A SIGNIFICANT PORTION OF THIS TEXT HAS BEEN ADAPTED FROM THE TYPED NOTES OF SEAN SATHER-WAGSTAFF, FROM A COURSE GIVEN BY BENEDICT GROSS IN UTAH IN 1999, WHICH IN TURN USED MANY IDEAS OF TATE'S UNPUBLISHED NOTES.

MARTIN HILLEL WEISSMAN

NUMBER THEORY

TYPESET WITH TUFTE-LATEX

First printing, May 2009

Contents

1
Lattices

This chapter introduces lattices, which can be thought of as integral structures on rational vector spaces. Most importantly, we study lattices in vector spaces endowed with a nondegenerate bilinear form, and introduce the discriminant of such lattices.

The study of lattices prepares us for the study of "rings of integers" in number fields. A more general discussion, including function fields, is left for the exercises.

1.1 Lattices

Definition 1.1 *Let V be a finite-dimensional vector space over $\mathbb{Q}$. A* ***lattice*** *in V is a free abelian subgroup $L \subset V$ such that* $\operatorname{span}_{\mathbb{Q}}(L) = V$.

Note that the vector space V is not yet endowed with a bilinear form. Other authors use the word lattice only when the ambient vector space is endowed with a nondegenerate symmetric or skew-symmetric bilinear form.

Given a vector space V over $\mathbb{Q}$ of finite dimension n and a subgroup L of V, we find that L is torsion-free, since V is torsion-free. For L to be a lattice, it is necessary and sufficient[1] that L be a free abelian group, isomorphic to $\mathbb{Z}^n$. Assume that L is a lattice in V in what follows. Giving an isomorphism $\iota\colon \mathbb{Z}^n \to L$ is equivalent to giving an ordered n-tuple $(v_1, \ldots, v_n)$ of vectors such that:

$$L = \mathbb{Z}v_1 \oplus \mathbb{Z}v_2 \oplus \cdots \oplus \mathbb{Z}v_n.$$

[1] This is an exercise to the reader. See the exercises at the end of the chapter

Such an ordered tuple of vectors $(v_1, \ldots, v_n)$ is called an ordered[2] **basis** of the lattice L.

[2] Many authors neglect the difference between bases and ordered bases. I recommend taking care to distinguish these notions

A basis of the lattice L is also a basis of the vector space V. Indeed, since L spans V, we immediately find that a basis of L spans V. Moreover, if there is a $\mathbb{Q}$-linear relation:

$$\sum_{i=1}^{n} c_i v_i = 0,$$

then after multiplying through by a "common denominator" D, one finds a $\mathbb{Z}$-linear relation:

$$\sum_{i=1}^{n} D c_i v_i = 0.$$

Since $L = \mathbb{Z}v_1 \oplus \cdots \mathbb{Z}v_n$, we find that $Dc_i = 0$ for all $1 \leq i \leq n$.

Fix an isomorphism $\iota\colon \mathbb{Z}^n \to L$, corresponding to an ordered basis $(v_1, \ldots, v_n)$ as above. If $j\colon \mathbb{Z}^n \to L$ is another isomorphism, corresponding to another ordered basis $(w_1, \ldots, w_n)$, then we find that $\iota^{-1} \circ j$ is an automorphism of $\mathbb{Z}^n$, i.e., an element of $GL_n(\mathbb{Z})$. This provides a map:

$$B\colon \{\text{ordered bases of } L\} \to GL_n(\mathbb{Z}),$$

This map is bijective, and depends upon an initial choice of ordered basis, i.e., the chosen initial isomorphism ι. A better way to think about this is the following:

Proposition 1.2 *The set of ordered bases of L is a torsor[3] for $GL_n(\mathbb{Z})$. In other words, $GL_n(\mathbb{Z})$ acts simply transitively on the set of ordered bases of L.*

[3] The word "torsor" seems to inspire fear in students, perhaps because of its common usage in very difficult mathematics. But, given a group G, a **torsor** for G is a G-set X, such that G acts transitively on X and the stabilizer of any element $x \in X$ is trivial. A torsor is also called a **principal homogeneous space**, by many authors. Fixing a "base point" $x \in X$ determines a bijection $g \mapsto gx$ from G to X. But no choice of base point is necessarily preferred in a torsor.

PROOF: Suppose that $(v_1, \ldots, v_n)$ is an ordered basis of L, and let $g = (g_{ij})$ be an element of $GL_n(\mathbb{Z})$. Then a new ordered basis of L is given by $(w_1, \ldots, w_n)$ where

$$w_i = \sum_j g_{ij} v_j.$$

We leave it to the reader to check that this defines a simply-transitive action of $GL_n(\mathbb{Z})$ on the set of ordered bases of L.

□

Similarly, an isomorphism $\iota\colon \mathbb{Q}^n \to V$ corresponds to an ordered basis of V. The set of ordered bases of V (as a vector space over $\mathbb{Q}$) is naturally a torsor for the group $GL_n(\mathbb{Q})$. Perhaps the most familiar elementary consequence is that given an invertible matrix $g \in GL_n(\mathbb{Q})$, the rows (or columns) form a basis of $\mathbb{Q}^n$.

More significant is the action of $GL(V)$ on the set of lattices. Observe that if L is a lattice in V as before, and $g \in GL(V)$, then gL is also a lattice.[4]

[4] Indeed, linear algebra implies that gL is a subgroup of V. Furthermore, the function $v \mapsto gv$ gives a group isomorphism from L to gL. It follows that gL is free of the appropriate rank.

Proposition 1.3 *Let $Lat(V)$ be the set of lattices in V, and fix a lattice $L \subset V$. The action of $GL(V)$ on $Lat(V)$ given above yields a bijection:*

$$Lat(V) \leftrightarrow GL(V)/Aut_{\mathbb{Z}}(L).$$

PROOF: Suppose that $g \in GL(V)$. We find that $gL = L$ if and only if $g \in Aut_{\mathbb{Z}}(L)$, the group of $\mathbb{Z}$-linear automorphisms of L. Indeed, if $gL = L$, then the map $v \mapsto gv$ is a $\mathbb{Z}$-linear automorphism of L. On the other hand, a $\mathbb{Z}$-linear automorphism of L extends uniquely to a $\mathbb{Q}$-linear automorphism of V, by considering a basis of L (which is

also a basis of V), for example. It follows that $GL(V)$ acts on $Lat(V)$, and the stabilizer of L is $Aut_{\mathbb{Z}}(L)$.

It remains to prove that the action of $GL(V)$ on $Lat(V)$ is transitive. If L and M are two lattices in V, then we may choose ordered bases $(v_1, \ldots, v_d)$ of L and $(w_1, \ldots, w_d)$ of M. Furthermore, since these bases are both bases of V, there exists a "change of basis matrix" $g \in GL(V)$ such that $g(v_1, \ldots, v_n) = (w_1, \ldots, w_n)$. It follows that $gL = M$.

□

A special case of the action of $GL(V)$ on $Lat(V)$ is given by **homotheties**. Namely, if $\alpha \in \mathbb{Q}^\times$, and $L \in Lat(V)$, then αL is also a lattice. When two lattices are related by such a scaling, they are called **homothetic**.

Proposition 1.4 *If L and M are lattices in V, then there exists a nonzero integer such that:*

$$\alpha M \subset L.$$

Proof: By the previous proposition, there exists $g \in GL(V)$ such that $g(L) = M$. Express g as a matrix $(g_{ij}) \in GL_n(\mathbb{Q})$, with respect to a basis $(v_1, \ldots, v_n)$ of L. Let α be the (nonzero integer) common denominator of the rational numbers g_{ij}. Then, we find that $\alpha gL = \alpha M$. Moreover, if $v \in L$, then $\alpha gv \in L$, since the entries of the matrix (αg_{ij}) are integers. Hence $\alpha M \subset L$.

□

We finish this section by discussing important facts about *pairs of lattices*. Namely, we often are led to consider a pair $L \subset M$ of lattices in a vector space V over $\mathbb{Q}$. We write $[M : L]$ for the **index** of L in M, both viewed as abelian groups.

Proposition 1.5 *Suppose that M is a lattice in a vector space V over $\mathbb{Q}$ and assume that L is a subgroup of M. Then L is a lattice in V if and only if $[M : L]$ is finite.*

Proof: First, suppose that $[M : L]$ is finite. Then, L, as a subgroup of a free fintely-generated abelian group, is again a finitely-generated abelian group. Since $[M : L]$ is finite, we find that the rank of L equals the rank of M. It follows that $\text{span}_{\mathbb{Q}}(L) = \text{span}_{\mathbb{Q}}(M) = V$. Hence L is a lattice in V.

Conversely, assume that $L \subset M$ is a pair of lattices in V. By Proposition 1.4, there exists a nonzero integer α such that $\alpha M \subset L$. Since homothety preserves inclusions and indices of pairs of lattices, we find that:

$$\alpha L \subset \alpha M \subset L, \text{ and}$$

$$[L : \alpha L] = [L : \alpha M][\alpha M : \alpha L] = [L : \alpha M][M : L].$$

Since $L \cong \mathbb{Z}^n$ as an abelian group, we find that $[L : \alpha L] = |\alpha|^n < \infty$. Since all terms above are cardinal numbers, it follows that[5]

$$[M : L] < [L : \alpha L] < |\alpha|^n < \infty.$$

□

[5] This actually provides a practical way to estimate, though coarsely, the index $[M : L]$. Squeeze L into a multiple αM, and the index $[M : L]$ is bounded by $|\alpha|^d$.

A deeper analysis demonstrates that, given a pair of lattices $L \subset M$, one may choose bases of these lattices which are compatible in a useful way.

Theorem 1.6 *Suppose that $L \subset M$ is a pair of lattices in a vector space V over $\mathbb{Q}$. Then, there exist positive integers $a_1, \ldots, a_n$, and an ordered basis $(w_1, \ldots, w_n)$ of M, such that $(a_1 w_1, \ldots, a_n w_n)$ is an ordered basis of L.*[6]

[6] Closely related to this theorem is the fundamental property of buildings of p-adic groups – that for any two points in such a building, there exists an apartment containing both points.

Proof: This theorem is usually stated as an immediate consequence of the "theory of elementary divisiors". We review the relevant results here. Since $L \subset M$ is a pair of lattices in V, there exist isomorphisms $\lambda : \mathbb{Z}^n \to L$ and $\mu : \mathbb{Z}^n \to M$. Let $\iota : L \hookrightarrow M$ denote the inclusion. There results an injective homomorphism of abelian groups:

$$\phi = \mu^{-1} \circ \iota \circ \lambda : \mathbb{Z}^n \to \mathbb{Z}^n.$$

As an endomorphism of $\mathbb{Z}^n$, we view ϕ as a n by n matrix with integer entries.

There is an algorithm[7] which constructs two matrices $g, h \in GL_n(\mathbb{Z})$ such that $g^{-1}\phi h$ is a diagonal matrix. The diagonal entries of $g^{-1}\phi h$ are nonzero, since ϕ (and hence $g^{-1}\phi h$) is an injective endomorphism of $\mathbb{Z}^n$.

[7] This algorithm brings the matrix ϕ into "Smith normal form". The entries of the resulting diagonal matrix are called the **elementary divisors** of ϕ. They are uniquely determined, up to re-ordering and sign. The algorithm works over any principal ideal domain, after which the elementary divisors are uniquely determined up to re-ordering and scaling by units. Algorithms are implemented in every major software mathematical software package, such as SAGE, Maple, PARI, etc..

Let $a_1, \ldots, a_n$ denote the nonzero diagonal entries of this matrix. Let $(e_1, \ldots, e_n)$ denote the standard basis of $\mathbb{Z}$, so that for all $1 \leq i \leq n$,

$$[g^{-1}\phi h](e_i) = a_i e_i.$$

For all $1 \leq i \leq d$, define $w_i = [\mu g](e_i) \in M$ and $v_i = [\lambda h](e_i) \in L$. Then $(w_1, \ldots, w_n)$ is an ordered basis of M and $(v_1, \ldots, v_n)$ is an ordered basis of L. We now compute:

$$\begin{aligned} \iota(v_i) &= [\mu\phi\lambda^{-1}](v_i) \\ &= [\mu\phi h](e_i) \\ &= [\mu g](a_i e_i) \\ &= a_i w_i. \end{aligned}$$

The basis $(w_1, \ldots, w_n)$ satisfies the desired condition.

□

1.2 Bilinear forms

The study of lattices in a vector space becomes much more interesting when the ambient vector space is endowed with a nondegenerate bilinear form. In this section, we will always consider a lattice L in a finite-dimensional vector space V over $\mathbb{Q}$, endowed with a bilinear form $\langle \cdot, \cdot \rangle$.

Definition 1.7 *A bilinear form $\langle \cdot, \cdot \rangle$ on V is called **symmetric** if $\langle v, w \rangle = \langle w, v \rangle$ for all $v, w \in V$. It is called **skew-symmetric** if $\langle v, w \rangle = -\langle w, v \rangle$ for all $v, w \in V$.*

We will *always* work with symmetric or skew-symmetric bilinear forms.

By working with either symmetric or skew-symmetric forms throughout, we avoid having to constantly distinguish between "left-nondegenerate" and "right-nondegenerate", or "left-dual" and "right-dual", etc..

Definition 1.8 *Suppose that $\langle \cdot, \cdot \rangle$ is a symmetric or skew-symmetric bilinear form on V. We say that this bilinear form is **nondegenerate** if for every linear functional $f \in V^* = \mathrm{Hom}_{\mathbb{Q}}(V, \mathbb{Q})$, there exists a unique $w \in V$ such that $f(v) = \langle w, v \rangle$ for all $v \in V$.*

*A **classical pairing** on V is a nondegenerate, symmetric or skew-symmetric, bilinear form on V.*

We work in this section with lattices L in a vector space V over $\mathbb{Q}$ endowed with a classical pairing.

The notation for "dual lattices" varies greatly from one author to the next. We prefer to use the rare notation $L^\sharp$ to avoid confusion with more common notions of duality. In particular, we believe that the notation L^* should be avoided, since L^* would naturally be a lattice in V^*, while $L^\sharp$ is a lattice in V itself. In addition, $L^\sharp$ should not be confused with the dual $\mathbb{Z}$-module $Hom(L, \mathbb{Z})$.

Definition 1.9 *Given a lattice $L \subset V$, and a classical pairing on V, the **dual lattice** $L^\sharp$ is the subgroup of V given by:*

$$L^\sharp = \{v \in V : \langle v, w \rangle \in \mathbb{Z} \text{ for all } w \in L\}.$$

Proposition 1.10 *With the assumptions of the previous definition, the dual lattice $L^\sharp$ is a lattice in V, and $L^{\sharp\sharp} = L$.*

Proof: Suppose that $(v_1, \ldots, v_n)$ is an ordered basis of L. Let $v_1^\sharp, \ldots, v_n^\sharp$ denote the dual ordered basis of V, in the sense that $\langle v_i^\sharp, v_j \rangle = \delta_{ij}$ (the Kronecker symbol[8]). From the definition of $L^\sharp$, it follows that $v_1^\sharp, \ldots, v_n^\sharp$ are elements of $L^\sharp$.

Conversely, if $w \in L^\sharp$, then there exist *integers* $c_1, \ldots, c_n$ such that $\langle w, v_i \rangle = c_i$ for all $1 \leq i \leq n$. It follows[9] that $w = \sum c_i v_i^\sharp$. It follows now that $L^\sharp$ is the lattice in V given by:

$$L^\sharp = \mathbb{Z}v_1^\sharp \oplus \cdots \oplus \mathbb{Z}v_n^\sharp.$$

Furthermore, the definition of "dual basis" is symmetric or skew-symmetric (depending upon the classical pairing) in that $(\pm v_1, \ldots, \pm v_n)$ is the ordered basis dual to $(v_1^\sharp, \ldots, v_n^\sharp)$. It follows that

$$L^{\sharp\sharp} = \mathbb{Z}v_1 \oplus \cdots \oplus \mathbb{Z}v_n = L.$$

[8] It is defined that $\delta_{ij} = 1$ if $i = j$, and $\delta_{ij} = 0$ otherwise

[9] This utilizes nondegeneracy of the bilinear form. The reader should verify this if it is not clear.

□

Definition 1.11 *Let $(v_1, \ldots, v_n)$ be an ordered basis of L. Let $\lambda_{ij} = \langle v_i, v_j \rangle$. The **discriminant** of L (with respect to this ordered basis) is the determinant of the matrix $\lambda = (\lambda_{ij})$.*

Suppose that $(v_1, \ldots, v_n)$ and $(w_1, \ldots, w_n)$ are two ordered bases of L. Let $\lambda_{ij} = \langle v_i, v_j \rangle$ and $\mu_{ij} = \langle w_i, w_j \rangle$. Then, by Proposition 1.2, there exists $g \in GL_n(\mathbb{Z})$ such that $w_i = \sum_j g_{ij} v_j$. It follows that:

$$\operatorname{Det} \mu = \operatorname{Det}(g \lambda^t g) = \operatorname{Det}(g)^2 \operatorname{Det}(\lambda).$$

But, observe that if $g \in GL_n(\mathbb{Z})$, then $\operatorname{Det}(g) \in \mathbb{Z}^\times = \pm 1$. It follows that $\operatorname{Det}(g)^2 = 1$. Hence we have proven that

Proposition 1.12 *The discriminant of a lattice L (in a vector space V with classical pairing) depends only upon the lattice and not upon the choice of ordered basis of V. Thus, we find an invariant:*

$$\operatorname{Disc}\colon Lat(V) \to \mathbb{Q}.$$

Proposition 1.13 *Suppose that $M = \alpha L$ are homothetic lattices. Then $Disc(M) = \alpha^2 Disc(L)$.*

Proof: If $(v_1, \ldots, v_n)$ is an ordered basis of L, then $(\alpha v_1, \ldots, \alpha v_n)$ is an ordered basis of M. The proposition now follows directly from the definition of the discriminant.

□

By applying a homothety, one can scale a lattice in such a way that its discriminant is an integer; in fact, one arrives at the following useful fact: every lattice L is homothetic to a unique lattice M such that $Disc(M)$ is a square-free integer.

More generally, using elementary divisors, one can prove

Proposition 1.14 *Suppose that $L \subset M$ are lattices. Then* $\operatorname{Disc}(L) = [M : L]^2 \operatorname{Disc}(M)$.

Proof: By Theorem 1.6, there exists an ordered basis $(v_1, \ldots, v_n)$ of M and nonnegative integers $a_1, \ldots, a_n$, such that $(a_1 v_1, \ldots, a_n v_n)$ is an ordered basis of L. Let $\lambda_{ij} = \langle v_i, v_j \rangle$. Let A denote the diagonal matrix with diagonal entries $a_1, \ldots, a_n$. Then we find that

$$\operatorname{Disc}(L) = \operatorname{Det}(A \lambda A) = \operatorname{Det}(A)^2 \operatorname{Det}(\lambda) = \operatorname{Det}(A)^2 \operatorname{Disc}(M).$$

Furthermore, the index of L in M is precisely the product $\prod_i a_i = \operatorname{Det}(A)$. The proposition follows.

□

TWO METHODS are now available to classify and describe a lattice L. First, one may describe a lattice L by describing *properties of its discriminant*. Second, one may describe a lattice L by describing *properties of the bilinear form, evaluated on L*. The following definitions fall within these frameworks.

Definition 1.15 *A lattice L is called **integral** if one of the following equivalent conditions holds:*

1. $L \subset L^\sharp$.
2. $\langle v, w \rangle \in \mathbb{Z}$ *for all* $v, w \in L$.

Proposition 1.16 *Suppose that L is an integral lattice. Then $[L^\sharp : L] = \pm \mathrm{Disc}(L)$. In particular, $\mathrm{Disc}(L) \in \mathbb{Z}$.*

PROOF: Since L is an integral lattice, $L \subset L^\sharp$ and by Theorem 1.6, there exists an ordered basis $(v_1^\sharp, \ldots, v_n^\sharp)$ of $L^\sharp$ and nonnegative integers $a_1, \ldots, a_n$, such that $(a_1 v_1^\sharp, \ldots, a_n v_n^\sharp)$ is an ordered basis of L.

Using this ordered basis, we find that

$$[L^\sharp : L] = \pm \prod_{i=1}^{n} a_i.$$

Since L and $L^\sharp$ are dual lattices, consider the basis $(v_1, \ldots, v_n)$ of L dual to the basis $(v_1^\sharp, \ldots, v_n^\sharp)$ of $L^\sharp$. We now consider the discriminant of L; let $\lambda = (\lambda_{ij})$ where $\lambda_{ij} = \langle v_i, v_j \rangle$. Thus $\mathrm{Disc}(L) = \mathrm{Det}(\lambda)$. Since $(v_1, \ldots, v_n)$ and $(a_1 v_1^\sharp, \ldots, a_n v_n^\sharp)$ are both ordered bases of L, there exists $g \in GL_n(\mathbb{Z})$ such that $a_i v_i^\sharp = \sum_j g_{ij} v_j$. It follows that:

$$\lambda g = \left(\langle v_i, a_j v_j^\sharp \rangle \right).$$

Thus λg is the diagonal matrix with diagonal entries $a_1, \ldots, a_n$. Since $\mathrm{Det}(g) = \pm 1$, we find that:

$$\mathrm{Disc}(L) = \mathrm{Det}(\lambda) = \pm \mathrm{Det}(\lambda g) = \pm \prod_{i=1}^{n} a_i.$$

□

1.3 *Examples and Properties of Lattices*

In this section, we consider lattices L in a fixed vector space V over $\mathbb{Q}$, endowed with a classical pairing $\langle \cdot, \cdot \rangle$.

Definition 1.17 *An* integral *lattice L is called **unimodular** if $L = L^\sharp$, or equivalently (by Proposition 1.16), if $Disc(L) = \pm 1$.*

Example 1.18 *The standard lattice $\mathbb{Z}^n$ in $\mathbb{Q}^n$ is unimodular, when $\mathbb{Q}^n$ is endowed with the usual "dot product":*

$$\langle \vec{x}, \vec{y} \rangle = x_1 y_1 + \cdots + x_n y_n.$$

The discriminant of this lattice is equal to 1.

If L is an integral lattice, then $L \subset L^\sharp$. It follows that the classical pairing on V restricts to a $\mathbb{Q}$-bilinear form on $L^\sharp$, which descends to a bilinear form:

$$\frac{L^\sharp}{L} \times \frac{L^\sharp}{L} \to \frac{\mathbb{Q}}{\mathbb{Z}}.$$

Proposition 1.19 *If L is an integral lattice, then the bilinear form above is a perfect pairing on the finite abelian group $L^\sharp/L$. In other words, it induces an isomorphism:*

$$L^\sharp/L \to \mathrm{Hom}_{\mathbb{Z}}(L^\sharp/L, \mathbb{Q}/\mathbb{Z}).$$

Proof: Since the group $L^\sharp/L$ is finite, it suffices to prove injectivity of the map $L^\sharp/L \to \mathrm{Hom}_{\mathbb{Z}}(L^\sharp/L, \mathbb{Q}/\mathbb{Z})$. An element of the kernel lifts to an element $v \in L^\sharp$ for which $\langle v, w \rangle \in \mathbb{Z}$ for all $w \in L^\sharp$. Such an element v lies in $L^{\sharp\sharp} = L$, by Proposition 1.10. It follows that the aforementioned map is injective.

□

An important consequence of this proposition is that it reduces the hunt for unimodular lattices to a problem about finite abelian groups.

Proposition 1.20 *Suppose that L is an integral lattice, and let A denote the finite abelian group $L^\sharp/L$, endowed with the perfect pairing of the previous proposition. If B is a subgroup of A, define*

$$B^\perp = \{a \in A \text{ such that } \langle b, a \rangle = 0 \text{ for all } b \in B\}.$$

If M is a lattice and $L \subset M \subset L^\sharp$, then M is unimodular if and only if $\bar{M} = \bar{M}^\perp$, where $\bar{M} = M/L \subset A$.

Proof: Suppose that M is a lattice and $L \subset M \subset L^\sharp$. We find that:

$$L = L^{\sharp\sharp} \subset M^\sharp \subset L^\sharp.$$

Hence M and $M^\sharp$ are uniquely determined by their images $\bar{M}$ and $\bar{M}^\sharp$ in $A = L^\sharp/L$. One may directly compute that $\bar{M}^\sharp = \bar{M}^\perp$, from which the proposition follows.

□

Definition 1.21 *An* integral[10] *lattice L is called* ***even*** *if for all $v \in L$, $\langle v, v \rangle \in 2\mathbb{Z}$.*

[10] If the classical pairing on V is symmetric, then the condition $\langle v, v \rangle \in 2\mathbb{Z}$ for all $v \in L$ implies that L is integral.

Example 1.22 *Let $\mathbb{Z}^n$ denote the standard lattice in $\mathbb{Q}^n$, endowed with the "dot product" bilinear form. Consider the sublattice $L \subset \mathbb{Z}^d$, given by*

$$L = \{(x_1, \ldots, x_n) \in \mathbb{Z}^n \text{ such that } \sum_{i=1}^{n} x_i \in 2\mathbb{Z}\}.$$

Then, we find that $[\mathbb{Z}^n : L] = 2$, since L is the kernel of the "sum mod 2" homomorphism from $\mathbb{Z}^n$ to $\mathbb{Z}/2\mathbb{Z}$. It follows that $\mathrm{Disc}(L) = 2^2 \mathrm{Disc}(\mathbb{Z}^n) = 4$. The lattice L is even, since for all $v = (x_1, \ldots, x_n) \in L$, we find that

$$\langle v, v \rangle = \sum_{i=1}^{n} x_i^2 \equiv \sum_{i=1}^{n} x_i \equiv 0 \ (mod\ 2).$$

Observe that $L \subset \mathbb{Z}^n \subset L^\sharp$, and $[L^\sharp : L] = 4$. It follows that $L^\sharp/L$ is a finite abelian group isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, or to $\mathbb{Z}/4\mathbb{Z}$. These cases can be distinguished by considering the element $\eta = 1/2(1, \ldots, 1) \in \mathbb{Q}^d$. Then $\eta \in L^\sharp$ and $\eta \notin \mathbb{Z}^n$. If n is odd, then $2\eta \notin L$. Hence, if n is odd, then $L^\sharp/L$ is not a 2-torsion group. Hence, if n is odd then $L^\sharp/L$ is isomorphic to $\mathbb{Z}/4\mathbb{Z}$. On the other hand, if n is even, and $v = (x_1, \ldots, x_n) \in L^\sharp$, then $2\eta \in L$ and

$$\langle v, 2\eta \rangle = x_1 + \cdots + x_n \in \mathbb{Z}.$$

It follows that $2x_1 + \cdots + 2x_n \in 2\mathbb{Z}$, so that $2v \in L$. Therefore, the group $L^\sharp/L$ is a 2-torsion group. We have found that if n is even then $L/L^\sharp \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

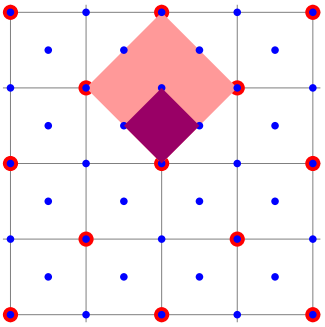

Figure 1.1: The lattice L and its dual $L^\sharp$, satisfying $L \subset \mathbb{Z}^2 \subset L^\sharp$. Elements of L are the red dots. Elements of $L^\sharp$ are blue dots. Observe that $L^\sharp/L$ is isomorphic to $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$.

1.4 Generalizations

Many definitions and results of this chapter, suitably modified, hold when $\mathbb{Z}$ is replaced by a principal ideal domain R, and $\mathbb{Q}$ is replaced by the field K of fractions of R. The definition of a lattice generalizes as follows:

Definition 1.23 *If V is a K-vector space of finite dimension d, then a R-**lattice** in V is an R-submodule L of V, such that L is free of rank d as an R-module and $K \cdot L = V$.*

The following generalizations are straightforward:

- The set of ordered R-bases of an R-lattice L is a torsor for $GL_n(R)$.
- Given an R-lattice L, there is a natural bijection between the set $Lat_R(V)$ of R-lattices in V and the quotient $GL(V)/Aut_R(L)$.
- If L and M are two R-lattices in V, then there exists a nonzero element $\alpha \in R$ such that $\alpha M \subset L$.
- If $L \subset M$ are two R-lattices in V, then there exist nonzero elements $a_1, \ldots, a_n \in R$ and an ordered R-basis $(w_1, \ldots, w_n)$, such that $(a_1 w_1, \ldots, a_n w_n)$ is an ordered R-basis of L.

Given a nondegenerate symmetric or skew-symmetric K-bilinear form on V, the other definitions and results generalize as well. If L is an R-lattice in V, we write

$$L^\sharp = \{v \in V \text{ such that } \langle v, w\rangle \in R \text{ for all } w \in L\}.$$

- If $L \subset M$ are lattices in V, then $M^\sharp \subset L^\sharp$.
- If L is a lattice in V, then $L^{\sharp\sharp} = L$.
- The discriminant $\mathrm{Disc}(L)$ of an R-lattice is well-defined, as an element of $K^\times / R^{\times 2}$, where $R^{\times 2}$ denotes the group of squares of units of R.

Beyond these basic properties, it is difficult and sometimes impossible to generalize results connecting the discriminant to indices of lattices, for example. The primary obstruction is that the elements of K or R no longer have any necessary relation to integers, and one cannot expect them to relate to indices and orders of finite abelian groups.

1.5 *Exercises*

Exercise 1.1 *Suppose that V is a finite-dimensional vector space over $\mathbb{Q}$ with classical pairing. Prove that every lattice L is homothetic to an integral lattice.*

Exercise 1.2 *Suppose that V is a finite-dimensional vector space over $\mathbb{Q}$ with classical pairing. Suppose that L is a lattice in V. Prove that if $\alpha \in \mathbb{Q}^\times$, then $(\alpha L)^\sharp = \alpha^{-1}(L^\sharp)$.*

Exercise 1.3 *Suppose that V and W are finite-dimensional vector spaces over $\mathbb{Q}$ endowed with classical pairings. Let L and M be lattices in V and W, respectively. Then $L \oplus M$ is a lattice in $V \oplus W$. How is the discriminant of $L \oplus M$ related to the discriminant of L and the discriminant of M?*

Exercise 1.4 *Suppose that V is a n-dimensional vector space over $\mathbb{Q}$. Suppose that L is a subgroup of V, and L is isomorphic to $\mathbb{Z}^n$. Prove that $\mathrm{span}(L) = V$. What if $\mathbb{Q}$ is replaced by $\mathbb{R}$? Can you think of a counterexample?*

Exercise 1.5 *Suppose that V is a n-dimensional vector space over $\mathbb{Q}$, and M is a lattice in V. Let p be a prime number.*

(a) Prove that if L is a lattice in V, and $L \subset M$ and $[M : L] = p$, then $p \cdot M \subset L$.

(b) Prove that there are $1 + p + \cdots + p^{n-1}$ *lattices* L *in* V*, such that* $L \subset M$ *and* $[M : L] = p$*. Hint: Find a correspondence between these lattices and hyperplanes (subspaces of codimension* 1*) in the* $\mathbb{F}_p$*-vector space* M/pM*.*

(c) Prove that $Aut_{\mathbb{Z}}(M)$ *acts transitively on the set of lattices of index* p *in* M*.*

Exercise 1.6 *Let* $R = \mathbb{Z}[i]$ *and* $K = \mathbb{Q}(i)$*; recall that* R *is a principal ideal domain. Let* V *be a finite-dimensional* K*-vector space. Fix a nondegenerate Hermitian form*[11] Φ *on* V*.*

(a) Let L *be a* R*-lattice in* V*. Define the discriminant of* L*, relative to an ordered* R*-basis of* L*. In what sense is it independent of the choice of basis?*

(b) Consider the "standard" Hermitian space $V = K^n$*, endowed with the Hermitian form:*

$$\Phi((x_1, \ldots, x_n), (y_1, \ldots, y_n)) = x_1\bar{y}_1 + \cdots + x_n\bar{y}_n.$$

Let $L = R^n \subset K^n$*. What is the discriminant of* L*?*

(c) Given an R*-lattice* L *in* V*, we may also view* L *as a* $\mathbb{Z}$*-lattice in* V *when* V *is viewed as a vector space over* $\mathbb{Q}$*. Consider the* $\mathbb{Q}$*-bilinear form on* V*, given by:*

$$\langle v, w \rangle = 2\Re(\Phi(v, w)).$$

Find a formula relating the discriminant of L *as a* $\mathbb{Z}$*-lattice in* V *(endowed with the bilinear form* $\langle \cdot, \cdot \rangle$*) to the discriminant of* L *as a* R*-lattice in* V *(endowed with the Hermitian form* Φ*).*

[11] Recall that this means that $\Phi\colon V \times V \to K$ is a $\mathbb{Q}$-bilinear form which satisfies the following axioms:

- $\Phi(zv, w) = \Phi(v, \bar{z}w) = z\Phi(v, w)$, for all $v, w \in V$ and all $z \in K$. Here, $\bar{z}$ denotes the complex conjugate of z.
- $\Phi(v, w) = \overline{\Phi(w, v)}$ for all $v, w \in V$. In particular, $\Phi(v, v) \in \mathbb{Q}$ for all $v \in V$.
- The $\mathbb{Q}$-linear map, sending $w \in V$ to the K-linear form $\Phi(\bullet, w) \in Hom_K(V, K)$ is an isomorphism of vector spaces over $\mathbb{Q}$. (It is conjugate-linear, as a map of K vector spaces).

2
Integers and Number Fields

A **number field** is a field F which is a finite extension of $\mathbb{Q}$, i.e., a field of characteristic zero, which is finite-dimensional as a vector space over $\mathbb{Q}$. If $\alpha \in F$, a number field, then the countable infinite set $\{1, \alpha, \alpha^2, \ldots\}$ cannot be linearly independent over $\mathbb{Q}$. A $\mathbb{Q}$-linear relation among these elements is precisely a polynomial with α as a root:

$$P(\alpha) = a_n \alpha^n + \cdots + a_1 \alpha + a_0 = 0,$$

for some $a_0, \ldots, a_n \in \mathbb{Q}$. In this way, every element of F is algebraic over $\mathbb{Q}$. [1]

[1] On the other hand, there exist fields $F/\mathbb{Q}$, in which every element is algebraic, but $[F : \mathbb{Q}] = \infty$. Indeed, any algebraic closure of $\mathbb{Q}$ has infinite dimension, as a $\mathbb{Q}$-vector space.

Given a number field F, we focus in this chapter on the subset $\mathcal{O}_F$ of "integers" in F. Viewing F as a finite-dimensional vector space over $\mathbb{Q}$, we will find that $\mathcal{O}_F$ is not only a ring, but also a lattice in F. Moreover, there is a natural classical pairing on F, from which $\mathcal{O}_F$ can be further studied using the techniques of the previous chapter. In particular, we arrive at invariants such as the "discriminant of F", defined as the discriminant of the lattice $\mathcal{O}_F$.

In this chapter, we assume some basic field theory, but we recall some important definitions along the way.

2.1 *Algebraic and integral elements*

Suppose that F is a field extension[2] of $\mathbb{Q}$. Recall that an element α of F is called **algebraic** (over $\mathbb{Q}$) if there exists a polynomial[3] $P \in \mathbb{Q}[X]$ such that $P \neq 0$ and $P(\alpha) = 0$. But it is convenient to think about algebraicity in a few different ways.

[2] This just means that F is a field which contains $\mathbb{Q}$

[3] If such a polynomial exists, then one may clear divide through by the leading coefficient to make it monic.

Proposition 2.1 *Suppose that F is a field extension of $\mathbb{Q}$ and $\alpha \in F$. The following conditions are equivalent.*

1. *α is algebraic.*
2. *The field[4] $\mathbb{Q}(\alpha)$ is a finite extension of $\mathbb{Q}$.*

[4] This is the smallest subfield of F containing α, i.e., the intersection of all subfields of F containing α

3. *There exists a subfield K of F, such that K is a finite extension of $\mathbb{Q}$, and K contains α.*

Proof:

(1) implies (2) Suppose that α is algebraic, and let I denote the set of polynomials P in $\mathbb{Q}[X]$ such that $P(\alpha) = 0$. Since α is algebraic, $I \neq \{0\}$. Furthermore, I is an ideal in $\mathbb{Q}[X]$, which is a principal ideal domain. Let g_α be a generator of I. Evaluation at α induces a ring homomorphism:

$$Ev_\alpha \colon {}^{\mathbb{Q}[X]}/_{I} \to \mathbb{Q}(\alpha), \text{ given by } P \mapsto P(\alpha).$$

Since $\mathbb{Q}(\alpha)$ is a domain, I is a nonzero prime ideal in $\mathbb{Q}[X]$. Since $\mathbb{Q}[X]$ is a PID, this implies that I is a maximal ideal and so $\mathrm{Im}(Ev_\alpha)$ is a subfield of $\mathbb{Q}(\alpha)$. Since $\mathbb{Q}(\alpha)$ is the smallest subfield of F containing α, and $\mathrm{Im}(Ev_\alpha)$ contains α, we find that $\mathrm{Im}(Ev_\alpha) = \mathbb{Q}(\alpha)$. Hence Ev_α is a field isomorphism.

The dimension of ${}^{\mathbb{Q}[X]}/_{I}$, as a $\mathbb{Q}$-vector space, is equal to the degree of g_α. Thus $\mathbb{Q}(\alpha)$ is a finite extension of $\mathbb{Q}$ of degree $\mathrm{Deg}(g_\alpha)$.

(2) implies (3) The field $\mathbb{Q}(\alpha)$ is a finite extension of $\mathbb{Q}$ containing α, by (2).

(3) implies (1) Suppose that K is a finite extension of $\mathbb{Q}$, and K contains α. Let m_α denote "multiplication by α", viewed as a $\mathbb{Q}$-linear endomorphism of the $\mathbb{Q}$-vector space K. The characteristic polynomial[5] of m_α is the polynomial

$$P_\alpha = X^n - \mathrm{Tr}(m_\alpha)x^{n-1} + \cdots \pm \mathrm{Det}(m_\alpha).$$

By the Cayley-Hamilton theorem, we find that $P_\alpha(m_\alpha) = 0$ in $End_{\mathbb{Q}}(K)$. Since K is a field, the map $\alpha \mapsto m_\alpha$ is an injective homomorphism from K into the $\mathbb{Q}$-algebra $End_{\mathbb{Q}}(K)$. Thus, the identity $P_\alpha(m_\alpha) = 0$ in $End_{\mathbb{Q}}(K)$ implies the identity $P_\alpha(\alpha) = 0$ in K. Since $P_\alpha \neq 0$, it follows that α is algebraic.

[5] The argument given here is a bit overpowered for the modest needs of this proposition. One may instead observe that the infinite set $\{1, \alpha, \alpha^2, \ldots\}$ cannot be linearly independent, in the finite-dimensional vector space K. A $\mathbb{Q}$-linear dependence among these powers of α yields a polynomial with α as a root. However, our stronger argument gives a specific polynomial of interest.

□

The previous proposition allows us to easily prove the algebraicity of numbers, even when we cannot easily write down polynomials for which they are roots.

Corollary 2.2 *Suppose that F is a field extension of $\mathbb{Q}$. Let K denote the set of elements of F which are algebraic over $\mathbb{Q}$. Then K is a subfield of F.*

Proof: It suffices to prove that, given (nonzero) algebraic elements $\alpha, \beta \in F$, the elements $\alpha \pm \beta$, $\alpha\beta$, and α/β are algebraic[6]. Let $\mathbb{Q}(\alpha, \beta)$

[6] Finding explicit polynomials is more difficult. For example, can you find a nonzero polynomial P with rational coefficients, such that $P(\sqrt{2} + \sqrt{3}) = 0$. The previous results imply that such a polynomial P exists; in fact, one can find P of degree 4. But finding such a polynomial, especially in more general circumstances, can be difficult.

denote the smallest[7] subfield of F containing α and β. Foundational results in field theory imply that

$$[\mathbb{Q}(\alpha,\beta):\mathbb{Q}] = [\mathbb{Q}(\alpha,\beta):\mathbb{Q}(\alpha)][\mathbb{Q}(\alpha):\mathbb{Q}], \text{ and}$$

$$[\mathbb{Q}(\alpha,\beta):\mathbb{Q}(\alpha)] \leq [\mathbb{Q}(\beta):\mathbb{Q}].$$

By algebraicity of α and β, we find that $[\mathbb{Q}(\alpha):\mathbb{Q}] < \infty$ and $[\mathbb{Q}(\beta):\mathbb{Q}] < \infty$. Hence

$$[\mathbb{Q}(\alpha,\beta):\mathbb{Q}] \leq [\mathbb{Q}(\alpha):\mathbb{Q}][\mathbb{Q}(\beta):\mathbb{Q}] < \infty.$$

Since $\alpha \pm \beta$, $\alpha\beta$ and α/β are contained in $\mathbb{Q}(\alpha,\beta)$, the third criterion of the previous proposition implies their algebraicity.

[7] The smallest such subfield can be obtained by intersecting all such subfields

□

Definition 2.3 *The **algebraic numbers**, denoted $\bar{\mathbb{Q}}$, are defined to be the set of elements of $\mathbb{C}$, which are algebraic over $\mathbb{Q}$. By the previous result, $\bar{\mathbb{Q}}$ is a subfield of $\mathbb{C}$.*

A very similar line of reasoning can be used to study *algebraic integers* in a field F containing $\mathbb{Q}$. Recall that an element α of F is called **integral** (over $\mathbb{Z}$) if there exists a monic[8] $P \in \mathbb{Z}[X]$ such that $P \neq 0$ and $P(\alpha) = 0$. Observe that *integrality implies algebraicity*: the condition defining integrality is stronger than the condition defining algebraicity.

[8] Unlike working over $\mathbb{Q}$, the monic condition is crucial.

Proposition 2.4 *Suppose that F is a field extension of $\mathbb{Q}$ and $\alpha \in F$. The following conditions are equivalent.*

1. *α is integral over $\mathbb{Z}$.*
2. *The ring[9] $\mathbb{Z}[\alpha]$ is a finite rank $\mathbb{Z}$-module.*
3. *There exists a subring M of F, such that M is finitely-generated as a $\mathbb{Z}$-module and M contains α.*

[9] This is the smallest subring of F containing α, i.e., the intersection of all subrings of F containing α

Proof:

(1) implies (2) Since α is integral over $\mathbb{Z}$, there exists a nontrivial monic polynomial having α as a root:

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

It follows that α^n may be expressed in terms of lower powers of α. Inductively, one may show that all powers of α may be expressed in terms of powers of α between α^0 and α^{n-1}. It follows that every element of $\mathbb{Z}[\alpha]$ can be expressed as an integer linear combination of the elements $\alpha^0, \ldots, \alpha^{n-1}$. Hence $\mathbb{Z}[\alpha]$ is finitely-generated, as a $\mathbb{Z}$-module.

(2) implies (3) Trivial.

(3) implies (1) The same argument as in Propositon 2.1 applies. Namely, multiplication by α is a $\mathbb{Z}$-endomorphism m_α of the finitely-generated $\mathbb{Z}$-module M. Note that since $M \subset F$, and F is a field, M is torsion-free and hence free. Thus m_α is represented by a matrix of integers, with respect to any $\mathbb{Z}$-basis of M. As in Proposition 2.1, α is a root of the characteristic polynomial P_α of m_α:

$$P_\alpha = X^n - \mathrm{Tr}(m_\alpha)X^{n-1} + \cdots \pm \mathrm{Det}(m_\alpha).$$

Indeed, m_α is also the matrix representing multiplication by α in the $\mathbb{Q}$-vector space $\mathbb{Q} \cdot M$ spanned by M. Since the entries of the matrix representing m_α are integers, it follows that every coefficient of P_α is an integer as well. Thus $P_\alpha(\alpha) = 0$, and $0 \neq 0 \in \mathbb{Z}[X]$. Since P_α is monic, we find that α is integral over $\mathbb{Z}$.

□

The previous proposition allows us to easily prove the integrality of numbers, even when we cannot easily write down monic polynomials with integer coefficients, for which they are roots.

Corollary 2.5 *Suppose that F is a field extension of $\mathbb{Q}$. Let A denote the set of elements of F which are integral over $\mathbb{Z}$. Then A is a subring of F.*

Proof: It suffices to prove that, given integral elements $\alpha, \beta \in F$, the elements $\alpha \pm \beta$ and $\alpha\beta$ are integral. Consider the ring $\mathbb{Z}[\alpha, \beta] \subset F$. By the integrality of α, β, there exist positive integers d, e, such that every element of $\mathbb{Z}[\alpha, \beta]$ can be expressed as a polynomial in α and β, whose α-degree is at most d, and whose β-degree is at most e.[10] It follows that $\mathbb{Z}[\alpha, \beta]$ has finite-rank as a $\mathbb{Z}$-module.

