A Brief Introduction to Classical and Adelic Algebraic Number Theory

William Stein
(based heavily on works of Swinnerton-Dyer and Cassels)

May 2004

Contents

Chapter 1

Preface

This book is based on notes I created for a one-semester undergraduate course on Algebraic Number Theory, which I taught at Harvard during Spring 2004. The primary sources for the course were chapter 1 of Swinnerton-Dyer's book *A Brief Guide to Algebraic Number Theory* [SD01] and chapter 2 of Cassels's article *Global Fields* [Cas67]. I wrote these notes by following closely the above two chapters; in some cases I added substantial text and examples. For example, chapter 1 of [SD01] is 30 pages, whereas my rewrite of it occupies over 100 pages. In contrast, I follow [Cas67] more closely. *I have no intent whatever to plagiarize. I acknowledge as such those chapters in this book which are simply a close rewrite of [Cas67].* My goal is to take the useful classical article ([Cas67]) and make it more accessible to students by modernizing the notation, and adding additional explanations and examples.

I have no intent to publish this book with a traditional publisher, so it will remain freely available indefinitely. If you have comments, corrections, suggestions for additions, etc., please send them to me!

Please send me any typos or corrections: `was@math.harvard.edu`.

Acknowledgement: This book closely builds on Swinnerton-Dyer's book [SD01] and Cassels's article [Cas67]. Many of the students of Math 129 at Harvard during Spring 2004 made helpful comments: Jennifer Balakrishnan, Peter Behrooz, Jonathan Bloom, David Escott Jayce Getz, Michael Hamburg, Deniz Kural, Danielle li, Andrew Ostergaard Gregory Price, Grant Schoenebeck, Jennifer Sinnott, Stephen Walker, Daniel Weissman, and Inna Zakharevich. Also the course assistant Matt Bainbridge made many helpful comments.

Chapter 2

Introduction

2.1 Mathematical background I assume you have

In addition to general mathematical maturity, this book assumes you have the following background:

- Basics of finite group theory
- Commutative rings, ideals, quotient rings
- Some elementary number theory
- Basic Galois theory of fields
- Point set topology
- Basic of topological rings, groups, and measure theory

For example, if you have never worked with finite groups before, you should read another book first. If you haven't seen much elementary ring theory, there is still hope, but you will have to do some additional reading and exercises. I will briefly review the basics of the Galois theory of number fields.

Some of the homework problems involve using a computer, but I'll give you examples which you can build on. I will not assume that you have a programming background or know much about algorithms. If you don't have PARI [ABC$^+$] or Magma [BCP97], and don't want to install either one on your computer, you might want to try the following online interface to PARI and Magma:

`http://modular.fas.harvard.edu/calc/`

2.2 What is algebraic number theory?

A *number field* K is a finite algebraic extension of the rational numbers $\mathbf{Q}$. Every such extension can be represented as all polynomials in an algebraic number α:

$$K = \mathbf{Q}(\alpha) = \left\{ \sum_{n=0}^{m} a_n \alpha^n : a_n \in \mathbf{Q} \right\}.$$

Here α is a root of a polynomial with coefficients in $\mathbf{Q}$.

Algebraic number theory involves using techniques from (mostly commutative) algebra and finite group theory to gain a deeper understanding of number fields. The main objects that we study in algebraic number theory are number fields, rings of integers of number fields, unit groups, ideal class groups,norms, traces, discriminants, prime ideals, Hilbert and other class fields and associated reciprocity laws, zeta and L-functions, and algorithms for computing each of the above.

2.2.1 Topics in this book

These are some of the main topics that are discussed in this book:

- Rings of integers of number fields
- Unique factorization of ideals in Dedekind domains
- Structure of the group of units of the ring of integers
- Finiteness of the group of equivalence classes of ideals of the ring of integers (the “class group”)
- Decomposition and inertia groups, Frobenius elements
- Ramification
- Discriminant and different
- Quadratic and biquadratic fields
- Cyclotomic fields (and applications)
- How to use a computer to compute with many of the above objects (both algorithms and actual use of PARI and Magma).
- Valuations on fields
- Completions (p-adic fields)
- Adeles and Ideles

Note that we will not do anything nontrivial with zeta functions or L-functions. This is to keep the prerequisites to algebra, and so we will have more time to discuss algorithmic questions. Depending on time and your inclination, I may also talk about integer factorization, primality testing, or complex multiplication elliptic curves (which are closely related to quadratic imaginary fields).

2.3 Some applications of algebraic number theory

The following examples are meant to convince you that learning algebraic number theory now will be an excellent investment of your time. If an example below seems vague to you, it is safe to ignore it.

1. **Integer factorization** using the number field sieve. The number field sieve is the asymptotically fastest known algorithm for factoring general large integers (that don't have too special of a form). Recently, in December 2003, the number field sieve was used to factor the RSA-576 \$10000 challenge:

$$
\begin{aligned}
&188198812920607963838697239461650439807163563379417382700 7\ldots\\
&\ldots 633564229888597152346654853190606065047430453173880113033 9\ldots\\
&\ldots 6716199692321205734031879550656996221305168759307650257059\\
&= 398075086424064937397125500550386491199064362342526708 40\ldots\\
&\quad \ldots 6385189575946388957261768583317\\
&\qquad \times 472772146107435302536223071973048224632914695302097 11\ldots\\
&\qquad\quad \ldots 6459852171130520711256363590397527
\end{aligned}
$$

   (The ... indicates that the newline should be removed, not that there are missing digits.) For more information on the NFS, see the paper by Lenstra et al. on the Math 129 web page.

2. **Primality test:** Agrawal and his students Saxena and Kayal from India recently (2002) found the first ever deterministic polynomial-time (in the number of digits) primality test. There methods involve arithmetic in quotients of $(\mathbf{Z}/n\mathbf{Z})[x]$, which are best understood in the context of algebraic number theory. For example, Lenstra, Bernstein, and others have done that and improved the algorithm significantly.

3. **Deeper point of view** on questions in number theory:

   (a) Pell's Equation ($x^2 - dy^2 = 1$) $\Longrightarrow$ Units in real quadratic fields $\Longrightarrow$ Unit groups in number fields

   (b) Diophantine Equations $\Longrightarrow$ For which n does $x^n + y^n = z^n$ have a nontrivial solution in $\mathbf{Q}(\sqrt{2})$?

   (c) Integer Factorization $\Longrightarrow$ Factorization of ideals

   (d) Riemann Hypothesis $\Longrightarrow$ Generalized Riemann Hypothesis

(e) Deeper proof of Gauss's quadratic reciprocity law in terms of arithmetic of cyclotomic fields $\mathbf{Q}(e^{2\pi i/n})$, which leads to class field theory.

4. Wiles's proof of **Fermat's Last Theorem**, i.e., $x^n+y^n = z^n$ has no nontrivial integer solutions, uses methods from algebraic number theory extensively (in addition to many other deep techniques). Attempts to prove Fermat's Last Theorem long ago were hugely influential in the development of algebraic number theory (by Dedekind, Kummer, Kronecker, et al.).

5. **Arithmetic geometry:** This is a huge field that studies solutions to polynomial equations that lie in arithmetically interesting rings, such as the integers or number fields. A famous major triumph of arithmetic geometry is Faltings's proof of Mordell's Conjecture.

   Theorem 2.3.1 (Faltings). *Let X be a plane algebraic curve over a number field K. Assume that the manifold $X(\mathbf{C})$ of complex solutions to X has genus at least 2 (i.e., $X(\mathbf{C})$ is topologically a donut with two holes). Then the set $X(K)$ of points on X with coordinates in K is finite.*

   For example, Theorem 2.3.1 implies that for any $n \geq 4$ and any number field K, there are only finitely many solutions in K to $x^n + y^n = 1$. A famous open problem in arithmetic geometry is the **Birch and Swinnerton-Dyer conjecture**, which gives a deep conjectural criterion for exactly when $X(K)$ should be infinite when $X(\mathbf{C})$ is a torus.

Part I

Classical Viewpoint

Chapter 3

Finitely generated abelian groups

We will now prove the structure theorem for finitely generated abelian groups, since it will be crucial for much of what we will do later.

Let $\mathbf{Z} = \{0, \pm 1, \pm 2, \ldots\}$ denote the ring of integers, and for each positive integer n let $\mathbf{Z}/n\mathbf{Z}$ denote the ring of integers modulo n, which is a cyclic abelian group of order n under addition.

Definition 3.0.2 (Finitely Generated). A group G is *finitely generated* if there exists $g_1, \ldots, g_n \in G$ such that every element of G can be obtained from the g_i.

Theorem 3.0.3 (Structure Theorem for Abelian Groups). *Let G be a finitely generated abelian group. Then there is an isomorphism*

$$G \cong (\mathbf{Z}/n_1\mathbf{Z}) \oplus (\mathbf{Z}/n_2\mathbf{Z}) \oplus \cdots \oplus (\mathbf{Z}/n_s\mathbf{Z}) \oplus \mathbf{Z}^r,$$

where $n_1 > 1$ and $n_1 \mid n_2 \mid \cdots \mid n_s$. Furthermore, the n_i and r are uniquely determined by G.

We will prove the theorem as follows. We first remark that any subgroup of a finitely generated free abelian group is finitely generated. Then we see that finitely generated abelian groups can be presented as quotients of finite rank free abelian groups, and such a presentation can be reinterpreted in terms of matrices over the integers. Next we describe how to use row and column operations over the integers to show that every matrix over the integers is equivalent to one in a canonical diagonal form, called the Smith normal form. We obtain a proof of the theorem by reinterpreting Smith normal form in terms of groups.

Proposition 3.0.4. *Suppose G is a free abelian group of finite rank n, and H is a subgroup of G. Then H is a free abelian group generated by at most n elements.*

The key reason that this is true is that G is a finitely generated module over the principal ideal domain $\mathbf{Z}$. We will give a complete proof of a beautiful generalization of this result in the context of Noetherian rings next time, but will not prove this proposition here.

Corollary 3.0.5. *Suppose G is a finitely generated abelian group. Then there are finitely generated free abelian groups F_1 and F_2 such that $G \cong F_1/F_2$.*

Proof. Let $x_1, \ldots, x_m$ be generators for G. Let $F_1 = \mathbf{Z}^m$ and let $\varphi : F_1 \to G$ be the map that sends the ith generator $(0, 0, \ldots, 1, \ldots, 0)$ of $\mathbf{Z}^m$ to x_i. Then φ is a surjective homomorphism, and by Proposition 3.0.4 the kernel F_2 of φ is a finitely generated free abelian group. This proves the corollary. □

Suppose G is a nonzero finitely generated abelian group. By the corollary, there are free abelian groups F_1 and F_2 such that $G \cong F_1/F_2$. Choosing a basis for F_1, we obtain an isomorphism $F_1 \cong \mathbf{Z}^n$, for some positive integer n. By Proposition 3.0.4, $F_2 \cong \mathbf{Z}^m$, for some integer m with $0 \leq m \leq n$, and the inclusion map $F_2 \hookrightarrow F_1$ induces a map $\mathbf{Z}^m \to \mathbf{Z}^n$. This homomorphism is left multiplication by the $n \times m$ matrix A whose columns are the images of the generators of F_2 in $\mathbf{Z}^n$. The *cokernel* of this homomorphism is the quotient of $\mathbf{Z}^n$ by the image of A, and the cokernel is isomorphic to G. By augmenting A with zero columns on the right we obtain a square $n \times n$ matrix A with the same cokernel. The following proposition implies that we may choose bases such that the matrix A is diagonal, and then the structure of the cokernel of A will be easy to understand.

Proposition 3.0.6 (Smith normal form). *Suppose A is an $n \times n$ integer matrix. Then there exist invertible integer matrices P and Q such that $A' = PAQ$ is a diagonal matrix with entries $n_1, n_2, \ldots, n_s, 0, \ldots, 0$, where $n_1 > 1$ and $n_1 \mid n_2 \mid \ldots \mid n_s$. This is called the Smith normal form of A.*

We will see in the proof of Theorem 3.0.3 that A' is uniquely determined by A.

Proof. The matrix P will be a product of matrices that define elementary row operations and Q will be a product corresponding to elementary column operations. The elementary operations are:

1. Add an integer multiple of one row to another (or a multiple of one column to another).

2. Interchange two rows or two columns.

3. Multiply a row by -1.

Each of these operations is given by left or right multiplying by an invertible matrix E with integer entries, where E is the result of applying the given operation to the identity matrix, and E is invertible because each operation can be reversed using another row or column operation over the integers.

To see that the proposition must be true, assume $A \neq 0$ and perform the following steps (compare [Art91, pg. 459]):

1. By permuting rows and columns, move a nonzero entry of A with smallest absolute value to the upper left corner of A. Now attempt to make all other entries in the first row and column 0 by adding multiples of row or column 1 to other rows (see step 2 below). If an operation produces a nonzero entry in the matrix with absolute value smaller than $|a_{11}|$, start the process over by permuting rows and columns to move that entry to the upper left corner of A. Since the integers $|a_{11}|$ are a decreasing sequence of positive integers, we will not have to move an entry to the upper left corner infinitely often.

2. Suppose a_{i1} is a nonzero entry in the first column, with $i > 1$. Using the division algorithm, write $a_{i1} = a_{11}q + r$, with $0 \leq r < a_{11}$. Now add $-q$ times the first row to the ith row. If $r > 0$, then go to step 1 (so that an entry with absolute value at most r is the upper left corner). Since we will only perform step 1 finitely many times, we may assume $r = 0$. Repeating this procedure we set all entries in the first column (except a_{11}) to 0. A similar process using column operations sets each entry in the first row (except a_{11}) to 0.

3. We may now assume that a_{11} is the only nonzero entry in the first row and column. If some entry a_{ij} of A is not divisible by a_{11}, add the column of A containing a_{ij} to the first column, thus producing an entry in the first column that is nonzero. When we perform step 2, the remainder r will be greater than 0. Permuting rows and columns results in a smaller $|a_{11}|$. Since $|a_{11}|$ can only shrink finitely many times, eventually we will get to a point where every a_{ij} is divisible by a_{11}. If a_{11} is negative, multiple the first row by -1.

After performing the above operations, the first row and column of A are zero except for a_{11} which is positive and divides all other entries of A. We repeat the above steps for the matrix B obtained from A by deleting the first row and column. The upper left entry of the resulting matrix will be divisible by a_{11}, since every entry of B is. Repeating the argument inductively proves the proposition. $\square$

Example 3.0.7. The matrix $\begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix}$ is equivalent to $\begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix}$ and the matrix $\begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 7 & 8 & 9 \end{pmatrix}$ is equivalent to $\begin{pmatrix} 1 & 0 & 0 \\ 0 & 3 & 0 \\ 0 & 0 & 0 \end{pmatrix}$. Note that the determinants match, up to sign.

Theorem 3.0.3. Suppose G is a finitely generated abelian group, which we may assume is nonzero. As in the paragraph before Proposition 3.0.6, we use Corollary 3.0.5 to write G as a the cokernel of an $n \times n$ integer matrix A. By Proposition 3.0.6 there are isomorphisms $Q : \mathbf{Z}^n \to \mathbf{Z}^n$ and $P : \mathbf{Z}^n \to \mathbf{Z}^n$ such that $A' = PAQ$ is a diagonal matrix with entries $n_1, n_2, \ldots, n_s, 0, \ldots, 0$, where $n_1 > 1$ and $n_1 \mid n_2 \mid \ldots \mid n_s$. Then G is isomorphic to the cokernel of the diagonal matrix A', so

$$G \cong (\mathbf{Z}/n_1\mathbf{Z}) \oplus (\mathbf{Z}/n_2\mathbf{Z}) \oplus \cdots \oplus (\mathbf{Z}/n_s\mathbf{Z}) \oplus \mathbf{Z}^r, \tag{3.0.1}$$

as claimed. The n_i are determined by G, because n_i is the smallest positive integer n such that nG requires at most $s + r - i$ generators (we see from the representation (3.0.1) of G as a product that n_i has this property and that no smaller positive integer does).

$\square$

Chapter 4

Commutative Algebra

We will do some serious commutative algebra in this chapter, which will provide a powerful algebraic foundation for understanding the more refined number-theoretic structures associated to number fields.

In the first section we establish the standard properties of Noetherian rings and modules, including the Hilbert basis theorem. We also observe that finitely generated abelian groups are Noetherian $\mathbf{Z}$-modules, which fills the gap in our proof of the structure theorem for finitely generated abelian groups. After establishing properties of Noetherian rings, we consider the rings of algebraic integers and discuss some of their properties.

4.1 Noetherian Rings and Modules

Let R be a commutative ring with unit element. We will frequently work with R-modules, which are like vector spaces but over a ring. More precisely, recall that an *R-module* is an additive abelian group M equipped with a map $R \times M \to M$ such that for all $r, r' \in R$ and all $m, m' \in M$ we have $(rr')m = r(r'm)$, $(r + r')m = rm + r'm$, $r(m + m') = rm + rm'$, and $1m = m$. A *submodule* is a subgroup of M that is preserved by the action of R.

Example 4.1.1. The set of abelian groups are in natural bijection with $\mathbf{Z}$-modules.

A *homomorphism* of R-modules $\varphi : M \to N$ is a abelian group homomorphism such that for any $r \in R$ and $m \in M$ we have $\varphi(rm) = r\varphi(m)$. A *short exact sequence* of R-modules

$$0 \to L \xrightarrow{f} M \xrightarrow{g} N \to 0$$

is a specific choice of injective homomorphism $f : L \to M$ and a surjective homomorphism $g : M \to N$ such that $\mathrm{im}(f) = \ker(g)$.

Definition 4.1.2 (Noetherian). An R-module M is *Noetherian* if every submodule of M is finitely generated. A ring R is *Noetherian* if R is Noetherian as a module over itself, i.e., if every ideal of R is finitely generated.

Notice that any submodule M' of M is Noetherian, because if every submodule of M is finitely generated then so is every submodule of M', since submodules of M' are also submodules of M.

Definition 4.1.3 (Ascending chain condition). An R-module M satisfies the *ascending chain condition* if every sequences $M_1 \subset M_2 \subset M_3 \subset \cdots$ of submodules of M eventually stabilizes, i.e., there is some n such that $M_n = M_{n+1} = M_{n+2} = \cdots$.

Proposition 4.1.4. *If M is an R-module, then the following are equivalent:*

1. *M is Noetherian,*
2. *M satisfies the ascending chain condition, and*
3. *Every nonempty set of submodules of M contains at least one maximal element.*

Proof. $1 \implies 2$**:** Suppose $M_1 \subset M_2 \subset \cdots$ is a sequence of submodules of M. Then $M_\infty = \cup_{n=1}^\infty M_n$ is a submodule of M. Since M is Noetherian, there is a finite set $a_1, \ldots, a_m$ of generators for M. Each a_i must be contained in some M_j, so there is an n such that $a_1, \ldots, a_m \in M_n$. But then $M_k = M_n$ for all $k \geq n$, which proves that the ascending chain condition holds for M.
$2 \implies 3$**:** Suppose 3 were false, so there exists a nonempty set S of submodules of M that does not contain a maximal element. We will use S to construct an infinite ascending chain of submodules of M that does not stabilize. Note that S is infinite, otherwise it would contain a maximal element. Let M_1 be any element of S. Then there is an M_2 in S that contains M_1, otherwise S would contain the maximal element M_1. Continuing inductively in this way we find an M_3 in S that properly contains M_2, etc., and we produce an infinite ascending chain of submodules of M, which contradicts the ascending chain condition.
$3 \implies 1$**:** Suppose 1 is false, so there is a submodule M' of M that is not finitely generated. We will show that the set S of all finitely generated submodules of M' does not have a maximal element, which will be a contradiction. Suppose S does have a maximal element L. Since L is finitely generated and $L \subset M'$, and M' is not finitely generated, there is an $a \in M'$ such that $a \notin L$. Then $L' = L + Ra$ is an element of S that strictly contains the presumed maximal element L, a contradiction. □

Lemma 4.1.5. *If*

$$0 \to L \xrightarrow{f} M \xrightarrow{g} N \to 0$$

is a short exact sequence of R-modules, then M is Noetherian if and only if both L and N are Noetherian.

Proof. First suppose that M is Noetherian. Then L is a submodule of M, so L is Noetherian. If N' is a submodule of N, then the inverse image of N' in M is a submodule of M, so it is finitely generated, hence its image N' is finitely generated. Thus N is Noetherian as well.

Next assume nothing about M, but suppose that both L and N are Noetherian. If M' is a submodule of M, then $M_0 = \varphi(L) \cap M'$ is isomorphic to a submodule of the Noetherian module L, so M_0 is generated by finitely many elements $a_1, \ldots, a_n$. The quotient M'/M_0 is isomorphic (via g) to a submodule of the Noetherian module N, so M'/M_0 is generated by finitely many elements $b_1, \ldots, b_m$. For each $i \leq m$, let c_i be a lift of b_i to M', modulo M_0. Then the elements $a_1, \ldots, a_n, c_1, \ldots, c_m$ generate M', for if $x \in M'$, then there is some element $y \in M_0$ such that $x - y$ is an R-linear combination of the c_i, and y is an R-linear combination of the a_i. □

Proposition 4.1.6. *Suppose R is a Noetherian ring. Then an R-module M is Noetherian if and only if it is finitely generated.*

Proof. If M is Noetherian then every submodule of M is finitely generated so M is finitely generated. Conversely, suppose M is finitely generated, say by elements $a_1, \ldots, a_n$. Then there is a surjective homomorphism from $R^n = R \oplus \cdots \oplus R$ to M that sends $(0, \ldots, 0, 1, 0, \ldots, 0)$ (1 in ith factor) to a_i. Using Lemma 4.1.5 and exact sequences of R-modules such as $0 \to R \to R \oplus R \to R \to 0$, we see inductively that R^n is Noetherian. Again by Lemma 4.1.5, homomorphic images of Noetherian modules are Noetherian, so M is Noetherian. □

Lemma 4.1.7. *Suppose $\varphi : R \to S$ is a surjective homomorphism of rings and R is Noetherian. Then S is Noetherian.*

Proof. The kernel of φ is an ideal I in R, and we have an exact sequence

$$0 \to I \to R \to S \to 0$$

with R Noetherian. By Lemma 4.1.5, it follows that S is a Noetherian R-modules. Suppose J is an ideal of S. Since J is an R-submodule of S, if we view J as an R-module, then J is finitely generated. Since R acts on J through S, the R-generators of J are also S-generators of J, so J is finitely generated as an ideal. Thus S is Noetherian. □

Theorem 4.1.8 (Hilbert Basis Theorem). *If R is a Noetherian ring and S is finitely generated as a ring over R, then S is Noetherian. In particular, for any n the polynomial ring $R[x_1, \ldots, x_n]$ and any of its quotients are Noetherian.*

Proof. Assume first that we have already shown that for any n the polynomial ring $R[x_1, \ldots, x_n]$ is Noetherian. Suppose S is finitely generated as a ring over R, so there are generators $s_1, \ldots, s_n$ for S. Then the map $x_i \mapsto s_i$ extends uniquely to a surjective homomorphism $\pi : R[x_1, \ldots, x_n] \to S$, and Lemma 4.1.7 implies that S is Noetherian.

The rings $R[x_1, \ldots, x_n]$ and $(R[x_1, \ldots, x_{n-1}])[x_n]$ are isomorphic, so it suffices to prove that if R is Noetherian then $R[x]$ is also Noetherian. (Our proof follows

[Art91, §12.5].) Thus suppose I is an ideal of $R[x]$ and that R is Noetherian. We will show that I is finitely generated.

Let A be the set of leading coefficients of polynomials in I along with 0. If $a, b \in A$ are nonzero with $a + b \neq 0$, then there are polynomials f and g in I with leading coefficients a and b. If $\deg(f) \leq \deg(g)$, then $a + b$ is the leading coefficient of $x^{\deg(g)-\deg(f)} f + g$, so $a + b \in A$. If $r \in R$ and $a \in A$ with $ra \neq 0$, then ra is the leading coefficient of rf, so $ra \in A$. Thus A is an ideal in R, so since R is Noetherian there exists $a_1, \ldots, a_n$ that generate A as an ideal. Since A is the set of leading coefficients of elements of I, and the a_j are in I, we can choose for each $j \leq n$ an element $f_j \in I$ with leading coefficient a_j. By multipying the f_j by some power of x, we may assume that the f_j all have the same degree d.

Let $S_{<d}$ be the set of elements of I that have degree strictly less than d. This set is closed under addition and under multiplication by elements of R, so $S_{<d}$ is a module over R. The module $S_{<d}$ is submodule of the R-module of polynomials of degree less than n, which is Noetherian because it is generated by $1, x, \ldots, x^{n-1}$. Thus $S_{<d}$ is finitely generated, and we may choose generators $h_1, \ldots, h_m$ for $S_{<d}$.

Suppose $g \in I$ is an arbitrary element. We will show by induction on the degree of g that g is an $R[x]$-linear combination of $f_1, \ldots, f_n, h_1, \ldots h_m$. Thus suppose this statement is true for all elements of I of degree less than the degree of g. If the degree of g is less than d, then $g \in S_{<d}$, so g is in the $R[x]$-ideal generated by $h_1, \ldots, h_m$. Next suppose that g has degree $e \geq d$. Then the leading coefficient b of g lies in the ideal A of leading coefficients of g, so there exist $r_i \in R$ such that $b = r_1 a_1 + \cdots + r_n a_n$. Since f_i has leading coefficient a_i, the difference $g - x^{e-d} r_i f_i$ has degree less than the degree e of g. By induction $g - x^{e-d} r_i f_i$ is an $R[x]$ linear combination of $f_1, \ldots, f_n, h_1, \ldots h_m$, so g is also an $R[x]$ linear combination of $f_1, \ldots, f_n, h_1, \ldots h_m$. Since each f_i and h_j lies in I, it follows that I is generated by $f_1, \ldots, f_n, h_1, \ldots h_m$, so I is finitely generated, as required. $\square$

Properties of Noetherian rings and modules will be crucial in the rest of this course. We have proved above that Noetherian rings have many desirable properties.

4.1.1 Z is Noetherian

The ring $\mathbf{Z}$ of integers is Noetherian because every ideal of $\mathbf{Z}$ is generated by one element.

Proposition 4.1.9. *Every ideal of the ring $\mathbf{Z}$ of integers is principal.*

Proof. Suppose I is a nonzero ideal in $\mathbf{Z}$. Let d the least positive element of I. Suppose that $a \in I$ is any nonzero element of I. Using the division algorithm, write $a = dq + r$, where q is an integer and $0 \leq r < d$. We have $r = a - dq \in I$ and $r < d$, so our assumption that d is minimal implies that $r = 0$, so $a = dq$ is in the ideal generated by d. Thus I is the principal ideal generated by d. $\square$

Proposition 4.1.6 and 4.1.9 together imply that any finitely generated abelian group is Noetherian. This means that subgroups of finitely generated abelian groups are finitely generated, which provides the missing step in our proof of the structure theorem for finitely generated abelian groups.

Chapter 5

Rings of Algebraic Integers

In this chapter we will learn about rings of algebraic integers and discuss some of their properties. We will prove that the ring of integers $\mathcal{O}_K$ of a number field is Noetherian. We will also develop some basic properties of norms, traces, and discriminants, and give more properties of rings of integers in the general context of Dedekind domains.

5.1 Rings of Algebraic Integers

Fix an algebraic closure $\overline{\mathbf{Q}}$ of $\mathbf{Q}$. For example, $\overline{\mathbf{Q}}$ could be the subfield of the complex numbers $\mathbf{C}$ generated by all roots in $\mathbf{C}$ of all polynomials with coefficients in $\mathbf{Q}$.

Much of this course is about algebraic integers.

Definition 5.1.1 (Algebraic Integer). An element $\alpha \in \overline{\mathbf{Q}}$ is an *algebraic integer* if it is a root of some monic polynomial with coefficients in $\mathbf{Z}$.

Definition 5.1.2 (Minimal Polynomial). The *minimal polynomial* of $\alpha \in \mathbf{Q}$ is the monic polynomial $f \in \mathbf{Q}[x]$ of least positive degree such that $f(\alpha) = 0$.

The minimal polynomial of α divides any polynomial h such that $h(\alpha) = 0$, for the following reason. If $h(\alpha) = 0$, use the division algorithm to write $h = qf + r$, where $0 \leq \deg(r) < \deg(f)$. We have $r(\alpha) = h(\alpha) - q(\alpha)f(\alpha) = 0$, so α is a root of r. However, f is the polynomial of least positive degree with root α, so $r = 0$.

Lemma 5.1.3. *If α is an algebraic integer, then the minimal polynomial of α has coefficients in $\mathbf{Z}$.*

Proof. Suppose $f \in \mathbf{Q}[x]$ is the minimal polynomial of α and $g \in \mathbf{Z}[x]$ is a monic integral polynomial such that $g(\alpha) = 0$. As mentioned after the definition of minimal polynomial, we have $g = fh$, for some $h \in \mathbf{Q}[x]$. If $f \notin \mathbf{Z}[x]$, then some prime p divides the denominator of some coefficient of f. Let p^i be the largest power of p that divides some denominator of some coefficient f, and likewise let p^j be the largest power of p that divides some denominator of a coefficient of g. Then $p^{i+j}g = (p^i f)(p^j g)$, and if we reduce both sides modulo p, then the left hand side is 0 but the right hand side is a product of two nonzero polynomials in $\mathbf{F}_p[x]$, hence nonzero, a contradiction. $\square$

Proposition 5.1.4. *An element $\alpha \in \overline{\mathbf{Q}}$ is integral if and only if $\mathbf{Z}[\alpha]$ is finitely generated as a $\mathbf{Z}$-module.*

Proof. Suppose α is integral and let $f \in \mathbf{Z}[x]$ be the monic minimal polynomial of α (that $f \in \mathbf{Z}[x]$ is Lemma 5.1.3). Then $\mathbf{Z}[\alpha]$ is generated by $1, \alpha, \alpha^2, \ldots, \alpha^{d-1}$, where d is the degree of f. Conversely, suppose $\alpha \in \overline{\mathbf{Q}}$ is such that $\mathbf{Z}[\alpha]$ is finitely generated, say by elements $f_1(\alpha), \ldots, f_n(\alpha)$. Let d be any integer bigger than the degree of any f_i. Then there exist integers a_i such that $\alpha^d = \sum a_i f_i(\alpha)$, hence α satisfies the monic polynomial $x^d - \sum a_i f_i(x) \in \mathbf{Z}[x]$, so α is integral. $\square$

The rational number $\alpha = 1/2$ is not integral. Note that $G = \mathbf{Z}[1/2]$ is not a finitely generated $\mathbf{Z}$-module, since G is infinite and $G/2G = 0$.

Proposition 5.1.5. *The set $\overline{\mathbf{Z}}$ of all algebraic integers is a ring, i.e., the sum and product of two algebraic integers is again an algebraic integer.*

Proof. Suppose $\alpha, \beta \in \mathbf{Z}$, and let m, n be the degrees of the minimal polynomials of α, β, respectively. Then $1, \alpha, \ldots, \alpha^{m-1}$ span $\mathbf{Z}[\alpha]$ and $1, \beta, \ldots, \beta^{n-1}$ span $\mathbf{Z}[\beta]$ as $\mathbf{Z}$-module. Thus the elements $\alpha^i\beta^j$ for $i \leq m, j \leq n$ span $\mathbf{Z}[\alpha, \beta]$. Since $\mathbf{Z}[\alpha+\beta]$ is a submodule of the finitely-generated module $\mathbf{Z}[\alpha, \beta]$, it is finitely generated, so $\alpha + \beta$ is integral. Likewise, $\mathbf{Z}[\alpha\beta]$ is a submodule of $\mathbf{Z}[\alpha, \beta]$, so it is also finitely generated and $\alpha\beta$ is integral. $\square$

Recall that a *number field* is a subfield K of $\overline{\mathbf{Q}}$ such that the degree $[K : \mathbf{Q}] := \dim_{\mathbf{Q}}(K)$ is finite.

Definition 5.1.6 (Ring of Integers). The *ring of integers* of a number field K is the ring

$$\mathcal{O}_K = K \cap \overline{\mathbf{Z}} = \{x \in K : \ x \text{ is an algebraic integer}\}.$$

The field $\mathbf{Q}$ of rational numbers is a number field of degree 1, and the ring of integers of $\mathbf{Q}$ is $\mathbf{Z}$. The field $K = \mathbf{Q}(i)$ of Gaussian integers has degree 2 and $\mathcal{O}_K = \mathbf{Z}[i]$. The field $K = \mathbf{Q}(\sqrt{5})$ has ring of integers $\mathcal{O}_K = \mathbf{Z}[(1+\sqrt{5})/2]$. Note that the Golden ratio $(1+\sqrt{5})/2$ satisfies $x^2 - x - 1$. According to Magma, the ring of integers of $K = \mathbf{Q}(\sqrt[3]{9})$ is $\mathbf{Z}[\sqrt[3]{3}]$, where $\sqrt[3]{3} = \frac{1}{3}(\sqrt[3]{9})^2$.

Definition 5.1.7 (Order). An *order* in $\mathcal{O}_K$ is any subring R of $\mathcal{O}_K$ such that the quotient $\mathcal{O}_K/R$ of abelian groups is finite. (Note that R must contain 1 because it is a ring, and for us every ring has a 1.)

As noted above, $\mathbf{Z}[i]$ is the ring of integers of $\mathbf{Q}(i)$. For every nonzero integer n, the subring $\mathbf{Z} + ni\mathbf{Z}$ of $\mathbf{Z}[i]$ is an order. The subring $\mathbf{Z}$ of $\mathbf{Z}[i]$ is not an order, because $\mathbf{Z}$ does not have finite index in $\mathbf{Z}[i]$. Also the subgroup $2\mathbf{Z} + i\mathbf{Z}$ of $\mathbf{Z}[i]$ is not an order because it is not a ring.

We will frequently consider orders in practice because they are often much easier to write down explicitly than $\mathcal{O}_K$. For example, if $K = \mathbf{Q}(\alpha)$ and α is an algebraic integer, then $\mathbf{Z}[\alpha]$ is an order in $\mathcal{O}_K$, but frequently $\mathbf{Z}[\alpha] \neq \mathcal{O}_K$.

Lemma 5.1.8. *Let $\mathcal{O}_K$ be the ring of integers of a number field. Then $\mathcal{O}_K \cap \mathbf{Q} = \mathbf{Z}$ and $\mathbf{Q}\mathcal{O}_K = K$.*

Proof. Suppose $\alpha \in \mathcal{O}_K \cap \mathbf{Q}$ with $\alpha = a/b$ in lowest terms and $b > 0$. The monic minimal polynomial of α is $bx - a \in \mathbf{Z}[x]$, so if $b \neq 1$ then Lemma 5.1.3 implies that α is not an algebraic integer, a contradiction.

To prove that $\mathbf{Q}\mathcal{O}_K = K$, suppose $\alpha \in K$, and let $f(x) \in \mathbf{Q}[x]$ be the minimal monic polynomial of α. For any positive integer d, the minimal monic polynomial of $d\alpha$ is $d^{\deg(f)} f(x/d)$, i.e., the polynomial obtained from $f(x)$ by multiplying the coefficient of $x^{\deg(f)}$ by 1, multiplying the coefficient of $x^{\deg(f)-1}$ by d, multiplying the coefficient of $x^{\deg(f)-2}$ by d^2, etc. If d is the least common multiple of the denominators of the coefficients of f, then the minimal monic polynomial of $d\alpha$ has integer coefficients, so $d\alpha$ is integral and $d\alpha \in \mathcal{O}_K$. This proves that $\mathbf{Q}\mathcal{O}_K = K$. $\square$

In the next two sections we will develop some basic properties of norms and traces, and deduce further properties of rings of integers.

5.2 Norms and Traces

Before discussing norms and traces we introduce some notation for field extensions. If $K \subset L$ are number fields, we let $[L : K]$ denote the dimension of L viewed as a K-vector space. If K is a number field and $a \in \overline{\mathbf{Q}}$, let $K(a)$ be the number field generated by a, which is the smallest number field that contains a. If $a \in \overline{\mathbf{Q}}$ then a has a minimal polynomial $f(x) \in \mathbf{Q}[x]$, and the *Galois conjugates* of a are the roots of f. For example the element $\sqrt{2}$ has minimal polynomial $x^2 - 2$ and the Galois conjugates of $\sqrt{2}$ are $\pm\sqrt{2}$.

Suppose $K \subset L$ is an inclusion of number fields and let $a \in L$. Then left multiplication by a defines a K-linear transformation $\ell_a : L \to L$. (The transformation ℓ_a is K-linear because L is commutative.)

Definition 5.2.1 (Norm and Trace). The *norm* and *trace* of a from L to K are

$$\mathrm{Norm}_{L/K}(a) = \mathrm{Det}(\ell_a) \quad \text{and} \quad \mathrm{tr}_{L/K}(a) = \mathrm{tr}(\ell_a).$$

It is standard from linear algebra that determinants are multiplicative and traces are additive, so for $a, b \in L$ we have

$$\mathrm{Norm}_{L/K}(ab) = \mathrm{Norm}_{L/K}(a) \cdot \mathrm{Norm}_{L/K}(b)$$

and

$$\mathrm{tr}_{L/K}(a + b) = \mathrm{tr}_{L/K}(a) + \mathrm{tr}_{L/K}(b).$$

Note that if $f \in \mathbf{Q}[x]$ is the characteristic polynomial of ℓ_a, then the constant term of f is $(-1)^{\deg(f)} \operatorname{Det}(\ell_a)$, and the coefficient of $x^{\deg(f)-1}$ is $-\operatorname{tr}(\ell_a)$.

Proposition 5.2.2. *Let $a \in L$ and let $\sigma_1, \ldots, \sigma_d$, where $d = [L : K]$, be the distinct field embeddings $L \hookrightarrow \overline{\mathbf{Q}}$ that fix every element of K. Then*

$$\operatorname{Norm}_{L/K}(a) = \prod_{i=1}^{d} \sigma_i(a) \quad \text{and} \quad \operatorname{tr}_{L/K}(a) = \sum_{i=1}^{d} \sigma_i(a).$$

Proof. We prove the proposition by computing the characteristic polynomial F of a. Let $f \in K[x]$ be the minimal polynomial of a over K, and note that f has distinct roots (since it is the polynomial in $K[x]$ of least degree that is satisfied by a). Since f is irreducible, $[K(a) : K] = \deg(f)$, and a satisfies a polynomial if and only if ℓ_a does, the characteristic polynomial of ℓ_a acting on $K(a)$ is f. Let $b_1, \ldots, b_n$ be a basis for L over $K(a)$ and note that $1, \ldots, a^m$ is a basis for $K(a)/K$, where $m = \deg(f) - 1$. Then $a^i b_j$ is a basis for L over K, and left multiplication by a acts the same way on the span of $b_j, ab_j, \ldots, a^m b_j$ as on the span of $b_k, ab_k, \ldots, a^m b_k$, for any pair $j, k \leq n$. Thus the matrix of ℓ_a on L is a block direct sum of copies of the matrix of ℓ_a acting on $K(a)$, so the characteristic polynomial of ℓ_a on L is $f^{[L:K(a)]}$. The proposition follows because the roots of $f^{[L:K(a)]}$ are exactly the images $\sigma_i(a)$, with multiplicity $[L : K(a)]$ (since each embedding of $K(a)$ into $\overline{\mathbf{Q}}$ extends in exactly $[L : K(a)]$ ways to L by Exercise 9). □

The following corollary asserts that the norm and trace behave well in towers.

Corollary 5.2.3. *Suppose $K \subset L \subset M$ is a tower of number fields, and let $a \in M$. Then*

$$\operatorname{Norm}_{M/K}(a) = \operatorname{Norm}_{L/K}(\operatorname{Norm}_{M/L}(a)) \quad \text{and} \quad \operatorname{tr}_{M/K}(a) = \operatorname{tr}_{L/K}(\operatorname{tr}_{M/L}(a)).$$

Proof. For the first equation, both sides are the product of $\sigma_i(a)$, where σ_i runs through the embeddings of M into K. To see this, suppose $\sigma : L \to \overline{\mathbf{Q}}$ fixes K. If σ' is an extension of σ to M, and $\tau_1, \ldots, \tau_d$ are the embeddings of M into $\overline{\mathbf{Q}}$ that fix L, then $\tau_1\sigma', \ldots, \tau_d\sigma'$ are exactly the extensions of σ to M. For the second statement, both sides are the sum of the $\sigma_i(a)$. □

The norm and trace down to $\mathbf{Q}$ of an algebraic integer a is an element of $\mathbf{Z}$, because the minimal polynomial of a has integer coefficients, and the characteristic polynomial of a is a power of the minimal polynomial, as we saw in the proof of Proposition 5.2.2.

Proposition 5.2.4. *Let K be a number field. The ring of integers $\mathcal{O}_K$ is a lattice in K, i.e., $\mathbf{Q}\mathcal{O}_K = K$ and $\mathcal{O}_K$ is an abelian group of rank $[K : \mathbf{Q}]$.*

Proof. We saw in Lemma 5.1.8 that $\mathbf{Q}\mathcal{O}_K = K$. Thus there exists a basis $a_1, \ldots, a_n$ for K, where each a_i is in $\mathcal{O}_K$. Suppose that as $x = \sum c_i a_i \in \mathcal{O}_K$ varies over all elements of $\mathcal{O}_K$ the denominators of the coefficients c_i are arbitrarily large. Then subtracting off integer multiples of the a_i, we see that as $x = \sum c_i a_i \in \mathcal{O}_K$ varies over elements of $\mathcal{O}_K$ with c_i between 0 and 1, the denominators of the c_i are also arbitrarily large. This implies that there are infinitely many elements of $\mathcal{O}_K$ in the bounded subset

$$S = \{c_1 a_1 + \cdots + c_n a_n : c_i \in \mathbf{Q},\, 0 \leq c_i \leq 1\} \subset K.$$

Thus for any $\varepsilon > 0$, there are elements $a, b \in \mathcal{O}_K$ such that the coefficients of $a - b$ are all less than ε (otherwise the elements of $\mathcal{O}_K$ would all be a "distance" of least ε from each other, so only finitely many of them would fit in S).

As mentioned above, the norms of elements of $\mathcal{O}_K$ are integers. Since the norm of an element is the determinant of left multiplication by that element, the norm is a homogenous polynomial of degree n in the indeterminate coefficients c_i. If the c_i get arbitrarily small for elements of $\mathcal{O}_K$, then the values of the norm polynomial get arbitrarily small, which would imply that there are elements of $\mathcal{O}_K$ with positive norm too small to be in $\mathbf{Z}$, a contradiction. So the set S contains only finitely many elements of $\mathcal{O}_K$. Thus the denominators of the c_i are bounded, so for some d, we have that $\mathcal{O}_K$ has finite index in $A = \frac{1}{d}\mathbf{Z}a_1 + \cdots + \frac{1}{d}\mathbf{Z}a_n$. Since A is isomorphic to $\mathbf{Z}^n$, it follows from the structure theorem for finitely generated abelian groups that $\mathcal{O}_K$ is isomorphic as a $\mathbf{Z}$-module to $\mathbf{Z}^n$, as claimed. $\square$

Corollary 5.2.5. *The ring of integers $\mathcal{O}_K$ of a number field is Noetherian.*

Proof. By Proposition 5.2.4, the ring $\mathcal{O}_K$ is finitely generated as a module over $\mathbf{Z}$, so it is certainly finitely generated as a ring over $\mathbf{Z}$. By the Hilbert Basis Theorem, $\mathcal{O}_K$ is Noetherian. $\square$

Chapter 6

Unique Factorization of Ideals

In this chapter we will deduce, with complete proofs, the most important basic property of the ring of integers $\mathcal{O}_K$ of an algebraic number, namely that every nonzero ideals can be written uniquely as products of prime ideals. After proving this fundamental theorem, we will compute some examples using MAGMA. The next chapter will consist mostly of examples illustrating the substantial theory we will have already developed, so hang in there!

6.1 Dedekind Domains

Recall (Corollary 5.2.5) that we proved that the ring of integers $\mathcal{O}_K$ of a number field is Noetherian. As we saw before using norms, the ring $\mathcal{O}_K$ is finitely generated as a module over $\mathbf{Z}$, so it is certainly finitely generated as a ring over $\mathbf{Z}$. By the Hilbert Basis Theorem, $\mathcal{O}_K$ is Noetherian.

If R is an integral domain, the *field of fractions* of R is the field of all elements a/b, where $a, b \in R$. The field of fractions of R is the smallest field that contains R. For example, the field of fractions of $\mathbf{Z}$ is $\mathbf{Q}$ and of $\mathbf{Z}[(1+\sqrt{5})/2]$ is $\mathbf{Q}(\sqrt{5})$.

Definition 6.1.1 (Integrally Closed). An integral domain R is *integrally closed in its field of fractions* if whenever α is in the field of fractions of R and α satisfies a monic polynomial $f \in R[x]$, then $\alpha \in R$.

