, x \mapsto \begin{cases} 1 & x > 0 \\ 0 & x = 0 \\ -1 & x < 0 \end{cases}.$$

Theorem 6.1. *Let K be a number field of degree N, with s complex conjugate pairs of complex embeddings. Then:*

$$\mathrm{sgn}(\delta_{\mathbb{Z}_K}) = (-1)^s.$$

Proof. Let $\sigma_1, \ldots, \sigma_N : K \hookrightarrow \mathbb{C}$ be the distinct field embeddings of K into $\overline{K}$. As we know, we may embed $\overline{K}$ into $\mathbb{C}$ and thereby view σ_i as a homomorphism into $\mathbb{C}$. Let $x_1, \ldots, x_N$ be a $\mathbb{Z}$-basis for $\mathbb{Z}_K$. As in §4.3, we put $\mathbf{x} = (x_1, \ldots, x_N) \in K^N$ and let $S(\mathbf{x})$ be the matrix with (i, j) entry $\sigma_i(x_j)$. By (7) we have

$$\delta_{\mathbb{Z}_K} = (\det S(\mathbf{x}))^2.$$

Since $\delta_{\mathbb{Z}_K} \in \mathbb{R}^\times$, this means that $\delta_{\mathbb{Z}_K} > 0$ if and only if $\det S(\mathbf{x}) \in \mathbb{R}$. But now consider the effect of complex conjuation on the rows of $S(\mathbf{x})$. The row corresponding to real embeddings are pointwise fixed. The rows corresponding to conjugate pairs of complex embeddings are pairwise interchanged. Since interchanging two rows of a matrix multiplies the determinant by -1, we find that

$$\det \overline{S(\mathbf{x})} = (-1)^s \det S(\mathbf{x}).$$

Thus $\det S(\mathbf{x}) \in \mathbb{R}$ if and only if s is even. □

Corollary 6.2. *Let K be a number field with s complex conjugate pairs of complex embeddings.*

a) *Let Λ be any $\mathbb{Z}$-lattice in K. Then* $\mathrm{sgn}(\delta_\Lambda) = (-1)^s$.
b) *In particular, for any $\mathbb{Z}$-order $\mathcal{O}$ in K, we have* $\mathrm{sgn}(\delta_{\mathcal{O}}) = (-1)^s$.

Exercise 6.1. *Prove Corollary 6.2.*

2. 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 $\mathcal{O} := A[\alpha]$.

Lemma 6.3. *We have*

$$\Delta(1, \alpha, \ldots, \alpha^{n-1}) = \prod_{1 \leq i < j \leq n} (\alpha_i - \alpha_j)^2.$$

Proof. $\square$

The siginificance of this is that if $f \in K[t]$ is the minimal polynomial for α, then $\prod_{1 \leq i < j \leq n} (\alpha_i - \alpha_j)^2 = \Delta(f)$ 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 $\operatorname{Res}(f, f')$ of f and f' (CITE). This makes the computation of the discriminant of a monogenic order $A[\alpha]$ very straightforward (especially for a computer).

Proposition 6.4. *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

$$P \coloneqq \prod_{1 \leq i < j \leq n} (\alpha_i + \alpha_j).$$

Then: P lies in L, is integral over A, and is invariant under $\operatorname{Aut}(L/K)$, 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 $\Delta(f) \equiv P^2 \pmod{4A}$. $\square$

Theorem 6.5 (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 $e \coloneqq e(\mathfrak{p}|(2)) \geq 2$. Then by Theorem 4.50b) we have $v_{\mathfrak{p}}(\Delta_{\mathbb{Z}_K/Z}) \geq e - 1$, with equality if and only if $2 \nmid e$, from which it follows that $v_{\mathfrak{p}}(\Delta_{\mathbb{Z}_K}/\mathbb{Z}) \geq 2$ and thus that δ_K is divisible by $||\mathfrak{p}^2|| = 2^{2f(\mathfrak{p}|2)}$, hence by 4.
Step 2: Suppose $2 \nmid \delta_K$, so we may write $\delta_K = u^2 d$ with d squarefree. If $d = 1$ then δ_K is a square in $\mathbb{Z}/4\mathbb{Z}$, hence $\delta_K \equiv 1 \pmod 4$. It $d \neq 1$, then $\mathbb{Q}(\sqrt{\delta_K}) = \mathbb{Q}(\sqrt{d}) \supsetneq \mathbb{Q}$, and if M is the Galois closure of $K/\mathbb{Q}$, then by Exercise 4.9 shows that $\sqrt{d} \in M$. Since δ_K is odd, 2 is unramified in K, hence also in the Galois closure L (Corollary 4.66), hence also in $\mathbb{Q}(\sqrt{d})$, which implies $d \equiv 1 \pmod 4$ and thus

$$\delta_K = u^2 d \equiv 1 \pmod 4. \qquad \square$$

Exercise 6.2. *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 $\delta_{\mathcal{O}_1} = \delta_{\mathcal{O}_2}$.*

Exercise 6.2 gives a converse to Theorem 6.5 for not necessarily maximal orders. In contrast, understanding which integers are **fundamental discriminants** – i.e., discriminants of the full ring of integers of some number field – is much harder. To the best of my knowledge this remains mostly open.

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-IS] P.L. Clark, *Invariant Subspaces.* alpha.math.uga.edu/~pete/invariant_subspaces.pdf

[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

[Co89] 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.

[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] P.L. Clark, *Field Theory.* http://math.uga.edu/~pete/FieldTheory.pdf

[GSS05] R. Guralnick, M.M. Schacher and J. Sonn, *Irreducible polynomials which are locally reducible everywhere.* Proc. Amer. Math. Soc. 133 (2005), 3171–3177.

[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.

[L] S. Lang, *Algebra.* Revised third edition. Graduate Texts in Mathematics, 211. Springer-Verlag, New York, 2002.

[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 Zahlkr̈per.* J. Sci. Hiroshima Univ. Ser. A. 16 (1953), 425–439.

[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.

[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.

[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.