By condition (3) of the previous Proposition 2.4, the elements $\alpha \pm \beta, \alpha\beta$ of $\mathbb{Z}[\alpha, \beta]$ are integral over $\mathbb{Z}$.

□

[10] This is a direct generalization of the argument used to prove (1) implies (2) in Proposition 2.4.

Definition 2.6 *The **algebraic integers**, denoted*[11] *$\bar{\mathbb{Z}}$, are defined to be the set of elements of $\mathbb{C}$, which are integral over $\mathbb{Z}$. By the previous result, $\bar{\mathbb{Z}}$ is a subring of $\mathbb{C}$.*

[11] This is not a completely standard notation, but we find it natural.

Definition 2.7 *Suppose that F is an algebraic extension of $\mathbb{Q}$. The ring of **integers** in F, denoted $\mathcal{O}_F$, is the set of elements of F which are integral over $\mathbb{Z}$. Again, $\mathcal{O}_F$ is a subring of F.*

For example, the ring of integers in $\bar{\mathbb{Q}}$ is precisely $\bar{\mathbb{Z}}$. The following lemma describes two basic properties of rings integers.

Lemma 2.8 *Suppose that F is an algebraic extension of $\mathbb{Q}$. Then $\mathcal{O}_F \cap \mathbb{Q} = \mathbb{Z}$ and $F/\mathcal{O}_F$ is a torsion[12] $\mathbb{Z}$-module.*

[12] In other words, for every $z \in F$, there exists a nonzero $N \in \mathbb{Z}$, such that $Nz \in \mathcal{O}_F$.

Proof: First, suppose that $\alpha \in \mathcal{O}_F \cap \mathbb{Q}$. Thus, $\alpha = u/v$ for two relatively prime integers a, b, and moreover α is a root of a monic polynomial with integer coefficients:

$$\frac{u^n}{v^n} + a_{n-1}\frac{u^{n-1}}{v^{n-1}} + \cdots + a_0 = 0.$$

Multiplying through by v^n, one finds that

$$u^n = -\left(a_{n-1}u^{n-1}v + \cdots + a_0 v^n\right).$$

Any prime number dividing v divides the right side, and hence divides the left side, and hence divides u. Since we assume that u and v are relatively prime, and $\alpha = u/v$, we find that α is an integer.

Now, in order to see that $F/\mathcal{O}_F$ is a torsion $\mathbb{Z}$-module, consider an element $z \in F$. Since F is an algebraic extension of $\mathbb{Q}$, there exists a nonzero polynomial with rational coefficients having z as a root; by dividing through by the leading coefficient, one may assume this polynomial is monic:

$$z^n + a_{n-1}z^{n-1} + \cdots + a_0 = 0, \text{ for some } a_0, \ldots, a_{n-1} \in \mathbb{Q}.$$

Choose an integer N, such that $a_{n-i}N^i \in \mathbb{Z}$, for $i = 0, \ldots, n-1$.[13] Then, we find that Nz satisfies the following identity:

[13] For example, one may take N to be the product of the denominators of the $a_0, \ldots, a_{n-1}$. But such a choice is far larger than necessary, in many practical instances.

$$(Nz)^n + a_{n-1}N(Nz)^{n-1} + a_{n-2}N^2(Nz)^{n-2} + \cdots + N^n a_0 = 0.$$

Thus Nz is a root of a monic polynomial with integer coefficients. Hence $Nz \in \mathcal{O}_F$. It follows that $F/\mathcal{O}_F$ is a torsion $\mathbb{Z}$-module.

□

2.2 *The lattice of integers*

Consider a number field F, with ring of integers $\mathcal{O}_F$. By proving that $\mathcal{O}_F$ is a $\mathbb{Z}$-lattice in the finite-dimensional $\mathbb{Q}$-vector space F, we can apply the results of the previous chapter to study the integers in a number field. We begin with a few definitions, and a lemma.

Definition 2.9 *Suppose that F is a number field, and $\alpha \in F$. The **trace** of α, denoted $\mathrm{Tr}(\alpha)$, or $\mathrm{Tr}_{F/\mathbb{Q}}(\alpha)$ if more clarity[14] is required, is the trace of the "multiplication by α" map $m_\alpha \colon F \to F$, viewed as a $\mathbb{Q}$-linear endomorphism of the finite-dimensional $\mathbb{Q}$-vector space F.*

*The **norm** of α, denoted $\mathrm{N}(\alpha)$ or $\mathrm{N}_{F/\mathbb{Q}}(\alpha)$ is the determinant of m_α.*

[14] And often, more clarity is required. It is crucial to remember that the "trace of α" depends on the choice of number field containing α. For example $\mathrm{Tr}_{\mathbb{Q}/\mathbb{Q}}(2) = 2$, but $\mathrm{Tr}_{\mathbb{Q}(i)/\mathbb{Q}}(2) = 4$.

Proposition 2.10 *Suppose that F is a number field. Then,*

1. *The function* $\mathrm{Tr}_{F/\mathbb{Q}}\colon F \to \mathbb{Q}$ *is a* $\mathbb{Q}$*-linear map.*
2. *The function* $\mathrm{N}_{F/\mathbb{Q}}\colon F^\times \to \mathbb{Q}^\times$ *is a group homomorphism.*
3. *The trace yields a symmetric* $\mathbb{Q}$*-bilinear form* $\langle \cdot, \cdot \rangle_{F/\mathbb{Q}}$ *:*

$$\langle \alpha, \beta \rangle = Tr(\alpha\beta).$$

Proof: If $\alpha \in F$, recall that both the trace and norm are determined by the multiplication by α map $m_\alpha \in \mathrm{End}_{\mathbb{Q}}(F)$. The distributive law implies that $m_{\alpha+\beta} = m_\alpha + m_\beta$. The associative law for multiplication implies that $m_{\alpha\beta} = m_\alpha m_\beta$. From this, and the basic properties of Tr and Det from linear algebra, we find that

(1) The function Tr is a $\mathbb{Q}$-linear map, using the following two identities.

$$\begin{aligned} \mathrm{Tr}(\alpha+\beta) &= \mathrm{Tr}(m_{\alpha+\beta}) = \mathrm{Tr}(m_\alpha + m_\beta) \\ &= \mathrm{Tr}(\alpha) + \mathrm{Tr}(\beta), \text{ for all } \alpha, \beta \in F. \end{aligned}$$

$$\begin{aligned} \mathrm{Tr}(q\alpha) &= \mathrm{Tr}(m_{q\alpha}) = \mathrm{Tr}(m_q m_\alpha) = \mathrm{Tr}(q \cdot m_\alpha) \\ &= q\,\mathrm{Tr}(\alpha), \text{ for all } q \in \mathbb{Q}, \alpha \in F. \end{aligned}$$

(2) The norm is a group homomorphism from $F^\times$ to $\mathbb{Q}^\times$, because of the following identity:

$$\begin{aligned} \mathrm{N}(\alpha\beta) &= \mathrm{Det}(m_{\alpha\beta}) = \mathrm{Det}(m_\alpha m_\beta) \\ &= \mathrm{Det}(m_\alpha)\,\mathrm{Det}(m_\beta) = \mathrm{N}(\alpha)\,\mathrm{N}(\beta), \text{ for all } \alpha, \beta \in F. \end{aligned}$$

(3) The trace yields a symmetric[15] $\mathbb{Q}$-bilinear form, by using the following identity, valid for all $q \in \mathbb{Q}$, and all $\alpha, \beta, \gamma \in F$:

$$\begin{aligned} \langle q\alpha+\beta, \gamma \rangle &= \mathrm{Tr}(m_{q\alpha\gamma+\beta\gamma}) = \mathrm{Tr}(q \cdot m_\alpha m_\gamma + m_\beta m_\gamma) \\ &= q\,\mathrm{Tr}(m_\alpha m_\gamma) + \mathrm{Tr}(m_\beta m_\gamma) = q\langle \alpha, \gamma \rangle + \langle \beta, \gamma \rangle. \end{aligned}$$

[15] Symmetry is obvious, by the commutativity of multiplication. Symmetry also implies that only the identity below suffices to prove bilinearity.

□

Lemma 2.11 *Suppose that* F *is a number field, and* $\alpha \in \mathcal{O}_F$ *is an integer in* F*. Then* $\mathrm{Tr}_{F/\mathbb{Q}}(\alpha) \in \mathbb{Z}$ *and* $\mathrm{N}_{F/\mathbb{Q}}(\alpha) \in \mathbb{Z}$*.*

Proof: Consider the field extensions $F \supset \mathbb{Q}(\alpha) \supset \mathbb{Q}$. Let P_α denote the minimal polynomial of α over $\mathbb{Q}$; P_α is a monic polynomial with integer coefficients:

$$P_\alpha(X) = X^d + a_{d-1}X^{d-1} + \cdots + a_0.$$

As we have seen before, $\mathbb{Q}(\alpha)$ is naturally isomorphic to $\mathbb{Q}[X]/\langle P_\alpha \rangle$. Let $d = \mathrm{Deg}(P_\alpha)$, so that a basis of $\mathbb{Q}(\alpha)$ as a $\mathbb{Q}$-vector space is given by $1, \alpha, \ldots, \alpha^{d-1}$.

Let $e = [F : \mathbb{Q}(\alpha)]$, so that $n = [F : \mathbb{Q}] = de$. Let $\beta_1, \ldots, \beta_e$ be a basis for F as a $\mathbb{Q}(\alpha)$-vector space. A basis[16] for F as a $\mathbb{Q}$-vector space is given by

$$\{\alpha^i \beta_j : 1 \leq j \leq e, 0 \leq i \leq d-1\}.$$

[16] In what follows, the basis is ordered "lexicographically".

The "multiplication by α" endomorphism of $\mathbb{Q}(\alpha)$ is represented[17] by the matrix:

$$T = \begin{pmatrix} 0 & 0 & 0 & \cdots & -a_0 \\ 1 & 0 & 0 & \cdots & -a_1 \\ 0 & 1 & 0 & \cdots & -a_2 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & -a_{d-1} \end{pmatrix}.$$

[17] Represented, with respect to the basis $1, \alpha, \alpha^2, \ldots, \alpha^{d-1}$, that is.

Since F can be identified with $\mathbb{Q}(\alpha)^e$, as a $\mathbb{Q}(\alpha)$-module, we find that the "multiplication by α" endomorphism of F is represented by the block-diagonal matrix:

$$m_\alpha = \left(\begin{array}{c|c|c|c} T & 0 & \cdots & 0 \\ \hline 0 & T & \ddots & \vdots \\ \hline \vdots & \ddots & \ddots & 0 \\ \hline 0 & \cdots & 0 & T \end{array}\right).$$

We find the following formula for the trace of α:

$$\mathrm{Tr}_{F/\mathbb{Q}}(\alpha) = -e a_{d-1} = e \,\mathrm{Tr}_{\mathbb{Q}(\alpha)/\mathbb{Q}}(\alpha).$$

In particular, since $a_{d-1} \in \mathbb{Z}$, we find that $\mathrm{Tr}_{F/\mathbb{Q}}(\alpha)$ is an integer.

Similarly, we find a formula for the norm of α:

$$\mathrm{N}_{F/\mathbb{Q}}(\alpha) = \mathrm{Det}(T)^e = (-1)^{de} a_0^e = \mathrm{N}_{\mathbb{Q}(\alpha)/\mathbb{Q}}(\alpha)^e.$$

Since $a_0 \in \mathbb{Z}$, we find that $\mathrm{N}_{F/\mathbb{Q}}(\alpha) \in \mathbb{Z}$ as well.

□

Now we demonstrate a fundamental result:

Theorem 2.12 *Let F be a number field. Then $\mathcal{O}_F$ is a $\mathbb{Z}$-lattice in the $\mathbb{Q}$-vector space F. Endowing F with the trace bilinear form, the lattice $\mathcal{O}_F$ is an integral lattice.*

Proof: We prove this theorem by a squeeze argument; we find a lattice $L \subset F$, such that $L \subset \mathcal{O}_F \subset L^\sharp$. If we can find such a lattice L, then $\mathcal{O}_F$ has finite index[18] in the lattice$L^\sharp$, which implies that $\mathcal{O}_F$ is a lattice itself.

[18] Index bounded above by $|\mathrm{Disc}(L)|$, in fact.

Now, to construct the lattice L, begin by choosing an ordered basis $v_1, \ldots, v_n$ of F as a $\mathbb{Q}$-vector space. By Proposition 2.8, $F/\mathcal{O}_F$ is a torsion $\mathbb{Z}$-module; it follows that there exist nonzero integers

$N_1, \ldots, N_n$ such that $N_1 v_1, \ldots, N_n v_n \in \mathcal{O}_F$. Let $L = N_1 v_1 \mathbb{Z} + \cdots + N_n v_n \mathbb{Z}$.

We find that L is a lattice, since L is a finitely-generated $\mathbb{Z}$-module, and

$$Span_{\mathbb{Q}}(L) = Span_{\mathbb{Q}}(v_1, \ldots, v_n) = F.$$

Hence L is a lattice and $L \subset \mathcal{O}_F$. It remains to show that $\mathcal{O}_F \subset L^\sharp$, where $L^\sharp$ is the dual lattice with respect to the trace bilinear form. So suppose that $\alpha \in \mathcal{O}_F$. Then, for every $\beta \in L \subset \mathcal{O}_F$, we find that $\alpha\beta \in \mathcal{O}_F$ (by Corollary 2.5, $\mathcal{O}_F$ is a subring of F). By the previous Lemma 2.11,

$$\langle \alpha, \beta \rangle = \mathrm{Tr}_{F/\mathbb{Q}}(\alpha\beta) \in \mathbb{Z}.$$

Hence $\alpha \in L^\sharp$.

We have proven that $L \subset \mathcal{O}_F \subset L^\sharp$. Hence $\mathcal{O}_F$ is a lattice. Integrality follows from the previous Lemma 2.11 again; for any $\alpha, \beta \in \mathcal{O}_F$,

$$\langle \alpha, \beta \rangle = \mathrm{Tr}_{F/\mathbb{Q}}(\alpha\beta) \in \mathbb{Z}.$$

□

This result allows us to study a number field F, by applying the machinery of the first chapter to the lattice $\mathcal{O}_F$, in the finite-dimensional $\mathbb{Q}$-vector space F, which is endowed with the trace bilinear form. In particular, the discriminant gives an invariant of F:

Definition 2.13 *Let F be a number field. The **discriminant** of F, often denoted*[19] $\mathrm{Disc}(F)$*, is defined to be the discriminant of the lattice $\mathcal{O}_F$ in the $\mathbb{Q}$-vector space F, with respect to the trace bilinear form. Since the lattice $\mathcal{O}_F$ is integral, $\mathrm{Disc}(F) \in \mathbb{Z}$.*

[19] This is slightly abusive notation. It would be more consistent with the previous chapter to write $\mathrm{Disc}(\mathcal{O}_F)$. But we follow common conventions here, and think about the discriminant as an invariant of a number field.

We will later see that $\mathrm{Disc}(F) = \pm 1$, if and only if $F = \mathbb{Q}$ (in which case, $\mathrm{Disc}(F) = 1$).

Definition 2.14 *Let F be a number field. The **inverse different***[20] *of F, usually denoted $\mathfrak{d}_F^{-1}$, is the lattice $\mathcal{O}_F^\sharp$ dual to $\mathcal{O}_F$, with respect to the trace bilinear form.*

[20] The inverse different arises more naturally than the different itself. We will define the different $\mathfrak{d}_F$ later, as the inverse of the inverse different, once we have the theory of fractional ideals

2.3 *Applications of field theory*

Suppose that F is a number field. Since F is a finite extension of $\mathbb{Q}$, we may apply some results of Galois theory, even though F is not assumed to be a Galois extension of $\mathbb{Q}$. When F is a Galois extension of $\mathbb{Q}$, these results simplify further.

Define $\mathrm{Emb}(F, \mathbb{C})$ to be the set of embeddings of F as a subfield of $\mathbb{C}$, i.e., the set of field homomorphisms from F to $\mathbb{C}$. Since F is algebraic, the image of any such embedding is contained in $\bar{\mathbb{Q}}$, the set of algebraic numbers. Furthermore, if $\eta \in \mathrm{Emb}(F, \mathbb{C})$, then

$\eta(\mathcal{O}_F) \subset \bar{\mathbb{Z}}$; the condition of integrality is preserved under such embeddings.

Recall the primitive element theorem[21] of field theory; we may (and do) choose an element $\phi \in F$, such that $F = \mathbb{Q}(\phi)$. Without loss of generality, we may assume that $\phi \in \mathcal{O}_F$, by multiplying ϕ by a suitable nonzero integer. Let P_ϕ denote the minimal polynomial of ϕ. Thus P_ϕ is a monic irreducible polynomial, with integer coefficients, of degree $n = [F : \mathbb{Q}]$. The following is a basic result of field theory:

[21] If F/K is a finite separable field extension, then there exists an element $\alpha \in F$ such that $F = K(\alpha)$

Proposition 2.15 *The number of embeddings* $\#\mathrm{Emb}(F, \mathbb{C})$ *is equal to the degree* $[F : \mathbb{Q}]$ *of the field extension* F*.*

Proof: Let $r_1, \ldots, r_n$ denote the roots of P_ϕ in $\mathbb{C}$, which are distinct by separability and irreducibility. Note that $n = [F : \mathbb{Q}] = \mathrm{Deg}(P_\phi)$, since every nonconstant polynomial with rational coefficients has a root in $\mathbb{C}$. An embedding of F in $\mathbb{C}$ is uniquely determined by where it sends α. Furthermore, an embedding of F in $\mathbb{C}$ can be given by sending α to any one of the roots $r_1, \ldots, r_n$. Hence there are n such embeddings.

□

Now, we may interpret the trace, norm, and trace pairing, using embeddings of F into $\mathbb{C}$.

Proposition 2.16 *Suppose that* $\alpha \in F$*. Then we have*

1. $\mathrm{Tr}_{F/\mathbb{Q}}(\alpha) = \sum_{\sigma \in \mathrm{Emb}(F,\mathbb{C})} \sigma(\alpha)$.
2. $\mathrm{N}_{F/\mathbb{Q}}(\alpha) = \prod_{\sigma \in \mathrm{Emb}(F,\mathbb{C})} \sigma(\alpha)$.
3. $\langle \alpha, \beta \rangle = \sum_{\sigma \in \mathrm{Emb}(F,\mathbb{C})} \sigma(\alpha)\sigma(\beta)$.

Proof: Let P_α denote the (monic) minimal polynomial of α, and let $e = [F : \mathbb{Q}(\alpha)]$. Let $s_1, \ldots, s_d$ denote the roots of P_α in $\mathbb{C}$. From the proof of Lemma 2.11, we find that:

$$\mathrm{Tr}_{F/\mathbb{Q}}(\alpha) = e\,\mathrm{Tr}_{\mathbb{Q}(\alpha)/\mathbb{Q}}(\alpha), \text{ and } \mathrm{N}_{F/\mathbb{Q}}(\alpha) = \mathrm{N}_{\mathbb{Q}(\alpha)/\mathbb{Q}}(\alpha)^e.$$

Moreover, these quantities are directly related to the polynomial P_α:

$$\mathrm{Tr}_{\mathbb{Q}(\alpha)/\mathbb{Q}}(\alpha) = \sum_{i=1}^{d} s_i, \text{ and } \mathrm{N}_{\mathbb{Q}(\alpha)/\mathbb{Q}}(\alpha) = \prod_{i=1}^{d} s_i.$$

Putting this together, we find that

$$\mathrm{Tr}_{F/\mathbb{Q}}(\alpha) = e \sum_{i=1}^{d} s_i, \text{ and } \mathrm{N}_{F/\mathbb{Q}}(\alpha) = \left(\prod_{i=1}^{d} s_i \right)^e.$$

On the other hand, the elements $s_1, \ldots, s_d$ are precisely the images $\sigma(\alpha)$ as σ ranges over embeddings of $\mathbb{Q}(\alpha)$ into $\mathbb{C}$. As one varies σ

over embeddings of F into $\mathbb{C}$, each embedding of $\mathbb{Q}(\alpha)$ into $\mathbb{C}$ occurs $e = [F : \mathbb{Q}(\alpha)]$ times. It follows that

$$\begin{aligned} \mathrm{Tr}_{F/\mathbb{Q}}(\alpha) &= e\sum_{i=1}^{d} s_i = \sum_{\sigma\in \mathrm{Emb}(F,\mathbb{C})} \sigma(\alpha). \\ \mathrm{N}_{F/\mathbb{Q}}(\alpha) &= \left(\prod_{i=1}^{d} s_i\right)^e = \prod_{\sigma\in \mathrm{Emb}(F,\mathbb{C})} \sigma(\alpha). \end{aligned}$$

The identity for the trace pairing follows directly from identity for the trace above.

□

Using this proposition, we find a new way of computing the discriminant.

Corollary 2.17 *Let F be a number field, and let $(\alpha_1, \ldots, \alpha_n)$ be an ordered $\mathbb{Z}$-basis for the lattice $\mathcal{O}_F$ (or any other lattice L in the $\mathbb{Q}$-vector space F). Let $(\sigma_1, \ldots, \sigma_n)$ be (an ordering on) the set of embeddings of F into $\mathbb{C}$. Let $B = (B_{ij})$ be the matrix with (complex) entries $B_{ij} = \sigma_j(\alpha_i)$. Then,*

$$\mathrm{Disc}(F) = \mathrm{Disc}(\mathcal{O}_F) = \mathrm{Det}(B)^2.$$

PROOF: By the definition of discriminant, we are led to consider the matrix $A = (A_{ij}) = (\langle \alpha_i, \alpha_j \rangle)$, which satisfies

$$\mathrm{Disc}(F) = \mathrm{Disc}(\mathcal{O}_F) = \mathrm{Det}(A).$$

Observe that for all i, j, we have:

$$A_{ij} = \langle \alpha_i \alpha_j \rangle = Tr(\alpha_i \alpha_j) = \sum_{k=1}^{n} \sigma_k(\alpha_i)\sigma_k(\alpha_j).$$

Hence $A_{ij} = \sum_k B_{ik}B_{jk}$. In terms of matrix multiplication, $A = B^t B$. Therefore we find that

$$Disc(F) = \mathrm{Det}(A) = \mathrm{Det}(B^t B) = \mathrm{Det}(B)^2.$$

□

Of course, in practice, number fields often arise as subfields of $\mathbb{C}$ already. If in addition, F is a subfield of $\mathbb{C}$, which is a finite Galois extension of $\mathbb{Q}$, then one may work with automorphisms of $F/\mathbb{Q}$, rather then embeddings of F into $\mathbb{C}$; in this case, it is safe to replace $\mathrm{Emb}(F, \mathbb{C})$ by $\mathrm{Gal}(F/\mathbb{Q})$.

An important result, obtained from this new formulation of the discriminant, is the following

Theorem 2.18 *Suppose that F is a number field. Then* $\mathrm{Disc}(F)$ *is congruent to* 0 *or* 1 *mod* 4.

PROOF: WIth the same notation as in the previous Corollary 2.17, let $B_{ij} = \sigma_j(\alpha_i)$. Since every element $\alpha_i \in \mathcal{O}_F$ is integral over $\mathbb{Z}$, and field embeddings preserve integrality, we find that $B_{ij} \in \bar{\mathbb{Z}} \subset \mathbb{C}$. The determinant of B can be expressed as a familiar sum of products, which we further partition based on signs of permutations[22]. Define, for every $\pi \in S_n$, the following contributor to the determinant:

$$T_\pi = \prod_{j=1}^{n} \sigma_j(\alpha_{\pi(j)}).$$

[22] We write S_n for the symmetric group acting upon $\{1, \ldots, n\}$, and A_n for the alternating group.

Aggregating these terms, define $T_{even} = \sum_{\pi \in A_n} T_\pi$ and $T_{odd} = \sum_{\pi \in S_n - A_n} T_\pi$. Then, we can express the discriminant of F as follows:

$$\text{Disc}(F) = \text{Det}(B)^2 = \left(\sum_{\pi \in S_n} \text{sgn}(\pi) T_\pi \right)^2 = (T_{even} - T_{odd})^2$$

As each term of B_{ij} is an algebraic integer, we find that $T_{even}, T_{odd} \in \bar{\mathbb{Z}}$ as well.

Since for all i, j, B_{ij} is algebraic over $\mathbb{Q}$, there exists a finite Galois extension $K/\mathbb{Q}$, such that $K \subset \mathbb{C}$ and $B_{ij} \in K$ for all i, j. It follows that $T_{even}, T_{odd} \in K$ as well. There exists an action of $Gal(K/\mathbb{Q})$ on $\text{Emb}(F, \mathbb{C})$, given by composition (since the image of every embedding of F into $\mathbb{C}$ lands inside of K). It follows that for all $\gamma \in Gal(K/\mathbb{Q})$, there exists a permutation $\gamma_g \in S_n$ such that for all j,

$$g(B_{ij}) = g(\sigma_j(\alpha_i)) = \sigma_{\gamma_g(j)}(\alpha_i) = B_{i\gamma_g(j)}.$$

Hence, for every $g \in Gal(K/\mathbb{Q})$, and every $\pi \in S_d$, we find that:

$$g(\sigma_j(\alpha_{\pi(j)})) = \sigma_{\gamma_g(j)}(\alpha_{\pi\gamma_g^{-1}\gamma_g(j)}).$$

Therefore, we find that g permutes the terms T_π

$$g(T_\pi) = T_{\pi\gamma_g^{-1}}$$

Depending on whether γ_g is even or odd, one of the following two facts holds (respectively):

1. $gT_{even} = T_{even}$ and $gT_{odd} = T_{odd}$, or
2. $gT_{even} = T_{odd}$ and $gT_{odd} = T_{even}$.

In both cases, $g(T_{even} + T_{odd}) = (T_{even} + T_{odd})$ and $g(T_{even}T_{odd}) = T_{even}T_{odd}$. We have proven that

$$(T_{even} + T_{odd}), T_{even}T_{odd} \in K^{\text{Gal}(K/\mathbb{Q})} = \mathbb{Q}.$$

Since $T_{even}, T_{odd} \in \bar{\mathbb{Z}}$, it follows from Lemma 2.8 that

$$(T_{even} + T_{odd}), T_{even}T_{odd} \in \mathbb{Z}.$$

Finally, we find that

$$\mathrm{Disc}(F) = \mathrm{Det}(B)^2 = (T_{even} - T_{odd})^2 = (T_{even} + T_{odd})^2 - 4T_{even}T_{odd}.$$

Since all squares of integers are congruent to 0 or 1, modulo 4, the theorem follows.

□

2.4 *Quadratic Fields*

A **quadratic field** is a field F, which contains $\mathbb{Q}$, and which satisfies $[F : \mathbb{Q}] = 2$. Basic algebra can be used to see the following:

Proposition 2.19 *If F is a quadratic field, then there exists an element $\alpha \in F$, such that $F = \mathbb{Q}(\alpha)$ and α^2 is a square-free integer.*

By reason of this proposition[23], we write $\mathbb{Q}(\sqrt{D})$ for the field $\mathbb{Q}[X]/\langle X^2 - D\rangle$, and in this circumstance always assume that D is a square-free integer. Every quadratic field is isomorphic to such a field. We write $\sqrt{D}$ for the canonical image of X in $\mathbb{Q}(\sqrt{D})$, the latter viewed as a quotient of the polynomial ring $\mathbb{Q}[X]$.

[23] Perhaps this paragraph seems excessive. The point is that we would rather not fix an embedding of $\mathbb{Q}(\sqrt{D})$ in $\mathbb{C}$, i.e., we would rather not choose a complex square root of D.

In this way, the field $\mathbb{Q}(\sqrt{D})$ has a natural basis as a $\mathbb{Q}$-vector space, given by the elements 1 and $\sqrt{D}$. Note that 1 and $\sqrt{D}$ are both integral over $\mathbb{Z}$. Define $\mathcal{O}_D$ to be the ring of integers of $\mathbb{Q}(\sqrt{D})$; then we find an inclusion of lattices:

$$\mathbb{Z}[\sqrt{D}] = \mathbb{Z} \oplus \mathbb{Z}\sqrt{D} \subset \mathcal{O}_D.$$

The squeeze method, which allowed us to prove that $\mathcal{O}_D$ is a lattice in Theorem 2.12, is effective, allowing us to determine $\mathcal{O}_D$ explicitly.

Proposition 2.20 *Let $\Delta = \mathrm{Disc}(\mathbb{Q}(\sqrt{D}))$. Then, a $\mathbb{Z}$-basis of the lattice $\mathcal{O}_D$ is given by the pair of elements 1 and $(\Delta+\sqrt{\Delta})/2$. There are two cases.*

1. *If D is congruent to 1, mod 4, then $\Delta = D$ and $\mathcal{O}_D = \mathbb{Z} + \mathbb{Z}(1+\sqrt{D})/2$.*
2. *If D is congruent[24] to 2 or 3, mod 4, then $\Delta = 4D$ and $\mathcal{O}_D = \mathbb{Z} + \mathbb{Z}\sqrt{D} = \mathbb{Z}[\sqrt{D}]$.*

[24] Notice, in this case, the discriminant Δ is congruent to zero, mod 4.

Proof: We first consider the chain of lattices

$$\mathbb{Z}[\sqrt{D}] \subset \mathcal{O}_D \subset \mathbb{Z}[\sqrt{D}]^\sharp.$$

The discriminant of $\mathbb{Z}[\sqrt{D}]$ can be computed directly, using the $\mathbb{Z}$-basis $(1, \sqrt{D})$. Indeed, $\mathrm{Tr}(1) = 2$, $\mathrm{Tr}(\sqrt{D}) = 0$, and we find that

$$\mathrm{Disc}(\mathbb{Z}[\sqrt{D}]) = \mathrm{Det}\begin{pmatrix} 2 & 0 \\ 0 & 2D \end{pmatrix} = 4D.$$

Let $N = [\mathcal{O}_D : \mathbb{Z}[\sqrt{D}]]$. Then we find that

$$N^2\Delta = N^2 \operatorname{Disc}(\mathcal{O}_D) = \operatorname{Disc}(\mathbb{Z}[\sqrt{D}]) = 4D.$$

Since D is square-free, we find that $N^2 = 1$ or $N^2 = 4$. Hence we have proven that

$$\Delta = D \text{ or } \Delta = 4D.$$

If D is congruent to 2 or 3, modulo 4, then $\Delta \neq D$ since Δ is congruent to 0 or 1, modulo 4 by Theorem 2.18. On the other hand, if D is congruent to 1, modulo 4, then we find that the element $z = {}^{(1+\sqrt{D})}/_2$ satisfies the monic polynomial identity

$$z^2 - z - \frac{D-1}{4} = 0.$$

Thus $z \in \mathcal{O}_D$. Since $z \notin \mathbb{Z}[\sqrt{D}]$, we find that $N \neq 1$, so $N = 2$ and $\Delta = D$.

We have now reduced our study to two cases.

$N^2 = 1$**:** In this case, $\mathcal{O}_D = \mathbb{Z}[\sqrt{D}]$, $\Delta = 4D$, and D is congruent to 2 or 3, modulo 4. Now, It follows from the fact that $\Delta = 4D$ that

$$\frac{\Delta + \sqrt{\Delta}}{2} = \frac{4D + 2\sqrt{D}}{2} = 2D + \sqrt{D}.$$

Hence we find that

$$\mathbb{Z}[\sqrt{D}] = \mathbb{Z} + \mathbb{Z}\sqrt{D} = \mathbb{Z} + \mathbb{Z}\frac{\Delta + \sqrt{\Delta}}{2}.$$

The conclusion of the proposition is verified in this case.

$N^2 = 4$**:** In this case $\mathcal{O}_D$ contains $\mathbb{Z}[\sqrt{D}]$ as an index two sublattice, $\Delta = D$, and D is congruent to 1, modulo 4. Since we have seen that $\mathcal{O}_D$ contains the element $z = {}^1/_2(1 + \sqrt{D}) \notin \mathbb{Z}[\sqrt{D}]$, and $\mathcal{O}_D$ contains $\mathbb{Z}[\sqrt{D}]$ with index two, it follows that

$$\mathcal{O}_D = \mathbb{Z} + \mathbb{Z}\frac{1 + \sqrt{D}}{2} = \mathbb{Z} + \mathbb{Z}\frac{D + \sqrt{D}}{2}.$$

The conclusion of the proposition is verified in this case.

□

By examining the list of discriminants of quadratic fields, we find

Corollary 2.21 *Suppose that Δ is an integer, and Δ is congruent to 0 or 1, modulo 4. Suppose, moreover, that Δ is square-free, except perhaps for a factor of 4. In other words, suppose that if p is an odd prime number dividing Δ, then p^2 does not divide Δ, and that 16 does not divide Δ. Then, there exists a unique quadratic field of discriminant Δ. The ring of integers in this quadratic field is*

$$\mathcal{O} = \mathbb{Z} + \mathbb{Z}\left(\frac{\Delta + \sqrt{\Delta}}{2}\right).$$

In fact, a stronger result of Stickelberger describes all "quadratic rings" – rings which are isomorphic to $\mathbb{Z}^2$ as a $\mathbb{Z}$-module. Such rings are all presentable as $\mathcal{O}$ is presented here, but all values Δ congruent to 0 or 1, modulo 4 are allowed (without the square-free condition). Most of these quadratic rings arise as "orders" in quadratic fields.

Definition 2.22 *Let F be a number field. An **order** in F is a subring $A \subset F$, such that A is a $\mathbb{Z}$-lattice in the $\mathbb{Q}$-vector space F.*

For example, the ring $\mathbb{Z}[\sqrt{D}]$ is always an order in $\mathbb{Q}(\sqrt{D})$; however it may or may not be the **maximal order**, i.e.[25] , the ring of integers $\mathcal{O}_D \subset \mathbb{Q}(\sqrt{D})$.

[25] It is a fact that the ring of integers in a number field can be alternatively characterized as the (unique) maximal order in a number field.

Consider a quadratic field $\mathbb{Q}(\sqrt{D})$ of discriminant Δ (recall $\Delta = D$ or $4D$, according to whether D is congruent to 1, or to 2 or 3, modulo 4). The following gives a construction of orders in $\mathbb{Q}(\sqrt{D})$:

Proposition 2.23 *Let f be a positive integer. Then, there is a unique order B of index f (equivalently, of discriminant Δf^2) in $\mathcal{O}_D$, and $B = \mathbb{Z} + f \cdot \mathcal{O}_D$.*

Proof: First, it is not difficult to see that $B = \mathbb{Z} + f \cdot \mathcal{O}_D$ is a subring of $\mathcal{O}_D$. Furthermore, since $\mathcal{O}_D$ can be described as a lattice $\mathbb{Z} + \mathbb{Z}\frac{\Delta+\sqrt{\Delta}}{2}$, we find that

$$B = \mathbb{Z} + f\frac{\Delta + \sqrt{\Delta}}{2} \cdot \mathbb{Z}.$$

This is a sublattice of index f in $\mathcal{O}_D$, equivalently of discriminant $f^2\Delta$.

On the other hand, suppose that B' is a order in $\mathbb{Q}(\sqrt{D})$, and B' has index f in $\mathcal{O}_D$. Then we find that

$$f\mathcal{O}_D \subset B' \subset \mathcal{O}_D.$$

Since B' is a ring, $\mathbb{Z} \subset B'$. It follows that $B \subset B' \subset \mathcal{O}_D$. By a squeeze argument – both B and B' have the same index in $\mathcal{O}_D$ – we find that $B = B'$.

□

2.5 *Exercises*

Exercise 2.1 *Consider the cubic field $F = \mathbb{Q}(\sqrt[3]{2})$, by which we mean the field $\mathbb{Q}[X]/\langle X^3 - 2\rangle$, and $\sqrt[3]{2}$ refers to the canonical image of X in F.*

(a) Compute $Tr_{F/\mathbb{Q}}(\sqrt[3]{2})$ in two ways: by directly writing the matrix for multiplication by this element, and by using the three embeddings of F into $\mathbb{C}$.

(b) Compute the discriminant of the lattice $\mathbb{Z}[\sqrt[3]{2}]$. Bound the index of $\mathbb{Z}[\sqrt[3]{2}]$ as a sublattice of $\mathcal{O}_F$.

(c) Challenge: Find (a basis for) $\mathcal{O}_F$.

Exercise 2.2 *Let A be a quadratic ring, i.e., a commutative unital ring which is isomorphic to $\mathbb{Z}^2$ as a $\mathbb{Z}$-module. Let $V = A \otimes_{\mathbb{Z}} \mathbb{Q}$ be the resulting 2-dimensional $\mathbb{Q}$-vector space, in which A sits as a lattice. Define an algebra structure on V, by extension of scalars. The trace and norm can be defined, for elements of V, using the trace and determinant of the "multiplication by α" matrices, for all $\alpha \in V$. This leads to the appropriate definition of the discriminant of A (viewed as a lattice in V).*

(a) Prove that if $\mathrm{Disc}(A) = 0$, then A is isomorphic to $\mathbb{Z}[X]/\langle X^2 \rangle$.

(b) Prove that if $\mathrm{Disc}(A) = 1$, then A is isomorphic to $\mathbb{Z} \times \mathbb{Z}$ (the Cartesian product of the two rings).

(c) Challenge: Prove that if $\mathrm{Disc}(A) \neq 0, 1$, then A is an integral domain.

Exercise 2.3 *Let $F = \mathbb{Q}(\sqrt{D})$ be a quadratic field (so we assume D is square-free). Describe explicitly the inverse different $\mathfrak{d}_D^{-1}$ of F.*

Exercise 2.4 *Let $F = \mathbb{Q}(\zeta)$, where $\zeta = e^{2\pi i/8}$ is a primitive eighth root of unity in $\mathbb{C}$.*

(a) Describe $Gal(F/\mathbb{Q})$, and its subgroups.

(b) Given that $\mathcal{O}_F = \mathbb{Z}[\zeta]$, compute the discriminant of F.

3
The geometry of numbers

In this chapter, we discuss the "geometry of numbers", in which we consider lattices in *real* vector spaces, from which we can apply classical geometric methods. In particular, this method allows us to estimate the discriminant, in terms of volumes of regions in $\mathbb{R}^n$. Later, as this method applies to lattices related to $\mathcal{O}_F$ (the ring of integers in a number field), this method will allow us to study the class number of a number field.

3.1 Lattices, algebra, and measures

Consider, for now, the general situation of a lattice L in a finite-dimensional vector space V over $\mathbb{Q}$. In this circumstance, define $V_{\mathbb{R}} = V \otimes_{\mathbb{Q}} \mathbb{R}$; thus L is isomorphic to $\mathbb{Z}^n$ (as a group) and $V_{\mathbb{R}}$ is isomorphic to $\mathbb{R}^n$ (as a $\mathbb{R}$-vector space). Moreover, L sits naturally[1] as a subgroup of $V_{\mathbb{R}}$, and L spans $V_{\mathbb{R}}$ as a $\mathbb{R}$-vector space[2].

[1] Compose the inclusion of L in V, with the inclusion $v \mapsto v \otimes 1$ of V in $V_{\mathbb{R}}$.

[2] Any $\mathbb{Z}$-basis of L will be a basis of $V_{\mathbb{R}}$ as an $\mathbb{R}$-vector space.

Proposition 3.1 *If L is a lattice in a finite-dimensional $\mathbb{Q}$-vector space V, then L is a discrete subgroup of $V_{\mathbb{R}}$, and the quotient $V_{\mathbb{R}}/L$ is a compact[3] Hausdorff space.*

[3] When $V_{\mathbb{R}}/L$ is compact, it is said that L is **cocompact** in $V_{\mathbb{R}}$.

It is obvious that L is isomorphic to $\mathbb{Z}^n$ and $V_{\mathbb{R}}$ is isomorphic to $\mathbb{R}^n$. However, this does not suffice to imply that L is discrete and cocompact in RR^n.

Proof: Choose a basis $v_1, \ldots, v_n$ of the lattice L in V; this is also a basis of $V_{\mathbb{R}}$ as a $\mathbb{R}$-vector space. Around the point $0 \in L$, consider the open set

$$U_0 = \{v = a_1 v_1 + \cdots + a_n v_n \in V_{\mathbb{R}} \text{ such that } \max\{|a_i|\} < 1/2\}.$$

Then U_0 is an open subset of $V_{\mathbb{R}}$, and $U_0 \cap L = \{0\}$. Translating U_0 by any element v of L yields an open subset $U_v \subset V_{\mathbb{R}}$ such that $U_v \cap L = \{v\}$. It follows that L is a discrete subset of $V_{\mathbb{R}}$.

As L is a closed subgroup of $V_{\mathbb{R}}$, it follows that $V_{\mathbb{R}}/L$ is a Hausdorff topological space. To prove compactness, consider the closure of a fundamental domain[4] $D \subset V_{\mathbb{R}}$ given by:

$$\bar{D} = \{v = a_1 v_1 + \cdots + a_n v_n \in V_{\mathbb{R}} : 0 \leq a_i \leq 1 \text{ for all } 1 \leq i \leq n\}.$$

[4] If G is a group acting upon a set X, then a **fundamental domain** for this action is a subset $D \subset X$, such that:

$$\forall x \in X, \exists! d \in D, \exists g \in G, gx = d.$$

In our context, we consider the action of L by translation on the vector space V. A fundamental domain is given by

$$D = \{a_1 v_1 + \cdots + a_n v_n : 0 \leq a_i < 1\}.$$

Then under the canonical projection from $V_{\mathbb{R}}$ onto $V_{\mathbb{R}}/L$, $\bar{D}$ surjects onto $V_{\mathbb{R}}/L$. Since $\bar{D}$ is compact (homeomorphic to the product of closed intervals), and projection is continuous, it follows that $V_{\mathbb{R}}/L$ is compact.

□

MOST INTERESTINGis when the finite-dimensional $\mathbb{Q}$-vector space arises as a number field. When F is a number field, the vector space $F_{\mathbb{R}} = F \otimes_{\mathbb{Q}} \mathbb{R}$ is endowed with a natural $\mathbb{R}$-algebra structure. To describe this, we define the set of real and complex "places" of F:

Definition 3.2 *A **real place** of a number field F is an embedding $\sigma : F \to \mathbb{R}$. A **complex place** of a number field is a (unordered) pair of embeddings $\{\sigma, \bar{\sigma}\}$ of F into $\mathbb{C}$, such that $\mathrm{Im}(\sigma) \not\subset \mathbb{R}$, and $\bar{\sigma}(x) = \overline{\sigma(x)}$ for all $x \in F$. Typically, one writes r_1 for the number of real places, and r_2 for the number of complex places of a given number field F. An **archimedean place** of a number field is a **place** which is either real or complex.*[5]

[5] Later, we will discuss nonarchimedean places, arising from the p-adic fields.

The first observation about archimedean places is the following:

Proposition 3.3 *Let F be a number field, with $[F : \mathbb{Q}] = n$. Let r_1 be the number of real places, and r_2 be the number of complex places of F. Then $n = r_1 + 2r_2$.*

PROOF: The number of embeddings of F into $\mathbb{C}$ equals n. Each such embedding has image contained in $\mathbb{R}$, and hence corresponds to a real place of F, or else has image not contained in $\mathbb{R}$. As those embeddings whose image is not contained in $\mathbb{R}$ come in conjugate pairs, each pair corresponding to a complex place, it follows that $n = r_1 + 2r_2$.

□

The structure of the $\mathbb{R}$-algebra $F_{\mathbb{R}}$ is related to the archimedean places as follows:

Proposition 3.4 *There is a isomorphism of $\mathbb{R}$-algebras $F_{\mathbb{R}} \cong \mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$, where r_1 denotes the number of real places of F, and r_2 denotes the number of complex places of F.*

PROOF: By the theorem of the primitive element, there exists $\alpha \in F$ such that $F = \mathbb{Q}(\alpha)$. Let P denote the minimal polynomial of α, i.e. the irreducible monic polynomial, with rational coefficients, of minimal degree having α as a root. There is a field isomorphism from F to $\mathbb{Q}[X]/\langle P \rangle$, which extends naturally to an algebra isomorphism from $F_{\mathbb{R}}$ to $\mathbb{R}[X]/\langle P \rangle$. On the other hand, the polynomial P factors over $\mathbb{R}$ into linear and quadratic terms. Each linear term $(X - x_i)$

corresponds to a real place of F, sending α to x_1. Each quadratic term $(X^2 - t_j X + n_j)$ corresponds to a complex place of F, sending α to the either of conjugate roots $z_j, \bar{z}_j$ of this quadratic polynomial. In this way, we find a factorization of P in $\mathbb{R}[X]$:

$$P = \prod_{i=1}^{r_1}(X - x_i) \cdot \prod_{j=1}^{r_2}(X^2 - t_j X + n_j).$$

By the Chinese remainder theorem (applied to the principal ideal domain $\mathbb{R}[X]$, we find an isomorphism of $\mathbb{R}$-algebras

$$F_{\mathbb{R}} \cong \frac{\mathbb{R}[X]}{\langle P \rangle} \cong \prod_{i=1}^{r_1} \frac{\mathbb{R}[X]}{\langle X - x_i \rangle} \times \prod_{j=1}^{r_2} \frac{\mathbb{R}[X]}{\langle X^2 - t_j X + n_j \rangle}.$$

It follows immediately that $F_{\mathbb{R}}$ is isomorphic, as an $\mathbb{R}$-algebra, to $\mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$.