Proposition 6.1.2. *If K is any number field, then $\mathcal{O}_K$ is integrally closed. Also, the ring $\overline{\mathbf{Z}}$ of all algebraic integers is integrally closed.*

Proof. We first prove that $\overline{\mathbf{Z}}$ is integrally closed. Suppose $c \in \overline{\mathbf{Q}}$ is integral over $\overline{\mathbf{Z}}$, so there is a monic polynomial $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$ with $a_i \in \overline{\mathbf{Z}}$ and $f(c) = 0$. The a_i all lie in the ring of integers $\mathcal{O}_K$ of the number field $K = \mathbf{Q}(a_0, a_1, \ldots a_{n-1})$, and $\mathcal{O}_K$ is finitely generated as a $\mathbf{Z}$-module, so $\mathbf{Z}[a_0, \ldots, a_{n-1}]$ is finitely generated as a $\mathbf{Z}$-module. Since $f(c) = 0$, we can write c^n as a $\mathbf{Z}[a_0, \ldots, a_{n-1}]$-linear combination of c^i for $i < n$, so the ring $\mathbf{Z}[a_0, \ldots, a_{n-1}, c]$ is also finitely generated as a $\mathbf{Z}$-module. Thus $\mathbf{Z}[c]$ is finitely generated as $\mathbf{Z}$-module because it is a submodule of a finitely generated $\mathbf{Z}$-module, which implies that c is integral over $\mathbf{Z}$.

Suppose $c \in K$ is integral over $\mathcal{O}_K$. Then since $\overline{\mathbf{Z}}$ is integrally closed, c is an element of $\overline{\mathbf{Z}}$, so $c \in K \cap \overline{\mathbf{Z}} = \mathcal{O}_K$, as required. □

Definition 6.1.3 (Dedekind Domain). An integral domain R is a *Dedekind domain* if it is Noetherian, integrally closed in its field of fractions, and every nonzero prime ideal of R is maximal.

The ring $\mathbf{Q} \oplus \mathbf{Q}$ is Noetherian, integrally closed in its field of fractions, and the two prime ideals are maximal. However, it is not a Dedekind domain because it is not an integral domain. The ring $\mathbf{Z}[\sqrt{5}]$ is not a Dedekind domain because it is not integrally closed in its field of fractions, as $(1+\sqrt{5})/2$ is integrally over $\mathbf{Z}$ and lies in $\mathbf{Q}(\sqrt{5})$, but not in $\mathbf{Z}[\sqrt{5}]$. The ring $\mathbf{Z}$ is a Dedekind domain, as is any ring of integers $\mathcal{O}_K$ of a number field, as we will see below. Also, any field K is a Dedekind domain, since it is a domain, it is trivially integrally closed in itself, and there are no nonzero prime ideals so that condition that they be maximal is empty.

Proposition 6.1.4. *The ring of integers $\mathcal{O}_K$ of a number field is a Dedekind domain.*

Proof. By Proposition 6.1.2, the ring $\mathcal{O}_K$ is integrally closed, and by Proposition 5.2.5 it is Noetherian. Suppose that $\mathfrak{p}$ is a nonzero prime ideal of $\mathcal{O}_K$. Let $\alpha \in \mathfrak{p}$ be a nonzero element, and let $f(x) \in \mathbf{Z}[x]$ be the minimal polynomial of α. Then

$$f(\alpha) = \alpha^n + a_{n-1}\alpha^{n-1} + \cdots + a_1\alpha + a_0 = 0,$$

so $a_0 = -(\alpha^n + a_{n-1}\alpha^{n-1} + \cdots + a_1\alpha) \in \mathfrak{p}$. Since f is irreducible, a_0 is a nonzero element of $\mathbf{Z}$ that lies in $\mathfrak{p}$. Every element of the finitely generated abelian group $\mathcal{O}_K/\mathfrak{p}$ is killed by a_0, so $\mathcal{O}_K/\mathfrak{p}$ is a finite set. Since $\mathfrak{p}$ is prime, $\mathcal{O}_K/\mathfrak{p}$ is an integral domain. Every finite integral domain is a field, so $\mathfrak{p}$ is maximal, which completes the proof. □

If I and J are ideals in a ring R, the product IJ is the ideal generated by all products of elements in I with elements in J:

$$IJ = (ab : a \in I, b \in J) \subset R.$$

Note that the set of all products ab, with $a \in I$ and $b \in J$, need not be an ideal, so it is important to take the ideal generated by that set. (See the homework problems for examples.)

Definition 6.1.5 (Fractional Ideal). A *fractional ideal* is an $\mathcal{O}_K$-submodule of $I \subset K$ that is finitely generated as an $\mathcal{O}_K$-module.

To avoid confusion, we will sometimes call a genuine ideal $I \subset \mathcal{O}_K$ an *integral ideal.* Also, since fractional ideals are finitely generated, we can clear denominators of a generating set to see that every fractional ideal is of the form $aI = \{ab : b \in I\}$ for some $a \in K$ and ideal $I \subset \mathcal{O}_K$.

For example, the collection $\frac{1}{2}\mathbf{Z}$ of rational numbers with denominator 1 or 2 is a fractional ideal of $\mathbf{Z}$.

Theorem 6.1.6. *The set of nonzero fractional ideals of a Dedekind domain R is an abelian group under ideal multiplication.*

Before proving Theorem 6.1.6 we prove a lemma. For the rest of this section $\mathcal{O}_K$ is the ring of integers of a number field K.

Definition 6.1.7 (Divides for Ideals). Suppose that I, J are ideals of $\mathcal{O}_K$. Then I *divides* J if $I \supset J$.

To see that this notion of divides is sensible, suppose $K = \mathbf{Q}$, so $\mathcal{O}_K = \mathbf{Z}$. Then $I = (n)$ and $J = (m)$ for some integer n and m, and I divides J means that $(n) \supset (m)$, i.e., that there exists an integer c such that $m = cn$, which exactly means that n divides m, as expected.

Lemma 6.1.8. *Suppose I is an ideal of $\mathcal{O}_K$. Then there exist prime ideals $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$ such that $\mathfrak{p}_1 \cdot \mathfrak{p}_2 \cdots \mathfrak{p}_n \subset I$. In other words, I divides a product of prime ideals. (By convention the empty product is the unit ideal. Also, if $I = 0$, then we take $\mathfrak{p}_1 = (0)$, which is a prime ideal.)*

Proof. The key idea is to use that $\mathcal{O}_K$ is Noetherian to deduce that the set S of ideals that do not satisfy the lemma is empty. If S is nonempty, then because $\mathcal{O}_K$ is Noetherian, there is an ideal $I \in S$ that is maximal as an element of S. If I were prime, then I would trivially contain a product of primes, so I is not prime. By definition of prime ideal, there exists $a, b \in \mathcal{O}_K$ such that $ab \in I$ but $a \notin I$ and $b \notin I$. Let $J_1 = I + (a)$ and $J_2 = I + (b)$. Then neither J_1 nor J_2 is in S, since I is maximal, so both J_1 and J_2 contain a product of prime ideals. Thus so does I, since

$$J_1 J_2 = I^2 + I(b) + (a)I + (ab) \subset I,$$

which is a contradiction. Thus S is empty, which completes the proof. $\square$

We are now ready to prove the theorem.

Proof of Theorem 6.1.6. The product of two fractional ideals is again finitely generated, so it is a fractional ideal, and $I\mathcal{O}_K = \mathcal{O}_K$ for any nonzero ideal I, so to prove that the set of fractional ideals under multiplication is a group it suffices to show the existence of inverses. We will first prove that if $\mathfrak{p}$ is a prime ideal, then $\mathfrak{p}$ has an inverse, then we will prove that nonzero integral ideals have inverses, and finally observe that every fractional ideal has an inverse.

Suppose $\mathfrak{p}$ is a nonzero prime ideal of $\mathcal{O}_K$. We will show that the $\mathcal{O}_K$-module

$$I = \{a \in K : a\mathfrak{p} \subset \mathcal{O}_K\}$$

is a fractional ideal of $\mathcal{O}_K$ such that $I\mathfrak{p} = \mathcal{O}_K$, so that I is an inverse of $\mathfrak{p}$.

For the rest of the proof, fix a nonzero element $b \in \mathfrak{p}$. Since I is an $\mathcal{O}_K$-module, $bI \subset \mathcal{O}_K$ is an $\mathcal{O}_K$ ideal, hence I is a fractional ideal. Since $\mathcal{O}_K \subset I$ we have $\mathfrak{p} \subset I\mathfrak{p} \subset \mathcal{O}_K$, hence either $\mathfrak{p} = I\mathfrak{p}$ or $I\mathfrak{p} = \mathcal{O}_K$. If $I\mathfrak{p} = \mathcal{O}_K$, we are done since then I is an inverse of $\mathfrak{p}$. Thus suppose that $I\mathfrak{p} = \mathfrak{p}$. Our strategy is to show that there is some $d \in I$ not in $\mathcal{O}_K$; such a d would leave $\mathfrak{p}$ invariant (i.e., $d\mathfrak{p} \subset \mathfrak{p}$), so since $\mathfrak{p}$ is an $\mathcal{O}_K$-module it will follow that $d \in \mathcal{O}_K$, a contradiction.

By Lemma 6.1.8, we can choose a product $\mathfrak{p}_1, \ldots, \mathfrak{p}_m$, with m minimal, such that

$$\mathfrak{p}_1\mathfrak{p}_2 \cdots \mathfrak{p}_m \subset (b) \subset \mathfrak{p}.$$

If no $\mathfrak{p}_i$ is contained in $\mathfrak{p}$, then we can choose for each i an $a_i \in \mathfrak{p}_i$ with $a_i \notin \mathfrak{p}$; but then $\prod a_i \in \mathfrak{p}$, which contradicts that $\mathfrak{p}$ is a prime ideal. Thus some $\mathfrak{p}_i$, say $\mathfrak{p}_1$, is contained in $\mathfrak{p}$, which implies that $\mathfrak{p}_1 = \mathfrak{p}$ since every nonzero prime ideal is maximal. Because m is minimal, $\mathfrak{p}_2 \cdots \mathfrak{p}_m$ is not a subset of (b), so there exists $c \in \mathfrak{p}_2 \cdots \mathfrak{p}_m$ that does not lie in (b). Then $\mathfrak{p}(c) \subset (b)$, so by definition of I we have $d = c/b \in I$. However, $d \notin \mathcal{O}_K$, since if it were then c would be in (b). We have thus found our element $d \in I$ that does not lie in $\mathcal{O}_K$. To finish the proof that $\mathfrak{p}$ has an inverse, we observe that d preserves the $\mathcal{O}_K$-module $\mathfrak{p}$, and is hence in $\mathcal{O}_K$, a contradiction. More precisely, if $b_1, \ldots, b_n$ is a basis for $\mathfrak{p}$ as a $\mathbf{Z}$-module, then the action of d on $\mathfrak{p}$ is given by a matrix with entries in $\mathbf{Z}$, so the minimal polynomial of d has coefficients in $\mathbf{Z}$. This implies that d is integral over $\mathbf{Z}$, so $d \in \mathcal{O}_K$, since $\mathcal{O}_K$ is integrally closed by Proposition 6.1.2. (Note how this argument depends strongly on the fact that $\mathcal{O}_K$ is integrally closed!)

So far we have proved that if $\mathfrak{p}$ is a prime ideal of $\mathcal{O}_K$, then $\mathfrak{p}^{-1} = \{a \in \mathbf{K} : a\mathfrak{p} \subset \mathcal{O}_K\}$ is the inverse of $\mathfrak{p}$ in the monoid of nonzero fractional ideals of $\mathcal{O}_K$. As mentioned after Definition 6.1.5 [on Tuesday], every nonzero fractional ideal is of the form aI for $a \in K$ and I an integral ideal, so since (a) has inverse $(1/a)$, it suffices to show that every integral ideal I has an inverse. If not, then there is a nonzero integral ideal I that is maximal among all nonzero integral ideals that do not have an inverse. Every ideal is contained in a maximal ideal, so there is a nonzero prime ideal $\mathfrak{p}$ such that $I \subset \mathfrak{p}$. Multiplying both sides of this inclusion by $\mathfrak{p}^{-1}$ and using that $\mathcal{O}_K \subset \mathfrak{p}^{-1}$, we see that $I \subset \mathfrak{p}^{-1}I \subset \mathcal{O}_K$. If $I = \mathfrak{p}^{-1}I$, then arguing as in the proof that $\mathfrak{p}^{-1}$ is the inverse of $\mathfrak{p}$, we see that each element of $\mathfrak{p}^{-1}$ preserves the finitely generated $\mathbf{Z}$-module I and is hence integral. But then $\mathfrak{p}^{-1} \subset \mathcal{O}_K$, which implies that $\mathcal{O}_K = \mathfrak{p}\mathfrak{p}^{-1} \subset \mathfrak{p}$, a contradiction. Thus $I \neq \mathfrak{p}^{-1}I$. Because I is maximal among ideals that do not have an inverse, the ideal $\mathfrak{p}^{-1}I$ does have an inverse, call it J. Then $\mathfrak{p}J$ is the inverse of I, since $\mathcal{O}_K = (\mathfrak{p}J)(\mathfrak{p}^{-1}I) = JI$. $\square$

We can finally deduce the crucial Theorem 6.1.10, which will allow us to show that any nonzero ideal of a Dedekind domain can be expressed uniquely as a product of primes (up to order). Thus unique factorization holds for ideals in a Dedekind domain, and it is this unique factorization that initially motivated the introduction of rings of integers of number fields over a century ago.

Theorem 6.1.9. *Suppose I is an integral ideal of $\mathcal{O}_K$. Then I can be written as a product*

$$I = \mathfrak{p}_1 \cdots \mathfrak{p}_n$$

of prime ideals of $\mathcal{O}_K$, and this representation is unique up to order. (Exception: If $I = 0$, then the representation is not unique.)

Proof. Suppose I is an ideal that is maximal among the set of all ideals in $\mathcal{O}_K$ that can not be written as a product of primes. Every ideal is contained in a maximal ideal, so I is contained in a nonzero prime ideal $\mathfrak{p}$. If $I\mathfrak{p}^{-1} = I$, then by Theorem 6.1.6 we can cancel I from both sides of this equation to see that $\mathfrak{p}^{-1} = \mathcal{O}_K$, a contradiction. Thus I is strictly contained in $I\mathfrak{p}^{-1}$, so by our maximality assumption on I there are maximal ideals $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$ such that $I\mathfrak{p}^{-1} = \mathfrak{p}_1 \cdots \mathfrak{p}_n$. Then $I = \mathfrak{p} \cdot \mathfrak{p}_1 \cdots \mathfrak{p}_n$, a contradiction. Thus every ideal can be written as a product of primes.

Suppose $\mathfrak{p}_1 \cdots \mathfrak{p}_n = \mathfrak{q}_1 \cdots \mathfrak{q}_m$. If no $\mathfrak{q}_i$ is contained in $\mathfrak{p}_1$, then for each i there is an $a_i \in \mathfrak{q}_i$ such that $a_i \notin \mathfrak{p}_1$. But the product of the a_i is in the $\mathfrak{p}_1 \cdots \mathfrak{p}_n$, which is a subset of $\mathfrak{p}_1$, which contradicts the fact that $\mathfrak{p}_1$ is a prime ideal. Thus $\mathfrak{q}_i = \mathfrak{p}_1$ for some i. We can thus cancel $\mathfrak{q}_i$ and $\mathfrak{p}_1$ from both sides of the equation. Repeating this argument finishes the proof of uniqueness. □

Corollary 6.1.10. *If I is a fractional ideal of $\mathcal{O}_K$ then there exists prime ideals $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$ and $\mathfrak{q}_1, \ldots, \mathfrak{q}_m$, unique up to order, such that*

$$I = (\mathfrak{p}_1 \cdots \mathfrak{p}_n)(\mathfrak{q}_1 \cdots \mathfrak{q}_m)^{-1}.$$

Proof. We have $I = (a/b)J$ for some $a, b \in \mathcal{O}_K$ and integral ideal J. Applying Theorem 6.1.10 to (a), (b), and J gives an expression as claimed. For uniqueness, if one has two such product expressions, multiply through by the denominators and use the uniqueness part of Theorem 6.1.10 □

Example 6.1.11. The ring of integers of $K = \mathbf{Q}(\sqrt{-6})$ is $\mathcal{O}_K = \mathbf{Z}[\sqrt{-6}]$. In $\mathcal{O}_K$, we have

$$6 = -\sqrt{-6}\sqrt{-6} = 2 \cdot 3.$$

If $ab = \sqrt{-6}$, with $a, b \in \mathcal{O}_K$ and neither a unit, then $\mathrm{Norm}(a)\,\mathrm{Norm}(b) = 6$, so without loss $\mathrm{Norm}(a) = 2$ and $\mathrm{Norm}(b) = 3$. If $a = c + d\sqrt{-6}$, then $\mathrm{Norm}(a) = c^2 + 6d^2$; since the equation $c^2 + 6d^2 = 2$ has no solution with $c, d \in \mathbf{Z}$, there is no element in $\mathcal{O}_K$ with norm 2, so $\sqrt{-6}$ is irreducible. Also, $\sqrt{-6}$ is not a unit times 2 or times 3, since again the norms would not match up. Thus 6 can not be written uniquely as a product of irreducibles in $\mathcal{O}_K$. Theorem 6.1.9, however, implies that the principal ideal (6) can, however, be written uniquely as a product of prime ideals. Using MAGMA we find such a decomposition:

```
> R<x> := PolynomialRing(RationalField());
> K := NumberField(x^2+6);
> OK := MaximalOrder(K);
```

```
> [K!b : b in Basis(OK)];
[
    1,
    K.1    // this is sqrt(-6)
]
> Factorization(6*OK);
[
    <Prime Ideal of OK
    Two element generators:
        [2, 0]
        [2, 1], 2>,
    <Prime Ideal of OK
    Two element generators:
        [3, 0]
        [3, 1], 2>
]
```

The output means that

$$(6) = (2, 2 + \sqrt{-6})^2 \cdot (3, 3 + \sqrt{-6})^2,$$

where each of the ideals $(2, 2 + \sqrt{-6})$ and $(3, 3 + \sqrt{-6})$ is prime. I will discuss algorithms for computing such a decomposition in detail, probably next week. The first idea is to write $(6) = (2)(3)$, and hence reduce to the case of writing the (p), for $p \in \mathbf{Z}$ prime, as a product of primes. Next one decomposes the Artinian ring $\mathcal{O}_K \otimes \mathbf{F}_p$ as a product of local Artinian rings.

Chapter 7

Computing

7.1 Algorithms for Algebraic Number Theory

I think the best overall reference for algorithms for doing basic algebraic number theory computations is [Coh93].

Our main long-term algorithmic goals for this book (which we won't succeed at reaching) are to understand good algorithms for solving the following problems in particular cases:

- **Ring of integers:** Given a number field K (by giving a polynomial), compute the full ring $\mathcal{O}_K$ of integers.
- **Decomposition of primes:** Given a prime number $p \in \mathbf{Z}$, find the decomposition of the ideal $p\mathcal{O}_K$ as a product of prime ideals of $\mathcal{O}_K$.
- **Class group:** Compute the group of equivalence classes of nonzero ideals of $\mathcal{O}_K$, where I and J are equivalent if there exists $\alpha \in \mathcal{O}_K$ such that $IJ^{-1} = (\alpha)$.
- **Units:** Compute generators for the group of units of $\mathcal{O}_K$.

As we will see, somewhat surprisingly it turns out that algorithmically by far the most time-consuming step in computing the ring of integers $\mathcal{O}_K$ seems to be to factor the discriminant of a polynomial whose root generates the field K. The algorithm(s) for computing $\mathcal{O}_K$ are quite complicated to describe, but the first step is to factor this discriminant, and it takes much longer in practice than all the other complicated steps.

7.2 Using MAGMA

This section is a first introduction to MAGMA for algebraic number theory. MAGMA is a good general purpose package for doing algebraic number theory computations. You can use it via the web page `http://modular.fas.harvard.edu/calc`. MAGMA is not free, but student discounts are available.

The following examples illustrate what we've done so far in the course using MAGMA, and a little of where we are going. Feel free to ask questions as we go.

7.2.1 Smith Normal Form

On the first day of class we learned about Smith normal forms of matrices.

```
> A := Matrix(2,2,[1,2,3,4]);
> A;
[1 2]
[3 4]
> SmithForm(A);
[1 0]
[0 2]

[ 1  0]
[-1  1]

[-1  2]
[ 1 -1]
```

As you can see, MAGMA computed the Smith form, which is $\begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix}$. What are the other two matrices it output? To see what any MAGMA command does, type the command by itself with no arguments followed by a semicolon.

```
> SmithForm;
Intrinsic 'SmithForm'

Signatures:

    (<Mtrx> X) -> Mtrx, AlgMatElt, AlgMatElt
    [
        k: RngIntElt,
        NormType: MonStgElt,
        Partial: BoolElt,
        RightInverse: BoolElt
    ]

        The smith form S of X, together with unimodular matrices
        P and Q such that P * X * Q = S.
```

As you can see, `SmithForm` returns three arguments, a matrix and matrices P and Q that transform the input matrix to Smith normal form. The syntax to "receive" three return arguments is natural, but uncommon in other programming languages:

```
> S, P, Q := SmithForm(A);
> S;
[1 0]
[0 2]
> P;
[ 1  0]
[-1  1]
> Q;
[-1  2]
[ 1 -1]
> P*A*Q;
[1 0]
[0 2]
```

Next, let's test the limits. We make a 10×10 integer matrix with entries between 0 and 99, and compute its Smith normal form.

```
> A := Matrix(10,10,[Random(100) : i in [1..100]]);
> time B := SmithForm(A);
Time: 0.000
```

Let's print the first row of A, the first and last row of B, and the diagonal of B:

```
> A[1];
( 4 48 84  3 58 61 53 26  9  5)
> B[1];
(1 0 0 0 0 0 0 0 0 0)
> B[10];
(0 0 0 0 0 0 0 0 0 51805501538039733)
> [B[i,i] : i in [1..10]];
[ 1, 1, 1, 1, 1, 1, 1, 1, 1, 51805501538039733 ]
```

Let's see how big we have to make A in order to slow down MAGMA. These timings below are on a 1.6Ghz Pentium 4-M laptop running Magma V2.11 under VMware Linux. I tried exactly the same computation running Magma V2.17 natively under Windows XP on the same machine, and it takes *twice* as long to do each computation, which is strange.

```
> n := 50; A := Matrix(n,n,[Random(100) : i in [1..n^2]]);
> time B := SmithForm(A);
Time: 0.050
> n := 100; A := Matrix(n,n,[Random(100) : i in [1..n^2]]);
> time B := SmithForm(A);
Time: 0.800
> n := 150; A := Matrix(n,n,[Random(100) : i in [1..n^2]]);
> time B := SmithForm(A);
```

```
Time: 4.900
> n := 200; A := Matrix(n,n,[Random(100) : i in [1..n^2]]);
> time B := SmithForm(A);
Time: 19.160
```

MAGMA can also work with finitely generated abelian groups.

```
> G := AbelianGroup([3,5,18]);
> G;
Abelian Group isomorphic to Z/3 + Z/90
Defined on 3 generators
Relations:
    3*G.1 = 0
    5*G.2 = 0
    18*G.3 = 0
> #G;
270
> H := sub<G | [G.1+G.2]>;
> #H;
15
> G/H;
Abelian Group isomorphic to Z/18
```

7.2.2 $\overline{\mathbf{Q}}$ and Number Fields

MAGMA has many commands for doing basic arithmetic with $\overline{\mathbf{Q}}$.

```
> Qbar := AlgebraicClosure(RationalField());
> Qbar;
> S<x> := PolynomialRing(Qbar);
> r := Roots(x^3-2);
> r;
[
    <r1, 1>,
    <r2, 1>,
    <r3, 1>
]
> a := r[1][1];
> MinimalPolynomial(a);
x^3 - 2
> s := Roots(x^2-7);
> b := s[1][1];
> MinimalPolynomial(b);
x^2 - 7
> a+b;
```

```
r4 + r1
> MinimalPolynomial(a+b);
x^6 - 21*x^4 - 4*x^3 + 147*x^2 - 84*x - 339
> Trace(a+b);
0
> Norm(a+b);
-339
```

There are few commands for general algebraic number fields, so usually we work in specific finitely generated subfields:

```
> MinimalPolynomial(a+b);
x^6 - 21*x^4 - 4*x^3 + 147*x^2 - 84*x - 339
> K := NumberField($1) ;  // $1 = result of previous computation.
> K;
Number Field with defining polynomial x^6 - 21*x^4 - 4*x^3 +
    147*x^2 - 84*x - 339 over the Rational Field
```

We can also define relative extensions of number fields and pass to the corresponding absolute extension.

```
> R<x> := PolynomialRing(RationalField());
> K<a> := NumberField(x^3-2);   // a is the image of x in Q[x]/(x^3-2)
> a;
a
> a^3;
2
> S<y> := PolynomialRing(K);
> L<b> := NumberField(y^2-a);
> L;
Number Field with defining polynomial y^2 - a over K
> b^2;
a
> b^6;
2
> AbsoluteField(L);
Number Field with defining polynomial x^6 - 2 over the Rational
Field
```

7.2.3 Rings of integers

MAGMA computes rings of integers of number fields.

```
> RingOfIntegers(K);
Maximal Equation Order with defining polynomial x^3 - 2 over ZZ
> RingOfIntegers(L);
```

```
Maximal Equation Order with defining polynomial x^2 + [0, -1, 0]
over its ground order
```

Sometimes the ring of integers of $\mathbf{Q}(a)$ isn't just $\mathbf{Z}[a]$. First a simple example, then a more complicated one:

```
> K<a> := NumberField(2*x^2-3);   // doesn't have to be monic
> 2*a^2 - 3;
0
> K;
Number Field with defining polynomial x^2 - 3/2 over the Rational
Field
> O := RingOfIntegers(K);
> O;
Maximal Order of Equation Order with defining polynomial 2*x^2 -
    3 over ZZ
> Basis(O);
[
    O.1,
    O.2
]
> [K!x : x in Basis(O)];
[
    1,
    2*a       // this is Sqrt(3)
]
```

Here's are some more examples:

```
> procedure ints(f)   // (procedures don't return anything; functions do)
      K<a> := NumberField(f);
      O := MaximalOrder(K);
      print [K!z : z in Basis(O)];
  end procedure;
> ints(x^2-5);
[
    1,
    1/2*(a + 1)
]
> ints(x^2+5);
[
    1,
    a
]
> ints(x^3-17);
```

```
[
    1,
    a,
    1/3*(a^2 + 2*a + 1)
]
> ints(CyclotomicPolynomial(7));
[
    1,
    a,
    a^2,
    a^3,
    a^4,
    a^5
]
> ints(x^5+&+[Random(10)*x^i : i in [0..4]]);  // RANDOM
[
    1,
    a,
    a^2,
    a^3,
    a^4
]
> ints(x^5+&+[Random(10)*x^i : i in [0..4]]);  // RANDOM
[
    1,
    a,
    a^2,
    1/2*(a^3 + a),
    1/16*(a^4 + 7*a^3 + 11*a^2 + 7*a + 14)
]
```

Lets find out how high of a degree MAGMA can easily deal with.

```
> d := 10; time ints(x^10+&+[Random(10)*x^i : i in [0..d-1]]);
[
    1, a, a^2, a^3, a^4, a^5, a^6, a^7, a^8, a^9
]
Time: 0.030
> d := 15; time ints(x^10+&+[Random(10)*x^i : i in [0..d-1]]);
[
    1,
    7*a,
    7*a^2 + 4*a,
    7*a^3 + 4*a^2 + 4*a,
    7*a^4 + 4*a^3 + 4*a^2 + a,
```

```
    7*a^5 + 4*a^4 + 4*a^3 + a^2 + a,
    7*a^6 + 4*a^5 + 4*a^4 + a^3 + a^2 + 4*a,
    7*a^7 + 4*a^6 + 4*a^5 + a^4 + a^3 + 4*a^2,
    7*a^8 + 4*a^7 + 4*a^6 + a^5 + a^4 + 4*a^3 + 4*a,
    7*a^9 + 4*a^8 + 4*a^7 + a^6 + a^5 + 4*a^4 + 4*a^2 + 5*a,
    7*a^10 + 4*a^9 + 4*a^8 + a^7 + a^6 + 4*a^5 + 4*a^3 + 5*a^2 +  4*a,
  ...
]
Time: 0.480
> d := 20; time ints(x^10+&+[Random(10)*x^i : i in [0..d-1]]);
[
    1,
    2*a,
    4*a^2,
    8*a^3,
    8*a^4 + 2*a^2 + a,
    8*a^5 + 2*a^3 + 3*a^2,
 ...]
Time: 3.940
> d := 25; time ints(x^10+&+[Random(10)*x^i : i in [0..d-1]]);
... I stopped it after a few minutes...
```

We can also define orders in rings of integers.

```
> R<x> := PolynomialRing(RationalField());
> K<a> := NumberField(x^3-2);
> O := Order([2*a]);
> O;
Transformation of Order over
Equation Order with defining polynomial x^3 - 2 over ZZ
Transformation Matrix:
[1 0 0]
[0 2 0]
[0 0 4]
> OK := MaximalOrder(K);
> Index(OK,O);
8
> Discriminant(O);
-6912
> Discriminant(OK);
-108
> 6912/108;
64    // perfect square...
```

7.2.4 Ideals

```
> R<x> := PolynomialRing(RationalField());
> K<a> := NumberField(x^3-2);
> O := Order([2*a]);
> O;
Transformation of Order over
Equation Order with defining polynomial x^3 - 2 over ZZ
Transformation Matrix:
[1 0 0]
[0 2 0]
[0 0 4]
> OK := MaximalOrder(K);
> Index(OK,O);
8
> Discriminant(O);
-6912
> Discriminant(OK);
-108
> 6912/108;
64    // perfect square...
> R<x> := PolynomialRing(RationalField());
> K<a> := NumberField(x^2-7);
> K<a> := NumberField(x^2-5);
> Discriminant(K);
20   // ????????? Yuck!
> OK := MaximalOrder(K);
> Discriminant(OK);
5    // better
> Discriminant(NumberField(x^2-20));
80
> I := 7*OK;
> I;
Principal Ideal of OK
Generator:
    [7, 0]
> J := (OK!a)*OK;    // the ! computes the natural image of a in OK
> J;
Principal Ideal of OK
Generator:
    [-1, 2]
> I*J;
Principal Ideal of OK
Generator:
```

```
    [-7, 14]
> J*I;
Principal Ideal of OK
Generator:
    [-7, 14]
> I+J;
Principal Ideal of OK
Generator:
    [1, 0]
>
> Factorization(I);
[
    <Principal Prime Ideal of OK
    Generator:
        [7, 0], 1>
]
> Factorization(3*OK);
[
    <Principal Prime Ideal of OK
    Generator:
        [3, 0], 1>
]
> Factorization(5*OK);
[
    <Prime Ideal of OK
    Two element generators:
        [5, 0]
        [4, 2], 2>
]
> Factorization(11*OK);
[
    <Prime Ideal of OK
    Two element generators:
        [11, 0]
        [14, 2], 1>,
    <Prime Ideal of OK
    Two element generators:
        [11, 0]
        [17, 2], 1>
]
```

We can even work with fractional ideals in Magma.

```
> K<a> := NumberField(x^2-5);
```

```
> OK := MaximalOrder(K);
> I := 7*OK;
> J := (OK!a)*OK;
> M := I/J;
> M;
Fractional Principal Ideal of OK
Generator:
    -7/5*OK.1 + 14/5*OK.2
> Factorization(M);
[
    <Prime Ideal of OK
    Two element generators:
        [5, 0]
        [4, 2], -1>,
    <Principal Prime Ideal of OK
    Generator:
        [7, 0], 1>
]
```

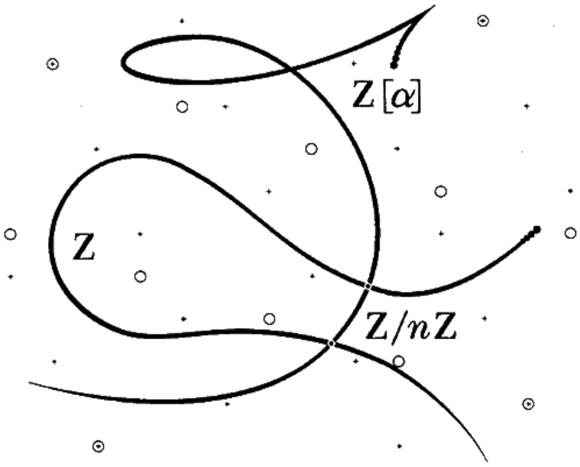
In the next chapter, we will learn about discriminants and an algorithm for "factoring primes", that is writing an ideal $p\mathcal{O}_K$ as a product of prime ideals of $\mathcal{O}_K$.

Chapter 8

Factoring Primes

First we will learn how, if $p \in \mathbf{Z}$ is a prime and $\mathcal{O}_K$ is the ring of integers of a number field, to write $p\mathcal{O}_K$ as a product of primes of $\mathcal{O}_K$. Then I will sketch the main results and definitions that we will study in detail during the next few chapters. We will cover discriminants and norms of ideals, define the class group of $\mathcal{O}_K$ and prove that it is finite and computable, and define the group of units of $\mathcal{O}_K$, determine its structure, and prove that it is also computable.

8.1 Factoring Primes



A diagram from [LL93].

"The obvious mathematical breakthrough would be development of an easy way to factor large prime numbers." –Bill Gates, *The Road Ahead*, pg. 265

Let $K = \mathbf{Q}(\alpha)$ be a number field, and let $\mathcal{O}_K$ be the ring of integers of K. To employ our geometric intuition, as the Lenstras did on the cover of [LL93], it is helpful to view $\mathcal{O}_K$ as a one-dimensional scheme

$$X = \mathrm{Spec}(\mathcal{O}_K) = \{ \text{ all prime ideals of } \mathcal{O}_K \ \}$$

over

$$Y = \mathrm{Spec}(\mathbf{Z}) = \{(0)\} \cup \{p\mathbf{Z} : p \in \mathbf{Z} \text{ is prime } \}.$$

There is a natural map $\pi : X \to Y$ that sends a prime ideal $\mathfrak{p} \in X$ to $\mathfrak{p} \cap \mathbf{Z} \in Y$. For much more on this point of view, see [EH00, Ch. 2].

Ideals were originally introduced by Kummer because, as we proved last Tuesday, in rings of integers of number fields ideals factor uniquely as products of primes ideals, which is something that is not true for general algebraic integers. (The failure of unique factorization for algebraic integers was used by Liouville to destroy Lamé's purported 1847 "proof" of Fermat's Last Theorem.)

If $p \in \mathbf{Z}$ is a prime number, then the ideal $p\mathcal{O}_K$ of $\mathcal{O}_K$ factors uniquely as a product $\prod \mathfrak{p}_i^{e_i}$, where the $\mathfrak{p}_i$ are maximal ideals of $\mathcal{O}_K$. We may imagine the decomposition of $p\mathcal{O}_K$ into prime ideals geometrically as the fiber $\pi^{-1}(p\mathbf{Z})$ (with multiplicities).

How can we compute $\pi^{-1}(p\mathbf{Z})$ in practice?

Example 8.1.1. The following MAGMA session shows the commands needed to compute the factorization of $p\mathcal{O}_K$ in MAGMA for K the number field defined by a root of $x^5 + 7x^4 + 3x^2 - x + 1$.

```
> R<x> := PolynomialRing(RationalField());
> K<a> := NumberField(x^5 + 7*x^4 + 3*x^2 - x + 1);
> OK := MaximalOrder(K);
> I := 2*OK;
> Factorization(I);
[
<Principal Prime Ideal of OK
Generator:
[2, 0, 0, 0, 0], 1>
]
> J := 5*OK;
> Factorization(J);
[
<Prime Ideal of OK
Two element generators:
[5, 0, 0, 0, 0]
[2, 1, 0, 0, 0], 1>,
<Prime Ideal of OK
Two element generators:
[5, 0, 0, 0, 0]
```

```
[3, 1, 0, 0, 0], 2>,
<Prime Ideal of OK
Two element generators:
[5, 0, 0, 0, 0]
[2, 4, 1, 0, 0], 1>
]
> [K!OK.i : i in [1..5]];
[ 1, a, a^2, a^3, a^4 ]
```

Thus $2\mathcal{O}_K$ is already a prime ideal, and

$$5\mathcal{O}_K = (5, 2+a) \cdot (5, 3+a)^2 \cdot (5, 2+4a+a^2).$$

Notice that in this example $\mathcal{O}_K = \mathbf{Z}[a]$. (Warning: There are examples of $\mathcal{O}_K$ such that $\mathcal{O}_K \neq \mathbf{Z}[a]$ for any $a \in \mathcal{O}_K$, as Example 8.1.6 below illustrates.) When $\mathcal{O}_K = \mathbf{Z}[a]$ it is very easy to factor $p\mathcal{O}_K$, as we will see below. The following factorization gives a hint as to why:

$$x^5 + 7x^4 + 3x^2 - x + 1 \equiv (x+2) \cdot (x+3)^2 \cdot (x^2+4x+2) \pmod 5.$$

The exponent 2 of $(5, 3+a)^2$ in the factorization of $5\mathcal{O}_K$ above suggests "ramification", in the sense that the cover $X \to Y$ has less points (counting their "size", i.e., their residue class degree) in its fiber over 5 than it has generically. Here's a suggestive picture:

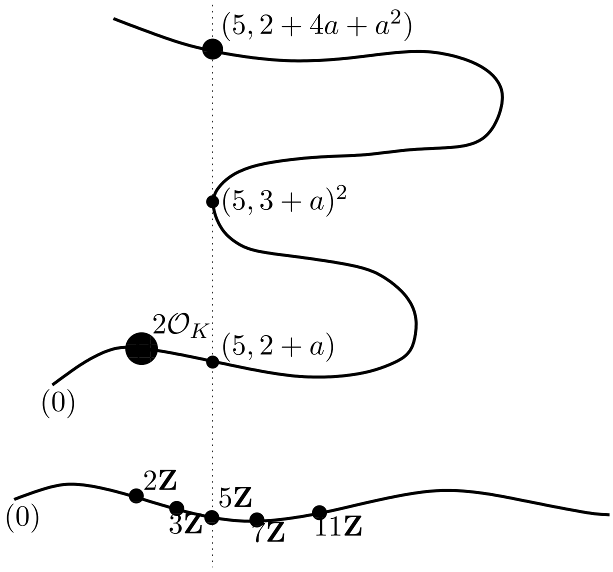


Diagram of $\mathrm{Spec}(\mathcal{O}_K) \to \mathrm{Spec}(\mathbf{Z})$

8.1.1 A Method for Factoring that Often Works

Suppose $a \in \mathcal{O}_K$ is such that $K = \mathbf{Q}(a)$, and let $g(x)$ be the minimal polynomial of a. Then $\mathbf{Z}[a] \subset \mathcal{O}_K$, and we have a diagram of schemes

$$\begin{tikzcd}
(??) \arrow[r, hook] \arrow[d] & \mathrm{Spec}(\mathcal{O}_K) \arrow[d] \\
\bigcup \mathrm{Spec}(\mathbf{F}_p[x]/(\overline{g}_i^{e_i})) \arrow[r, hook] \arrow[d] & \mathrm{Spec}(\mathbf{Z}[a]) \arrow[d] \\
\mathrm{Spec}(\mathbf{F}_p) \arrow[r, hook] & \mathrm{Spec}(\mathbf{Z})
\end{tikzcd}$$

where $\overline{g} = \prod_i \overline{g}_i^{e_i}$ is the factorization of the image of g in $\mathbf{F}_p[x]$.

The cover $\pi : \mathrm{Spec}(\mathbf{Z}[a]) \to \mathrm{Spec}(\mathbf{Z})$ is easy to understand because it is defined by the single equation $g(x)$. To give a maximal ideal $\mathfrak{p}$ of $\mathbf{Z}[a]$ such that $\pi(\mathfrak{p}) = p\mathbf{Z}$ is the same as giving a homomorphism $\varphi : \mathbf{Z}[x]/(g) \to \overline{\mathbf{F}}_p$ (up to automorphisms of the image), which is in turn the same as giving a root of g in $\overline{\mathbf{F}}_p$ (up to automorphism), which is the same as giving an irreducible factor of the reduction of g modulo p.

Lemma 8.1.2. *Suppose the index of $\mathbf{Z}[a]$ in $\mathcal{O}_K$ is coprime to p. Then the primes $\mathfrak{p}_i$ in the factorization of $p\mathbf{Z}[a]$ do not decompose further going from $\mathbf{Z}[a]$ to $\mathcal{O}_K$, so finding the prime ideals of $\mathbf{Z}[a]$ that contain p yields the factorization of $p\mathcal{O}_K$.*

Proof. Hi-brow argument: By hypothesis we have an exact sequence of abelian groups

$$0 \to \mathbf{Z}[a] \to \mathcal{O}_K \to H \to 0,$$

where H is a finite abelian group of order coprime to p. Tensor product is right exact, and there is an exact sequence

$$\mathrm{Tor}_1(H, \mathbf{F}_p) \to \mathbf{Z}[a] \otimes \mathbf{F}_p \to \mathcal{O}_K \otimes \mathbf{F}_p \to H \otimes \mathbf{F}_p \to 0,$$

and $\mathrm{Tor}_1(H, \mathbf{F}_p) = H \otimes \mathbf{F}_p = 0$, so $\mathbf{Z}[a] \otimes \mathbf{F}_p \cong \mathcal{O}_K \otimes \mathbf{F}_p$.
Low-brow argument: The inclusion map $\mathbf{Z}[a] \hookrightarrow \mathcal{O}_K$ is defined by a matrix over $\mathbf{Z}$ that has determinant $\pm[\mathcal{O}_K : \mathbf{Z}[a]]$, which is coprime to p. The reduction of this matrix modulo p is invertible, so it defines an isomorphism $\mathbf{Z}[a] \otimes \mathbf{F}_p \to \mathcal{O}_K \otimes \mathbf{F}_p$. Any homomorphism $\mathcal{O}_K \to \overline{\mathbf{F}}_p$ is the composition of a homomorphism $\mathcal{O}_K \to \mathcal{O}_K \otimes \mathbf{F}_p$ with a homomorphism $\mathcal{O}_K \otimes \mathbf{F}_p \to \overline{\mathbf{F}}_p$. Since $\mathcal{O}_K \otimes \mathbf{F}_p \cong \mathbf{Z}[a] \otimes \mathbf{F}_p$, the homomorphisms $\mathcal{O}_K \to \overline{\mathbf{F}}_p$ are in bijection with the homomorphisms $\mathbf{Z}[a] \to \overline{\mathbf{F}}_p$, which proves the lemma. □

As suggested in the proof of the lemma, we find all homomorphisms $\mathcal{O}_K \to \overline{\mathbf{F}}_p$ by finding all homomorphism $\mathbf{Z}[a] \to \overline{\mathbf{F}}_p$. In terms of ideals, if $\mathfrak{p} = (g(a), p)\mathbf{Z}[a]$ is a maximal ideal of $\mathbf{Z}[a]$, then the ideal $\mathfrak{p}' = (g(a), p)\mathcal{O}_K$ of $\mathcal{O}_K$ is also maximal, since

$$\mathcal{O}_K/\mathfrak{p}' \cong (\mathcal{O}_K \otimes \mathbf{F}_p)/(g(\tilde{a})) \cong (\mathbf{Z}[a] \otimes \mathbf{F}_p)/(g(\tilde{a})) \subset \overline{\mathbf{F}}_p.$$

We formalize the above discussion in the following theorem:

Theorem 8.1.3. *Let $f(x)$ denote the minimal polynomial of a over $\mathbf{Q}$. Suppose that $p \nmid [\mathcal{O}_K : \mathbf{Z}[a]]$ is a prime. Let*

$$\overline{f} = \prod_{i=1}^{t} \overline{f}_i^{e_i} \in \mathbf{F}_p[x]$$

where the $\overline{f}_i$ are distinct monic irreducible polynomials. Let $\mathfrak{p}_i = (p, f_i(a))$ where $f_i \in \mathbf{Z}[x]$ is a lift of $\overline{f}_i$ in $\mathbf{F}_p[X]$. Then

$$p\mathcal{O}_K = \prod_{i=1}^{t} \mathfrak{p}_i^{e_i}.$$

We return to the example from above, in which $K = \mathbf{Q}(a)$, where a is a root of $x^5+7x^4+3x^2-x+1$. According to MAGMA, the maximal order $\mathcal{O}_K$ has discriminant 2945785:

```
> Discriminant(MaximalOrder(K));
2945785
```

The order $\mathbf{Z}[a]$ has the same discriminant as $\mathcal{O}_K$, so $\mathbf{Z}[a] = \mathcal{O}_K$ and we can apply the above theorem.

```
> Discriminant(x^5 + 7*x^4 + 3*x^2 - x + 1);
2945785
```

We have

$$x^5 + 7x^4 + 3x^2 - x + 1 \equiv (x+2) \cdot (x+3)^2 \cdot (x^2 + 4x + 2) \pmod{5},$$

which yields the factorization of $5\mathcal{O}_K$ given before the theorem.