□

One subtle issue with the previous proposition is that there is not a *unique* (or natural) isomorphism from $F_{\mathbb{R}}$ to $\mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$; indeed, the construction of such an isomorphism relied on an initial choice of "primitive element", for which there are an infinitude of choices. Nor is it true that the resulting isomorphism is independent of choices. Instead, we must be content to prove that there are "not too many" such isomorphisms.

Proposition 3.5 *Suppose that F is a number field, and ι_1, ι_2 are $\mathbb{R}$-algebra isomorphisms from $F_{\mathbb{R}}$ to $\mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$. Let $c \in Gal(\mathbb{C}/\mathbb{R})$ denote complex conjugation. Then, there exist permutations $\sigma \in S_{r_1}$ and $\tau \in S_{r_2}$, and a "conjugation datum" $e_1, \ldots, e_{r_2} \in \{0,1\}^{r_2}$, such that for all $x \in F_{\mathbb{R}}$,*

$$\begin{aligned} \iota_1(x) &= (x_1, \ldots, x_{r_1}, z_1, \ldots, z_{r_2}) \text{ if and only if} \\ \iota_2(x) &= (x_{\sigma(1)}, \ldots, x_{\sigma(r_2)}, c^{e_1} z_{\tau(1)}, \ldots, c^{e_{r_2}} z_{\tau(r_2)}). \end{aligned}$$

In other words, there is a unique isomorphism from $F_{\mathbb{R}}$ to $\mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$, up to reordering and complex conjugation.

Proof: Let $A = \mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$, to abbreviate. If ι_1, ι_2 are $\mathbb{R}$-algebra isomorphisms from $F_{\mathbb{R}}$ to A, then $\iota = \iota_2 \circ \iota_1^{-1}$ is an $\mathbb{R}$-algebra automorphism of A. Thus, it suffices to prove that every such automorphism arises from reordering and complex conjugations.

Recall that an **idempotent** in a commutative ring is an element e such that $e^2 = e$. The set of idempotents form a partially ordered set, by defining $e \leq f$ if $ef = e$ for all idempotents e, f. A **minimal idempotent** is a minimal nonzero idempotent, for this partial order.

The idempotents in the ring A are precisely those expressions $(x_1, \ldots, x_{r_1}, z_1, \ldots, z_{r_2})$ such that for all i, j, $x_i \in \{0,1\}$ and $z_j \in$

$\{0,1\}$. Among these $2^{r_1+r_2}$ idempotents, there are $r_1 + r_2$ minimal idempotents in the ring A, given by

$$(1,0,\ldots,0),\ldots,(0,\ldots,0,1).$$

We call a minimal idempotent $e \in A$ real or complex, depending on whether eA is isomorphic to $\mathbb{R}$ or to $\mathbb{C}$, respectively.

As the property of "being a minimal idempotent" is certainly preserved by ring automorphisms, we find that for any minimal idempotent $e \in A$, there exists a minimal idempotent $f \in A$ such that $\iota(e) = f$. We find that ι induces a ring isomorphism[6] from eA to fA. For our ring A, and a minimal idempotent e, we find that eA is isomorphic to $\mathbb{R}$ or to $\mathbb{C}$. as ι induces a ring isomorphism from eA to fA, we find that ι permutes the real idempotents with real idempotents, and complex idempotents to complex idempotents.

[6] When e is an idempotent in a ring A, the set eA forms a commutative unital ring, with e as its unit element.

Let σ and τ denote the resulting permutations. Since the only $\mathbb{R}$-algebra isomorphism from $\mathbb{R}$ to $\mathbb{R}$ is the identity, and the only $\mathbb{R}$-algebra isomorphisms from $\mathbb{C}$ to $\mathbb{C}$ are the identity and complex conjugation, the proposition follows immediately.

□

When F is a number field, the real vector space $F_{\mathbb{R}}$ is endowed with an $\mathbb{R}$-algebra structure. From the previous proposition, this algebra structure is quite "rigid" – there are few automorphisms, all arising from reorderings and complex conjugations. It follows that $F_{\mathbb{R}}$ is endowed with a canonical **lax basis**, i.e., a basis as a $\mathbb{R}$-vector space, unordered, and only defined up to sign. Namely, if r_1 and r_2 denote the number of real and complex places, and $F_{\mathbb{R}} \cong \mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$ is a fixed isomorphism, then we may consider the real idempotents $e_1,\ldots,e_{r_1}$ and complex idempotents $f_1,\ldots,f_{r_2}$. A basis for $F_{\mathbb{R}}$ as a real vector space is given by the set:

$$\{e_1,\ldots,e_{r_1},f_1,\ldots,f_{r_2},f_1\sqrt{-1},\ldots,f_{r_2}\sqrt{-1}\}.$$

Changing the algebra isomorphism $F_{\mathbb{R}} \cong \mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$ will only reorder these basis elements, and perhaps change some of the signs (changing one square root of -1 to the other in $\mathbb{C}$).

From these observations, the real vector space $F_{\mathbb{R}} \cong \mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$ is also endowed with a natural measure, given by the absolute value of a top-degree differential form dV:

$$dV = dx_1 \wedge \cdots \wedge dx_{r_1} \wedge du_1 \wedge dv_1 \wedge \cdots \wedge du_{r_2} \wedge dv_{r_2}.$$

Here, $z_i = u_i + v_i\sqrt{-1}$, for each coordinate z_i on $\mathbb{C}^{r_2}$ Observe that, upon reordering the coordinates $x_1,\ldots,x_{r_1}$, and the coordinates

$z_1, \ldots, z_{r_2}$, and upon conjugating various complex coordinates, volume form dV only changes in sign, and the measure $|dV|$ does not change.

It now follows that, given only the data of a number field F over $\mathbb{Q}$, one arrives at a lattice $\mathcal{O}_F$ in the $\mathbb{Q}$-vector space F (which in turn is endowed with the trace pairing), as well as a discrete cocompact subgroup $\mathcal{O}_F$ in the $\mathbb{R}$-vector space $F_{\mathbb{R}}$ (which in turn is endowed with a canonical measure). The previous chapter applied the theory of $\mathbb{Z}$-lattices in $\mathbb{Q}$-vector spaces with classical pairings to the special case $\mathcal{O}_F$ in F. This chapter applies the theory of discrete cocompact subgroups of $\mathbb{R}$-vector spaces with measures to the special case $\mathcal{O}_F$ in $F_{\mathbb{R}}$.

Example 3.6 *Consider first the fields $G = \mathbb{Q}(\sqrt{-1})$ and $E = \mathbb{Q}(\sqrt{-3})$. Let i denote a complex square root of -1, and let $\omega = e^{2\pi i/3}$ denote a complex cube root of 1. Then $\mathcal{O}_G = \mathbb{Z}[i]$ and $\mathcal{O}[E] = \mathbb{Z}[\omega]$ by the results of the previous chapter*[7]*. Both of these fields are **totally complex**, meaning that all archimedean places are complex. We have $G_{\mathbb{C}} \cong \mathbb{C} \cong E_{\mathbb{C}}$. The resulting measure on $\mathbb{C}$ is the usual measure. In this way, we find the **covolume** (i.e., the volume of the quotient) to be:*

$$\mathrm{Vol}(\mathbb{C}/\mathcal{O}_G) = 1, \text{ and } \mathrm{Vol}(\mathbb{C}/\mathcal{O}_E) = \frac{\sqrt{3}}{2}.$$

[7] Note that $\omega = 1/2(-1 + \sqrt{-3})$.

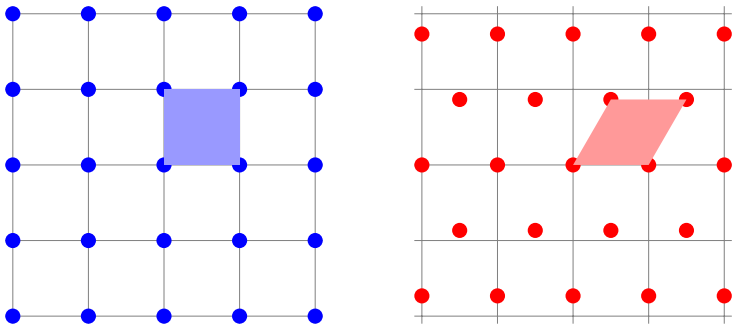

Figure 3.1: The lattice $\mathcal{O}_G = \mathbb{Z}[i]$, represented by blue dots in $\mathbb{C} \cong G_{\mathbb{R}}$. The lattice $\mathcal{O}_E = \mathbb{Z}[\omega]$, represented by red dots in $\mathbb{C} \cong E_{\mathbb{R}}$

Example 3.7 *Consider the field $F = \mathbb{Q}(\sqrt{5})$, with ring of integers $\mathcal{O}_F = \mathbb{Z}[\gamma]$, where $\gamma = 1/2(1 + \sqrt{5})$. This field is **totally real**, meaning that all archimedean places are real. We have $F_{\mathbb{R}} \cong \mathbb{R}^2$. One embeds F (and $\mathcal{O}_F$) in $\mathbb{R}^2$ by sending an element $a + b\sqrt{5} \in \mathbb{Q}(\sqrt{5})$ to the pair of real numbers $(a + b\sqrt{5}, a - b\sqrt{5})$ (for $\sqrt{5}$ a fixed square root of 5 in $\mathbb{R}$).*

In this way, the $\mathbb{Z}$-basis $\{1, \gamma\}$ of the lattice $\mathcal{O}_F$ becomes identified with the vectors $(1, 1)$ and $1/2(1 + \sqrt{5}, 1 - \sqrt{5})$ in the real vector space $\mathbb{R}^2$.

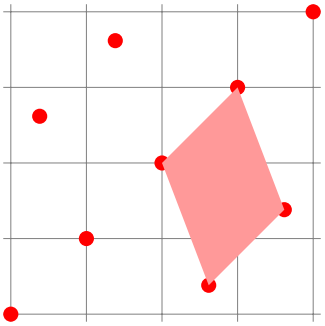

Figure 3.2: The lattice $\mathcal{O}_F = \mathbb{Z}[\gamma]$, represented by red dots in $\mathbb{R}^2 \cong F_{\mathbb{R}}$.

3.2 *Geometry and applications*

Consider here a number field F, with r_1, r_2 the numbers of real and complex places as before. Fix an identification $F_{\mathbb{R}} \cong \mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$, although the results of this section will be independent on this choice. Also, fix a lattice L in the $\mathbb{Q}$-vector space F; for example, L might be $\mathcal{O}_F$, but other lattices will be important as well. Then L is discrete and cocompact in $F_{\mathbb{R}}$.

Consider a $\mathbb{Z}$-basis $(v_1, \ldots, v_n)$ of the lattice L. This is also a basis of F, as a $\mathbb{Q}$-vector space, and of $F_{\mathbb{R}}$, as a $\mathbb{R}$-vector space. This basis also yields a fundamental domain D for the action of L on $F_{\mathbb{R}}$ by translation:

$$D = \{a_1 v_1 + \cdots + a_n v_n : 0 \leq a_i < 1 \text{ for all } i\}.$$

Its closure $\bar{D}$ is a closed **parallelotope**, i.e., the image of a closed n-cube under a linear invertible map.

Since the measure dV on $F_{\mathbb{R}}$ is translation invariant, it descends to a measure on the compact Hausdorff space $F_{\mathbb{R}}/L$. Explicitly, if $\pi : F_{\mathbb{R}} \to F_{\mathbb{R}}/L$ is the projection map, and X is a locally closed subset of $F_{\mathbb{R}}/L$, the measure of a subset X is given by

$$Vol(X) = Vol(\pi^{-1}(X) \cap \bar{D}).$$

In particular, $Vol(F_{\mathbb{R}}/L) = Vol(\bar{D})$ is the measure of the parallelotope $\bar{D}$. This can be related to the discriminant of L by the following

Proposition 3.8 *The discriminant $Disc(L)$ is equal to $(-4)^{r_2} \cdot Vol(\bar{D})^2$.*

Proof: Consider the set of embeddings $\mathrm{Emb}(F, \mathbb{C})$, partitioned into the subset $\{\sigma_1, \ldots, \sigma_{r_1}\}$ of embeddings into $\mathbb{R}$, and the subset $\{\tau_1, \bar{\tau}_1, \ldots, \tau_{r_2}, \bar{\tau}_{r_2}\}$ of embeddings into $\mathbb{C}$, whose image is not contained in $\mathbb{R}$, and which come in conjugate pairs.

Recall that $(v_1, \ldots, v_n)$ is a basis of L, and $n = r_1 + 2r_2$. We have seen previously, in Proposition 2.17 that the discriminant of L can be computed using the embeddings of F into $\mathbb{C}$:

$$\mathrm{Disc}(L) = \mathrm{Det}(B^t B) = \mathrm{Det}(B)^2,$$

where B_{ij} is the matrix whose i^{th} row has the form

$$(\sigma_1(v_i), \ldots, \sigma_{r_1}(v_i), \tau_1(v_i), \bar{\tau}_1(v_i), \ldots, \tau_{r_2}(v_i), \bar{\tau}_{r_2}(v_i)).$$

On the other hand, the (signed) volume of the parallelotope corresponding to the basis $v_1, \ldots, v_n \in F_{\mathbb{R}}$ can be computed as $\mathrm{Det}(C)$, where the i^{th} row of C_{ij} has the form

$$(\sigma_1(v_i), \ldots, \sigma_{r_1}(v_i), \Re(\tau_1(v_i)), \Im(\tau_1(v_i)), \ldots, \Re(\tau_{r_2}(v_i)), \Im(\tau_{r_2}(v_i))).$$

Thus, it remains to relate the matrices B and C.

Let $\phi\colon \mathbb{C}^2 \to \mathbb{C}^2$ be the map defined by:

$$\phi(z, w) = \frac{1}{2}(z + w, i(z - w)).$$

In particular, when $w = \bar{z}$, we find that

$$\phi(z, \bar{z}) = (\Re(z), \Im(z)).$$

Let $\Phi = \begin{pmatrix} 1/2 & -i/2 \\ 1/2 & i/2 \end{pmatrix}$ denote the corresponding invertible matrix. Let Φ_F denote the n by n matrix, given in blocks down the diagonal: the first r_1 blocks are 1×1 blocks with 1 in each entry; the last r_2 blocks are 2×2 blocks with Φ in each block. Then we find that $B \cdot \Phi_F = C$, and so

$$\mathrm{Det}(B)\,\mathrm{Det}(\Phi_F) = \mathrm{Det}(C).$$

On the other hand, we can compute $\mathrm{Det}(\Phi_F)$:

$$\mathrm{Det}(\Phi_F) = \mathrm{Det}(\Phi)^{r_2} = (i/2)^{r_2}.$$

It follows that

$$\mathrm{Det}(B) = (2i)^{r_2}\,\mathrm{Det}(C) = (-2i)^{r_2} \cdot Vol(D).$$

Since $\mathrm{Disc}(L) = \mathrm{Det}(B)^2$, we get

$$\mathrm{Disc}(L) = \mathrm{Det}(B)^2 = (-4)^{r_2} Vol(D)^2.$$

□

For example, consider the lattice L spanned by 1 and i in $F = \mathbb{Q}(i)$. The discriminant can be computed via embeddings

$$\mathrm{Disc}(L) = \mathrm{Det}\begin{pmatrix} 1 & 1 \\ i & -i \end{pmatrix}^2 = (-2i)^2 = -4.$$

In particular, the sign of the discriminant is uniquely determined by the number of complex places:

Corollary 3.9 *If L is a $\mathbb{Z}$-lattice in a number field F, then* $\mathrm{Disc}(L) = (-1)^{r_2}$, *where r_2 is the number of complex places of F.*

Our next geometric result is crucial for estimates involving discriminants and class numbers. We begin with

Definition 3.10 *Let P be a subset of a real vector space V. Then P is called* ***convex*** *if for all $p, q \in P$, and all $t \in [0,1]$ (the closed unit interval in $\mathbb{R}$), the point $tp + (1-t)q$ is also in P. In other words P is convex if for any two points of P, the line segment joining p and q is also fully contained in P.*

P is called ***centrally symmetric*** *if for all $p \in P$, $-p$ is also a point of P.*

Theorem 3.11 *Suppose that $L \cong \mathbb{Z}^n$ is embedded as a discrete cocompact subgroup of a real vector space V , endowed with a "usual measure" (arising from an identification with Euclidean space). Let P be a compact, convex, centrally symmetric subset of V, and suppose that $Vol(P) \geq 2^n Vol(V/L)$. Then P contains a nonzero*[8] *point of L.*

[8] If P is a subset of V, and P is centrally symmetric, convex, and nonempty, then $0 \in P$.

Proof: Suppose first that $Vol(P) > 2^n Vol(D)$ (a strict inequality, unlike the nonstrict inequality given in the theorem). Let $H = {}^1/_2 P$, so that $Vol(H) = 2^{-n} Vol(P) > Vol(\mathbb{R}^n/L)$. Consider the projection $\pi\colon V \to V/L$. For every non-negative integer k, define measurable subsets of V/L by:

$$M_k = \{\bar{v} \in C/L \text{ such that } \pi^{-1}(\bar{v}) \cap H \text{ has cardinality } k\}.$$

The compactness (the boundedness, in fact) of H implies that

$$V/L = \bigsqcup_{k=0}^{\infty} M_k.$$

Namely, the cardinality of $\pi^{-1}(\bar{v}) \cap H$ is always finite, since otherwise we would find an infinite discrete subset of H. We can use this partition to compute the volume of H in a new way[9]:

$$Vol(H) = \sum_{k=0}^{\infty} k \cdot Vol(M_k).$$

[9] Essentially, we are partitioning H into subsets H_k ($0 \leq k < \infty$), in such a way that the projection map from H_k to M_k is a k to 1 map. Since the volume form on H_k is precisely the pullback of the volume form on M_k, we have $Vol(H_k) = k \cdot Vol(M_k)$

In particular, since $0 \cdot Vol(M_0) = 0$, and $1 \cdot Vol(M_1) = Vol(M_1) \leq Vol(\mathbb{R}^n/L)$, and $Vol(H) > Vol(V/L)$, we find that there exists $k \geq 2$ such that $M_k \neq \emptyset$.

Hence, there exists $\bar{v} \in \pi(H)$ such that $\pi^{-1}(\bar{v}) \cap H$ has cardinality at least two. In other words, there exist points $p, q \in H$, such that $\pi(p) = \pi(q)$. In other words, there exist $p, q \in H$, and a nonzero $v \in L$, such that $p - q = v$.

Since H is centrally symmetric, we find that p and $-q$ are elements of H, and so $2p$ and $-2q$ are elements of P. It follows from convexity of P that

$$v = p - q = \frac{1}{2}(2p + (-2q)) \in (L \cap P) - \{0\}.$$

Hence P contains a nonzero point of the lattice L.

Now, we prove the theorem, in case of the nonstrict inequality. Thus, we suppose that $Vol(P) \geq 2^n Vol(D)$. Consider the family

$P_t = t \cdot P$, for $0 < t \in \mathbb{R}$. For $t > 1$, we find that $P_t \cap L$ contains a nonzero lattice point, since $Vol(P_t) > Vol(P) \geq 2^n Vol(D)$ in this case.

Thus, we find a sequence of nonzero lattice points $v_1, v_2, \ldots$, such that $v_i \in P_{1+1/i}$ for all $i \geq 1$. By the compactness of P_2, this sequence has a convergent subsequence; by the discreteness of L, we find that there exists a single nonzero lattice point v such that $v \in P_{1+1/i}$ for all i sufficiently large. It follows that v (the limit of this sequence) lies in the compact set $P = P_1$.

□

In the next theorem, we choose a compact, convex, centrally symmetric subset of $F_{\mathbb{R}} \cong \mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$ in such a way that we can prove the existence of a "short vector" in a lattice.

Theorem 3.12 *Suppose that L is a $\mathbb{Z}$-lattice in a number field F with $n = [F : \mathbb{Q}]$. Then, there exists a nonzero element $\alpha \in L$, such that*

$$|N_{F/\mathbb{Q}}(\alpha)| \leq \frac{n!}{n^n} \left(\frac{4}{\pi}\right)^{r_2} \cdot \sqrt{|\operatorname{Disc}(L)|}.$$

Proof: For all $t > 0$, consider the compact, convex, centrally symmetric subset of $F_{\mathbb{R}}$ given by

$$P_t = \{x \in F_{\mathbb{R}} : \sum_{\sigma \in \mathrm{Emb}(F,\mathbb{C})} |\sigma(x)| \leq t\}.$$

Here, we are using the fact that any embedding σ of F into $\mathbb{C}$ extends uniquely to an $\mathbb{R}$-algebra homomorphism from $F_{\mathbb{R}}$ to $\mathbb{C}$, by sending $x \otimes r$ to rx for all $x \in F$ and $r \in \mathbb{R}$.

The fact that P_t is compact follows from the observation that P_t is closed and (almost by definition) bounded. The fact that P_t is centrally symmetric follows from the observation that its definition is symmetric with respect to the transformation $v \mapsto -v$ of $F_{\mathbb{R}}$. The fact that P_t is centrally symmetric follows from the triangle inequality.

Note that the definition of P_t essentially depends only upon r_1, r_2, and t (and not otherwise on the number field F); thus we write $P_t(r_1, r_2)$. Furthermore, since $P_t(r_1, r_2)$ is obtained by scaling $P_1(r_1, r_2)$ uniformly by a factor of t, there is a function $V(r_1, r_2) = Vol(P_1(r_1, r_2))$, such that:

$$Vol(P_t(r_1, r_2)) = V(r_1, r_2)t^n.$$

We compute the function $V(r_1, r_2)$, recursively with respect to r_2.

$r_2 = 0$: When $r_2 = 0$, the region P_1 is an "orthoplex":

$$P_1 = \{(x_1, \ldots, x_n) \in \mathbb{R}^n \text{ such that } \sum |x_i| \leq 1\}.$$

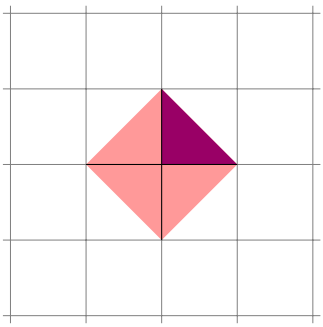

Figure 3.3: The orthoplex P_1 in $\mathbb{R}^2$, dissected into 2^2 right triangles (one of which is shaded).

This orthoplex can be dissected into 2^n congruent pieces, based on the signs of the coordinates:

$$V(n,0) = 2^n \operatorname{Vol}\{(x_1,\ldots,x_n) \in \mathbb{R}^n \colon \sum x_i \leq 1 \text{ and } \forall i, x_i > 0\}.$$

Each of these pieces is a right pyramid, and the volume can be computed without too much trouble:

$$V(n,0) = \frac{2^n}{n!}.$$

$r_2 > 0$**:** When $r_2 > 0$, we may express $V(r_1,r_2)$ as an iterated integral, by slicing along one complex coordinate, which we express in polar coordinates ρ and θ:

$$V(r_1,r_2) = \int_0^{1/2}\int_0^{2\pi} V(r_1,r_2-1)(1-2\rho)^{n-2}\rho d\theta d\rho.$$

Computing this integral, using integration by parts,

$$\begin{aligned} V(r_1,r_2) &= 2\pi V(r_1,r_2-1)\int_0^{1/2}(1-2\rho)^{n-2}\rho d\rho \\ &= 2\pi V(r_1,r_2-1)\int_0^{1/2}\frac{1}{2(n-1)}(1-2\rho)^{n-1}d\rho \\ &= 2\pi V(r_1,r_2-1)\frac{1}{4n(n-1)}(1-2\rho)^n|_0^{t/2} \\ &= V(r_1,r_2-1)\frac{\pi}{2n(n-1)}. \end{aligned}$$

The recursive relation $V(r_1,r_2) = V(r_1,r_2-1)\pi/2n(n-1)$ implies that

$$V(r_1,r_2) = V(r_1,0)\left(\frac{\pi}{2}\right)^{r_2}\frac{1}{n(n-1)\cdots(n-2r_2+1)}.$$

From our previous result on $V(r_1,0)$ (and as usual, recalling that $n = r_1 + 2r_2$), we find that

$$V(r_1,r_2) = 2^{r_1}\left(\frac{\pi}{2}\right)^{r_2}\frac{1}{n!}.$$

In particular, we find that

$$Vol(P_t) = Vol(P_t(r_1,r_2)) = 2^{r_1}\left(\frac{\pi}{2}\right)^{r_2}\frac{t^n}{n!}.$$

Choose[10] t such that $Vol(P_t) = 2^n Vol(F_{\mathbb{R}}/L)$. By Proposition 3.8, and a bit of algebra

$$Vol(P_t) = 2^n Vol(F_{\mathbb{R}}/L) = 2^{r_1+r_2}\sqrt{|\operatorname{Disc}(L)|}.$$

Since P_t satisfies the hypotheses of the previous Theorem 3.11, there exists a nonzero element $\alpha \in L \cap P_t$. The norm of α can be

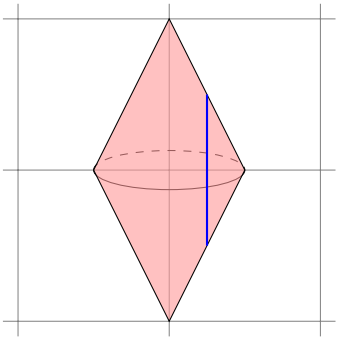

Figure 3.4: $V(1,1)$ is computed by integrating over the disc of radius $1/2$. The blue line segment is a 1-dimensional orthoplex, with length $V(1,0)(1-2\cdot 1/4)^{3-2}$.

[10] Explicitly, we are choosing t so that

$$t^n = 2^{r_1+r_2}2^{-r_1}d!2^{r_2}\pi^{-r_2}\sqrt{|\operatorname{Disc}(L)|}.$$

To simplify,

$$t^n = n!\left(\frac{4}{\pi}\right)^{r_2}\sqrt{|\operatorname{Disc}(L)|}.$$

computed via embeddings, and estimated using the fact that the geometric mean is bounded by the arithmetic mean:

$$|\,\mathrm{N}(\alpha)|^{1/n} = \left(\prod_{i=1}^{n} |\sigma_i(\alpha)|\right)^{1/n} \leq \frac{1}{n}\sum_{i=1}^{n} |\sigma_i(\alpha)| \leq \frac{t}{n}.$$

It follows that $|\,\mathrm{N}(\alpha)| \leq {}^{t^n}/_{n^n}$. Hence we find that

$$|\,\mathrm{N}(\alpha)| \leq \frac{t^n}{n^n} = \frac{n!}{n^n}\left(\frac{4}{\pi}\right)^{r_2}\sqrt{|\,\mathrm{Disc}(L)|}.$$

□

In the particular case when the lattice is the ring of integers in a number field, we find that

Corollary 3.13 *If $\mathcal{O}_F$ is the ring of integers in a number field, so* $\mathrm{Disc}(F) = \mathrm{Disc}(\mathcal{O}_F)$*, then we find that*

$$\sqrt{|\,\mathrm{Disc}(F)|} \geq \frac{n^n}{n!}\left(\frac{\pi}{4}\right)^{r_2}.$$

Proof: Applying the previous theorem, there exists a nonzero element $\alpha \in \mathcal{O}_F$, such that

$$|\,\mathrm{N}(\alpha)| \leq \frac{n!}{n^n}\left(\frac{4}{\pi}\right)^{r_2}\sqrt{|\,\mathrm{Disc}(L)|}.$$

However, for a nonzero element $\alpha \in \mathcal{O}_F$, we also find that $0 \neq \mathrm{N}(\alpha) \in \mathbb{Z}$. It follows that $|\,\mathrm{N}(\alpha)| \geq 1$. Hence we have

$$\frac{n!}{n^n}\left(\frac{4}{\pi}\right)^{r_2}\sqrt{|\,\mathrm{Disc}(L)|} \geq 1.$$

The result follows immediately.

□

Finally, we achieve the theorem of Minkowski

Corollary 3.14 *If F is a number field, and* $\mathrm{Disc}(F) = \pm 1$*, then* $\mathrm{Disc}(F) = 1$ *and* $F = \mathbb{Q}$*.*

Proof: Consider the function

$$\mu(n, r_2) = \frac{n^n}{n!}\left(\frac{\pi}{4}\right)^{r_2}.$$

Since $n \geq 2r_2$, we find that

$$\mu(n, r_2) \geq \frac{n^n}{n!}\left(\frac{\pi}{4}\right)^{n/2}.$$

The right side of the above inequality is monotonic strictly increasing, as a function of $n \geq 1$ (as can be seen by induction). Hence $\sqrt{|\,\mathrm{Disc}(F)|} = 1 \geq \mu(n, r_2)$ implies that $n = 1$, so $F = \mathbb{Q}$.

□

Consider the quantity occurring in the Minkowsi bound:

$$\mu(n, r_2) = \frac{n^n}{n!}\left(\frac{\pi}{4}\right)^{r_2}.$$

This can be analytically approximated, using a "double-inequality" version of Stirling's formula, due to H. Robbins[11]. Specifically, Robbins prove that

[11] Herbert Robbins. A remark on Stirling's formula. *Amer. Math. Monthly*, 62:26–29, 1955. ISSN 0002-9890

$$n! = \sqrt{2\pi}n^{n+1/2}e^{-n}e^{r_n} = \sqrt{2\pi n}n^n e^{-n+r_n},$$

where for all $n \geq 1$,

$$\frac{1}{12n+1} < r_n < \frac{1}{12n}.$$

From this formula, we deduce that

$$\mu(n, r_2) = \frac{e^{n-r_n}}{\sqrt{2\pi n}}\left(\frac{\pi}{4}\right)^{r_2}.$$

As $\sqrt{|Disc(F)|} \geq \mu(n, r_2)$, raising both sides of this inquality to the $2/n$ power yields

$$|\operatorname{Disc}(F)|^{1/n} \geq e^2\left(\frac{\pi}{4}\right)^{2r_2/n}\left(\frac{e^{2r_n/n}}{\sqrt[n]{2\pi n}}\right).$$

Now we may expand

$$e^2 = e^{2n/n} = (e^2)^{\frac{r_1}{n}+\frac{2r_2}{n}},$$

and we find

$$\sqrt[n]{|\operatorname{Disc}(F)|} \geq (e^2)^{r_1/n}\left(e^2\pi/4\right)^{2r_2/n}\left(\frac{e^{2r_n/n}}{\sqrt[n]{2\pi n}}\right).$$

The final term approaches 1 as n approaches infinity. It follows that

$$\sqrt[n]{|\operatorname{Disc}(F)|} \gtrsim (7.3)^{r_1/n}(5.8)^{2r_2/n},$$

where the symbol $\gtrsim$ denotes that the left side is greater than the right side, for all sufficiently large values of n.

3.3 *Exercises*

Exercise 3.1 *Suppose that F is a number field, and $Disc(F) = \pm 4$. Describe the possible values of r_1, r_2, and d, using the "Minkowski bounds". How about $Disc(F) = 5, 8$? How about $Disc(F) = -7, -8$?*

Exercise 3.2 *Suppose that L is an even unimodular lattice, in an 8-dimensional vector space endowed with a nondegenerate, positive-definite, symmetric bilinear form. Prove that L contains a vector v such that $\langle v, v\rangle = 2$. Hint: you might as well assume that L sits in the Euclidean space $\mathbb{R}^8$. Compute (or look up) the volume of an 8-dimensional sphere of radius ρ for some values of $\rho < 4$..*

Exercise 3.3 *Consider the number field $F = \mathbb{Q}(\sqrt{2}, \sqrt{-3})$. Compute the discriminant of F. Find $\mathcal{O}_F$. Recompute the discriminant of $\mathcal{O}_F$ by computing the volume of a parallelotope in $\mathbb{C}^2$.*

4
Ideals

One of the gems of number theory, from the second half of the nineteenth century, is the theory of algebraic integers and ideals. While germs of ideal theory can be found in the work of Kummer and Kronecker, the modern theory owes much to Dedekind's 1877 work[1] (translated into English with an historical introduction by Stillwell[2]).

We develop the theory of "ideal factorization" in this chapter. As the theory of unique factorization of integers into primes fails in most rings of integers (such as $\mathbb{Z}[e^{2\pi i/23}]$, for example), one replaces this by the unique factorization of ideals into prime ideals (valid in any "Dedekind domain").

[1] Richard Dedekind. Sur la théorie des nombres entiers algébriques. *Darboux Bull. (2)*, I:17–41; 69–92; 114–164; 207–248, 1877

[2] Richard Dedekind. *Theory of algebraic integers*. Cambridge Mathematical Library. Cambridge University Press, Cambridge, 1996. ISBN 0-521-56518-9. Translated from the 1877 French original and with an introduction by John Stillwell

4.1 Ideals and orders

Let F be a number field, with $n = [F : \mathbb{Q}]$. Let $\mathcal{O}_F$ be the ring of integers in F. We have studied $\mathbb{Z}$-lattices in F quite extensively, and proven that $\mathcal{O}_F$ is a $\mathbb{Z}$-lattice in F. It is important not only to study $\mathcal{O}_F$, but other orders in F:

Definition 4.1 *An **order** in F is a $\mathbb{Z}$-lattice $\mathcal{O}$ in F, such that $\mathcal{O}$ is a subring of F.*

It turns out that every order $\mathcal{O}$ in F is contained in the ring of integers $\mathcal{O}_F$; for that reason, $\mathcal{O}_F$ is often referred to as the **maximal order** in F.

Proposition 4.2 *Suppose that $\mathcal{O}$ is an order in the number field F. Then every element of $\mathcal{O}$ is integral over $\mathbb{Z}$, i.e., $\mathcal{O} \subset \mathcal{O}_F$. Hence $\mathcal{O}_F$ is the unique maximal order in F.*

Proof: Let α be an element of $\mathcal{O}$. Since $\mathcal{O}$ is a $\mathbb{Z}$-lattice and a ring, we may consider the "multiplication by α" endomorphism m_α of the $\mathbb{Z}$-module $\mathcal{O}$. Then m_α, as an endomorphism of a free finite-rank $\mathbb{Z}$-module, has a characteristic polynomial which is monic with integer

coefficients. By the Cayley-Hamilton theorem, we find that m_α is a root of this polynomial, from which we deduce that α is a root of this polynomial in $\mathcal{O}$. Thus α is integral over $\mathbb{Z}$.

□

Within an order $\mathcal{O}$ in F, other arithmetically important lattices in F are given by ideals in $\mathcal{O}$:

Proposition 4.3 *Suppose that I is a nonzero ideal in the ring $\mathcal{O}$. Then $[\mathcal{O} : I]$ is finite*[3]*, and is a $\mathbb{Z}$-lattice in F. Furthermore, the index $[\mathcal{O} : I]$ is bounded above by $|\mathrm{N}_{F/\mathbb{Q}}(\alpha)|^n$, for every nonzero $\alpha \in I$.*

[3] By $[\mathcal{O} : I]$, we mean the index of I in $\mathcal{O}$, as a group under addition.

Proof: Suppose that $\alpha \in I$ and $\alpha \neq 0$. Then $0 \neq N_{\mathbb{Q}(\alpha)/\mathbb{Q}}(\alpha) \in \mathbb{Z}$. Moreover, the identity

$$\alpha^d - Tr_{\mathbb{Q}(\alpha)/\mathbb{Q}}(\alpha)\alpha^{d-1} + \cdots \pm N_{\mathbb{Q}(\alpha)/\mathbb{Q}}(\alpha) = 0$$

implies that $N_{\mathbb{Q}(\alpha)/\mathbb{Q}}(\alpha)$ is a multiple of α in $\mathcal{O}$. It follows that

$$N = N_{\mathbb{Q}(\alpha)/\mathbb{Q}}(\alpha) \in I \subset \mathcal{O}.$$

It follows that $N\mathcal{O} \subset I \subset \mathcal{O}$. Therefore, we find a bound on $[\mathcal{O} : I]$:

$$[\mathcal{O} : I] \text{ divides } [\mathcal{O} : N\mathcal{O}] = |N|^n.$$

It follows that I is a $\mathbb{Z}$-lattice in F.

□

Corollary 4.4 *Suppose that P is a nonzero prime ideal in the order $\mathcal{O}$. Then P is a maximal ideal.*[4]

[4] We say that $\mathcal{O}$ is one-dimensional since any maximal chain of prime ideals has length 1: $(0) \subset P$ for some nonzero prime ideal P which is maximal.

Proof: By the previous proposition, we find that $k_P = \mathcal{O}/P$ is a finite integral domain. Suppose that $0 \neq \bar{\alpha} \in k_P$; let $m_{\bar{\alpha}}$ denote the multiplication by $\bar{\alpha}$ map from k_P to k_P. Then $m_{\bar{\alpha}}$ is injective, since k_P is an integral domain. By the finiteness of k_P, we find that $m_{\bar{\alpha}}$ is surjective; hence there exists $\bar{\beta} \in k_P$ such that $\bar{\alpha}\bar{\beta} = \bar{1} \in k_P$. Thus k_P is a field.

□

Corollary 4.5 *Suppose that $I_1 \subset I_2 \subset \cdots$ is a chain of ideals in the ring $\mathcal{O}$. Then the chain stabilizes, i.e., there exists a natural number m such that $I_i = I_j$ for all $i, j \geq m$. In other words, the ring $\mathcal{O}$ is Noetherian.*

Proof: We have seen that the indices $[\mathcal{O} : I_i]$ are finite for all i; moreover, the inclusions imply divisibility:

$$[\mathcal{O} : I_i] \text{ divides } [\mathcal{O} : I_j], \text{ if } i > j.$$

Since any decreasing chain of natural numbers eventually stabilizes, we find that these indices stabilize, and hence the chain of ideals stabilize.

□

Definition 4.6 *Suppose that I is an ideal in $\mathcal{O}$. The **norm** of I (in $\mathcal{O}$), denoted $\mathrm{N}(I)$ is defined to be the index $[\mathcal{O} : I]$, or equivalently, the order of the finite ring $\mathcal{O}/I$.*

For principal ideals, the norm coincides with our previous definition:

Proposition 4.7 *Suppose that $\alpha \in \mathcal{O}$. Then $|\mathrm{N}_{F/\mathbb{Q}}(\alpha)| = \mathrm{N}((\alpha))$, where (α) denotes the principal ideal generated by α.*

Proof: On the one hand, $\mathrm{N}((\alpha)) = [\mathcal{O} : (\alpha)] = [\mathcal{O} : \alpha\mathcal{O}]$. But the index of $\alpha\mathcal{O}$ in $\mathcal{O}$ is precisely the absolute value of the determinant of the endomorphism m_α of $\mathcal{O}$, which is precisely the absolute value of $\mathrm{N}_{F/\mathbb{Q}}(\alpha)$.

□

4.2 *Operations on lattices and ideals*

Fix an order $\mathcal{O}$ in F, for this section. We introduce some operations on ideals which are valid more generally for lattices in F.

Definition 4.8 *Suppose that L and M are $\mathbb{Z}$-lattices in F. The **sum of lattices** $L + M$ is defined to be the smallest $\mathbb{Z}$-submodule of F containing both L and M, or equivalently, the $\mathbb{Z}$-module whose elements are all sums of elements of L with elements of M. The **product of lattices** $L \cdot M$ is defined to be the smallest $\mathbb{Z}$-submodule of F containing all elements $v \cdot w$, whenever $v \in L$ and $w \in M$. Equivalently, $L \cdot M$ is the lattice whose elements are finite sums of the form $\sum v_i \cdot w_i$, where v_i, w_i are elements of L and M, respectively.*

Proposition 4.9 *Given two $\mathbb{Z}$-lattices L and M in F, $L + M$ is a lattice in F and $L \cdot M$ is a lattice in F. Furthermore, if L and M are stable under the action of $\mathcal{O}$, i.e., $\mathcal{O}L = L$ and $\mathcal{O}M = M$, then the same is true for $L + M$ and $L \cdot M$: $\mathcal{O} \cdot (L + M) = (L + M)$ and $\mathcal{O} \cdot (L \cdot M) = L \cdot M$.*

Proof: The fact that $L + M$ and $L \cdot M$ are $\mathbb{Z}$-submodules of F follows directly from their definition. To demonstrate that these are lattices, we use a typical squeeze argument. There exists a nonzero integer ℓ such that $\ell L \subset M$ by Proposition 1.4. It follows that

$$L + M \subset \ell^{-1}M + M \subset \ell^{-1}M, \text{ and } \ell L \subset L + M.$$

Hence $L + M$ is a lattice. There also exist nonzero integers ℓ, m, such that $\ell L \subset \mathcal{O}$ and $mM \subset \mathcal{O}$. It follows that

$$L \cdot M \subset (\ell m)^{-1}\mathcal{O}.$$

Also, there exist nonzero integers ℓ', m' such that $\ell'\mathcal{O} \subset L$ and $m'\mathcal{O} \subset M$. Hence

$$\mathcal{O} \cdot \mathcal{O} = \mathcal{O} \subset (\ell' m')^{-1} LM,$$

so that $(\ell' m')\mathcal{O} \subset L \cdot M$. Hence $L \cdot M$ is a lattice.

Now, if L and M are stable for the action of $\mathcal{O}$, then certainly $\mathcal{O} \cdot (L + M) = (L + M)$ and $\mathcal{O} \cdot (L \cdot M) = (L \cdot M)$, by the distributive and associative properties of multiplication.

□

In particular, when L and M are ideals in $\mathcal{O}$, we find that $L + M$ and $L \cdot M$ are ideals in $\mathcal{O}$. There are two inclusions to remember in this case:

Proposition 4.10 *Suppose that L and M are ideals in $\mathcal{O}$. Then*

$$(L \cup M) \subset L + M, \text{ and } L \cdot M \subset L \cap M.$$

PROOF: The first inclusion, $L \cup M \subset L + M$ is obvious from the definition of $L + M$ (and is true for lattices, and not just ideals). The second inclusion follows directly from the definition of an ideal.

□

Next, we discuss the "lattices quotient", in a number field F.

Definition 4.11 *Suppose that L and M are lattices in a number field F. Define the **lattice quotient** $(L \div M)$ to be the $\mathbb{Z}$-submodule of F given by*

$$L \div M = \{\alpha \in F \text{ such that } \alpha\beta \in L \text{ for all } \beta \in M\}.$$

Proposition 4.12 *Suppose that L and M are lattices in a number field F. Then $(L \div M)$ is also a lattice in F and $M \cdot (L \div M) \subset \mathcal{O}$. If L is $\mathcal{O}$-stable, then $(L \div M)$ is $\mathcal{O}$-stable.*

PROOF: Let $(m_1, \ldots, m_n)$ be a $\mathbb{Z}$-basis of M. Then

$$(L \div M) = \bigcap_{i=1}^{n} L \cdot m_i^{-1}.$$

Therefore $(L \div M)$ is the intersection of a finite number of lattices, and so it is a lattice. The fact that $M \cdot (L \div M) \subset \mathcal{O}$ follows directly from the definition of $(L \div M)$. If $\mathcal{O}L = L$, then one can check directly that $\mathcal{O}(L \div M) = (L \div M)$.

□

Next, we discuss endomorphisms of lattices. Suppose that L is a lattice in F. Then, we may consider the (noncommutative, unless $n = 1$) ring of endomorphisms[5] of L as a $\mathbb{Z}$-module:

$$\mathrm{End}_{\mathbb{Z}}(L) = \{\mathbb{Z}\text{-linear maps, } e\colon L \to L\}.$$

[5] Since L is isomorphic to $\mathbb{Z}^n$ as a $\mathbb{Z}$-module, $\mathrm{End}_{\mathbb{Z}}(L)$ is isomorphic to $M_n(\mathbb{Z})$, the algebra of n by n integer matrices.