If we replace a by $b = 7a$, then the index of $\mathbf{Z}[b]$ in $\mathcal{O}_K$ will be a power of 7, which is coprime to 5, so the above method will still work.

```
> f:=MinimalPolynomial(7*a);
> f;
x^5 + 49*x^4 + 1029*x^2 - 2401*x + 16807
> Discriminant(f);
235050861175510968365785
> Discriminant(f)/Discriminant(MaximalOrder(K));
79792266297612001    // coprime to 5
> S<t> := PolynomialRing(GF(5));
> Factorization(S!f);
[
    <t + 1, 2>,
    <t + 4, 1>,
    <t^2 + 3*t + 3, 1>
]
```

Thus 5 factors in $\mathcal{O}_K$ as

$$5\mathcal{O}_K = (5, 7a+1)^2 \cdot (5, 7a+4) \cdot (5, (7a)^2 + 3(7a) + 3).$$

If we replace a by $b = 5a$ and try the above algorithm with $\mathbf{Z}[b]$, then the method fails because the index of $\mathbf{Z}[b]$ in $\mathcal{O}_K$ is divisible by 5.

```
> f:=MinimalPolynomial(5*a);
> f;
x^5 + 35*x^4 + 375*x^2 - 625*x + 3125
> Discriminant(f) / Discriminant(MaximalOrder(K));
95367431640625    // divisible by 5
> Factorization(S!f);
[
    <t, 5>
]
```

8.1.2 A Method for Factoring that Always Works

There are numbers fields K such that $\mathcal{O}_K$ is not of the form $\mathbf{Z}[a]$ for any $a \in K$. Even worse, Dedekind found a field K such that $2 \mid [\mathcal{O}_K : \mathbf{Z}[a]]$ for *all* $a \in \mathcal{O}_K$, so there is no choice of a such that Theorem 8.1.3 can be used to factor 2 for K (see Example 8.1.6 below).

Most algebraic number theory books do not describe an algorithm for decomposing primes in the general case. Fortunately, Cohen's book [Coh93, §6.2]) describes how to solve the general problem. The solutions are somewhat surprising, since the algorithms are much more sophisticated than the one suggested by Theorem 8.1.3. However, these complicated algorithms all run very quickly in practice, even without assuming the maximal order is already known.

For simplicity we consider the following slightly easier problem whose solution contains the key ideas: *Let $\mathcal{O}$ be any order in $\mathcal{O}_K$ and let p be a prime of $\mathbf{Z}$. Find the prime ideals of $\mathcal{O}$ that contain p.*

To go from this special case to the general case, given a prime p that we wish to factor in $\mathcal{O}_K$, we find a p-maximal order $\mathcal{O}$, i.e., an order $\mathcal{O}$ such that $[\mathcal{O}_K : \mathcal{O}]$ is coprime to p. A p-maximal order can be found very quickly in practice using the "round 2" or "round 4" algorithms. (Remark: Later we will see that to compute $\mathcal{O}_K$, we take the sum of p-maximal orders, one for every p such that p^2 divides $\mathrm{Disc}(\mathcal{O}_K)$. The time-consuming part of this computation of $\mathcal{O}_K$ is finding the primes p such that $p^2 \mid \mathrm{Disc}(\mathcal{O}_K)$, not finding the p-maximal orders. Thus a fast algorithm for factoring integers would not only break many cryptosystems, but would massively speed up computation of the ring of integers of a number field.)

Algorithm 8.1.4. Suppose $\mathcal{O}$ is an order in the ring $\mathcal{O}_K$ of integers of a number field K. For any prime $p \in \mathbf{Z}$, the following (sketch of an) algorithm computes the set of maximal ideals of $\mathcal{O}$ that contain p.

Sketch of algorithm. Let $K = \mathbf{Q}(a)$ be a number field given by an algebraic integer a as a root of its minimal monic polynomial f of degree n. We assume that an order $\mathcal{O}$ has been given by a basis $w_1, \ldots, w_n$ and that $\mathcal{O}$ that contains $\mathbf{Z}[a]$. Each of the following steps can be carried out efficiently using little more than linear algebra over $\mathbf{F}_p$. The details are in [Coh93, §6.2.5].

1. [Check if easy] If $p \nmid \mathrm{disc}(\mathbf{Z}[a])/\mathrm{disc}(\mathcal{O})$ (so $p \nmid [\mathcal{O} : \mathbf{Z}[a]]$), then by a slight modification of Theorem 8.1.3, we easily factor $p\mathcal{O}$.

2. [Compute radical] Let I be the *radical* of $p\mathcal{O}$, which is the ideal of elements $x \in \mathcal{O}$ such that $x^m \in p\mathcal{O}$ for some positive integer m. Using linear algebra over the finite field $\mathbf{F}_p$, we can quickly compute a basis for $I/p\mathcal{O}$. (We never compute $I \subset \mathcal{O}$.)

3. [Compute quotient by radical] Compute an $\mathbf{F}_p$ basis for
$$A = \mathcal{O}/I = (\mathcal{O}/p\mathcal{O})/(I/p\mathcal{O}).$$
The second equality comes from the fact that $p\mathcal{O} \subset I$, which is clear by definition. Note that $\mathcal{O}/p\mathcal{O} \cong \mathcal{O} \otimes \mathbf{F}_p$ is obtained by simply reducing the basis $w_1, \ldots, w_n$ modulo p.

4. [Decompose quotient] The ring A is a finite Artin ring with no nilpotents, so it decomposes as a product $A \cong \prod \mathbf{F}_p[x]/g_i(x)$ of fields. We can quickly find such a decomposition explicitly, as described in [Coh93, §6.2.5].

5. [Compute the maximal ideals over p] Each maximal ideal $\mathfrak{p}_i$ lying over p is the kernel of $\mathcal{O} \to A \to \mathbf{F}_p[x]/g_i(x)$.

The algorithm finds all primes of $\mathcal{O}$ that contain the radical I of $p\mathcal{O}$. Every such prime clearly contains p, so to see that the algorithm is correct, we must prove that the primes $\mathfrak{p}$ of $\mathcal{O}$ that contain p also contain I. If $\mathfrak{p}$ is a prime of $\mathcal{O}$ that contains p, then $p\mathcal{O} \subset \mathfrak{p}$. If $x \in I$ then $x^m \in p\mathcal{O}$ for some m, so $x^m \in \mathfrak{p}$ which implies that $x \in \mathfrak{p}$ by primality of $\mathfrak{p}$. Thus $\mathfrak{p}$ contains I, as required.

8.1.3 Essential Discriminant Divisors

Definition 8.1.5. A prime p is an *essential discriminant divisor* if $p \mid [\mathcal{O}_K : \mathbf{Z}[a]]$ for *every* $a \in \mathcal{O}_K$.

Since $[\mathcal{O}_K : \mathbf{Z}[a]]$ is the absolute value of $\mathrm{Disc}(f(x))/\mathrm{Disc}(\mathcal{O}_K)$, where $f(x)$ is the characteristic polynomial of $f(x)$, an essential discriminant divisor divides the discriminant of the characteristic polynomial of any element of $\mathcal{O}_K$.

Example 8.1.6 *(Dedekind).* Let $K = \mathbf{Q}(a)$ be the cubic field defined by a root a of the polynomial $f = x^3 + x^2 - 2x + 8$. We will use MAGMA, which implements the algorithm described in the previous section, to show that 2 is an essential discriminant divisor for K.

```
> K<a> := NumberField(x^3 + x^2 - 2*x + 8);
> OK := MaximalOrder(K);
> Factorization(2*OK);
[
<Prime Ideal of OK
Basis:
[2 0 0]
[0 1 0]
[0 0 1], 1>,
<Prime Ideal of OK
Basis:
[1 0 1]
[0 1 0]
[0 0 2], 1>,
<Prime Ideal of OK
Basis:
[1 0 1]
[0 1 1]
[0 0 2], 1>
]
```

Thus $2\mathcal{O}_K = \mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3$, with the $\mathfrak{p}_i$ distinct. Moreover, one can check that $\mathcal{O}_K/\mathfrak{p}_i \cong \mathbf{F}_2$. If $\mathcal{O}_K = \mathbf{Z}[a]$ for some $a \in \mathcal{O}_K$ with minimal polynomial g, then $\overline{g}(x) \in \mathbf{F}_2[x]$ must be a product of three *distinct* linear factors, which is impossible.

Chapter 9

Chinese Remainder Theorem

In this section we will prove the Chinese Remainder Theorem for rings of integers, deduce several surprising and useful consequences, then learn about discriminants, and finally norms of ideals. We will also define the class group of $\mathcal{O}_K$ and state the main theorem about it. The tools we develop here illustrate the power of what we have already proved about rings of integers, and will be used over and over again to prove other deeper results in algebraic number theory. It is essentially to understand everything we discuss in this chapter very well.

9.1 The Chinese Remainder Theorem

Recall that the Chinese Remainder Theorem from elementary number theory asserts that if $n_1, \ldots, n_r$ are integers that are coprime in pairs, and $a_1, \ldots, a_r$ are integers, then there exists an integer a such that $a \equiv a_i \pmod{n_i}$ for each $i = 1, \ldots, r$. In terms of rings, the Chinese Remainder Theorem asserts that the natural map

$$\mathbf{Z}/(n_1 \cdots n_r)\mathbf{Z} \to (\mathbf{Z}/n_1\mathbf{Z}) \oplus \cdots \oplus (\mathbf{Z}/n_r\mathbf{Z})$$

is an isomorphism. This result generalizes to rings of integers of number fields.

Lemma 9.1.1. *If I and J are coprime ideals in $\mathcal{O}_K$, then $I \cap J = IJ$.*

Proof. The ideal $I \cap J$ is the largest ideal of $\mathcal{O}_K$ that is divisible by (contained in) both I and J. Since I and J are coprime, $I \cap J$ is divisible by IJ, i.e., $I \cap J \subset IJ$. By definition of ideal $IJ \subset I \cap J$, which completes the proof. □

Remark 9.1.2. This lemma is true for any ring R and ideals $I, J \subset R$ such that $I + J = R$. For the general proof, choose $x \in I$ and $y \in J$ such that $x + y = 1$. If $c \in I \cap J$ then

$$c = c \cdot 1 = c \cdot (x + y) = cx + cy \in IJ + IJ = IJ,$$

so $I \cap J \subset IJ$, and the other inclusion is obvious by definition.

Theorem 9.1.3 (Chinese Remainder Theorem). *Suppose $I_1, \ldots, I_r$ are ideals of $\mathcal{O}_K$ such that $I_m + I_n = \mathcal{O}_K$ for any $m \neq n$. Then the natural homomorphism $\mathcal{O}_K \to \bigoplus_{n=1}^r (\mathcal{O}_K/I_n)$ induces an isomorphism*

$$\mathcal{O}_K/\left(\prod_{n=1}^r I_n\right) \to \bigoplus_{n=1}^r (\mathcal{O}_K/I_n).$$

Thus given any $a_n \in I_n$ then there exists $a \in \mathcal{O}_K$ such that $a \equiv a_n \pmod{I_n}$ for $n = 1, \ldots, r$.

Proof. First assume that we know the theorem in the case when the I_n are powers of prime ideals. Then we can deduce the general case by noting that each $\mathcal{O}_K/I_n$ is isomorphic to a product $\prod \mathcal{O}_K/\mathfrak{p}_m^{e_m}$, where $I_n = \prod \mathfrak{p}_m^{e_m}$, and $\mathcal{O}_K/(\prod_n I_n)$ is isomorphic to the product of the $\mathcal{O}_K/\mathfrak{p}^e$, where the $\mathfrak{p}$ and e run through the same prime powers as appear on the right hand side.

It thus suffices to prove that if $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ are distinct prime ideals of $\mathcal{O}_K$ and $e_1, \ldots, e_r$ are positive integers, then

$$\psi : \mathcal{O}_K/\left(\prod_{n=1}^r \mathfrak{p}_n^{e_n}\right) \to \bigoplus_{n=1}^r (\mathcal{O}_K/\mathfrak{p}_n^{e_n})$$

is an isomorphism. Let $\varphi : \mathcal{O}_K \to \oplus_{n=1}^r (\mathcal{O}_K/\mathfrak{p}_n^{e_n})$ be the natural map induced by reduction mod $\mathfrak{p}_n^{e_n}$. Then kernel of φ is $\cap_{n=1}^r \mathfrak{p}_n^{e_n}$, which by Lemma 9.1.1 is equal to $\prod_{n=1}^r \mathfrak{p}_n^{e_n}$, so ψ is injective. Note that the projection $\mathcal{O}_K \to \mathcal{O}_K/\mathfrak{p}_n^{e_n}$ of φ onto each factor is obviously surjective, so it suffices to show that the element $(1, 0, \ldots, 0)$ is in the image of φ (and the similar elements for the other factors). Since $J = \prod_{n=2}^r \mathfrak{p}_n^{e_n}$ is not divisible by $\mathfrak{p}_1$, hence not contained in $\mathfrak{p}_1$, there is an element $a \in J$ with $a \notin \mathfrak{p}_1$. Since $\mathfrak{p}_1$ is maximal, $\mathcal{O}_K/\mathfrak{p}_1$ is a field, so there exists $b \in \mathcal{O}_K$ such that $ab = 1 - c$, for some $c \in \mathfrak{p}_1$. Then

$$1 - c^{n_1} = (1 - c)(1 + c + c^2 + \cdots + c^{n_1 - 1}) = ab(1 + c + c^2 + \cdots + c^{n_1 - 1})$$

is congruent to 0 mod $\mathfrak{p}_n^{e_n}$ for each $n \geq 2$ since it is in $\prod_{n=2}^r \mathfrak{p}_n^{e_n}$, and it is congruent to 1 modulo $\mathfrak{p}_1^{n_1}$. ∎

Remark 9.1.4. In fact, the surjectivity part of the above proof is easy to prove for any commutative ring; indeed, the above proof illustrates how trying to prove something in a special case can result in a more complicated proof!! Suppose R is a ring and I, J are ideals in R such that $I + J = R$. Choose $x \in I$ and $y \in J$ such that $x + y = 1$. Then $x = 1 - y$ maps to $(0, 1)$ in $R/I \oplus R/J$ and $y = 1 - x$ maps to $(1, 0)$ in $R/I \oplus R/J$. Thus the map $R/(I \cap J) \to R/I \oplus R/J$ is surjective. Also, as mentioned above, $R/(I \cap J) = R/(IJ)$.

Example 9.1.5. The MAGMA command `ChineseRemainderTheorem` implements the algorithm suggested by the above theorem. In the following example, we compute a prime over (3) and a prime over (5) of the ring of integers of $\mathbf{Q}(\sqrt[3]{2})$, and find an element of $\mathcal{O}_K$ that is congruent to $\sqrt[3]{2}$ modulo one prime and 1 modulo the other.

```
> R<x> := PolynomialRing(RationalField());
> K<a> := NumberField(x^3-2);
> OK := MaximalOrder(K);
> I := Factorization(3*OK)[1][1];
> J := Factorization(5*OK)[1][1];
> I;
Prime Ideal of OK
Two element generators:
    [3, 0, 0]
    [4, 1, 0]
> J;
Prime Ideal of OK
Two element generators:
    [5, 0, 0]
    [7, 1, 0]
> b := ChineseRemainderTheorem(I, J, OK!a, OK!1);
> b - a in I;
true
> b - 1 in J;
true
> K!b;
-4
```

The element found by the Chinese Remainder Theorem algorithm in this case is -4.

The following lemma is a nice application of the Chinese Remainder Theorem. We will use it to prove that every ideal of $\mathcal{O}_K$ can be generated by two elements. Suppose I is a nonzero integral ideals of $\mathcal{O}_K$. If $a \in I$, then $(a) \subset I$, so I divides (a) and the quotient $(a)/I$ is an integral ideal. The following lemma asserts that (a) can be chosen so the quotient $(a)/I$ is coprime to any given ideal.

Lemma 9.1.6. *If I, J are nonzero integral ideals in $\mathcal{O}_K$, then there exists an $a \in I$ such that $(a)/I$ is coprime to J.*

Proof. Let $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ be the prime divisors of J. For each n, let v_n be the largest power of $\mathfrak{p}_n$ that divides I. Choose an element $a_n \in \mathfrak{p}_n^{v_n}$ that is not in $\mathfrak{p}_n^{v_n+1}$ (there is such an element since $\mathfrak{p}_n^{v_n} \neq \mathfrak{p}_n^{v_n+1}$, by unique factorization). By Theorem 9.1.3, there exists $a \in \mathcal{O}_K$ such that

$$a \equiv a_n \pmod{\mathfrak{p}_n^{v_n+1}}$$

for all $n = 1, \ldots, r$ and also

$$a \equiv 0 \pmod{I/\prod \mathfrak{p}_n^{v_n}}.$$

(We are applying the theorem with the coprime integral ideals $\mathfrak{p}_n^{v_n+1}$, for $n = 1, \ldots, r$ and the integral ideal $I/\prod \mathfrak{p}_n^{v_n}$.)

To complete the proof we must show that $(a)/I$ is not divisible by any $\mathfrak{p}_n$, or equivalently, that the $\mathfrak{p}_n^{v_n}$ exactly divides (a). Because $a \equiv a_n \pmod{\mathfrak{p}_n^{v_n+1}}$, there is $b \in \mathfrak{p}_n^{v_n+1}$ such that $a = a_n + b$. Since $a_n \in \mathfrak{p}_n^{v_n}$, it follows that $a \in \mathfrak{p}_n^{v_n}$, so $\mathfrak{p}_n^{v_n}$ divides (a). If $a \in \mathfrak{p}_n^{v_n+1}$, then $a_n = a - b \in \mathfrak{p}_n^{v_n+1}$, a contradiction, so $\mathfrak{p}_n^{v_n+1}$ does not divide (a), which completes the proof. $\square$

Suppose I is a nonzero ideal of $\mathcal{O}_K$. As an abelian group $\mathcal{O}_K$ is free of rank equal to the degree $[K : \mathbf{Q}]$ of K, and I is of finite index in $\mathcal{O}_K$, so I can be generated as an abelian group, hence as an ideal, by $[K : \mathbf{Q}]$ generators. The following proposition asserts something much better, namely that I can be generated *as an ideal* in $\mathcal{O}_K$ by at most two elements.

Proposition 9.1.7. *Suppose I is a fractional ideal in the ring $\mathcal{O}_K$ of integers of a number field. Then there exist $a, b \in K$ such that $I = (a, b)$.*

Proof. If $I = (0)$, then I is generated by 1 element and we are done. If I is not an integral ideal, then there is $x \in K$ such that xI is an integral ideal, and the number of generators of xI is the same as the number of generators of I, so we may assume that I is an integral ideal.

Let a be any nonzero element of the integral ideal I. We will show that there is some $b \in I$ such that $I = (a, b)$. Let $J = (b)$. By Lemma 9.1.6, there exists $a \in I$ such that $(a)/I$ is coprime to (b). The ideal $(a, b) = (a)+(b)$ is the greatest common divisor of (a) and (b), so I divides (a, b), since I divides both (a) and (b). Suppose $\mathfrak{p}^n$ is a prime power that divides (a, b), so $\mathfrak{p}^n$ divides both (a) and (b). Because $(a)/I$ and (b) are coprime and $\mathfrak{p}^n$ divides (b), we see that $\mathfrak{p}^n$ does not divide $(a)/I$, so $\mathfrak{p}^n$ must divide I. Thus (a, b) divides I, so $(a, b) = I$ as claimed. $\square$

We can also use Theorem 9.1.3 to determine the $\mathcal{O}_K$-module structure of the successive quotients $\mathfrak{p}^n/\mathfrak{p}^{n+1}$.

Proposition 9.1.8. *Let $\mathfrak{p}$ be a nonzero prime ideal of $\mathcal{O}_K$, and let $n \geq 0$ be an integer. Then $\mathfrak{p}^n/\mathfrak{p}^{n+1} \cong \mathcal{O}_K/\mathfrak{p}$ as $\mathcal{O}_K$-modules.*

Proof. (Compare page 13 of Swinnerton-Dyer.) Since $\mathfrak{p}^n \neq \mathfrak{p}^{n+1}$ (by unique factorization), we can fix an element $b \in \mathfrak{p}^n$ such that $b \notin \mathfrak{p}^{n+1}$. Let $\varphi : \mathcal{O}_K \to \mathfrak{p}^n/\mathfrak{p}^{n+1}$ be the $\mathcal{O}_K$-module morphism defined by $\varphi(a) = ab$. The kernel of φ is $\mathfrak{p}$ since clearly $\varphi(\mathfrak{p}) = 0$ and if $\varphi(a) = 0$ then $ab \in \mathfrak{p}^{n+1}$, so $\mathfrak{p}^{n+1} \mid (a)(b)$, so $\mathfrak{p} \mid (a)$, since $\mathfrak{p}^{n+1}$ does not divide (b). Thus φ induces an injective $\mathcal{O}_K$-module homomorphism $\mathcal{O}_K/\mathfrak{p} \hookrightarrow \mathfrak{p}^n/\mathfrak{p}^{n+1}$.

It remains to show that φ is surjective, and this is where we will use Theorem 9.1.3. Suppose $c \in \mathfrak{p}^n$. By Theorem 9.1.3 there exists $d \in \mathcal{O}_K$ such that

$$d \equiv c \pmod{\mathfrak{p}^{n+1}} \qquad \text{and} \qquad d \equiv 0 \pmod{(b)/\mathfrak{p}^n}.$$

We have $\mathfrak{p}^n \mid (c)$ since $c \in \mathfrak{p}^n$ and $(b)/\mathfrak{p}^n \mid (d)$ by the second displayed condition, so $(b) = \mathfrak{p}^n \cdot (b)/\mathfrak{p}^n \mid (d)$, hence $d/b \in \mathcal{O}_K$. Finally

$$\varphi\left(\frac{d}{b}\right) = \frac{d}{b} \cdot b \pmod{\mathfrak{p}^{n+1}} = b \pmod{p^{n+1}} = c \pmod{p^{n+1}},$$

so φ is surjective. $\square$

Chapter 10

Discrimannts, Norms, and Finiteness of the Class Group

10.1 Preliminary Remarks

Let K be a number field of degree n. Then there are n embeddings

$$\sigma_1, \ldots, \sigma_n : K \hookrightarrow \mathbf{C}.$$

Let $\sigma : K \to \mathbf{C}^n$ be the product map $a \mapsto (\sigma_1(a), \ldots, \sigma_n(a))$. Let $V = \mathbf{R}\sigma(K)$ be the $\mathbf{R}$-span of $\sigma(K)$ inside $\mathbf{C}^n$.

Proposition 10.1.1. *The $\mathbf{R}$-vector space $V = \mathbf{R}\sigma(K)$ spanned by the image $\sigma(K)$ has dimension n.*

Proof. We prove this by showing that the image $\sigma(\mathcal{O}_K)$ is discrete. If $\sigma(\mathcal{O}_K)$ were not discrete it would contain elements all of whose coordinates are simultaneously arbitrarily small. The norm of an element $a \in \mathcal{O}_K$ is the product of the entries of $\sigma(a)$, so the norms of nonzero elements of $\mathcal{O}_K$ would go to 0. This is a contradiction, since the norms of elements of $\mathcal{O}_K$ are integers.

The fact that $\sigma(\mathcal{O}_K)$ is discrete in $\mathbf{C}^n$ implies that $\mathbf{R}\sigma(\mathcal{O}_K)$ has dimension equal to the rank n of $\sigma(\mathcal{O}_K)$, as claimed. This last assertion is not obvious, and requires observing that if L if a free abelian group that is discrete in a real vector space W and $\mathbf{R}L = W$, then the rank of L equals the dimension of W. Here's why this is true. If $x_1, \ldots, x_m \in L$ are a basis for $\mathbf{R}L$, then $\mathbf{Z}x_1 + \cdots + \mathbf{Z}x_m$ has finite index in L, since otherwise there would be infinitely many elements of L in a fundamental domain for $\mathbf{Z}x_1 + \cdots + \mathbf{Z}x_m$, which would contradict discreteness of L. Thus the rank of L is $m = \dim(\mathbf{R}L)$, as claimed. $\square$

Since $\sigma(\mathcal{O}_K)$ is a lattice in V, the volume of $V/\sigma(\mathcal{O}_K)$ is finite. Suppose $w_1, \ldots, w_n$ is a basis for $\mathcal{O}_K$. Then if A is the matrix whose ith row is $\sigma(w_i)$, then $|\operatorname{Det}(A)|$ is the volume of $V/\sigma(\mathcal{O}_K)$. (Take this determinant as the definition of the volume—we won't be using "volume" here except in a formal motivating way.)

Example 10.1.2. Let $\mathcal{O}_K = \mathbf{Z}[i]$ be the ring of integers of $K = \mathbf{Q}(i)$. Then $w_1 = 1$, $w_2 = i$ is a basis for $\mathcal{O}_K$. The map $\sigma : K \to \mathbf{C}^2$ is given by

$$\sigma(a + bi) = (a + bi, a - bi) \in \mathbf{C}^2.$$

The image $\sigma(\mathcal{O}_K)$ is spanned by $(1, 1)$ and $(i, -i)$. The volume determinant is

$$\left|\begin{pmatrix} 1 & 1 \\ i & -i \end{pmatrix}\right| = | - 2i| = 2.$$

Let $\mathcal{O}_K = \mathbf{Z}[\sqrt{2}]$ be the ring of integers of $K = \mathbf{Q}(\sqrt{2})$. The map σ is

$$\sigma(a + b\sqrt{2}) = (a + b\sqrt{2}, a - b\sqrt{2}) \in \mathbf{R}^2,$$

and

$$A = \begin{pmatrix} 1 & 1 \\ \sqrt{2} & -\sqrt{2} \end{pmatrix},$$

which has determinant $-2\sqrt{2}$, so the volume of the ring of integers is $2\sqrt{2}$.

As the above example illustrates, the volume of the ring of integers is not a great invariant of $\mathcal{O}_K$. For example, it need not be an integer. If we consider $\mathrm{Det}(A)^2$ instead, we obtain a number that is a well-defined integer which can be either positive or negative. In the next section we will do just this.

10.2 Discriminants

Suppose $w_1, \ldots, w_n$ are a basis for a number field K, which we view as a $\mathbf{Q}$-vector space. Let $\sigma : K \hookrightarrow \mathbf{C}^n$ be the embedding $\sigma(a) = (\sigma_1(a), \ldots, \sigma_n(a))$, where $\sigma_1, \ldots, \sigma_n$ are the distinct embeddings of K into $\mathbf{C}$. Let A be the matrix whose rows are $\sigma(w_1), \ldots, \sigma(w_n)$. The quantity $\mathrm{Det}(A)$ depends on the ordering of the w_i, and need not be an integer.

If we consider $\mathrm{Det}(A)^2$ instead, we obtain a number that is a well-defined integer which can be either positive or negative. Note that

$$\begin{aligned}
\mathrm{Det}(A)^2 &= \mathrm{Det}(AA) = \mathrm{Det}(AA^t) \\
&= \mathrm{Det}\left(\sum_{k=1,\ldots,n} \sigma_k(w_i)\sigma_k(w_j)\right) \\
&= \mathrm{Det}(\mathrm{Tr}(w_i w_j)_{1\leq i,j\leq n}),
\end{aligned}$$

so $\mathrm{Det}(A)^2$ can be defined purely in terms of the trace without mentioning the embeddings σ_i. Also, changing the basis for $\mathcal{O}_K$ is the same as left multiplying A by an integer matrix U of determinant ± 1, which does not change the squared determinant, since $\mathrm{Det}(UA)^2 = \mathrm{Det}(U)^2\,\mathrm{Det}(A)^2 = \mathrm{Det}(A)^2$. Thus $\mathrm{Det}(A)^2$ is well defined, and does not depend on the choice of basis.

If we view K as a $\mathbf{Q}$-vector space, then $(x, y) \mapsto \mathrm{Tr}(xy)$ defines a bilinear pairing $K \times K \to \mathbf{Q}$ on K, which we call the *trace pairing*. The following lemma asserts that this pairing is nondegenerate, so $\mathrm{Det}(\mathrm{Tr}(w_i w_j)) \neq 0$ hence $\mathrm{Det}(A) \neq 0$.

Lemma 10.2.1. *The trace pairing is nondegenerate.*

Proof. If the trace pairing is degenerate, then there exists $a \in K$ such that for every $b \in K$ we have $\mathrm{Tr}(ab) = 0$. In particularly, taking $b = a^{-1}$ we see that $0 = \mathrm{Tr}(aa^{-1}) = \mathrm{Tr}(1) = [K : \mathbf{Q}] > 0$, which is absurd. □

Definition 10.2.2 (Discriminant). Suppose $a_1, \ldots, a_n$ is any $\mathbf{Q}$-basis of K. The *discriminant* of $a_1, \ldots, a_n$ is

$$\mathrm{Disc}(a_1, \ldots, a_n) = \mathrm{Det}(\mathrm{Tr}(a_i a_j)_{1 \leq i,j \leq n}) \in \mathbf{Q}.$$

The *discriminant* $\mathrm{Disc}(\mathcal{O})$ of an order $\mathcal{O}$ in $\mathcal{O}_K$ is the discriminant of any basis for $\mathcal{O}$. The *discriminant* $d_K = \mathrm{Disc}(K)$ of the number field K is the discrimimant of $\mathcal{O}_K$.

Note that the discriminants defined above are all nonzero by Lemma 10.2.1.

Warning: In Magma $\mathrm{Disc}(K)$ is defined to be the discriminant of the polynomial you happened to use to define K, which is (in my opinion) a poor choice and goes against most of the literature.

The following proposition asserts that the discriminant of an order $\mathcal{O}$ in $\mathcal{O}_K$ is bigger than $\mathrm{disc}(\mathcal{O}_K)$ by a factor of the square of the index.

Proposition 10.2.3. *Suppose $\mathcal{O}$ is an order in $\mathcal{O}_K$. Then*

$$\mathrm{Disc}(\mathcal{O}) = \mathrm{Disc}(\mathcal{O}_K) \cdot [\mathcal{O}_K : \mathcal{O}]^2.$$

Proof. Let A be a matrix whose rows are the images via σ of a basis for $\mathcal{O}_K$, and let B be a matrix whose rows are the images via σ of a basis for $\mathcal{O}$. Since $\mathcal{O} \subset \mathcal{O}_K$ has finite index, there is an integer matrix C such that $CA = B$, and $|\mathrm{Det}(C)| = [\mathcal{O}_K : \mathcal{O}]$. Then

$$\mathrm{Disc}(\mathcal{O}) = \mathrm{Det}(B)^2 = \mathrm{Det}(CA)^2 = \mathrm{Det}(C)^2\,\mathrm{Det}(A)^2 = [\mathcal{O}_K : \mathcal{O}]^2 \cdot \mathrm{Disc}(\mathcal{O}_K).$$

□

This result is enough to give an algorithm for computing $\mathcal{O}_K$, albeit a potentially slow one. Given K, find some order $\mathcal{O} \subset K$, and compute $d = \mathrm{Disc}(\mathcal{O})$. Factor d, and use the factorization to write $d = s \cdot f^2$, where f^2 is the largest square that divides d. Then the index of $\mathcal{O}$ in $\mathcal{O}_K$ is a divisor of f, and we (tediously) can enumerate all rings R with $\mathcal{O} \subset R \subset K$ and $[R : \mathcal{O}] \mid f$, until we find the largest one all of whose elements are integral.

Example 10.2.4. Consider the ring $\mathcal{O}_K = \mathbf{Z}[(1+\sqrt{5})/2]$ of integers of $K = \mathbf{Q}(\sqrt{5})$. The discriminant of the basis $1, a = (1+\sqrt{5})/2$ is

$$\mathrm{Disc}(\mathcal{O}_K) = \left| \begin{pmatrix} 2 & 1 \\ 1 & 3 \end{pmatrix} \right| = 5.$$

Let $\mathcal{O} = \mathbf{Z}[\sqrt{5}]$ be the order generated by $\sqrt{5}$. Then $\mathcal{O}$ has basis $1, \sqrt{5}$, so

$$\mathrm{Disc}(\mathcal{O}) = \left| \begin{pmatrix} 2 & 0 \\ 0 & 10 \end{pmatrix} \right| = 20 = [\mathcal{O}_K : \mathcal{O}]^2 \cdot 5.$$

10.3 Norms of Ideals

In this section we extend the notion of norm to ideals. This will be helpful in proving of class groups in the next section. For example, we will prove that the group of fractional ideals modulo principal fractional ideals of a number field is finite by showing that every ideal is equivalent to an ideal with norm at most some a priori bound.

Definition 10.3.1 (Lattice Index). If L and M are two lattices in vector space V, then the *lattice index* $[L : M]$ is by definition the absolute value of the determinant of any linear automorphism A of V such that $A(L) = M$.

The lattice index has the following properties:

- If $M \subset L$, then $[L : M] = \#(L/M)$.
- If M, L, N are lattices then $[L : N] = [L : M] \cdot [M : N]$.

Definition 10.3.2 (Norm of Fractional Ideal). Suppose I is a fractional ideal of $\mathcal{O}_K$. The *norm* of I is the lattice index

$$\mathrm{Norm}(I) = [\mathcal{O}_K : I] \in \mathbf{Q}_{\geq 0},$$

or 0 if $I = 0$.

Note that if I is an integral ideal, then $\mathrm{Norm}(I) = \#(\mathcal{O}_K/I)$.

Lemma 10.3.3. *Suppose $a \in K$ and I is an integral ideal. Then*

$$\mathrm{Norm}(aI) = |\,\mathrm{Norm}_{K/\mathbf{Q}}(a)|\,\mathrm{Norm}(I).$$

Proof. By properties of the lattice index mentioned above we have

$$[\mathcal{O}_K : aI] = [\mathcal{O}_K : I] \cdot [I : aI] = \mathrm{Norm}(I) \cdot |\,\mathrm{Norm}_{K/\mathbf{Q}}(a)|.$$

Here we have used that $[I : aI] = |\,\mathrm{Norm}_{K/\mathbf{Q}}(a)|$, which is because left multiplication ℓ_a is an automorphism of K that sends I onto aI, so $[I : aI] = |\,\mathrm{Det}(\ell_a)| = |\,\mathrm{Norm}_{K/\mathbf{Q}}(a)|$. □

Proposition 10.3.4. *If I and J are fractional ideals, then*

$$\mathrm{Norm}(IJ) = \mathrm{Norm}(I) \cdot \mathrm{Norm}(J).$$

Proof. By Lemma 10.3.3, it suffices to prove this when I and J are integral ideals. If I and J are coprime, then Theorem 9.1.3 (Chinese Remainder Theorem) implies that $\mathrm{Norm}(IJ) = \mathrm{Norm}(I)\cdot\mathrm{Norm}(J)$. Thus we reduce to the case when $I = \mathfrak{p}^m$ and $J = \mathfrak{p}^k$ for some prime ideal $\mathfrak{p}$ and integers m, k. By Proposition 9.1.8 (consequence of CRT that $\mathcal{O}_K/\mathfrak{p} \cong \mathfrak{p}^n/\mathfrak{p}^{n+1}$), the filtration of $\mathcal{O}_K/\mathfrak{p}^n$ given by powers of $\mathfrak{p}$ has successive quotients isomorphic to $\mathcal{O}_K/\mathfrak{p}$, so we see that $\#(\mathcal{O}_K/\mathfrak{p}^n) = \#(\mathcal{O}_K/\mathfrak{p})^n$, which proves that $\mathrm{Norm}(\mathfrak{p}^n) = \mathrm{Norm}(\mathfrak{p})^n$. □

Lemma 10.3.5. *Fix a number field K. Let B be a positive integer. There are only finitely many integral ideals I of $\mathcal{O}_K$ with norm at most B.*

Proof. An integral ideal I is a subgroup of $\mathcal{O}_K$ of index equal to the norm of I. If G is any finitely generated abelian group, then there are only finitely many subgroups of G of index at most B, since the subgroups of index dividing an integer n are all subgroups of G that contain nG, and the group G/nG is finite. This proves the lemma. □

10.4 Finiteness of the Class Group via Geometry of Numbers

We have seen examples in which $\mathcal{O}_K$ is not a unique factorization domain. If $\mathcal{O}_K$ is a principal ideal domain, then it is a unique factorization domain, so it is of interest to understand how badly $\mathcal{O}_K$ fails to be a principal ideal domain. The class group of $\mathcal{O}_K$ measures this failure. As one sees in a course on Class Field Theory, the class group and its generalizations also yield deep insight into the possible abelian Galois extensions of K.

Definition 10.4.1 (Class Group). Let $\mathcal{O}_K$ be the ring of integers of a number field K. The *class group* C_K of K is the group of nonzero fractional ideals modulo the sugroup of principal fractional ideals (a), for $a \in K$.

Note that if we let $\mathrm{Div}(K)$ denote the group of nonzero fractional ideals, then there is an exact sequence

$$0 \to \mathcal{O}_K^* \to K^* \to \mathrm{Div}(K) \to C_K \to 0.$$

A basic theorem in algebraic number theory is that the class group C_K is finite, which follows from the first part of the following theorem and the fact that there are only finitely many ideals of norm less than a given integer.

Theorem 10.4.2 (Finiteness of the Class Group). *Let K be a number field. There is a constant $C_{r,s}$ that depends only on the number r, s of real and pairs of complex conjugate embeddings of K such that every ideal class of $\mathcal{O}_K$ contains an integral ideal of norm at most $C_{r,s}\sqrt{|d_K|}$, where $d_K = \mathrm{Disc}(\mathcal{O}_K)$. Thus by Lemma 10.3.5 the class group C_K of K is finite. One can choose $C_{r,s}$ such that every ideal class in C_K contains an integral ideal of norm at most*

$$\sqrt{|d_K|} \cdot \left(\frac{4}{\pi}\right)^s \frac{n!}{n^n}.$$

The explicit bound in the theorem is called the Minkowski bound, and I think it is the best known unconditional general bound (though there are better bounds in certain special cases).

Before proving Theorem 10.4.2, we prove a few lemmas. The strategy of the proof will be to start with any nonzero ideal I, and prove that there is some nonzero $a \in K$, with very small norm, such that aI is an integral ideal. Then $\mathrm{Norm}(aI) = \mathrm{Norm}_{K/\mathbf{Q}}(a)\,\mathrm{Norm}(I)$ will be small, since $\mathrm{Norm}_{K/\mathbf{Q}}(a)$ is small. The trick is to determine precisely how small an a we can choose subject to the condition that aI be an integral ideal, i.e., that $a \in I^{-1}$.

Let S be a subset of $V = \mathbf{R}^n$. Then S is *convex* if whenever $x, y \in S$ then the line connecting x and y lies entirely in S. We say that S is *symmetric about the origin* if whenever $x \in S$ then $-x \in S$ also. If L is a lattice in V, then the *volume* of V/L is the volume of the compact real manifold V/L, which is the same thing as the absolute value of the determinant of any matrix whose rows form a basis for L.

Lemma 10.4.3 (Blichfeld). *Let L be a lattice in $V = \mathbf{R}^n$, and let S be a bounded closed convex subset of V that is symmetric about the origin. Assume that $\mathrm{Vol}(S) \geq 2^n \,\mathrm{Vol}(V/L)$. Then S contains a nonzero element of L.*

Proof. First assume that $\mathrm{Vol}(S) > 2^n \cdot \mathrm{Vol}(V/L)$. If the map $\pi : \frac{1}{2}S \to V/L$ is injective, then

$$\frac{1}{2^n}\,\mathrm{Vol}(S) = \mathrm{Vol}\left(\frac{1}{2}S\right) \leq \mathrm{Vol}(V/L),$$

a contradiction. Thus π is not injective, so there exist $P_1 \neq P_2 \in \frac{1}{2}S$ such that $P_1 - P_2 \in L$. By symmetry $-P_2 \in \frac{1}{2}S$. By convexity, the average $\frac{1}{2}(P_1 - P_2)$ of P_1 and $-P_2$ is also in $\frac{1}{2}S$. Thus $0 \neq P_1 - P_2 \in S \cap L$, as claimed.

Next assume that $\mathrm{Vol}(S) = 2^n \cdot \mathrm{Vol}(V/L)$. Then for all $\varepsilon > 0$ there is $0 \neq Q_\varepsilon \in L \cap (1+\varepsilon)S$, since $\mathrm{Vol}((1+\varepsilon)S) > \mathrm{Vol}(S) = 2^n \cdot \mathrm{Vol}(V/L)$. If $\varepsilon < 1$ then the Q_ε are all in $L \cap 2S$, which is finite since $2S$ is bounded and L is discrete. Hence there exists $Q = Q_\varepsilon \in L \cap (1+\varepsilon)S$ for arbitrarily small ε. Since S is closed, $Q \in L \cap S$. □

Lemma 10.4.4. *If L_1 and L_2 are lattices in V, then*

$$\mathrm{Vol}(V/L_2) = \mathrm{Vol}(V/L_1) \cdot [L_1 : L_2].$$

Proof. Let A be an automorphism of V such that $A(L_1) = L_2$. Then A defines an isomorphism of real manifolds $V/L_1 \to V/L_2$ that changes volume by a factor of $|\mathrm{Det}(A)| = [L_1 : L_2]$. The claimed formula then follows. □

Fix a number field K with ring of integers $\mathcal{O}_K$. Let $\sigma : K \to V = \mathbf{R}^n$ be the embedding

$$\begin{aligned}\sigma(x) = \big(&\sigma_1(x), \sigma_2(x), \ldots, \sigma_r(x),\\ &\mathrm{Re}(\sigma_{r+1}(x)), \ldots, \mathrm{Re}(\sigma_{r+s}(x)), \mathrm{Im}(\sigma_{r+1}(x)), \ldots, \mathrm{Im}(\sigma_{r+s}(x))\big),\end{aligned}$$

where $\sigma_1, \ldots, \sigma_r$ are the real embeddings of K and $\sigma_{r+1}, \ldots, \sigma_{r+s}$ are half the complex embeddings of K, with one representative of each pair of complex conjugate embeddings. Note that this σ is *not* exactly the same as the one at the beginning of Section 10.2.

Lemma 10.4.5.
$$\mathrm{Vol}(V/\sigma(\mathcal{O}_K)) = 2^{-s}\sqrt{|d_K|}.$$

Proof. Let $L = \sigma(\mathcal{O}_K)$. From a basis $w_1, \ldots, w_n$ for $\mathcal{O}_K$ we obtain a matrix A whose ith row is

$$(\sigma_1(w_i), \cdots, \sigma_r(w_i), \mathrm{Re}(\sigma_{r+1}(w_i)), \ldots, \mathrm{Re}(\sigma_{r+s}(w_1)), \mathrm{Im}(\sigma_{r+1}(w_i)), \ldots, \mathrm{Im}(\sigma_{r+s}(w_1)))$$

and whose determinant has absolute value equal to the volume of V/L. By doing the following three column operations, we obtain a matrix whose rows are exactly the images of the w_i under *all* embeddings of K into $\mathbf{C}$, which is the matrix that came up when we defined d_K.

1. Add $i = \sqrt{-1}$ times each column with entries $\mathrm{Im}(\sigma_{r+j}(w_i))$ to the column with entries $\mathrm{Re}(\sigma_{r+j}(w_i))$.

2. Multiply all columns $\mathrm{Im}(\sigma_{r+j}(w_i))$ by $-2i$, thus changing the determinant by $(-2i)^s$.

3. Add each columns with entries $\mathrm{Re}(\sigma_{r+j}(w_i))$ to the the column with entries $-2i\mathrm{Im}(\sigma_{r+j}(w_i))$.

Recalling the definition of discriminant, we see that if B is the matrix constructed by the above three operations, then $\mathrm{Det}(B)^2 = d_K$. Thus

$$\mathrm{Vol}(V/L) = |\,\mathrm{Det}(A)| = |(-2i)^{-s} \cdot \mathrm{Det}(B)| = 2^{-s}\sqrt{|d_K|}.$$

□

Lemma 10.4.6. *If I is a nonzero fractional ideal for $\mathcal{O}_K$, then $\sigma(I)$ is a lattice in V, and*
$$\mathrm{Vol}(V/\sigma(I)) = 2^{-s}\sqrt{|d_K|} \cdot \mathrm{Norm}(I).$$

Proof. We know that $[\mathcal{O}_K : I] = \mathrm{Norm}(I)$ is a nonzero rational number. Lemma 10.4.5 implies that $\sigma(\mathcal{O}_K)$ is a lattice in V, since $\sigma(\mathcal{O}_K)$ has rank n as abelian group and spans V, so $\sigma(I)$ is also a lattice in V. For the volume formula, combine Lemmas 10.4.4–10.4.5 to get

$$\mathrm{Vol}(V/\sigma(I)) = \mathrm{Vol}(V/\sigma(\mathcal{O}_K)) \cdot [\mathcal{O}_K : I] = 2^{-s}\sqrt{|d_K|}\,\mathrm{Norm}(I).$$

□

Proof of Theorem 10.4.2. Let K be a number field with ring of integers $\mathcal{O}_K$, let $\sigma : K \hookrightarrow V \cong \mathbf{R}^n$ be as above, and let $f : V \to \mathbf{R}$ be the function defined by

$$f(x_1, \ldots, x_n) = |x_1 \cdots x_r \cdot (x_{r+1}^2 + x_{(r+1)+s}^2) \cdots (x_{r+s}^2 + x_n^2).$$

Notice that if $x \in K$ then $f(\sigma(x)) = |\,\mathrm{Norm}_{K/\mathbf{Q}}(x)|$.

Let $S \subset V$ be any closed, bounded, convex, subset that is symmetric with respect to the origin and has positive volume. Since S is closed and bounded,

$$M = \max\{f(x) : x \in S\}$$

exists.

Suppose I is any nonzero fractional ideal of $\mathcal{O}_K$. Our goal is to prove there is an integral ideal aI with small norm. We will do this by finding an appropriate $a \in I^{-1}$. By Lemma 10.4.6,

$$c = \mathrm{Vol}(V/I^{-1}) = \frac{2^{-s}\sqrt{|d_K|}}{\mathrm{Norm}(I)}.$$

Let $\lambda = 2 \cdot \left(\frac{c}{v}\right)^{1/n}$, where $v = \mathrm{Vol}(S)$. Then

$$\mathrm{Vol}(\lambda S) = \lambda^n \mathrm{Vol}(S) = 2^n \frac{c}{v} \cdot v = 2^n \cdot c = 2^n \mathrm{Vol}(V/I^{-1}),$$

so by Lemma 10.4.3 there exists $0 \neq a \in I^{-1} \cap \lambda S$. Since M is the largest norm of an element of S, the largest norm of an element of $I^{-1} \cap \lambda S$ is at most $\lambda^n M$, so

$$|\mathrm{Norm}_{K/\mathbf{Q}}(a)| \leq \lambda^n M.$$

Since $a \in I^{-1}$, we have $aI \subset \mathcal{O}_K$, so aI is an integral ideal of $\mathcal{O}_K$ that is equivalent to I, and

$$\begin{aligned}
\mathrm{Norm}(aI) &= |\mathrm{Norm}_{K/\mathbf{Q}}(a)| \cdot \mathrm{Norm}(I) \\
&\leq \lambda^n M \cdot \mathrm{Norm}(I) \\
&\leq 2^n \frac{c}{v} M \cdot \mathrm{Norm}(I) \\
&\leq 2^n \cdot 2^{-s}\sqrt{|d_K|} \cdot M \cdot v^{-1} \\
&= 2^{r+s}\sqrt{|d_K|} \cdot M \cdot v^{-1}.
\end{aligned}$$

Notice that the right hand side is independent of I. It depends only on r, s, $|d_K|$, and our choice of S. This completes the proof of the theorem, except for the assertion that S can be chosen to give the claim at the end of the theorem, which we leave as an exercise. □

Corollary 10.4.7. *Suppose that $K \neq \mathbf{Q}$ is a number field. Then $|d_K| > 1$.*

Proof. Applying Theorem 10.4.2 to the unit ideal, we get the bound

$$1 \leq \sqrt{|d_K|} \cdot \left(\frac{4}{\pi}\right)^s \frac{n!}{n^n}.$$

Thus

$$\sqrt{|d_K|} \geq \left(\frac{\pi}{4}\right)^s \frac{n^n}{n!},$$

and the right hand quantity is strictly bigger than 1 for any $s \leq n/2$ and any $n > 1$ (exercise). □

10.4.1 An Open Problem

Conjecture 10.4.8. *There are infinitely many number fields K such that the class group of K has order* 1*.*

For example, if we consider real quadratic fields $K = \mathbf{Q}(\sqrt{d})$, with d positive and square free, many class numbers are probably 1, as suggested by the MAGMA output below. It looks like 1's will keep appearing infinitely often, and indeed Cohen and Lenstra conjecture that they do. Nobody has found a way to prove this yet.

```
> for d in [2..1000] do
     if d eq SquareFree(d) then
        h := ClassNumber(NumberField(x^2-d));
        if h eq 1 then
           printf "%o, ", d;
        end if;
     end if;
   end for;

2, 3, 5, 6, 7, 11, 13, 14, 17, 19, 21, 22, 23, 29, 31, 33, 37,
38, 41, 43, 46, 47, 53, 57, 59, 61, 62, 67, 69, 71, 73, 77, 83,
86, 89, 93, 94, 97, 101, 103, 107, 109, 113, 118, 127, 129, 131,
133, 134, 137, 139, 141, 149, 151, 157, 158, 161, 163, 166, 167,
173, 177, 179, 181, 191, 193, 197, 199, 201, 206, 209, 211, 213,
214, 217, 227, 233, 237, 239, 241, 249, 251, 253, 262, 263, 269,
271, 277, 278, 281, 283, 293, 301, 302, 307, 309, 311, 313, 317,
329, 331, 334, 337, 341, 347, 349, 353, 358, 367, 373, 379, 381,
382, 383, 389, 393, 397, 398, 409, 413, 417, 419, 421, 422, 431,
433, 437, 446, 449, 453, 454, 457, 461, 463, 467, 478, 479, 487,
489, 491, 497, 501, 502, 503, 509, 517, 521, 523, 526, 537, 541,
542, 547, 553, 557, 563, 566, 569, 571, 573, 581, 587, 589, 593,
597, 599, 601, 607, 613, 614, 617, 619, 622, 631, 633, 641, 643,
647, 649, 653, 661, 662, 669, 673, 677, 681, 683, 691, 694, 701,
709, 713, 717, 718, 719, 721, 734, 737, 739, 743, 749, 751, 753,
757, 758, 766, 769, 773, 781, 787, 789, 797, 809, 811, 813, 821,
823, 827, 829, 838, 849, 853, 857, 859, 862, 863, 869, 877, 878,
881, 883, 886, 887, 889, 893, 907, 911, 913, 917, 919, 921, 926,
929, 933, 937, 941, 947, 953, 958, 967, 971, 973, 974, 977, 983,
989, 991, 997, 998,
```

In contrast, if we look at class numbers of quadratic imaginary fields, only a few at the beginning have class number 1.

```
> for d in [1..1000] do
     if d eq SquareFree(d) then
        h := ClassNumber(NumberField(x^2+d));
```

```
          if h eq 1 then
             printf "%o, ", d;
          end if;
       end if;
    end for;
 1, 2, 3, 7, 11, 19, 43, 67, 163
```

It is a theorem that the above list of 9 fields is the complete list with class number 1. More generally, it is possible (in theory), using deep work of Gross, Zagier, and Goldfeld involving zeta functions and elliptic curves, to enumerate all quadratic number fields with a given class number.

Chapter 11

Computing Class Groups

In this chapter we discuss how to compute class groups in some examples, then introduce the group of units. We will prove the main structure theorem for the group of units in the next chapter.

11.1 Remarks on Computing the Class Group

If $\mathfrak{p}$ is a prime of $\mathcal{O}_K$, then the intersection $\mathfrak{p} \cap \mathbf{Z} = p\mathbf{Z}$ is a prime ideal of $\mathbf{Z}$. We say that $\mathfrak{p}$ *lies over* $p \in \mathbf{Z}$. Note $\mathfrak{p}$ lies over $p \in \mathbf{Z}$ if and only if $\mathfrak{p}$ is one of the prime factors in the factorization of the ideal $p\mathcal{O}_K$. Geometrically, $\mathfrak{p}$ is a point of $\mathrm{Spec}(\mathcal{O}_K)$ that lies over the point $p\mathbf{Z}$ of $\mathrm{Spec}(\mathbf{Z})$ under the map induced by the inclusion $\mathbf{Z} \hookrightarrow \mathcal{O}_K$.

Lemma 11.1.1. *Let K be a number field with ring of integers $\mathcal{O}_K$. Then the class group* $\mathrm{Cl}(K)$ *is generated by the prime ideals $\mathfrak{p}$ of $\mathcal{O}_K$ lying over primes $p \in \mathbf{Z}$ with $p \leq B_K = \sqrt{|d_K|} \cdot \left(\frac{4}{\pi}\right)^s \cdot \frac{n!}{n^n}$, where s is the number of complex conjugate pairs of embeddings $K \hookrightarrow \mathbf{C}$.*

Proof. We proved before that every ideal class in $\mathrm{Cl}(K)$ is represented by an ideal I with $\mathrm{Norm}(I) \leq B_K$. Write $I = \prod_{i=1}^m \mathfrak{p}_i^{e_i}$, with each $e_i \geq 1$. Then by multiplicativity of the norm, each $\mathfrak{p}_i$ also satisfies $\mathrm{Norm}(\mathfrak{p}_i) \leq B_K$. If $\mathfrak{p}_i \cap \mathbf{Z} = p\mathbf{Z}$, then $p \mid \mathrm{Norm}(\mathfrak{p}_i)$, since p is the residue characteristic of $\mathcal{O}_K/\mathfrak{p}$, so $p \leq B_K$. Thus I is a product of primes $\mathfrak{p}$ that satisfies the norm bound of the lemma, whcih proves the lemma. $\square$

This is a sketch of how to compute $\mathrm{Cl}(K)$:

1. Use the "factoring primes" algorithm to list all prime ideals $\mathfrak{p}$ of $\mathcal{O}_K$ that appear in the factorization of a prime $p \in \mathbf{Z}$ with $p \leq B_K$.

2. Find the group generated by the ideal classes $[\mathfrak{p}]$, where the $\mathfrak{p}$ are the prime ideals found in step 1. (In general, one must think more carefully about how to do this step.)

The following three examples illustrate computation of $\mathrm{Cl}(K)$ for $K = \mathbf{Q}(i), \mathbf{Q}(\sqrt{5})$ and $\mathbf{Q}(\sqrt{-6})$.

Example 11.1.2. We compute the class group of $K = \mathbf{Q}(i)$. We have

$$n = 2, \quad r = 0, \quad s = 1, \quad d_K = -4,$$

so

$$B_K = \sqrt{4} \cdot \left(\frac{4}{\pi}\right)^1 \cdot \left(\frac{2!}{2^2}\right) = \frac{8}{\pi} < 3.$$

Thus $\mathrm{Cl}(K)$ is generated by the prime divisors of 2. We have

$$2\mathcal{O}_K = (1+i)^2,$$

so $\mathrm{Cl}(K)$ is generated by the principal prime ideal $\mathfrak{p} = (1+i)$. Thus $\mathrm{Cl}(K) = 0$ is trivial.

Example 11.1.3. We compute the class group of $K = \mathbf{Q}(\sqrt{5})$. We have

$$n = 2, \quad r = 2, \quad s = 0, \quad d_K = 5,$$

so

$$B = \sqrt{5} \cdot \left(\frac{4}{\pi}\right)^0 \cdot \left(\frac{2!}{2^2}\right) < 3.$$

Thus $\mathrm{Cl}(K)$ is generated by the primes that divide 2. We have $\mathcal{O}_K = \mathbf{Z}[\gamma]$, where $\gamma = \frac{1+\sqrt{5}}{2}$ satisfies $x^2 - x - 1$. The polynomial $x^2 - x - 1$ is irreducible mod 2, so $2\mathcal{O}_K$ is prime. Since it is principal, we see that $\mathrm{Cl}(K) = 1$ is trivial.

Example 11.1.4. In this example, we compute the class group of $K = \mathbf{Q}(\sqrt{-6})$. We have

$$n = 2, \quad r = 0, \quad s = 1, \quad d_K = -24,$$

so

$$B = \sqrt{24} \cdot \frac{4}{\pi} \cdot \left(\frac{2!}{2^2}\right) \sim 3.1.$$

Thus $\mathrm{Cl}(K)$ is generated by the prime ideals lying over 2 and 3. We have $\mathcal{O}_K = \mathbf{Z}[\sqrt{-6}]$, and $\sqrt{-6}$ satisfies $x^2 + 6 = 0$. Factoring $x^2 + 6$ modulo 2 and 3 we see that the class group is generated by the prime ideals

$$\mathfrak{p}_2 = (2, \sqrt{-6}) \qquad \text{and} \qquad \mathfrak{p}_3 = (3, \sqrt{-6}).$$

Also, $\mathfrak{p}_2^2 = 2\mathcal{O}_K$ and $\mathfrak{p}_3^2 = 3\mathcal{O}_K$, so $\mathfrak{p}_2$ and $\mathfrak{p}_3$ define elements of order dividing 2 in $\mathrm{Cl}(K)$.

Is either $\mathfrak{p}_2$ or $\mathfrak{p}_3$ principal? Fortunately, there is an easier norm trick that allows us to decide. Suppose $\mathfrak{p}_2 = (\alpha)$, where $\alpha = a + b\sqrt{-6}$. Then

$$2 = \mathrm{Norm}(\mathfrak{p}_2) = |\,\mathrm{Norm}(\alpha)| = (a + b\sqrt{-6})(a - b\sqrt{-6}) = a^2 + 6b^2.$$

Trying the first few values of $a, b \in \mathbf{Z}$, we see that this equation has no solutions, so $\mathfrak{p}_2$ can not be principal. By a similar argument, we see that $\mathfrak{p}_3$ is not principal either. Thus $\mathfrak{p}_2$ and $\mathfrak{p}_3$ define elements of order 2 in $\mathrm{Cl}(K)$.

Does the class of $\mathfrak{p}_2$ equal the class of $\mathfrak{p}_3$? Since $\mathfrak{p}_2$ and $\mathfrak{p}_3$ define classes of order 2, we can decide this by finding the class of $\mathfrak{p}_2 \cdot \mathfrak{p}_3$. We have

$$\mathfrak{p}_2 \cdot \mathfrak{p}_3 = (2, \sqrt{-6}) \cdot (3, \sqrt{-6}) = (6, 2\sqrt{-6}, 3\sqrt{-6}) \subset (\sqrt{-6}).$$

The ideals on both sides of the inclusion have norm 6, so by multiplicativity of the norm, they must be the same ideal. Thus $\mathfrak{p}_2 \cdot \mathfrak{p}_3 = (\sqrt{-6})$ is principal, so $\mathfrak{p}_2$ and $\mathfrak{p}_3$ represent the same element of $\mathrm{Cl}(K)$. We conclude that

$$\mathrm{Cl}(K) = \langle \mathfrak{p}_2 \rangle = \mathbf{Z}/2\mathbf{Z}.$$

Chapter 12

Dirichlet's Unit Theorem

In this chapter we will prove the main structure theorem for the group of units of the ring of integers of a number field. The answer is remarkably simple: if K has r real and s complex embeddings, then

$$\mathcal{O}_K^* \approx \mathbf{Z}^{r+s-1} \oplus W,$$

where W is the finite cyclic group of roots of unity in K. Examples will follow on Thursday (application: the solutions to Pell's equation $x^2 - dy^2 = 1$, for $d > 1$ squarefree, form a free abelian group of rank 1).

12.1 The Group of Units

Definition 12.1.1 (Unit Group). The *group of units* U_K associated to a number field K is the group of elements of $\mathcal{O}_K$ that have an inverse in $\mathcal{O}_K$.

Theorem 12.1.2 (Dirichlet). *The group U_K is the product of a finite cyclic group of roots of unity with a free abelian group of rank $r+s-1$, where r is the number of real embeddings of K and s is the number of complex conjugate pairs of embeddings.*

We prove the theorem by defining a map $\varphi : U_K \to \mathbf{R}^{r+s}$, and showing that the kernel of φ is finite and the image of φ is a lattice in a hyperplane in $\mathbf{R}^{r+s}$. The trickiest part of the proof is showing that the image of φ spans a hyperplane, and we do this by a clever application of Blichfeldt's lemma (that if S is closed, bounded, symmetric, etc., and has volume at least $2^n \cdot \mathrm{Vol}(V/L)$, then $S \cap L$ contains a nonzero element).

Remark 12.1.3. Theorem 12.1.2 is due to Dirichlet who lived 1805–1859. Thomas Hirst described Dirichlet as follows:

> He is a rather tall, lanky-looking man, with moustache and beard about to turn grey with a somewhat harsh voice and rather deaf. He was unwashed, with his cup of coffee and cigar. One of his failings is forgetting time, he pulls his watch out, finds it past three, and runs out without even finishing the sentence.

Koch wrote that:

> ... important parts of mathematics were influenced by Dirichlet. His proofs characteristically started with surprisingly simple observations, followed by extremely sharp analysis of the remaining problem.

I think Koch's observation nicely describes the proof we will give of Theorem 12.1.2.

The following proposition explains how to think about units in terms of the norm.

Proposition 12.1.4. *An element $a \in \mathcal{O}_K$ is a unit if and only if* $\mathrm{Norm}_{K/\mathbf{Q}}(a) = \pm 1$.

Proof. Write $\mathrm{Norm} = \mathrm{Norm}_{K/\mathbf{Q}}$. If a is a unit, then a^{-1} is also a unit, and $1 = \mathrm{Norm}(a)\,\mathrm{Norm}(a^{-1})$. Since both $\mathrm{Norm}(a)$ and $\mathrm{Norm}(a^{-1})$ are integers, it follows that $\mathrm{Norm}(a) = \pm 1$. Conversely, if $a \in \mathcal{O}_K$ and $\mathrm{Norm}(a) = \pm 1$, then the equation $aa^{-1} = 1 = \pm\,\mathrm{Norm}(a)$ implies that $a^{-1} = \pm\,\mathrm{Norm}(a)/a$. But $\mathrm{Norm}(a)$ is the product of the images of a in $\mathbf{C}$ by all embeddings of K into $\mathbf{C}$, so $\mathrm{Norm}(a)/a$ is also a product of images of a in $\mathbf{C}$, hence a product of algebraic integers, hence an algebraic integer. Thus $a^{-1} \in \mathcal{O}_K$, which proves that a is a unit. $\square$

Let r be the number of real and s the number of complex conjugate embeddings of K into $\mathbf{C}$, so $n = [K : \mathbf{Q}] = r + 2s$. Define a map

$$\varphi : U_K \to \mathbf{R}^{r+s}$$

by

$$\varphi(a) = (\log|\sigma_1(a)|, \ldots, \log|\sigma_{r+s}(a)|).$$

Lemma 12.1.5. *The image of φ lies in the hyperplane*

$$H = \{(x_1, \ldots, x_{r+s}) \in \mathbf{R}^{r+s} : x_1 + \cdots + x_r + 2x_{r+1} + \cdots + 2x_{r+s} = 0\}. \quad (12.1.1)$$

Proof. If $a \in U_K$, then by Proposition 12.1.4,

$$\left(\prod_{i=1}^{r} |\sigma_i(a)|\right) \cdot \left(\prod_{i=r+1}^{s} |\sigma_i(a)|^2\right) = 1.$$

Taking logs of both sides proves the lemma. $\square$

Lemma 12.1.6. *The kernel of φ is finite.*

Proof. We have

$$\begin{aligned}\mathrm{Ker}(\varphi) &\subset \{a \in \mathcal{O}_K : |\sigma_i(a)| = 1 \text{ for all } i = 1, \ldots, r+2s\}\\ &\subset \sigma(\mathcal{O}_K) \cap X,\end{aligned}$$

where X is the bounded subset of $\mathbf{R}^{r+2s}$ of elements all of whose coordinates have absolute value at most 1. Since $\sigma(\mathcal{O}_K)$ is a lattice (see Proposition 5.2.4), the intersection $\sigma(\mathcal{O}_K) \cap X$ is finite, so $\mathrm{Ker}(\varphi)$ is finite. $\square$

Lemma 12.1.7. *The kernel of φ is a finite cyclic group.*

Proof. It is a general fact that any finite subgroup of the multiplicative group of a field is cyclic. [Homework.] $\square$

To prove Theorem 12.1.2, it suffices to proove that $\mathrm{Im}(\varphi)$ is a lattice in the hyperplane H from (12.1.1), which we view as a vector space of dimension $r+s-1$.

Define an embedding

$$\sigma : K \hookrightarrow \mathbf{R}^n \tag{12.1.2}$$

given by $\sigma(x) = (\sigma_1(x), \ldots, \sigma_{r+s}(x))$, where we view $\mathbf{C} \cong \mathbf{R}\times\mathbf{R}$ via $a+bi \mapsto (a,b)$. Note that this is exactly the same as the embedding

$$\begin{aligned} x \mapsto \big(&\sigma_1(x), \sigma_2(x), \ldots, \sigma_r(x),\\ &\mathrm{Re}(\sigma_{r+1}(x)), \ldots, \mathrm{Re}(\sigma_{r+s}(x)), \mathrm{Im}(\sigma_{r+1}(x)), \ldots, \mathrm{Im}(\sigma_{r+s}(x))\big), \end{aligned}$$

from before, except that we have re-ordered the last s imaginary components to be next to their corresponding real parts.

Lemma 12.1.8. *The image of φ is discrete in $\mathbf{R}^{r+s}$.*

Proof. Suppose X is any bounded subset of $\mathbf{R}^{r+s}$. Then for any $u \in Y = \varphi^{-1}(X)$ the coordinates of $\sigma(u)$ are bounded in terms of X (since log is an increasing function). Thus $\sigma(Y)$ is a bounded subset of $\mathbf{R}^n$. Since $\sigma(Y) \subset \sigma(\mathcal{O}_K)$, and $\sigma(\mathcal{O}_K)$ is a lattice in $\mathbf{R}^n$, it follows that $\sigma(Y)$ is finite. Since σ is injective, Y is finite, and φ has finite kernel, so $\varphi(U_K) \cap X$ is finite, which implies that $\varphi(U_K)$ is discrete. $\square$

To finish the proof of Theorem 12.1.2, we will show that the image of φ spans H. Let W be the $\mathbf{R}$-span of the image $\varphi(U_K)$, and note that W is a subspace of H. We will show that $W = H$ indirectly by showing that if $v \notin H^\perp$, where $\perp$ is with respect to the dot product on $\mathbf{R}^{r+s}$, then $v \notin W^\perp$. This will show that $W^\perp \subset H^\perp$, hence that $H \subset W$, as required.

Thus suppose $z = (z_1, \ldots, z_{r+s}) \notin H^\perp$. Define a function $f : K^* \to \mathbf{R}$ by

$$f(x) = z_1 \log|\sigma_1(x)| + \cdots z_{r+s} \log|\sigma_{r+s}(x)|. \tag{12.1.3}$$

To show that $z \notin W^\perp$ we show that there exists some $u \in U_K$ with $f(u) \neq 0$.

Let

$$A = \sqrt{|d_K|} \cdot \left(\frac{2}{\pi}\right)^s \in \mathbf{R}_{>0}.$$

Choose any positive real numbers $c_1, \ldots, c_{r+s} \in \mathbf{R}_{>0}$ such that

$$c_1 \cdots c_r \cdot (c_{r+1} \cdots c_{r+s})^2 = A.$$

Let

$$\begin{aligned} S = \{&(x_1, \ldots, x_n) \in \mathbf{R}^n :\\ &|x_i| \le c_i \text{ for } 1 \le i \le r,\\ &|x_i^2 + x_{i+s}^2| \le c_i^2 \text{ for } r < i \le r+s\} \subset \mathbf{R}^n. \end{aligned}$$

Then S is closed, bounded, convex, symmetric with respect to the origin, and of dimension $r+2s$, since S is a product of r intervals and s discs, each of which has these properties. Viewing S as a product of intervals and discs, we see that the volume of S is

$$\mathrm{Vol}(S) = \prod_{i=1}^{r}(2c_i) \cdot \prod_{i=1}^{s}(\pi c_i^2) = 2^r \cdot \pi^s \cdot A.$$

Recall *Blichfeldt's lemma* that if L is a lattice and S is closed, bounded, etc., and has volume at least $2^n \cdot \mathrm{Vol}(V/L)$, then $S \cap L$ contains a nonzero element. To apply this lemma, we take $L = \sigma(\mathcal{O}_K) \subset \mathbf{R}^n$, where σ is as in (12.1.2). We showed, when proving finiteness of the class group, that $\mathrm{Vol}(\mathbf{R}^n/L) = 2^{-s}\sqrt{|d_K|}$. To check the hypothesis to Blichfeld's lemma, note that

$$\mathrm{Vol}(S) = 2^{r+s}\sqrt{|d_K|} = 2^n 2^{-s}\sqrt{|d_K|} = 2^n \,\mathrm{Vol}(\mathbf{R}^n/L).$$

Thus there exists a nonzero element $a \in S \cap \sigma(\mathcal{O}_K)$, i.e., a nonzero $a \in \mathcal{O}_K$ such that $|\sigma_i(a)| \leq c_i$ for $1 \leq i \leq r+s$. We then have

$$\begin{aligned} |\,\mathrm{Norm}_{K/\mathbf{Q}}(a)| &= \left|\prod_{i=1}^{r+2s} \sigma_i(a)\right| \\ &= \prod_{i=1}^{r} |\sigma_i(a)| \cdot \prod_{i=r+1}^{s} |\sigma_i(a)|^2 \\ &\leq c_1 \cdots c_r \cdot (c_{r+1} \cdots c_{r+s})^2 = A. \end{aligned}$$

Since $a \in \mathcal{O}_K$ is nonzero, we also have

$$|\,\mathrm{Norm}_{K/\mathbf{Q}}(a)| \geq 1.$$

Moreover, if for any $i \leq r$, we have $|\sigma_i(a)| < \frac{c_i}{A}$, then

$$1 \leq |\,\mathrm{Norm}_{K/\mathbf{Q}}(a)| < c_1 \cdots \frac{c_i}{A} \cdots c_r \cdot (c_{r+1} \cdots c_{r+s})^2 = \frac{A}{A} = 1,$$

a contradiction, so $|\sigma_i(a)| \geq \frac{c_i}{A}$ for $i = 1, \ldots, r$. Likewise, $|\sigma_i(a)|^2 \geq \frac{c_i^2}{A}$, for $i = r+1, \ldots, r+s$. Rewriting this we have

$$\frac{c_i}{|\sigma_i(a)|} \leq A \quad \text{for } i \leq r \quad \text{and} \quad \left(\frac{c_i}{|\sigma_i(a)|}\right)^2 \leq A \quad \text{for } i = r+1, \ldots, r+s.$$

Our strategy is to use an appropriately chosen a to construct a unit $u \in U_K$ such $f(u) \neq 0$. First, let $b_1, \ldots, b_m$ be representative generators for the finitely many nonzero principal ideals of $\mathcal{O}_K$ of norm at most A. Since $|\,\mathrm{Norm}_{K/\mathbf{Q}}(a)| \leq A$, we have $(a) = (b_j)$, for some j, so there is a unit $u \in \mathcal{O}_K$ such that $a = ub_j$.

Let

$$s = s(c_1, \ldots, c_{r+s}) = z_1 \log(c_1) + \cdots + z_{r+s} \log(c_{r+s}),$$

and recall $f : K^* \to \mathbf{R}$ defined in (12.1.3) above. We first show that

$$|f(u) - s| \leq B = |f(b_j)| + \log(A) \cdot \left(\sum_{i=1}^{r} |z_i| + \frac{1}{2} \cdot \sum_{i=r+1}^{s} |z_i| \right). \tag{12.1.4}$$

We have

$$\begin{aligned}
|f(u) - s| &= |f(a) - f(b_j) - s| \\
&\leq |f(b_j)| + |s - f(a)| \\
&= |f(b_j)| + |z_1(\log(c_1) - \log(|\sigma_1(a)|)) + \cdots + z_{r+s}(\log(c_{r+s}) - \log(|\sigma_{r+s}(a)|))| \\
&= |f(b_j)| + |z_1 \cdot \log(c_1/|\sigma_1(a)|) + \cdots + \frac{z_{r+s}}{2} \cdot \log((c_{r+s}/|\sigma_{r+s}(a)|)^2)| \\
&\leq |f(b_j)| + \log(A) \cdot \left(\sum_{i=1}^{r} |z_i| + \frac{1}{2} \cdot \sum_{i=r+1}^{s} |z_i| \right).
\end{aligned}$$

The amazing thing about (12.1.4) is that the bound B on the right hand side does not depend on the c_i. Suppose we can choose positive real numbers c_i such that

$$c_1 \cdots c_r \cdot (c_{r+1} \cdots c_{r+s})^2 = A$$

and $s = s(c_1, \ldots, c_{r+s})$ is such that $|s| > B$. Then $|f(u) - s| \leq B$ would imply that $|f(u)| > 0$, which is exactly what we aimed to prove. It is possible to choose such c_i, by proceeding as follows. If $r + s = 1$, then we are trying to prove that $\varphi(U_K)$ is a lattice in $\mathbf{R}^0 = \mathbf{R}^{r+s-1}$, which is automatically true, so assume $r + s > 1$. Then there are at least two distinct c_i. Let j be such that $z_j \neq 0$ (which exists since $z \neq 0$). Then $|z_j \log(c_j)| \to \infty$ as $c_j \to \infty$, so we choose c_j very large and the other c_i, for $i \neq j$, in any way we want subject to the condition

$$\prod_{i=1, i\neq j}^{r} c_i \cdot \prod_{i=r+1}^{s} c_i^2 = \frac{A}{c_j}.$$

Since it is possible to choose the c_i as needed, it is possible to find a unit u such that $f(u) > 0$. We conclude that $z \notin W^\perp$, so $W^\perp \subset Z^\perp$, whence $Z \subset W$, which finishes the proof Theorem 12.1.2.

12.2 Finishing the proof of Dirichlet's Unit Theorem

We begin by finishing Dirichlet's proof that the group of units U_K of $\mathcal{O}_K$ is isomorphic to $\mathbf{Z}^{r+s-1} \oplus \mathbf{Z}/m\mathbf{Z}$, where r is the number of real embeddings, s is half the number of complex embeddings, and m is the number of roots of unity in K. Recall that we defined a map $\varphi : U_K \to \mathbf{R}^{r+s}$ by

$$\varphi(x) = (\log |\sigma_1(x)|, \ldots, \log |\sigma_{r+s}(x)|).$$

Without much trouble, we proved that the kernel of φ if finite and the image φ is discrete, and in the last section we were finishing the proof that the image of φ spans the subspace H of elements of $\mathbf{R}^{r+s}$ that are orthogonal to $v = (1, \ldots, 1, 2, \ldots, 2)$, where r of the entries are 1's and s of them are 2's. The somewhat indirect route we followed was to suppose

$$z \notin H^{\perp} = \mathrm{Span}(v),$$

i.e., that z is not a multiple of v, and prove that z is not orthogonal to some element of $\varphi(U_K)$. Writing $W = \mathrm{Span}(\varphi(U_K))$, this would show that $W^{\perp} \subset H^{\perp}$, so $H \subset W$. We ran into two problems: (1) we ran out of time, and (2) the notes contained an incomplete argument that a quantity $s = s(c_1, \ldots, c_{r+s})$ can be chosen to be arbitrarily large. We will finish going through a complete proof, then compute many examples of unit groups using Magma.

Recall that $f : K^* \to \mathbf{R}$ was defined by

$$f(x) = z_1 \log|\sigma_1(x)| + \cdots + z_{r+s} \log|\sigma_{r+s}(x)| = z \bullet \varphi(x) \qquad \text{(dot product)},$$

and our goal is to show that there is a $u \in U_K$ such that $f(u) \neq 0$.

Our strategy is to use an appropriately chosen a to construct a unit $u \in U_K$ such $f(u) \neq 0$. Recall that we used Blichfeld's lemma to find an $a \in \mathcal{O}_K$ such that $1 \leq |\mathrm{Norm}_{K/\mathbf{Q}}(a)| \leq A$, and

$$\frac{c_i}{|\sigma_i(a)|} \leq A \quad \text{for } i \leq r \quad \text{and} \quad \left(\frac{c_i}{|\sigma_i(a)|}\right)^2 \leq A \quad \text{for } i = r+1, \ldots, r+s. \tag{12.2.1}$$

Let $b_1, \ldots, b_m$ be representative generators for the finitely many nonzero principal ideals of $\mathcal{O}_K$ of norm at most $A = A_K = \sqrt{|d_K|} \cdot \left(\frac{2}{\pi}\right)^s$. Modify the b_i to have the property that $|f(b_i)|$ is minimal among generators of (b_i) (this is possible because ideals are discrete). Note that the set $\{|f(b_i)| : i = 1, \ldots, m\}$ depends only on A. Since $|\mathrm{Norm}_{K/\mathbf{Q}}(a)| \leq A$, we have $(a) = (b_j)$, for some j, so there is a unit $u \in \mathcal{O}_K$ such that $a = ub_j$.

Let

$$s = s(c_1, \ldots, c_{r+s}) = z_1 \log(c_1) + \cdots + z_{r+s} \log(c_{r+s}) \in \mathbf{R}.$$

Lemma 12.2.1. *We have*

$$|f(u) - s| \leq B = \max_i(|f(b_i)|) + \log(A) \cdot \left(\sum_{i=1}^{r} |z_i| + \frac{1}{2} \cdot \sum_{i=r+1}^{s} |z_i|\right),$$

and B depends only on K and our fixed choice of $z \in H^{\perp}$.

Proof. By properties of logarithms, $f(u) = f(a/b_j) = f(a) - f(b_j)$. We next use the triangle inequality $|a + b| \leq |a| + |b|$ in various ways, properties of logarithms, and the bounds (12.2.1) in the following computation:

$$\begin{aligned}
|f(u) - s| &= |f(a) - f(b_j) - s| \\
&\le |f(b_j)| + |s - f(a)| \\
&= |f(b_j)| + |z_1(\log(c_1) - \log(|\sigma_1(a)|)) + \cdots + z_{r+s}(\log(c_{r+s}) - \log(|\sigma_{r+s}(a)|))| \\
&= |f(b_j)| + |z_1 \cdot \log(c_1/|\sigma_1(a)|) + \cdots + \frac{1}{2} \cdot z_{r+s} \log((c_{r+s}/|\sigma_{r+s}(a)|)^2)| \\
&\le |f(b_j)| + \log(A) \cdot \left(\sum_{i=1}^{r} |z_i| + \frac{1}{2} \cdot \sum_{i=r+1}^{s} |z_i| \right).
\end{aligned}$$

The inequality of the lemma now follows. That B only depends on K and our choice of z follows from the formula for A and how we chose the b_i. □

The amazing thing about Lemma 12.2.1 is that the bound B on the right hand side does not depend on the c_i. Suppose we could somehow cleverly choose the positive real numbers c_i in such a way that

$$c_1 \cdots c_r \cdot (c_{r+1} \cdots c_{r+s})^2 = A \qquad \text{and} \qquad |s(c_1, \ldots, c_{r+s})| > B.$$

Then the facts that $|f(u) - s| \le B$ and $|s| > B$ would together imply that $|f(u)| > 0$ (since $f(u)$ is closer to s than s is to 0), which is exactly what we aimed to prove. We finish the proof by showing that it is possible to choose such c_i. Note that if we change the c_i, then a could change, hence the j such that a/b_j is a unit could change, but the b_j don't change, just the subscript j. Also note that if $r + s = 1$, then we are trying to prove that $\varphi(U_K)$ is a lattice in $\mathbf{R}^0 = \mathbf{R}^{r+s-1}$, which is automatically true, so we may assume that $r + s > 1$.

Lemma 12.2.2. *Assume $r + s > 1$. Then there is a choice of $c_1, \ldots, c_{r+s} \in \mathbf{R}_{>0}$ such that*

$$|z_1 \log(c_1) + \cdots + z_{r+s} \log(c_{r+s})| > B.$$

Proof. It is easier if we write

$$\begin{aligned}
&z_1 \log(c_1) + \cdots + z_{r+s} \log(c_{r+s}) = \\
&\qquad z_1 \log(c_1) + \cdots + z_r \log(c_r) + \frac{1}{2} \cdot z_{r+1} \log(c_{r+1}^2) + \cdots + \frac{1}{2} \cdot z_{r+s} \log(c_{r+s}^2) \\
&\qquad = w_1 \log(d_1) + \cdots + w_r \log(d_r) + w_{r+1} \log(d_{r+1}) + \cdots + \cdot w_{r+s} \log(d_{r+s}),
\end{aligned}$$

where $w_i = z_i$ and $d_i = c_i$ for $i \le r$, and $w_i = \frac{1}{2} z_i$ and $d_i = c_i^2$ for $r < i \le s$,

The condition that $z \notin H^{\perp}$ is that the w_i are not all the same, and in our new coordinates the lemma is equivalent to showing that $|\sum_{i=1}^{r+s} w_i \log(d_i)| > B$, subject to the condition that $\prod_{i=1}^{r+s} d_i = A$. Order the w_i so that $w_1 \ne 0$. By hypothesis there exists a w_j such that $w_j \ne w_1$, and again re-ordering we may assume that

$j = 2$. Set $d_3 = \cdots = d_{r+s} = 1$. Then $d_1 d_2 = A$ and $\log(1) = 0$, so

$$\begin{aligned}\left|\sum_{i=1}^{r+s} w_i \log(d_i)\right| &= |w_1 \log(d_1) + w_2 \log(d_2)| \\ &= |w_1 \log(d_1) + w_2 \log(A/d_1)| \\ &= |(w_1 - w_2)\log(d_1) + w_2 \log(A)|\end{aligned}$$

Since $w_1 \neq w_2$, we have $|(w_1 - w_2)\log(d_1) + w_2 \log(A)| \to \infty$ as $d_1 \to \infty$. □

12.3 Some Examples of Units in Number Fields

The classical Pell's equation is, given square-free $d > 0$, to find all positive integer solutions (x, y) to the equation $x^2 - dy^2 = 1$. Note that if $x + y\sqrt{d} \in \mathbf{Q}(\sqrt{d})$, then

$$\mathrm{Norm}(x + y\sqrt{d}) = (x + y\sqrt{d})(x - y\sqrt{d}) = x^2 - dy^2.$$

The solutions to Pell's equation thus form a finite-index subgroup of the group of units in the ring of integers of $\mathbf{Q}(\sqrt{d})$. Dirichlet's unit theorem implies that for any d the solutions to Pell's equation form an infinite cyclic group, a fact that takes substantial work to prove using only elementary number theory (for example, using continued fractions).

We first solve the Pell equation $x^2 - 5y^2 = 1$ by finding the units of a field using Magma (we will likely discuss algorithms for computing unit groups later in the course...).

```
> R<x> := PolynomialRing(RationalField());
> K<a> := NumberField(x^2-5);
> G, phi := UnitGroup(K);
> G;
Abelian Group isomorphic to Z/2 + Z
Defined on 2 generators
Relations:
    2*G.1 = 0
> K!phi(G.1);
-1
> u := K!phi(G.2); u;
1/2*(a + 1)
> u^2;
1/2*(a + 3)
> u^3;
a + 2
> Norm(u);
-1
> Norm(u^3);
```

```
-1
> Norm(u^6);
1
> fund := u^6;
> fund;
4*a + 9
> 9^2 - 5*4^2;
1
> fund^2;
72*a + 161
> fund^3;
1292*a + 2889
> fund^4;
23184*a + 51841
> fund^5;
416020*a + 930249
```

I think in practice for solving Pell's equation it's best to use the ideas in the paper [Len02]. A review of this paper says: "This wonderful article begins with history and some elementary facts and proceeds to greater and greater depth about the existence of solutions to Pell equations and then later the algorithmic issues of finding those solutions. The cattle problem is discussed, as are modern smooth number methods for solving Pell equations and the algorithmic issues of representing very large solutions in a reasonable way." You can get the paper freely online from the Notices web page.

The simplest solutions to Pell's equation can be huge, even when d is quite small. Read Lenstra's paper for some awesome examples from antiquity.

```
K<a> := NumberField(x^2-NextPrime(10^7));
> G, phi := UnitGroup(K);
> K!phi(G.2);
    163580259880346328225592238121094625499142677693142915506747253O\
    003400641003657678728904388162492712664239981750303094365756\
    106316392723776016806037958837914778176119741840754457028237\
    899759459100428895693238165048098039*a +
    517286692885814967470170672368346798303629034373575202975075\
    605058714958080893991274427903448098643836512878351227856269\
    086856679078304979321047765031073345259902622712059164969008\
    633603603640331175663456220418293622240930
```

The Magma `Signature` command returns the number of real and complex conjugate embeddings of K into $\mathbf{C}$. The command `UnitGroup`, which we used above, returns the unit group U_K as an abstract abelian group and a homomorphism $U_K \to \mathcal{O}_K$. Note that we have to bang (!) into K to get the units as elements of K.

First we consider $K = \mathbf{Q}(i)$.

```
> R<x> := PolynomialRing(RationalField());
> K<a> := NumberField(x^2+1);
> Signature(K);
0 1    // r=0, s=1
> G,phi := UnitGroup(K);
> G;
Abelian Group isomorphic to Z/4
Defined on 1 generator
Relations:
    4*G.1 = 0
> K!phi(G.1);
-a
```

Next we consider $K = \mathbf{Q}(\sqrt[3]{2})$.

```
> K<a> := NumberField(x^3-2);
> Signature(K);
1 1
> G,phi := UnitGroup(K);
> G;
Abelian Group isomorphic to Z/2 + Z
Defined on 2 generators
Relations:
    2*G.1 = 0
> K!phi(G.2);
-a + 1
```

The `Conjugates` command returns the sequence $(\sigma_1(x), \ldots, \sigma_{r+2s}(x))$ of all embeddings of $x \in K$ into $\mathbf{C}$. The `Logs` command returns the sequence

$$(\log(|\sigma_1(x)|), \ldots, \log(|\sigma_{r+s}(x)|)).$$

Continuing the above example, we have

```
> Conjugates(K!phi(G.2));
[ -0.2599210498948731647672106072782283505702514647009999999999995,
1.62996052494743658238360530363911417528512573235138439231O4 -
1.0911236359717214035600726141898088813258733387401854737O560*i,
1.62996052494743658238360530363911417528512573235138439231O4 +
1.0911236359717214035600726141898088813258733387401854737O560*i ]
> Logs(K!phi(G.2));   // image of infinite order unit -- generates a lattice
[ -1.3473773483293841009181878914456530462830622733209999999999989\
, 0.6736886741646920504590939457228265231415311366603288999999 ]
> Logs(K!phi(G.1));   // image of -1
[ 0.E-57, 0.E-57 ]
```

Let's try a field such that $r + s - 1 = 2$. First, one with $r = 0$ and $s = 3$:

```
> K<a> := NumberField(x^6+x+1);
> Signature(K);
0 3
> G, phi := UnitGroup(K);
> G;
Abelian Group isomorphic to Z/2 + Z + Z
Defined on 3 generators
Relations:
    2*G.1 = 0
> u1 := K!phi(G.2); u1;
a
> u2 := K!phi(G.3); u2;
-2*a^5 - a^3 + a^2 + a
> Logs(u1);
[ 0.11877157353322375762475480482285510811783185904379239999998,
0.04864390975267339963515094053332998614834212839311989999997,
-0.16741548328589715725990574535618509426617398743691229999999 ]
> Logs(u2);
[ 1.6502294567845884711894772749682228152154948421589999999997,
-2.0963853913452777953249166008337095194338210890229999999997,
0.4461559345606893241354393258654867042183262468643346999994 ]
```

Notice that the log image of u_1 is clearly not a real multiple of the log image of u_2 (e.g., the scalar would have to be positive because of the first coefficient, but negative because of the second). This illustrates the fact that the log images of u_1 and u_2 span a two-dimensional space.

Next we compute a field with $r = 3$ and $s = 0$. (A field with $s = 0$ is called "totally real".)

```
> K<a> := NumberField(x^3 + x^2 - 5*x - 1);
> Signature(K);
3 0
> G, phi := UnitGroup(K);
> G;
Abelian Group isomorphic to Z/2 + Z + Z
Defined on 3 generators
Relations:
    2*G.1 = 0
> u1 := K!phi(G.2); u1;
1/2*(a^2 + 2*a - 1)
> u2 := K!phi(G.3); u2;
a
> Logs(u1);
```

```
[ 1.1676157469275875715959825186368130294698776047489999999995,
-0.3928487245813982612917986258343595187584142264304436999996,
-0.77476702234618931030418389280245351071146337831817669999998 ]
> Logs(u2);
[ 0.6435429462288618773851817227686467257757954024463081999999,
-1.640224150322317146910150555170085057558346422666999999999,
0.9966812040934552695249688324014383317825510202205498999998 ]
```

A family of fields with $r = 0$ (totally complex) is the *cyclotomic fields* $\mathbf{Q}(\zeta_n)$. The degree of $\mathbf{Q}(\zeta_n)$ over $\mathbf{Q}$ is $\varphi(n)$ and $r = 0$, so $s = \varphi(n)/2$ (assuming $n > 2$).

```
> K := CyclotomicField(11); K;
Cyclotomic Field of order 11 and degree 10
> G, phi := UnitGroup(K);
> G;
Abelian Group isomorphic to Z/22 + Z + Z + Z + Z
Defined on 5 generators
Relations:
    22*G.1 = 0
> u := K!phi(G.2); u;
zeta_11^9 + zeta_11^8 + zeta_11^7 + zeta_11^6 + zeta_11^5 +
    zeta_11^3 + zeta_11^2 + zeta_11 + 1
> Logs(u);
[ -1.256566324178728487453222159299768039916630803888999999999969,
0.6517968940331400079717923884685099182823284402303273999999,
-0.1853300465598621409492216392019722155643154217181926999999,
0.5202849820300749393306985734118507551388955065272236999998,
0.26981449467537568109995283662137958205972227885009159999993 ]
> K!phi(G.3);
zeta_11^9 + zeta_11^7 + zeta_11^6 + zeta_11^5 + zeta_11^4 +
    zeta_11^3 + zeta_11^2 + zeta_11 + 1
> K!phi(G.4);
zeta_11^9 + zeta_11^8 + zeta_11^7 + zeta_11^6 + zeta_11^5 +
    zeta_11^4 + zeta_11^3 + zeta_11^2 + zeta_11
> K!phi(G.5);
zeta_11^9 + zeta_11^8 + zeta_11^7 + zeta_11^6 + zeta_11^5 +
    zeta_11^4 + zeta_11^2 + zeta_11 + 1
```

How far can we go computing unit groups of cyclotomic fields directly with Magma?

```
> time G,phi := UnitGroup(CyclotomicField(13));
Time: 2.210
> time G,phi := UnitGroup(CyclotomicField(17));
Time: 8.600
```

```
> time G,phi := UnitGroup(CyclotomicField(23));
.... I waited over 10 minutes (usage of 300MB RAM) and gave up.
```

12.4 Preview

In the next chapter we will study extra structure in the case when K is Galois over $\mathbf{Q}$; the results are nicely algebraic, beautiful, and have interesting ramifications. We'll learn about Frobenius elements, the Artin symbol, decomposition groups, and how the Galois group of K is related to Galois groups of residue class fields. These are the basic structures needed to make any sense of representations of Galois groups, which is at the heart of much of number theory.