When $\mathcal{O}L = L$, so that L is naturally a $\mathcal{O}$-module, we my consider the subring of $\mathcal{O}$-linear endomorphisms:

$$\mathrm{End}_{\mathcal{O}}(L) = \{\mathcal{O}\text{-linear maps, } e\colon L \to L\}.$$

Since any $\mathcal{O}$-linear endomorphism of L extends uniquely to a $\mathcal{O}$-linear endomorphism of $F = \mathbb{Q} \cdot L$, on which it is a F-linear endomorphism, we find an inclusion $\mathrm{End}_{\mathcal{O}}(L) \hookrightarrow \mathrm{End}_F(F) = F$. In other words, every element $e \in \mathrm{End}_{\mathcal{O}}(L)$ has the form $e(v) = \alpha \cdot v$ for some $\alpha \in F$, uniquely determined by e (and depending only on e and not on v). In this way, we identify $\mathrm{End}_{\mathcal{O}}(L)$ with its canonical image in F. Another characterization of its image is the following:

$$\mathrm{End}_{\mathcal{O}}(L) = (L \div L) = \{\alpha \in F\colon \alpha L \subset L\}.$$

Proposition 4.13 *Suppose that L is a lattice in F, and $\mathcal{O}L = L$. Then $\mathrm{End}_{\mathcal{O}}(L)$ is an order in F containing $\mathcal{O}$.*

Proof: We have seen that $\mathrm{End}_{\mathcal{O}}(L)$ is a subring of F, so it remains to prove that $\mathrm{End}_{\mathcal{O}}(L)$ is a lattice in F. Since $\mathcal{O}L = L$, we have $\mathcal{O} \subset \mathrm{End}_{\mathcal{O}}(L)$. On the other hand, $\mathrm{End}_{\mathcal{O}}(L) = (L \div L)$ is a lattice, and hence is an order in F.

□

Corollary 4.14 *Suppose that L is a lattice in F, and $\mathcal{O}_F L = L$. Then $\mathrm{End}_{\mathcal{O}_F}(L) = (L \div L) = \mathcal{O}_F$.*

Proof: Since $\mathrm{End}_{\mathcal{O}_F}(L)$ an order containing $\mathcal{O}_F$, and $\mathcal{O}_F$ is a maximal order, $\mathrm{End}_{\mathcal{O}_F}(L) = \mathcal{O}_F$.

□

Proposition 4.15 *Suppose that $L = \alpha\mathcal{O}$ is a principal ideal in the order $\mathcal{O}$. Then $\mathrm{End}_{\mathcal{O}}(L) = \mathcal{O}$.*

Proof: The previous proposition implies that $\mathrm{End}_{\mathcal{O}}(L)$ contains $\mathcal{O}$. Furthermore, if $\beta \in \mathrm{End}_{\mathcal{O}}(L)$, then $\beta \cdot \alpha \in \alpha\mathcal{O}$. It follows that $\beta \in \mathcal{O}$.

□

4.3 *Prime ideals in orders*

While the factorization of ideals into prime ideals does not behave well in general orders, the following lemma holds in this level of generality.

Lemma 4.16 *Suppose that I is a nonzero ideal in an order $\mathcal{O}$. Then there exist nonzero prime ideals $P_1, \ldots, P_t$ of $\mathcal{O}$ such that I contains $P_1 \cdot \cdots \cdot P_t$ and $\mathrm{N}(I) = \prod \mathrm{N}(P_i)$. Furthermore, if P is a prime ideal containing I, then P occurs among the prime ideals $P_1, \ldots, P_t$.*

Proof: Consider the quotient $M = \mathcal{O}/I$, as a $\mathcal{O}$-module. There exists a filtration

$$M = M_0 \supset M_1 \supset \cdots \supset M_t = \{0\}$$

of this module, such that the successive quotients M_i/M_{i+1} are simple $\mathcal{O}$-modules. As each submodule of M corresponds to an ideal containing I, we find a sequence of ideals

$$I = I_0 \subset I_1 \subset \cdots \subset I_t = \mathcal{O},$$

for which $M_i = \mathcal{O}/I$ and so I_{i+1}/I_i is a simple $\mathcal{O}$-module.

As a nonzero, finite (in cardinality!), simple $\mathcal{O}$-module, each quotient I_{i+1}/I_i is cyclic, generated by some (any nonzero) element $\bar{e}_i \in I_{i+1}/I_i$. Define

$$P_i = Ann(\bar{e}_i) = \{\alpha \in \mathcal{O} \colon \alpha\bar{e}_i = \bar{0}\}.$$

The map $\mathcal{O}/P_i \to I_{i+1}/I_i$, sending α to $\alpha\bar{e}_i$, is an isomorphism of $\mathcal{O}$-modules by the simplicity of the target. Furthermore, the simplicity implies that P_i is a maximal ideal. By analyzing indices, we see that

$$\begin{aligned} \mathrm{N}(I) &= [\mathcal{O} : I] = [I_t : I_{t-1}] \cdots [I_1 : I_0] \\ &= [\mathcal{O} : P_t] \cdots [\mathcal{O} : P_1] \\ &= \mathrm{N}(P_t) \cdots \mathrm{N}(P_1). \end{aligned}$$

It now follows that there are nonzero prime (maximal) ideals $P_1, \ldots, P_t$ such that $P_i \cdot I_{i+1} \subset I_i$. Hence $P_1 \cdots P_t \subset I_0 = I$.

Furthermore, if P is any prime ideal containing I, then we claim that P contains some ideal P_i. Indeed, if P contains none of the ideals P_i, then there exist elements $\alpha_i \in P_i$ for all i such that $\alpha_i \notin P$. However, since I contains $P_1 \cdots P_t$, we find that $\prod \alpha_i \in I \subset P$. It follows that one of the factors α_i must contain P, a contradiction. It follows that P contains some ideal P_i; since both are nonzero, both are maximal, and it follows that $P = P_i$.

□

To begin our approach to factorization, we have

Theorem 4.17 *Suppose that $\mathcal{O}$ is an order in F, and P a nonzero prime ideal in $\mathcal{O}$. Then $(\mathcal{O} \div P)$ contains, but is not equal to $\mathcal{O}$.*

PROOF: It is clear from the definition that $(\mathcal{O} \div P)$ contains $\mathcal{O}$. To see that equality does not hold, let α be a nonzero element of P, and consider $I = \alpha\mathcal{O} \subset P \subset \mathcal{O}$. By the previous lemma, there are prime ideals $P_1, \ldots, P_t$ such that $I \supset PP_1 \cdots P_t$. If I contains $P_1 \cdots P_t$, then $P = P_i$ for some $1 \leq i \leq t$; assuming that $i = t$ in this case, we have $I \supset PP_1 \cdots P_{t-1}$. Continuing in this fashion, we may "cancel" as many factors of P as possible until

$$P_1 \cdots P_u \not\subset I \text{ and } PP_1 \cdots P_u \subset I.$$

Fix $\beta \in (P_1 \cdots P_u) \backslash I$. Let $\gamma = \beta/\alpha \in F$, so that $\gamma \notin \mathcal{O}$ (since $\beta \notin I = \alpha\mathcal{O}$). Then we find that $\gamma P \subset \mathcal{O}$; hence $\gamma \in (\mathcal{O} \div P)$.

□

Corollary 4.18 *Suppose that $\mathcal{O}$ is an order in F and P is a nonzero prime ideal in $\mathcal{O}$. Then either $P \cdot (\mathcal{O} \div P) = \mathcal{O}$, or else $(P \div P)$ contains but does not equal $\mathcal{O}$.*

PROOF: In general, we have $P = \mathcal{O} \cdot P \subset (\mathcal{O} \div P) \cdot P \subset \mathcal{O}$. If $(\mathcal{O} \div P) \cdot P \neq \mathcal{O}$, then we find that $(\mathcal{O} \div P) \cdot P$ is a proper ideal in $\mathcal{O}$ (since it is a sub-$\mathcal{O}$-module of $\mathcal{O}$). Furthermore, $(\mathcal{O} \div P) \cdot P$ contains P, a maximal ideal, and hence $(\mathcal{O} \div P) \cdot P = P$. By the previous theorem, there exists $\gamma \in (\mathcal{O} \div P)$, such that $\gamma \notin \mathcal{O}$. But then $\gamma P \subset P$, so that $\gamma \in (P \div P)$. Hence $(P \div P)$ contains, but does not equal $\mathcal{O}$.

□

4.4 *Factorization in the maximal order*

We may characterize the nonzero ideals in any order $\mathcal{O}$ precisely as the sublattices of $\mathcal{O}$, which are stable under multiplication by $\mathcal{O}$. Such a characterization leads directly to a generalization:

Definition 4.19 *A **fractional ideal** in F is a $\mathbb{Z}$-lattice $L \subset F$, such that*[6] *$\mathcal{O}_F \cdot L = L$.*

[6] Note that the definition of a fractional ideal references the maximal order $\mathcal{O}_F$, not an arbitrary order $\mathcal{O}$.

In particular, a nonzero ideal in $\mathcal{O}_F$ is simply a fractional ideal which is contained in $\mathcal{O}_F$. Just as one may construct a principal ideal (α), for every element $\alpha \in \mathcal{O}_F$, one may construct a **principal fractional ideal** (α) for every nonzero element $\alpha \in F$:

$$(\alpha) = \mathcal{O}_F\alpha = \{z \in F : z = \beta\alpha \text{ for some } \beta \in \mathcal{O}_F\}.$$

Proposition 4.20 *For any nonzero element $\alpha \in F$, (α) is a fractional ideal.*

PROOF: To see that (α) is a fractional ideal, it is clear that (α) is a $\mathbb{Z}$-submodule of F and stable under multiplication by $\mathcal{O}_F$. To see that (α) is a lattice, recall that by Proposition 2.8 there exists a nonzero $N \in \mathbb{Z}$ such that $N\alpha \in \mathcal{O}_F$. Similarly, there exists a nonzero $M \in \mathbb{Z}$ such that $M\alpha^{-1} \in \mathcal{O}_F$. It follows that if $z \in M\mathcal{O}_F$, then $z\alpha^{-1} \in M\alpha^{-1}\mathcal{O}_F$, so $z\alpha^{-1} \in \mathcal{O}_F$ and $z \in \alpha\mathcal{O}_F$. We have proven that

$$M\mathcal{O}_F \subset (\alpha) \subset \frac{1}{N}\mathcal{O}_F.$$

It follows that (α) is a $\mathbb{Z}$-lattice in F, so (α) is a fractional ideal.

□

A direct consequence of Proposition 4.9 and Proposition 4.12 is the following

Proposition 4.21 *If L and M are fractional ideals in F, then $L + M$ and $L \cdot M$ are fractional ideals in F. Also, $L \div M$ is a fractional ideal in F.*

Inversion of fractional ideals leads to a very important cancellation principle; we begin proving this for prime ideals.

Lemma 4.22 *Suppose that P is a prime ideal in $\mathcal{O}_F$. Then, the fractional ideal $(\mathcal{O}_F \div P)$ satisfies $(\mathcal{O}_F \div P) \cdot P = \mathcal{O}_F$.*

PROOF: If $(\mathcal{O}_F \div P) \cdot P \neq \mathcal{O}_F$, then by Corollary 4.18, we find that $\mathrm{End}(P) = (P \div P)$ properly contains $\mathcal{O}_F$; but this contradicts the maximality of the order $\mathcal{O}_F$.

□

The most important implication of this lemma is the following "prime cancellation" lemma:

Lemma 4.23 *Suppose that P is a prime ideal in $\mathcal{O}_F$. Then, for any fractional ideals I, J in F, $I = J$ if and only if $I \cdot P = J \cdot P$.*

PROOF: If $I = J$, then clearly $I \cdot P = J \cdot P$. On the other hand, if $I \cdot P = J \cdot P$, then $I \cdot P \cdot (\mathcal{O} \div P) = J \cdot P \cdot (\mathcal{O} \div P)$. Hence $I \cdot \mathcal{O}_F = J \cdot \mathcal{O}_F$. As I and J are fractional ideals, this implies that $I = J$.

□

With this lemma in place, it makes sense to define

Definition 4.24 *Suppose that I is a fractional ideal. Define the **inverse fractional ideal** $I^{-1} = (\mathcal{O}_F \div I)$.*

In particular, $P^{-1} \cdot P = \mathcal{O}_F$, for every prime ideal P of $\mathcal{O}_F$. We will se that this generalizes to any fractional ideal.

Theorem 4.25 (Dedekind) *Every nonzero ideal I in $\mathcal{O}_F$ can be expressed as the (possibly empty) product $P_1 \cdots P_t$ of prime ideals, and this factorization is unique up to order.*

PROOF: If I is a nonzero proper ideal in $\mathcal{O}_F$, then we have seen that there is a chain of ideals $I = I_0 \subset \cdots I_t = \mathcal{O}_F$ for which the successive quotients I_{i+1}/I_i are simple $\mathcal{O}_F$-modules isomorphic to quotients $\mathcal{O}_F/P_i$ for some maximal ideals P_i, and the data $P_1, \ldots, P_t$ is uniquely determined (up to order) by I, using the Jordan-Hölder theorem. The number t is called the length of the module $\mathcal{O}_F/I$.

We prove that $I = P_1 \cdots P_t$ in this circumstance, by induction on the length of $\mathcal{O}_F/I$.

When $t = 1$, we find that the only prime ideal containing I is P_1, and $P_1 \subset I \subset P_1 \subset \mathcal{O}_F$, which implies that $I = P_1$. Now, we assume that $t > 1$, and that the result has been proven for smaller lengths. In particular, we find that

$$P_1 \cdots P_t \subset I = I_0 \subset I_1 \subset \cdots \subset I_t = \mathcal{O}_F.$$

As I_1/I_0 is isomorphic to $\mathcal{O}_F/P_1$, we find that the Jordan-Hölder components for $\mathcal{O}_F/I_1$ are precisely $P_2, \ldots, P_t$. It follows from the inductive hypothesis that

$$P_2 \cdots P_t = I_1 \subset \cdots \subset I_t = \mathcal{O}_F.$$

Thus we find that

$$P_1 I_1 = P_1 P_2 \cdots P_t \subset I \subset I_1 = P_2 \cdots P_t.$$

Multiplying by $P_2^{-1} \cdots P_t^{-1}$ yields

$$P_1 \subset I P_2^{-1} \cdots P_t^{-1} \subset \mathcal{O}_F.$$

If $\mathcal{O}_F = I P_2^{-1} \cdots P_t^{-1}$, then we find that $I = P_2 \cdots P_t$. This implies that $\mathcal{O}_F/I$ has a Jordan-Hölder series of length $t-1$, a contradiction. Hence, the maximality of P_1 implies that

$$P_1 = I P_2^{-1} \cdots P_t^{-1}.$$

Therefore, $I = P_1 \cdots P_t$.

For uniqueness, one may apply the uniqueness of the simple factors in the Jordan-Hölder series of I.

□

Lemma 4.26 *Suppose that I, J are fractional ideals, with $I \subset J$. Then, there exists an ideal M in $\mathcal{O}_F$, such that $J \cdot M = I$.*

PROOF: There exists an integer n, such that $n \cdot I \subset n \cdot J \subset \mathcal{O}_F$. It follows that both nI and nJ are ideals in $\mathcal{O}_F$, and hence have factorizations into prime ideals:

$$n \cdot I = P_1 \cdots P_s, \text{ and } n \cdot J = Q_1 \cdots Q_t.$$

The containment $nI \subset nJ$ implies that Q_1 (as a Jordan-Hölder component of $\mathcal{O}_F/nJ$) also occurs in the factorization of I (as a Jordan-Hölder component of $\mathcal{O}_F/nI$). Without loss of generality, we find that $Q_1 = P_1$. Thus we find that $nIP_1^{-1} \subset nJP_1^{-1}$. Continuing this process, we see that

$$nI = P_1 \cdots P_s = Q_1 \cdots Q_t P_{t+1} \cdots P_s = nJP_{t+1} \cdots P_s.$$

It follows that

$$I = J \cdot (P_{t+1} \cdots P_s).$$

□

Proposition 4.27 *Suppose that J is a fractional ideal in F. Then there exist ideals $I, M \subset \mathcal{O}_F$, such that $J \cdot M = I$.*

PROOF: If J is a fractional ideal in F, then $I = J \cap \mathcal{O}_F$ is an ideal in $\mathcal{O}_F$. Applying the previous lemma to the inclusion $I \subset J$, we find that there exists an ideal M in $\mathcal{O}_F$ such that $J \cdot M = I$.

□

Theorem 4.28 *The set $\mathcal{I}(F)$ of fractional ideals in F forms a group under the operation $(I, J) \mapsto I \cdot J$. The identity element is furnished by $\mathcal{O}_F$, and the inverse is furnished by $I \mapsto I^{-1} = (\mathcal{O}_F \div I)$. This group is a free abelian group, generated by the set of nonzero prime ideals in $\mathcal{O}_F$.*

PROOF: The operation $I, J \mapsto I \cdot J$ is certainly commutative and associative, and $\mathcal{O}_F \cdot I = I$ for all fractional ideals I. Thus $\mathcal{I}(F)$ is a commutative monoid.[7] It remains to check that $I \cdot I^{-1} = \mathcal{O}_F$ for all fractional ideals I. If I is an ideal in $\mathcal{O}_F$, then $I = P_1 \cdots P_t$ for some prime ideals. I^{-1} is a fractional ideal which contains $\mathcal{O}_F$. It follows that there exists an ideal J in $\mathcal{O}_F$, such that $I^{-1} \cdot J = \mathcal{O}_F$. The ideal J has a factorization into prime ideals $J = Q_1 \cdots Q_s$. Since $I \cdot I^{-1} \subset \mathcal{O}_F$, we find that

$$I^{-1} \cdot P_1 \cdots P_t \subset I^{-1} \cdot Q_1 \cdots Q_s.$$

Multiplying through by J (which satisfies $JI^{-1} = \mathcal{O}_F$ we find that

$$P_1 \cdots P_t \subset Q_1 \cdots Q_s.$$

It follows that each prime $Q_1, \ldots, Q_s$ occurs among the primes $P_1, \ldots, P_t$. After reordering, if necessary, we find that

$$P_1 = Q_1, \ldots, P_s = Q_s.$$

[7] A **monoid** is an algebraic structure given by a set with a binary composition and identity element, satisfying all of the group axioms with the exception of the axiom of inverses.

Hence, we find that

$$I^{-1} = Q_1^{-1} \cdots Q_s^{-1} = P_1^{-1} \cdots P_s^{-1} \subset P_1^{-1} \cdots P_t^{-1} \subset I^{-1}$$

where the last inclusion follows from the fact that $I = P_1 \cdots P_t$. It follows by squeezing that

$$P_1^{-1} \cdots P_s^{-1} = P_1^{-1} \cdots P_t^{-1}.$$

Therefore,

$$P_{s+1} \cdots P_t = \mathcal{O}_F.$$

Hence $s = t$, $I^{-1} = P_1^{-1} \cdots P_t^{-1}$, and $I \cdot I^{-1} = \mathcal{O}_F$. We have proven that $\mathcal{I}(F)$ is an abelian group.

This group is certainly generated by the nonzero prime ideals in $\mathcal{O}_F$, since it is generated by the monoid of ideals in $\mathcal{O}_F$, each of which may be factored into prime ideals. If there was any relation among these prime ideals:

$$P_1^{e_1} \cdots P_s^{e_s} = \mathcal{O}_F,$$

for integers $e_1, \ldots, e_s$, then one may multiply both sides by powers of primes ideals in order to find such a relation in positive powers of the prime ideals P_i. No nontrivial relations among such powers exists, by the uniqueness of prime factorization for ideals in $\mathcal{O}_F$. Hence the group $\mathcal{I}(F)$ is a free abelian group generated by the nonzero prime ideals in $\mathcal{O}_F$.

□

Corollary 4.29 *The norm, $I \mapsto \mathrm{N}(I)$, initially defined for ideals in the maximal order $\mathcal{O}_F$, extends uniquely to an abelian group homomorphism from $\mathcal{I}(F)$ to $\mathbb{R}^\times_{pos}$ (the group of positive real numbers, under multiplication).*

Proof: For any ideal I in $\mathcal{O}_F$, we have seen that I has a prime factorization $I = P_1 \cdots P_t$, and $\mathrm{N}(I)$ equals $\prod \mathrm{N}(P_i)$. From the uniqueness of factorization, we find that if J is another ideal in $\mathcal{O}_F$, with factorization $J = Q_1 \cdots Q_s$, then

$$\mathrm{N}(IJ) = \mathrm{N}(P_1) \cdots \mathrm{N}(P_t)\,\mathrm{N}(Q_1) \cdots \mathrm{N}(Q_s) = \mathrm{N}(I)\,\mathrm{N}(J).$$

Since $\mathcal{I}(F)$ is generated by the ideals in $\mathcal{O}_F$, it follows that N extends uniquely to a group homomorphism from $\mathcal{I}(F)$ to $\mathbb{R}^\times_{pos}$.

□

According to this corollary, we may define the **norm of a fractional ideal** I, by expressing I as a quotient $I = (J \div K)$ of ideals in $\mathcal{O}_F$, and defining $\mathrm{N}(I) = \mathrm{N}(J)\,\mathrm{N}(K)^{-1}$. Alternatively, given a fractional ideal I, there exists an integer N such that $N \cdot I$ is an ideal in $\mathcal{O}_F$. It follows that

$$|\,\mathrm{N}(N)| \cdot \mathrm{N}(I) = \mathrm{N}(N \cdot I) = [\mathcal{O}_F : NI].$$

Proposition 4.30 *If J is a fractional ideal in F, then* $\mathrm{Disc}(J) = \mathrm{Disc}(F)\,\mathrm{N}(J)$.

Proof: We have seen this result, when J is an ideal in $\mathcal{O}_F$. When J is a fractional ideal, let N be a nonzero integer such that $N \cdot J$ is an ideal in $\mathcal{O}_F$. Then we find that

$$\mathrm{N}(N)\,\mathrm{Disc}(J) = \mathrm{Disc}(N \cdot J) = \mathrm{Disc}(F)\,\mathrm{N}(N \cdot J)\,\mathrm{Disc}(F)\,\mathrm{N}(N)\,\mathrm{N}(J),$$

from which the result follows.

□

4.5 *The class group*

Within the group $\mathcal{I}(F)$ of fractional ideals in F, a natural subgroup is provided by the set $\mathcal{P}(F)$ of principal ideals $\alpha\mathcal{O}_F$ for various $\alpha \in F^\times$. Two elements α and β of $F^\times$ generate the same principal ideal if and only if $\alpha\beta^{-1} \in \mathcal{O}_F^\times$. In this way, we may identify groups

$$\mathcal{P}(F) = F^\times/\mathcal{O}_F^\times.$$

As the multiplication on $F^\times$ is compatible with the multiplication of ideals, we find a subgroup embedded in $\mathcal{I}(F)$:

$$F^\times/\mathcal{O}_F^\times = \mathcal{P}(F) \hookrightarrow \mathcal{I}(F).$$

Definition 4.31 *The **ideal class group** of F, denoted $\mathcal{H}(F)$, is the quotient $\mathcal{H}(F) = \mathcal{I}(F)/\mathcal{P}(F)$. The **class number** of F, denoted $h(F)$ is the cardinality of the group $\mathcal{H}(F)$.*

The class group fits into a very important 4-term exact sequence of abelian groups:

$$1 \to \mathcal{O}_F^\times \to F^\times \to \mathcal{I}(F) \to \mathcal{H}(F) \to 1.$$

In particular, we find that $\mathcal{H}(F)$ is the trivial group if and only if $\mathcal{O}_F$ is a principal ideal domain.

Theorem 4.32 *The ideal class group of F is a finite abelian group. Furthermore, every ideal class in $\mathcal{H}(F)$ is represented by an ideal in $\mathcal{O}_F$, whose norm is bounded by*

$$\eta(n, r_2, \mathrm{Disc}(\mathcal{O}_F)) = \frac{n!}{n^n}\left(\frac{4}{\pi}\right)^{r_2}\sqrt{|\,\mathrm{Disc}(\mathcal{O}_F)|}.$$

Proof: Suppose that $J \in \mathcal{I}(F)$ is a fractional ideal, and consider the inverse J^{-1}. By the Minkowski estimates of the previous chapter, there exists a nonzero element α of the lattice J^{-1} such that

$$|\,\mathrm{N}(\alpha)| \le \frac{n!}{n^n}\left(\frac{4}{\pi}\right)^{r_2}\sqrt{|\,\mathrm{Disc}(J^{-1})|} = \frac{n!}{n^n}\left(\frac{4}{\pi}\right)^{r_2}\frac{\sqrt{|\,\mathrm{Disc}(\mathcal{O}_F)|}}{\mathrm{N}(J)}.$$

Above, we use the fact that $J \cdot J^{-1} = \mathcal{O}_F$, and so $\mathrm{N}(J^{-1}) = \mathrm{N}(J)^{-1}$, and thus

$$\mathrm{Disc}(J^{-1}) = \mathrm{Disc}(\mathcal{O}_F)\,\mathrm{N}(J^{-1}) = \mathrm{Disc}(\mathcal{O}_F)\,\mathrm{N}(J)^{-1}.$$

Since $\alpha \in J^{-1}$, $\alpha\mathcal{O}_F \subset J^{-1}$, and $I := (\alpha) \cdot J \subset \mathcal{O}_F$. Note that I and J are in the same class (in the ideal class group). We find that

$$\mathrm{N}(I) = |\,\mathrm{N}(\alpha)| \cdot \mathrm{N}(J) \leq \frac{n!}{n^n}\left(\frac{4}{\pi}\right)^{r_2}\sqrt{|\,\mathrm{Disc}(\mathcal{O}_F)|}.$$

It follows that every fractional ideal J is in the same ideal class as an ideal $I \subset \mathcal{O}_F$, whose norm is bounded by a constant only depending on the number field F (in fact, on n, $\mathrm{Disc}(F) = \mathrm{Disc}(\mathcal{O}_F)$, and r_2).

□

4.6 Exercises

Exercise 4.1 *Suppose that F is a number field, and $\mathcal{O}_F$ is its ring of integers. Let P be an ideal in $\mathcal{O}_F$. Prove that if $\mathrm{N}(P)$ is a prime number (a prime in $\mathbb{Z}$, that is), then P is a prime ideal.*

Exercise 4.2 *Let $F = \mathbb{Q}(\sqrt{-5})$. The ring $\mathcal{O}_F = \mathbb{Z}[\sqrt{-5}]$ is not a principal ideal domain; for example $6 = 2 \cdot 3 = (1+\sqrt{-5})(1-\sqrt{-5})$ is a non-unique factorization of 6 into irreducible elements.*

(a) Let $P = (2, 1+\sqrt{-5})$. Prove that P is a prime ideal.

(b) Factor the principal ideal (6) into prime ideals.

(c) Prove that $\mathcal{H}(F)$ is a group of order two.

(d) Suppose that p is a prime number (a prime in $\mathbb{Z}$, that is), then the principal ideal $p\mathcal{O}_F$ is either prime, or else factors as $P \cdot \bar{P}$, where P is a prime ideal in $\mathcal{O}_F$, and $\bar{P}$ is its Galois conjugate. Extra: prove that $P = \bar{P}$, in this case, if and only if $p = 2$ or $p = 5$ (i.e., p divides $\mathrm{Disc}(\mathcal{O}_F)$.

Exercise 4.3 *Prove that $h(\mathbb{Q}(\sqrt{13})) = 1$.*

Exercise 4.4 *Prove that $h(\mathbb{Q}(\sqrt{-19})) = 1$. Hint: use the fact that any ideal class can be represented by an ideal in $\mathcal{O}_F$ of norm 1 or 2. Prove that no prime ideal in $\mathcal{O}_F$ has norm 2, and use multiplicativity of the norm.*

Exercise 4.5 *Compute $h(F)$, where $F = \mathbb{Q}(\sqrt[3]{2})$.*

5
Units

In this chapter, F will always denote a number field, and $\mathcal{O}_F$ its ring of integers. Occasionally, we discuss an arbitrary order $\mathcal{O} \subset \mathcal{O}_F \subset F$. We have seen in the previous chapter that there is an exact sequence of abelian groups

$$1 \to \mathcal{O}_F^\times \to F^\times \to \mathcal{I}(F) \to \mathcal{H}(F) \to 1.$$

In addition, we have prove that the group $\mathcal{H}(F)$ is a finite abelian group. The subject of the current chapter is the group $\mathcal{O}_F^\times$, called the unit group of the number field F.

Even in simple cases, such as when F is a real quadratic field, understanding the group $\mathcal{O}_F^\times$ has significant Diophantine implications. We will completely describe the structure of the group $\mathcal{O}_F^\times$, as an abelian group, and discuss a related invariant called the regulator of F.

5.1 The norm, and quadratic fields

Recall that $\mathrm{N} = \mathrm{N}_{F/\mathbb{Q}} \colon F^\times \to \mathbb{Q}^\times$ is a group homomorphism; it can be computed in practice either by considering the "multiplication by α" endomorphisms of F (for $\alpha \in F^\times$), or by considering the product of the images of α, under all field embeddings $F \hookrightarrow \mathbb{C}$. Furthermore, we have seen that if $\alpha \in \mathcal{O}_F$, then $\mathrm{N}(\alpha) \in \mathbb{Z}$. A consequence is the following:

Proposition 5.1 *Suppose that $\alpha \in \mathcal{O}_F$. Then $\alpha \in \mathcal{O}_F^\times$ if and only if $\mathrm{N}(\alpha) = \pm 1$.*

Proof: First, suppose that $\alpha \in \mathcal{O}_F^\times$, so that $\alpha^{-1} \in \mathcal{O}_F$ as well. Then we find that

$$\mathrm{N}(\alpha)\,\mathrm{N}(\alpha^{-1}) = \mathrm{N}(\alpha\alpha^{-1}) = \mathrm{N}(1) = 1.$$

It follows that $\mathrm{N}(\alpha) \in \mathbb{Z}^\times = \{\pm 1\}$.

Conversely, suppose that $\alpha \in \mathcal{O}_F$ and $\mathrm{N}(\alpha) = \pm 1$. Recall that if $e = [F : \mathbb{Q}(\alpha)]$, then $\mathrm{N}(\alpha) = \mathrm{N}_{F/\mathbb{Q}}(\alpha) = \mathrm{N}_{\mathbb{Q}(\alpha)/\mathbb{Q}}(\alpha)^e$ and all of these quantities are in $\mathbb{Z}$. It follows that $\mathrm{N}_{\mathbb{Q}(\alpha)/\mathbb{Q}}(\alpha) = \pm 1$, since the only integer roots of ± 1 are ± 1.

Considering the minimal monic polynomial of α, we find that

$$\alpha^d - \mathrm{Tr}_{\mathbb{Q}(\alpha)/\mathbb{Q}}(\alpha)\alpha^{d-1} + \cdots \pm \mathrm{N}_{\mathbb{Q}(\alpha)/\mathbb{Q}}(\alpha) = 0.$$

We find an identity in $\mathcal{O}_F$:

$$\pm 1 = \alpha \cdot \left(\alpha^{d-1} - \mathrm{Tr}_{\mathbb{Q}(\alpha)/\mathbb{Q}}(\alpha)\alpha^{d-2} + \cdots\right).$$

It follows that $\alpha \in \mathcal{O}_F^\times$ (and we have in fact found a formula for α^{-1}).

□

Example 5.2 *Suppose that $F = \mathbb{Q}(\sqrt{D})$ is a quadratic field, with D a square-free integer. If $\alpha = a + b\sqrt{D} \in F$, then $\mathrm{N}(\alpha) = \alpha\bar{\alpha}$, where $\bar{\alpha} = a - b\sqrt{D}$ is the Galois conjugate of α. Thus we find that*

$$\mathrm{N}(\alpha) = (a + b\sqrt{D})(a - b\sqrt{D}) = a^2 - Db^2.$$

If α is in $\mathcal{O}_F$, then we find that $\alpha \in \mathcal{O}_F^\times$ if and only if

$$a^2 - Db^2 = \pm 1.$$

Recall that, depending on whether D is congruent to 1, or to 2 or 3, modulo 4, there are two possibilities for $\mathcal{O}_F$.

*$D \equiv 1$, **mod** 4: In this case, $\mathcal{O}_F = \mathbb{Z}[1/2(1 + \sqrt{D})]$. Thus $\alpha \in \mathcal{O}_F$ if and only if*

$$\alpha = \frac{a}{2} + \frac{b}{2}\sqrt{D}, \text{ and } a, b \in \mathbb{Z} \text{ and } a - b \text{ is even}.$$

We find that the units $\mathcal{O}_F^\times$ correspond precisely to pairs of integers $(a, b) \in \mathbb{Z}^2$ such that $a^2 - Db^2 = \pm 4$ (note that this condition implies that $a - b$ is even, since D is congruent to 1 modulo 4).

*$D \equiv 2, 3$, **mod** 4: In this case, $\mathcal{O}_F = \mathbb{Z}[\sqrt{D}]$ Thus $\alpha \in \mathcal{O}_F$ if and only if $\alpha = a + b\sqrt{D}$ for some integers a, b. Thus the units of $\mathcal{O}_F$ correspond precisely to pairs of integers $(a, b) \in \mathbb{Z}^2$ such that $a^2 - Db^2 = \pm 1$.*

In particular, when D is a square-free positive integer, we find that a complete understanding of $\mathcal{O}_F^\times$ is equivalent to a complete solution of "Pell's equation"[1]

One particular case can be analyzed now by explicit methods.

Proposition 5.3 *Suppose that $F = \mathbb{Q}(\sqrt{-D})$ is a quadratic field, where D is a* positive *square-free integer (the case $r_1 = 0, r_2 = 1$).*[2] *Then $\mathcal{O}_F^\times$ is a finite cyclic group, whose order is 4 or 6 or 2, corresponding to the cases when $D = -1$, $D = -3$, and all other cases, respectively.*

[1] Euler is responsible for naming such Diophantine equations after Pell, and historians (reference needed!) have suggested that Euler confused Brouncker and Pell in this attribution. In any case, there was great progress on Pell's equation by Brahmagupta around 630 A.D., and later by Bhaskara II around 1150 A.D..

[2] We say that F is an **imaginary quadratic field** in this case

PROOF: Observe that the norm is a positive-definite quadratic form in this case: $\mathrm{N}(a + b\sqrt{-D}) = a^2 + Db^2$. In particular the equation $\mathrm{N}(\alpha) = \pm 1$ implies $\mathrm{N}(\alpha) = 1$. We consider two cases now.

$-D \equiv 1$**, mod** 4**:** In this case, recall that the units correspond to integer solutions of $a^2 + Db^2 = 4$. If $-D = -3$, then we seek solutions to $a^2 + 3b^2 = 4$. There are precisely six solutions:

$$a = \pm 1, b = \pm 1, \text{ and } a = \pm 2, b = 0.$$

If $-D \leq -7$, then there are only two integer solutions to $a^2 + Db^2 = 4$: $a = \pm 1, b = 0$. We have found that when $-D = -3$, $\mathcal{O}_F^\times$ is a cyclic group, consisting of all sixth roots of unity. When $-D \leq -7$, $\mathcal{O}_F^\times = \{\pm 1\}$ is a cyclic group of order two.

$-D \equiv 2, 3$**, mod** 4**:** In this case, recall that the units correspond to integer solutions of $a^2 + Db^2 = 1$. If $-D = -1$, then we seek integer solutions to $a^2 + b^2 = 1$. There are precisely four solutions:

$$a = \pm 1, b = \pm 1.$$

If $-D < -1$, then we seek integer solutions to $a^2 + Db^2 = 1$, and there are only two solutions:

$$a = \pm 1, b = 0.$$

We have found that when $-D = -1$, $\mathcal{O}_F^\times$ is a cyclic group, consisting of all fourth roots of unity. When $-D \leq -1$, $\mathcal{O}_F^\times = \{\pm 1\}$ is a cyclic group of order two.

□

5.2 *Geometry of units*

We have seen that understanding the units $\mathcal{O}_F^\times$ in a number field is equivalent to finding all solutions to $\mathbb{N}(\alpha) = \pm 1$ in $\mathcal{O}_F$; if $n = [F : \mathbb{Q}]$, then every element of $\mathcal{O}_F$ can be expressed as a $\mathbb{Z}$-linear combination $\alpha = a_1 v_1 + \cdots + a_n v_n$ of a $\mathbb{Z}$-basis of $\mathcal{O}_F$. The condition $\mathbb{N}(\alpha) = \pm 1$ can be rephrased as a Diophantine equation in the integer variables $a_1, \ldots, a_n$; however, the degree of this Diophantine equation is n – solving general Diophantine equations of degree n in n variables is intractable.

However, the specific Diophantine equations involved in finding $\mathcal{O}_F^\times$ are tractable, largely because the solution set $\mathcal{O}_F^\times$ is a group. We will prove that $\mathcal{O}_F^\times$ is a finitely-generated group, and thus every unit can be expressed as a product involving a finite number of "fundamental units" (generators).

Recall that a **real place** of F is a field embedding $F \hookrightarrow \mathbb{R}$, and a **complex place** of F is a conjugate pair of field embeddings $F \hookrightarrow \mathbb{C}$. We define $V_{\mathbb{R}}$ to be the set of real places and $V_{\mathbb{C}}$ to be the set of complex places of F. We write V_{arc} for the resulting set of **archimedean places**, called **infinite places** by many authors:

$$V_{\text{arc}} = V_{\mathbb{R}} \sqcup V_{\mathbb{C}}, \text{ satisfying } \#V_{arc} = r_1 + r_2.$$

To each archimedean place of F, we associate an "absolute value"; if $v \in V_{\mathbb{R}}$, and $\alpha \in F$, we define $|\alpha|_v = |v(\alpha)|$, where the latter denotes the usual real absolute value. For a complex place w, we use the square of the usual complex absolute value:

$$|\alpha|_w = |w(\alpha)|^2 = w(\alpha)\overline{w(\alpha)}.$$

The absolute value of the norm $\mathrm{N}_{F/\mathbb{Q}}(\alpha)$ can now be expressed using absolute values:

$$|\mathrm{N}(\alpha)| = \prod_{v \in V_{\text{arc}}} |\alpha|_v.$$

Thus, we can study the units $\mathcal{O}_F$ using the following characterization:

$$\mathcal{O}_F^\times = \{\alpha \in \mathcal{O}_F \colon \prod_{v \in V_{\text{arc}}} |\alpha|_v = 1\}.$$

While this characterization is highly nonlinear, we may linearize via the "logarithmic modulus" map; let $\mathbb{R}_{pos}^\times$ denote the group of positive real numbers, under multiplication. Then the natural logarithm provides a continuous group isomorphism

$$\log \colon \mathbb{R}_{pos}^\times \to \mathbb{R}.$$

Recall that there is a unique, up to reordering and conjugation, algebra isomorphism

$$F_{\mathbb{R}} \cong \mathbb{R}^{r_1} \times \mathbb{C}^{r_2}.$$

The logarithm, composed with the absolute value, yields the **logarithmic modulus** homomorphism:

$$\lambda \colon F_{\mathbb{R}}^\times = (\mathbb{R}^\times)^{r_1} \times (\mathbb{C}^\times)^{r_2} \to \mathbb{R}^{r_1+r_2},$$

$$\lambda(x_1, \ldots, x_{r_1}, z_1, \ldots, z_{r_2}) = (\log|x_1|, \ldots, \log|x_{r_1}|, 2\log|z_1|, \ldots, 2\log|z_{r_2}|).$$

The coefficient 2, at each complex place, arises since $\log|z^2| = 2\log|z|$, and we use the square of the usual complex absolute value. In particular, the logarithmic modulus on elements $\alpha \in F$ can be computed:

$$\lambda(\alpha) = (\log|\alpha|_v)_{v \in V_{\text{arc}}}.$$

Let $H \subset \mathbb{R}^{r_1+r_2}$ be the hyperplane (subspace of codimension 1), cut out by the condition:

$$H = \{(t_1, \ldots, t_{r_1+r_2}) \colon \sum_{i=1}^{r_1+r_2} t_i = 0\}.$$

Thus H is a real vector space of dimension $r_1 + r_2 - 1$.

Proposition 5.4 *The group $\mathcal{O}_F^\times$, viewed as a subset of the real vector space $F_\mathbb{R}$, can be identified as the intersection of the lattice $\mathcal{O}_F$ with the set $\lambda^{-1}(H)$. In other words,*

$$\mathcal{O}_F^\times = \{\alpha \in \mathcal{O}_F \colon \lambda(\alpha) \in H\}.$$

PROOF: Given that $\alpha \in \mathcal{O}_F$, we find that $\alpha \in \mathcal{O}_F^\times$ if and only if $\mathrm{N}(\alpha) = \pm 1$. This occurs if and only if $|\mathrm{N}(\alpha)| = 1$. This occurs if and only if

$$\prod_{v \in V_{arc}} |\alpha|_v = 1.$$

Applying the logarithm to both sides, we see that this occurs if and only if

$$\sum_{v \in V_{arc}} \log |\alpha|_v = 0.$$

This is equivalent to the condition that $\lambda(\alpha) \in H$.

□

Geometrically, the condition $\lambda(\alpha) \in H$ may describe a somewhat complicated region in the real vector space $F_\mathbb{R}$. When F is an imaginary quadratic field, this describes the unit circle in $\mathbb{C}$. But when F is a real quadratic field, the condition $\lambda(\alpha) \in H$ describes a union of two hyperbolas.

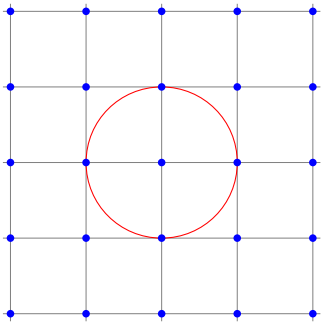

Figure 5.1: The lattice $\mathcal{O}_F$ in blue dots, and the curve $\lambda(\alpha) \in H$ in red. Here $F = \mathbb{Q}(\sqrt{-1})$.

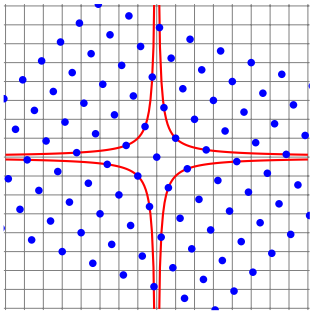

Figure 5.2: The lattice $\mathcal{O}_F$ in blue dots, and the curve $\lambda(\alpha) \in H$ in red. Here $F = \mathbb{Q}(\sqrt{5})$

5.3 *Torsion units*

Lemma 5.5 *The function $\lambda \colon F_\mathbb{R}^\times \to \mathbb{R}^{r_1+r_2}$ is "proper"; in other words, for every element $(t_1, \ldots, t_{r_1+r_2}) \in \mathbb{R}^{r_1+r_2}$, the preimage $\lambda^{-1}(t_1, \ldots, t_{r_1+r_2})$ is a compact subset of $F_\mathbb{R}^\times$.*

PROOF: Since λ is a homomorphism, it suffices to prove that $\lambda^{-1}(0, \ldots, 0)$ is compact. This preimage can be described as a direct product:

$$\lambda^{-1}(0, \cdots, 0) = \left(\prod_{i=1}^{r_1} \{\pm 1\}\right) \times \left(\prod_{j=1}^{r_2} \{z \in \mathbb{C} \colon |z| = 1\}\right).$$

As the finite product of compact spaces, this is compact.

□

For any field K, we write $\mu(K)$ for the torsion subgroup of $K^\times$. When F is a number field, $\mu(F) \subset \mathcal{O}_F^\times$, since every torsion element of $K^\times$ is a root of a monic polynomial of the form $X^n - 1$ for some $n \geq 1$.

We will study the group $\mathcal{O}_F^\times$ of units by studying its image $\Lambda = \lambda(\mathcal{O}_F^\times)$, which satisfies

$$\Lambda \subset H \subset \mathbb{R}^{r_1+r_2}.$$

Proposition 5.6 *There is a short exact sequence*

$$1 \to \mu(F) \to \mathcal{O}_F^\times \to \Lambda \to 1,$$

The group $\mu(F)$ is finite.

PROOF: The map $\mathcal{O}_F^\times \to \Lambda$ is surjective, by definition, since $\Lambda = \lambda(\mathcal{O}_F^\times)$. Its kernel consists of all units ϵ satisfying $\lambda(\epsilon) = (0, \ldots, 0)$. Such units lie in the intersection of a compact set (the set $\lambda^{-1}(0, \ldots, 0)$) and a discrete set (the set $\mathcal{O}_F$ of integers in F) in the vector space $F_{\mathbb{R}}$. As such, the kernel is a finite subgroup of $\mathcal{O}_F^\times$. As such, every element of the kernel is a torsion element of $\mathcal{O}_F^\times$, i.e., a root of unity.

Conversely, if ζ is a root of unity in F, then $\zeta^n = 1$ for some positive integer n. It follows that ζ is integral, a unit, and the image of ζ is a root of unity in any embedding of F in $\mathbb{C}$. It follows that $|\zeta|_v = 1$ for all $v \in V_{\text{arc}}$. Thus ζ is in the kernel of $\mathcal{O}_F^\times \to \Lambda$.

□

We write $w = w(F) = \#\mu(F)$ for the number of roots of unity in a number field F. If $r_1 > 0$, then we immediately find that $w = 2$ since $\mathbb{R}$ only has two roots of unity. In general, we find the following

Proposition 5.7 *If F is a number field, then $\mu(F)$ is a finite cyclic group.*[3]

[3] In fact, if F is any field, and C is a finite subgroup of $F^\times$, then C is cyclic. This is proven, for example, in J. P. Serre's "A Course in Arithmetic".

PROOF: Consider any embedding $F \hookrightarrow \mathbb{C}$. This embedding induces an isomorphism from $\mathcal{W}(F)$ to a finite subgroup of the group $\mu(\mathbb{C})$ of complex roots of unity. Thus it suffices to prove that every finite group of complex roots of unity is cyclic.

Let $\mathbf{e}\colon \mathbb{Q} \to \mu(\mathbb{C})$ denote the group homomorphism given by

$$\mathbf{e}(q) = e^{2\pi i q}.$$

Then $\mathbf{e}$ yields a short exact sequence

$$0 \to \mathbb{Z} \to \mathbb{Q} \to \mu(\mathbb{C}) \to 0.$$

In this way, every[4] finite subgroup of $\mathbb{C}^\times_{tor}$ is the image of a finitely-generated subgroup of $\mathbb{Q}$ containing $\mathbb{Z}$. Every finitely-generated

[4] To see that every complex root of unity occurs in the image of $\mathbf{e}$, one may observe that $\mathbf{e}(j/n)$ produces n distinct n^{th} roots of unity, as $1 \leq j \leq n$. Thus the homomorphism $\mathbf{e}$ contains all n^{th} roots of unity, for all positive integers n.

subgroup of $\mathbb{Q}$ is a $\mathbb{Z}$-lattice in $\mathbb{Q}$, hence isomorphic to $\mathbb{Z}$; in other words, every finitely-generated subgroup of $\mathbb{Q}$ is cyclic. Hence every finite subgroup of $\mu(\mathbb{C})$ is the image of a cyclic group, and hence is cyclic.

□

5.4 *The unit theorem*

We have found that the unit group $\mathcal{O}_F^\times$ fits into a short exact sequence

$$1 \to \mu(F) \to \mathcal{O}_F^\times \to \Lambda \to 1,$$

where $\mu(F) = (\mathcal{O}_F^\times)_{tor}$ is a finite cyclic group. In this section, we prove the unit theorem, which describes the quotient Λ, which is a subgroup of the real vector space $H \subset \mathbb{R}^{r_1+r_2}$.

The discreteness of $\mathcal{O}_F$ in $F_\mathbb{R}$ immediately yields an "upper bound" for Λ, using the following geometric lemma:

Lemma 5.8 *Suppose that L is a discrete subgroup of a finite-dimensional real vector space V, with $dim(V) = d$. Then L is isomorphic, as a group, to $\mathbb{Z}^e$ for some integer $e \leq d$.*

Proof: As a subgroup of a torsion-free group, we know that L is torsion-free. Let $U = \text{span}_\mathbb{R}(L)$ denote the span of L; thus Λ is a discrete subgroup spanning the real vector space U, with $dim_\mathbb{R}(U) = e \leq d$. Since L spans U, there exists a basis $\{v_1, \ldots, v_e\}$ of U such that $v_1, \ldots, v_e \in L$.

Let D be a fundamental parallelotope given by this basis, and $\bar{D}$ its closure. Let $L_0 \subset L$ denote the $\mathbb{Z}$-span of $\{v_1, \ldots, v_d\}$. Since L is discrete in V, and $\bar{D}$ is compact, the intersection $L \cap \bar{D}$ is finite. Since every element of L can be translated, via L_0, to an element of $\bar{D}$, we find that L is generated by L_0 together with $L \cap \bar{D}$.

Hence L is a finitely-generated torsion-free abelian group; L is isomorphic to $\mathbb{Z}^f$ for some integer f, and $f \geq e$ since L spans the real vector space U of dimension e. Let $u_1, \ldots, u_f$ denote a $\mathbb{Z}$-basis of L. After reordering, we may assume that $u_1, \ldots, u_e$ is a maximal $\mathbb{R}$-linearly independent subset of this $\mathbb{Z}$-basis, and let L' denote the $\mathbb{Z}$-span of $\{u_1, \ldots, u_e\}$. In particular, U/L' is a compact Hausdorff space. If $f > e$, then observe that the set $\mathbb{Z}u_f$ projects onto an infinite subset of U/L' since the set $\{u_1, \ldots, u_f\}$ is $\mathbb{Z}$-linearly independent.

Hence the projection of $\mathbb{Z} \cdot u_f$ onto U/L' has an accumulation point. Lifting the projection $\mathbb{Z}u_f$ to the fundamental parallelotope for L' in U, we find an accumulation point in the lattice L, contradicting discreteness.

Hence $f = e$, and so L is isomorphic to $\mathbb{Z}^e$.

□

Proposition 5.9 *The group Λ is a discrete subgroup of $H \cong \mathbb{R}^{r_1+r_2-1}$. It follows that Λ is a free abelian group of rank bounded by $r_1 + r_2 - 1$.*

PROOF: We find that Λ is discrete in H, since $\mathcal{O}_F^\times$ is discrete in $F_{\mathbb{R}}^\times$, and the logarithmic modulus map $\lambda\colon F_{\mathbb{R}}^\times \to \mathbb{R}^{r_1+r_2}$ is proper.

As a discrete subgroup of $H \cong \mathbb{R}^{r_1+r_2-1}$, we find that $\Lambda \cong \mathbb{Z}^e$ for some $e \leq r_1 + r_2 - 1$.

□

Since H has dimension $r_1 + r_2 - 1$, Λ is trivial in two basic cases; if $r_1 = 1$ and $r_2 = 0$, then $F = \mathbb{Q}$, and $\mathcal{O}_F^\times\{\pm 1\}$, and $\Lambda = \{0\}$. If $r_1 = 0$ and $r_2 = 1$, then F is a quadratic imaginary field, $\mathcal{O}_F^\times = \mathcal{W}(F)$ is a cyclic group of order 2, 4, or 6, and again $\Lambda = \{0\}$. Therefore, it suffices to consider the cases when $r_1 + r_2 \geq 2$.

We will soon prove a much more difficult result, that Λ is a lattice in H, i.e., that Λ is isomorphic to $\mathbb{Z}^{r_1+r_2-1}$, embedded discretely in H. Our approach is based on that of Anthony Knapp[5], beginning with the following:

[5] Anthony W. Knapp. *Advanced algebra*. Cornerstones. Birkhäuser Boston Inc., Boston, MA, 2007. ISBN 978-0-8176-4522-9

Proposition 5.10 *Fix an archimedean place $w \in V_{\text{arc}}$. There exists an infinite sequence $\alpha^{(1)}, \alpha^{(2)}, \ldots$ in $\mathcal{O}_F$, satisfying the following three properties:*

1. $|\mathrm{N}(\alpha^{(i)})| \leq 2^n Vol(F_{\mathbb{R}}/\mathcal{O}_F)$ *for all i.*
2. *For every archimedean place $v \neq w$,*
$$\lim_{i\to\infty} |\alpha^{(i)}|_v = 0.$$
3. *At the archimedean place w,*
$$\lim_{i\to\infty} |\alpha^{(i)}|_w = \infty.$$

PROOF: In order to construct such elements of $\mathcal{O}_F$, we use our results on existence of lattice points within compact convex centrally symmetric regions of sufficient volume. First, for all $i \geq 1$, we define a compact convex centrally symmetric subset $\Omega_j \subset F_{\mathbb{R}}$. Note that each absolute value $|\cdot|_v$ (for $v \in V_{\text{arc}}$) defines a **gauge** on $F_{\mathbb{R}}$; in particular, for all $v \in V_{\text{arc}}$, and all positive real numbers ρ, the following is a closed, convex, centrally symmetric subset of $F_{\mathbb{R}}$:

$$D_v(\rho) = \{\alpha \in F_{\mathbb{R}} \colon |\alpha|_v \leq \rho\}.$$

Furthermore, if one is given a positive real number ρ_v for each archimedean place v, then

$$D(\vec{\rho}) = \bigcap_{v\in V_{\text{arc}}} D_v(\rho_v)$$

is a compact, convex, centrally symmetric subset of $F_{\mathbb{R}}$. It is a product of intervals and discs, centered at the origin.

Define, for all $i \geq 1$, a collection $\vec{\rho}^{(i)}$ of radii, by:

1. $\rho_v^{(i)} i^{-1}$, for all archimedean places $v \neq w$.
2. If w is real, then $\rho_w^{(i)} = 2^{n-r_1}\pi^{-r_2} i^{n-1} Vol(F_{\mathbb{R}}/\mathcal{O}_F)$.
3. If w is complex, then $\rho_w^{(i)} = \sqrt{2^{n-r_1}\pi^{-r_2} i^{n-2} Vol(F_{\mathbb{R}}/\mathcal{O}_F)}$.

In this way, we get a sequence of compact, convex, centrally symmetric subsets $D(\vec{\rho}^{(i)})$; the volume of each may be computed directly, and

$$\mathrm{Vol}(D(\vec{\rho}^{(i)})) = 2^n Vol(F_{\mathbb{R}}/\mathcal{O}_F).$$

Thus, we find that there exists a sequence of nonzero lattice points $\alpha^{(i)}$, such that

$$\alpha^{(i)} \in D(\vec{\rho}^{(i)}) \cap \mathcal{O}_F.$$

For all $i \geq 1$, we find that

$$|\,\mathrm{N}(\alpha^{(i)})| = \prod_{v \in V_{\mathrm{arc}}} |\alpha^{(i)}|_v \leq 2^n Vol(F_{\mathbb{R}}/\mathcal{O}_F) 2^{-r_1} 2^{-r_2} \leq 2^n Vol(F_{\mathbb{R}}/\mathcal{O}_F).$$

We find directly that, for all place $v \neq w$, $|\alpha^{(i)}|_v \leq i^{-1}$ approaches zero as i approaches infinity. The boundedness of the product

$$|\,\mathrm{N}(\alpha^{(i)})| = \prod_{v \in V_{\mathrm{arc}}} |\alpha^{(i)}|_v,$$

and the decay of all but one term in the product, implies the growth of the single term $|\alpha^{(i)}|_w$.

□

Proposition 5.11 *Fix an archimedean place $w \in V_{\mathrm{arc}}$. Then, there exists a sequence $\epsilon^{(i)}$ of units such that*

1. *For all places $v \neq w$,*
$$\lim_{i \to \infty} |\epsilon^{(i)}|_v = 0.$$
2. *At the place w,*
$$\lim_{i \to \infty} |\epsilon^{(i)}|_w = \infty.$$

Let $\alpha^{(i)}$ be a sequence of elements of $\mathcal{O}_F$, constructed to satisfy the conditions of the previous proposition. Thus, the sequence $|\,\mathrm{N}(\alpha^{(i)})|$ is a bounded sequence of integers. By restricting to a subsequence, we may assume that $\mathrm{N}(\alpha^{(i)})$ is a constant integer, M. Furthermore, since $\mathcal{O}_F/M\mathcal{O}_F$ is a finite set, we may restrict further to a subsequence on which $\alpha^{(i)}$ lies in a single residue class modulo $M\mathcal{O}_F$.

Define now $\epsilon^{(i)} = \alpha^{(i)}/\alpha^{(1)}$. Since $\alpha^{(i)}$ and $\alpha^{(1)}$ are nonzero elements of $\mathcal{O}_F$, of the same norm, we find that $\epsilon^{(i)}$ is an element of $F^\times$ of norm 1. Since $\alpha^{(i)}$ and $\alpha^{(1)}$ are in the same residue class, modulo $M\mathcal{O}_F$, we find that

$$(\alpha^{(i)} - \alpha^{(1)}) \in M\mathcal{O}_F.$$

Since $M = \mathrm{N}_{F/\mathbb{Q}}(\alpha^{(1)})$, we find by a now familiar argument that

$$M \in \alpha^{(1)}\mathcal{O}_F.$$

Putting these observations together, we find that

$$(\alpha^{(i)} - \alpha^{(1)}) \in \alpha^{(1)}\mathcal{O}_F.$$

We deduce that

$$\epsilon^{(i)} = 1 + \frac{\alpha^{(i)} - \alpha^{(1)}}{\alpha^{(1)}} \in \mathcal{O}_F.$$

We have found that $\epsilon^{(i)} \in \mathcal{O}_F$ and $|\mathrm{N}(\epsilon^{(i)})| = 1$, so $\epsilon^{(i)} \in \mathcal{O}_F^\times$.

The decay of $|\epsilon^{(i)}|_v$ (for $v \neq w$), and the growth of $|\epsilon^{(i)}|_w$ now follow from the corresponding conditions on $\alpha^{(i)}$.

□

We have found, for every archimedean place w, a sequence of units $\epsilon_w^{(i)}$; by choosing i sufficiently large, we find units ϵ_w for all places w, satisfying the following identities:

1. For all archimedean places $v \neq w$, $\log |\epsilon_w|_v < 0$.
2. At the place w, $\log |\epsilon_w|_w > 0$.
3. Since ϵ_w is a unit,
$$\sum_{v \in V_{\mathrm{arc}}} \log |\epsilon_w|_v = 0.$$

Proposition 5.12 *Fix an archimedean place w. Define for all $u, v \in V_{\mathrm{arc}}$, with $u \neq w$, $v \neq w$,*

$$\lambda_{u,v} = \log |\epsilon_u|_v.$$

Then the matrix $(\lambda_{u,v})$ is a nonsingular square matrix with $r_1 + r_2 - 1$ rows and columns.

Proof: We find that the diagonal entries of this matrix are positive, and the off-diagonal entries of this matrix are negative. Moreover, within each row, we find that

$$\sum_{v \neq u} |\lambda_{u,v}| < \lambda_{u,u}.$$

Roughly speaking, the entries of the matrix are "concentrated" on the diagonal. To prove invertibility, suppose to the contrary that there

was a linear relation among the rows; suppose that there exist real numbers c_v, not all zero, such that

$$\sum_v \lambda_{u,v} c_v = 0, \text{ for all } u.$$

Let u be a place at which $|c_u|$ is maximal. Then we find that

$$\begin{aligned} |c_u \lambda_{u,u}| &= |c_u| \lambda_{u,u} \\ &> |c_v| \sum_{v \neq u} |\lambda_{u,v}| \\ &\geq |c_v| \cdot |\sum_{v \neq u} \lambda_{u,v}| \\ &= \sum_{v \neq u} |c_v \lambda_{u,v}| \\ &\geq |\sum_{v \neq u} c_v \lambda_{u,v}|. \end{aligned}$$

But the strictness of this inequality contradicts the assumption that

$$\sum_{v \in V_{\text{arc}}} \lambda_{u,v} c_v = 0.$$

Hence the matrix $(\lambda_{u,v})$ is non-singular.

□

Finally, we have proven

Theorem 5.13 (Dirichlet unit theorem) *The discrete subgroup $\Lambda \subset H \subset \mathbb{R}^{r_1+r_2}$ is a lattice in the real vector space H of dimension $r_1 + r_2 - 1$.*

Proof: We have seen already that Λ is a discrete subgroup of $H \cong \mathbb{R}^{r_1+r_2-1}$. Thus, it only remains to prove that Λ is a "full-rank" subgroup, i.e., $\Lambda \cong \mathbb{Z}^{r_1+r_2-1}$. Let $\Lambda' \subset \Lambda$ be the subgroup generated by the logarithmic modulus of the units ϵ_v for all $v \neq w$, discussed in the previous proposition. The matrix $(\lambda_{u,v})$ describes precisely the projection of $\Lambda' \subset \mathbb{R}^{r_1+r_2}$ onto a coordinate hyperplane corresponding to all archimedean places but one. The nonsingularity of the matrix $(\lambda_{u,v})$ implies that Λ' is a full rank lattice in $\mathbb{R}^{r_1+r_2-1}$. Since Λ contains Λ', we find that the rank of Λ is at least $r_1 + r_2 - 1$. Since earlier results imply that the rank of Λ is at most $r_1 + r_2 - 1$, we have precisely determined the rank of Λ.

□

From Dirichlet's unit theorem, we find that there exists a system of **fundamental units** $\epsilon_1, \ldots, \epsilon_{r_1+r_2-1}$, such that every element ϵ of $\mathcal{O}_F^\times$ has a unique expression of the form:

$$\epsilon = \zeta \cdot \epsilon_1^{e_1} \cdots \epsilon_{r_1+r_2-1}^{e_{r_1+r_2-1}},$$

for a root of unity ζ. Observe that there is not a canonical splitting of the short exact sequence

$$1 \to \mathcal{W}(F) \to \mathcal{O}_F^\times \to \Lambda \to 1,$$

but giving such a system of fundamental units yields such a splitting (as well as an ordered $\mathbb{Z}$-basis of Λ).

We finish with a definition, which follows from the Dirichlet unit theorem. We have seen that Λ is a lattice in the real vector space $H \subset \mathbb{R}^{r_1+r_2-1}$. As H is a hyperplane in the real vector space $\mathbb{R}^{r_1+r_2}$, and the latter has a natural basis (up to reordering), H is endowed with a canonical measure. The regulator of F is the volume $Vol(H/\Lambda)$, divided by $\sqrt{r_1+r_2}$; this can be explicitly computed by the following, which we take as our working definition:

Definition 5.14 *Let $\epsilon_1, \ldots, \epsilon_{r_1+r_2-1}$ be a system of fundamental units for the number field F. Choose an archimedean place w. Then, the **regulator** of F is defined to be the absolute value of the determinant of the $r_1 + r_2 - 1$ by $r_1 + r_2 - 1$ square matrix $(\lambda_{i,v})$, where*

$$\lambda_{i,v} = \log |\epsilon_i|_v, \text{ for all } v \neq w.$$

On the surface, it seems that the regulator depends on the choice of a system of fundamental units, as well as the choice of an archimedean place w. It is not difficult to see that changing a system of fundamental units corresponds to multiplying the matrix $(\lambda_{i,v})$ by an invertible integer matrix, which has determinant ± 1. Thus the choice of system of fundamental units does not affect the regulator.

On the other hand, it is not as clear that the choice of archimedean place does not affect the regulator. But this follows from a result in linear algebra:

Proposition 5.15 *Suppose that (m_{ij}) is a t by $t+1$ matrix of real numbers, for some positive integer t. Suppose that every row sum equals zero:*

$$\sum_{j=1}^{t+1} m_{ij} = 0, \text{ for all } 1 \leq i \leq t.$$

For all $1 \leq j \leq t+1$, let M_j denote the matrix obtained by deleting the j^{th} column of (m_{ij}). Then the absolute value of the determinant $|\mathrm{Det}(M_j)|$ is independent of j.

Since the sums $\sum_v \log |\epsilon|_v$ equal zero, for any unit ϵ, the previous proposition implies that the regulator is well-defined, regardless of the choice of a specific "fixed archimedean place".

5.5 Concluding remarks

At this point, we have seen a number of "invariants" of a number field F; these are numbers which we can associate in a natural way to

a number field. These invariants occur together in the Dirichlet class number formula; like Euler's formula $e^{i\pi} + 1 = 0$, the Dirichlet class number formula unites these disparate invariants in a surprisingly clean way, relating them to the residue of the Dedekind zeta function.

The **Riemann zeta function** refers to the function

$$\zeta(s) = \sum_{n=1}^{\infty} n^{-s} = \prod_{p} (1 - p^{-s})^{-1},$$

which converges (both the sum and the "Euler product" converge and are equal) when $\Re(s) > 1$. The function $\zeta(s)$ is holomorphic in the open subset of $\mathbb{C}$ given by $\Re(s) > 1$; moreover, there is a unique meromorphic extension of $\zeta(s)$ to the complex plane, whose only pole is a simple pole at $s = 1$.

The Riemann zeta function generalizes to the **Dedekind zeta function**, associated to a number field F. It is also defined by a Dirichlet series:

$$\zeta_F(s) = \sum_{I \subset \mathcal{O}_F} \mathrm{N}(I)^{-s} = \prod_{P \subset \mathcal{O}_F} (1 - \mathrm{N}(P)^{-s})^{-1},$$

where the sum ranges over all nonzero ideals I of $\mathcal{O}_F$ and the product over all nonzero prime ideals P of $\mathcal{O}_F$. Once again, it can be proven that $\zeta_F(s)$, while initially defined and holomorphic in a right half-plane, extends uniquely to a meromorphic function in the complex plane, whose only pole is a simple pole at $s = 1$.

We have now defined all of the terms occurring in the following

Theorem 5.16 (Class number formula) *The Dedekind zeta function $\zeta_F(s)$ has meromorphic continuation to the complex plane. At $s = 1$, ζ_F has a simple pole and*

$$\lim_{s \to 1} (s - 1)\zeta_F(s) = \frac{2^{r_1}(2\pi)^{r_2} h(F) \mathcal{R}(F)}{w(F)\sqrt{|\operatorname{Disc}(F)|}}.$$

This formula brings together all of the invariants of a number field that we have encountered. To recall these invariants we have:

Discriminant $\operatorname{Disc}(F) = \operatorname{Disc}(\mathcal{O}_F)$ arises from viewing $\mathcal{O}_F$ as a $\mathbb{Z}$-lattice in the $\mathbb{Q}$-vector space F, which is endowed with a nondegenerate symmetric bilinear form given by the trace pairing.

Places r_1 is the number of real places, and r_2 is the number of complex places. These arise naturally, in that $F_{\mathbb{R}} \cong \mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$ as a $\mathbb{R}$-algebra.

Class number $h(F)$ is the class number of F, i.e., the cardinality of the finite group $\mathcal{H}(F) = \mathcal{I}(F)/\mathcal{P}(F)$. It measures the extent to which $\mathcal{O}_F$ might fail to be a principal ideal domain.

Roots of unity $w(F)$ is the cardinality of the finite group $\mathcal{W}(F) = (\mathcal{O}_F^\times)_{tor}$ of roots of unity in F.

Regulator $\mathcal{R}(F)$ is the regulator of F, given as the covolume of the lattice $\Lambda \cong \mathcal{O}_F^\times / \mathcal{W}(F)$ in the real vector space $H \cong \mathbb{R}^{r_1+r_2-1}$.

Zeta function The Dedekind zeta function $\zeta_F(s)$ is defined above.

5.6 Exercises

Exercise 5.1 *Describe explicitly the Diophantine equation which corresponds to finding the units in the ring $\mathbb{Z}[\sqrt[3]{2}]$. What does the unit theorem imply in this case? Can you find a non-torsion unit?*

Exercise 5.2 *Suppose that p is a prime number, and F is a number field which is a Galois extension of $\mathbb{Q}$. Suppose that p is totally ramified in F, which means that $p\mathcal{O}_F = P^n$ for some prime ideal P of $\mathcal{O}_F$.*

(a) Prove that if $\sigma \in Gal(F/\mathbb{Q})$, then $\sigma(P) = P$.

(b) Suppose that P is a principal ideal, $P = \alpha \cdot \mathcal{O}_F$. Prove that $\alpha/\sigma(\alpha) \in \mathcal{O}_F^\times$.

Exercise 5.3 *A CM-field is a number field F, which contains a subfield K, such that K is totally real (all archimedean places are real), F is totally complex (all archimedean places are complex), and $[F : K] = 2$.*

(a) Suppose that F is a CM field. Prove that there is a unique subfield K such that K is totally real and $[F : K] = 2$. Hint: prove that if K_1, K_2 are totally real subfields of F, then K_1K_2 is a totally real subfield of F. When F is a CM field, we write F^+ for this uniquely determined totally real subfield satisfying $[F : F^+] = 2$.

(b) Suppose that $K \subset F$ is any proper inclusion of number fields. Prove that F is a CM field with $K = F^+$ if and only if $\mathcal{O}_F^\times / \mathcal{O}_K^\times$ is a finite group. Hint: analyze how r_1 and r_2 change in an extension of number fields, and apply Dirichlet's unit theorem.

6
Cyclotomic Fields

We have developed a great deal of theory, covering the most important basic invariants of a number field. However, our examples have been quite limited, covering quadratic fields and occasionally (in the exercises) cubic or biquadratic quartic fields.

Historically and today, cyclotomic fields are some of the most important number fields. In the nineteenth century, they motivated much of the development of number theory due to their relevance to Fermat's Last Theorem. Later, with the Kronecker-Weber theorem, it was realized that cyclotomic fields play an important role in understanding the abelian Galois extensions of $\mathbb{Q}$. They play a basic role in Iwasawa theory, developed in the late twentieth century.

There are many books on cyclotomic fields; we mention Washington [1] and Lang [2] as two that are well-known. In this chapter, we use cyclotomic fields to review all we have studied in the previous chapters, and to prove an important case of Fermat's Last Theorem.

[1]
[2]

6.1 Cyclotomic polynomials and fields

Let m be a positive integer, and let F be a number field. An m^{th} **root of unity** in F is an element $\zeta \in F$ satisfying $\zeta^m = 1$. A **primitive** m^{th} root of unity is an element $\zeta \in F$ satisfying $\zeta^m = 1$, and not satisfying $\zeta^n = 1$ for any positive integer $n < m$. One writes $\mu_m(F)$ for the cyclic[3] group of m^{th} roots of unity in F. The generators of this cyclic group are precisely the primitive m^{th} roots of unity.

[3] We have proven that this group is cyclic when F is a number field, in Proposition 5.7

Lemma 6.1 *Suppose that ζ is a primitive m^{th} root of unity in a number field F. Let Φ_m be the minimal polynomial of ζ, called the m^{th}* ***cyclotomic polynomial****. Then, if p is a prime number not dividing m, and r is a root of Φ_m, then $\Phi_m(r^p) = 0$.*

Proof: Note that since $\zeta^m = 1$, ζ is an algebraic integer, and Φ_m is a monic polynomial with integer coefficients. There exists a monic

polynomial $\Psi_m \in \mathbb{Z}[X]$ such that

$$X^m - 1 = \Phi_m(X) \cdot \Psi_m(X).$$

Observe that $\mu_m(F)$ is a cyclic group of order m, and therefore the roots of $X^m - 1$ are all distinct; it follows that every root of $X^m - 1$ is either a root of Φ_m or is a root of Ψ_m (but never both).

Now consider a root r of Φ_m and a prime number p not dividing m. We immediately know that r^p is a root of $X^m - 1$, and hence r^p is a root of Φ_m or of Ψ_m. We seek to prove that r^p is a root of Φ_m.

Let $\mathcal{O}$ denote the ring of integers in $\mathbb{Q}(\zeta)$. Let P be a prime ideal of $\mathcal{O}$ occurring in the factorization of the principal ideal $p\mathcal{O}$. Since $\Phi_m(r) = 0$ and the coefficients of Φ_m are integers, we may reduce mod P to obtain:

$$\Phi_m(r) \equiv 0, \text{ modulo } P.$$

Note that $\mathcal{O}/P$ is a field of characteristic p, since $p \in P$. Hence, the **Frobenius map** sending every element to its p^{th} power is a field automorphism of $\mathcal{O}/P$. We find that

$$\Phi_m(r^p) \equiv 0, \text{ modulo } P.$$

Note that, since p does not divide m, the polynomial $X^m - 1$ is relatively prime[4] to its derivative mX^{m-1}, not only in $\mathbb{Z}[X]$, but also in $(\mathcal{O}/P)[X]$. It follows that $X^m - 1$ has no repeated roots in the field $\mathcal{O}/P$. In particular, since $\Phi_m(r^p) \equiv 0$, modulo P, we find that $\Psi_m(r^p) \not\equiv 0$, modulo P. Therefore, $\Psi_m(r^p) \neq 0$.

We have demonstrated that r^p is a root of $X^m - 1$, but not a root of Ψ_m. Hence r^p is a root of Φ_m.

[4] In the Euclidean domain $(\mathcal{O}/P)[X]$, one may check that these two polynomials are relatively prime, since polynomial division leaves a remainder of 1.

□

Proposition 6.2 *Let ζ be a primitive m^{th} root of unity in a number field F. The roots of the cyclotomic polynomial Φ_m are precisely the primitive m^{th} roots of unity. In particular, $\mathbb{Q}(\zeta)$ is a Galois extension of $\mathbb{Q}$, and $\mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$ is isomorphic to the group $(\mathbb{Z}/m\mathbb{Z})^\times$.*

PROOF: Every root of Φ_m is a primitive m^{th} root of unity, since Φ_m is the minimal polynomial of ζ. Furthermore, every primitive m^{th} root of unity can be expressed as ζ^e, for some exponent e relatively prime to m. Factoring e into primes, we have $e = q_1 \cdots q_t$, for some sequence of prime numbers $q_1, \ldots, q_t$, none of which divide m.

By the previous lemma, we find that ζ is a root of Φ_m, hence ζ^{q_1} is a root of Φ_m. Applying the previous lemma to ζ^{q_1}, we find that $(\zeta^{q_1})^{q_2} = \zeta^{q_1 q_2}$ is a root of Φ_m. Continuing inductively with the previous lemma, we find that $\zeta^{q_1 \cdots q_t} = \zeta^e$ is a root of Φ_m. Thus every primitive m^{th} root of unity is a root of Φ_m. The roots of Φ_m are precisely all primitive m^{th} roots of unity, i.e., the generators of $\mu_m(F)$.

As the polynomial Φ_m is irreducible, and all roots of Φ_m are powers of ζ, we find that $\mathbb{Q}(\zeta)$ is a Galois extension of $\mathbb{Q}$. An element $g \in \mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$ is uniquely determined by $g(\zeta)$, since the other roots of Φ_m have the form ζ^e for some integer e. Furthermore, $g(\zeta) = \zeta^{f(g)}$, for some integer $f(g)$ relatively prime to m, unique modulo m, since $g(\zeta)$ is again a primitive m^{th} root of unity.

If $g, g' \in \mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$, then we find that:

$$\zeta^{f(gg')} = [gg'](\zeta) = g(\zeta^{f(g')}) = \zeta^{f(g)f(g')}.$$

It follows that f is a well-defined injective homomorphism from $\mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$ to the group $(\mathbb{Z}/m\mathbb{Z})^\times$. Since $\mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$ must act transitively on the roots of Φ_m, a set with cardinality equal to the cardinality[5] of $(\mathbb{Z}/m\mathbb{Z})^\times$, we find that this homomorphism f is surjective.

□

[5] The cardinality of $(\mathbb{Z}/m\mathbb{Z})^\times$ is the number of integers k satisfying $1 \leq k < m$ and relatively prime to m. This cardinality is called the (Euler's) **totient** of m, and denoted $\phi(m)$. Note that $\phi(m)$ is the degree of the cyclotomic polynomial Φ_m.

The subject of this chapter is the following:

Definition 6.3 *A **cyclotomic field** is a number field F, such that $F = \mathbb{Q}(\zeta)$ for some root of unity $\zeta \in F$. Without loss of generality, a cyclotomic field can also be thought of as a field $F = \mathbb{Q}(\zeta)$ for some primitive root of unity ζ.*

Let $\phi(m)$ denote the degree of Φ_m, i.e., the **totient**[6] of m, or the cardinality of $(\mathbb{Z}/m\mathbb{Z})^\times$. By the Chinese remainder theorem, a prime factorization $m = p_1^{e_1} \cdots p_t^{e_t}$ yields a decomposition of rings:

$$\frac{\mathbb{Z}}{m\mathbb{Z}} \cong \frac{\mathbb{Z}}{p_1^{e_1}\mathbb{Z}} \times \cdots \times \frac{\mathbb{Z}}{p_t^{e_t}\mathbb{Z}}.$$

[6] Euler's totient, $\phi(m)$ may be described as "the number of integers between 1 and m (inclusive), which are relatively prime to m".

This yields a decomposition of unit groups:

$$\left(\frac{\mathbb{Z}}{m\mathbb{Z}}\right)^\times \cong \left(\frac{\mathbb{Z}}{p_1^{e_1}\mathbb{Z}}\right)^\times \times \cdots \times \left(\frac{\mathbb{Z}}{p_t^{e_t}\mathbb{Z}}\right)^\times.$$

Observe that, if p is a prime number, and e is a positive integer, one may identify:

$$\left(\frac{\mathbb{Z}}{p^e\mathbb{Z}}\right)^\times = \frac{\mathbb{Z}}{p^e\mathbb{Z}} - \frac{p\mathbb{Z}}{p^e\mathbb{Z}},$$

from which one finds that $\phi(p^e) = p^e - p^{e-1}$. Using the factorization above, we find more generally that

$$\phi(m) = \prod_{i=1}^{t} \phi(p_i^{e_i}) = \prod_{i=1}^{t} \left(p_i^{e_i} - p_i^{e_i-1}\right).$$

The above product has at least one even factor, unless $m = 1$ or $m = 2$ (in which cases $\phi(m) = 1$). Of course, when $m = 1$ or $m = 2$, the

m^{th} roots of unity are already contained in $\mathbb{Q}$, so this is not a very interesting case to study.

Observe that the only roots of unity in $\mathbb{R}$ are ± 1. It follows that if $m > 2$ and $F = \mathbb{Q}(\zeta)$ for a primitive m^{th} root of unity ζ, then $r_1 = 0$, $[F : \mathbb{Q}] = \phi(m)$, and the number of complex places of F is given by $r_2 = 1/2 \cdot \phi(m)$.

From considering the degrees of field extensions, we may prove the following

Proposition 6.4 *Suppose that $F = \mathbb{Q}(\zeta)$ is a cyclotomic field, where ζ is a primitive m^{th} root of unity. Let $\mu(F)$ denote the group of all roots of unity in F (the group law given by multiplication, of course). Then, if m is even, then $\mu(F)$ is generated by ζ, and has order m. If m is odd, then $\mu(F)$ is generated by $-\zeta$, and has order $2m$.*

PROOF: We have seen that $[F : \mathbb{Q}] = \phi(m)$. Furthermore, $\mu(F)$ is a finite subgroup of $\mathcal{O}_F^\times$, hence cyclic. Let η be a generator of $\mu(F)$. Then, we find that η is a primitive n^{th} root of unity, and m divides n. Hence $F = \mathbb{Q}(\zeta) = \mathbb{Q}(\eta)$, and it must be the case that

$$[F : \mathbb{Q}] = \phi(m) = \phi(n).$$

The totients $\phi(m)$ and $\phi(n)$ may be computed from the prime factorizations of m and n. Let M be the set of prime numbers dividing m, and N the set of prime factors dividing n. The prime factorizations of m and n may now be expressed as:

$$m = \prod_p p^{e_p}, \text{ and } n = \prod_p p^{f_p},$$

where e_p, f_p are positive integers. Note that $M \subset N$ since m divides n. We find that

$$\phi(m) = \prod_{p \in M} (p-1)p^{e_p - 1} = \prod_{p \in N} (p-1)p^{f_p - 1} = \phi(n).$$

Observe that if $p \in M$, and $f_p > e_p$, then $\phi(n) > \phi(m)$, a contradiction. If $p \in N$ but $p \notin M$, then we again find a contradiction, unless $p = 2$ and $f_p = 1$.

Thus, we find that $\phi(m) = \phi(n)$ implies that $m = n$, or else $n = 2m$ and m is odd. The converse is not difficult to check by direct computation in the above formula.

Thus we find that $\mu(F)$ is generated by ζ if m is even. If m is odd, then we find that $\mu(F)$ is a cyclic group of order $2m$. The element $-\zeta$ satisfies $(-\zeta)^{2m} = 1$, and $(-\zeta)^m = -1$. It follows directly that $-\zeta$ generates $\mu(F)$.

□

6.2 *Integers*

Our first task, in the spirit of the second chapter of this text, is to determine the ring of integers in the number field $F = \mathbb{Q}(\zeta)$. We focus hereafter on the case when ζ is an $(\ell^d)^{th}$ root of unity, where ℓ is a prime number and $d \geq 1$. In this case, the cyclotomic polynomial Φ_{ℓ^d} has degree

$$n = \ell^d - \ell^{d-1} = \ell^{d-1}(\ell - 1),$$

and it has the simple form[7]

$$\begin{aligned} \Phi_{\ell^d}(X) &= \frac{X^{\ell^d} - 1}{X^{\ell^{d-1}} - 1} \\ &= (X^{\ell^{d-1}})^{\ell-1} + (X^{\ell^{d-1}})^{\ell-2} + \cdots + (X^{\ell^{d-1}})^1 + 1. \end{aligned}$$

[7] One may see this by observing that the primitive $(\ell^d)^{th}$ roots of unity are all $(\ell^d)^{th}$ roots of unity, excluding the $(\ell^{d-1})^{th}$ roots of unity.

In particular, when $d = 1$,

$$\Phi_\ell(X) = X^{\ell-1} + X^{\ell-2} + \cdots + X + 1.$$

Let $\pi = \zeta - 1$ and define $P_\pi(X) = \Phi_{\ell^d}(X + 1)$. The irreducibility of Φ_{ℓ^d} implies the irreducibility of P_π. Observing that $P_\pi(\pi) = 0$, it follows that P_π is the minimal polynomial of π, and $F = \mathbb{Q}(\zeta) = \mathbb{Q}(\pi)$.

Proposition 6.5 *The element $\pi \in \mathcal{O}_F$ has norm $(-1)^n \cdot \ell$, and hence the principal ideal $\pi\mathcal{O}$ is prime.*

PROOF: The norm of π equals the constant term of its minimal polynomial P_π, times $(-1)^{\mathrm{Deg}(P_\pi)} = (-1)^n$. The proposition now follows from the computation[8]

$$P_\pi(0) = \Phi_{\ell^d}(1) = \ell.$$

[8] This is not really a computation; simply observe that Φ_{ℓ^d} is a polynomial with ℓ terms, each of which is a power of X.

□

In what follows we frequently use the following "indexing set":

$$I = \{i \in \mathbb{Z} \colon 1 \leq i \leq \ell^d, \text{ and } \ell \nmid i\}.$$

Thus, I is an ordered set of representatives for the finite group $(\mathbb{Z}/\ell^d\mathbb{Z})^\times$. Now we may factor ℓ in the ring $\mathcal{O}_F$:

$$\ell = \prod_{i \in I} (\zeta^i - 1)$$

since the terms in this product are precisely the Galois conjugates of π.

On the other hand, we may prove

Proposition 6.6 *For all $i \in I$, the element $1-\zeta^i/1-\zeta$ is an element of $\mathcal{O}_F^\times$.*

PROOF: There exists $g \in G = \mathrm{Gal}(F/\mathbb{Q})$, such that $g(1-\zeta) = 1-\zeta^i$, and so these elements have the same norm. Thus $1-\zeta^i/1-\zeta$ has norm 1. Furthermore, we may expand a partial geometric series:

$$\frac{1-\zeta^i}{1-\zeta} = 1 + \zeta + \zeta^2 + \cdots + \zeta^{i-1}.$$

It follows that $1-\zeta^i/1-\zeta$ is an element of $\mathcal{O}$. The proposition follows.

□

The units of the form $1-\zeta^i/1-\zeta$ are called **cyclotomic units**[9] in $\mathcal{O}_F$. Since these are units, we find the following

[9] The cyclotomic units provide a quite large supply of units in $\mathcal{O}_F^\times$. In fact, the subgroup generated by the cyclotomic units in $\mathcal{O}_F^\times$ (modulo torsion units) has finite index. This index is equal to the class number of the maximal totally real subfield F^+ in F, discussed later. Reminder:

$$n = \ell^d - \ell^{d-1} = \ell^{d-1}(\ell-1).$$

$$I = \{i \in \mathbb{Z} \colon 1 \leq i \leq \ell^d, \text{ and } \ell \nmid i\}.$$

Corollary 6.7 *In the ring $\mathcal{O}_F$, there exists a unit ϵ such that $\ell = \epsilon\pi^n$. Moreover, the principal ideal $\ell\mathcal{O}_F$ factors into prime ideals as:*

$$\ell\mathcal{O}_F = (\pi\mathcal{O}_F)^n.$$

PROOF: Recalling that $\pi = \zeta - 1$, we have

$$\ell = \prod_{i\in I}(\zeta^i - 1) = \prod_{i\in I}\frac{\zeta^i - 1}{\zeta - 1}(\zeta - 1) = \epsilon \cdot \pi^n,$$

for a suitable product ϵ of cyclotomic units. This corresponds to a factorization of the principal ideal $\ell\mathcal{O}_F$ as a power $(\pi\mathcal{O})^n$ of the principal ideal $\pi\mathcal{O}_F$. Since $|\mathrm{N}(\pi)| = \ell$ is a prime number, we see that $\pi\mathcal{O}_F$ is a prime ideal in $\mathcal{O}_F$. Hence, this is the (unique) factorization of the principal ideal ℓ into prime ideals in $\mathcal{O}_F$.

□

Consider the order $\mathcal{O} = \mathbb{Z}[\zeta] \subset \mathcal{O}_F$. A natural $\mathbb{Z}$-basis of $\mathcal{O}$ is given by the set of powers $1, \zeta, \zeta^2, \ldots, \zeta^{n-1}$. On the other hand, the Galois conjugates of ζ are precisely ζ^i for $i \in I$. Thus we are led to consider the square matrix

$$V = \left(\zeta^{ij}\right)_{i\in I, 0\leq j<n}.$$

The discriminant of $\mathcal{O}$ can now be expressed as

$$\mathrm{Disc}(\mathcal{O}) = \mathrm{Det}(V)^2.$$

In order to evaluate this determinant, we apply the following result of independent interest

Proposition 6.8 *Consider the following **Vandermonde determinant** as an element of the polynomial ring $\mathbb{Z}[X_1, \ldots, X_n]$:*

$$v(X_1, \ldots, X_n) = \mathrm{Det}\begin{pmatrix} 1 & X_1 & X_1^2 & \cdots & X_1^{n-1} \\ 1 & X_2 & X_2^2 & \cdots & X_2^{n-1} \\ 1 & X_3 & X_3^2 & \cdots & X_3^{n-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & X_n & X_n^2 & \cdots & X_n^{n-1} \end{pmatrix}.$$

Then the following is an equality in the ring $\mathbb{Z}[X_1, \ldots, X_n]$:

$$v(X_1, \ldots, X_n) = \prod_{1 \le i < j \le n} (X_j - X_i).$$

PROOF: If one expands the determinant, each summand is a product of the form $\prod_{i=1}^{n} X_{\sigma(i)}^{i-1}$, for some permutation σ of $\{1, \ldots, n\}$. It follows that the determinant $v(X_1, \ldots, X_n)$ is a homogeneous polynomial of total degree $0 + 1 + \cdots + (n-1) = {}^{n(n-1)}/_{2}$.

Suppose for a moment that $1 \le i < j \le n$. Consider the quotient ring $\mathbb{Z}[X_1, \ldots, X_n]/\langle X_j - X_i \rangle$. In this quotient, the images $\bar{X}_i$ and $\bar{X}_j$ are equal; it follows that the determinant $v(\bar{X}_1, \ldots, \bar{X}_n)$ equals zero in this quotient ring, since two rows of the Vandermonde matrix are equal. Hence we find that the polynomial $v(X_1, \ldots, X_n)$ is a multiple of $(X_j - X_i)$ in the ring $\mathbb{Z}[X_1, \ldots, X_n]$.

We find that $v(X_1, \ldots, X_n)$ is a polynomial of degree ${}^{n(n-1)}/_{2}$ in the unique factorization domain $\mathbb{Z}[X_1, \ldots, X_n]$, and the irreducible polynomials $(X_j - X_i)$ are factors of v for all ${}^{n(n-1)}/_{2}$ possible $1 \le i < j \le n$. It follows now that there exists a constant $r \in \mathbb{Z}$ such that

$$v(X_1, \ldots, X_n) = r \cdot \prod_{1 \le i < j \le n} (X_j - X_i).$$

Consider the coefficient of the term

$$X_1^0 \cdot X_2^1 \cdot \cdots \cdot X_n^{n-1}.$$

In the Vandermonde determinant, this term occurs only on the main diagonal, where it has coefficient 1. In the product $\prod(X_j - X_i)$, this term occurs only once, by choosing the first summand in each term in the product. Hence the coefficient r equals 1.