Chapter 13

Decomposition and Inertia Groups

13.1 Galois Extensions

Suppose $K \subset \mathbf{C}$ is a number field. Then K is *Galois* if every field homomorphism $K \to \mathbf{C}$ has image K, or equivalently, $\#\operatorname{Aut}(K) = [K : \mathbf{Q}]$. More generally, we have the following definition.

Definition 13.1.1 (Galois). An extension K/L of number fields is *Galois* if $\#\operatorname{Aut}(K/L) = [K : L]$, where $\operatorname{Aut}(K/L)$ is the group of automorphisms of K that fix L. We write $\operatorname{Gal}(K/L) = \operatorname{Aut}(K/L)$.

For example, $\mathbf{Q}$ is Galois (over itself), any quadratic extension K/L is Galois, since it is of the form $L(\sqrt{a})$, for some $a \in L$, and the nontrivial embedding is induced by $\sqrt{a} \mapsto -\sqrt{a}$, so there is always one nontrivial automorphism. If $f \in L[x]$ is an irreducible cubic polynomial, and a is a root of f, then one proves in a course in Galois theory that $L(a)$ is Galois over L if and only if the discriminant of f is a perfect square in L. Random number fields of degree bigger than 2 are rarely Galois (I will not justify this claim further in this course).

If $K/\mathbf{Q}$ is a number field, then the Galois closure K^{gc} of K is the field generated by all images of K under all embeddings in $\mathbf{C}$ (more generally, if K/L is an extension, the Galois closure of K over L is the field generated by images of embeddings $K \to \mathbf{C}$ that are the identity map on L). If $K = \mathbf{Q}(a)$, then K^{gc} is generated by each of the conjugates of a, and is hence Galois over $\mathbf{Q}$, since the image under an embedding of any polynomial in the conjugates of a is again a polynomial in conjugates of a.

How much bigger can the degree of K^{gc} be as compared to the degree of $K = \mathbf{Q}(a)$? There is a natural embedding of $\operatorname{Gal}(K^{\mathrm{gc}}/\mathbf{Q})$ into the group of permutations of the conjugates of a. If there are n conjugates of a, then this is an embedding $\operatorname{Gal}(K^{\mathrm{gc}}/\mathbf{Q}) \hookrightarrow S_n$, where S_n is the symmetric group on n symbols, which has order $n!$. Thus the degree of the K^{gc} over $\mathbf{Q}$ is a divisor of $n!$. Also the Galois group is a transitive subgroup of S_n, which constrains the possibilities further. When

$n = 2$, we recover the fact that quadratic extensions are Galois. When $n = 3$, we see that the Galois closure of a cubic extension is either the cubic extension or a quadratic extension of the cubic extension. It turns out that that Galois closure of a cubic extension is obtained by adjoining the square root of the discriminant. For an extension K of degree 5, it is "frequently" the case that the Galois closure has degree 120, and in fact it is a difficult and interesting problem to find examples of degree 5 extension in which the Galois closure has degree smaller than 120 (according to MAGMA: the only possibilities for the order of a transitive proper subgroup of S_5 are 5, 10, 20, and 60; there are five transitive subgroups of S_5 out of the total of 19 subgroups of S_5).

Let n be a positive integer. Consider the field $K = \mathbf{Q}(\zeta_n)$, where $\zeta_n = e^{2\pi i/n}$ is a primitive nth root of unity. If $\sigma : K \to \mathbf{C}$ is an embedding, then $\sigma(\zeta_n)$ is also an nth root of unity, and the group of nth roots of unity is cyclic, so $\sigma(\zeta_n) = \zeta_n^m$ for some m which is invertible modulo n. Thus K is Galois and $\mathrm{Gal}(K/\mathbf{Q}) \hookrightarrow (\mathbf{Z}/n\mathbf{Z})^*$. However, $[K : \mathbf{Q}] = n$, so this map is an isomorphism. (Side note: Taking a p-adic limit and using the maps $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \to \mathrm{Gal}(\mathbf{Q}(\zeta_{p^r})/\mathbf{Q})$, we obtain a homomorphism $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \to \mathbf{Z}_p^*$, which is called the p-adic cyclotomic character.)

Compositums of Galois extensions are Galois. For example, the biquadratic field $K = \mathbf{Q}(\sqrt{5}, \sqrt{-1})$ is a Galois extension of $\mathbf{Q}$ of degree 4.

Fix a number field K that is Galois over a subfield L. Then the Galois group $G = \mathrm{Gal}(K/L)$ acts on many of the object that we have associated to K, including:

- the integers $\mathcal{O}_K$,
- the units U_K,
- the group of nonzero fractional ideals of $\mathcal{O}_K$,
- the class group $\mathrm{Cl}(K)$, and
- the set $S_\mathfrak{p}$ of prime ideals $\mathfrak{P}$ lying over a given prime $\mathfrak{p}$ of $\mathcal{O}_L$.

In the next section we will be concerned with the action of $\mathrm{Gal}(K/L)$ on $S_\mathfrak{p}$, though actions on each of the other objects, especially $\mathrm{Cl}(K)$, will be of further interest.

13.2 Decomposition of Primes

Fix a prime $\mathfrak{p} \subset \mathcal{O}_K$ and write $\mathfrak{p}\mathcal{O}_K = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_g^{e_g}$, so $S_\mathfrak{p} = \{\mathfrak{P}_1, \ldots, \mathfrak{P}_g\}$.

Definition 13.2.1 (Residue class degree). Suppose $\mathfrak{P}$ is a prime of $\mathcal{O}_K$ lying over $\mathfrak{p}$. Then the *residue class degree* of $\mathfrak{P}$ is

$$f_{\mathfrak{P}/\mathfrak{p}} = [\mathcal{O}_K/\mathfrak{P} : \mathcal{O}_L/\mathfrak{p}],$$

i.e., the degree of the extension of residue class fields.

If $M/K/L$ is a tower of field extensions and $\mathfrak{q}$ is a prime of M over $\mathfrak{P}$, then

$$f_{\mathfrak{q}/\mathfrak{p}} = [\mathcal{O}_M/\mathfrak{q} : \mathcal{O}_L/\mathfrak{p}] = [\mathcal{O}_M/\mathfrak{q} : \mathcal{O}_K/\mathfrak{P}] \cdot [\mathcal{O}_K/\mathfrak{P} : \mathcal{O}_L/\mathfrak{p}] = f_{\mathfrak{q}/\mathfrak{P}} \cdot f_{\mathfrak{P}/\mathfrak{p}},$$

so the residue class degree is multiplicative in towers.

Note that if $\sigma \in \mathrm{Gal}(K/L)$ and $\mathfrak{P} \in S_p$, then σ induces an isomorphism of finite fields $\mathcal{O}_K/\mathfrak{P} \to \mathcal{O}_K/\sigma(\mathfrak{P})$ that fixes the common subfield $\mathcal{O}_L/\mathfrak{p}$. Thus the residue class degrees of $\mathfrak{P}$ and $\sigma(\mathfrak{P})$ are the same. In fact, much more is true.

Theorem 13.2.2. *Suppose K/L is a Galois extension of number fields, and let $\mathfrak{p}$ be a prime of $\mathcal{O}_L$. Write $\mathfrak{p}\mathcal{O}_K = \prod_{i=1}^{g} \mathfrak{P}_i^{e_i}$, and let $f_i = f_{\mathfrak{P}_i/\mathfrak{p}}$. Then $G = \mathrm{Gal}(K/L)$ acts transitively on the set $S_\mathfrak{p}$ of primes $\mathfrak{P}_i$,*

$$e_1 = \cdots = e_g, \qquad f_1 = \cdots = f_g,$$

and $efg = [K : L]$, where e is the common value of the e_i and f is the common value of the f_i.

Proof. For simplicity, we will give the proof only in the case $L = \mathbf{Q}$, but the proof works in general. Suppose $p \in \mathbf{Z}$ and $p\mathcal{O}_K = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_g^{e_g}$, and $S = \{\mathfrak{p}_1, \ldots, \mathfrak{p}_g\}$. We will first prove that G acts transitively on S. Let $\mathfrak{p} = \mathfrak{p}_i$ for some i. Recall that we proved long ago, using the Chinese Remainder Theorem (Theorem 9.1.3) that there exists $a \in \mathfrak{p}$ such that $(a)/\mathfrak{p}$ is an integral ideal that is coprime to $p\mathcal{O}_K$. The product

$$I = \prod_{\sigma \in G} \sigma((a)/\mathfrak{p}) = \prod_{\sigma \in G} \frac{(\sigma(a))\mathcal{O}_K}{\sigma(\mathfrak{p})} = \frac{(\mathrm{Norm}_{K/\mathbf{Q}}(a))\mathcal{O}_K}{\prod_{\sigma \in G} \sigma(\mathfrak{p})} \tag{13.2.1}$$

is a nonzero integral $\mathcal{O}_K$ ideal since it is a product of nonzero integral $\mathcal{O}_K$ ideals. Since $a \in \mathfrak{p}$ we have that $\mathrm{Norm}_{K/\mathbf{Q}}(a) \in \mathfrak{p} \cap \mathbf{Z} = p\mathbf{Z}$. Thus the numerator of the rightmost expression in (13.2.1) is divisible by $p\mathcal{O}_K$. Also, because $(a)/\mathfrak{p}$ is coprime to $p\mathcal{O}_K$, each $\sigma((a)/\mathfrak{p})$ is coprime to $p\mathcal{O}_K$ as well. Thus I is coprime to $p\mathcal{O}_K$. Thus the denominator of the rightmost expression in (13.2.1) must also be divisibly by $p\mathcal{O}_K$ in order to cancel the $p\mathcal{O}_K$ in the numerator. Thus for any i we have

$$\prod_{j=1}^{g} \mathfrak{p}_j^{e_j} = p\mathcal{O}_K \;\Big|\; \prod_{\sigma \in G} \sigma(\mathfrak{p}_i),$$

which in particular implies that G acts transitively on the $\mathfrak{p}_i$.

Choose some j and suppose that $k \neq j$ is another index. Because G acts transitively, there exists $\sigma \in G$ such that $\sigma(\mathfrak{p}_k) = \mathfrak{p}_j$. Applying σ to the factorization $p\mathcal{O}_K = \prod_{i=1}^{g} \mathfrak{p}_i^{e_i}$, we see that

$$\prod_{i=1}^{g} \mathfrak{p}_i^{e_i} = \prod_{i=1}^{g} \sigma(\mathfrak{p}_i)^{e_i}.$$

Taking $\mathrm{ord}_{\mathfrak{p}_j}$ on both sides we get $e_j = e_k$. Thus $e_1 = e_2 = \cdots = e_g$.

As was mentioned right before the statement of the theorem, for any $\sigma \in G$ we have $\mathcal{O}_K/\mathfrak{p}_i \cong \mathcal{O}_K/\sigma(\mathfrak{p}_i)$, so by transitivity $f_1 = f_2 = \cdots = f_g$. Since $\mathcal{O}_K$ is a lattice in K, we have

$$\begin{aligned}[K : \mathbf{Q}] &= \dim_{\mathbf{Z}} \mathcal{O}_K = \dim_{\mathbf{F}_p} \mathcal{O}_K/p\mathcal{O}_K \\ &= \dim_{\mathbf{F}_p} \left(\bigoplus_{i=1}^{g} \mathcal{O}_K/\mathfrak{p}_i^{e_i} \right) = \sum_{i=1}^{g} e_i f_i = efg,\end{aligned}$$

which completes the proof. □

The rest of this section illustrates the theorem for quadratic fields and a cubic field and its Galois closure.

13.2.1 Quadratic Extensions

Suppose $K/\mathbf{Q}$ is a quadratic field. Then K is Galois, so for each prime $p \in \mathbf{Z}$ we have $2 = efg$. There are exactly three possibilties:

- **Ramified:** $e = 2$, $f = g = 1$: The prime p ramifies in $\mathcal{O}_K$, so $p\mathcal{O}_K = \mathfrak{p}^2$. There are only finitely many such primes, since if $f(x)$ is the minimal polynomial of a generator for $\mathcal{O}_K$, then p ramifies if and only if $f(x)$ has a multiple root modulo p. However, $f(x)$ has a multiple root modulo p if and only if p divides the discriminant of $f(x)$, which is nonzero because $f(x)$ is irreducible over $\mathbf{Z}$. (This argument shows there are only finitely many ramified primes in any number field. In fact, we will later show that the ramified primes are exactly the ones that divide the discriminant.)

- **Inert:** $e = 1$, $f = 2$, $g = 1$: The prime p is inert in $\mathcal{O}_K$, so $p\mathcal{O}_K = \mathfrak{p}$ is prime. This happens 50% of the time, which is suggested by quadratic reciprocity (but not proved this way), as we will see illustrated below for a particular example.

- **Split:** $e = f = 1$, $g = 2$: The prime p splits in $\mathcal{O}_K$, in the sense that $p\mathcal{O}_K = \mathfrak{p}_1\mathfrak{p}_2$ with $\mathfrak{p}_1 \neq \mathfrak{p}_2$. This happens the other 50% of the time.

Suppose, in particular, that $K = \mathbf{Q}(\sqrt{5})$, so $\mathcal{O}_K = \mathbf{Z}[\gamma]$, where $\gamma = (1+\sqrt{5})/2$. Then $p = 5$ is ramified, since $p\mathcal{O}_K = (\sqrt{5})^2$. More generally, the order $\mathbf{Z}[\sqrt{5}]$ has index 2 in $\mathcal{O}_K$, so for any prime $p \neq 2$ we can determine the factorization of p in $\mathcal{O}_K$ by finding the factorization of the polynomial $x^2 - 5 \in \mathbf{F}_p[x]$. The polynomial $x^2 - 5$ splits as a product of two distinct factors in $\mathbf{F}_p[x]$ if and only if $e = f = 1$ and $g = 2$. For $p \neq 2, 5$ this is the case if and only if 5 is a square in $\mathbf{F}_p$, i.e., if $\left(\frac{5}{p}\right) = 1$, where $\left(\frac{5}{p}\right)$ is $+1$ if 5 is a square mod p and -1 if 5 is not. By quadratic reciprocity,

$$\left(\frac{5}{p}\right) = (-1)^{\frac{5-1}{2}\cdot\frac{p-1}{2}} \cdot \left(\frac{p}{5}\right) = \left(\frac{p}{5}\right) = \begin{cases} +1 & \text{if } p \equiv \pm 1 \pmod{5} \\ -1 & \text{if } p \equiv \pm 2 \pmod{5}. \end{cases}$$

Thus whether p splits or is inert in $\mathcal{O}_K$ is determined by the residue class of p modulo 5.

13.2.2 The Cube Roots of Two

Suppose $K/\mathbf{Q}$ is not Galois. Then e_i, f_i, and g are defined for each prime $p \in \mathbf{Z}$, but we need not have $e_1 = \cdots = e_g$ or $f_1 = \cdots = f_g$. We do still have that $\sum_{i=1}^{g} e_i f_i = n$, by the Chinese Remainder Theorem.

For example, let $K = \mathbf{Q}(\sqrt[3]{2})$. We know that $\mathcal{O}_K = \mathbf{Z}[\sqrt[3]{2}]$. Thus $2\mathcal{O}_K = (\sqrt[3]{2})^3$, so for 2 we have $e = 3$ and $f = g = 1$. To factor $3\mathcal{O}_K$, we note that working modulo 3 we have

$$x^3 - 2 = (x-2)(x^2+2x+1) = (x-2)(x+1)^2 \in \mathbf{F}_3[x],$$

so

$$3\mathcal{O}_K = (3, \sqrt[3]{2} - 2) \cdot (3, \sqrt[3]{2} + 1)^2.$$

Thus $e_1 = 1$, $e_2 = 2$, $f_1 = f_2 = 1$, and $g = 2$. Next, working modulo 5 we have

$$x^3 - 2 = (x+2)(x^2+3x+4) \in \mathbf{F}_5[x],$$

and the quadratic factor is irreducible. Thus

$$5\mathcal{O}_K = (5, \sqrt[3]{2} + 2) \cdot (5, \sqrt[3]{2}^2 + 3\sqrt[3]{2} + 4).$$

Thus here $e_1 = e_2 = 1$, $f_1 = 1$, $f_2 = 2$, and $g = 2$.

Next we consider what happens in the Galois closure of K. Since the three embeddings of $\sqrt[3]{2}$ in $\mathbf{C}$ are $\sqrt[3]{2}$, $\zeta_3\sqrt[3]{2}$, and $\zeta_3^2\sqrt[3]{2}$, we have

$$M = K^{\mathrm{gc}} = \mathbf{Q}(\sqrt[3]{2}, \zeta_3) = K.L,$$

where $L = \mathbf{Q}(\zeta_3) = \mathbf{Q}(\sqrt{-3})$, since $\zeta_3 = (-1+\sqrt{-3})/2$ is a primitive cube root of unity. The notation $K.L$ means the "compositum of K and L", which is the smallest field generated by K and L.

Let's figure out e, f, and g for the prime $p = 3$ relative to the degree six Galois field $M/\mathbf{Q}$ by using Theorem 13.2.2 and what we can easily determine about K and L. First, we know that $efg = 6$. We have $3\mathcal{O}_K = \mathfrak{p}_1\mathfrak{p}_2^2$, so $3\mathcal{O}_M = \mathfrak{p}_1\mathcal{O}_M \cdot (\mathfrak{p}_2\mathcal{O}_M)^2$, and the prime factors of $\mathfrak{p}_1\mathcal{O}_M$ are disjoint from the prime factors of $\mathfrak{p}_2\mathcal{O}_M$. Thus $e > 1$ is even and also $g > 1$. The only possibility for e, f, g satisfying these two conditions is $e = 2$, $f = 1$, $g = 3$, so we conclude that $3\mathcal{O}_M = \mathfrak{q}_1^2\mathfrak{q}_2^2\mathfrak{q}_3^2$ without doing any further work, and without actually knowing the $\mathfrak{q}_i$ explicitly.

Here's another interesting deduction that we can make "by hand". Suppose for the moment that $\mathcal{O}_M = \mathbf{Z}[\sqrt[3]{2}, \zeta_3]$ (this will turn out to be false). Then the factorization of $(\sqrt{-3}) \subset \mathcal{O}_L$ in $\mathcal{O}_M$ would be exactly reflected by the factorization of $x^3 - 2$ in $\mathbf{F}_3 = \mathcal{O}_L/(\sqrt{-3})$. Modulo 3 we have $x^3 - 2 = x^3 + 1 = (x+1)^3$, which would imply that $(\sqrt{-3}) = \mathfrak{q}^3$ for some prime $\mathfrak{q}$ of $\mathcal{O}_M$, i.e., that $e = 6$ and $f = g = 1$, which is incorrect. Thus $\mathcal{O}_M \neq \mathbf{Z}[\sqrt[3]{2}, \zeta_3]$. Indeed, this conclusion agrees with the following Magma computation, which asserts that $[\mathcal{O}_M : \mathbf{Z}[\sqrt[3]{2}, \zeta_3]] = 24$:

```
> R<x> := PolynomialRing(RationalField());
> K := NumberField(x^3-2);
> L := NumberField(x^2+3);
> M := CompositeFields(K,L)[1];
> O_M := MaximalOrder(M);
> a := M!K.1;
> b := M!L.1;
> O := Order([a,b]);
> Index(O_M,O);
24
```

Chapter 14

Decomposition Groups and Galois Representations

14.1 The Decomposition Group

Suppose K is a number field that is Galois over $\mathbf{Q}$ with group $G = \mathrm{Gal}(K/\mathbf{Q})$. Fix a prime $\mathfrak{p} \subset \mathcal{O}_K$ lying over $p \in \mathbf{Z}$.

Definition 14.1.1 (Decomposition group). The *decomposition group* of $\mathfrak{p}$ is the subgroup

$$D_{\mathfrak{p}} = \{\sigma \in G : \sigma(\mathfrak{p}) = \mathfrak{p}\} \leq G.$$

(Note: The decomposition group is called the "splitting group" in Swinnerton-Dyer. Everybody I know calls it the decomposition group, so we will too.)

Let $\mathbf{F}_{\mathfrak{p}} = \mathcal{O}_K/\mathfrak{p}$ denote the residue class field of $\mathfrak{p}$. In this section we will prove that there is a natural exact sequence

$$1 \to I_{\mathfrak{p}} \to D_{\mathfrak{p}} \to \mathrm{Gal}(\mathbf{F}_{\mathfrak{p}}/\mathbf{F}_p) \to 1,$$

where $I_{\mathfrak{p}}$ is the *inertia subgroup* of $D_{\mathfrak{p}}$, and $\#I_{\mathfrak{p}} = e$. The most interesting part of the proof is showing that the natural map $D_{\mathfrak{p}} \to \mathrm{Gal}(\mathbf{F}_{\mathfrak{p}}/\mathbf{F}_p)$ is surjective.

We will also discuss the structure of $D_{\mathfrak{p}}$ and introduce Frobenius elements, which play a crucial roll in understanding Galois representations.

Recall that G acts on the set of primes $\mathfrak{p}$ lying over p. Thus the decomposition group is the stabilizer in G of $\mathfrak{p}$. The orbit-stabilizer theorem implies that $[G : D_{\mathfrak{p}}]$ equals the orbit of $\mathfrak{p}$, which by Theorem 13.2.2 equals the number g of primes lying over p, so $[G : D_{\mathfrak{p}}] = g$.

Lemma 14.1.2. *The decomposition subgroups $D_{\mathfrak{p}}$ corresponding to primes $\mathfrak{p}$ lying over a given p are all conjugate in G.*

Proof. We have $\tau(\sigma(\tau^{-1}(\mathfrak{p}))) = \mathfrak{p}$ if and only if $\sigma(\tau^{-1}(\mathfrak{p})) = \tau^{-1}\mathfrak{p}$. Thus $\tau\sigma\tau^{-1} \in D_p$ if and only if $\sigma \in D_{\tau^{-1}\mathfrak{p}}$, so $\tau^{-1}D_p\tau = D_{\tau^{-1}\mathfrak{p}}$. The lemma now follows because, by Theorem 13.2.2, G acts transitively on the set of $\mathfrak{p}$ lying over p. $\square$

The decomposition group is extremely useful because it allows us to see the extension $K/\mathbf{Q}$ as a tower of extensions, such that at each step in the tower we understand well the splitting behavior of the primes lying over p. Now might be a good time to glance ahead at Figure 14.1.2 on page 101.

We characterize the fixed field of $D = D_{\mathfrak{p}}$ as follows.

Proposition 14.1.3. *The fixed field K^D of D*

$$K^D = \{a \in K : \sigma(a) = a \text{ for all } \sigma \in D\}$$

is the smallest subfield $L \subset K$ such that $\mathfrak{p} \cap L$ does not split in K (i.e., $g(K/L) = 1$).

Proof. First suppose $L = K^D$, and note that by Galois theory $\mathrm{Gal}(K/L) \cong D$, and by Theorem 13.2.2, the group D acts transitively on the primes of K lying over $\mathfrak{p} \cap L$. One of these primes is $\mathfrak{p}$, and D fixes $\mathfrak{p}$ by definition, so there is only one prime of K lying over $\mathfrak{p} \cap L$, i.e., $\mathfrak{p} \cap L$ does not split in K. Conversely, if $L \subset K$ is such that $\mathfrak{p} \cap L$ does not split in K, then $\mathrm{Gal}(K/L)$ fixes $\mathfrak{p}$ (since it is the only prime over $\mathfrak{p} \cap L$), so $\mathrm{Gal}(K/L) \subset D$, hence $K^D \subset L$. □

Thus p does not split in going from K^D to K—it does some combination of ramifying and staying inert. To fill in more of the picture, the following proposition asserts that p splits completely and does not ramify in $K^D/\mathbf{Q}$.

Proposition 14.1.4. *Let $L = K^D$ for our fixed prime p and Galois extension $K/\mathbf{Q}$. Let $e = e(L/\mathbf{Q}), f = f(L/\mathbf{Q}), g = g(L/\mathbf{Q})$ be for $L/\mathbf{Q}$ and p. Then $e = f = 1$ and $g = [L : \mathbf{Q}]$, i.e., p does not ramify and splits completely in L. Also $f(K/\mathbf{Q}) = f(K/L)$ and $e(K/\mathbf{Q}) = e(K/L)$.*

Proof. As mentioned right after Definition 14.1.1, the orbit-stabilizer theorem implies that $g(K/\mathbf{Q}) = [G : D]$, and by Galois theory $[G : D] = [L : \mathbf{Q}]$. Thus

$$\begin{aligned} e(K/L) \cdot f(K/L) &= [K : L] = [K : \mathbf{Q}]/[L : \mathbf{Q}] \\ &= \frac{e(K/\mathbf{Q}) \cdot f(K/\mathbf{Q}) \cdot g(K/\mathbf{Q})}{[L : \mathbf{Q}]} = e(K/\mathbf{Q}) \cdot f(K/\mathbf{Q}). \end{aligned}$$

Now $e(K/L) \leq e(K/\mathbf{Q})$ and $f(K/L) \leq f(K/\mathbf{Q})$, so we must have $e(K/L) = e(K/\mathbf{Q})$ and $f(K/L) = f(K/\mathbf{Q})$. Since $e(K/\mathbf{Q}) = e(K/L) \cdot e(L/\mathbf{Q})$ and $f(K/\mathbf{Q}) = f(K/L) \cdot f(L/\mathbf{Q})$, the proposition follows. □

14.1.1 Galois groups of finite fields

Each $\sigma \in D = D_{\mathfrak{p}}$ acts in a well-defined way on the finite field $\mathbf{F}_{\mathfrak{p}} = \mathcal{O}_K/\mathfrak{p}$, so we obtain a homomorphism

$$\varphi : D_{\mathfrak{p}} \to \mathrm{Gal}(\mathbf{F}_{\mathfrak{p}}/\mathbf{F}_p).$$

We pause for a moment and derive a few basic properties of $\mathrm{Gal}(\mathbf{F}_{\mathfrak{p}}/\mathbf{F}_p)$, which are in fact general properties of Galois groups for finite fields. Let $f = [\mathbf{F}_{\mathfrak{p}} : \mathbf{F}_p]$.

The group $\mathrm{Aut}(\mathbf{F}_{\mathfrak{p}}/\mathbf{F}_p)$ contains the element Frob_p defined by

$$\mathrm{Frob}_p(x) = x^p,$$

because $(xy)^p = x^p y^p$ and

$$(x+y)^p = x^p + px^{p-1}y + \cdots + y^p \equiv x^p + y^p \pmod{p}.$$

By Exercise 29 (see Chapter 22), the group $\mathbf{F}_{\mathfrak{p}}^*$ is cyclic, so there is an element $a \in \mathbf{F}_{\mathfrak{p}}^*$ of order $p^f - 1$, and $\mathbf{F}_{\mathfrak{p}} = \mathbf{F}_p(a)$. Then $\mathrm{Frob}_p^n(a) = a^{p^n} = a$ if and only if $(p^f-1) \mid p^n - 1$ which is the case preciselywhen $f \mid n$, so the order of Frob_p is f. Since the order of the automorphism group of a field extension is at most the degree of the extension, we conclude that $\mathrm{Aut}(\mathbf{F}_{\mathfrak{p}}/\mathbf{F}_p)$ is generated by Frob_p. Also, since $\mathrm{Aut}(\mathbf{F}_{\mathfrak{p}}/\mathbf{F}_p)$ has order equal to the degree, we conclude that $\mathbf{F}_{\mathfrak{p}}/\mathbf{F}_p$ is Galois, with group $\mathrm{Gal}(\mathbf{F}_{\mathfrak{p}}/\mathbf{F}_p)$ cyclic of order f generated by Frob_p. (Anther general fact: Up to isomorphism there is exactly one finite field of each degree. Indeed, if there were two of degree f, then both could be characterized as the set of roots in the compositum of $x^{p^f} - 1$, hence they would be equal.)

14.1.2 The Exact Sequence

There is a natural reduction homomorphism

$$\varphi : D_{\mathfrak{p}} \to \mathrm{Gal}(\mathbf{F}_{\mathfrak{p}}/\mathbf{F}_p).$$

Theorem 14.1.5. *The homomorphism φ is surjective.*

Proof. Let $\tilde{a} \in \mathbf{F}_{\mathfrak{p}}$ be an element such that $\mathbf{F}_{\mathfrak{p}} = \mathbf{F}_p(a)$. Lift $\tilde{a}$ to an algebraic integer $a \in \mathcal{O}_K$, and let $f = \prod_{\sigma \in D_p}(x - \sigma(a)) \in K^D[x]$ be the characteristic polynomial of a over K^D. Using Proposition 14.1.4 we see that f reduces to the minimal polynomial $\tilde{f} = \prod(x - \widetilde{\sigma(a)}) \in \mathbf{F}_p[x]$ of $\tilde{a}$ (by the Proposition the coefficients of $\tilde{f}$ are in $\mathbf{F}_p$, and $\tilde{a}$ satisfies $\tilde{f}$, and the degree of $\tilde{f}$ equals the degree of the minimal polynomial of $\tilde{a}$). The roots of $\tilde{f}$ are of the form $\tilde{\sigma}(a)$, and the element $\mathrm{Frob}_p(a)$ is also a root of $\tilde{f}$, so it is of the form $\widetilde{\sigma(a)}$. We conclude that the generator Frob_p of $\mathrm{Gal}(\mathbf{F}_{\mathfrak{p}}/\mathbf{F}_p)$ is in the image of φ, which proves the theorem. □

Definition 14.1.6 (Inertia Group). The *inertia group* is the kernel $I_{\mathfrak{p}}$ of $D_{\mathfrak{p}} \to \mathrm{Gal}(\mathbf{F}_{\mathfrak{p}}/\mathbf{F}_p)$.

Combining everything so far, we find an exact sequence of groups

$$1 \to I_{\mathfrak{p}} \to D_{\mathfrak{p}} \to \mathrm{Gal}(\mathbf{F}_{\mathfrak{p}}/\mathbf{F}_p) \to 1. \tag{14.1.1}$$

The inertia group is a measure of how p ramifies in K.

Corollary 14.1.7. *We have $\#I_{\mathfrak{p}} = e(\mathfrak{p}/p)$, where $\mathfrak{p}$ is a prime of K over p.*

Proof. The sequence (14.1.1) implies that $\#I_{\mathfrak{p}} = \#D_{\mathfrak{p}}/f(K/\mathbf{Q})$. Applying Propositions 14.1.3–14.1.4, we have

$$\#D_{\mathfrak{p}} = [K : L] = \frac{[K : \mathbf{Q}]}{g} = \frac{efg}{g} = ef.$$

Dividing both sides by $f = f(K/\mathbf{Q})$ proves the corollary. $\square$

We have the following characterization of $I_{\mathfrak{p}}$.

Proposition 14.1.8. *Let $K/\mathbf{Q}$ be a Galois extension with group G, let $\mathfrak{p}$ be a prime lying over a prime p. Then*

$$I_{\mathfrak{p}} = \{\sigma \in G : \sigma(a) = a \pmod{\mathfrak{p}} \text{ for all } a \in \mathcal{O}_K\}.$$

Proof. By definition $I_{\mathfrak{p}} = \{\sigma \in D_{\mathfrak{p}} : \sigma(a) = a \pmod{\mathfrak{p}} \text{ for all } a \in \mathcal{O}_K\}$, so it suffices to show that if $\sigma \notin D_{\mathfrak{p}}$, then there exists $a \in \mathcal{O}_K$ such that $\sigma(a) = a \pmod{\mathfrak{p}}$. If $\sigma \notin D_{\mathfrak{p}}$, we have $\sigma^{-1}(\mathfrak{p}) \neq \mathfrak{p}$, so since both are maximal ideals, there exists $a \in \mathfrak{p}$ with $a \notin \sigma^{-1}(\mathfrak{p})$, i.e., $\sigma(a) \notin \mathfrak{p}$. Thus $\sigma(a) \not\equiv a \pmod{\mathfrak{p}}$. $\square$

Figure 14.1.2 is a picture of the splitting behavior of a prime $p \in \mathbf{Z}$.

14.2 Frobenius Elements

Suppose that $K/\mathbf{Q}$ is a finite Galois extension with group G and p is a prime such that $e = 1$ (i.e., an unramified prime). Then $I = I_{\mathfrak{p}} = 1$ for any $\mathfrak{p} \mid p$, so the map φ of Theorem 14.1.5 is a canonical isomorphism $D_{\mathfrak{p}} \cong \mathrm{Gal}(\mathbf{F}_{\mathfrak{p}}/\mathbf{F}_p)$. By Section 14.1.1, the group $\mathrm{Gal}(\mathbf{F}_{\mathfrak{p}}/\mathbf{F}_p)$ is cyclic with canonical generator Frob_p. The *Frobenius element* corresponding to $\mathfrak{p}$ is $\mathrm{Frob}_{\mathfrak{p}} \in D_{\mathfrak{p}}$. It is the unique element of G such that for all $a \in \mathcal{O}_K$ we have

$$\mathrm{Frob}_{\mathfrak{p}}(a) \equiv a^p \pmod{\mathfrak{p}}.$$

(To see this argue as in the proof of Proposition 14.1.8.) Just as the primes $\mathfrak{p}$ and decomposition groups D are all conjugate, the Frobenius elements over a given prime are conjugate.

Proposition 14.2.1. *For each $\sigma \in G$, we have*

$$\mathrm{Frob}_{\sigma\mathfrak{p}} = \sigma \, \mathrm{Frob}_{\mathfrak{p}} \, \sigma^{-1}.$$

In particular, the Frobenius elements lying over a given prime are all conjugate.

Proof. Fix $\sigma \in G$. For any $a \in \mathcal{O}_K$ we have $\mathrm{Frob}_{\mathfrak{p}}(\sigma^{-1}(a)) - \sigma^{-1}(a) \in \mathfrak{p}$. Multiply by σ we see that $\sigma \, \mathrm{Frob}_{\mathfrak{p}}(\sigma^{-1}(a)) - a \in \sigma\mathfrak{p}$, which proves the proposition. $\square$

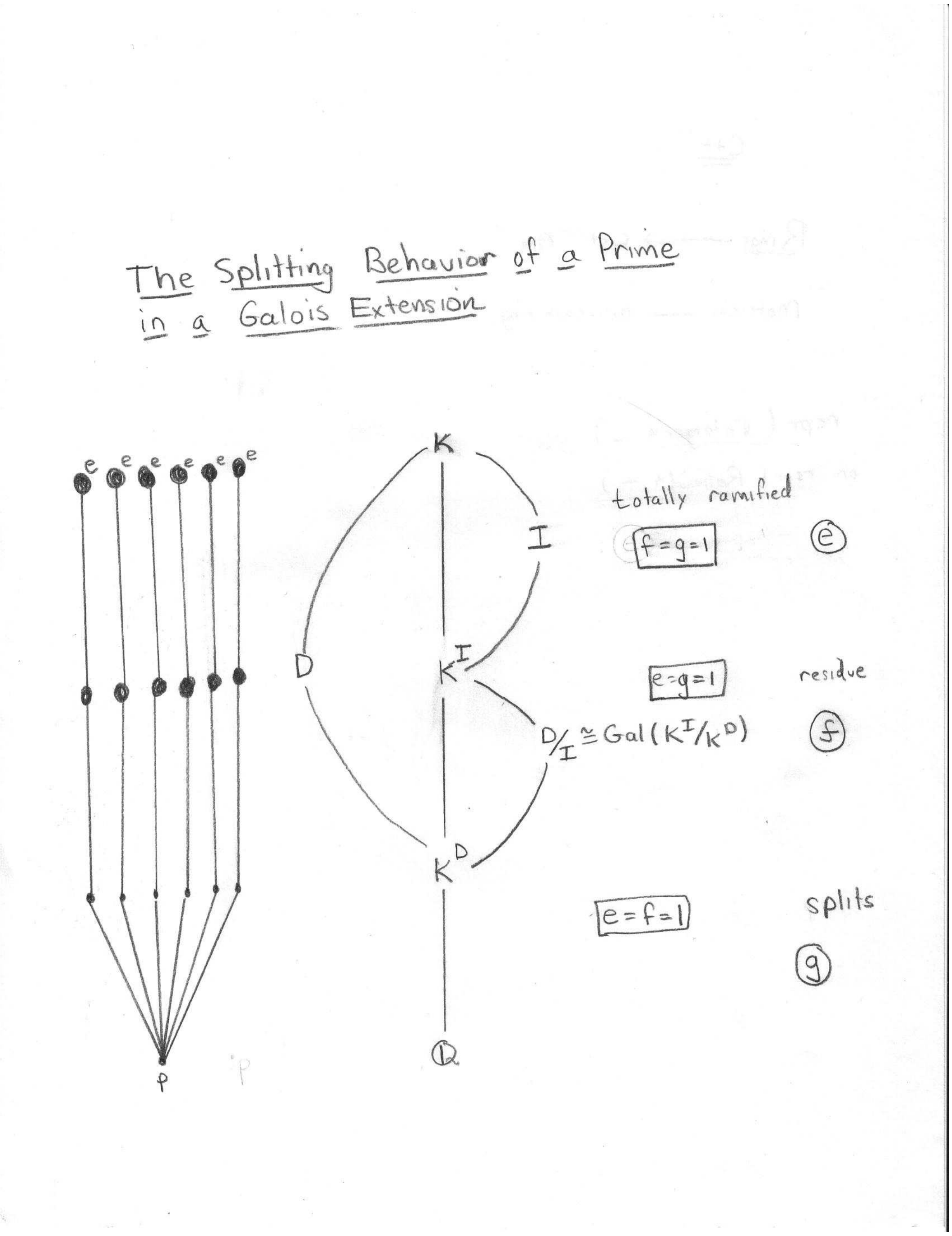


Figure 14.1.1: The Splitting of Behavior of a Prime in a Galois Extension

Thus the conjugacy class of $\mathrm{Frob}_{\mathfrak{p}}$ in G is a well defined function of p. For example, if G is abelian, then $\mathrm{Frob}_{\mathfrak{p}}$ does not depend on the choice of $\mathfrak{p}$ lying over p and we obtain a well defined symbol $\left(\frac{K/\mathbf{Q}}{p}\right) = \mathrm{Frob}_{\mathfrak{p}} \in G$ called the *Artin symbol*. It extends to a map from the free abelian group on unramified primes to the group G (the fractional ideals of $\mathbf{Z}$). Class field theory (for $\mathbf{Q}$) sets up a natural bijection between abelian Galois extensions of $\mathbf{Q}$ and certain maps from certain subgroups of the group of fractional ideals for $\mathbf{Z}$. We have just described one direction of this bijection, which associates to an abelian extension the Artin symbol (which induces a homomorphism). The Kronecker-Weber theorem asserts that the abelian extensions of $\mathbf{Q}$ are exactly the subfields of the fields $\mathbf{Q}(\zeta_n)$, as n varies over all positive integers. By Galois theory there is a correspondence between the subfields of $\mathbf{Q}(\zeta_n)$ (which has Galois group $(\mathbf{Z}/n\mathbf{Z})^*$) and the subgroups of $(\mathbf{Z}/n\mathbf{Z})^*$. Giving an abelian extension of $\mathbf{Q}$ is *exactly the same* as giving an integer n and a subgroup of $(\mathbf{Z}/n\mathbf{Z})^*$. Even more importantly, the reciprocity map $p \mapsto \left(\frac{Q(\zeta_n)/\mathbf{Q}}{p}\right)$ is simply $p \mapsto p \in (\mathbf{Z}/n\mathbf{Z})^*$. This is a nice generalization of quadratic reciprocity: for $\mathbf{Q}(\zeta_n)$, the efg for a prime p depends in a simple way on nothing but $p \mod n$.

14.3 Galois Representations and a Conjecture of Artin

The Galois group $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ is an object of central importance in number theory, and I've often heard that in some sense number theory is the study of this group. A good way to study a group is to study how it acts on various objects, that is, to study its representations.

Endow $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ with the topology which has as a basis of open neighborhoods of the origin the subgroups $\mathrm{Gal}(\overline{\mathbf{Q}}/K)$, where K varies over finite Galois extensions of $\mathbf{Q}$. (Note: This is **not** the topology got by taking as a basis of open neighborhoods the collection of finite-index normal subgroups of $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$.) Fix a positive integer n and let $\mathrm{GL}_n(\mathbf{C})$ be the group of $n \times n$ invertible matrices over $\mathbf{C}$ with the discrete topology.

Definition 14.3.1. A *complex n-dimensional representation* of $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ is a continuous homomorphism

$$\rho : \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \to \mathrm{GL}_n(\mathbf{C}).$$

For ρ to be continuous means that there is a finite Galois extension $K/\mathbf{Q}$ such that ρ factors through $\mathrm{Gal}(K/\mathbf{Q})$:

$$\begin{tikzcd}
\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \arrow[rr, "\rho"] \arrow[dr] & & \mathrm{GL}_n(\mathbf{C}) \\
& \mathrm{Gal}(K/\mathbf{Q}) \arrow[ur, "\rho'"'] &
\end{tikzcd}$$

For example, one could take K to be the fixed field of $\ker(\rho)$. (Note that continous implies that the image of ρ is finite, but using Zorn's lemma one can show that there are homomorphisms $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \to \{\pm 1\}$ with finite image that are not continuous, since they do not factor through the Galois group of any finite Galois extension.)

Fix a Galois representation ρ and a finite Galois extension K such that ρ factors through $\mathrm{Gal}(K/\mathbf{Q})$. For each prime $p \in \mathbf{Z}$ that is not ramified in K, there is an element $\mathrm{Frob}_{\mathfrak{p}} \in \mathrm{Gal}(K/\mathbf{Q})$ that is well-defined up to conjugation by elements of $\mathrm{Gal}(K/\mathbf{Q})$. This means that $\rho'(\mathrm{Frob}_p) \in \mathrm{GL}_n(\mathbf{C})$ is well-defined up to conjugation. Thus the characteristic polynomial $F_p \in \mathbf{C}[x]$ is a well-defined invariant of p and ρ. Let

$$R_p(x) = x^{\deg(F_p)} \cdot F_p(1/x) = 1 + \cdots + \mathrm{Det}(\mathrm{Frob}_p) \cdot x^{\deg(F_p)}$$

be the polynomial obtain by reversing the order of the coefficients of F_p. Following E. Artin, set

$$L(\rho, s) = \prod_{p \text{ unramified}} \frac{1}{R_p(p^{-s})}. \tag{14.3.1}$$

We view. $L(\rho, s)$ as a function of a single complex variable s. One can prove that $L(\rho, s)$ is holomorphic on some right half plane, and extends to a meromorphic function on all $\mathbf{C}$.

Conjecture 14.3.2 (Artin). *The L-series of any continuous representation*

$$\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \to \mathrm{GL}_n(\mathbf{C})$$

is an entire function on all $\mathbf{C}$, except possibly at 1.

This conjecture asserts that there is some way to analytically continue $L(\rho, s)$ to the whole complex plane, except possibly at 1. (A standard fact from complex analysis is that this analytic continuation must be unique.) The simple pole at $s = 1$ corresponds to the trivial representation (the Riemann zeta function), and if $n \geq 2$ and ρ is irreducible, then the conjecture is that ρ extends to a holomorphic function on all $\mathbf{C}$.

The conjecture follows from class field theory for $\mathbf{Q}$ when $n = 1$. When $n = 2$ and the image of ρ in $\mathrm{PGL}_2(\mathbf{C})$ is a solvable group, the conjecture is known, and is a deep theorem of Langlands and others (see [Lan80]), which played a crucial roll in Wiles's proof of Fermat's Last Theorem. When $n = 2$ and the projective image is not solvable, the only possibility is that the projective image is isomorphic to the alternating group A_5. Because A_5 is the symmetric group of the icosahedron, these representations are called *icosahedral*. In this case, Joe Buhler's Harvard Ph.D. thesis gave the first example, there is a whole book [Fre94], which proves Artin's conjecture for 7 icosahedral representation (none of which are twists of each other). Kevin Buzzard and I (Stein) proved the conjecture for 8 more examples. Subsequently, Richard Taylor, Kevin Buzzard, and Mark Dickinson proved the conjecture for an infinite class of icosahedral Galois representations (disjoint from the examples). The general problem for $n = 2$ is still open, but perhaps Taylor and others are still making progress toward it.