□

This proposition allows one to evaluate the Vandermonde determinant "generically"; we are interested in the special case where the variables X_i are replaced by the distinct powers ζ^i for $i \in I$. We find that

$$\mathrm{Det}(V) = \prod_{\substack{i<j \\ i,j \in I}} (\zeta^i - \zeta^j).$$

With the aid of cyclotomic units , each term can be expressed as

$$(\zeta^i - \zeta^j) = \zeta^i(1 - \zeta^{j-i}) = \epsilon_{ij} \cdot \pi,$$

for some units ϵ_{ij}. Here, we observe that since i and j are not multi-

Reminder:

$$n = \ell^d - \ell^{d-1} = \ell^{d-1}(\ell - 1).$$

$$I = \{i \in \mathbb{Z} \colon 1 \le i \le \ell^d, \text{ and } \ell \nmid i\}.$$

ples of ℓ, neither is $j - i$. Finally, we arrive at:

$$\begin{aligned}
\mathrm{Disc}(\mathcal{O}) &= \mathrm{Det}(V)^2 \\
&= \prod_{i<j}(\zeta^i - \zeta^j)^2 \\
&= \prod_{i<j}\epsilon_{ij}^2\pi^2, \\
&= \left(\prod_{i<j}\epsilon_{ij}^2\right)\cdot\pi^{n(n-1)}, \\
&= u\ell^{n-1}.
\end{aligned}$$

for some unit $u \in \mathcal{O}_F^\times$. Note that we use our previous factorization, $\ell = \epsilon\pi^n$ in the last step above. Since the discriminant $\mathrm{Disc}(\mathcal{O})$ is necessarily an integer, we find that

$$\mathrm{Disc}(\mathcal{O}) = \pm\ell^{n-1} = \pm\ell^{\ell^d - \ell^{d-1} - 1}.$$

In particular, if $d = 1$, then we find that $\mathrm{Disc}(\mathcal{O}) = \pm\ell^{\ell-2}$.[10]

[10] The sign of the discriminant, we recall, can be obtained from the number of complex places.

We have one more lemma to prove, before the main theorem of this section:

Lemma 6.9 *$\pi/\ell \in \mathcal{O}_F^\sharp$. In other words, for every $\alpha \in \mathcal{O}_F$, $Tr(\pi\alpha/\ell) \in \mathbb{Z}$.*

PROOF: To prove that $Tr(\pi\alpha/\ell) \in \mathbb{Z}$ for all $\alpha \in \mathcal{O}_F$, it suffices to prove that $Tr(\pi\alpha) \in \ell\mathbb{Z}$ for all $\alpha \in \mathcal{O}_F$. Recall that $G = \mathrm{Gal}(F/\mathbb{Q})$; for each $i \in I$, let $g_i \in G$ be the unique element for which $g_i(\zeta) = \zeta^i$. Now we compute

$$\begin{aligned}
Tr(\pi\alpha) &= Tr((\zeta - 1)\alpha) \\
&= \sum_{i\in I}(\zeta^i - 1)g_i(\alpha) \\
&= \sum_{i\in I}(\zeta - 1)(\zeta^{i-1} + \cdots + \zeta + 1)g_i(\alpha) \\
&\in \pi\mathcal{O}_F \cap \mathbb{Z}.
\end{aligned}$$

Thus, it suffices to prove that $\pi\mathcal{O}_F \cap \mathbb{Z} = \ell\mathbb{Z}$. On the one hand, $\pi\mathcal{O}_F \cap \mathbb{Z}$ is a prime ideal in $\mathbb{Z}$, since the quotient $\mathbb{Z}/(\pi\mathcal{O}_F \cap \mathbb{Z})$ is naturally a subring of the integral domain $\mathcal{O}_F/\pi\mathcal{O}_F$. Furthermore, $\ell \in \pi\mathcal{O}_F \cap \mathbb{Z}$, and ℓ is a prime number. Thus $\pi\mathcal{O}_F \cap \mathbb{Z}$ contains the maximal ideal $\ell\mathbb{Z}$, and hence must equal $\ell\mathbb{Z}$.

□

Theorem 6.10 *The ring of integers $\mathcal{O}_F$ in $F = \mathbb{Q}(\zeta)$ is equal to $\mathcal{O} = \mathbb{Z}[\zeta]$.*

PROOF: We have found that $\mathbb{Z}[\zeta] = \mathcal{O} \subset \mathcal{O}_F$ and $|\mathrm{Disc}(\mathbb{Z}[\zeta])| = \ell^{n-1}$. Consider the following sequence of lattices and inclusions:

$$\mathcal{O} \subset \mathcal{O}_F \subset \mathcal{O}_F^\sharp \subset \mathcal{O}^\sharp.$$

By multiplicativity of the index, we find that

$$\ell^{n-1} = |\operatorname{Disc}(\mathcal{O})| = [\mathcal{O}^\sharp : \mathcal{O}] = [\mathcal{O}^\sharp : \mathcal{O}_F^\sharp][\mathcal{O}_F^\sharp : \mathcal{O}_F][\mathcal{O}_F : \mathcal{O}].$$

Therefore, in order to prove that $\mathcal{O}_F = \mathcal{O}$, it suffices to prove that $[\mathcal{O}_F : \mathcal{O}] = 1$, for which it suffices to prove that $[\mathcal{O}_F^\sharp : \mathcal{O}_F] \geq \ell^{n-1}$.

Consider now the inclusions $\ell\mathcal{O}_F \subset \pi\mathcal{O}_F \subset \mathcal{O}_F$. Since the absolute value of the norm of π is ℓ, and the norm of ℓ is ℓ^n, we find that $[\pi\mathcal{O}_F : \ell\mathcal{O}_F] = \ell^{n-1}$. Dividing through by ℓ, we have an inclusion of lattices:

$$\mathcal{O}_F \subset \frac{\pi}{\ell}\mathcal{O}_F \subset \mathcal{O}_F^\sharp.$$

Since the first inclusion has index ℓ^{n-1}, we find that $[\mathcal{O}_F^\sharp : \mathcal{O}_F] \geq \ell^{n-1}$. This completes the squeeze.[11]

[11] In fact, we have additionally proven that $\mathcal{O}_F^\sharp = (\pi/\ell) \cdot \mathcal{O}_F$.

□

Corollary 6.11 *The discriminant of the number field $F = \mathbb{Q}(\zeta)$ is equal to ℓ^{n-1}.*

6.3 The totally real subfield

Observe that if ζ is a primitive $(\ell^d)^{th}$ root of unity, then ζ^{-1} is also a primitive $(\ell^d)^{th}$ root of unity. Thus, there is a canonical element of $G = \operatorname{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$, which sends ζ to ζ^{-1}. If $\alpha \in \mathbb{Q}(\zeta)$, we write $\bar{\alpha}$ for the image of α under this field automorphism; in particular, $\bar{\zeta} = \zeta^{-1}$. Of course $\overline{\bar{\alpha}} = \alpha$; the field automorphism is an **involution**.

We define F^+ to be the fixed subfield of $F = \mathbb{Q}(\zeta)$, under this involution:

$$F^+ = \mathbb{Q}(\zeta)^+ = \{\alpha \in F : \alpha = \bar{\alpha}\}.$$

The cyclotomic field F is a quadratic extension of F^+. Observe that if v is any embedding of F into $\mathbb{C}$, then ζ and $\bar{\zeta}$ get mapped, via v, to complex conjugate elements of $\mathbb{C}$. It follows that $v(F^+) \subset \mathbb{R}$. Since every embedding of F^+ in $\mathbb{C}$ extends to an embedding of F into $\mathbb{C}$, we find that every embedding of F^+ in $\mathbb{C}$ lands inside of $\mathbb{R}$. Therefore F^+ is a **totally real** number field, and F is a **totally complex** quadratic extension of F^+.

Proposition 6.12 *The unit group $\mathcal{O}_F^\times$ contains the unit group $\mathcal{O}_{F^+}^\times$ with finite index.*

PROOF: The field F has $n/2$ complex places and 0 real places, and degree n over $\mathbb{Q}$. On the other hand, F^+ has zero complex places, degree $n/2$ over $\mathbb{Q}$, and hence has $n/2$ real places.

It follows from the unit theorem that the free rank[12] of $\mathcal{O}_F^\times$ and the free rank of $\mathcal{O}_{F^+}^\times$ are the same:

$$\operatorname{Rank}(\mathcal{O}_F^\times) = \operatorname{Rank}(\mathcal{O}_{F^+}^\times) = \frac{n}{2} - 1.$$

[12] If A is a finitely generated abelian group, then A is isomorphic to $A_{tor} \times \mathbb{Z}^r$, for some torsion abelian group A_{tor} and some non-negative integer r. The integer r is called the free rank of A.

□

In fact, we can go further and express the units in $\mathcal{O}_F^\times$ in terms of units from $\mathcal{O}_{F^+}^\times$ and roots of unity. In what follows, we write $\mu(F)$ for the group of torsion units in $\mathcal{O}_F^\times$, i.e., roots of unity. Note that, for all $\epsilon \in \mu(F)$, $\bar{\epsilon} = \epsilon^{-1}$. If ℓ is an odd prime, then

$$\mu(F) = \{\pm\zeta^r : 0 \leq r < \ell^d - 1\},$$

and $\mu(F)^2$ is the cyclic subgroup generated by ζ. On the other hand, if $\ell = 2$, then $\mu(F)$ is generated by ζ, and $\mu(F)^2$ is generated by ζ^2.

Proposition 6.13 *Suppose that $u \in \mathcal{O}_F^\times$. Then, there exists a unit $v \in \mathcal{O}_{F^+}^\times$, and a root of unity $\epsilon \in \mu(F)$ such that $u = \epsilon \cdot v$.*

Proof: Some parts of the following proof are loosely based on Proposition 5.12 of Milne's text[13].

[13] James S. Milne. Algebraic number theory (v3.02), 2009. Available at www.jmilne.org/math/

Consider the map $u \mapsto u/\bar{u}$ from $\mathcal{O}_F^\times$ to $\mathcal{O}_F^\times$. It is a group homomorphism, whose kernel is contained in $\mathcal{O}_{F^+}^\times$.

Since complex conjugation preserves *every* archimedean absolute value, we find that $\lambda(u/\bar{u}) = 0$, where λ denotes the logarithmic modulus map of the previous chapter. Thus $u/\bar{u}$ is a torsion unit, i.e., $u/\bar{u} \in \mu(F)$.

Furthermore, if $u/\bar{\in}\mu(F)^2$, then $u = \bar{u}\epsilon^2$ for some $\epsilon \in \mu(F)$. It follows (since $\bar{\epsilon} = \epsilon^{-1}$) that $(u\bar{\epsilon})/(\bar{u}\epsilon) = 1$. Thus $u\bar{\epsilon} \in \mathcal{O}_{F^+}^\times$, and we find that $u \in \mu(F) \cdot \mathcal{O}_{F^+}^\times$.

We now have the following commutative diagram of abelian groups and homomorphisms, whose columns arise from inclusion, equality, and projection, from left to right:

$$\begin{array}{ccccccccc}
1 & \longrightarrow & \mathcal{O}_{F^+}^\times & \longrightarrow & \mathcal{O}_F^\times & \xrightarrow{u\mapsto u/\bar{u}} & \mu(F) & \longrightarrow & 1 \\
 & & \downarrow & & \downarrow{\scriptstyle =} & & \downarrow & & \\
1 & \longrightarrow & \mu(F)\mathcal{O}_{F^+}^\times & \longrightarrow & \mathcal{O}_F^\times & \longrightarrow & \mu(F)/\mu(F)^2 & \longrightarrow & 1
\end{array}$$

Now, in order to prove that $\mathcal{O}_F^\times = \mu(F)\mathcal{O}_{F^+}^\times$, it suffices to prove that $u/\bar{u}$ is always a square in $\mu(F)$. There are two cases to consider:

Much of this reasoning goes through, without changes, to the case of a CM field and its totally real subfield. In that generality, one finds always that $\mathcal{O}_F^\times$ contains $\mathcal{O}_{F^+}^\times \mu(F)$ with index 1 or 2.

ℓ odd: When ℓ is odd, $\mu(F)^2$ is generated by ζ. Observe that if $u \in \mathcal{O}_F^\times$, then there exist integers $a_0, \ldots, a_{n-1}$ such that

$$u = a_0 + a_1\zeta + \cdots + a_{n-1}\zeta^{n-1}.$$

Since integers are fixed under the involution, we find that

$$\bar{u} = a_0 + a_1\bar{\zeta} + \cdots + a_{n-1}\bar{\zeta}^{n-1}.$$

Modulo $\pi = \zeta - 1$, we find that $u \equiv \bar{u}$. If $u/\bar{u}$ is not in $\mu(F)^2$, then $u/\bar{u} = -\zeta^r$, for some integer r, then we find that $u = -\zeta^r \bar{u}$, and

$$u \equiv -zeta^r u \equiv -u, \text{ modulo } \pi.$$

Hence $2u \equiv 0$, modulo π. Note that $2 \not\equiv 0$, modulo π, since ℓ is odd; it follows that $u \equiv 0$, modulo π, contradicting the fact that u is a unit. Therefore, we find that $u/\bar{u} \in \mu(F)^2$.

$\ell = 2$: When $\ell = 2$ (and $d > 1$, so $F \neq \mathbb{Q}$, of course), we find that $\mu(F)$ is generated by ζ, and $\mu(F)^2$ is generated by ζ^2. Thus, if $u/\bar{u}$ is not in $\mu(F)^2$, then $u/\bar{u} = \zeta \cdot \zeta^{2r}$ for some integer r. In this case, we work modulo $\varpi = 1 - \zeta^2$; note that π is not a multiple of ϖ. Working modulo ϖ we find that $u \equiv \zeta\bar{u}$. Note that $\zeta^{-1} \equiv \zeta$, modulo ϖ, and hence $u \equiv \bar{u}$, modulo ϖ. Thus $u \equiv \zeta u$, modulo ϖ. It follows that πu is a multiple of ϖ. But this is a contradiction; π is not a multiple of ϖ. Hence $u/\bar{u} \in \mu(F)^2$.

Thus $u/\bar{u} \in \mu(F)^2$ for all $u \in \mathcal{O}_F^\times$. The result follows.

□

6.4 *The first case of Fermat's Last Theorem*

Fermat's Last Theorem, proven by Andrew Wiles, is the following

Theorem 6.14 *Suppose that n is an integer, and $n \geq 3$. Suppose that $x, y, z \in \mathbb{Z}$ and $x^n + y^n = z^n$. Then $xyz = 0$. In other words, there are no solutions to the equation $X^n + Y^n = Z^n$, except for the "trivial solutions" in which at least one coordinate vanishes.*

It was long ago realized that it suffices to prove Fermat's Last Theorem for odd prime exponents. Indeed, any nontrivial solution (x, y, z) to $X^n + Y^n = Z^n$ yields a nontrivial solution

$$(x^{n/\ell})^\ell + (y^{n/\ell})^\ell = (z^{n/\ell})^\ell$$

to the equation $X^\ell + Y^\ell = Z^\ell$, if ℓ is a prime factor of n. For this reason, it is natural to restrict to the case of Fermat's Last Theorem with odd prime exponent.

Historically, Fermat's Last Theorem has been approached in two cases.

Case 1: Suppose that $x, y, z \in \mathbb{Z}$ and $x^\ell + y^\ell = z^\ell$. Then ℓ must divide xyz.

Case 2: Suppose that $x, y, z \in \mathbb{Z}$ and $\ell \mid (xyz)$. Then if $x^\ell + y^\ell = z^\ell$, then $xyz = 0$.

In other words, the first case of Fermat's Last Theorem states that there are no solutions (x, y, z) to $X^\ell + Y^\ell = Z^\ell$ in which ℓ does not divide any x, y, z. The second case begins with the assumption that ℓ divides one of x, y, z.

In this section, we prove the first case of Fermat's Last Theorem, for "regular primes" ℓ.

Definition 6.15 *A prime number ℓ is a **regular prime** if ℓ does* not *divide the class number $h(\mathbb{Q}(\zeta))$ where ζ is a primitive ℓ^{th} root of unity. Otherwise, ℓ is called an **irregular prime**.*[14]

[14] While "irregular" primes appear rare among small prime numbers, it has not been proven that irregular primes occur less often than regular primes, asympotically. In fact, it has been proven that there are infinitely many irregular primes, and it has not been proven that there are infinitely many regular primes!

Hereafter, fix an odd prime number ℓ, and a primitive ℓ^{th} root of unity ζ. Let $F = \mathbb{Q}(\zeta)$ denote the resulting cyclotomic field. Let $\pi = \zeta - 1$. Recall that $n = [F : \mathbb{Q}] = \ell - 1$, and $\pi^{\ell-1}$ is a unit multiple of ℓ. Also, the discriminant of F is equal to $\ell^{\ell-2}$, and $\mathcal{O}_F = \mathbb{Z}[\zeta]$.

The relevance of cyclotomic fields to Fermat's Last Theorem is that the equation $X^\ell - Y^\ell = Z^\ell$ can be factored in the ring $\mathcal{O}_F[X, Y, Z]$:

$$X^\ell - Y^\ell = \prod_{i=0}^{\ell-1}(X - \zeta^i Y) = Z^\ell.$$

Note that the switch in sign, $Y^\ell \mapsto -Y^\ell$ does not affect the study of Fermat's Last Theorem, since we assume that ℓ is an odd prime.

Theorem 6.16 (Case 1, Regular Primes) *Suppose that $\ell > 5$. Suppose that ℓ does not divide the order $h(F)$ of the ideal class group of F, i.e., ℓ is a regular prime. Then if $(x, y, z) \in \mathbb{Z}$ and $x^\ell - y^\ell = z^\ell$, then $\ell \mid (xyz)$.*

Proof: First, note that it suffices to assume that $(x, y, z) = 1$, i.e., x, y, and z do not have any common integer factors except for ± 1. Indeed, if d were a common factor of x, y, and z, then a new "smaller" solution to Fermat's Last Theorem would be obtained by dividing through by d.

So hereafter, we assume that x, y, z generate the unit ideal in $\mathbb{Z}$. It follows that x, y, z generate the unit ideal in $\mathcal{O}_F$ as well. We work in the ring $\mathcal{O}_F$ throughout the rest of the proof.

Given that $x^\ell - y^\ell = z^\ell$, for $x, y, z \in \mathcal{O}_F$, we find an identity in $\mathcal{O}_F$:

$$\prod_{i=0}^{\ell-1}(x - \zeta^i y) = z^\ell.$$

This may also be interpreted as an equality of principal ideals in $\mathcal{O}_F$:

$$\prod_{i=0}^{\ell-1}(x - \zeta^i y)\mathcal{O}_F = (z\mathcal{O}_F)^\ell.$$

Now, suppose that two ideals $(x - \zeta^i y)\mathcal{O}_F$ and $(x - \zeta^j y)\mathcal{O}_F$ have a common prime ideal factor P. Thus $(x - \zeta^i y) \in P$ and $(x - \zeta^j y) \in P$.

It follows (from subtracting) that $(\zeta^i - \zeta^j)y \in P$. Since P is prime, we find that $(\zeta^i - \zeta^j) \in P$ or $y \in P$. Hence $\pi \in P$ or $y \in P$.

Similarly, by considering $\zeta^{-i}(x - \zeta^i y) - \zeta^{-j}(x - \zeta^j y)$, we find that $(\zeta^{-i} - \zeta^{-j})x \in P$. It follows that $\pi \in P$ or $x \in P$. To summarize, either $\pi \in P$ or $x, y \in P$. Of course, if $x, y \in P$, then $z \in P$. This contradicts our assumption that x, y, z generate the unit ideal in $\mathcal{O}_F$.

We have proven that, if two ideals $(x - \zeta^i y)\mathcal{O}_F$ and $(x - \zeta^j y)\mathcal{O}_F$ have a common prime ideal factor P, then $\pi \in P$; it follows that $P = \pi\mathcal{O}_F$. In this case, we find that $P = \pi\mathcal{O}_F$ is a prime factor of $(z\mathcal{O}_F)$. Therefore $z \in (\pi\mathcal{O}_F) \cap \mathbb{Z} = \ell\mathbb{Z}$, and we are done.

It remains to prove the theorem when the ideals $(x - \zeta^i)\mathcal{O}_F$ (for $0 \leq i \leq \ell - 1$) are pairwise relatively prime. In this case, let the prime factorization of $z\mathcal{O}_F$ be given by

$$z\mathcal{O}_F = P_1^{e_1} \cdots P_t^{e_t},$$

for distinct prime ideals $P_1, \ldots, P_t$ in $\mathcal{O}_F$. Then, after reordering, we find that the prime factorization of $(x - \zeta^i y)\mathcal{O}_F$ is given by

$$(x - \zeta^i y)\mathcal{O}_F = P_1^{\ell e_1} \cdots P_s^{\ell e_s},$$

for some $0 \leq s \leq t$. Let $I = P_1^{e_1} \cdots P_s^{e_s}$. Then we find that I^ℓ is a principal ideal in $\mathcal{O}_F$. Since ℓ does not divide the order of the group $\mathcal{H}(F)$, this implies that I itself is principal: $I = (w_i)$ for some $w_i \in \mathcal{O}_F$. We find that for all $0 \leq i \leq \ell - 1$, there exists $\omega_i \in \mathcal{O}_F$ such that:

$$(x - \zeta^i y)\mathcal{O}_F = \omega_i^\ell \mathcal{O}_F.$$

Hence there exist units u_i such that

$$x - \zeta^i y = u_i \omega_i^\ell.$$

We now "reduce mod ℓ". Observe that every element of $\mathcal{O}_F$ is congruent to an element of $\mathbb{Z}$, modulo $\pi = \zeta - 1$; it follows that every ℓ^{th} power in $\mathcal{O}_F$ is congruent to an element of $\mathbb{Z}$, modulo $\ell\mathcal{O}_F$. In particular, ω_i^ℓ is congruent to an integer w_i, modulo $\ell\mathcal{O}_F$:

$$x - \zeta^i y \equiv u_i w_i, \text{ modulo } \ell\mathcal{O}_F.$$

Recall now that if u is a unit in $\mathcal{O}_F^\times$, then $u = \zeta^r v$ for some integer $0 \leq r < \ell - 1$ and some unit $v \in \mathcal{O}_{F^+}^\times$. Considering $i = 1$, and omitting subscripts accordingly, we find that:

$$x - \zeta y \equiv \zeta^r v w, \text{ and } x - \zeta^{-1} y \equiv \zeta^{-r} v w, \text{ modulo } \ell\mathcal{O}_F.$$

Identifying vw in both equalities, we find that

$$\zeta^{-r} x - \zeta^{1-r} y = \zeta^r x - \zeta^{r-1} y.$$

Simplifying, by multiplying through by ζ^r,

$$x - \zeta y - \zeta^{2r} x + \zeta^{2r-1} y = 0.$$

Now, we have three possibilities to consider, depending on whether the coefficients $1, \zeta, \zeta^{2r}, \zeta^{2r-1}$ are distinct elements of $\mathcal{O}_F$:

All distinct: If the elements $1, \zeta, \zeta^{2r}, \zeta^{2r-1}$ are all distinct, then since $\ell > 5$, we find that the set $\{1, \zeta, \zeta^{2r}, \zeta^{2r-1}\}$ is $\mathbb{Z}$-linearly independent in $\mathcal{O}_F = \mathbb{Z}[\zeta]$. Thus we find a contradiction, since $x, y \in \mathbb{Z}$.

$1 = \zeta^{2r}$**:** If $1 = \zeta^{2r}$, then we find that $\zeta(1 - \zeta^{-1})y = 0$. It follows that $y \in \pi\mathcal{O}_F \cap \mathbb{Z} = \ell\mathbb{Z}$. Hence ℓ divides y.

$1 = \zeta^{2r-1}$**:** If $1 = \zeta^{2r-1}$, then we find that $(1 - \zeta)(x + y) = 0$. It follows that $x + y \in \pi\mathcal{O}_F \cap \mathbb{Z} = \ell\mathbb{Z}$. Hence x is congruent to y, modulo ℓ. Since $x^\ell - y^\ell = z^\ell$, it follows that ℓ divides z.

$\zeta = \zeta^{2r-1}$**:** If $\zeta = \zeta^{2r-1}$, then $(1 - \zeta^2)x = 0$. Hence $x \in \pi\mathcal{O}_F \cap \mathbb{Z} = \ell\mathbb{Z}$. Hence ℓ divides x.

As such coincidences include all possible equalities among elements $1, \zeta, \zeta^{2r}, \zeta^{2r-1}$, we find in all possible cases that ℓ divides xyz.

□

6.5 *Exercises*

Exercise 6.1 *Write down the cyclotomic polynomial* $\Phi_{12}(X)$.

Exercise 6.2 *Let* ζ *be a primitive* 7^{th} *root of unity and let* $F = \mathbb{Q}(\zeta)$. *What is the minimal polynomial of* $\zeta + \zeta^{-1}$*? Can you determine* $\mathcal{O}_{F^+}$*?*

Exercise 6.3 *Suppose that* ζ *is a primitive* ℓ^{th} *root of unity, for an odd prime number* ℓ. *Prove that the cyclotomic field* $\mathbb{Q}(\zeta)$ *has a unique subfield* K *such that* $[K : \mathbb{Q}] = 2$. *Challenge: identify this field* K *explicitly.*

Exercise 6.4 *Suppose that* ℓ *is an odd prime number, and* ζ *is a primitive* $(\ell^d)^{th}$ *root of unity. Let* $G = \mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$. *Let* $H = \{g \in G : g^{\ell-1} = 1\}$. *Prove that* H *has order* $\ell - 1$, *and thus* $\mathbb{Q}(\zeta)$ *contains a subfield* M *such that* $[M : \mathbb{Q}] = \ell^{d-1}$. *Challenge: prove that if* C *is a finite cyclic group, then there exists a Galois extension of* $\mathbb{Q}$ *with Galois group isomorphic to* C.

Exercise 6.5 *Prove the first case of Fermat's last theorem, for* $\ell = 3$ *and* $\ell = 5$. *In other words, prove that if* $x^\ell + y^\ell = z^\ell$, *then* ℓ *divides* xyz. *Hint: Consider the cubes, modulo* 9, *and the fifth powers, modulo* 25.

7
Valued fields

Much of our analysis of number fields has followed from embedding the number field into the real or complex numbers. After this embedding, we may apply our knowledge of geometry and analysis (computing volumes, for example), to study the number field within a real or complex vector space.

There are other fields which, like the real or complex numbers, possess topological and analytic structure; the most important ones for number theory are the p-adic fields. By embedding into p-adic fields, we will be able to exploit geometry and analysis in these fields to obtain results about number fields.

We present the general theory of valuations on fields in this chapter, a theory which encompasses both real numbers and p-adic numbers. By classifying these valuations on number fields, we justify the central role of p-adic valuations in later chapters.

Much of the material in this chapter, including of course Ostrowski's theorem, owes a great deal to the original work of Ostrowski from 1916[1].

[1] Alexander Ostrowski. Über einige Lösungen der Funktionalgleichung $\psi(x) \cdot \psi(x) = \psi(xy)$. *Acta Math.*, 41(1): 271–284, 1916. ISSN 0001-5962

7.1 Valuations

Let F be any field, for the moment. The following is an abstraction of the idea of "absolute value" on F:

Definition 7.1 *A **valuation**[2] on F is a function $|\cdot| \colon F \to \mathbb{R}$, which is*

Multiplicative $|xy| = |x| \cdot |y|$, *for all $x, y \in F$.*

Positive-definite $|x| \geq 0$, *for all $x \in F$, and $|x| = 0$ if and only if $x = 0$.*

Metric $|x + y| \leq |x| + |y|$, *for all $x, y \in F$.*

*A pair consisting of a field F, together with a valuation $|\cdot|$ on F, is called a **valued field**.[3] Often one just says that F is a valued field, if the valuation is to be understood, and written with the standard notation.*

[2] The term valuation is used differently by different authors, and in different contexts. In commutative ring theory, one often works with "valuation rings". The valuations discussed there are different from our valuations; in some cases, valuations on rings are logarithms of the valuations we study here.

[3] Some authors use the term "valued field" only to refer to nonarchimedean valued fields, which we introduce momentarily.

An immediate consequence of this definition is the following:

Proposition 7.2 *Let $|\cdot|$ be a valuation on a field F. Then the valuation restricts to a group homomorphism from $F^\times$ to the group $\mathbb{R}^\times_{pos}$ of positive real numbers under multiplication. For every $\epsilon \in \mu(F)$, $|\epsilon| = 1$.*

PROOF: The fact that $|xy| = |x| \cdot |y|$ implies that the valuation defines a group homomorphism from $F^\times$ to the group $\mathbb{R}^\times$. Since all valuations are non-negative, its image lies in $\mathbb{R}^\times_{pos}$.

If $\epsilon \in \mu(F)$ is a root of unity, then we find that $\epsilon^n = 1$ for some positive integer n. It follows that $|\epsilon|^n = 1$ in $\mathbb{R}^\times_{pos}$. Since the only positive root of unity in $\mathbb{R}$ is 1, we find that $|\epsilon| = 1$.

□

There is a surprising dichotomy among valuations, suggested by the following

Definition 7.3 *Let $|\cdot|$ be a valuation on a field F. It is called **archimedean** if for all $x, y \in F^\times$, there exists an integer[4] n such that $|nx| > |y|$.*

*The valuation is called **nonarchimedean** if for all $x, y \in F$, the following **ultrametric** triangle inequality is satisfied:*

$$|x + y| \leq \max\{|x|, |y|\}.$$

[4] Here, we are viewing any integer n as an element of F, via the unique "characteristic" ring homomorphism from $\mathbb{Z}$ to F.

Lemma 7.4 *If F is an archimedean valued field, then the set $\{|n| : n \in \mathbb{Z}\}$ is unbounded in $\mathbb{R}$. If F is a nonarchimedean valued field, then the set $\{|n| : n \in \mathbb{Z}\}$ is bounded by 1. In particular, a valued field cannot be both archimedean and nonarchimedean.*

PROOF: First, suppose that F is an archimedean valued field. Then there exists an integer n such that

$$|n| = |n \cdot 1| > |1| = 1.$$

It follows that the sequence $|n^k| = |n|^k$ is unbounded, for positive integers k.

Next, suppose that F is a nonarchimedean valued field. Then the ultrametric triangle inequality implies that for every positive integer n,

$$|n| = |1 + (n-1)| \leq \max\{1, |n-1|\}.$$

By induction, we find that $|n| \leq 1$ for all positive integers n. Since $|-1| = 1$ and $|0| = 0$, we find that $|n| \leq 1$ for all integers n.

□

With this lemma in place, we can prove the following dichotomy:

Proposition 7.5 *Suppose that F is a field with valuation $|\cdot|$. Then the valuation is either archimedean or nonarchimedean.*

PROOF: Suppose first that $|\cdot|$ is **not** archimedean[5]. It follows that there exist $x, y \in F^\times$, such that $|nx| \leq |y|$, for all $n \in \mathbb{Z}$. It follows that $|n| \leq |x^{-1}y|$ for all $n \in \mathbb{Z}$. In other words, the absolute values $|1|, |2|, \ldots$ are bounded by some nonzero constant M.

Suppose, without loss of generality, that $|x| \geq |y|$. Then we find that

$$\begin{aligned}
|x+y| &= \sqrt[n]{|x+y|^n} \\
&= \sqrt[n]{|(x+y)^n|} \\
&= \sqrt[n]{|x^n + nx^{n-1}y + \cdots nxy^{n-1} + y^n|} \\
&\leq \sqrt[n]{|x^n| + |y^n| + M(n-1)|x|^n} \\
&\leq \sqrt[n]{(2 + M(n-1))|x|^n} \\
&= \sqrt[n]{2 + M(n-1)} \cdot |x|.
\end{aligned}$$

We find that $|x+y|$ is a real number, bounded above by $\sqrt[n]{2 + M(n-1)} \cdot |x|$, for all positive integers n. Since the sequence $\sqrt[n]{2 + M(n-1)}$ approaches 1, as n grows large, we find that $|x+y| \leq (1+\epsilon)|x|$ for all positive real numbers ϵ. Hence

$$|x+y| \leq |x| = \max\{|x|, |y|\}.$$

□

With the previous lemma in mind, we find that

Corollary 7.6 *A valued field is archimedean if and only if the set* $\{|n| : n \in \mathbb{Z}\}$ *is unbounded.*

7.2 Completion

When F is a valued field, it has a natural Hausdorff topology induced by the metric $d(x,y) = |x-y|$. If $x \in F$, and $0 < r \in \mathbb{R}$, we write $D(x,r)$ for the "open disc" in F:

$$D(x,r) = \{y \in F : |x-y| < r\}.$$

Such discs form a basis for the topology on F.

In order to see that the topology on F is "compatible" with the field structure, it is important to see the effect of addition, subtraction, multiplication, and [in a field]inversion (the map $x \mapsto x^{-1}$ on $F^\times$) on discs.

Lemma 7.7 *Suppose that* $x_1, x_2 \in F$, *and* $0 < r_1, r_2 \in \mathbb{R}$. *Then*

$$D(x_1, r_1) \pm D(x_2, r_2) \subset D(x_1 \pm x_2, r_1 + r_2).$$

[5] Note here that the condition "not archimedean" does not yet imply "nonarchimedean". That is the conclusion of the proposition.

PROOF: If $y_1 \in D(x_1, r_1)$ and $y_2 \in D(x_2, r_2)$, then we find that

$$\begin{aligned} |(y_1 \pm y_2) - (x_1 \pm x_2)| &= |(y_1 - x_1) \pm (y_2 - x_2)| \\ &\leq |y_1 - x_1| + |y_2 - x_2| \\ &< r_1 + r_2. \end{aligned}$$

Lemma 7.8 *Suppose that $x_1, x_2 \in F$, and $0 < r_1, r_2 \in \mathbb{R}$, and $|x_1|, |x_2| < R$. Then*

$$D(x_1, r_1) \cdot d(x_2, r_2) \subset D(x_1 x_2, R(r_1 + r_2) + r_1 r_2).$$

PROOF: If $y_1 \in D(x_1, r_1)$ and $y_2 \in D(x_2, r_2)$, then we find that

$$\begin{aligned} |(y_1 \cdot y_2) - (x_1 \cdot x_2)| &= |y_1 y_2 - y_1 x_2 + y_1 x_2 - x_1 x_2| \\ &= |y_1(y_2 - x_2) + x_2(y_1 - x_1)| \\ &\leq |y_1||y_2 - x_2| + |x_2||y_1 - x_1| \\ &< (R + r_1)(r_2) + (R)(r_1) \\ &= R(r_1 + r_2) + r_1 r_2. \end{aligned}$$

□

Lemma 7.9 *Suppose that $x \in F^\times$ and $0 < r \in \mathbb{R}$, and $R_{min} < |x|$. Also, suppose that $r < R_{min}$. Then*

$$D(x, r)^{-1} \subset D(x^{-1}, r R_{min}^{-1} (R_{min} - r)^{-1}).$$

PROOF: If $y \in D(x, r)$, then observe first that

$$|y| + |x - y| \geq |x| > R_{min}.$$

It follows that $|y| > R_{min} - r > 0$, and so $y \in F^\times$.

Continuing, we find that

$$\begin{aligned} |y^{-1} - x^{-1}| &= |x - y||x^{-1} y^{-1}| \\ &< r \cdot |x|^{-1} \cdot |y|^{-1} \\ &< r \cdot R_{min}^{-1} \cdot |y|^{-1} \\ &< r \cdot R_{min}^{-1} \cdot (R_{min} - r)^{-1}. \end{aligned}$$

□

One construction of the real numbers uses Cauchy sequences. For a general valuation on a field F, we define these by

Definition 7.10 *Suppose that $(a_i)_{i=0}^{\infty}$ is a sequence of elements of a valued field F. It is called a **Cauchy sequence** if for every real[6] $\epsilon > 0$, there exists N such that $n, m \geq N$ implies that $|a_n - a_m| < \epsilon$.*

*A valued field F is called **complete** if every Cauchy sequence in F converges to some element of F.*

[6] If one wishes to use Cauchy sequences to define the real numbers, this definition is circular, at least on the surface. However, one may restrict to $0 < \epsilon \in \mathbb{Q}$, and only consider rational-valued valuations as well, if one wishes to use Cauchy sequences to define the real numbers from the rationals.

An important first observation about Cauchy sequences in a valued field is the following

Lemma 7.11 *If (a_i) is a Cauchy sequence in a valued field F, then the sequence $|a_i|$ is a Cauchy sequence in $\mathbb{R}$. It follows that there exists a real number α such that $|a_i| \to \alpha$.*

PROOF: For all $\epsilon > 0$, there exists N such that $n, m \geq N$ implies that $|a_n - a_m| < \epsilon$. It follows that for all $n, m \geq N$.

$$\begin{aligned} |a_n| - |a_m| &\leq |a_n - a_m + a_m| - |a_m| \\ &\leq |a_n - a_m| + |a_m| - |a_m| \\ &\leq \epsilon. \end{aligned}$$

Thus the sequence $(|a_i|)$ is a Cauchy sequence in $\mathbb{R}$.

□

Fortunately, in a valued field, sums, products, and often inverses of Cauchy sequences are again Cauchy sequences.

Lemma 7.12 *Suppose that $(a_i), (b_i)$ are Cauchy sequences in a valued field F. Then $(a_i \pm b_i)$ and $(a_i b_i)$ are Cauchy sequences in F.*

PROOF: Let ϵ be a positive real number. Let N be sufficiently large so that

$$|a_n - a_m| < \epsilon/2 \text{ and } |b_n - b_m| < \epsilon/2,$$

for all $n, m \geq N$. Then we find that

$$a_n \pm b_n \in D(a_m, \epsilon/2) \pm D(b_m, \epsilon/2) \subset D(a_m \pm b_m, \epsilon).$$

It follows directly that $(a_i \pm b_i)$ is a Cauchy sequence in F.

Now consider the elements $\alpha, \beta \in \mathbb{R}$ such that $|a_i| \to \alpha$ and $|b_i| \to \beta$. Let R be a real number greater than $\max\{\alpha, \beta\}$. Let δ be any positive real number satisfying

$$2R\delta + \delta^2 < \epsilon.$$

Let M be sufficiently large so that

$$|a_n - a_m| < \delta, \text{ and } |b_n - b_m| < \delta,$$

and $|a_n| < R$ and $|b_n| < R$, for all $n, m \geq M$. Then we find that

$$a_n \cdot b_n \in D(a_m, \delta) \cdot D(b_m, \delta) \subset D(a_m b_m, 2R\delta + \delta^2) \subset D(a_m b_m, \epsilon).$$

It follows directly that $(a_i \cdot b_i)$ is a Cauchy sequence in F.

□

Lemma 7.13 *Suppose that (a_i) is a Cauchy sequence in a valued field F. Suppose moreover that $a_i \neq 0$ for all i and $|a_i|$ does not approach 0, as $i \to \infty$. Then (a_i^{-1}) is a Cauchy sequence in F.*

PROOF: Let ϵ be a positive real number, and let α be the positive real number such that $|a_i| \to \alpha$. Let R_{min} be any real number satisfying $0 < R_{min} < \alpha$. Let δ be a positive real number satisfying

$$\delta R_{min}^{-1}(R_{min} - \delta)^{-1} < \epsilon.$$

Let N be sufficiently large so that

$$|a_n - a_m| < \delta, \text{ and } R_{min} < |a_n|,$$

for all $m, n \geq N$. Then we find that

$$a_n^{-1} \in D(a_m, \delta)^{-1} \subset D(a_m^{-1}, \delta R_{min}^{-1}(R_{min} - \delta)^{-1}) \subset D(a_m^{-1}, \epsilon).$$

It follows that (a_i^{-1}) is a Cauchy sequence in F.

□

Just as one may construct the real numbers as the set of equivalence classes of Cauchy sequences of rational numbers, one may "complete" any valued field by considering Cauchy sequences modulo "null sequences".

Definition 7.14 *If F is a valued field, then a **null sequence** in F is a Cauchy sequence (a_i) in F such that $|a_i| \to 0$.*

We are now prepared to prove

Proposition 7.15 *Suppose that F is a valued field. Then, there exists a complete valued field $\hat{F}$ containing F (the valuation on $\hat{F}$ restricting to that on F), such that F is dense in $\hat{F}$. Such a complete valued field $\hat{F}$ is called a **completion** of F.*

PROOF: Let R be the set of all Cauchy sequences (a_I) of elements of F. This set forms a ring, by termwise addition and multiplication; this assertion requires the previous analytic lemmas to prove that the sum, difference, and product of Cauchy sequences is a Cauchy sequence.

Let N be the subset of R consisting of null sequences. We claim that the ideal N is maximal; indeed, suppose that $(a_i) \in R \backslash N$. Then $|a_i| \to \alpha$ for some real number $\alpha > 0$. Since (a_i) is Cauchy, there exists an integer M, such that $a_i \neq 0$ for all $i \geq M$.

Let $\tilde{a}_i = a_i$, if $i \geq M$, and let $\tilde{a}_i = 1$ if $0 \leq i < M$. Thus, we find that $(\tilde{a}_i)$ is a Cauchy sequence, not a null sequence, and every term is

invertible. It follows (from a previous lemma) that $(b_i) = (\tilde{a}_i^{-1})$ is a Cauchy sequence. Furthermore, in the ring R,

$$(a_i) \cdot (b_i) - (1) \in N.$$

Indeed, $a_i b_i - 1 = 0$ for all $i \geq M$.

Thus, every sequence in $R \backslash N$ is invertible, modulo N. Hence N is a maximal ideal. Define $\hat{F} = R/N$.

We now claim that $\hat{F}$ is a complete valued field containing F as a dense subfield. Indeed, $\hat{F}$ is a field, defined as the quotient of a ring by a maximal ideal. F embeds as a subfield of $\hat{F}$, by associating to an element $x \in F$ the constant sequence (x). If $(a_i) \in R$, then we may define

$$|(a_i)| = \lim_{i \to \infty} |a_i|,$$

since this limit converges by the completeness of $\mathbb{R}$. We leave it to the reader to check that this makes $\hat{F}$ a valued field, containing F as a valued subfield (i.e., the valuation on F is the restriction of that on $\hat{F}$.

The completeness of $\hat{F}$ follows from a "diagonal argument", using a Cauchy sequence of Cauchy sequences. The density of F in $\hat{F}$ follows from the fact that every Cauchy sequence in F converges to an element of $\hat{F}$.

□

The completion $\hat{F}$ satisfies the following universal property.

Proposition 7.16 *Let F be a valued field, and K be any complete valued field. Then, any continuous field homomorphism from F to K factors uniquely through $\hat{F}$.*

Proof: In fact, by the universal property of completions of metric spaces, there is a unique continuous map from $\hat{F}$ to K which restricts to F. One may check directly that this unique map is a field homomorphism, given that $F \to K$ is a field homomorphism.

□

7.3 *Valuations on the rational numbers*

In this section, we prove Ostrowski's theorem, which classifies all of the valuations on $\mathbb{Q}$. We have found a dichotomy among these valuations. Some are archimedean, and some are nonarchimedean, depending on whether $|\mathbb{Z}|$ is bounded or unbounded.

It will be useful to prove strong statements about archimedean and nonarchimedean valuations. These stronger statements rely on the following analytic lemma:

Lemma 7.17 *Suppose that $|\cdot|$ is any valuation on $\mathbb{Q}$, and m, n are positive integers with $n > 1$. Then,*

$$|m| \leq \max\{1, |n|\}^{\log(m)/\log(n)}.$$

PROOF: Consider the expression of m, "base n":

$$m = a_0 + a_1 n + \cdots a_d n^d,$$

where

$$d = \lfloor \log_n(m) \rfloor = \lfloor \frac{\log(m)}{\log(n)} \rfloor$$

and $0 \leq a_i < n$ for all $0 \leq i \leq d$. The triangle inequality implies[7] that $|a_i| \leq a_i < n$, for all $0 \leq i \leq d$. It follows that

$$\begin{aligned} |m| &= |a_0 + a_1 n + \cdots a_d n^d| \\ &\leq (d+1) n \max\{1, |n|\}^d \\ &\leq \left(1 + \frac{\log(m)}{\log(n)}\right) n \max\{1, |n|\}^{\frac{\log(m)}{\log(n)}}. \end{aligned}$$

Carrying out this estimate with m^t instead of m, for t a positive integer, yields

$$|m^t| \leq \left(1 + t\frac{\log(m)}{\log(n)}\right) n \max\{1, |n|\}^{t\frac{\log(m)}{\log(n)}}.$$

Taking t^{th} roots of both sides yields

$$|m| \leq \sqrt[t]{n\left(1 + t\frac{\log(m)}{\log(n)}\right)} \max\{1, |n|\}^{\frac{\log(m)}{\log(n)}}.$$

As t approaches infinity, the quantity still under the t^{th} root above approaches 1. It follows that

$$|m| \leq \max\{1, |n|\}^{\log(m)/\log(n)}.$$

□

Corollary 7.18 *Suppose that $|\cdot|$ is a valuation on $\mathbb{Q}$, $n > 1$ is an integer, and $|n| \leq 1$. Then the valuation is nonarchimedean.*

PROOF: Suppose that $m > 1$ is an integer. Then, the previous lemma implies that

$$|m| \leq \max\{1, |n|\}^{\log(m)/\log(n)} = 1^{\log(m)/\log(n)} = 1.$$

It follows that the valuation is bounded on $\mathbb{Z}$, and hence nonarchimedean.

□

[7] Here, we use the fact that

$$|1 + \cdots + 1| \leq |1| + \cdots + |1|,$$

with the same number of terms on both sides.

Proposition 7.19 *Suppose that $|\cdot|$ is an archimedean valuation on $\mathbb{Q}$. Let $|\cdot|_{\mathbb{R}}$ denote the usual absolute value on $\mathbb{Q}$. Then there exists a positive real number $0 < \alpha \leq 1$, such that $|x| = |x|_{\mathbb{R}}^{\alpha}$ for all $x \in \mathbb{Q}$.*

Proof: Since $|\cdot|$ is an archimedean valuation, it follows that $|n| > 1$ for all integers $n > 1$. For any integer $m > 1$, we find that

$$|m| \leq |n|^{\log(m)/\log(n)}, \text{ and } |n| \leq |m|^{\log(n)/\log(m)}.$$

It follows that

$$|m|^{1/\log(m)} \leq |n|^{1/\log(n)} \text{ and } |n|^{1/\log(n)} = |m|^{1/\log(m)}.$$

Hence we find that there exists a real constant $\beta > 1$ such that $|m|^{1/\log(m)} = \beta$ for all integers $m > 1$. It follows that

$$|m| = \beta^{\log(m)} = |m|_{\mathbb{R}}^{\alpha},$$

where $\alpha = \log(\beta) > 0$. Since $\mathbb{Q}^{\times}$ is generated by the set of integers $m > 1$, it follows that for all $q \in \mathbb{Q}$,

$$|q| = |q|_{\mathbb{R}}^{\alpha}.$$

Finally, the triangle inequality implies that

$$2^{\alpha} = |1+1| \leq |1| + |1| = 2.$$

Hence $0 < \alpha \leq 1$.

□

This proposition classifies all of the archimedean valuations on $\mathbb{Q}$; any such valuation must equal $|\cdot|_{\mathbb{R}}^{\alpha}$ for some $0 < \alpha \leq 1$. Conversely, we have

Proposition 7.20 *If $0 < \alpha \leq 1$, then $|\cdot|_{\mathbb{R}}^{\alpha}$ is an archimedean valuation on $\mathbb{Q}$.*

Proof: The facts that $|\cdot|_{\mathbb{R}}^{\alpha}$ is multiplicative, and positive-definite, follow quickly from the corresponding facts about $|\cdot|_{\mathbb{R}}$. For the triangle inequality, observe that the convexity of the positive real-valued function $x \mapsto x^{\alpha}$ implies that

$$|x+y|_{\mathbb{R}}^{\alpha} \leq |x|_{\mathbb{R}}^{\alpha} + |y|_{\mathbb{R}}^{\alpha},$$

for all $x, y \in \mathbb{Q}$.

□

From this proposition, we may classify all of the continuous valuations on $\mathbb{R}$ and $\mathbb{C}$:

Proposition 7.21 *Suppose that $|\cdot|$ is a continuous valuation on $\mathbb{R}$ or $\mathbb{C}$. Then, there exists a real number α such that $0 < \alpha \leq 1$, and $|x| = |x|_{\mathbb{R}}^{\alpha}$ or $|x|_{\mathbb{C}}^{\alpha}$ accordingly.*

Proof: Given that $|\cdot|$ is a continuous valuation on $\mathbb{R}$, it is completely determined by its values on the dense subset $\mathbb{Q}$. We claim that $|\cdot|$ is an archimedean valuation. It cannot be the trivial valuation, since this valuation is clearly not continuous[8] as a function from $\mathbb{R}$ to $\mathbb{R}$.

[8] Recall that the trivial valuation "jumps" from 1 to 0 at 0.

Indeed, if it were nonarchimedean and nontrivial, then there would exist a positive integer n such that $|n| < 1$. In this case, we find that the sequence $|n^{-k}|$ is unbounded. However, the sequence n^{-k} approaches zero in the usual topology of $\mathbb{R}$, and hence $|n^{-k}|$ must approach $|0| = 0$ in $\mathbb{R}$, a contradiction.

Thus the continuous valuation on $\mathbb{R}$ restricts to an archimedean valuation on $\mathbb{Q}$, which must be $|\cdot|_{\mathbb{R}}^{\alpha}$ for some $0 < \alpha \leq 1$. As the continuous valuation on $\mathbb{R}$ is uniquely determined by its restriction to the dense set $\mathbb{Q}$, this classifies the continuous valuations on $\mathbb{R}$.

Now, if $|\cdot|$ is a continuous valuation on $\mathbb{C}$, then it restricts to a continuous valuation on $\mathbb{R}$. Hence $|x| = |x|_{\mathbb{R}}^{\alpha}$ for some $0 < \alpha \leq 1$. Furthermore, it can be checked that the set $\mu(\mathbb{C}) \cdot \mathbb{R}$ is dense in $\mathbb{C}$. Since, for any valuation on $\mathbb{C}$, $|\mu(F)| = \{1\}$, we find that $|x| = |x|_{\mathbb{C}}^{\alpha}$ for all $x \in \mathbb{C}$.

□

The nonarchimedean valuations cannot be related directly to the usual absolute value. But we begin their study with the following

Lemma 7.22 *Suppose that $|\cdot|$ is a nonarchimedean valuation on $\mathbb{Q}$. Let I be the set of integers n, for which $|n| < 1$. Then I is a prime ideal in $\mathbb{Z}$.*

Proof: Since $|\cdot|$ is a nonarchimedean valuation on $\mathbb{Q}$, we have seen that $|\mathbb{Z}|$ is bounded by 1. It follows directly that I is an ideal in $\mathbb{Z}$. Furthermore, if $a, b \in \mathbb{Z}$, and $ab \in I$, then we find that $|ab| = |a| \cdot |b| < 1$. It follows directly that $a \in I$ or $b \in I$. Hence I is a prime ideal.

□

This lemma suggests that we classify nonarchimedean valuations on $\mathbb{Q}$ by their associated prime ideals in $\mathbb{Z}$. If this associated prime ideal is the zero ideal, then $|n| = 1$ for all nonzero integers n. This implies that $|q| = 1$ for all nonzero $q \in \mathbb{Q}$. Thus, if the associated prime ideal is the zero ideal, then the valuation is the **trivial valuation** on $\mathbb{Q}$.

If, on the other hand, the associated prime ideal is a nonzero ideal, then it is a prime ideal (p) for some prime number p. In this case, we say that the valuation is a **p-adic valuation**. Such valuations may also be completely described.

Recall that any nonzero rational number x has a unique decomposition into powers of primes:

$$x = \prod_p p^{e_p},$$

where p ranges over the set of prime numbers, $e_p \in \mathbb{Z}$, and all but finitely many e_p are equal to zero. The constant e_p is also called $\mathrm{ord}_p(x)$, the **order** of x at p. The quantity $p^{\mathrm{ord}_p(x)}$ is called the **p-part** of x. If $x = 0$, we define $\mathrm{ord}_p(x) = -\infty$ so that the p-part of 0 is 0.

Proposition 7.23 *Suppose that $|\cdot|$ is a p-adic valuation. Then there exists a real number α such that $0 < \alpha < \infty$, and such that*

$$|x| = p^{-\alpha\,\mathrm{ord}_p(x)}.$$

Proof: Since $|\cdot|$ is a p-adic valuation, we find that $|q| = 1$ for all prime numbers $q \neq p$. It follows that, if x is a rational number (decomposed into prime powers), then the valuation of x is equal to the valuation of its p-part:

$$|x| = |p^{ord_p(x)}|.$$

Furthermore, this valuation depends only upon $|p|$, which must be a real number β such that $0 < \beta < 1$:

$$|x| = \beta^{ord_p(x)}.$$

Letting $\alpha = -\log_p(\beta) = -\log(\beta)/\log(p)$, we find that

$$|x| = p^{-\alpha\,\mathrm{ord}_p(x)}$$

and $0 < \alpha < \infty$.

□

Setting $\alpha = 1$ in the previous proposition, we are led to consider the standard p-adic valuation:

$$|x|_p = p^{-\,\mathrm{ord}_p(x)},$$

for which every p-adic valuation $|\cdot|$ satisfies $|x| = |x|_p^\alpha$ for $0 < \alpha < \infty$. At this point, it is perhaps important to observe that

Proposition 7.24 *For every positive[9] real number α, the function $|\cdot|_p^\alpha$ is a valuation on $\mathbb{Q}$.*

Proof: The facts that $|\cdot|_p^\alpha$ is multiplicative, and positive-definite, follow quickly from the corresponding facts about $|\cdot|_p$. For the

[9] This should be contrasted with the archimedean case, where only powers of the standard valuation between 0 and 1 occur in valuations.

triangle inequality, observe that $|\cdot|_p$ satisfies the stronger *ultrametric* triangle inequality:

$$|x+y|_p \leq \max\{|x|_p, |y|_p\},$$

for all x and y in $\mathbb{Q}$. Indeed, if $\operatorname{ord}_p(x) = m$ and $\operatorname{ord}_p(y) = n$, then $x = p^m x_0$ and $y = p^n y_0$ for rational numbers x_0, y_0 which are "p-free", i.e., have no p in their numerator or denominator. Without loss of generality, suppose that $m < n$. Then we find that

$$x + y = p^m(x_0 + p^e y_0),$$

for some non-negative integer e. Thus we find that

$$\operatorname{ord}_p(x+y) \geq \max\{\operatorname{ord}_p(x), \operatorname{ord}_p(y)\}.$$

The ultrametric triangle inequality follows:

$$|x+y|_p = p^{-\operatorname{ord}_p(x+y)} \leq \max\{p^{-\operatorname{ord}_p(x)}, p^{-\operatorname{ord}_p(y)}\} = \max\{|x|_p, |y|_p\}.$$

Now, after taking α powers, we find that

$$|x+y|_p^\alpha \leq \max\{|x|_p^\alpha, |y|_p^\alpha\}.$$

Since the ultrametric triangle inequality is satisfied, we find that $|\cdot|_p^\alpha$ is a valuation.

□

We have now proven the following

Theorem 7.25 (Ostrowski) *Suppose that $|\cdot|$ is a valuation on $\mathbb{Q}$. Then, this valuation is one of the following:*

Trivial: $|x| = 1$ *for all nonzero $x \in \mathbb{Q}$, and $|0| = 0$.*

p-adic: *There exists a prime number p, and a positive real number α, such that*

$$|x| = |x|_p^\alpha = p^{-\alpha \operatorname{ord}_p(x)}.$$

Real: *There exists a real number α, such that $0 < \alpha \leq 1$ and*

$$|x| = |x|_{\mathbb{R}}^\alpha.$$

Within each family of valuations on $\mathbb{Q}$, we have chosen a representative

$$|x|_p = p^{-\operatorname{ord}_p(x)}, \text{ and } |x|_{\mathbb{R}},$$

which is normalized in a somewhat special way. One motivation for this normalization is the following:

Proposition 7.26 (Product Formula) *For any $x \in \mathbb{Q}$,*

$$|x|_{\mathbb{R}} \cdot \prod_p |x|_p = 1.$$

PROOF: The proof is a quick computation. If $x \in \mathbb{Q}$, then x has a canonical decomposition

$$x = \pm \prod_p p^{\mathrm{ord}_p(x)} = \pm \prod_p |x|_p^{-1}.$$

It follows that

$$|x|_{\mathbb{R}} = \prod_p |x|_p^{-1}.$$

The product formula follows directly.

□

7.4 *Valuations on number fields*

In the last section, we classified valuations on $\mathbb{Q}$. From this classification, one may classify valuations on any number field F. For the purposes of classification, one should note that any valuation on F restricts to one on $\mathbb{Q}$, on which it is trivial, p-adic, or real.

We begin with the archimedean valuations on F.

Proposition 7.27 *Suppose that F is a number field. If $|\cdot|$ is an archimedean valuation on F, then there exists an embedding $\sigma\colon F \to \mathbb{C}$, and a real number $0 < \alpha \leq 1$, such that:*

$$|x| = |\sigma(x)|_{\mathbb{C}}^{\alpha}, \text{ for all } x \in F.$$

Conversely, the above formula defines a valuation on F, for all such σ and α.

PROOF: If $|\cdot|$ is an archimedean valuation on F, then $|\cdot|$ restricts to an archimedean valuation on $\mathbb{Q}$; by the results of the previous section, we find that

$$|x| = |x|_{\mathbb{R}}^{\alpha},$$

for all $x \in \mathbb{Q}$. Let $\hat{F}$ be the completion of F with respect to the given archimedean valuation. By the universal property of completion, the inclusion of $\mathbb{Q}$ into F extends uniquely to a continuous inclusion of $\hat{\mathbb{Q}} = \mathbb{R}$ into $\hat{F}$. In this way, we find a canonical ring homomorphism:

$$F_{\mathbb{R}} = F \otimes_{\mathbb{Q}} \mathbb{R} \to \hat{F}.$$

Any ring homomorphism from $F_{\mathbb{R}} \cong \mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$ to the field $\hat{F}$ factors through a projection onto $\mathbb{R}$ or $\mathbb{C}$. In this way, we find a sequence of rings and homomorphisms:

$$F \to F_{\mathbb{R}} \to K \to \hat{F},$$

where $K = \mathbb{R}$ or $K = \mathbb{C}$. It follows that the archimedean valuation on F, after extending to $\hat{F}$, restricts to a continuous archimedean valuation on $\mathbb{R}$ or $\mathbb{C}$. Such valuations are all given by powers of the usual absolute value. Since $|x| = |x|_{\mathbb{R}}^{\alpha}$ for $x \in \mathbb{Q}$, we find that

$$|x| = |x|_K^{\alpha},$$

for all $x \in K$. Restricting from K to F yields the desired result.

□

From this proposition, we find that the archimedean places of F correspond bijectively to archimedean valuations on F. If v is an archimedean place of F (so v is an embedding of F into $\mathbb{R}$ or a pair of conjugate embeddings of F into $\mathbb{C}$), we write $|\cdot|_v$ for the resulting archimedean valuation.

For the nonarchimedean valuations, we begin with the following

Proposition 7.28 *Let F be a number field, and $|\cdot|$ a nonarchimedean valuation on F. Then $|x| \leq 1$ for all $x \in \mathcal{O}_F$.*

Proof: We have seen already that $|x| \leq 1$ for all $x \in \mathbb{Z} \subset F$. On the other hand, $\mathcal{O}_F$ is a lattice, and we may choose a $\mathbb{Z}$-basis $\alpha_1, \ldots, \alpha_d$ of $\mathcal{O}_F$ as such. We find that, for all $c_1, \ldots, c_d \in \mathbb{Z}$,

$$\begin{aligned} |\sum_i c_i \alpha_i| &\leq \max\{|c_i \alpha_i|\} \\ &\leq \max\{1 \cdot |\alpha_i|\} \\ &\leq \max\{|\alpha_i|\}. \end{aligned}$$

In this way, we find that $|\mathcal{O}_F|$ is bounded by some positive real constant $C = \max\{|\alpha_i|\}$. If $C > 1$, then we find that $|\alpha_i| > 1$ for some i. But then $|\alpha_i^2| > |\alpha_i|$, and $\alpha_i^2 \in \mathcal{O}_F$, a contradiction. Thus $C \leq 1$.

□

From this proposition, we may easily prove the following

Corollary 7.29 *Let F be a number field, and $|\cdot|$ a nonarchimedean valuation on F. Let I be the set of elements x of $\mathcal{O}_F$ satisfying $|x| < 1$. Then I is a prime ideal in $\mathcal{O}_F$.*

Proof: The proof is precisely the same as for $\mathbb{Z}$.

□

It follows that, to every nonarchimedean valuation on F, one may associate a prime ideal P. If $P = (0)$, then the valuation is trivial. Otherwise, we call the valuation a P-adic valuation. The P-adic valuations on F can be described in much the same way as p-adic valuations on $\mathbb{Q}$, using the factorization theory for fractional ideals.

Consider an element $x \in F^\times$, and the resulting principal fractional ideal $x\mathcal{O}_F$. We have seen that this fractional ideal can be factored, in a unique way, into integer powers of prime ideals

$$(x) = \prod_P P^{e_P}.$$

The resulting exponent of P is called the **order** of x at P: $\mathrm{ord}_p(x) = e_p$ in the above decomposition. If $x = 0$, then we define $\mathrm{ord}_p(x) = -\infty$ as before. The following lemma is influenced by the notes of Keith Conrad [10].

[10]

Lemma 7.30 *Let P be a prime ideal in $\mathcal{O}_F$. If $x \in F^\times$ and $\mathrm{ord}_P(x) \geq 0$, then there exist $\alpha, \beta \in \mathcal{O}_F$ such that $x = \alpha/\beta$, $\mathrm{ord}_P(\alpha) = \mathrm{ord}_P(x)$, and $\mathrm{ord}_P(\beta) = 0$.*

Proof: There exist ideals $I, J \subset \mathcal{O}_F$, such that $x\mathcal{O}_F = I \cdot J^{-1}$, and I and J have no common prime ideal factors. Moreover, since $\mathrm{ord}_P(x) \geq 0$, we find that P is not a prime factor of J, i.e., $J \not\subset P$. Observe that I and J are in the same ideal class, since $I = (x) \cdot J$.

Choose an element $j \in \mathcal{O}_F$ such that $j \in J$ and $j \notin P$. It follows that $(j) \subset J$, so $(j) = JK$ for some integral ideal $K \subset \mathcal{O}_F$. Furthermore, P is not a factor of K, since otherwise $j \in JK \subset P$, a contradiction. Since I and J are in the same ideal class, and $JK = (j)$ is principal, we find that IK is principal $IK = (i)$ for some $i \in \mathcal{O}_F$.

We find that

$$(x) = I \cdot J^{-1} = IK(JK)^{-1} = (i) \cdot (j)^{-1}.$$

Thus $x = \alpha/\beta$, where α and β are unit multiples of i and j. Since $j \notin P$, we find that $\beta \notin P$, so $\mathrm{ord}_P(\beta) = 0$.

□

Lemma 7.31 *Let P be a prime ideal in $\mathcal{O}_F$. If $x \in F^\times$ and $\mathrm{ord}_P(x) = 0$, then $|x| = 1$ for any P-adic valuation.*

Proof: Since $\mathrm{ord}_P(x) = 0$, there exist $\alpha, \beta \in \mathcal{O}_F$ such that $x = \alpha/\beta$, $\mathrm{ord}_P(\alpha) = 0$ and $\mathrm{ord}_P(\beta) = 0$. It follows that $|\alpha| = |\beta| = 1$. Hence $|x| = 1$.

□

Proposition 7.32 *Suppose that $|\cdot|$ is a P-adic valuation on a number field F. Then there exists a real number α such that $0 < \alpha < \infty$ and such that*

$$|x| = \mathrm{N}(P)^{-\alpha\,\mathrm{ord}_P(x)}.$$

PROOF: Begin by fixing an element $\varpi \in P - P^2$ (sometimes called a **uniformizing element**). Thus $|\varpi| < 1$. Then, for any nonzero $x \in \mathcal{O}_F$, we find that

$$\mathrm{ord}_P\left(\frac{x}{\varpi^{\mathrm{ord}_P(x)}}\right) = 0, \text{ and } |\left(\frac{x}{\varpi^{\mathrm{ord}_P(x)}}\right)| = 1.$$

It follows that

$$|x| = |\varpi|^{\mathrm{ord}_P(x)}.$$

Letting $\alpha = -\log_{\mathrm{N}(P)}(|\varpi|)$, we find that $0 < \alpha \in \mathbb{R}$ and

$$|x| = \mathrm{N}(P)^{-\alpha\,\mathrm{ord}_P(x)}.$$

□

We have now proven the analogue of Ostrowski's theorem for number fields:

Theorem 7.33 *Suppose that $|\cdot|$ is a valuation on a number field F. Then, this valuation is one of the following:*

Trivial: *$|x| = 1$ for all nonzero $x \in \mathbb{Q}$, and $|0| = 0$.*

P-adic: *There exists a prime ideal P, and a positive real number α, such that*

$$|x| = |x|_P^\alpha = \mathrm{N}(P)^{-\alpha\,\mathrm{ord}_P(x)}.$$

Archimedean: *There exists a realarchimedean place σ or complex archimedean place $\{\tau, \bar{\tau}\}$ and a real number α, such that $0 < \alpha \leq 1$ and*

$$|x| = |\sigma(x)|_{\mathbb{R}}^\alpha \text{ or } |x| = |\tau(x)|_{\mathbb{C}}^\alpha.$$

7.5 Exercises

Exercise 7.1 *Let $F = \mathbb{Q}(i)$. Let $\lambda = 1 + i \in F$. Prove that (λ) is a prime ideal in $\mathcal{O}_F$. Let $|\cdot|_\lambda$ denote the associated valuation. Compute $|2|$. Compute $|3|$. Compute $|1 - i|$.*

Exercise 7.2 *Let $\mathbb{C}((X))$ be the field of Laurent series with coefficients in $\mathbb{C}$. These are formal series*

$$f = \sum_{i=N}^{\infty} c_i X^i,$$

where N is allowed to be any integer, positive or negative. Define $\mathrm{ord}(f)$ to be the smallest integer i for which c_i is nonzero. Prove that the function $|f| = e^{-\alpha\,\mathrm{ord}(f)}$ defines a nonarchimedean valuation on $\mathbb{C}((X))$ for all positive real numbers α.

Exercise 7.3 *Suppose that p is a prime number, F is a number field, and $(p) = P_1 \cdots P_t$ is the factorization of (p) in $\mathcal{O}_F$. Suppose moreover that the prime ideals $P_1, \ldots, P_t$ are distinct. Suppose that $|\cdot|$ is a valuation on F which restricts to $|\cdot|_p$ on $\mathbb{Q}$. Prove that $|\cdot| = |\cdot|_{P_i}$ for some $1 \leq i \leq t$.*

Exercise 7.4 *Suppose that p is a prime number. Let $x, y \in \mathbb{Q}$. Prove that for all $\epsilon > 0$, there exists an element $z \in \mathbb{Q}$ such that (simultaneously!):*

$$|z - x|_{\mathbb{R}} < \epsilon \text{ and } |z - y|_p < \epsilon.$$

Challenge: Generalize this to simultaneous approximation at any finite number of primes and $\mathbb{R}$.

8
P-adic fields

Let F be a number field, and let P be a prime ideal in $\mathcal{O}_F$. Recall that if $x \in F^\times$, then (x) denotes the principal fractional ideal $x\mathcal{O}_F \subset F$. The integer $\mathrm{ord}_P(x)$ is the power of P occurring in the factorization of (x). The resulting "P-adic absolute value" is defined by

$$|x|_P = \mathrm{N}(P)^{-\mathrm{ord}_P(x)}.$$

This is a nonarchimedean valuation on F.

Recall that $P \cap \mathbb{Z} = p\mathbb{Z}$ is a nonzero prime ideal in $\mathbb{Z}$. It follows that $\mathcal{O}_F/P$ is a finite field extension of $\mathbb{F}_p := \mathbb{Z}/p\mathbb{Z}$. Thus there exists a positive integer f, such that $\mathcal{O}_F/P = \mathbb{F}_q$ is a finite field with $q := p^f$ elements; simply put, $q = \mathrm{N}(P)$.

For this reason, we can rewrite the P-adic absolute value

$$|x|_P = q^{-\mathrm{ord}_P(x)}.$$

In this chapter, we will study the field obtained by completing F with respect to this valuation.

Definition 8.1 *A **p-adic field** is a field which arises as the completion of a number field F with respect to a nonarchimedean valuation associated to a prime ideal $P \subset \mathcal{O}_F$ whose intersection with $\mathbb{Z}$ is $p\mathbb{Z}$.*

The most basic example of a p-adic field is "the field of p-adic numbers", denoted $\mathbb{Q}_p$, which arises by completing $\mathbb{Q}$ with respect to the p-adic absolute value $|x|_p = p^{-\mathrm{ord}_p(x)}$. Though we do not prove it here, the previous definition has an alternative characterization: a p-adic field is a field which is a finite extension of $\mathbb{Q}_p$.

8.1 Systems of Congruences

Let K be the completion of F with respect to the valuation

$$|x|_P = q^{-\mathrm{ord}_P(x)}.$$

An element of K (by definition) is an equivalence class of Cauchy sequences from F, modulo null sequences. K is a field, and the valuation on F extends uniquely to a continuous valuation on K. Since the valuation on $F^\times$ has discrete image in $\mathbb{R}$, we find that the valuation on $K^\times$ also has discrete image. If $x \in K^\times$, then $|x| \in q^{\mathbb{Z}}$.

Definition 8.2 *A **uniformizing element** in K is some element $\varpi \in K^\times$, such that $|\varpi| < 1$, and such that if $x \in K^\times$ satisfies $|x| < 1$ then $|x| \leq |\varpi|$.*

Lemma 8.3 *There exists a uniformizing element in K.*

Proof: If $\varpi \in P$, and $\varpi \notin P^2$, then we find that $\mathrm{ord}_P(\varpi) = 1$. Since $\mathrm{ord}_P(\varpi)$ must be an integer and $|x| = q^{-\mathrm{ord}_P(x)}$, we find that ϖ satisfies the required property.

□

Recall that F is dense in K (with respect to the topology arising from the P-adic valuation. Let A be the closure of $\mathcal{O}_F$ in K. On the one hand, if $x \in \mathcal{O}_F$, then $|x| \leq 1$. A stronger result is the following

Lemma 8.4 *A is precisely the closed unit disc in K:*

$$A = \{x \in K \text{ such that } |x| \leq 1\}.$$

Proof: Suppose that x is contained in the closed unit disk in K: $|x| \leq 1$. Then, since F is dense in K, we find that for any $0 < \epsilon \leq 1$ there exists $y \in F$ such that $|y - x| < \epsilon$. The ultrametric triangle inequality implies that

$$|y| = |y - x + x| \leq \max\{\epsilon, |x|\} \leq 1.$$

Thus, by Lemma 7.30 there exists $\alpha, \beta \in \mathcal{O}_F$, such that $y = \alpha/\beta$ and $\beta \notin P$ (so $|\beta| = 1$).

It remains to find an element $\gamma \in A$ such that $|\gamma - y| < \epsilon$, since then $|\gamma - x| < \epsilon$ by the ultrametric triangle inequality. Equivalently, it remains to find $\gamma \in A$ such that $|\alpha - \gamma\beta| < \epsilon$.

For this, it suffices to solve the congruence:

$$\gamma\beta \equiv \alpha, \text{ modulo } P^N,$$

for arbitrarily large N. Observe that P (modulo P^N) is the unique maximal ideal[1] in $\mathcal{O}_F/P^N$, since P is a maximal ideal in $\mathcal{O}_F$. Since $\beta \notin P$, we find that β is invertible[2] in $\mathcal{O}_F/P^N$. Thus there exists an element $\delta \in \mathcal{O}_F$ such that $\beta\delta \equiv 1$, modulo P^N. Letting $\gamma = \delta\alpha$ solves the required congruence.

□

[1] The maximal ideals of $\mathcal{O}_F/P^N$ correspond to the maximal ideals of $\mathcal{O}_F$ containing P^N. These correspond to the nonzero prime ideals of $\mathcal{O}_F$ occurring in the factorization of P^N. By the uniqueness of factorization of ideals, the only such prime ideal is P itself.

[2] Either β is contained in a maximal ideal or β is invertible. But P is the unique maximal ideal in $\mathcal{O}_F/P^N$.

The closed unit disc $A \subset K$ is thus a subring of K. Its ideals can be characterized as discs of varying radii:

Theorem 8.5 *There is a natural order-preserving bijection between the ideals in A and the non-negative integers $k = 0, 1, 2, \ldots$, given by:*

$$I_k = \{x \in A \colon |x| \leq q^{-k}\}.$$

Every ideal I_k in A is principal. If $x \in A$ and $|x| = q^{-k}$, then $I_k = (x)$.

Proof: Suppose first that I is an ideal in A. Since, for every element $x \in I$, $|x| = q^{-m}$ for some non-negative integer m, there exists $x \in I$ such that $|x| \geq |y|$ for all $y \in I$. We find that for any such element x, $xA \subset I$. Also, if $y \in I$ then $|y/x| \leq 1$. Thus $y/x \in A$ (since A is the closed unit disc in K). Hence $y \in xA$. Furthermore, this argument demonstrates that if $|y| \leq |x|$ then $y \in I = xA$.

In this way, we find that every nonzero ideal in A is principal, and can be described as a closed disc. The multiplicativity of the absolute value implies that every such closed disc is an ideal in A.

□

An important special case of the above classification of ideals is the following:

Corollary 8.6 *Let ϖ be any uniformizing element of K, e.g., $\varpi \in P$ and $\varpi \notin P^2$. Then ϖA is the unique maximal ideal in the ring A. Furthermore,*

$$\varpi A = \{x \in A \text{ such that } |x| < 1\}.$$

Proof: Given a uniformizing element ϖ of K, we find that $|\varpi|$ is maximal among absolute values occurring which are less than 1. It immediately follows that ϖA is the unique maximal ideal in A. The previous lemma also implies that ϖA is characterized as:

$$\varpi A = \{x \in A \text{ such that } |x| \leq |\varpi|\} = \{x \in A \text{ such that } |x| < 1\}.$$

□

Using a uniformizing element ϖ, we can describe all of the ideals in A:

$$A \supset \varpi A \supset \varpi^2 A \supset \varpi^3 A \supset \cdots.$$

These ideals can also be described as closed discs of radii q^{-k} for $k \geq 0$. On the other hand, these *closed discs* are also *open discs*, since the metric is discretely-valued. In this way, every ideal in A is simultaneously closed and open (sometimes called **clopen**).

Since ϖA is the unique maximal ideal in A, it follows that

$$A^\times = A \setminus \varpi A.$$

Geometrically, this can be viewed as an annulus:

$$A^\times = \{x \in K : q^{-1} < |x| \leq 1\}.$$

Now we are ready to consider a new perspective on the ring A:

Theorem 8.7 *The inclusion $\mathcal{O}_F \hookrightarrow A$ induces a ring isomorphism $\mathcal{O}_F/P^k \cong A/\varpi^k A$ for all $k \geq 1$. Furthermore, there is a continuous ring isomorphism*

$$A \cong \varprojlim_k \frac{\mathcal{O}_F}{P^k},$$

in which the right side is given the subspace topology from the infinite product $\prod_k \mathcal{O}_F/P^k$.

Proof: Consider the map $\mathcal{O}_F \to A/\varpi^k A$, given by composing the inclusion $\mathcal{O}_F \hookrightarrow A$ with the projection map. Recall that $\varpi^k A$ is an open subset of A for all $k \geq 1$. It follows that for all $a \in A$, the coset $a + \varpi^k A$ is an open subset[3] of A. Since $\mathcal{O}_F$ is dense in A, there exists $\alpha \in \mathcal{O}_F$ such that

$$\alpha \in a + \varpi^k A.$$

[3] Translation by a is a homeomorphism from K to K, by the continuity of addition.

It follows that the map $\mathcal{O}_F \to A/\varpi^k A$ is surjective. The kernel is precisely $\varpi^k A \cap \mathcal{O}_F$. This is precisely the set

$$\{x \in \mathcal{O}_F : |x| \leq q^{-k}\} = \{x \in \mathcal{O}_F : \mathrm{ord}_P(x) \geq k\} = P^k.$$

It follows that the map $\mathcal{O}_F \to A/\varpi^k A$ descends to a ring isomorphism

$$\frac{\mathcal{O}_F}{P^k} \to \frac{A}{\varpi^k A}.$$

Now consider the family of continuous[4] projections $A \to A/\varpi^k A$; by the universal property of inverse limits, this factors through the inverse limit via a continuous ring homomorphism:

[4] Continuity follows from the fact that $\varpi^k A$ is closed and open, so the quotient topology on $A/\varpi^k A$ is precisely the discrete topology.

$$A \to \varprojlim_k \frac{A}{\varpi^k A}.$$

Here, the right side is given the inverse limit topology. The inverse limit can be thought of as the set of sequences (a_k), where for each $k \geq 1$, $a_k \in A/\varpi^k A$, and for each pair $k \geq \ell \geq 1$, $a_k \equiv a_\ell$, modulo $\varpi^\ell A$. In other words, the inverse limit is the set of **compatible systems** of congruences, modulo all powers of ϖ. As a set of sequences, the natural topology is the subspace topology from the infinite product $\prod_k (A/\varpi^k A)$.

Now that we have a continuous ring homomorphism from A to $\varprojlim_k A/\varpi^k A$, and $A/\varpi^k A$ is isomorphic to $\mathcal{O}_F/P^k$, it remains to show that this continuous ring homomorphism is bijective.

The kernel of this ring homomorphism is an ideal in A. If it were not injective, then the kernel would contain $\varpi^k A$ for some $k \geq 0$ by our classification of ideals in A. But certainly ϖ^k does not map to zero in $A/\varpi^{k+1}A$, and hence does not map to zero in the projective limit. Thus we find that A maps injectively to $\varprojlim_k A/\varpi^k A$.

For surjectivity, consider a compatible system of congruences (α_k) where for each $k \geq 1$, $\alpha_k \in \mathcal{O}_F/P^k$. Then we find that the sequence (α_k) is a Cauchy sequence in $\mathcal{O}_F$, and hence converges to an element $a \in A$. In this way, we find that A maps surjectively onto $\varprojlim_k A/\varpi^k A$.

□

The above theorem should be thought of as a second perspective on p-adic fields (or rather the unit discs therein). An element of A can be thought of as a compatible sequence of congruences, modulo all powers of P. When $K = \mathbb{Q}_p$, the unit disc is called $\mathbb{Z}_p$, and $\mathbb{Z}$ is dense in $\mathbb{Z}_p$. An element of $\mathbb{Z}_p$ can be thought of as a compatible system of congruences, modulo $p\mathbb{Z}$, $p^2\mathbb{Z}$, $p^3\mathbb{Z}$, etc.. In this way, "working p-adically" allows us to work simultaneously with an infinite tower of congruences.

For example, to say that $5 \in (\mathbb{Z}/3\mathbb{Z})^\times$ means that there exists $x \in \mathbb{Z}$ such that $5x \equiv 1$, modulo 3 (for example, $x = 2$). To say that $5 \in (\mathbb{Z}/9\mathbb{Z})^\times$ means that there exists $x \in \mathbb{Z}$ such that $5x \equiv 1$, modulo 9 (for example $x = 2$ again). To say that $5 \in (\mathbb{Z}/27\mathbb{Z})^\times$ means that there exists $x \in \mathbb{Z}$ such that $5x \equiv 1$, modulo 27 (for example $x = 11$).

To say that $5 \in \mathbb{Z}_3^\times$ means that one may find a sequence (x_k) of integers, such that

$$5 \cdot x_k \equiv 1 \text{ modulo } 3^k, \text{ for all } k \geq 1.$$

In this way, a 3-adic number (i.e., an element of $\mathbb{Z}_3$) encodes an infinite system of congruences.

As another example, suppose that $x \in \mathbb{Z}_3$ and $x^2 = 7$. Then we find a sequence (x_k) of integers, such that

$$x_k^2 \equiv 7 \text{ modulo } 3^k, \text{ for all } k \geq 1.$$

From this perspective, the p-adic fields are most useful, since solving equations p-adically (where analytic methods apply) allow for the solution of infinite families of congruences.

8.2 Analysis of series

In complete nonarchimedean fields, one may consider "special functions" defined by infinite series in one or more variables. We begin with an analytic lemma.

Lemma 8.8 *Suppose that (a_i) is a sequence of elements of K. Then $\sum a_i$ converges in K (i.e., the sequence of partial sums is a Cauchy sequence in K) if and only if (a_i) is a null sequence.*

PROOF: Let $s_i = \sum_{j=0}^{i} a_i$ denote the sequence of partial sums. If s_i is a Cauchy sequence, then for any $\epsilon > 0$, there exists a positive integer N such that

$$|s_i - s_{i-1}| = |a_i| < \epsilon,$$

for all $i > N$. It follows that (a_i) is a null sequence.

Conversely, suppose that (a_i) is a null sequence. Let ϵ be a positive real number, and let N be a positive integer such that for all $i > N$, $|a_i| < \epsilon$. Then, if $j \geq i > N$, then we find that

$$\begin{aligned} |s_j - s_i| &= |\sum_{k=i+1}^{j} a_k| \\ &\leq \max\{|a_k| : i+1 \leq k \leq j\} \\ &< \epsilon. \end{aligned}$$

Thus the sequence (s_i) is a Cauchy sequence, converging to an element of K.

□

This result sharply contrasts with our knowledge about archimedean complete fields such as $\mathbb{R}$ and $\mathbb{C}$, in which many divergent sums have terms approaching zero. Convergence in nonarchimedean complete fields is far simpler!

As a first example, we may consider geometric series. Suppose that $x \in K$ and $|x| < 1$; in other words, $x \in \varpi A$. Then we find that $|x^k| \to 0$, and so the sum

$$\sum_{k=0}^{\infty} x^k \text{ converges.}$$

The usual argument from analysis[5] implies that

$$(1-x) \cdot \sum_{k=0}^{\infty} x^k = 1.$$

[5] We are using the interchange of limits and the basic arithmetic operations in K.

Hence the usual formula for geometric series holds in the ring A:

$$\sum_{k=0}^{\infty} x^k = \frac{1}{1-x}, \text{ if } |x| < 1.$$

Example 8.9 *If p is a prime number, then $|p| = p^{-1} < 1$ in the p-adic field $\mathbb{Q}_p$. It follows that:*

$$\frac{1}{1-p} = \sum_{k=0}^{\infty} p^k \in \mathbb{Z}_p.$$

As another example, we can consider the exponential and logarithm maps, viewed as power series. We begin with the "formal logarithm":

$$\log(1-x) = -\left(x + \frac{x^2}{2} + \frac{x^3}{3} + \cdots\right).$$

Suppose that $|x| = r < 1$ in a p-adic field K. Since the P-adic absolute value restricts to a p-adic valuation on $\mathbb{Q}$, we find that

$$|k| = |p|^{\mathrm{ord}_p(k)} = q^{-e\,\mathrm{ord}_p(k)}, \text{ for all positive } k \in \mathbb{Z}.$$

Since $\mathrm{ord}_p(k) \leq \log_p(k)$, and $q = p^f$, we find that

$$|k| \geq k^{-ef}.$$

Then we find that

$$\left|\frac{x^k}{k}\right| = r^k |k|^{-1} \leq r^k k^{ef},$$

for all $k > 0$. Since $r^k k^{ef} \to 0$ (since $0 < r < 1$ and $0 < ef < \infty$), we find that the series defining $\log(1-x)$ converges for all $|x| < 1$.

The "formal exponential" is more difficult to analyze:

$$\exp(x) = 1 + x + \frac{x^2}{2!} + \frac{x^3}{3!} + \cdots.$$

Suppose again that $|x| = r < 1$ in a p-adic field K. We can estimate the P-adic valuation of factorials using the following[6]

$$\begin{aligned}
\mathrm{ord}_p(k!) &= \sum_{i=1}^{\lfloor \log_p(k) \rfloor} \lfloor \frac{k}{p^i} \rfloor \\
&\leq \sum_{i=1}^{\lfloor \log_p(k) \rfloor} \frac{k}{p^i} \\
&= kp^{-1} \cdot \frac{p^{-\lfloor \log_p(k) \rfloor} - 1}{p^{-1} - 1} \\
&\leq kp^{-1} \cdot \frac{k^{-1}p - 1}{p^{-1} - 1} \\
&= \frac{p-k}{1-p}.
\end{aligned}$$

[6] In order to determine $\mathrm{ord}_p(k!)$, we count multiples. There are $\lfloor k/p \rfloor$ multiples of p occurring among $1, \ldots, k$. There are $\lfloor k/p^2 \rfloor$ multiples of p^2 occurring among $1, \ldots, k$. Continuing, there are $\lfloor k/p^i \rfloor$ multiples of p^i among $1, \ldots, k$. This number becomes zero, as soon as p^i exceeds k, i.e., as soon as i exceeds $\lfloor \log_p(k) \rfloor$.

From this, we find that

$$\left|\frac{1}{k!}\right| \leq p^{ef\frac{k-p}{p-1}}.$$

It follows that

$$\left|\frac{x^k}{k!}\right| \leq r^k p^{ef\frac{k-p}{p-1}} = \left(r \cdot p^{\frac{ef}{p-1}}\right)^k \cdot p^{\frac{efp}{p-1}}.$$

From this we find that

Proposition 8.10 *The exponential function* $\exp(x)$ *converges for all* $|x| \leq r$*, as long as*

$$r < p^{-\frac{ef}{p-1}} = |p|^{1/(p-1)}.$$

Example 8.11 *Let* $U_1 = 1 + p\mathbb{Z}_p$*, i.e.,*

$$U_1 = \{x \in \mathbb{Q}_p : |x - 1| < 1\}.$$

Then U_1 *is a subgroup of* $\mathbb{Z}_p^\times$*, i.e.,* U_1 *is closed under multiplication and inversion. In fact, inverses may be easily computed using geometric series.*

The open disc $p\mathbb{Z}_p = \{x \in \mathbb{Q}_p : |x| < 1\}$ *is an additive subgroup of* $\mathbb{Q}_p$*, i.e., it is closed under addition and subtraction. The convergence of* $\log(1 - x)$ *for* $|x| < 1$ *implies that* log *defines a function:*

$$\log\colon U_1 \to p\mathbb{Z}_p.$$

On the other hand, if $x \in p\mathbb{Z}_p$*, and* $p \neq 2$*, then* $1 > (p-1)^{-1}$ *and*

$$|x| \leq p^{-1} < p^{-1/(p-1)}.$$

Thus when $p \neq 2$*, the exponential series defines a function:*

$$\exp\colon p\mathbb{Z}_p \to U_1.$$

The reader may apply analytic methods to verify that log *and* exp *define continuous group homomorphisms, within their radii of convergence, and are inverses when convergence is satisfied. In that way, we find a continuous group isomorphism, when* $p \neq 2$*:*

$$U_1 \cong p\mathbb{Z}_p.$$

8.3 Hensel's Lemma

We have already seen the interpretation of $A \subset K$, as the set of compatible systems of congruences:

$$A \cong \varprojlim_k \frac{\mathcal{O}_F}{P^k}.$$

In this way, an element of A encodes an infinite sequence of congruences. Such an encoding is not worthwhile unless we can, in the end, carry out only a finite number of computations.

Hensel's lemma is a "lifting theorem", which approximately says that once a sufficiently long chain of congruences has been solved (modulo P, P^2, P^3, ..., P^t), there exists an infinite sequence of solutions (modulo P^k for all $k > 0$). For example, in order to prove that the equation $x^2 = 7$ has a solution in $\mathbb{Z}_3$, it suffices to prove that

$x^2 = 7$ has a solution in $\mathbb{Z}/3\mathbb{Z}$ – Hensel's lemma takes care of the rest.

There are many other interpretations, reformulations, and generalizations of Hensel's lemma. A good exposition and historical treatment of Hensel's lemma can be found in the article of Brink[7] or the article of Ribenboim[8].

[7] David Brink. New light on Hensel's lemma. *Expo. Math.*, 24(4):291–306, 2006. ISSN 0723-0869

[8] Paulo Ribenboim. Equivalent forms of Hensel's lemma. *Exposition. Math.*, 3(1): 3–24, 1985. ISSN 0723-0869

Consider a polynomial $F \in A[X]$. We are interested foremost in the question of finding roots to the equation $F(x) = 0$, in the ring A. In other words, we are interested in finding a compatible sequence of congruences (x_k), with $x_k \in \mathcal{O}_F/P^k$, such that for all $k \geq 1$, $F(x_k) \equiv 0$, modulo P^k.

Let $F' \in A[X]$ denote the derivative of F. Using the binomial theorem, one may check directly that

$$F(x_0 + \delta) - F(x_0) = \delta F'(x_0) + \delta^2 \alpha,$$

for some $\alpha \in A$. Thus in nonarchimedean fields, we see that (at least for polynomials) results from calculus on linear approximation are still valid.

One application of linear approximation (of polynomials) is Newton's method for finding roots of polynomials. Hensel's lemma demonstrates that Newton's method applies in the ring A as well:

Theorem 8.12 *Suppose that $F \in A[X]$, $a \in A$, and $F(a)$ is close to zero in the precise sense that*

$$|F(a)| < |F'(a)|^2.$$

Then there exists $x \in A$ such that $F(x) = 0$ and

$$|x - a| \leq |\frac{F(a)}{F'(a)^2}|.$$

Proof: Our proof follows Theorem 6.28 of Knapp text[9]. Suppose that $|F(a)| \leq |F'(a)|^2$. If $F'(a) = 0$, then $F(a) = 0$ and the result is proven. Thus we assume hereafter that $F'(a) \neq 0$.

[9] Anthony W. Knapp. *Advanced algebra*. Cornerstones. Birkhäuser Boston Inc., Boston, MA, 2007. ISBN 978-0-8176-4522-9

Consider the sequence defined recursively [10] by $a_0 = a$ and

$$a_{i+1} = a_i - \frac{F(a_i)}{F'(a_i)}.$$

[10] This recursive process is known as Newton's method for finding roots of a polynomial.