Part II

Adelic Viewpoint

Chapter 15

Valuations

The rest of this book is a partial rewrite of [Cas67] meant to make it more accessible. I have attempted to add examples and details of the implicit exercises and remarks that are left to the reader.

15.1 Valuations

Definition 15.1.1 (Valuation). A *valuation* $|\cdot|$ on a field K is a function defined on K with values in $\mathbf{R}_{\geq 0}$ satisfying the following axioms:

(1) $|a| = 0$ if and only if $a = 0$,

(2) $|ab| = |a|\,|b|$, and

(3) there is a constant $C \geq 1$ such that $|1 + a| \leq C$ whenever $|a| \leq 1$.

The *trivial valuation* is the valuation for which $|a| = 1$ for all $a \neq 0$. We will often tacitly exclude the trivial valuation from consideration.

From (2) we have

$$|1| = |1| \cdot |1|\,,$$

so $|1| = 1$ by (1). If $w \in K$ and $w^n = 1$, then $|w| = 1$ by (2). In particular, the only valuation of a finite field is the trivial one. The same argument shows that $|-1| = |1|$, so

$$|-a| = |a| \qquad \text{all } a \in K.$$

Definition 15.1.2 (Equivalent). Two valuations $|\cdot|_1$ and $|\cdot|_2$ on the same field are *equivalent* if there exists $c > 0$ such that

$$|a|_2 = |a|_1^c$$

for all $a \in K$.

Note that if $|\cdot|_1$ is a valuation, then $|\cdot|_2 = |\cdot|_1^c$ is also a valuation. Also, equivalence of valuations is an equivalence relation.

If $|\cdot|$ is a valuation and C is the constant from Axiom (3), then there is a $c > 0$ such that $C^c = 2$ (i.e., $c = \log(C)/\log(2)$). Then we can take 2 as constant for the equivalent valuation $|\cdot|^c$. Thus every valuation is equivalent to a valuation with $C = 2$. Note that if $C = 1$, e.g., if $|\cdot|$ is the trivial valuation, then we could simply take $C = 2$ in Axiom (3).

Proposition 15.1.3. *Suppose $|\cdot|$ is a valuation with $C = 2$. Then for all $a, b \in K$ we have*

$$|a + b| \leq |a| + |b| \qquad \textit{(triangle inequality).} \tag{15.1.1}$$

Proof. Suppose $a_1, a_2 \in K$ with $|a_1| \geq |a_2|$. Then $a = a_2/a_1$ satisfies $|a| \leq 1$. By Axiom (3) we have $|1 + a| \leq 2$, so multiplying by a_1 we see that

$$|a_1 + a_2| \leq 2|a_1| = 2 \cdot \max\{|a_1|, |a_2|\}.$$

Also we have

$$|a_1 + a_2 + a_3 + a_4| \leq 2 \cdot \max\{|a_1 + a_2|, |a_3 + a_4|\} \leq 4 \cdot \max\{|a_1|, |a_2|, |a_3|, |a_4|\},$$

and inductively we have for any $r > 0$ that

$$|a_1 + a_2 + \cdots + a_{2^r}| \leq 2^r \cdot \max |a_j|.$$

If n is any positive integer, let r be such that $2^{r-1} \leq n \leq 2^r$. Thenn

$$|a_1 + a_2 + \cdots + a_n| \leq 2^r \cdot \max\{|a_j|\} \leq 2n \cdot \max\{|a_j|\},$$

since $2^r \leq 2n$. In particular,

$$|n| \leq 2n \cdot |1| = 2n \qquad \text{(for } n > 0\text{).} \tag{15.1.2}$$

Applying (15.1.2) to $\left|\binom{n}{j}\right|$ and using the binomial expansion, we have for any $a, b \in K$ that

$$\begin{aligned}
|a + b|^n &= \left|\sum_{j=0}^{n} \binom{n}{j} a^j b^{n-j}\right| \\
&\leq 2(n+1) \max_j \left\{ \left|\binom{n}{j}\right| |a|^j \, |b|^{n-j} \right\} \\
&\leq 2(n+1) \max_j \left\{ 2\binom{n}{j} |a|^j \, |b|^{n-j} \right\} \\
&\leq 4(n+1) \max_j \left\{ \binom{n}{j} |a|^j \, |b|^{n-j} \right\} \\
&\leq 4(n+1)(|a| + |b|)^n.
\end{aligned}$$

Now take nth roots of both sides to obtain

$$|a+b| \leq \sqrt[n]{4(n+1)} \cdot (|a|+|b|).$$

We have by elementary calculus that

$$\lim_{n\to\infty} \sqrt[n]{4(n+1)} = 1,$$

so $|a+b| \leq |a|+|b|$. (The "elementary calculus": We instead prove that $\sqrt[n]{n} \to 1$, since the argument is the same and the notation is simpler. First, for any $n \geq 1$ we have $\sqrt[n]{n} \geq 1$, since upon taking nth powers this is equivalent to $n \geq 1^n$, which is true by hypothesis. Second, suppose there is an $\varepsilon > 0$ such that $\sqrt[n]{n} \geq 1+\varepsilon$ for all $n \geq 1$. Then taking logs of boths sides we see that $\frac{1}{n}\log(n) \geq \log(1+\varepsilon) > 0$. But $\log(n)/n \to 0$, so there is no such ε. Thus $\sqrt[n]{n} \to 1$ as $n \to \infty$.) □

Note that Axioms (1), (2) and Equation (15.1.1) imply Axiom (3) with $C = 2$. We take Axiom (3) instead of Equation (15.1.1) for the technical reason that we will want to call the square of the absolute value of the complex numbers a valuation.

Lemma 15.1.4. *Suppose $a, b \in K$, and $|\cdot|$ is a valuation on K with $C \leq 2$. Then*

$$\Big||a|-|b|\Big| \leq |a-b|\,.$$

(Here the big absolute value on the outside of the left-hand side of the inequality is the usual absolute value on real numbers, but the other absolute values are a valuation on an arbitrary field K.)

Proof. We have

$$|a| = |b+(a-b)| \leq |b|+|a-b|,$$

so $|a|-|b| \leq |a-b|$. The same argument with a and b swapped implies that $|b|-|a| \leq |a-b|$, which proves the lemma. □

15.2 Types of Valuations

We define two important properties of valuations, both of which apply to equivalence classes of valuations (i.e., the property holds for $|\cdot|$ if and only if it holds for a valuation equivalent to $|\cdot|$).

Definition 15.2.1 (Discrete). A valuation $|\cdot|$ is *discrete* if there is a $\delta > 0$ such that for any $a \in K$

$$1-\delta < |a| < 1+\delta \implies |a| = 1.$$

Thus the absolute values are bounded away from 1.

To say that $|\cdot|$ is discrete is the same as saying that the set

$$G = \{\log |a| : a \in K, a \neq 0\} \subset \mathbf{R}$$

forms a discrete subgroup of the reals under addition (because the elements of the group G are bounded away from 0).

Proposition 15.2.2. *A nonzero discrete subgroup G of $\mathbf{R}$ is free on one generator.*

Proof. Since G is discrete there is a positive $m \in G$ such that for any positive $x \in G$ we have $m \leq x$. Suppose $x \in G$ is an arbitrary positive element. By subtracting off integer multiples of m, we find that there is a unique n such that

$$0 \leq x - nm < m.$$

Since $x - nm \in G$ and $0 < x - nm < m$, it follows that $x - nm = 0$, so x is a multiple of m. $\square$

By Proposition 15.2.2, the set of $\log |a|$ for nonzero $a \in K$ is free on one generator, so there is a $c < 1$ such that $|a|$, for $a \neq 0$, runs precisely through the set

$$c^{\mathbf{Z}} = \{c^m : m \in \mathbf{Z}\}$$

(Note: we can replace c by c^{-1} to see that we can assume that $c < 1$).

Definition 15.2.3 (Order). If $|a| = c^m$, we call $m = \operatorname{ord}(a)$ the *order* of a.

Axiom (2) of valuations translates into

$$\operatorname{ord}(ab) = \operatorname{ord}(a) + \operatorname{ord}(b).$$

Definition 15.2.4 (Non-archimedean). A valuation $|\cdot|$ is *non-archimedean* if we can take $C = 1$ in Axiom (3), i.e., if

$$|a + b| \leq \max\{|a|, |b|\}. \tag{15.2.1}$$

If $|\cdot|$ is not non-archimedean then it is *archimedean.*

Note that if we can take $C = 1$ for $|\cdot|$ then we can take $C = 1$ for any valuation equivalent to $|\cdot|$. To see that (15.2.1) is equivalent to Axiom (3) with $C = 1$, suppose $|b| \leq |a|$. Then $|b/a| \leq 1$, so Axiom (3) asserts that $|1 + b/a| \leq 1$, which implies that $|a + b| \leq |a| = \max\{|a|, |b|\}$, and conversely.

We note at once the following consequence:

Lemma 15.2.5. *Suppose $|\cdot|$ is a non-archimedean valuation. If $a, b \in K$ with $|b| < |a|$, then $|a + b| = |a|$.*

Proof. Note that $|a+b| \leq \max\{|a|, |b|\} = |a|$, which is true even if $|b| = |a|$. Also,

$$|a| = |(a+b) - b| \leq \max\{|a+b|, |b|\} = |a+b|,$$

where for the last equality we have used that $|b| < |a|$ (if $\max\{|a+b|, |b|\} = |b|$, then $|a| \leq |b|$, a contradiction). □

Definition 15.2.6 (Ring of Integers). Suppose $|\cdot|$ is a non-archimedean absolute value on a field K. Then

$$\mathcal{O} = \{a \in K : |a| \leq 1\}$$

is a ring called the *ring of integers* of K with respect to $|\cdot|$.

Lemma 15.2.7. *Two non-archimedean valuations $|\cdot|_1$ and $|\cdot|_2$ are equivalent if and only if they give the same $\mathcal{O}$.*

We will prove this modulo the claim (to be proved later in Section 16.1) that valuations are equivalent if (and only if) they induce the same topology.

Proof. Suppose suppose $|\cdot|_1$ is equivalent to $|\cdot|_2$, so $|\cdot|_1 = |\cdot|_2^c$, for some $c > 0$. Then $|c|_1 \leq 1$ if and only if $|c|_2^c \leq 1$, i.e., if $|c|_2 \leq 1^{1/c} = 1$. Thus $\mathcal{O}_1 = \mathcal{O}_2$.

Conversely, suppose $\mathcal{O}_1 = \mathcal{O}_2$. Then $|a|_1 < |b|_1$ if and only if $a/b \in \mathcal{O}_1$ and $b/a \notin \mathcal{O}_1$, so

$$|a|_1 < |b|_1 \iff |a|_2 < |b|_2. \tag{15.2.2}$$

The topology induced by $|\ |_1$ has as basis of open neighborhoods the set of open balls

$$B_1(z, r) = \{x \in K : |x - z|_1 < r\},$$

for $r > 0$, and likewise for $|\ |_2$. Since the absolute values $|b|_1$ get arbitrarily close to 0, the set $\mathcal{U}$ of open balls $B_1(z, |b|_1)$ also forms a basis of the topology induced by $|\ |_1$ (and similarly for $|\ |_2$). By (15.2.2) we have

$$B_1(z, |b|_1) = B_2(z, |b|_2),$$

so the two topologies both have $\mathcal{U}$ as a basis, hence are equal. That equal topologies imply equivalence of the corresponding valuations will be proved in Section 16.1. □

The set of $a \in \mathcal{O}$ with $|a| < 1$ forms an ideal $\mathfrak{p}$ in $\mathcal{O}$. The ideal $\mathfrak{p}$ is maximal, since if $a \in \mathcal{O}$ and $a \notin \mathfrak{p}$ then $|a| = 1$, so $|1/a| = 1/|a| = 1$, hence $1/a \in \mathcal{O}$, so a is a unit.

Lemma 15.2.8. *A non-archimedean valuation $|\cdot|$ is discrete if and only if $\mathfrak{p}$ is a principal ideal.*

Proof. First suppose that $|\cdot|$ is discrete. Choose $\pi \in \mathfrak{p}$ with $|\pi|$ maximal, which we can do since

$$S = \{\log|a| : a \in \mathfrak{p}\} \subset (-\infty, 1],$$

so the discrete set S is bounded above. Suppose $a \in \mathfrak{p}$. Then

$$\left|\frac{a}{\pi}\right| = \frac{|a|}{|\pi|} \leq 1,$$

so $a/\pi \in \mathcal{O}$. Thus

$$a = \pi \cdot \frac{a}{\pi} \in \pi\mathcal{O}.$$

Conversely, suppose $\mathfrak{p} = (\pi)$ is principal. For any $a \in \mathfrak{p}$ we have $a = \pi b$ with $b \in \mathcal{O}$. Thus

$$|a| = |\pi| \cdot |b| \leq |\pi| < 1.$$

Thus $\{|a| : |a| < 1\}$ is bounded away from 1, which is exactly the definition of discrete. $\square$

Example 15.2.9. For any prime p, define the p-adic valuation $|\cdot|_p : \mathbf{Q} \to \mathbf{R}$ as follows. Write a nonzero $\alpha \in K$ as $p^n \cdot \frac{a}{b}$, where $\gcd(a,p) = \gcd(b,p) = 1$. Then

$$\left|p^n \cdot \frac{a}{b}\right|_p := p^{-n} = \left(\frac{1}{p}\right)^n.$$

This valuation is both discrete and non-archimedean. The ring $\mathcal{O}$ is the local ring

$$\mathbf{Z}_{(p)} = \left\{\frac{a}{b} \in \mathbf{Q} : p \nmid b\right\},$$

which has maximal ideal generated by p. Note that $\mathrm{ord}(p^n \cdot \frac{a}{b}) = p^n$.

We will using the following lemma later (e.g., in the proof of Corollary 16.2.4 and Theorem 15.3.2).

Lemma 15.2.10. *A valuation $|\cdot|$ is non-archimedean if and only if $|n| \leq 1$ for all n in the ring generated by 1 in K.*

Note that we cannot identify the ring generated by 1 with $\mathbf{Z}$ in general, because K might have characteristic $p > 0$.

Proof. If $|\cdot|$ is non-archimedean, then $|1| \leq 1$, so by Axiom (3) with $a = 1$, we have $|1 + 1| \leq 1$. By induction it follows that $|n| \leq 1$.

Conversely, suppose $|n| \leq 1$ for all integer multiples n of 1. This condition is also true if we replace $|\cdot|$ by any equivalent valuation, so replace $|\cdot|$ by one with $C \leq 2$, so that the triangle inequality holds. Suppose $a \in K$ with $|a| \leq 1$. Then by the triangle inequality,

$$\begin{aligned}|1+a|^n &= |(1+a)^n| \\ &\leq \sum_{j=0}^{n} \left|\binom{n}{j}\right| |a| \\ &\leq 1 + 1 + \cdots + 1 = n.\end{aligned}$$

Now take nth roots of both sides to get

$$|1+a| \leq \sqrt[n]{n},$$

and take the limit as $n \to \infty$ to see that $|1+a| \leq 1$. This proves that one can take $C = 1$ in Axiom (3), hence that $|\cdot|$ is non-archimedean. $\square$

15.3 Examples of Valuations

The archetypal example of an archimedean valuation is the absolute value on the complex numbers. It is essentially the only one:

Theorem 15.3.1 (Gelfand-Tornheim). *Any field K with an archimedean valuation is isomorphic to a subfield of $\mathbf{C}$, the valuation being equivalent to that induced by the usual absolute value on $\mathbf{C}$.*

We do not prove this here as we do not need it. For a proof, see [Art59, pg. 45, 67].

There are many non-archimedean valuations. On the rationals $\mathbf{Q}$ there is one for every prime $p > 0$, the p-adic valuation, as in Example 15.2.9.

Theorem 15.3.2 (Ostrowski). *The nontrivial valuations on $\mathbf{Q}$ are those equivalent to $|\cdot|_p$, for some prime p, and the usual absolute value $|\cdot|_\infty$.*

Remark 15.3.3. Before giving the proof, we pause with a brief remark about Ostrowski. According to

`http://www-gap.dcs.st-and.ac.uk/~history/Mathematicians/Ostrowski.html`

Ostrowski was a Ukrainian mathematician who lived 1893–1986. Gautschi writes about Ostrowski as follows: "... you are able, on the one hand, to emphasise the abstract and axiomatic side of mathematics, as for example in your theory of general norms, or, on the other hand, to concentrate on the concrete and constructive aspects of mathematics, as in your study of numerical methods, and to do both with equal ease. *You delight in finding short and succinct proofs, of which you have given many examples* ..." [italics mine]

We will now give an example of one of these short and succinct proofs.

Proof. Suppose $|\cdot|$ is a nontrivial valuation on $\mathbf{Q}$.

Nonarchimedean case: Suppose $|c| \leq 1$ for all $c \in \mathbf{Z}$, so by Lemma 15.2.10, $|\cdot|$ is nonarchimedean. Since $|\cdot|$ is nontrivial, the set

$$\mathfrak{p} = \{a \in \mathbf{Z} : |a| < 1\}$$

is nonzero. Also $\mathfrak{p}$ is an ideal and if $|ab| < 1$, then $|a|\,|b| = |ab| < 1$, so $|a| < 1$ or $|b| < 1$, so $\mathfrak{p}$ is a prime ideal of $\mathbf{Z}$. Thus $\mathfrak{p} = p\mathbf{Z}$, for some prime number p. Since every element of $\mathbf{Z}$ has valuation at most 1, if $u \in \mathbf{Z}$ with $\gcd(u, p) = 1$, then $u \notin \mathfrak{p}$, so $|u| = 1$. Let $\alpha = \log_{|p|} \frac{1}{p}$, so $|p|^\alpha = \frac{1}{p}$. Then for any r and any $u \in \mathbf{Z}$ with $\gcd(u,p) = 1$, we have

$$|up^r|^\alpha = |u|^\alpha\,|p|^{\alpha r} = |p|^{\alpha r} = p^{-r} = |up^r|_p\,.$$

Thus $|\cdot|^\alpha = |\cdot|_p$ on $\mathbf{Z}$, hence on $\mathbf{Q}$ by multiplicativity, so $|\cdot|$ is equivalent to $|\cdot|_p$, as claimed.

Archimedean case: By replacing $|\cdot|$ by a power of $|\cdot|$, we may assume without loss that $|\cdot|$ satisfies the triangle inequality. We first make some general remarks about any valuation that satisfies the triangle inequality. Suppose $a \in \mathbf{Z}$ is greater than 1. Consider, for any $b \in \mathbf{Z}$ the base-a expansion of b:

$$b = b_m a^m + b_{m-1}a^{m-1} + \cdots + b_0,$$

where

$$0 \le b_j < a \qquad (0 \le j \le m),$$

and $b_m \neq 0$. Since $a^m \le b$, taking logs we see that $m\log(a) \le \log(b)$, so

$$m \le \frac{\log(b)}{\log(a)}.$$

Let $M = \max_{1\le d<a} |d|$. Then by the triangle inequality for $|\cdot|$, we have

$$\begin{aligned}
|b| &\le |b_m|\,a^m + \cdots + |b_1|\,|a| + |b_0| \\
&\le M\cdot(|a|^m + \cdots + |a| + 1) \\
&\le M\cdot(m+1)\cdot\max(1,|a|^m) \\
&\le M\cdot\left(\frac{\log(b)}{\log(a)} + 1\right)\cdot\max\left(1, |a|^{\log(b)/\log(a)}\right),
\end{aligned}$$

where in the last step we use that $m \le \frac{\log(b)}{\log(a)}$. Setting $b = c^n$, for $c \in \mathbf{Z}$, in the above inequality and taking nth roots, we have

$$\begin{aligned}
|c| &\le \left(M\cdot\left(\frac{\log(c^n)}{\log(a)} + 1\right)\cdot\max(1,|a|^{log(c^n)/\log(a)})\right)^{1/n} \\
&= M^{1/n}\cdot\left(\frac{\log(c^n)}{\log(a)} + 1\right)^{1/n}\cdot\max\left(1,|a|^{\log(c^n)/\log(a)}\right)^{1/n}.
\end{aligned}$$

The first factor $M^{1/n}$ converges to 1 as $n \to \infty$, since $M \ge 1$ (because $|1| = 1$). The second factor is

$$\left(\frac{\log(c^n)}{\log(a)} + 1\right)^{1/n} = \left(n\cdot\frac{\log(c)}{\log(a)} + 1\right)^{1/n}$$

which also converges to 1, for the same reason that $n^{1/n} \to 1$ (because $\log(n^{1/n}) = \frac{1}{n}\log(n) \to 0$ as $n \to \infty$). The third factor is

$$\max\left(1,|a|^{\log(c^n)/\log(a)}\right)^{1/n} = \begin{cases} 1 & \text{if } |a| < 1, \\ |a|^{\log(c)/\log(a)} & \text{if } |a| \ge 1. \end{cases}$$

Putting this all together, we see that

$$|c| \le \max\left(1, |a|^{\frac{\log(c)}{\log(a)}}\right).$$

Our assumption that $|\cdot|$ is nonarchimedean implies that there is $c \in \mathbf{Z}$ with $c > 1$ and $|c| > 1$. Then for all $a \in \mathbf{Z}$ with $a > 1$ we have

$$1 < |c| \le \max\left(1, |a|^{\frac{\log(c)}{\log(a)}}\right), \tag{15.3.1}$$

so $1 < |a|^{\log(c)/\log(a)}$, so $1 < |a|$ as well (i.e., any $a \in \mathbf{Z}$ with $a > 1$ automatically satisfies $|a| > 1$). Also, taking the $1/\log(c)$ power on both sides of (15.3.1) we see that

$$|c|^{\frac{1}{\log(c)}} \le |a|^{\frac{1}{\log(a)}}. \tag{15.3.2}$$

Because, as mentioned above, $|a| > 1$, we can interchange the roll of a and c to obtain the reverse inequality of (15.3.2). We thus have

$$|c| = |a|^{\frac{\log(c)}{\log(a)}}.$$

Letting $\alpha = \log(2) \cdot \log_{|2|}(e)$ and setting $a = 2$, we have

$$|c|^{\alpha} = |2|^{\frac{\alpha}{\log(2)} \cdot \log(c)} = \left(|2|^{\log_{|2|}(e)}\right)^{\log(c)} = e^{\log(c)} = c = |c|_{\infty}.$$

Thus for all integers $c \in \mathbf{Z}$ with $c > 1$ we have $|c|^{\alpha} = |c|_{\infty}$, which implies that $|\cdot|$ is equivalent to $|\cdot|_{\infty}$. $\square$

Let k be any field and let $K = k(t)$, where t is transcendental. Fix a real number $c > 1$. If $p = p(t)$ is an irreducible polynomial in the ring $k[t]$, we define a valuation by

$$\left|p^a \cdot \frac{u}{v}\right|_p = c^{-\deg(p)\cdot a}, \tag{15.3.3}$$

where $a \in \mathbf{Z}$ and $u, v \in k[t]$ with $p \nmid u$ and $p \nmid v$.

Remark 15.3.4. This definition differs from the one page 46 of [Cassels-Frohlich, Ch. 2] in two ways. First, we assume that $c > 1$ instead of $c < 1$, since otherwise $|\cdot|_p$ does not satisfy Axiom 3 of a valuation. Also, we write $c^{-\deg(p)\cdot a}$ instead of c^{-a}, so that the product formula will hold. (For more about the product formula, see Section 20.1.)

In addition there is a a non-archimedean valuation $|\cdot|_{\infty}$ defined by

$$\left|\frac{u}{v}\right|_{\infty} = c^{\deg(u) - \deg(v)}. \tag{15.3.4}$$

This definition differs from the one in [Cas67, pg. 46] in two ways. First, we assume that $c > 1$ instead of $c < 1$, since otherwise $|\cdot|_p$ does not satisfy Axiom 3 of a valuation. Here's why: Recall that Axiom 3 for a non-archimedean valuation on K asserts that whenever $a \in K$ and $|a| \leq 1$, then $|a+1| \leq 1$. Set $a = p - 1$, where $p = p(t) \in K[t]$ is an irreducible polynomial. Then $|a| = c^0 = 1$, since $\mathrm{ord}_p(p-1) = 0$. However, $|a+1| = |p-1+1| = |p| = c^1 < 1$, since $\mathrm{ord}_p(p) = 1$. If we take $c > 1$ instead of $c < 1$, as I propose, then $|p| = c^1 > 1$, as required.

Note the (albeit imperfect) analogy between $K = k(t)$ and $\mathbf{Q}$. If $s = t^{-1}$, so $k(t) = k(s)$, the valuation $|\cdot|_\infty$ is of the type (15.3.3) belonging to the irreducible polynomial $p(s) = s$.

The reader is urged to prove the following lemma as a homework problem.

Lemma 15.3.5. *The only nontrivial valuations on $k(t)$ which are trivial on k are equivalent to the valuation (15.3.3) or (15.3.4).*

For example, if k is a finite field, there are no nontrivial valuations on k, so the only nontrivial valuations on $k(t)$ are equivalent to (15.3.3) or (15.3.4).

Chapter 16

Topology and Completeness

16.1 Topology

A valuation $|\cdot|$ on a field K induces a topology in which a basis for the neighborhoods of a are the *open balls*

$$B(a, d) = \{x \in K : |x - a| < d\}$$

for $d > 0$.

Lemma 16.1.1. *Equivalent valuations induce the same topology.*

Proof. If $|\cdot|_1 = |\cdot|_2^r$, then $|x - a|_1 < d$ if and only if $|x - a|_2^r < d$ if and only if $|x - a|_2 < d^{1/r}$ so $B_1(a, d) = B_2(a, d^{1/r})$. Thus the basis of open neighborhoods of a for $|\cdot|_1$ and $|\cdot|_2$ are identical. $\square$

A valuation satisfying the triangle inequality gives a metric for the topology on defining the distance from a to b to be $|a - b|$. Assume for the rest of this section that we only consider valuations that satisfy the triangle inequality.

Lemma 16.1.2. *A field with the topology induced by a valuation is a* topological field*, i.e., the operations sum, product, and reciprocal are continuous.*

Proof. For example (product) the triangle inequality implies that

$$|(a + \varepsilon)(b + \delta) - ab| \leq |\varepsilon|\,|\delta| + |a|\,|\delta| + |b|\,|\varepsilon|$$

is small when $|\varepsilon|$ and $|\delta|$ are small (for fixed a, b). $\square$

Lemma 16.1.3. *Suppose two valuations $|\cdot|_1$ and $|\cdot|_2$ on the same field K induce the same topology. Then for any sequence $\{x_n\}$ in K we have*

$$|x_n|_1 \to 0 \iff |x_n|_2 \to 0.$$

Proof. It suffices to prove that if $|x_n|_1 \to 0$ then $|x_n|_2 \to 0$, since the proof of the other implication is the same. Let $\varepsilon > 0$. The topologies induced by the two absolute values are the same, so $B_2(0, \varepsilon)$ can be covered by open balls $B_1(a_i, r_i)$. One of these open balls $B_1(a, r)$ contains 0. There is $\varepsilon' > 0$ such that

$$B_1(0, \varepsilon') \subset B_1(a, r) \subset B_2(0, \varepsilon).$$

Since $|x_n|_1 \to 0$, there exists N such that for $n \geq N$ we have $|x_n|_1 < \varepsilon'$. For such n, we have $x_n \in B_1(0, \varepsilon')$, so $x_n \in B_2(0, \varepsilon)$, so $|x_n|_2 < \varepsilon$. Thus $|x_n|_2 \to 0$. $\square$

Proposition 16.1.4. *If two valuations $|\cdot|_1$ and $|\cdot|_2$ on the same field induce the same topology, then they are equivalent in the sense that there is a positive real α such that $|\cdot|_1 = |\cdot|_2^\alpha$.*

Proof. If $x \in K$ and $i = 1, 2$, then $|x^n|_i \to 0$ if and only if $|x|_i^n \to 0$, which is the case if and only if $|x|_i < 1$. Thus Lemma 16.1.3 implies that $|x|_1 < 1$ if and only if $|x|_2 < 1$. On taking reciprocals we see that $|x|_1 > 1$ if and only if $|x|_2 > 1$, so finally $|x|_1 = 1$ if and only if $|x|_2 = 1$.

Let now $w, z \in K$ be nonzero elements with $|w|_i \neq 1$ and $|z|_i \neq 1$. On applying the foregoing to

$$x = w^m z^n \qquad (m, n \in \mathbf{Z})$$

we see that

$$m \log |w|_1 + n \log |z|_1 \geq 0$$

if and only if

$$m \log |w|_2 + n \log |z|_2 \geq 0.$$

Dividing through by $\log |z|_i$, and rearranging, we see that for every rational number $\alpha = -n/m$,

$$\frac{\log |w|_1}{\log |z|_1} \geq \alpha \iff \frac{\log |w|_2}{\log |z|_2} \geq \alpha.$$

Thus

$$\frac{\log |w|_1}{\log |z|_1} = \frac{\log |w|_2}{\log |z|_2},$$

so

$$\frac{\log |w|_1}{\log |w|_2} = \frac{\log |z|_1}{\log |z|_2}.$$

Since this equality does not depend on the choice of z, we see that there is a constant c $(= \log |z|_1 / \log |z|_2)$ such that $\log |w|_1 / \log |w|_2 = c$ for all w. Thus $\log |w|_1 = c \cdot \log |w|_2$, so $|w|_1 = |w|_2^c$, which implies that $|\cdot|_1$ is equivalent to $|\cdot|_2$. $\square$

16.2 Completeness

We recall the definition of metric on a set X.

Definition 16.2.1 (Metric). A *metric* on a set X is a map

$$d : X \times X \to \mathbf{R}$$

such that for all $x, y, z \in X$,

1. $d(x, y) \geq 0$ and $d(x, y) = 0$ if and only if $x = y$,
2. $d(x, y) = d(y, x)$, and
3. $d(x, z) \leq d(x, y) + d(y, z)$.

A *Cauchy sequence* is a sequence (x_n) in X such that for all $\varepsilon > 0$ there exists M such that for all $n, m > M$ we have $d(x_n, x_m) < \varepsilon$. The *completion* of X is the set of Cauchy sequences (x_n) in X modulo the equivalence relation in which two Cauchy sequences (x_n) and (y_n) are equivalent if $\lim_{n\to\infty} d(x_n, y_n) = 0$. A metric space is *complete* if every Cauchy sequence converges, and one can show that the completion of X with respect to a metric is complete.

For example, $d(x, y) = |x - y|$ (usual archimedean absolute value) defines a metric on $\mathbf{Q}$. The completion of $\mathbf{Q}$ with respect to this metric is the field $\mathbf{R}$ of real numbers. More generally, whenever $|\cdot|$ is a valuation on a field K that satisfies the triangle inequality, then $d(x, y) = |x - y|$ defines a metric on K. Consider for the rest of this section only valuations that satisfy the triangle inequality.

Definition 16.2.2 (Complete). A field K is *complete* with respect to a valuation $|\cdot|$ if given any Cauchy sequence a_n, $(n = 1, 2, \ldots)$, i.e., one for which

$$|a_m - a_n| \to 0 \qquad (m, n \to \infty, \infty),$$

there is an $a^* \in K$ such that

$$a_n \to a^* \qquad \text{w.r.t. } |\cdot|$$

(i.e., $|a_n - a^*| \to 0$).

Theorem 16.2.3. *Every field K with valuation $v = |\cdot|$ can be embedded in a complete field K_v with a valuation $|\cdot|$ extending the original one in such a way that K_v is the closure of K with respect to $|\cdot|$. Further K_v is unique up to a unique isomorphism fixing K.*

Proof. Define K_v to be the completion of K with respect to the metric defined by $|\cdot|$. Thus K_v is the set of equivalence classes of Cauchy sequences, and there is a natural injective map from K to K_v sending an element $a \in K$ to the constant Cauchy sequence (a). Because the field operations on K are continuous, they induce well-defined field operations on equivalence classes of Cauchy sequences componentwise. Also, define a valuation on K_v by

$$|(a_n)_{n=1}^{\infty}| = \lim_{n\to\infty} |a_n|,$$

and note that this is well defined and extends the valuation on K.

To see that K_v is unique up to a unique isomorphism fixing K, we observe that there are no nontrivial continuous automorphisms $K_v \to K_v$ that fix K. This is because, by denseness, a continuous automorphism $\sigma : K_v \to K_v$ is determined by what it does to K, and by assumption σ is the identity map on K. More precisely, suppose $a \in K_v$ and n is a positive integer. Then by continuity there is $\delta > 0$ (with $\delta < 1/n$) such that if $a_n \in K_v$ and $|a - a_n| < \delta$ then $|\sigma(a) - \sigma(a_n)| < 1/n$. Since K is dense in K_v, we can choose the a_n above to be an element of K. Then by hypothesis $\sigma(a_n) = a_n$, so $|\sigma(a) - a_n| < 1/n$. Thus $\sigma(a) = \lim_{n\to\infty} a_n = a$. □

Corollary 16.2.4. *The valuation $|\cdot|$ is non-archimedean on K_v if and only if it is so on K. If $|\cdot|$ is non-archimedean, then the set of values taken by $|\cdot|$ on K and K_v are the same.*

Proof. The first part follows from Lemma 15.2.10 which asserts that a valuation is non-archimedean if and only if $|n| < 1$ for all integers n. Since the valuation on K_v extends the valuation on K, and all n are in K, the first statement follows.

For the second, suppose that $|\cdot|$ is non-archimedean (but not necessarily discrete). Suppose $b \in K_v$ with $b \neq 0$. First I claim that there is $c \in K$ such that $|b - c| < |b|$. To see this, let $c' = b - \frac{b}{a}$, where a is some element of K_v with $|a| > 1$, note that $|b - c'| = \left|\frac{b}{a}\right| < |b|$, and choose $c \in K$ such that $|c - c'| < |b - c'|$, so

$$|b - c| = \left|b - c' - (c - c')\right| \leq \max\left(\left|b - c'\right|, \left|c - c'\right|\right) = \left|b - c'\right| < |b|.$$

Since $|\cdot|$ is non-archimedean, we have

$$|b| = |(b - c) + c| \leq \max\left(|b - c|, |c|\right) = |c|,$$

where in the last equality we use that $|b - c| < |b|$. Also,

$$|c| = |b + (c - b)| \leq \max\left(|b|, |c - b|\right) = |b|,$$

so $|b| = |c|$, which is in the set of values of $|\cdot|$ on K. □

16.2.1 p-adic Numbers

This section is about the p-adic numbers $\mathbf{Q}_p$, which are the completion of $\mathbf{Q}$ with respect to the p-adic valuation. Alternatively, to give a p-adic *integer* in $\mathbf{Z}_p$ is the same as giving for every prime power p^r an element $a_r \in \mathbf{Z}/p^r\mathbf{Z}$ such that if $s \leq r$ then a_s is the reduction of a_r modulo p^s. The field $\mathbf{Q}_p$ is then the field of fractions of $\mathbf{Z}_p$.

We begin with the definition of the N-adic numbers for any positive integer N. Section 16.2.1 is about the N-adics in the special case $N = 10$; these are fun because they can be represented as decimal expansions that go off infinitely far to the left. Section 16.2.3 is about how the topology of $\mathbf{Q}_N$ is nothing like the topology of $\mathbf{R}$. Finally, in Section 16.2.4 we state the Hasse-Minkowski theorem, which shows how to use p-adic numbers to decide whether or not a quadratic equation in n variables has a rational zero.

The N-adic Numbers

Lemma 16.2.5. *Let N be a positive integer. Then for any nonzero rational number α there exists a unique $e \in \mathbf{Z}$ and integers a, b, with b positive, such that $\alpha = N^e \cdot \frac{a}{b}$ with $N \nmid a$, $\gcd(a, b) = 1$, and $\gcd(N, b) = 1$.*

Proof. Write $\alpha = c/d$ with $c, d \in \mathbf{Z}$ and $d > 0$. First suppose d is exactly divisible by a power of N, so for some r we have $N^r \mid d$ but $\gcd(N, d/N^r) = 1$. Then

$$\frac{c}{d} = N^{-r}\frac{c}{d/N^r}.$$

If N^s is the largest power of N that divides c, then $e = s - r$, $a = c/N^s$, $b = d/N^r$ satisfy the conclusion of the lemma.

By unique factorization of integers, there is a smallest multiple f of d such that fd is exactly divisible by N. Now apply the above argument with c and d replaced by cf and df. $\square$

Definition 16.2.6 (N-adic valuation). Let N be a positive integer. For any positive $\alpha \in \mathbf{Q}$, the *N-adic valuation* of α is e, where e is as in Lemma 16.2.5. The N-adic valuation of 0 is ∞.

We denote the N-adic valuation of α by $\mathrm{ord}_N(\alpha)$. (Note: Here we are using "valuation" in a different way than in the rest of the text. This valuation is not an absolute value, but the logarithm of one.)

Definition 16.2.7 (N-adic metric). For $x, y \in \mathbf{Q}$ the *N-adic distance* between x and y is

$$d_N(x, y) = N^{-\mathrm{ord}_N(x-y)}.$$

We let $d_N(x, x) = 0$, since $\mathrm{ord}_N(x - x) = \mathrm{ord}_N(0) = \infty$.

For example, $x, y \in \mathbf{Z}$ are close in the N-adic metric if their difference is divisible by a large power of N. E.g., if $N = 10$ then 93427 and 13427 are close because their difference is 80000, which is divisible by a large power of 10.

Proposition 16.2.8. *The distance d_N on $\mathbf{Q}$ defined above is a metric. Moreover, for all $x, y, z \in \mathbf{Q}$ we have*

$$d(x, z) \leq \max(d(x, y), d(y, z)).$$

(This is the "nonarchimedean" triangle inequality.)

Proof. The first two properties of Definition 16.2.1 are immediate. For the third, we first prove that if $\alpha, \beta \in \mathbf{Q}$ then

$$\mathrm{ord}_N(\alpha + \beta) \geq \min(\mathrm{ord}_N(\alpha), \mathrm{ord}_N(\beta)).$$

Assume, without loss, that $\mathrm{ord}_N(\alpha) \leq \mathrm{ord}_N(\beta)$ and that both α and β are nonzero. Using Lemma 16.2.5 write $\alpha = N^e(a/b)$ and $\beta = N^f(c/d)$ with a or c possibly negative. Then

$$\alpha + \beta = N^e \left(\frac{a}{b} + N^{f-e}\frac{c}{d}\right) = N^e \left(\frac{ad + bcN^{f-e}}{bd}\right).$$

Since $\gcd(N, bd) = 1$ it follows that $\mathrm{ord}_N(\alpha + \beta) \geq e$. Now suppose $x, y, z \in \mathbf{Q}$. Then

$$x - z = (x - y) + (y - z),$$

so

$$\mathrm{ord}_N(x - z) \geq \min(\mathrm{ord}_N(x - y), \mathrm{ord}_N(y - z)),$$

hence $d_N(x, z) \leq \max(d_N(x, y), d_N(y, z))$. □

We can finally define the N-adic numbers.

Definition 16.2.9 (The N-adic Numbers). The set of *N-adic numbers*, denoted $\mathbf{Q}_N$, is the completion of $\mathbf{Q}$ with respect to the metric d_N.

The set $\mathbf{Q}_N$ is a ring, but it need not be a field as you will show in Exercises 57 and 58. It is a field if and only if N is prime. Also, $\mathbf{Q}_N$ has a "bizarre" topology, as we will see in Section 16.2.3.

The 10-adic Numbers

It's a familiar fact that every real number can be written in the form

$$d_n \ldots d_1 d_0 . d_{-1} d_{-2} \ldots = d_n 10^n + \cdots + d_1 10 + d_0 + d_{-1}10^{-1} + d_{-2}10^{-2} + \cdots$$

where each digit d_i is between 0 and 9, and the sequence can continue indefinitely to the right.

The 10-adic numbers also have decimal expansions, but everything is backward! To get a feeling for why this might be the case, we consider Euler's nonsensical series

$$\sum_{n=1}^{\infty} (-1)^{n+1} n! = 1! - 2! + 3! - 4! + 5! - 6! + \cdots.$$

One can prove (see Exercise 55) that this series converges in $\mathbf{Q}_{10}$ to some element $\alpha \in \mathbf{Q}_{10}$.

What is α? How can we write it down? First note that for all $M \geq 5$, the terms of the sum are divisible by 10, so the difference between α and $1! - 2! + 3! - 4!$ is divisible by 10. Thus we can compute α modulo 10 by computing $1! - 2! + 3! - 4!$ modulo 10. Likewise, we can compute α modulo 100 by compute $1! - 2! + \cdots + 9! - 10!$, etc. We obtain the following table:

α	mod 10^r
1	mod 10
81	mod 10^2
981	mod 10^3
2981	mod 10^4
22981	mod 10^5
422981	mod 10^6

Continuing we see that

$$1! - 2! + 3! - 4! + \cdots = \ldots 637838364422981 \qquad \text{in } \mathbf{Q}_{10}\ !$$

Here's another example. Reducing $1/7$ modulo larger and larger powers of 10 we see that

$$\frac{1}{7} = \ldots 857142857143 \qquad \text{in } \mathbf{Q}_{10}.$$

Here's another example, but with a decimal point.

$$\frac{1}{70} = \frac{1}{10} \cdot \frac{1}{7} = \ldots 85714285714.3$$

We have

$$\frac{1}{3} + \frac{1}{7} = \ldots 66667 + \ldots 57143 = \frac{10}{21} = \ldots 23810,$$

which illustrates that addition with carrying works as usual.

Fermat's Last Theorem in $\mathbf{Z}_{10}$

An amusing observation, which people often argued about on USENET news back in the 1990s, is that Fermat's last theorem is false in $\mathbf{Z}_{10}$. For example, $x^3+y^3 = z^3$ has a nontrivial solution, namely $x = 1$, $y = 2$, and $z = \ldots 60569$. Here z is a cube root of 9 in $\mathbf{Z}_{10}$. Note that it takes some work to prove that there is a cube root of 9 in $\mathbf{Z}_{10}$ (see Exercise 56).

16.2.2 The Field of p-adic Numbers

The ring $\mathbf{Q}_{10}$ of 10-adic numbers is isomorphic to $\mathbf{Q}_2 \times \mathbf{Q}_5$ (see Exercise 58), so it is not a field. For example, the element $\ldots 8212890625$ corresponding to $(1, 0)$ under this isomorphism has no inverse. (To compute n digits of $(1, 0)$ use the Chinese remainder theorem to find a number that is 1 modulo 2^n and 0 modulo 5^n.)

If p is prime then $\mathbf{Q}_p$ is a field (see Exercise 57). Since $p \neq 10$ it is a little more complicated to write p-adic numbers down. People typically write p-adic numbers in the form

$$\frac{a_{-d}}{p^d} + \cdots + \frac{a_{-1}}{p} + a_0 + a_1 p + a_2 p^2 + a_3 p^3 + \cdots$$

where $0 \leq a_i < p$ for each i.

16.2.3 The Topology of $\mathbf{Q}_N$ (is Weird)

Definition 16.2.10 (Connected). Let X be a topological space. A subset S of X is *disconnected* if there exist open subsets $U_1, U_2 \subset X$ with $U_1 \cap U_2 \cap S = \emptyset$ and $S = (S \cap U_1) \cup (S \cap U_2)$ with $S \cap U_1$ and $S \cap U_2$ nonempty. If S is not disconnected it is *connected*.

The topology on $\mathbf{Q}_N$ is induced by d_N, so every open set is a union of open balls

$$B(x, r) = \{y \in \mathbf{Q}_N : d_N(x, y) < r\}.$$

Recall Proposition 16.2.8, which asserts that for all x, y, z,

$$d(x, z) \leq \max(d(x, y), d(y, z)).$$

This translates into the following shocking and bizarre lemma:

Lemma 16.2.11. *Suppose $x \in \mathbf{Q}_N$ and $r > 0$. If $y \in \mathbf{Q}_N$ and $d_N(x, y) \geq r$, then $B(x, r) \cap B(y, r) = \emptyset$.*

Proof. Suppose $z \in B(x, r)$ and $z \in B(y, r)$. Then

$$r \leq d_N(x, y) \leq \max(d_N(x, z), d_N(z, y)) < r,$$

a contradiction. □

You should draw a picture to illustrates Lemma 16.2.11.

Lemma 16.2.12. *The open ball $B(x, r)$ is also closed.*

Proof. Suppose $y \notin B(x, r)$. Then $r \leq d(x, y)$ so

$$B(y, d(x, y)) \cap B(x, r) \subset B(y, d(x, y)) \cap B(x, d(x, y)) = \emptyset.$$

Thus the complement of $B(x, r)$ is a union of open balls. □

The lemmas imply that $\mathbf{Q}_N$ is *totally disconnected*, in the following sense.