In order to prove that this sequence converges, it is natural to consider the associated sequences:

$$\delta_i = a_{i+1} - a_i = -\frac{F(a_i)}{F'(a_i)}, \text{ and } \rho_i = |\delta|.$$

Also define

$$C = \frac{\rho_0}{|F'(a_0)|} = \frac{|F(a_0)|}{|F'(a_0)|^2}.$$

Thus $C < 1$ and $\rho_0 = C \cdot |F'(a_0)| < 1$ as well.

We prove by induction that for all $i \geq 0$ the following statements hold:

(1_i) a_i is an element of A.

(2_i) $|F'(a_i)| = |F'(a_0)| \neq 0$.

(3_i) $\rho_i \leq C^{2^i}|F'(a_0)|$.

When $i = 0$, every one of the above statements are trivially true. Assume now that Statements 1_i, 2_i, 3_i are true. Then by Statement 2_i , we find that

$$a_{i+1} = a_i - \frac{F(a_i)}{F'(a_i)}$$

is well-defined. By Statement 3_i, we find that

$$|a_{i+1} - a_i| = \frac{|F(a_i)|}{|F'(a_i)|} \leq C^{2^i}|F'(a_0)|.$$

Since $a_i \in A$ (by Statement 1_i) and ρ_0, $F'(a_0)$ are elements of A, we find that $a_{i+1} \in A$ by the ultrametric triangle inequality. Thus we have proven Statement 1_{i+1}.

Now, by linear approximation, we find that

$$F(a_{i+1}) = F(a_i + \delta_i) = F(a_i) + F'(a_i)\delta_i + \delta_i^2\alpha,$$

$$F'(a_{i+1}) = F'(a_i + \delta_i) = F'(a_i) + \delta_i\beta,$$

for some $\alpha, \beta \in A$. It follows that

$$|F'(a_{i+1})| = |F'(a_i) + \delta_i\beta|.$$

By Statement 2_i, we have

$$|\delta_i| = \rho_i \leq C^{2^i}|F'(a_0)| = C^{2^i}|F'(a_i)| < |F'(a_i)|,$$

and so

$$|F'(a_{i+1})| = |F'(a_i)|.$$

Thus we have proven Statement 2_{i+1}.

Finally, we are left to consider

$$\rho_{i+1} = \left|\frac{F(a_{i+1})}{F'(a_{i+1})}\right|.$$

Note that since $(a_{i+1} - a_i)F'(a_i) = -F(a_i)$,

$$F(a_{i+1}) = F(a_i) + F'(a_i)\delta_i + \delta_i^2\alpha = \delta_i^2\alpha.$$

By Statements 2_{i+1} and 2_i, we find that

$$\begin{aligned}\frac{\rho_{i+1}}{F'(a_0)} &= |\frac{F(a_{i+1})}{F'(a_0)^2}| \\ &= |\frac{\delta_i^2\alpha}{F'(a_0)^2}| \\ &\leq |\frac{\delta}{F'(a_0)}|^2 \\ &\leq (C^{2_i})^2 \\ &= C^{2^{i+1}}.\end{aligned}$$

Statement 3_{i+1} follows immediately.

Now that we have a sequence (a_i) in A, satisfying Statements 1_i, 2_i, 3_i, we find that the sequence is a Cauchy sequence by Statement 3_i (and basic results on geometric series). Thus we consider the limit $a = \lim(a_i)$, which is an element of A. We find that $|a - a_0| \leq C$ as well by Statements 3_i.

Finally, we find that

$$|F(a_i)| = |a_{i+1} - a_i| \cdot |F'(a_i)| = \rho_i \cdot |F'(a_i)| = \rho_i |F'(a_0)| \to 0,$$

using Properties 2_i and 3_i. Since $|F(a_i)|$ approaches zero, we find (by the continuity of polynomials) that $F(a) = 0$.

□

The previous lemma is one of the more powerful of many equivalent statements to Hensel's lemma. In practice, a very important case arises when $F'(a)$ is a unit in A:

Corollary 8.13 *Suppose that $F \in A[X]$, $a \in A$, $|F'(a)| = 1$, and $|F(a)| < 1$. Then there exists $x \in A$ such that $F(x) = 0$ and $|x - a| \leq |F(a)|$.*

One important case of this is the following

Corollary 8.14 *Let C be an integer, and n be a positive integer. Let p be a prime number. Then, if p does not divide n, and p does not divide C, and there exists $a \in \mathbb{Z}$ such that $a^n \equiv C$ modulo p, then there exists $x \in \mathbb{Z}_p$ such that $x^n = C$. Thus there exists a sequence of integer (x_k), such that for every $k \geq 1$,*

$$x^k \equiv C \text{ modulo } p^k.$$

Proof: Let $F \in \mathbb{Z}[X]$ be the polynomial $F(X) = X^n - C$. Since $a^n \equiv C$, modulo p, we find that $|F(a)| < 1$. Moreover, $|a|^n = |C| = 1$ since p does not divide C, and hence $|a| = 1$ as well. If we consider the derivative, we find that

$$|F'(a)| = |n| \cdot |a|^{n-1} = 1,$$

since p does not divide n.

Thus by Hensel's lemma, there exists $x \in \mathbb{Z}_p$ such that $F(x) = 0$. The result follows from our interpretation of $\mathbb{Z}_p$ as the ring of compatible congruences, modulo powers of p.

□

Example 8.15 *There exists a sequence of integers (x_k) such that $x_k^2 \equiv 7$, modulo 3^k. Indeed, $7 \equiv 1$, modulo 3^1, so 7 is a "quadratic residue", modulo 3. Since 3 divides neither 2 nor 7, the hypotheses of the previous corollary hold.*

8.4 Another Hensel's Lemma

Hensel's lemma immediate implies the following statement:

Proposition 8.16 *Suppose that $k = A/\varpi A$ is the **residue field** of A, and for $f \in A[X]$ write $\bar{f}$ for its reduction in $k[X]$. Suppose that $f \in A[X]$ is a monic polynomial. Then if $\bar{f} = \bar{g}\bar{h}$ for a linear monic polynomial $\bar{g} \in k[X]$ and a monic polynomial $\bar{h} \in k[X]$ such that $\bar{g}$ and $\bar{h}$ are coprime, then there exist monic polynomials $g, h \in A[X]$ which reduce to $\bar{g}$, $\bar{h}$, and which satisfy $f = gh$.*

Proof: Given the decomposition $\bar{f} = \bar{g}\bar{h}$, with $\bar{g}$ monic and linear, we find that $\bar{f}$ has a root $\bar{r}$ in $k = A/\varpi A$. Let $r \in A$ be any lift of $\bar{r}$; Thus we find that $\bar{f}(r) = 0$, so $f(r) \in \varpi A$. Furthermore, since $\bar{g}$ and $\bar{h}$ are coprime, we find that $\bar{r}$ is not a repeated root of $\bar{f}$. Thus $\bar{f}'(\bar{r}) \neq 0$. Therefore $f'(r) \notin \varpi A$, and so $|f'(r)| = 1$.

It follows that $|f(r)| < |f'(r)|^2$, and Hensel's lemma applies. We may find a root x of f which reduces to $\bar{r}$, modulo ϖA. Thus f has a monic linear factor g which reduces to $\bar{g}$, and the quotient $h = f/g$ reduces to $\bar{h}$ as desired.

□

The following theorem generalizes the above proposition, removing assumptions on the degree of $\bar{g}$ and $\bar{h}$, and it is often called Hensel's lemma as well. While the following theorem is stronger than the previous proposition, it is somewhat weaker than Hensel's lemma since it does not allow one to find roots of polynomials f whose reduction has multiple roots.

Theorem 8.17 *Let $k = A/\varpi A$ be the **residue field** of A, and for $f \in A[X]$ write $\bar{f}$ for its reduction in $k[X]$. Suppose that $f \in A[X]$ is a monic polynomial. Then if $\bar{f} = \bar{g}\bar{h}$ for two monic coprime (in $k[X]$) polynomials $\bar{g}$ and $\bar{h}$, then there exist monic polynomials $g, h \in A[X]$ which reduce to $\bar{g}$, $\bar{h}$, and satisfy $f = gh$.*

PROOF: Our proof follows the proof of Theorem 7.33 in Milne's excellent notes.[11]

We begin with $f \in A[X]$ monic, and $\bar{g}, \bar{h} \in k[X]$ monic and coprime, such that $\bar{f} = \bar{g}\bar{h}$. We can immediately find monic g_1, h_1 lifting[12] $\bar{g}$, $\bar{h}$, from which we find that

$$f - g_1 h_1 \in \varpi A[X], \text{ and } \mathrm{Deg}(f) = \mathrm{Deg}(g_1 h_1)$$

We prove, by induction, that there exists a sequence of pairs $(g_n, h_n) \in A[X]^2$ such that

- The polynomials g_n, h_n are monic and reduce to $\bar{g}$, $\bar{h}$.
- $\mathrm{Deg}(g_n) \leq \mathrm{Deg}(g_1)$ and $\mathrm{Deg}(h_n) \leq \mathrm{Deg}(h_1)$.
- $f - g_n h_n \in \varpi^n A[X]$.

The base step of induction has already been demonstrated. So suppose that a pair (g_n, h_n) has been found satisfying the above conditions. It suffices to find $u, v \in A[X]$ with $\mathrm{Deg}(u) < \mathrm{Deg}(g_1)$ and $\mathrm{Deg}(v) < \mathrm{Deg}(h_1)$ such that

$$f - (g_n + \varpi^n u)(h_n + \varpi^n v) \in \varpi^{n+1} A[X].$$

Indeed, we could then define $g_{n+1} = g_n + \varpi^{n+1} u$ and $h_{n+1} = h_n + \varpi^{n+1}$ to achieve the next step in the induction. Observe that the degree of g_{n+1} and h_{n+1} remains bounded above by $\mathrm{Deg}(g_1)$ and $\mathrm{Deg}(h_1)$. g_{n+1} and h_{n+1} remain monic, since they only differ from g_n and h_n in terms below the dominant term.

Simplifying the conditions on u and v, it suffices to find $u, v \in A[X]$ of degrees bounded as before, such that

$$u h_n + v g_n \equiv \frac{f - g_n h_n}{\varpi^n} \text{ modulo } \varpi A[X].$$

For this, consider the $A[X]$-module $M = A[X]/(g_n, h_n)$. This is finitely-generated, as an A-module since g_n (and h_n) is monic[13]. Since $\bar{g}$, $\bar{h}$ are coprime, we find that $M/\varpi M = 0$. It follows by Nakayama's lemma[14] that $M = 0$.

Hence $(g_n, h_n) = A[X]$, i.e. g_n and h_n are coprime in $A[X]$. It follows that there exist $u, v \in A[X]$ such that

$$u h_n + v g_n = \frac{f - g_n h_n}{\varpi^n}.$$

If $\mathrm{Deg}(v) \geq \mathrm{Deg}(h_n)$, we may divide polynomials[15] with remainder to find $v = q h_n + r$ for polynomials $q, r \in A[X]$ with $\mathrm{Deg}(r) < \mathrm{Deg}(h_n)$. In this case we find

$$(u + q g_n) h_n + r g_n = \frac{f - g_n h_n}{\varpi^n}.$$

[11]

[12] We say that g **lifts** $\bar{g}$ if $\bar{g} \in k[X]$ and $g \in A[X]$, and g reduces (mod ϖA) to $\bar{g}$

[13] M is generated as an A-module by $1, X, X^2, \ldots, X^{\mathrm{Deg}(g_n)-1}$, since higher powers of X can be expressed in terms of these powers

[14] Nakayama's lemma: If R is a local ring, i.e., a ring with a unique maximal ideal m, and M is a finitely-generated R-module, and $M/mM = 0$, then $M = 0$.

[15] Division of monic polynomials with coefficients in a PID has the expected properties.

Not only is $\mathrm{Deg}(r) < \mathrm{Deg}(h_n)$, but moreover $\mathrm{Deg}(u + qg_n) < \mathrm{Deg}(g_n)$ since

$$\mathrm{Deg}(u+qg_n)+\mathrm{Deg}(h_n) = \mathrm{Deg}(\frac{f - g_n h_n}{\varpi^n} - rg_n) < \mathrm{Deg}(h_n)+\mathrm{Deg}(g_n).$$

In this way, we find by division with remainder that there exist u, v in $A[X]$ such that

- $uh_n + vg_n = 1$.
- $\mathrm{Deg}(u) < \mathrm{Deg}(g_n)$ and $\mathrm{Deg}(v) < \mathrm{Deg}(h_n)$.
- $f - (g_n + \varpi^n u)(h_n + \varpi^n v) \in \varpi^{n+1} A[X]$.

Thus we find a sequence of polynomials g_n, h_n satisfying the desired three conditions. Observe that the coefficients of these polynomials form Cauchy sequences, and the degrees of these polynomials are bounded. Hence, there are limiting polynomials g, h such that:

- g and h are monic and reduce to $\bar{g}$ and $\bar{h}$.
- $\mathrm{Deg}(g) \leq \mathrm{Deg}(g_1)$ and $\mathrm{Deg}(h) \leq \mathrm{Deg}(h_1)$.
- $f = gh$.

Example 8.18 *An important application of the above formulation of Hensel's lemma is given by the* ***Teichmuller representatives****. Recall that $q = \mathrm{N}(P)$ is the cardinality of the field $k = A/\varpi A$. Thus the polynomial $f(X) = X^q - X$ has q distinct roots in k. The resulting factorization of $f(X)$ in $k[X]$, into distinct monic linear factors, lifts by the previous theorem to a factorization of $f(X)$ in $A[X]$ into distinct monic linear factors. In this way, we find a canonical injective function (not a homomorphism!) $\theta\colon k \to A$. One may check directly that θ does restrict to an injective group homomorphism from $k^\times$ into $A^\times$.*

8.5 Extension of the valuation

Suppose that K is a p-adic field, and $K \subset L$ is a finite extension of fields. Thus L is a finite-dimensional K-vector space, endowed with the product topology from that on K. Recall that A is the closed unit disc in K, also called the **valuation ring** of K. Fix a uniformizer ϖ for K, and recall that the nonzero ideals of A are precisely the principal ideals $\varpi^k A$ for $0 \leq k \in \mathbb{Z}$. In particular, A is a PID and UFD.

Since A is a PID, Proposition 2.4 holds, replacing $\mathbb{Z}$ by A everywhere:

Proposition 8.19 *Suppose that L is a field extension of K and $\alpha \in L$. The following conditions are equivalent.*

1. *α is integral over A.*

2. *$A[\alpha]$ is a finite rank A-module.*

3. *There exists a subring M of K, such that M is finitely-generated as a A-module and M contains α.*

Consider the set B of elements of L which are integral of A (also called the **integral closure** of A in L). An immediate corollary of the previous proposition, following Corollary 2.5 for $\mathbb{Z}$, is that B is a subring of L.

Let $M = \varpi A$ be the unique maximal ideal in A; we consider the prime ideals of B containing M.

Lemma 8.20 *There exists a unique (and hence maximal) prime ideal in B containing M.*

Proof: Suppose that M_1, M_2 are distinct prime ideals of B containing M. If $M_1 \neq M_2$, then we may choose $\beta \in M_1$ such that $\beta \notin M_2$ (without loss of generality). Let $f \in A[X]$ be the minimal polynomial of β; thus f is monic and irreducible, since every element of B is integral over A. Then we find that $A[\beta]$ is isomorphic to $A[X]/\langle f \rangle$.

Let $k = A/M$ be the residue field of A, and consider the reduction $\bar{f} \in k[X]$. If $\bar{f}$ had two distinct irreducible factors in $k[X]$, this factorization would lift (by the previous Hensel's lemma) to a factorization of $f \in A[X]$, contradicting irreducibility. Thus $\bar{f}$ is a power of an irreducible polynomial $\bar{g}$ in $k[X]$. Therefore, we find that:

$$A[\beta]/\varpi A[\beta] \cong k[X]/\langle \bar{f} \rangle = k[X]/\langle \bar{g}^d \rangle.$$

It follows that $A[\beta]/\varpi A[\beta]$ has only one nonzero prime ideal, contradicting our assumption that there were two prime ideals M_1, M_2 containing M such that $M_1 \cap A[\beta] \neq M_2 \cap A[\beta]$.

□

Much of the first four chapters of this text go through easily, replacing $\mathbb{Z}$ by A and $\mathbb{Q}$ by K. In particular, we find that the "ring of integers" B is an A-lattice in the K-vector space L. Moreover, B is a UFD, and ideals in B factor uniquely into powers of the unique nonzero prime ideal $N \subset B$. Just as in the proof of Ostrowski's theorem, every nonarchimedean valuation on B arises as an "N-adic valuation":

$$|x| = e^{-\alpha \operatorname{ord}_N(x)}.$$

Theorem 8.21 *The P-adic valuation on K extends uniquely to a valuation on L. L is complete with respect to this valuation.*

PROOF: Observe that K is the fraction field of B (by the same arguments as in Chapter 2), and so any valuation of L is uniquely determined by its restriction to B. In this way, it suffices to classify the valuations on the ring B which extend the P-adic valuation on A.

Let N be the maximal ideal of B containing the maximal ideal M of A. Observe that the ideal MB factors as N^e, as ideals in B. Moreover, B/N is a finite extension of the field A/M, since B is a finitely-generated A-module. Recalling that $[A : M] = q$, a power of p,

$$[B : N] = q^f, \text{ for some } 0 < f \in \mathbb{Z}.$$

Now, if $|\cdot|$ is a valuation on L extending the P-adic valuation on K, we find that

$$|x| = q^{-f\alpha \operatorname{ord}_N(x)},$$

for some $\alpha \in \mathbb{R}$. Since it extends the P-adic valuation on K, we find that

$$|m| = q^{-f\alpha \operatorname{ord}_N(m)} = q^{-fe\alpha} = q^{-1}.$$

Thus $\alpha = (ef)^{-1}$. This proves the uniqueness of the extension of the P-adic valuation. For existence, one may simply define

$$|x| = q^{-\operatorname{ord}_N(x)/e}.$$

For the completeness of L, observe that L is isometric to the vector space K^n, where $n = [L : K]$. One can directly prove completeness from this fact.

□

Corollary 8.22 *If L is a finite extension of K, then L also satisfies Hensel's Lemma in all its variants. There is a natural Teichmuller lift from the residue field $\ell = B/N$ to L, extending the Teichmuller lift from $k = A/M$ to K.*

8.6 Exercises

Exercise 8.1 *Prove that if p is a prime number, and p is congruent to 1 mod 4, then there exists $x \in \mathbb{Z}_p$ such that $x^2 = -1$.*

Exercise 8.2 *Let K be a p-adic field, with valuation ring A. Let ϖ be a uniformizing element, and let $k = A/\varpi A$ be the residue field. Let $\theta : k \to A$ denote the Teichmuller map.*

Prove that every element of A can be expressed as a convergent series of the form:

$$\sum_{i=0}^{\infty} \theta(a_i)\varpi^i,$$

where for all i, $a_i \in k$.

Exercise 8.3 *Suppose that K is a p-adic field, and L is a finite Galois extension of K. Prove that if $\gamma \in \mathrm{Gal}(L/K)$, and L is given the topology from the unique valuation extending that on K, then γ is a continuous map from L to L.*

9
Galois Theory

In this chapter, we study the Galois theory of extensions of number fields, and the related theory of extensions of p-adic fields. This will culminate in the statements of global and local class field theory.

9.1 Extensions of p-adic fields

Suppose that K is a p-adic field, and L is a finite extension of K. In particular, the P-adic valuation on K extends uniquely to a valuation on L, and we fix this valuation on L throughout. Let A be the unit disc in K, and B the unit disc in L (also the integral closure of A in L). Let $M = \varpi A$ be the unique maximal ideal of A, and $N = \nu B$ the unique maximal ideal of B.

We have seen previously that the extension L/K has two numerical invariants, defined as follows:

Definition 9.1 *The **ramification degree** of L over K is the positive integer e which satisfies $MB = N^e$. The **inertial degree** of L over K is the positive integer f which satisfies $[B : N] = [A : M]^f$. L/K is called an **unramified** extension if $e = 1$. L/K is called a **totally ramified** extension if $f = 1$.*

These two invariants are connected to the degree of the field extension L/K by the following

Proposition 9.2 *Let $n = [L : K]$. Then $n = ef$, the product of the ramification degree and the inertial degree.*

Proof: The theory of A-lattices demonstrates that n is equal to the rank of the A-lattice B. Moreover, since B is a free A-module of rank n, we find that:

$$[B : \varpi B] = [A : \varpi A]^n.$$

Now, we have $\varpi B = \nu^e B$, and so

$$[B : \varpi B] = [B : \nu B]^e = [A : \varpi A]^{fe}.$$

Thus $n = ef$.

□

The extension L/K yields an extension of residue fields $k = A/M \subset \ell = B/N$ in a canonical way. The extension L/K is unramified if $e = 1$ (so $n = f$). In this case, n equals not only $[L : K]$, but also the degree of the extension of residue fields $[\ell : k]$.

The ramification of an extension can be detected numerically by the discriminant:

Proposition 9.3 *The extension L/K is ramified if and only if $\wp$ divides the discriminant* $\mathrm{Disc}(B)$ *of B as an A-lattice.*

Proof: Let $\beta_1, \ldots, \beta_n$ be an A-basis of B; thus $\mathrm{Disc}(B)$ is the determinant of the matrix $(\mathrm{Tr}(\beta_i\beta_j))$, and $\mathrm{Disc}(B) \in A$.

On the other hand, consider the k-algebra

$$B_k := B \otimes_A k = \frac{B}{\wp B} = \frac{B}{\nu^e B}.$$

The discriminant of B_k is (defined to be) the determinant of the matrix $\mathrm{Tr}(\bar{\beta}_i\bar{\beta}_j)$, where here the trace denotes the trace of the resulting matrix with entries in k. We find that $\mathrm{Disc}(B_k)$ is precisely the reduction, mod $\wp$, of $\mathrm{Disc}(B)$. Thus $\wp$ divides $\mathrm{Disc}(B)$ if and only if $\mathrm{Disc}(B_k) = 0$.

It is a general fact about finite-dimensional k-algebras[1] B_k that $\mathrm{Disc}(B_k) = 0$ if and only if B_k has a nonzero nilpotent element. Since $B_k = \frac{B}{\nu^e B}$, and νB is a maximal ideal in B, we find that B_k has a nonzero nilpotent element if and only if $e > 1$.

[1] The only assumption is that k is a perfect field and B_k is a finite-dimensional associative k-algebra. See, for example, Lemma 3.38 of Milne's notes

□

Consider an unramified extension L/K, so that $n = f = [L\colon K] = [\ell\colon k]$. Let q be the cardinality of k, so q^f is the cardinality of ℓ. The extension ℓ/k can be defined as the splitting field of an irreducible monic polynomial $\bar{\Phi}_f$ of degree f in $k[X]$. We may choose a monic lift Φ_f of degree f in $A[X]$ as well, which is then irreducible in $A[X]$ and in $K[X]$. By Hensel's lemma, the distinct roots of $\bar{\Phi}_f$ in ℓ lift to distinct roots of Φ_f in L. In this way, we see that L is the splitting field of an irreducible polynomial in $K[X]$. In particular, we find that

Proposition 9.4 *Every unramified extension L/K is a Galois extension.*

A much stronger result is the following:

Proposition 9.5 *There is a canonical bijection (really, an equivalence of categories) between the finite unramified extensions of K and the finite extensions of k, which preserves inclusions and Galois groups.*

Proof: Every finite unramified extension L/K yields a finite extension ℓ/k of the same degree, as we have already seen. Furthermore,

any inclusion $L_1 \hookrightarrow L_2$ of unramified extensions of K must be compatible with valuations, by the uniqueness of extension of valuations. Thus any such inclusion induces an inclusion of discs of any radius, and hence induces an inclusion of residue fields $\ell_1 \hookrightarrow \ell_2$.

Conversely, any finite extension ℓ/k arises as $\ell = k[\bar{z}]$ for some element $\bar{z} \in \ell$. Letting $\bar{P}_z$ be the minimal polynomial of $\bar{z}$ in $k[X]$, one may lift $\bar{P}_z$ to a monic irreducible polynomial P_z of the same degree in $A[X]$ (which is then also irreducible in $K[X]$). Let L be a splitting field of P_z, which is then a finite extension of K. Then, there is a unique valuation on L extending that on K. If r is any root of P_z in L, then we find that $r \in B$ (the valuation ring of L) since P_z is monic and irreducible in $A[X]$. It follows that the reduction $\bar{r}$ is a root of $\bar{P}_z$ in B/N (the residue field of L). It follows that B/N is a field containing k and a root of $\bar{P}_z$; thus B/N is isomorphic to ℓ. Note that L/K is unramified, since its degree equals the degree of P_z, which equals the degree of ℓ as an extension of k.

Thus, we find a correspondence between finite unramified extensions of K and finite extensions ℓ/k. To be precise, one may consider the category $Unr(K)$ of finite unramified field extensions of K and K-algebra homomorphisms, and the cateogry $Fie(k)$ of finite field extensions of k and k-algebra homomorphisms. Our work so far has constructed a functor from $Unr(K)$ to $Fie(k)$, and we have demonstrated that this functor is essentially surjective (every object of $Fie(k)$ is isomorphic to the image of an object of $Unr(K)$).

To finish the proof[2], it suffices to show that the induced maps $\mathrm{Gal}(L/K) \to \mathrm{Gal}(\ell/k)$ are isomorphisms for any finite unramified extension L/K with residue field ℓ. For this, we may realize $L = K[\beta]$ and $\ell = k[\bar{\beta}]$, for some $\beta \in B$ such that the Galois conjugates of β have distinct reductions in ℓ. Every automorphism in $\mathrm{Gal}(L/K)$ is determined by where it sends β, and this is determined by where $\bar{\beta}$ is sent. By such an argument, one verifies that $\mathrm{Gal}(L/K)$ injects into $\mathrm{Gal}(\ell/k)$. Surjectivity follows from the fact that both groups have order f.

[2] To prove that a functor defines an equivalence of categories, one must show that it is essentially surjective, full, and faithful. We have, so far, constructed an essentially surjective functor. The morphism sets are either empty, or are torsors for Galois groups. For this reason, the remaining argument is sufficient.

□

Recall that any finite extension of finite fields ℓ/k is cyclic, generated by a **Frobenius** automorphism[3] $Fr\colon \ell \to \ell$ given by:

$$Fr(x) = x^q.$$

By the previous proposition, we find:

Corollary 9.6 *Every finite unramified extension L/K is cyclic, generated by a Frobenius[4] automorphism $Fr \in \mathrm{Gal}(L/K)$ which reduces to the usual Frobenius automorphism of the residue fields ℓ/k.*

[3] This is often called the **arithmetic Frobenius** automorphism. Its inverse is called the **geometric Frobenius** automorphism.

[4] In other words, the phrase "Frobenius automorphism" is used both to denote the automorphism of finite fields given by $x \mapsto x^q$ and to the unique automorphism of L reducing to this automorphism.

In addition, we find

Corollary 9.7 *If L_1, L_2 are finite unramified extensions of K, contained in some larger finite extension L/K, then L_1L_2 is a finite unramified extension of K.*[5]

[5] This corollary can also be proven using the discriminant. The discriminant is multiplicative in towers, in the sense that if $K \subset L \subset L'$ with valuation rings $A \subset B \subset B'$, then

$$\mathrm{Disc}_A(B) \cdot \mathrm{N}_{L/K} \mathrm{Disc}_B(B') = \mathrm{Disc}_A(B').$$

The corollary follows quickly from this fact.

PROOF: Let ℓ_1, ℓ_2 denote the residue fields of L_1, L_2, respectively, and ℓ the residue field of L. Let $L_0 = L_1 \cap L_2$, which is then an unramified extension of K by the previous proposition. Let ℓ_0 be the residue field of L_0.

Consider the compositum $\ell' = \ell_1\ell_2$ of finite fields, in ℓ. Then, there exists an unramified extension L' of K, with residue field $\ell_1\ell_2$, such that the inclusions among the fields K, L_0, L_1, L_2, L' and among the fields $k, \ell_0, \ell_1, \ell_2, \ell'$ are compatible. As one may construct L' as the splitting field of a polynomial with roots in $\ell_1\ell_2 \subset \ell$, one may construct L' as a subfield of L containing L_1 and L_2. It follows by looking at degrees, that $L' = L_1L_2$.

□

From this, we find

Proposition 9.8 *Let L be a finite extension of a p-adic field K. Then there exists a unique intermediate field $K \subset L^u \subset L$, such that L^u/K is unramified and L/L^u is totally ramified:*

$$e = [L : L^u], \text{ and } f = [L^u : K].$$

PROOF: Let L^u be the compositum of all unramified extensions of K in L.

□

9.2 *Local class field theory*

The unramified extensions of K provide a source of cyclic Galois extensions of K. In this section, we state the main results of local class field theory, describing to some extent, the abelian Galois extensions of K. First, we mention some infinite Galois theory.

Let L/K be an algebraic extension of fields, not necessarily finite. We say that L is a Galois extension if every polynomial in $K[X]$ which has a root in L splits completely in L. Note that, whether or not L is finite, L is the compositum of all of its subfields L' such that L'/K is a finite Galois extension. Using inverse limits, which we have seen previously in "compatible systems of congruences", we may define $\mathrm{Gal}(L/K)$ when L/K is an infinite Galois extension:

Definition 9.9 *Let L/K be a (finite or infinite) Galois extension of fields. Let S be the set of intermediate extensions L'/K such that $L' \subset L$, L'/K is*

Galois, and $[L' : K] < \infty$. *Then* $\mathrm{Gal}(L/K)$ *is the group whose elements are collections* $(\gamma_{L'})$, *where for each* $L' \in S$, $\gamma_{L'} \in \mathrm{Gal}(L'/K)$, *and where for any pair* $L' \subset L''$ *of elements of* S,

$$pr(\gamma_{L''}) = \gamma_{L'},$$

where $pr\colon \mathrm{Gal}(L''/K) \to \mathrm{Gal}(L'/K)$ *is the canonical projection homomorphism. The group law on* $\mathrm{Gal}(L/K)$ *is obtained "component-wise" from the Galois groups* $\mathrm{Gal}(L'/K)$. $\mathrm{Gal}(L/K)$ *is given the subspace topology, from the direct product topology on* $\prod_{L' \in S} \mathrm{Gal}(L'/K)$; *in this way* $\mathrm{Gal}(L/K)$ *is a compact topological group.*

In other words, $\mathrm{Gal}(L/K)$ is the group of "compatible systems" of elements of Galois groups of intermediate extensions $L/L'/K$ with $[L'/K]$ finite. As a first example we consider the absolute Galois group of a finite field:

Example 9.10 *Let* k *be a finite field (for example, the residue field of* K*) with* q *elements. Let* $\bar{k}$ *be an algebraic closure of* k. *Then, it is a standard fact of field theory that for every positive integer* f, *there exists a unique subfield* ℓ_f *of* $\bar{k}$ *with* q^f *elements, and* $\mathrm{Gal}(\ell_f/k)$ *is cyclic of order* f. *Moreover, inclusions correspond to divisibility of these positive integers* f: *if* f *divides* f', *then* $\ell_f \subset \ell_{f'}$, *and the resulting map on Galois groups corresponds to the reduction map of cyclic groups:*

$$pr\colon \frac{\mathbb{Z}}{f'\mathbb{Z}} \to \frac{\mathbb{Z}}{f\mathbb{Z}}.$$

Here, the generator 1 *of the cyclic groups* $\mathbb{Z}/f\mathbb{Z}$ *and* $\mathbb{Z}/f'\mathbb{Z}$ *corresponds to the Frobenius automorphism* $x \mapsto x^q$ *of fields.*

Since all finite extensions of k *arise as fields* ℓ_f, *one for each* f, *we find that* $\mathrm{Gal}(\bar{k}/k)$ *is isomorphic to* $\hat{\mathbb{Z}}$, *the group of compatible systems of congruences, one for each modulus* $1 \leq f \in \mathbb{Z}$. *By the Chinese remainder theorem, such a compatible system of congruences is determined by a compatible system of congruences mod powers of* p *for every prime number* p:

$$\hat{\mathbb{Z}} \cong \prod_p \mathbb{Z}_p.$$

Let $\bar{K}$ be any algebraic closure of K. Let K^{unr} be the **maximal unramified extension** of K in $\bar{K}$, i.e., the compositum of all finite unramified extensions of K in $\bar{K}$. Then, we find a short exact sequence of topological groups (and continuous homomorphisms, in fact):

$$1 \to \mathrm{Gal}(\bar{K}/K^{unr}) \to \mathrm{Gal}(\bar{K}/K) \to \mathrm{Gal}(K^{unr}/K) \to 1.$$

By the previous example, we find

$$1 \to \mathrm{Gal}(\bar{K}/K^{unr}) \to \mathrm{Gal}(\bar{K}/K) \to \hat{\mathbb{Z}} \to 1.$$

If G is a topological group, let G^{ab} denote the quotient $G/\overline{[G,G]}$ of G by the closure[6] of its commutator subgroup. This is called the (topological) **abelianization** of G, and it satisfies the following important property:

[6] The quotient of a topological group by a closed subgroup is again a Hausdorff topological group. With a non-closed subgroup, one ends up with a non-Hausdorff quotient.

Proposition 9.11 *Every continuous homomorphism from G to a topological abelian group A factors uniquely through the quotient G^{ab}.*

For Galois extensions with Galois group G, the group G^{ab} plays an important role:

Proposition 9.12 *Let L/K be a (finite or infinite) Galois extensions of fields, with Galois group G. Let K^{ab} be the fixed field of $\overline{[G,G]}$, so $\mathrm{Gal}(K^{ab}/K) \cong G^{ab}$. Then K^{ab} is the maximal abelian Galois extension of K in L: every abelian Galois extension of K in L is contained in K^{ab}.*

The following is the main theorem of local class field theory:

Theorem 9.13 *Fix an algebraic closure $\bar{K}$ of K, and let K^{ab} be the maximal abelian extension of K in $\bar{K}$. There is a canonical embedding of groups:*

$$I\colon K^\times \to \mathrm{Gal}(\bar{K}/K)^{ab} = \mathrm{Gal}(K^{ab}/K),$$

which makes $K^\times$ a dense subgroup of $\mathrm{Gal}(K^{ab}/K)$, and for which the following diagram commutes:

$$\begin{array}{ccccccccc}
1 & \longrightarrow & A^\times & \longrightarrow & K^\times & \longrightarrow & \mathbb{Z} & \longrightarrow & 1 \\
 & & \downarrow{\scriptstyle \sim} & & \downarrow{\scriptstyle I} & & \downarrow & & \\
1 & \longrightarrow & \mathrm{Gal}(K^{ab}/K^{unr}) & \longrightarrow & \mathrm{Gal}(K^{ab}/K) & \longrightarrow & \hat{\mathbb{Z}} & \longrightarrow & 1.
\end{array}$$

Closely related to the above theorem is the following: there is a canonical inclusion

$$\mathrm{Hom}_{cont}(\mathrm{Gal}(\bar{K}/K), \mathbb{C}^\times) \hookrightarrow \mathrm{Hom}_{cont}(K^\times, \mathbb{C}^\times).$$

In other words, the continuous characters of $\mathrm{Gal}(\bar{K}/K^{unr})$ correspond to continuous characters of $K^\times$ (specifically, those whose image is contained in a subgroup of $\mathbb{C}^\times$ of finite order).

This is an important step towards understanding $G = \mathrm{Gal}(\bar{K}/K)$. Indeed, since G is a compact topological group, Tannaka duality implies that G is determined by the category of continuous finite-dimensional complex representations, i.e. the category whose objects are elements of $Hom_{cont}(G, GL_n(\mathbb{C}))$ for various n. Local class field theory describes these objects when $n = 1$. The recent proofs by Harris-Taylor and Henniart of the "local Langlands conjectures for GL_n" describe $\mathrm{Hom}_{cont}(G, GL_n(\mathbb{C}))$ as well.

9.3 *Global Fields*

Let us return, finally, to a number field $F/\mathbb{Q}$, and assume that F is a Galois extension of $\mathbb{Q}$ with $\Gamma = Gal(F/\mathbb{Q})$. Consider a prime number $p \in \mathbb{Z}$. By the factorization theory of ideals in $\mathcal{O}_F$, we find that there are distinct prime ideals $P_1, \ldots, P_t$ in $\mathcal{O}_F$, and positive integers $e_1, \ldots, e_t$, such that:

$$p\mathcal{O}_F = P_1^{e_1} \cdots P_t^{e_t}.$$

Furthermore, since $p\mathcal{O}_F$ is a Γ-fixed ideal in $\mathcal{O}_F$, we find that Γ acts on the set $\{P_1, \ldots, P_t\}$ of primes of $\mathcal{O}_F$ which **lie above** p. In fact, we have

Proposition 9.14 *Γ acts transitively on the set of primes of $\mathcal{O}_F$ which lie above p, and there exists a positive integer e such that*

$$p\mathcal{O}_F = P_1^e \cdots P_t^e.$$

Proof: For each prime ideal P of $\mathcal{O}_F$ lying above p, let F_P be the completion of F with respect to the P-adic valuation. One can check, using the universal property of completion, that F_P embeds topologically, and as an F-algebra, in $\mathbb{Q}_p \otimes_{\mathbb{Q}} F$. In particular, we find that F_P is an algebraic extension of $\mathbb{Q}_p$.

Conversely, every embedding of F into an algebraic closure of $\mathbb{Q}_p$ yields a valuation on F which restricts to the p-adic valuation on $\mathbb{Q}$, and hence yields a prime ideal P of $\mathcal{O}_F$ lying above p. In this way, we find a surjective function from the set of embeddings of F into a fixed algebraic closure of $\mathbb{Q}_p$ to the set of prime ideals of $\mathcal{O}_F$ lying above p. Moreover, this function is compatible with the natural action of Γ on each set; since Γ acts transitively on the set of embeddings of F into any algebraically closed field, we find that Γ acts transitively on the set of prime ideals of $\mathcal{O}_F$ lying above p.

Finally, since Γ acts transitively on the set $\{P_1, \ldots, P_t\}$, and

$$P_1^{e_1} \cdots P_t^{e_t} = p\mathcal{O}_F = \gamma(p\mathcal{O}_F) = P_{\gamma(1)}^{e_1} \cdots P_{\gamma(t)}^{e_t},$$

we find that $e_1 = e_2 = \cdots = e_t$.

□

Definition 9.15 *Suppose that p is a prime number, and P is a prime ideal of $\mathcal{O}_F$ lying above p. The **decomposition group** Γ_P at P is the subgroup of $\Gamma = \mathrm{Gal}(F/\mathbb{Q})$ which fixes P.*

In particular, since Γ acts transitively on the primes $\{P_1, \ldots, P_t\}$ above p, we find that

$$[\Gamma : \Gamma_P] = t.$$

Since Γ_P fixes P, Γ_P preserves the P-adic valuation on F. It follows directly that Γ_P maps injectively to the automorphism group $(F_P/\mathbb{Q}_p)$, where F_P is the finite extension of $\mathbb{Q}_p$ obtained by completing F.

On the other hand, we find that:

$$F \otimes_{\mathbb{Q}} \mathbb{Q}_p \cong F_{P_1} \times \cdots \times F_{P_t}.$$

It follows that (for any prime P lying above p):

$$n = t \cdot [F_P : \mathbb{Q}_p] = t \cdot \#\Gamma_P.$$

Thus F_P is a Galois extension of $\mathbb{Q}_p$, and Γ_p is isomorphic to $\mathrm{Gal}(F_P/\mathbb{Q}_p)$.

Once we can identify Γ_P with a Galois group of an extension $F_P/\mathbb{Q}_p$ of p-adic fields, we find a canonical subgroup Γ_P^{unr} whose fixed field is F_p^u, the maximal unramified extension of $\mathbb{Q}_p$ in F_P. This is called the **inertia subgroup** of Γ at P. We find a tower of subgroups and subfields:

$$\Gamma \supset \Gamma_P \supset \Gamma_P^{unr} \supset \{1\},$$

$$\mathbb{Q} \subset F^{\Gamma_P} \subset F^{\Gamma_P^{unr} \subset F.}$$

A corollary of our results is the following:

Proposition 9.16 *A prime p ramifies in F (i.e., $e > 1$) if and only if p divides* $\mathrm{Disc}(F)$.

Proof: The discriminant of F, i.e., the discriminant of $\mathcal{O}_F$ as a $\mathbb{Z}$-lattice with respect to the trace form, can also be computed "locally", i.e., in the valuation ring $\mathbb{Z}_p$ for any prime p. We have already seen that p divides this locally computed discriminant if and only if the extension of p-adic fields ramifies. The previous proposition demonstrates that this local ramification is equivalent to global ramification at p.

□

Corollary 9.17 *If F is a number field, and $F \neq \mathbb{Q}$, let $Ram(F)$ be the set of prime numbers which ramify in $\mathcal{O}_F$. Then $Ram(F)$ is finite and non-empty.*

Proof: If $F \neq \mathbb{Q}$, then we have seen that $\mathrm{Disc}(F) \neq \pm 1$. Thus $\mathrm{Disc}(F)$ has a prime factor p, which then ramifies. On the other hand, $\mathrm{Disc}(F)$ is an integer, and hence has only finitely many prime factors. Thus $Ram(F)$ is a finite set.

□

On the other hand, if F is a number field, it is often possible to find a larger number field $H \supset F$ such that no prime ideals of $\mathcal{O}_F$ ramify when factored in $\mathcal{O}_H$. The following result is quite deep, and belongs in a course on class field theory:

Theorem 9.18 *Let F be a number field. There exists a finite extension $H \supset F$, which is maximal among extensions of F in which no prime ideals of $\mathcal{O}_F$ ramify. Furthermore, the field H, called the* ***Hilbert class field*** *of F, is an abelian Galois extension of F, and $\mathrm{Gal}(H/F)$ is canonically isomorphic to the ideal class group $H(F)$.*

We finish by mentioning one more deep result. Suppose that p is a prime number, which does not ramify in $\mathcal{O}_F$. Thus we find that $F_P/\mathbb{Q}_p$ is an unramified extension of p-adic fields, for any prime P of $\mathcal{O}_F$ lying above p. In particular, there is a Frobenius element $Fr_P \in \Gamma_P$ for any such prime P. As all primes P above p are Γ-conjugate, we find that there is a well-defined *conjugacy class* Fr_p of Frobenius elements "at p": Fr_p is the conjugacy class in Γ, containing all of the elements Fr_P, for all primes P above p.

Theorem 9.19 (Tchebotarev density) *Let $Unr(F)$ be the set of prime numbers, which are unramified in the number field F, with $\Gamma = \mathrm{Gal}(F/\mathbb{Q})$ as before. Let C be a conjugacy class in Γ. Let $Unr_C(F)$ be the subset of $Unr(F)$, consisting of prime numbers p for which $Fr_p = C$. Then $Unr_C(F)$ is a subset of $Unr(F)$ with Dirichlet density $\#C/\#\Gamma$.*

It turns out that for any prime number p with $(p, n) = 1$, the conjugacy class of Fr_p in $\Gamma = \mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) = (\mathbb{Z}/n\mathbb{Z})^\times$ is determined by the congruence class of p modulo n. Tchebotarev density then implies that the prime numbers are equally distributed among the (possible) congruence classes modulo n.

Index

Bibliography

[1] David Brink. New light on Hensel's lemma. *Expo. Math.*, 24(4): 291–306, 2006. ISSN 0723-0869.

[2] Richard Dedekind. Sur la théorie des nombres entiers algébriques. *Darboux Bull. (2)*, I:17–41; 69–92; 114–164; 207–248, 1877.

[3] Richard Dedekind. *Theory of algebraic integers*. Cambridge Mathematical Library. Cambridge University Press, Cambridge, 1996. ISBN 0-521-56518-9. Translated from the 1877 French original and with an introduction by John Stillwell.

[4] Anthony W. Knapp. *Advanced algebra*. Cornerstones. Birkhäuser Boston Inc., Boston, MA, 2007. ISBN 978-0-8176-4522-9.

[5] James S. Milne. Algebraic number theory (v3.02), 2009. Available at www.jmilne.org/math/.

[6] Alexander Ostrowski. Über einige Lösungen der Funktionalgleichung $\psi(x) \cdot \psi(x) = \psi(xy)$. *Acta Math.*, 41(1):271–284, 1916. ISSN 0001-5962.

[7] Paulo Ribenboim. Equivalent forms of Hensel's lemma. *Exposition. Math.*, 3(1):3–24, 1985. ISSN 0723-0869.

[8] Herbert Robbins. A remark on Stirling's formula. *Amer. Math. Monthly*, 62:26–29, 1955. ISSN 0002-9890.