Proposition 16.2.13. *The only connected subsets of $\mathbf{Q}_N$ are the singleton sets $\{x\}$ for $x \in \mathbf{Q}_N$ and the empty set.*

Proof. Suppose $S \subset \mathbf{Q}_N$ is a nonempty connected set and x, y are distinct elements of S. Let $r = d_N(x, y) > 0$. Let $U_1 = B(x, r)$ and U_2 be the complement of U_1, which is open by Lemma 16.2.12. Then U_1 and U_2 satisfies the conditions of Definition 16.2.10, so S is not connected, a contradiction. □

16.2.4 The Local-to-Global Principle of Hasse and Minkowski

Section 16.2.3 might have convinced you that $\mathbf{Q}_N$ is a bizarre pathology. In fact, $\mathbf{Q}_N$ is omnipresent in number theory, as the following two fundamental examples illustrate.

In the statement of the following theorem, a *nontrivial solution* to a homogeneous polynomial equation is a solution where not all indeterminates are 0.

Theorem 16.2.14 (Hasse-Minkowski). *The quadratic equation*

$$a_1x_1^2 + a_2x_2^2 + \cdots + a_nx_n^2 = 0, \tag{16.2.1}$$

with $a_i \in \mathbf{Q}^\times$, has a nontrivial solution with $x_1, \ldots, x_n$ in $\mathbf{Q}$ if and only if (16.2.1) has a solution in $\mathbf{R}$ and in $\mathbf{Q}_p$ for all primes p.

This theorem is very useful in practice because the p-adic condition turns out to be easy to check. For more details, including a complete proof, see [Ser73, IV.3.2].

The analogue of Theorem 16.2.14 for cubic equations is false. For example, Selmer proved that the cubic

$$3x^3 + 4y^3 + 5z^3 = 0$$

has a solution other than $(0, 0, 0)$ in $\mathbf{R}$ and in $\mathbf{Q}_p$ for all primes p but has no solution other than $(0, 0, 0)$ in $\mathbf{Q}$ (for a proof see [Cas91, §18]).

Open Problem. Give an algorithm that decides whether or not a cubic

$$ax^3 + by^3 + cz^3 = 0$$

has a nontrivial solution in $\mathbf{Q}$.

This open problem is closely related to the Birch and Swinnerton-Dyer Conjecture for elliptic curves. The truth of the conjecture would follow if we knew that "Shafarevich-Tate Groups" of elliptic curves were finite.

16.3 Weak Approximation

The following theorem asserts that inequivalent valuations are in fact almost totally indepedent. For our purposes it will be superseded by the strong approximation theorem (Theorem 20.4.4).

Theorem 16.3.1 (Weak Approximation). *Let $|\cdot|_n$, for $1 \leq n \leq N$, be inequivalent nontrivial valuations of a field K. For each n, let K_n be the topological space consisting of the set of elements of K with the topology induced by $|\cdot|_n$. Let Δ be the image of K in the topological product*

$$A = \prod_{1 \leq n \leq N} K_n$$

equipped with the product topology. Then Δ is dense in A.

The conclusion of the theorem may be expressed in a less topological manner as follows: given any $a_n \in K$, for $1 \le n \le N$, and real $\varepsilon > 0$, there is an $b \in K$ such that simultaneously

$$|a_n - b|_n < \varepsilon \qquad (1 \le n \le N).$$

If $K = \mathbf{Q}$ and the $|\cdot|$ are p-adic valuations, Theorem 16.3.1 is related to the Chinese Remainder Theorem (Theorem 9.1.3), but the strong approximation theorem (Theorem 20.4.4) is the real generalization.

Proof. We note first that it will be enough to find, for each n, an element $c_n \in K$ such that

$$|c_n|_n > 1 \quad \text{ and } \quad |c_n|_m < 1 \quad \text{ for } n \neq m,$$

where $1 \le n, m \le N$. For then as $r \to +\infty$, we have

$$\frac{c_n^r}{1 + c_n^r} = \frac{1}{1 + \left(\frac{1}{c_n}\right)^r} \to \begin{cases} 1 & \text{with respect to } |\cdot|_n \text{ and} \\ 0 & \text{with respect to } |\cdot|_m \text{, for } m \neq n. \end{cases}$$

It is then enough to take

$$b = \sum_{n=1}^{N} \frac{c_n^r}{1 + c_n^r} \cdot a_n$$

By symmetry it is enough to show the existence of $c = c_1$ with

$$|c|_1 > 1 \qquad \text{and} \qquad |c|_n < 1 \quad \text{for} \quad 2 \le n \le N.$$

We will do this by induction on N.

First suppose $N = 2$. Since $|\cdot|_1$ and $|\cdot|_2$ are inequivalent (and all absolute values are assumed nontrivial) there is an $a \in K$ such that

$$|a|_1 < 1 \qquad \text{and} \qquad |a|_2 \ge 1 \tag{16.3.1}$$

and similarly a b such that

$$|b|_1 \ge 1 \qquad \text{and} \qquad |b|_2 < 1.$$

Then $c = \dfrac{b}{a}$ will do.

Remark 16.3.2. It is not completely clear that one can choose an a such that (16.3.1) is satisfied. Suppose it were impossible. Then because the valuations are nontrivial, we would have that for any $a \in K$ if $|a|_1 < 1$ then $|a|_2 < 1$. This implies the converse statement: if $a \in K$ and $|a|_2 < 1$ then $|a|_1 < 1$. To see this, suppose there is an $a \in K$ such that $|a|_2 < 1$ and $|a|_1 \ge 1$. Choose $y \in K$ such that $|y|_1 < 1$. Then for any integer $n > 0$ we have $|y/a^n|_1 < 1$, so by hypothesis $|y/a^n|_2 < 1$. Thus $|y|_2 < |a|_2^n < 1$ for all n. Since $|a|_2 < 1$ we have $|a|_2^n \to 0$ as $n \to \infty$, so $|y|_2 = 0$, a contradiction since $y \neq 0$. Thus $|a|_1 < 1$ if and only if $|a|_2 < 1$, and we have proved before that this implies that $|\cdot|_1$ is equivalent to $|\cdot|_2$.

Next suppose $N \geq 3$. By the case $N-1$, there is an $a \in K$ such that

$$|a|_1 > 1 \qquad \text{and} \qquad |a|_n < 1 \quad \text{for} \quad 2 \leq n \leq N-1.$$

By the case for $N = 2$ there is a $b \in K$ such that

$$|b|_1 > 1 \qquad \text{and} \qquad |b|_N < 1.$$

Then put

$$c = \begin{cases} a & \text{if } |a|_N < 1 \\ a^r \cdot b & \text{if } |a|_N = 1 \\ \dfrac{a^r}{1+a^r} \cdot b & \text{if } |a|_N > 1 \end{cases}$$

where $r \in \mathbf{Z}$ is sufficiently large so that $|c|_1 > 1$ and $|c|_n < 1$ for $2 \leq n \leq N$. □

Example 16.3.3. Suppose $K = \mathbf{Q}$, let $|\cdot|_1$ be the archimedean absolute value and let $|\cdot|_2$ be the 2-adic absolute value. Let $a_1 = -1$, $a_2 = 8$, and $\varepsilon = 1/10$, as in the remark right after Theorem 16.3.1. Then the theorem implies that there is an element $b \in \mathbf{Q}$ such that

$$|-1-b|_1 < \frac{1}{10} \qquad \text{and} \qquad |8-b|_2 < \frac{1}{10}.$$

As in the proof of the theorem, we can find such a b by finding a $c_1, c_2 \in \mathbf{Q}$ such that $|c_1|_1 > 1$ and $|c_1|_2 < 1$, and a $|c_2|_1 < 1$ and $|c_2|_2 > 1$. For example, $c_1 = 2$ and $c_2 = 1/2$ works, since $|2|_1 = 2$ and $|2|_2 = 1/2$ and $|1/2|_1 = 1/2$ and $|1/2|_2 = 2$. Again following the proof, we see that for sufficiently large r we can take

$$\begin{aligned} b_r &= \frac{c_1^r}{1+c_1^r} \cdot a_1 + \frac{c_2^r}{1+c_2^r} \cdot a_2 \\ &= \frac{2^r}{1+2^r} \cdot (-1) + \frac{(1/2)^r}{1+(1/2)^r} \cdot 8. \end{aligned}$$

We have $b_1 = 2$, $b_2 = 4/5$, $b_3 = 0$, $b_4 = -8/17$, $b_5 = -8/11$, $b_6 = -56/55$. None of the b_i work for $i < 6$, but b_6 works.

Chapter 17

Adic Numbers: The Finite Residue Field Case

17.1 Finite Residue Field Case

Let K be a field with a non-archimedean valuation $v = |\cdot|$. Recall that the set of $a \in K$ with $|a| \leq 1$ forms a ring $\mathcal{O}$, the ring of integers for v. The set of $u \in K$ with $|u| = 1$ are a group U under multiplication, the group of units for v. Finally, the set of $a \in K$ with $|a| < 1$ is a maximal ideal $\mathfrak{p}$, so the quotient ring $\mathcal{O}/\mathfrak{p}$ is a field. In this section we consider the case when $\mathcal{O}/\mathfrak{p}$ is a finite field of order a prime power q. For example, K could be $\mathbf{Q}$ and $|\cdot|$ could be a p-adic valuation, or K could be a number field and $|\cdot|$ could be the valuation corresponding to a maximal ideal of the ring of integers. Among other things, we will discuss in more depth the topological and measure-theoretic nature of the completion of K at v.

Suppose further for the rest of this section that $|\cdot|$ is discrete. Then by Lemma 15.2.8, the ideal $\mathfrak{p}$ is a principal ideal (π), say, and every $a \in K$ is of the form $a = \pi^n \varepsilon$, where $n \in \mathbf{Z}$ and $\varepsilon \in U$ is a unit. We call

$$n = \mathrm{ord}(a) = \mathrm{ord}_\pi(a) = \mathrm{ord}_\mathfrak{p}(a) = \mathrm{ord}_v(a)$$

the ord of a at v. (Some authors, including me (!) also call this integer the *valuation* of a with respect to v.) If $\mathfrak{p} = (\pi')$, then π/π' is a unit, and conversely, so $\mathrm{ord}(a)$ is independent of the choice of π.

Let $\mathcal{O}_v$ and $\mathfrak{p}_v$ be defined with respect to the completion K_v of K at v.

Lemma 17.1.1. *There is a natural isomorphism*

$$\varphi : \mathcal{O}_v/\mathfrak{p}_v \to \mathcal{O}/\mathfrak{p},$$

and $\mathfrak{p}_v = (\pi)$ *as an* $\mathcal{O}_v$*-ideal.*

Proof. We may view $\mathcal{O}_v$ as the set of equivalence classes of Cauchy sequences (a_n) in K such that $a_n \in \mathcal{O}$ for n sufficiently large. For any ε, given such a sequence

(a_n), there is N such that for $n, m \geq N$, we have $|a_n - a_m| < \varepsilon$. In particular, we can choose N such that $n, m \geq N$ implies that $a_n \equiv a_m \pmod{\mathfrak{p}}$. Let $\varphi((a_n)) = a_N \pmod{\mathfrak{p}}$, which is well-defined. The map φ is surjective because the constant sequences are in $\mathcal{O}_v$. Its kernel is the set of Cauchy sequences whose elements are eventually all in $\mathfrak{p}$, which is exactly $\mathfrak{p}_v$. This proves the first part of the lemma. The second part is true because any element of $\mathfrak{p}_v$ is a sequence all of whose terms are eventually in $\mathfrak{p}$, hence all a multiple of π (we can set to 0 a finite number of terms of the sequence without changing the equivalence class of the sequence). □

Assume for the rest of this section that K is complete with respect to $|\cdot|$.

Lemma 17.1.2. *Then ring $\mathcal{O}$ is precisely the set of infinite sums*

$$a = \sum_{j=0}^{\infty} a_j \cdot \pi^j \tag{17.1.1}$$

where the a_j run independently through some set $\mathcal{R}$ of representatives of $\mathcal{O}$ in $\mathcal{O}/\mathfrak{p}$.

By (17.1.1) is meant the limit of the Cauchy sequence $\sum_{j=0}^{n} a_j \cdot \pi^j$ as $j \to \infty$.

Proof. There is a uniquely defined $a_0 \in \mathcal{R}$ such that $|a - a_0| < 1$. Then $a' = \pi^{-1} \cdot (a - a_0) \in \mathcal{O}$. Now define $a_1 \in \mathcal{R}$ by $|a' - a_1| < 1$. And so on. □

Example 17.1.3. Suppose $K = \mathbf{Q}$ and $|\cdot| = |\cdot|_p$ is the p-adic valuation, for some prime p. We can take $\mathcal{R} = \{0, 1, \ldots, p-1\}$. The lemma asserts that

$$\mathcal{O} = \mathbf{Z}_p = \left\{ \sum_{j=0}^{\infty} a_n p^n : 0 \leq a_n \leq p-1 \right\}.$$

Notice that $\mathcal{O}$ is uncountable since there are p choices for each p-adic "digit". We can do arithmetic with elements of $\mathbf{Z}_p$, which can be thought of "backwards" as numbers in base p. For example, with $p = 3$ we have

$$\begin{aligned}
&(1 + 2\cdot 3 + 3^2 + \cdots) + (2 + 2\cdot 3 + 3^2 + \cdots) \\
&= 3 + 4\cdot 3 + 2\cdot 3^2 + \cdots \qquad \text{not in canonical form} \\
&= 0 + 2\cdot 3 + 3\cdot 3 + 2\cdot 3^2 + \cdots \qquad \text{still not canonical} \\
&= 0 + 2\cdot 3 + 0\cdot 3^2 + \cdots
\end{aligned}$$

Basic arithmetic with the p-adics in MAGMA is really weird (even weirder than it was a year ago... There are presumably efficiency advantages to using the MAGMA formalization, and it's supposed to be better for working with extension fields. But I can't get it to do even the calculation below in a way that is clear.) In PARI (gp) the p-adics work as expected:

```
? a = 1 + 2*3 + 3^2 + O(3^3);
? b = 2 + 2*3 + 3^2 + O(3^3);
? a+b
%3 = 2*3 + O(3^3)
? sqrt(1+2*3+O(3^20))
%5 = 1 + 3 + 3^2 + 2*3^4 + 2*3^7 + 3^8 + 3^9 + 2*3^10 + 2*3^12
       + 2*3^13 + 2*3^14 + 3^15 + 2*3^17 + 3^18 + 2*3^19 + O(3^20)
? 1/sqrt(1+2*3+O(3^20))
%6 = 1 + 2*3 + 2*3^2 + 2*3^7 + 2*3^10 + 2*3^11 + 2*3^12 + 2*3^13
       + 2*3^14 + 3^15 + 2*3^16 + 2*3^17 + 3^18 + 3^19 + O(3^20)
```

Theorem 17.1.4. *Under the conditions of the preceding lemma, $\mathcal{O}$ is compact with respect to the $|\cdot|$-topology.*

Proof. Let V_λ, for λ running through some index set Λ, be some family of open sets that cover $\mathcal{O}$. We must show that there is a finite subcover. We suppose not.

Let $\mathcal{R}$ be a set of representatives for $\mathcal{O}/\mathfrak{p}$. Then $\mathcal{O}$ is the union of the finite number of cosets $a + \pi\mathcal{O}$, for $a \in \mathcal{R}$. Hence for at lest one $a_0 \in \mathcal{R}$ the set $a_0 + \pi\mathcal{O}$ is not covered by finitely many of the V_λ. Then similarly there is an $a_1 \in \mathcal{R}$ such that $a_0 + a_1\pi + \pi^2\mathcal{O}$ is not finitely covered. And so on. Let

$$a = a_0 + a_1\pi + a_2\pi^2 + \cdots \in \mathcal{O}.$$

Then $a \in V_{\lambda_0}$ for some $\lambda_0 \in \Lambda$. Since V_{λ_0} is an open set, $a + \pi^J \cdot \mathcal{O} \subset V_{\lambda_0}$ for some J (since those are exactly the open balls that form a basis for the topology). This is a contradiction because we constructed a so that none of the sets $a + \pi^n \cdot \mathcal{O}$, for each n, are not covered by any finite subset of the V_λ. $\square$

Definition 17.1.5 (Locally compact). A topological space X is *locally compact* at a point x if there is some compact subset C of X that contains a neighborhood of x. The space X is locally compact if it is locally compact at each point in X.

Corollary 17.1.6. *The complete local field K is locally compact.*

Proof. If $x \in K$, then $x \in C = x + \mathcal{O}$, and C is a compact subset of K by Theorem 17.1.4. Also C contains the neighborhood $x + \pi\mathcal{O} = B(x, 1)$ of x. Thus K is locally compact at x. $\square$

Remark 17.1.7. The converse is also true. If K is locally compact with respect to a non-archimedean valuation $|\cdot|$, then

1. K is complete,

2. the residue field is finite, and

3. the valuation is discrete.

For there is a compact neighbourhood C of 0. Let π be any nonzero with $|\pi| < 1$. Then $\pi^n \cdot \mathcal{O} \subset C$ for sufficiently large n, so $\pi^n \cdot \mathcal{O}$ is compact, being closed. Hence $\mathcal{O}$ is compact. Since $|\cdot|$ is a metric, $\mathcal{O}$ is sequentially compact, i.e., every fundamental sequence in $\mathcal{O}$ has a limit, which implies (1). Let a_λ (for $\lambda \in \Lambda$) be a set of representatives in $\mathcal{O}$ of $\mathcal{O}/\mathfrak{p}$. Then $\mathcal{O}_\lambda = \{z : |z - a_\lambda| < 1\}$ is an open covering of $\mathcal{O}$. Thus (2) holds since $\mathcal{O}$ is compact. Finally, $\mathfrak{p}$ is compact, being a closed subset of $\mathcal{O}$. Let S_n be the set of $a \in K$ with $|a| < 1 - 1/n$. Then S_n (for $1 \leq n < \infty$) is an open covering of $\mathfrak{p}$, so $\mathfrak{p} = S_n$ for some n, i.e., (3) is true.

If we allow $|\cdot|$ to be archimedean the only further possibilities are $k = \mathbf{R}$ and $k = \mathbf{C}$ with $|\cdot|$ equivalent to the usual absolute value.

We denote by K^+ the commutative topological group whose points are the elements of K, whose group law is addition and whose topology is that induced by $|\cdot|$. General theory tells us that there is an invariant Haar measure defined on K^+ and that this measure is unique up to a multiplicative constant.

Definition 17.1.8 (Haar Measure). A *Haar measure* on a locally compact topological group G is a translation invariant measure such that every open set can be covered by open sets with finite measure.

Lemma 17.1.9. *Haar measure of any compact subset C of G is finite.*

Proof. The whole group G is open, so there is a covering U_α of G by open sets each of which has finite measure. Since C is compact, there is a finite subset of the U_α that covers C. The measure of C is at most the sum of the measures of these finitely many U_α, hence finite. $\square$

Remark 17.1.10. Usually one defined Haar measure to be a translation invariant measure such that the measure of compact sets is finite. Because of local compactness, this definition is equivalent to Definition 17.1.8. We take this alternative viewpoint because Haar measure is constructed naturally on the topological groups we will consider by defining the measure on each member of a basis of open sets for the topology.

We now deduce what any such measure μ on $G = K^+$ must be. Since $\mathcal{O}$ is compact (Theorem 17.1.4), the measure of $\mathcal{O}$ is finite. Since μ is translation invariant,

$$\mu_n = \mu(a + \pi^n \mathcal{O})$$

is independent of a. Further,

$$a + \pi^n \mathcal{O} = \bigcup_{1 \leq j \leq q} a + \pi^n a_j + \pi^{n+1}\mathcal{O}, \qquad \text{(disjoint union)}$$

where a_j (for $1 \leq j \leq q$) is a set of representatives of $\mathcal{O}/\mathfrak{p}$. Hence

$$\mu_n = q \cdot \mu_{n+1}.$$

If we normalize μ by putting

$$\mu(\mathcal{O}) = 1$$

we have $\mu_0 = 1$, hence $\mu_1 = q$, and in general

$$\mu_n = q^{-n}.$$

Conversely, without the theory of Haar measure, we could *define* μ to be the necessarily unique measure on K^+ such that $\mu(\mathcal{O}) = 1$ that is translation invariant. This would have to be the μ we just found above.

Everything so far in this section has depended not on the valuation $|\cdot|$ but only on its equivalence class. The above considerations now single out one valuation in the equivalence class as particularly important.

Definition 17.1.11 (Normalized valuation). Let K be a field equipped with a discrete valuation $|\cdot|$ and residue class field with $q < \infty$ elements. We say that $|\cdot|$ is *normalized* if

$$|\pi| = \frac{1}{q},$$

where $\mathfrak{p} = (\pi)$ is the maximal ideal of $\mathcal{O}$.

Example 17.1.12. The normalized valuation on the p-adic numbers $\mathbf{Q}_p$ is $|u \cdot p^n| = p^{-n}$, where u is a rational number whose numerator and denominator are coprime to p.

Next suppose $K = \mathbf{Q}_p(\sqrt{p})$. Then the p-adic valuation on $\mathbf{Q}_p$ extends uniquely to one on K such that $\left|\sqrt{p}\right|^2 = |p| = 1/p$. Since $\pi = \sqrt{p}$ for K, this valuation is not normalized. (Note that the ord of $\pi = \sqrt{p}$ is $1/2$.) The normalized valuation is $v = |\cdot|' = |\cdot|^2$. Note that $|\cdot|' \, p = 1/p^2$, or $\mathrm{ord}_v(p) = 2$ instead of 1.

Finally suppose that $K = \mathbf{Q}_p(\sqrt{q})$ where $x^2 - q$ has not root mod p. Then the residue class field degree is 2, and the normalized valuation must satisfy $\left|\sqrt{q}\right| = 1/p^2$.

The following proposition makes clear why this is the best choice of normalization.

Theorem 17.1.13. *Suppose further that K is complete with respect to the normalized valuation $|\cdot|$. Then*

$$\mu(a + b\mathcal{O}) = |b|,$$

where μ is the Haar measure on K^+ normalized so that $\mu(\mathcal{O}) = 1$.

Proof. Since μ is translation invariant, $\mu(a + b\mathcal{O}) = \mu(b\mathcal{O})$. Write $b = u \cdot \pi^n$, where u is a unit. Then since $u \cdot \mathcal{O} = \mathcal{O}$, we have

$$\mu(b\mathcal{O}) = \mu(u \cdot \pi^n \cdot \mathcal{O}) = \mu(\pi^n \cdot u \cdot \mathcal{O}) = \mu(\pi^n \cdot \mathcal{O}) = q^{-n} = |\pi^n| = |b|.$$

Here we have $\mu(\pi^n \cdot \mathcal{O}) = q^{-n}$ by the discussion before Definition 17.1.11. $\square$

We can express the result of the theorem in a more suggestive way. Let $b \in K$ with $b \neq 0$, and let μ be a Haar measure on K^+ (not necessarily normalized as in the theorem). Then we can define a new Haar measure μ_b on K^+ by putting $\mu_b(E) = \mu(bE)$ for $E \subset K^+$. But Haar measure is unique up to a multiplicative constant and so $\mu_b(E) = \mu(bE) = c \cdot \mu(E)$ for all measurable sets E, where the factor c depends only on b. Putting $E = \mathcal{O}$, shows that the theorem implies that c is just $|b|$, when $|\cdot|$ is the normalized valuation.

Remark 17.1.14. The theory of locally compact topological groups leads to the consideration of the dual (character) group of K^+. It turns out that it is isomorphic to K^+. We do not need this fact for class field theory, so do not prove it here. For a proof and applications see Tate's thesis or Lang's *Algebraic Numbers*, and for generalizations see Weil's *Adeles and Algebraic Groups* and Godement's Bourbaki seminars 171 and 176. The determination of the character group of K^* is local class field theory.

The set of nonzero elements of K is a group K^* under multiplication. Multiplication and inverses are continuous with respect to the topology induced on K^* as a subset of K, so K^* is a topological group with this topology. We have

$$U_1 \subset U \subset K^*$$

where U is the group of units of $\mathcal{O} \subset K$ and U_1 is the group of 1-units, i.e., those units $\varepsilon \in U$ with $|\varepsilon - 1| < 1$, so

$$U_1 = 1 + \pi\mathcal{O}.$$

The set U is the open ball about 0 of radius 1, so is open, and because the metric is nonarchimedean U is also closed. Likewise, U_1 is both open and closed.

The quotient $K^*/U = \{\pi^n \cdot U : n \in \mathbf{Z}\}$ is isomorphic to the additive group $\mathbf{Z}^+$ of integers with the discrete topology, where the map is

$$\pi^n \cdot U \mapsto n \qquad \text{for } n \in \mathbf{Z}.$$

The quotient U/U_1 is isomorphic to the multiplicative group $\mathbf{F}^*$ of the nonzero elements of the residue class field, where the finite gorup $\mathbf{F}^*$ has the discrete topology. Note that $\mathbf{F}^*$ is cyclic of order $q-1$, and Hensel's lemma implies that K^* contains a primitive $(q-1)$th root of unity ζ. Thus K^* has the following structure:

$$K^* = \{\pi^n \zeta^m \varepsilon : n \in \mathbf{Z}, m \in \mathbf{Z}/(q-1)\mathbf{Z}, \varepsilon \in U_1\} \cong \mathbf{Z} \times \mathbf{Z}/(q-1)\mathbf{Z} \times U_1.$$

(How to apply Hensel's lemma: Let $f(x) = x^{q-1} - 1$ and let $a \in \mathcal{O}$ be such that $a \bmod \mathfrak{p}$ generates K^*. Then $|f(a)| < 1$ and $|f'(a)| = 1$. By Hensel's lemma there is a $\zeta \in K$ such that $f(\zeta) = 0$ and $\zeta \equiv a \pmod{\mathfrak{p}}$.)

Since U is compact and the cosets of U cover K, we see that K^* is locally compact.

Lemma 17.1.15. *The additive Haar measure μ on K^+, when restricted to U_1 gives a measure on U_1 that is also invariant under multiplication, so gives a Haar measure on U_1.*

Proof. It suffices to show that

$$\mu(1+\pi^n\mathcal{O}) = \mu(u\cdot(1+\pi^n\mathcal{O})),$$

for any $u \in U_1$ and $n > 0$. Write $u = 1 + a_1\pi + a_2\pi^2 + \cdots$. We have

$$\begin{aligned} u\cdot(1+\pi^n\mathcal{O}) &= (1 + a_1\pi + a_2\pi^2 + \cdots)\cdot(1+\pi^n\mathcal{O}) \\ &= 1 + a_1\pi + a_2\pi^2 + \cdots + \pi^n\mathcal{O} \\ &= a_1\pi + a_2\pi^2 + \cdots + (1+\pi^n\mathcal{O}), \end{aligned}$$

which is an additive translate of $1+\pi^n\mathcal{O}$, hence has the same measure. □

Thus μ gives a Haar measure on K^* by translating U_1 around to cover K^*.

Lemma 17.1.16. *The topological spaces K^+ and K^* are totally disconnected (the only connected sets are points).*

Proof. The proof is the same as that of Proposition 16.2.13. The point is that the non-archimedean triangle inequality forces the complement an open disc to be open, hence any set with at least two distinct elements "falls apart" into a disjoint union of two disjoint open subsets. □

Remark 17.1.17. Note that K^* and K^+ are locally isomorphic if K has characteristic 0. We have the exponential map

$$a \mapsto \exp(a) = \sum_{n=0}^{\infty} \frac{a^n}{n!}$$

defined for all sufficiently small a with its inverse

$$\log(a) = \sum_{n=1}^{\infty} \frac{(-1)^{n-1}(a-1)^n}{n},$$

which is defined for all a sufficiently close to 1.

Chapter 18

Normed Spaces and Tensor Products

Much of this chapter is preparation for what we will do later when we will prove that if K is complete with respect to a valuation (and locally compact) and L is a finite extension of K, then there is a *unique* valuation on L that extends the valuation on K. Also, if K is a number field, $v = |\cdot|$ is a valuation on K, K_v is the completion of K with respect to v, and L is a finite extension of K, we'll prove that

$$K_v \otimes_K L = \bigoplus_{j=1}^{J} L_j,$$

where the L_j are the completions of L with respect to the equivalence classes of extensions of v to L. In particular, if L is a number field defined by a root of $f(x) \in \mathbf{Q}[x]$, then

$$\mathbf{Q}_p \otimes_{\mathbf{Q}} L = \bigoplus_{j=1}^{J} L_j,$$

where the L_j correspond to the irreducible factors of the polynomial $f(x) \in \mathbf{Q}_p[x]$ (hence the extensions of $|\cdot|_p$ correspond to irreducible factors of $f(x)$ over $\mathbf{Q}_p[x]$).

In preparation for this clean view of the local nature of number fields, we will prove that the norms on a finite-dimensional vector space over a complete field are all equivalent. We will also explicitly construct tensor products of fields and deduce some of their properties.

18.1 Normed Spaces

Definition 18.1.1 (Norm). Let K be a field with valuation $|\cdot|$ and let V be a vector space over K. A real-valued function $\|\cdot\|$ on V is called a *norm* if

1. $\|v\| > 0$ for all nonzero $v \in V$ (positivity).

2. $\|v+w\| \leq \|v\| + \|w\|$ for all $v, w \in V$ (triangle inequality).
3. $\|av\| = |a|\,\|v\|$ for all $a \in K$ and $v \in V$ (homogeneity).

Note that setting $\|v\| = 1$ for all $v \neq 0$ does *not* define a norm unless the absolute value on K is trivial, as $1 = \|av\| = |a|\,\|v\| = |a|$. We assume for the rest of this section that $|\cdot|$ is not trivial.

Definition 18.1.2 (Equivalent). Two norms $\|\cdot\|_1$ and $\|\cdot\|_2$ on the same vector space V are *equivalent* if there exists positive real numbers c_1 and c_2 such that for all $v \in V$

$$\|v\|_1 \leq c_1 \|v\|_2 \qquad \text{and} \qquad \|v\|_2 \leq c_2 \|v\|_1 .$$

Lemma 18.1.3. *Suppose that K is a field that is complete with respect to a valuation $|\cdot|$ and that V is a finite dimensional K vector space. Continue to assume, as mentioned above, that K is complete with respect to $|\cdot|$. Then any two norms on V are equivalent.*

Remark 18.1.4. As we shall see soon (see Theorem 19.1.8), the lemma is usually false if we do not assume that K is complete. For example, when $K = \mathbf{Q}$ and $|\cdot|_p$ is the p-adic valuation, and V is a number field, then there may be several extensions of $|\cdot|_p$ to inequivalent norms on V.

If two norms are equivalent then the corresponding topologies on V are equal, since very open ball for $\|\cdot\|_1$ is contained in an open ball for $\|\cdot\|_2$, and conversely. (The converse is also true, since, as we will show, all norms on V are equivalent.)

Proof. Let $v_1, \ldots, v_N$ be a basis for V. Define the max norm $\|\cdot\|_0$ by

$$\left\| \sum_{n=1}^{N} a_n v_n \right\|_0 = \max\{|a_n| : n = 1, \ldots, N\}.$$

It is enough to show that any norm $\|\cdot\|$ is equivalent to $\|\cdot\|_0$. We have

$$\begin{aligned} \left\| \sum_{n=1}^{N} a_n v_n \right\| &\leq \sum_{n=1}^{N} |a_n|\,\|v_n\| \\ &\leq \sum_{n=1}^{N} \max|a_n|\,\|v_n\| \\ &= c_1 \cdot \left\| \sum_{n=1}^{N} a_n v_n \right\|_0 , \end{aligned}$$

where $c_1 = \sum_{n=1}^{N} \|v_n\|$.

To finish the proof, we show that there is a $c_2 \in \mathbf{R}$ such that for all $v \in V$,

$$\|v\|_0 \leq c_2 \cdot \|v\| .$$

We will only prove this in the case when K is not just merely complete with respect to $|\cdot|$ but also locally compact. This will be the case of primary interest to us. For a proof in the general case, see the original article by Cassels (page 53).

By what we have already shown, the function $\|v\|$ is continuous in the $\|\cdot\|_0$-topology, so by local compactness it attains its lower bound δ on the unit circle $\{v \in V : \|v\|_0 = 1\}$. (Why is the unit circle compact? With respect to $\|\cdot\|_0$, the topology on V is the same as that of a product of copies of K. If the valuation is archimedean then $K \cong \mathbf{R}$ or $\mathbf{C}$ with the standard topology and the unit circle is compact. If the valuation is non-archimedean, then we saw (see Remark 17.1.7) that if K is locally compact, then the valuation is discrete, in which case we showed that the unit disc is compact, hence the unit circle is also compact since it is closed.) Note that $\delta > 0$ by part 1 of Definition 18.1.1. Also, by definition of $\|\cdot\|_0$, for any $v \in V$ there exists $a \in K$ such that $\|v\|_0 = |a|$ (just take the max coefficient in our basis). Thus we can write any $v \in V$ as $a \cdot w$ where $a \in K$ and $w \in V$ with $\|w\|_0 = 1$. We then have

$$\frac{\|v\|_0}{\|v\|} = \frac{\|aw\|_0}{\|aw\|} = \frac{|a|\,\|w\|_0}{|a|\,\|w\|} = \frac{1}{\|w\|} \leq \frac{1}{\delta}.$$

Thus for all v we have

$$\|v\|_0 \leq c_2 \cdot \|v\|,$$

where $c_2 = 1/\delta$, which proves the theorem. □

18.2 Tensor Products

We need only a special case of the tensor product construction. Let A and B be commutative rings containing a field K and suppose that B is of finite dimension N over K, say, with basis

$$1 = w_1, w_2, \ldots, w_N.$$

Then B is determined up to isomorphism as a ring over K by the multiplication table $(c_{i,j,n})$ defined by

$$w_i \cdot w_j = \sum_{n=1}^{N} c_{i,j,n} \cdot w_n.$$

We define a new ring C containing K whose elements are the set of all expressions

$$\sum_{n=1}^{N} a_n \underline{w}_n$$

where the $\underline{w}_n$ have the same multiplication rule

$$\underline{w}_i \cdot \underline{w}_j = \sum_{n=1}^{N} c_{i,j,n} \cdot \underline{w}_n$$

as the w_n.

There are injective ring homomorphisms

$$i : A \hookrightarrow C, \qquad i(a) = a\underline{w}_1 \qquad \text{(note that } \underline{w}_1 = 1\text{)}$$

and

$$j : B \hookrightarrow C, \qquad j\left(\sum_{n=1}^{N} c_n w_n\right) = \sum_{n=1}^{N} c_n \underline{w}_n.$$

Moreover C is defined, up to isomorphism, by A and B and is independent of the particular choice of basis w_n of B (i.e., a change of basis of B induces a canonical isomorphism of the C defined by the first basis to the C defined by the second basis). We write

$$C = A \otimes_K B$$

since C is, in fact, a special case of the ring tensor product.

Let us now suppose, further, that A is a topological ring, i.e., has a topology with respect to which addition and multiplication are continuous. Then the map

$$C \to A \oplus \cdots \oplus A, \qquad \sum_{m=1}^{N} a_m \underline{w}_m \mapsto (a_1, \ldots, a_N)$$

defines a bijection between C and the product of N copies of A (considered as sets). We give C the product topology. It is readily verified that this topology is independent of the choice of basis $w_1, \ldots, w_N$ and that multiplication and addition on C are continuous, so C is a topological ring. We call this topology on C the *tensor product topology.*

Now drop our assumption that A and B have a topology, but suppose that A and B are not merely rings but fields. Recall that a finite extension L/K of fields is *separable* if the number of embeddings $L \hookrightarrow \overline{K}$ that fix K equals the degree of L over K, where $\overline{K}$ is an algebraic closure of K. The primitive element theorem from Galois theory asserts that any such extension is generated by a single element, i.e., $L = K(a)$ for some $a \in L$.

Lemma 18.2.1. *Let A and B be fields containing the field K and suppose that B is a separable extension of finite degree $N = [B : K]$. Then $C = A \otimes_K B$ is the direct sum of a finite number of fields K_j, each containing an isomorphic image of A and an isomorphic image of B.*

Proof. By the primitive element theorem, we have $B = K(b)$, where b is a root of some separable irreducible polynomial $f(x) \in K[x]$ of degree N. Then $1, b, \ldots, b^{N-1}$ is a basis for B over K, so

$$A \otimes_K B = A[\underline{b}] \cong A[x]/(f(x))$$

where $1, \underline{b}, \underline{b}^2, \ldots, \underline{b}^{N-1}$ are linearly independent over A and $\underline{b}$ satisfies $f(\underline{b}) = 0$.

Although the polynomial $f(x)$ is irreducible as an element of $K[x]$, it need not be irreducible in $A[x]$. Since A is a field, we have a factorization

$$f(x) = \prod_{j=1}^{J} g_j(x)$$

where $g_j(x) \in A[x]$ is irreducible. The $g_j(x)$ are distinct because $f(x)$ is separable (i.e., has distinct roots in any algebraic closure).

For each j, let $\underline{b}_j \in \overline{A}$ be a root of $g_j(x)$, where $\overline{A}$ is a fixed algebraic closure of the field A. Let $K_j = A(\underline{b}_j)$. Then the map

$$\varphi_j : A \otimes_K B \to K_j \tag{18.2.1}$$

given by sending any polynomial $h(\underline{b})$ in $\underline{b}$ (where $h \in A[x]$) to $h(\underline{b}_j)$ is a ring homomorphism, because the image of $\underline{b}$ satisfies the polynomial $f(x)$, and $A \otimes_K B \cong A[x]/(f(x))$.

By the Chinese Remainder Theorem, the maps from (18.2.1) combine to define a ring isomorphism

$$A \otimes_K B \cong A[x]/(f(x)) \cong \bigoplus_{j=1}^{J} A[x]/(g_j(x)) \cong \bigoplus_{j=1}^{J} K_j.$$

Each K_j is of the form $A[x]/(g_j(x))$, so contains an isomorphic image of A. It thus remains to show that the ring homomorphisms

$$\lambda_j : B \xrightarrow{b \mapsto 1 \otimes b} A \otimes_K B \xrightarrow{\varphi_j} K_j$$

are injections. Since B and K_j are both fields, λ_j is either the 0 map or injective. However, λ_j is not the 0 map since $\lambda_j(1) = 1 \in K_j$. $\square$

Example 18.2.2. If A and B are finite extensions of $\mathbf{Q}$, then $A \otimes_{\mathbf{Q}} B$ is an algebra of degree $[A : \mathbf{Q}] \cdot [B : \mathbf{Q}]$. For example, suppose A is generated by a root of $x^2 + 1$ and B is generated by a root of $x^3 - 2$. We can view $A \otimes_{\mathbf{Q}} B$ as either $A[x]/(x^3 - 2)$ or $B[x]/(x^2 + 1)$. The polynomial $x^2 + 1$ is irreducible over $\mathbf{Q}$, and if it factored over the cubic field B, then there would be a root of x^2+1 in B, i.e., the quadratic field $A = \mathbf{Q}(i)$ would be a subfield of the cubic field $B = \mathbf{Q}(\sqrt[3]{2})$, which is impossible. Thus $x^2 + 1$ is irreducible over B, so $A \otimes_{\mathbf{Q}} B = A.B = \mathbf{Q}(i, \sqrt[3]{2})$ is a degree 6 extension of $\mathbf{Q}$. Notice that $A.B$ contains a copy A and a copy of B. By the primitive element theorem the composite field $A.B$ can be generated by the root of a single polynomial. For example, the minimal polynomial of $i + \sqrt[3]{2}$ is $x^6 + 3x^4 - 4x^3 + 3x^2 + 12x + 5$, hence $\mathbf{Q}(i + \sqrt[3]{2}) = A.B$.

Example 18.2.3. The case $A \cong B$ is even more exciting. For example, suppose $A = B = \mathbf{Q}(i)$. Using the Chinese Remainder Theorem we have that

$$\mathbf{Q}(i) \otimes_{\mathbf{Q}} \mathbf{Q}(i) \cong \mathbf{Q}(i)[x]/(x^2 + 1) \cong \mathbf{Q}(i)[x]/((x - i)(x + i)) \cong \mathbf{Q}(i) \oplus \mathbf{Q}(i),$$

since $(x-i)$ and $(x+i)$ are coprime. The last isomorphism sends $a+bx$, with $a,b\in\mathbf{Q}(i)$, to $(a+bi,a-bi)$. Since $\mathbf{Q}(i)\oplus\mathbf{Q}(i)$ has zero divisors, the tensor product $\mathbf{Q}(i)\otimes_{\mathbf{Q}}\mathbf{Q}(i)$ must also have zero divisors. For example, $(1,0)$ and $(0,1)$ is a zero divisor pair on the right hand side, and we can trace back to the elements of the tensor product that they define. First, by solving the system

$$a+bi=1 \qquad \text{and} \qquad a-bi=0$$

we see that $(1,0)$ corresponds to $a=1/2$ and $b=-i/2$, i.e., to the element

$$\frac{1}{2}-\frac{i}{2}x\in\mathbf{Q}(i)[x]/(x^2+1).$$

This element in turn corresponds to

$$\frac{1}{2}\otimes 1-\frac{i}{2}\otimes i\in\mathbf{Q}(i)\otimes_{\mathbf{Q}}\mathbf{Q}(i).$$

Similarly the other element $(0,1)$ corresponds to

$$\frac{1}{2}\otimes 1+\frac{i}{2}\otimes i\in\mathbf{Q}(i)\otimes_{\mathbf{Q}}\mathbf{Q}(i).$$

As a double check, observe that

$$\begin{aligned}\left(\frac{1}{2}\otimes 1-\frac{i}{2}\otimes i\right)\cdot\left(\frac{1}{2}\otimes 1+\frac{i}{2}\otimes i\right)&=\frac{1}{4}\otimes 1+\frac{i}{4}\otimes i-\frac{i}{4}\otimes i-\frac{i^2}{4}\otimes i^2\\&=\frac{1}{4}\otimes 1-\frac{1}{4}\otimes 1=0\in\mathbf{Q}(i)\otimes_{\mathbf{Q}}\mathbf{Q}(i).\end{aligned}$$

Clearing the denominator of 2 and writing $1\otimes 1=1$, we have $(1-i\otimes i)(1+i\otimes i)=0$, so $i\otimes i$ is a root of the polynomimal x^2-1, and $i\otimes i$ is not ± 1, so x^2-1 has more than 2 roots.

In general, to understand $A\otimes_K B$ explicitly is the same as factoring either the defining polynomial of B over the field A, or factoring the defining polynomial of A over B.

Corollary 18.2.4. *Let $a\in B$ be any element and let $f(x)\in K[x]$ be the characteristic polynomials of a over K and let $g_j(x)\in A[x]$ (for $1\le j\le J$) be the characteristic polynomials of the images of a under $B\to A\otimes_K B\to K_j$ over A, respectively. Then*

$$f(x)=\prod_{j=1}^{J}g_j(X). \tag{18.2.2}$$

Proof. We show that both sides of (18.2.2) are the characteristic polynomial $T(x)$ of the image of a in $A\otimes_K B$ over A. That $f(x)=T(x)$ follows at once by computing the characteristic polynomial in terms of a basis $\underline{w}_1,\ldots,\underline{w}_N$ of $A\otimes_K B$, where $w_1,\ldots,w_N$ is a basis for B over K (this is because the matrix of left multiplication by b on $A \otimes_K B$ is exactly the same as the matrix of left multiplication on B, so the characteristic polynomial doesn't change). To see that $T(X) = \prod g_j(X)$, compute the action of the image of a in $A \otimes_K B$ with respect to a basis of

$$A \otimes_K B \cong \bigoplus_{j=1}^{J} K_j \tag{18.2.3}$$

composed of basis of the individual extensions K_j of A. The resulting matrix will be a block direct sum of submatrices, each of whose characteristic polynomials is one of the $g_j(X)$. Taking the product gives the claimed identity (18.2.2). $\square$

Corollary 18.2.5. *For $a \in B$ we have*

$$\mathrm{Norm}_{B/K}(a) = \prod_{j=1}^{J} \mathrm{Norm}_{K_j/A}(a),$$

and

$$\mathrm{Tr}_{B/K}(a) = \sum_{j=1}^{J} \mathrm{Tr}_{K_j/A}(a),$$

Proof. This follows from Corollary 18.2.4. First, the norm is $\pm$ the constant term of the characteristic polynomial, and the constant term of the product of polynomials is the product of the constant terms (and one sees that the sign matches up correctly). Second, the trace is minus the second coefficient of the characteristic polynomial, and second coefficients add when one multiplies polynomials:

$$(x^n + a_{n-1}x^{n-1} + \cdots) \cdot (x^m + a_{m-1}x^{m-1} + \cdots) = x^{n+m} + x^{n+m-1}(a_{m-1} + a_{n-1}) + \cdots .$$

One could also see both the statements by considering a matrix of left multiplication by a first with respect to the basis of $\underline{w}_n$ and second with respect to the basis coming from the left side of (18.2.3).

$\square$

Chapter 19

Extensions and Normalizations of Valuations

19.1 Extensions of Valuations

In this section we continue to tacitly assume that all valuations are nontrivial. We do not assume all our valuations satisfy the triangle

Suppose $K \subset L$ is a finite extension of fields, and that $|\cdot|$ and $\|\cdot\|$ are valuations on K and L, respectively.

Definition 19.1.1 (Extends). We say that $\|\cdot\|$ *extends* $|\cdot|$ if $|a| = \|a\|$ for all $a \in K$.

Theorem 19.1.2. *Suppose that K is a field that is complete with respect to $|\cdot|$ and that L is a finite extension of K of degree $N = [L : K]$. Then there is precisely one extension of $|\cdot|$ to K, namely*

$$\|a\| = \left|\mathrm{Norm}_{L/K}(a)\right|^{1/N}, \tag{19.1.1}$$

where the Nth root is the non-negative real Nth root of the nonnegative real number $\left|\mathrm{Norm}_{L/K}(a)\right|$.

Proof. We may assume that $|\cdot|$ is normalized so as to satisfy the triangle inequality. Otherwise, normalize $|\cdot|$ so that it does, prove the theorem for the normalized valuation $|\cdot|^c$, then raise both sides of (19.1.1) to the power $1/c$. In the uniqueness proof, by the same argument we may assume that $\|\cdot\|$ also satisfies the triangle inequality.

Uniqueness. View L as a finite-dimensional vector space over K. Then $\|\cdot\|$ is a norm in the sense defined earlier (Definition 18.1.1). Hence any two extensions $\|\cdot\|_1$ and $\|\cdot\|_2$ of $|\cdot|$ are equivalent as norms, so induce the same topology on K. But as we have seen (Proposition 16.1.4), two valuations which induce the same topology are equivalent valuations, i.e., $\|\cdot\|_1 = \|\cdot\|_2^c$, for some positive real c. Finally $c = 1$ since $\|a\|_1 = |a| = \|a\|_2$ for all $a \in K$.

Existence. We do not give a proof of existence in the general case. Instead we give a proof, which was suggested by Dr. Geyer at the conference out of which [Cas67] arose. It is valid when K is locally compact, which is the only case we will use later.

We see at once that the function defined in (19.1.1) satisfies the condition (i) that $\|a\| \geq 0$ with equality only for $a = 0$, and (ii) $\|ab\| = \|a\| \cdot \|b\|$ for all $a, b \in L$. The difficult part of the proof is to show that there is a constant $C > 0$ such that

$$\|a\| \leq 1 \implies \|1 + a\| \leq C.$$

Note that we do not know (and will not show) that $\|\cdot\|$ as defined by (19.1.1) is a norm as in Definition 18.1.1, since showing that $\|\cdot\|$ is a norm would entail showing that it satisfies the triangle inequality, which is not obvious.

Choose a basis $b_1, \ldots, b_N$ for L over K. Let $\|\cdot\|_0$ be the max norm on L, so for $a = \sum_{i=1}^N c_i b_i$ with $c_i \in K$ we have

$$\|a\|_0 = \left\| \sum_{i=1}^N c_i b_i \right\|_0 = \max\{|c_i| : i = 1, \ldots, N\}.$$

(Note: in Cassels's original article he let $\|\cdot\|_0$ be *any* norm, but we don't because the rest of the proof does not work, since we can't use homogeneity as he claims to do. This is because it need not be possible to find, for any nonzero $a \in L$ some element $c \in K$ such that $\|ac\|_0 = 1$. This would fail, e.g., if $\|a\|_0 \neq |c|$ for any $c \in K$.) The rest of the argument is very similar to our proof from Lemma 18.1.3 of uniqueness of norms on vector spaces over complete fields.

With respect to the $\|\cdot\|_0$-topology, L has the product topology as a product of copies of K. The function $a \mapsto \|a\|$ is a composition of continuous functions on L with respect to this topology (e.g., $\mathrm{Norm}_{L/K}$ is the determinant, hence polynomial), hence $\|\cdot\|$ defines nonzero continuous function on the compact set

$$S = \{a \in L : \|a\|_0 = 1\}.$$

By compactness, there are real numbers $\delta, \Delta \in \mathbf{R}_{>0}$ such that

$$0 < \delta \leq \|a\| \leq \Delta \qquad \text{for all } a \in S.$$

For any nonzero $a \in L$ there exists $c \in K$ such that $\|a\|_0 = |c|$; to see this take c to be a c_i in the expression $a = \sum_{i=1}^N c_i b_i$ with $|c_i| \geq |c_j|$ for any j. Hence $\|a/c\|_0 = 1$, so $a/c \in S$ and

$$0 \leq \delta \leq \frac{\|a/c\|}{\|a/c\|_0} \leq \Delta.$$

Then by homogeneity

$$0 \leq \delta \leq \frac{\|a\|}{\|a\|_0} \leq \Delta.$$

Suppose now that $\|a\| \le 1$. Then $\|a\|_0 \le \delta^{-1}$, so

$$\begin{aligned}\|1+a\| &\le \Delta \cdot \|1+a\|_0 \\ &\le \Delta \cdot (\|1\|_0 + \|a\|_0) \\ &\le \Delta \cdot \left(\|1\|_0 + \delta^{-1}\right) \\ &= C \quad \text{(say)},\end{aligned}$$

as required. $\square$

Example 19.1.3. Consider the extension $\mathbf{C}$ of $\mathbf{R}$ equipped with the archimedean valuation. The unique extension is the ordinary absolute value on $\mathbf{C}$:

$$\|x+iy\| = \left(x^2+y^2\right)^{1/2}.$$

Example 19.1.4. Consider the extension $\mathbf{Q}_2(\sqrt{2})$ of $\mathbf{Q}_2$ equipped with the 2-adic absolute value. Since x^2-2 is irreducible over $\mathbf{Q}_2$ we can do some computations by working in the subfield $\mathbf{Q}(\sqrt{2})$ of $\mathbf{Q}_2(\sqrt{2})$.

```
> K<a> := NumberField(x^2-2);
> K;
Number Field with defining polynomial x^2 - 2 over the Rational Field
> function norm(x) return Sqrt(2^(-Valuation(Norm(x),2))); end function;
> norm(1+a);
1.00000000000000000000000000000
> norm(1+a+1);
0.707106781186547524400844362109
> z := 3+2*a;
> norm(z);
1.00000000000000000000000000000
> norm(z+1);
0.353553390593273762200422181049
```

Remark 19.1.5. Geyer's existence proof gives (19.1.1). But it is perhaps worth noting that in any case (19.1.1) is a consequence of unique existence, as follows. Suppose L/K is as above. Suppose M is a finite Galois extension of K that contains L. Then by assumption there is a unique extension of $|\cdot|$ to M, which we shall also denote by $\|\cdot\|$. If $\sigma \in \mathrm{Gal}(M/K)$, then

$$\|a\|_\sigma := \|\sigma(a)\|$$

is also an extension of $|\cdot|$ to M, so $\|\cdot\|_\sigma = \|\cdot\|$, i.e.,

$$\|\sigma(a)\| = \|a\| \qquad \text{for all } a \in M.$$

But now

$$\mathrm{Norm}_{L/K}(a) = \sigma_1(a) \cdot \sigma_2(a) \cdots \sigma_N(a)$$

for $a \in K$, where $\sigma_1, \ldots, \sigma_N \in \mathrm{Gal}(M/K)$ extend the embeddings of L into M. Hence

$$\begin{aligned} \left|\mathrm{Norm}_{L/K}(a)\right| &= \left\|\mathrm{Norm}_{L/K}(a)\right\| \\ &= \prod_{1\leq n\leq N} \|\sigma_n(a)\| \\ &= \|a\|^N, \end{aligned}$$

as required.

Corollary 19.1.6. *Let $w_1, \ldots, w_N$ be a basis for L over K. Then there are positive constants c_1 and c_2 such that*

$$c_1 \leq \frac{\left\|\sum_{n=1}^{N} b_n w_n\right\|}{\max\{|b_n| : n = 1, \ldots, N\}} \leq c_2$$

for any $b_1, \ldots, b_N \in K$ not all 0.

Proof. For $\left|\sum_{n=1}^{N} b_n w_n\right|$ and $\max|b_n|$ are two norms on L considered as a vector space over K.

I don't believe this proof, which I copied from Cassels's article. My problem with it is that the proof of Theorem 19.1.2 does not give that $C \leq 2$, i.e., that the triangle inequality holds for $\|\cdot\|$. By changing the basis for L/K one can make any nonzero vector $a \in L$ have $\|a\|_0 = 1$, so if we choose a such that $|a|$ is very large, then the Δ in the proof will also be very large. One way to fix the corollary is to only claim that there are positive constants c_1, c_2, c_3, c_4 such that

$$c_1 \leq \frac{\left\|\sum_{n=1}^{N} b_n w_n\right\|^{c_3}}{\max\{|b_n|^{c_4} : n = 1, \ldots, N\}} \leq c_2.$$

Then choose c_3, c_4 such that $\|\cdot\|^{c_3}$ and $|\cdot|^{c_4}$ satisfies the triangle inequality, and prove the modified corollary using the proof suggested by Cassels. □

Corollary 19.1.7. *A finite extension of a completely valued field K is complete with respect to the extended valuation.*

Proof. By the proceeding corollary it has the topology of a finite-dimensional vector space over K. (The problem with the proof of the previous corollary is not an issue, because we can replace the extended valuation by an inequivalent one that satisfies the triangle inequality and induces the same topology.) □

When K is no longer complete under $|\cdot|$ the position is more complicated:

Theorem 19.1.8. *Let L be a separable extension of K of finite degree $N = [L : K]$. Then there are at most N extensions of a valuation $|\cdot|$ on K to L, say $\|\cdot\|_j$, for $1 \leq j \leq J$. Let K_v be the completion of K with respect to $|\cdot|$, and for each j let L_j be the completion of L with respect to $\|\cdot\|_j$. Then*

$$K_v \otimes_K L \cong \bigoplus_{1 \leq j \leq J} L_j \tag{19.1.2}$$

algebraically and topologically, where the right hand side is given the product topology.

Proof. We already know (Lemma 18.2.1) that $K_v \otimes_K L$ is of the shape (19.1.2), where the L_j are finite extensions of K_v. Hence there is a unique extension $|\cdot|_j^*$ of $|\cdot|$ to the L_j, and by Corollary 19.1.7 the L_j are complete with respect to the extended valuation. Further, the ring homomorphisms

$$\lambda_j : L \to K_v \otimes_K L \to L_j$$

are injections. Hence we get an extension $\|\cdot\|_j$ of $|\cdot|$ to L by putting

$$\|b\|_j = |\lambda_j(b)|_j^* .$$

Further, $L \cong \lambda_j(L)$ is dense in L_j with respect to $\|\cdot\|_j$ because $L = K \otimes_K L$ is dense in $K_v \otimes_K L$ (since K is dense in K_v). Hence L_j is exactly the completion of L.

It remains to show that the $\|\cdot\|_j$ are distinct and that they are the only extensions of $|\cdot|$ to L.

Suppose $\|\cdot\|$ is any valuation of L that extends $|\cdot|$. Then $\|\cdot\|$ extends by continuity to a real-valued function on $K_v \otimes_K L$, which we also denote by $\|\cdot\|$. (We are again using that L is dense in $K_v \otimes_K L$.) By continuity we have for all $a, b \in K_v \otimes_K L$,

$$\|ab\| = \|a\| \cdot \|b\|$$

and if C is the constant in axiom (iii) for L and $\|\cdot\|$, then

$$\|a\| \leq 1 \implies \|1 + a\| \leq C.$$

(In Cassels, he inexplicable assume that $C = 1$ at this point in the proof.)

We consider the restriction of $\|\cdot\|$ to one of the L_j. If $\|a\| \neq 0$ for some $a \in L_j$, then $\|a\| = \|b\| \cdot \left\|ab^{-1}\right\|$ for every $b \neq 0$ in L_j so $\|b\| \neq 0$. Hence either $\|\cdot\|$ is identically 0 on L_j or it induces a valuation on L_j.

Further, $\|\cdot\|$ cannot induce a valuation on two of the L_j. For

$$(a_1, 0, \ldots, 0) \cdot (0, a_2, 0, \ldots, 0) = (0, 0, 0, \ldots, 0),$$

so for any $a_1 \in L_1$, $a_2 \in L_2$,

$$\|a_1\| \cdot \|a_2\| = 0.$$

Hence $\|\cdot\|$ induces a valuation in precisely one of the L_j, and it extends the given valuation $|\cdot|$ of K_v. Hence $\|\cdot\| = \|\cdot\|_j$ for precisely one j.

It remains only to show that (19.1.2) is a topological homomorphism. For

$$(b_1, \ldots, b_J) \in L_1 \oplus \cdots \oplus L_J$$

put

$$\|(b_1, \ldots, b_J)\|_0 = \max_{1 \le j \le J} \|b_j\|_j .$$

Then $\|\cdot\|_0$ is a norm on the right hand side of (19.1.2), considered as a vector space over K_v and it induces the product topology. On the other hand, any two norms are equivalent, since K_v is complete, so $\|\cdot\|_0$ induces the tensor product topology on the left hand side of (19.1.2). □

Corollary 19.1.9. *Suppose $L = K(a)$, and let $f(x) \in K[x]$ be the minimal polynomial of a. Suppose that*

$$f(x) = \prod_{1 \le j \le J} g_j(x)$$

in $K_v[x]$, where the g_j are irreducible. Then $L_j = K_v(b_j)$, where b_j is a root of g_j.

19.2 Extensions of Normalized Valuations

Let K be a complete field with valuation $|\cdot|$. We consider the following three cases:

(1) $|\cdot|$ is discrete non-archimedean and the residue class field is finite.

(2i) The completion of K with respect to $|\cdot|$ is $\mathbf{R}$.

(2ii) The completion of K with respect to $|\cdot|$ is $\mathbf{C}$.

(Alternatively, these cases can be subsumed by the hypothesis that the completion of K is locally compact.)

In case (1) we defined the normalized valuation to be the one such that if Haar measure of the ring of integers $\mathcal{O}$ is 1, then $\mu(a\mathcal{O}) = |a|$ (see Definition 17.1.11). In case (2i) we say that $|\cdot|$ is normalized if it is the ordinary absolute value, and in (2ii) if it is the *square* of the ordinary absolute value:

$$|x + iy| = x^2 + y^2 \qquad \text{(normalized)}.$$

In every case, for every $a \in K$, the map

$$a : x \mapsto ax$$

on K^+ multiplies any choice of Haar measure by $|a|$, and this characterizes the normalized valuations among equivalent ones.

We have already verified the above characterization for non-archimedean valuations, and it is clear for the ordinary absolute value on $\mathbf{R}$, so it remains to verify it for $\mathbf{C}$. The additive group $\mathbf{C}^+$ is topologically isomorphic to $\mathbf{R}^+ \oplus \mathbf{R}^+$, so a choice of Haar measure of $\mathbf{C}^+$ is the usual area measure on the Euclidean plane. Multiplication by $x+iy \in \mathbf{C}$ is the same as rotation followed by scaling by a factor of $\sqrt{x^2+y^2}$, so if we rescale a region by a factor of $x+iy$, the area of the region changes by a factor of the square of $\sqrt{x^2+y^2}$. This explains why the normalized valuation on $\mathbf{C}$ is the square of the usual absolute value. Note that the normalized valuation on $\mathbf{C}$ does not satisfy the triangle inequality:

$$|1+(1+i)| = |2+i| = 2^2+1^2 = 5 \not\leq 3 = 1^2 + (1^2+1^2) = |1| + |1+i|.$$

The constant C in axiom (3) of a valuation for the ordinary absolute value on $\mathbf{C}$ is 2, so the constant for the normalized valuation $|\cdot|$ is $C \leq 4$:

$$|x+iy| \leq 1 \implies |x+iy+1| \leq 4.$$

Note that $x^2+y^2 \leq 1$ implies

$$(x+1)^2 + y^2 = x^2 + 2x + 1 + y^2 \leq 1 + 2x + 1 \leq 4$$

since $x \leq 1$.

Lemma 19.2.1. *Suppose K is a field that is complete with respect to a normalized valuation $|\cdot|$ and let L be a finite extension of K of degree $N = [L:K]$. Then the normalized valuation $\|\cdot\|$ on L which is equivalent to the unique extension of $|\cdot|$ to L is given by the formula*

$$\|a\| = \left|\mathrm{Norm}_{L/K}(a)\right| \qquad \text{all } a \in L. \tag{19.2.1}$$

Proof. Let $\|\cdot\|$ be the normalized valuation on L that extends $|\cdot|$. Our goal is to identify $\|\cdot\|$, and in particular to show that it is given by (19.2.1).

By the preceding section there is a positive real number c such that for all $a \in L$ we have

$$\|a\| = \left|\mathrm{Norm}_{L/K}(a)\right|^c.$$

Thus all we have to do is prove that $c = 1$. In case 2 the only nontrivial situation is $L = \mathbf{C}$ and $K = \mathbf{R}$, in which case $\left|\mathrm{Norm}_{\mathbf{C}/\mathbf{R}}(x+iy)\right| = \left|x^2+y^2\right|$, which is the normalized valuation on $\mathbf{C}$ defined above.

One can argue in a unified way in all cases as follows. Let $w_1, \ldots, w_N$ be a basis for L/K. Then the map

$$\varphi : L^+ \to \bigoplus_{n=1}^{N} K^+, \qquad \sum a_n w_n \mapsto (a_1, \ldots, a_N)$$

is an isomorphism between the additive group L^+ and the direct sum $\oplus_{n=1}^N K^+$, and this is a homeomorphism if the right hand side is given the product topology. In particular, the Haar measures on L^+ and on $\oplus_{n=1}^N K^+$ are the same up to a multiplicative constant in $\mathbf{Q}^*$.

Let $b \in K$. Then the left-multiplication-by-b map

$$b : \sum a_n w_n \mapsto \sum b a_n w_n$$

on L^+ is the same as the map

$$(a_1, \ldots, a_N) \mapsto (ba_1, \ldots, ba_N)$$

on $\oplus_{n=1}^N K^+$, so it multiplies the Haar measure by $|b|^N$, since $|\cdot|$ on K is assumed normalized (the measure of each factor is multiplied by $|b|$, so the measure on the product is multiplied by $|b|^N$). Since $\|\cdot\|$ is assumed normalized, so multiplication by b rescales by $\|b\|$, we have

$$\|b\| = |b|^N .$$

But $b \in K$, so $\mathrm{Norm}_{L/K}(b) = b^N$. Since $|\cdot|$ is nontrivial and for $a \in K$ we have

$$\|a\| = |a|^N = \left|a^N\right| = \left|\mathrm{Norm}_{L/K}(a)\right| ,$$

so we must have $c = 1$ in (19.2.1), as claimed. □

In the case when K need not be complete with respect to the valuation $|\cdot|$ on K, we have the following theorem.

Theorem 19.2.2. *Suppose $|\cdot|$ is a (nontrivial as always) normalized valuation of a field K and let L be a finite extension of K. Then for any $a \in L$,*

$$\prod_{1 \le j \le J} \|a\|_j = \left|\mathrm{Norm}_{L/K}(a)\right|$$

where the $\|\cdot\|_j$ are the normalized valuations equivalent to the extensions of $|\cdot|$ to K.

Proof. Let K_v denote the completion of K with respect to $|\cdot|$. Write

$$K_v \otimes_K L = \bigoplus_{1 \le j \le J} L_j .$$

Then Theorem 19.2.2 asserts that

$$\mathrm{Norm}_{L/K}(a) = \prod_{1 \le j \le J} \mathrm{Norm}_{L_j/K_v}(a). \tag{19.2.2}$$

By Theorem 19.1.8, the $\|\cdot\|_j$ are exactly the normalizations of the extensions of $|\cdot|$ to the L_j (i.e., the L_j are in bijection with the extensions of valuations, so there are no other valuations missed). By Lemma 19.1.1, the normalized valuation $\|\cdot\|_j$ on L_j is $|a| = \left|\mathrm{Norm}_{L_J/K_v}(a)\right|$. The theorem now follows by taking absolute values of both sides of (19.2.2). □

What next?! We'll building up to giving a new proof of finiteness of the class group that uses that the class group naturally has the discrete topology and is the continuous image of a compact group.

Chapter 20

Global Fields and Adeles

20.1 Global Fields

Definition 20.1.1 (Global Field). A *global field* is a number field or a finite separable extension of $\mathbf{F}(t)$, where $\mathbf{F}$ is a finite field, and t is transcendental over $\mathbf{F}$.

Below we will focus attention on number fields leaving the function field case to the reader.

The following lemma essentially says that the denominator of an element of a global field is only "nontrivial" at a finite number of valuations.

Lemma 20.1.2. *Let $a \in K$ be a nonzero element of a global field K. Then there are only finitely many inequivalent valuations $|\cdot|$ of K for which*

$$|a| > 1.$$

Proof. If $K = \mathbf{Q}$ or $\mathbf{F}(t)$ then the lemma follows by Ostrowski's classification of all the valuations on K (see Theorem 15.3.2). For example, when $a = \frac{n}{d} \in \mathbf{Q}$, with $n, d \in \mathbf{Z}$, then the valuations where we could have $|a| > 1$ are the archimedean one, or the p-adic valuations $|\cdot|_p$ for which $p \mid d$.

Suppose now that K is a finite extension of $\mathbf{Q}$, so a satisfies a monic polynomial

$$a^n + c_{n-1}a^{n-1} + \cdots + c_0 = 0,$$

for some n and $c_0, \ldots, c_{n-1} \in \mathbf{Q}$. If $|\cdot|$ is a non-archimedean valuation on K, we have

$$\begin{aligned} |a|^n &= \left|-(c_{n-1}a^{n-1} + \cdots + c_0)\right| \\ &\leq \max(1, |a|^{n-1}) \cdot \max(|c_0|, \ldots, |c_{n-1}|). \end{aligned}$$

Dividing each side by $|a|^{n-1}$, we have that

$$|a| \leq \max(|c_0|, \ldots, |c_{n-1}|),$$

so in all cases we have

$$|a| \leq \max(1, |c_0|, \ldots, |c_{n-1}|)^{1/(n-1)}. \qquad (20.1.1)$$

We know the lemma for $\mathbf{Q}$, so there are only finitely many valuations $|\cdot|$ on $\mathbf{Q}$ such that the right hand side of (20.1.1) is bigger than 1. Since each valuation of $\mathbf{Q}$ has finitely many extensions to K, and there are only finitely many archimedean valuations, it follows that there are only finitely many valuations on K such that $|a| > 1$. $\square$

Any valuation on a global field is either archimedean, or discrete non-archimedean with finite residue class field, since this is true of $\mathbf{Q}$ and $\mathbf{F}(t)$ and is a property preserved by extending a valuation to a finite extension of the base field. Hence it makes sense to talk of normalized valuations. Recall that the normalized p-adic valuation on $\mathbf{Q}$ is $|x|_p = p^{-\operatorname{ord}_p(x)}$, and if v is a valuation on a number field K equivalent to an extension of $|\cdot|_p$, then the normalization of v is the composite of the sequence of maps

$$K \hookrightarrow K_v \xrightarrow{\text{Norm}} \mathbf{Q}_p \xrightarrow{|\cdot|_p} \mathbf{R},$$

where K_v is the completion of K at v.

Example 20.1.3. Let $K = \mathbf{Q}(\sqrt{2})$, and let $p = 2$. Because $\sqrt{2} \notin \mathbf{Q}_2$, there is exactly one extension of $|\cdot|_2$ to K, and it sends $a = 1/\sqrt{2}$ to

$$\left|\text{Norm}_{\mathbf{Q}_2(\sqrt{2})/\mathbf{Q}_2}(1/\sqrt{2})\right|_2^{1/2} = \sqrt{2}.$$

Thus the normalized valuation of a is 2.

There are two extensions of $|\cdot|_7$ to $\mathbf{Q}(\sqrt{2})$, since $\mathbf{Q}(\sqrt{2}) \otimes_{\mathbf{Q}} \mathbf{Q}_7 \cong \mathbf{Q}_7 \oplus \mathbf{Q}_7$, as $x^2 - 2 = (x-3)(x-4) \pmod{7}$. The image of $\sqrt{2}$ under each embedding into $\mathbf{Q}_7$ is a unit in $\mathbf{Z}_7$, so the normalized valuation of $a = 1/\sqrt{2}$ is, in both cases, equal to 1. More generally, for any valuation of K of characteristic an odd prime p, the normalized valuation of a is 1.

Since $K = \mathbf{Q}(\sqrt{2}) \hookrightarrow \mathbf{R}$ in two ways, there are exactly two normalized archimedean valuations on K, and both of their values on a equal $1/\sqrt{2}$. Notice that the product of the absolute values of a with respect to all normalized valuations is

$$2 \cdot \frac{1}{\sqrt{2}} \cdot \frac{1}{\sqrt{2}} \cdot 1 \cdot 1 \cdot 1 \cdots = 1.$$

This "product formula" holds in much more generality, as we will now see.

Theorem 20.1.4 (Product Formula). *Let $a \in K$ be a nonzero element of a global field K. Let $|\cdot|_v$ run through the normalized valuations of K. Then $|a|_v = 1$ for almost all v, and*

$$\prod_{\text{all } v} |a|_v = 1 \qquad \text{(the product formula)}.$$

We will later give a more conceptual proof of this using Haar measure (see Remark 20.3.9).

Proof. By Lemma 20.1.2, we have $|a|_v \leq 1$ for almost all v. Likewise, $1/|a|_v = |1/a|_v \leq 1$ for almost all v, so $|a|_v = 1$ for almost all v.

Let w run through all normalized valuations of $\mathbf{Q}$ (or of $\mathbf{F}(t)$), and write $v \mid w$ if the restriction of v to $\mathbf{Q}$ is equivalent to w. Then by Theorem 19.2.2,

$$\prod_v |a|_v = \prod_w \left(\prod_{v|w} |a|_v\right) = \prod_w \left|\mathrm{Norm}_{K/\mathbf{Q}}(a)\right|_w,$$

so it suffices to prove the theorem for $K = \mathbf{Q}$.

By multiplicativity of valuations, if the theorem is true for b and c then it is true for the product bc and quotient b/c (when $c \neq 0$). The theorem is clearly true for -1, which has valuation 1 at all valuations. Thus to prove the theorem for $\mathbf{Q}$ it suffices to prove it when $a = p$ is a prime number. Then we have $|p|_\infty = p$, $|p|_p = 1/p$, and for primes $q \neq p$ that $|p|_q = 1$. Thus

$$\prod_v |p|_v = p \cdot \frac{1}{p} \cdot 1 \cdot 1 \cdot 1 \cdots = 1,$$

as claimed. □

If v is a valuation on a field K, recall that we let K_v denote the completion of K with respect to v. Also when v is non-archimedean, let

$$\mathcal{O}_v = \mathcal{O}_{K,v} = \{x \in K_v : |x| \leq 1\}$$

be the ring of integers of the completion.

Definition 20.1.5 (Almost All). We say a condition holds for *almost all* elements of a set if it holds for all but finitely many elements.

We will use the following lemma later (see Lemma 20.3.3) to prove that formation of the adeles of a global field is compatible with base change.

Lemma 20.1.6. *Let $\omega_1, \ldots, \omega_n$ be a basis for L/K, where L is a finite separable extension of the global field K of degree n. Then for almost all normalized non-archimedean valuations v on K we have*

$$\omega_1 \mathcal{O}_v \oplus \cdots \oplus \omega_n \mathcal{O}_v = \mathcal{O}_{w_1} \oplus \cdots \oplus \mathcal{O}_{w_g} \subset K_v \otimes_K L, \tag{20.1.2}$$

where $w_1, \ldots, w_g$ are the extensions of v to L. Here we have identified $a \in L$ with its canonical image in $K_v \otimes_K L$, and the direct sum on the left is the sum taken inside the tensor product (so directness means that the intersections are trivial).

Proof. The proof proceeds in two steps. First we deduce easily from Lemma 20.1.2 that for almost all v the left hand side of (20.1.2) is contained in the right hand side. Then we use a trick involving discriminants to show the opposite inclusion for all but finitely many primes.

Since $\mathcal{O}_v \subset \mathcal{O}_{w_i}$ for all i, the left hand side of (20.1.2) is contained in the right hand side if $|\omega_i|_{w_j} \leq 1$ for $1 \leq i \leq n$ and $1 \leq j \leq g$. Thus by Lemma 20.1.2, for all but finitely many v the left hand side of (20.1.2) is contained in the right hand side. We have just eliminated the finitely many primes corresponding to "denominators" of some ω_i, and now only consider v such that $\omega_1, \ldots, \omega_n \in \mathcal{O}_w$ for all $w \mid v$.

For any elements $a_1, \ldots, a_n \in K_v \otimes_K L$, consider the discriminant

$$D(a_1, \ldots, a_n) = \mathrm{Det}(\mathrm{Tr}(a_i a_j)) \in K_v,$$

where the trace is induced from the L/K trace. Since each ω_i is in each $\mathcal{O}_w$, for $w \mid v$, the traces lie in $\mathcal{O}_v$, so

$$d = D(\omega_1, \ldots, \omega_n) \in \mathcal{O}_v.$$

Also note that $d \in K$ since each ω_i is in L. Now suppose that

$$\alpha = \sum_{i=1}^{n} a_i \omega_i \in \mathcal{O}_{w_1} \oplus \cdots \oplus \mathcal{O}_{w_g},$$

with $a_i \in K_v$. Then by properties of determinants for any m with $1 \leq m \leq n$, we have

$$D(\omega_1, \ldots, \omega_{m-1}, \alpha, \omega_{m+1}, \ldots, \omega_n) = a_m^2 D(\omega_1, \ldots, \omega_n). \tag{20.1.3}$$

The left hand side of (20.1.3) is in $\mathcal{O}_v$, so the right hand side is well, i.e.,

$$a_m^2 \cdot d \in \mathcal{O}_v, \qquad (\text{for } m = 1, \ldots, n),$$

where $d \in K$. Since $\omega_1, \ldots, \omega_n$ are a basis for L over K and the trace pairing is nondegenerate, we have $d \neq 0$, so by Theorem 20.1.4 we have $|d|_v = 1$ for all but finitely many v. Then for all but finitely many v we have that $a_m^2 \in \mathcal{O}_v$. For these v, that $a_m^2 \in \mathcal{O}_v$ implies $a_m \in \mathcal{O}_v$ since $a_m \in K_v$, i.e., α is in the left hand side of (20.1.2). ∎

Example 20.1.7. Let $K = \mathbf{Q}$ and $L = \mathbf{Q}(\sqrt{2})$. Let $\omega_1 = 1/3$ and $\omega_2 = 2\sqrt{2}$. In the first stage of the above proof we would eliminate $|\cdot|_3$ because ω_2 is not integral at 3. The discriminant is

$$d = D\left(\frac{1}{3}, 2\sqrt{2}\right) = \mathrm{Det}\begin{pmatrix} \frac{2}{9} & 0 \\ 0 & 16 \end{pmatrix} = \frac{32}{9}.$$

As explained in the second part of the proof, as long as $v \neq 2, 3$, we have equality of the left and right hand sides in (20.1.2).

20.2 Restricted Topological Products

In this section we describe a topological tool, which we need in order to define adeles (see Definition 20.3.1).

Definition 20.2.1 (Restricted Topological Products). Let X_λ, for $\lambda \in \Lambda$, be a family of topological spaces, and for almost all λ let $Y_\lambda \subset X_\lambda$ be an open subset of X_λ. Consider the space X whose elements are sequences $\mathbf{x} = \{x_\lambda\}_{\lambda\in\Lambda}$, where $x_\lambda \in X_\lambda$ for every λ, and $x_\lambda \in Y_\lambda$ for almost all λ. We give X a topology by taking as a basis of open sets the sets $\prod U_\lambda$, where $U_\lambda \subset X_\lambda$ is open for all λ, and $U_\lambda = Y_\lambda$ for almost all λ. We call X with this topology the *restricted topological product* of the X_λ with respect to the Y_λ.

Corollary 20.2.2. *Let S be a finite subset of Λ, and let X_S be the set of $\mathbf{x} \in X$ with $x_\lambda \in Y_\lambda$ for all $\lambda \notin S$, i.e.,*

$$X_S = \prod_{\lambda\in S} X_\lambda \times \prod_{\lambda\notin S} Y_\lambda \subset X.$$

Then X_S is an open subset of X, and the topology induced on X_S as a subset of X is the same as the product topology.

The restricted topological product depends on the totality of the Y_λ, but not on the individual Y_λ:

Lemma 20.2.3. *Let $Y'_\lambda \subset X_\lambda$ be open subsets, and suppose that $Y_\lambda = Y'_\lambda$ for almost all λ. Then the restricted topological product of the X_λ with respect to the Y'_λ is canonically isomorphic to the restricted topological product with respect to the Y_λ.*

Lemma 20.2.4. *Suppose that the X_λ are locally compact and that the Y_λ are compact. Then the restricted topological product X of the X_λ is locally compact.*

Proof. For any finite subset S of Λ, the open subset $X_S \subset X$ is locally compact, because by Lemma 20.2.2 it is a product of finitely many locally compact sets with an infinite product of compact sets. (Here we are using Tychonoff's theorem from topology, which asserts that an arbitrary product of compact topological spaces is compact (see Munkres's *Topology, a first course*, chapter 5).) Since $X = \cup_S X_S$, and the X_S are open in X, the result follows. $\square$

The following measure will be extremely important in deducing topological properties of the ideles, which will be used in proving finiteness of class groups. See, e.g., the proof of Lemma 20.4.1, which is a key input to the proof of strong approximation (Theorem 20.4.4).

Definition 20.2.5 (Product Measure). For all $\lambda \in \Lambda$, suppose μ_λ is a measure on X_λ with $\mu_\lambda(Y_\lambda) = 1$ when Y_λ is defined. We define the *product measure* μ on X to be that for which a basis of measurable sets is

$$\prod_\lambda M_\lambda$$

where each $M_\lambda \subset X_\lambda$ has finite μ_λ-measure and $M_\lambda = Y_\lambda$ for almost all λ, and where

$$\mu\left(\prod_\lambda M_\lambda\right) = \prod_\lambda \mu_\lambda(M_\lambda).$$

20.3 The Adele Ring

Let K be a global field. For each normalization $|\cdot|_v$ of K, let K_v denote the completion of K. If $|\cdot|_v$ is non-archimedean, let $\mathcal{O}_v$ denote the ring of integers of K_v.

Definition 20.3.1 (Adele Ring). The *adele ring* $\mathbb{A}_K$ of K is the topological ring whose underlying topological space is the restricted topological product of the K_v with respect to the $\mathcal{O}_v$, and where addition and multiplication are defined componentwise:

$$(\mathbf{xy})_v = \mathbf{x}_v\mathbf{y}_v \qquad (\mathbf{x}+\mathbf{y})_v = \mathbf{x}_v + \mathbf{y}_v \qquad \text{for } \mathbf{x}, \mathbf{y} \in \mathbb{A}_K. \tag{20.3.1}$$

It is readily verified that (i) this definition makes sense, i.e., if $\mathbf{x}, \mathbf{y} \in \mathbb{A}_K$, then $\mathbf{xy}$ and $\mathbf{x}+\mathbf{y}$, whose components are given by (20.3.1), are also in $\mathbb{A}_K$, and (ii) that addition and multiplication are continuous in the $\mathbb{A}_K$-topology, so $\mathbb{A}_K$ is a topological ring, as asserted. Also, Lemma 20.2.4 implies that $\mathbb{A}_K$ is locally compact because the K_v are locally compact (Corollary 17.1.6), and the $\mathcal{O}_v$ are compact (Theorem 17.1.4).

There is a natural continuous ring inclusion

$$K \hookrightarrow \mathbb{A}_K \tag{20.3.2}$$

that sends $x \in K$ to the adele every one of whose components is x. This is an adele because $x \in \mathcal{O}_v$ for almost all v, by Lemma 20.1.2. The map is injective because each map $K \to K_v$ is an inclusion.

Definition 20.3.2 (Principal Adeles). The image of (20.3.2) is the ring of *principal adeles*.

It will cause no trouble to identify K with the principal adeles, so we shall speak of K as a subring of $\mathbb{A}_K$.

Formation of the adeles is compatibility with base change, in the following sense.

Lemma 20.3.3. *Suppose L is a finite (separable) extension of the global field K. Then*
$$\mathbb{A}_K \otimes_K L \cong \mathbb{A}_L \tag{20.3.3}$$
both algebraically and topologically. Under this isomorphism,
$$L \cong K \otimes_K L \subset \mathbb{A}_K \otimes_K L$$
maps isomorphically onto $L \subset \mathbb{A}_L$.

Proof. Let $\omega_1, \ldots, \omega_n$ be a basis for L/K and let v run through the normalized valuations on K. The left hand side of (20.3.3), with the tensor product topology, is the restricted product of the tensor products
$$K_v \otimes_K L \cong K_v \cdot \omega_1 \oplus \cdots \oplus K_v \cdot \omega_n$$
with respect to the integers
$$\mathcal{O}_v \cdot \omega_1 \oplus \cdots \oplus \mathcal{O}_v \cdot \omega_n. \tag{20.3.4}$$
(An element of the left hand side is a finite linear combination $\sum \mathbf{x}_i \otimes a_i$ of adeles $\mathbf{x}_i \in \mathbb{A}_K$ and coefficients $a_i \in L$, and there is a natural isomorphism from the ring of such formal sums to the restricted product of the $K_v \otimes_K L$.)

We proved before (Theorem 19.1.8) that
$$K_v \otimes_K L \cong L_{w_1} \oplus \cdots \oplus L_{w_g},$$
where $w_1, \ldots, w_g$ are the normalizations of the extensions of v to L. Furthermore, as we proved using discriminants (see Lemma 20.1.6), the above identification identifies (20.3.4) with
$$\mathcal{O}_{L_{w_1}} \oplus \cdots \oplus \mathcal{O}_{L_{w_g}},$$
for almost all v. Thus the left hand side of (20.3.3) is the restricted product of the $L_{w_1} \oplus \cdots \oplus L_{w_g}$ with respect to the $\mathcal{O}_{L_{w_1}} \oplus \cdots \oplus \mathcal{O}_{L_{w_g}}$. But this is canonically isomorphic to the restricted product of all completions L_w with respect to $\mathcal{O}_w$, which is the right hand side of (20.3.3). This establishes an isomorphism between the two sides of (20.3.3) as topological spaces. The map is also a ring homomorphism, so the two sides are algebraically isomorphic, as claimed. $\square$

Corollary 20.3.4. *Let $\mathbb{A}_K^+$ denote the topological group obtained from the additive structure on $\mathbb{A}_K$. Suppose L is a finite seperable extension of K. Then*
$$\mathbb{A}_L^+ = \mathbb{A}_K^+ \oplus \cdots \oplus \mathbb{A}_K^+, \qquad ([L:K] \textit{ summands}).$$
In this isomorphism the additive group $L^+ \subset \mathbb{A}_L^+$ of the principal adeles is mapped isomorphically onto $K^+ \oplus \cdots \oplus K^+$.

Proof. For any nonzero $\omega \in L$, the subgroup $\omega \cdot \mathbb{A}_K^+$ of $\mathbb{A}_L^+$ is isomorphic as a topological group to $\mathbb{A}_K^+$ (the isomorphism is multiplication by $1/\omega$). By Lemma 20.3.3, we have isomorphisms

$$\mathbb{A}_L^+ = \mathbb{A}_K^+ \otimes_K L \cong \omega_1 \cdot \mathbb{A}_K^+ \oplus \cdots \oplus \omega_n \cdot \mathbb{A}_K^+ \cong \mathbb{A}_K^+ \oplus \cdots \oplus \mathbb{A}_K^+.$$

If $a \in L$, write $a = \sum b_i \omega_i$, with $b_i \in K$. Then a maps via the above map to

$$x = (\omega_1 \cdot \{b_1\}, \ldots, \omega_n \cdot \{b_n\}),$$

where $\{b_i\}$ denotes the principal adele defined by b_i. Under the final map, x maps to the tuple

$$(b_1, \ldots, b_n) \in K \oplus \cdots \oplus K \subset \mathbb{A}_K^+ \oplus \cdots \oplus \mathbb{A}_K^+.$$

The dimensions of L and of $K \oplus \cdots \oplus K$ over K are the same, so this proves the final claim of the corollary. $\square$

Theorem 20.3.5. *The global field K is discrete in $\mathbb{A}_K$ and the quotient $\mathbb{A}_K^+/K^+$ of additive groups is compact in the quotient topology.*

At this point Cassels remarks

> "It is impossible to conceive of any other uniquely defined topology on K. This metamathematical reason is more persuasive than the argument that follows!"

Proof. Corollary 20.3.4, with K for L and $\mathbf{Q}$ or $\mathbf{F}(t)$ for K, shows that it is enough to verify the theorem for $\mathbf{Q}$ or $\mathbf{F}(t)$, and we shall do it here for $\mathbf{Q}$.

To show that $\mathbf{Q}^+$ is discrete in $\mathbb{A}_{\mathbf{Q}}^+$ it is enough, because of the group structure, to find an open set U that contains $0 \in \mathbb{A}_{\mathbf{Q}}^+$, but which contains no other elements of $\mathbf{Q}^+$. (If $\alpha \in \mathbf{Q}^+$, then $U + \alpha$ is an open subset of $\mathbb{A}_{\mathbf{Q}}^+$ whose intersection with $\mathbf{Q}^+$ is $\{\alpha\}$.) We take for U the set of $\mathbf{x} = \{x_v\}_v \in \mathbb{A}_{\mathbf{Q}}^+$ with

$$|x_\infty|_\infty < 1 \qquad \text{and} \qquad |x_p|_p \leq 1 \quad (\text{all } p),$$

where $|\cdot|_p$ and $|\cdot|_\infty$ are respectively the p-adic and the usual archimedean absolute values on $\mathbf{Q}$. If $b \in \mathbf{Q} \cap U$, then in the first place $b \in \mathbf{Z}$ because $|b|_p \leq 1$ for all p, and then $b = 0$ because $|b|_\infty < 1$. This proves that K^+ is discrete in $\mathbb{A}_{\mathbf{Q}}^+$. (If we leave out one valuation, as we will see later (Theorem 20.4.4), this theorem is false—what goes wrong with the proof just given?)

Next we prove that the quotient $\mathbb{A}_{\mathbf{Q}}^+/\mathbf{Q}^+$ is compact. Let $W \subset \mathbb{A}_{\mathbf{Q}}^+$ consist of the $\mathbf{x} = \{x_v\}_v \in \mathbb{A}_{\mathbf{Q}}^+$ with

$$|x_\infty|_\infty \leq \frac{1}{2} \qquad \text{and} \qquad |x_p|_p \leq 1 \qquad \text{for all primes } p.$$

We show that every adele $\mathbf{y} = \{y_v\}_v$ is of the form

$$\mathbf{y} = a + \mathbf{x}, \qquad a \in \mathbf{Q}, \quad \mathbf{x} \in W,$$

which will imply that the compact set W maps surjectively onto $\mathbb{A}_{\mathbf{Q}}^{+}/\mathbf{Q}^{+}$. Fix an adele $\mathbf{y} = \{y_v\} \in \mathbb{A}_{\mathbf{Q}}^{+}$. Since $\mathbf{y}$ is an adele, for each prime p we can find a rational number

$$r_p = \frac{z_p}{p^{n_p}} \qquad \text{with} \quad z_p \in \mathbf{Z} \quad \text{and} \quad n_p \in \mathbf{Z}_{\geq 0}$$

such that

$$|y_p - r_p|_p \leq 1,$$

and

$$r_p = 0 \qquad \text{almost all } p.$$

More precisely, for the finitely many p such that

$$y_p = \sum_{n \geq -|s|} a_n p^n \notin \mathbf{Z}_p,$$

choose r_p to be a rational number that is the value of an appropriate truncation of the p-adic expansion of y_p, and when $y_p \in \mathbf{Z}_p$ just choose $r_p = 0$. Hence $r = \sum_p r_p \in \mathbf{Q}$ is well defined. The r_q for $q \neq p$ do not mess up the inequality $|y_p - r|_p \leq 1$ since the valuation $|\cdot|_p$ is non-archimedean and the r_q do not have any p in their denominator:

$$|y_p - r|_p = \left| y_p - r_p - \sum_{q \neq p} r_q \right|_p \leq \max\left(|y_p - r_p|_p, \left| \sum_{q \neq p} r_q \right|_p \right) \leq \max(1,1) = 1.$$

Now choose $s \in \mathbf{Z}$ such that

$$|b_\infty - r - s| \leq \frac{1}{2}.$$

Then $a = r + s$ and $\mathbf{x} = \mathbf{y} - a$ do what is required, since $\mathbf{y} - a = \mathbf{y} - r - s$ has the desired property (since $s \in \mathbf{Z}$ and the p-adic valuations are non-archimedean).

Hence the continuous map $W \to \mathbb{A}_{\mathbf{Q}}^{+}/\mathbf{Q}^{+}$ induced by the quotient map $\mathbb{A}_{\mathbf{Q}}^{+} \to \mathbb{A}_{\mathbf{Q}}^{+}/\mathbf{Q}^{+}$ is surjective. But W is compact (being the topological product of the compact spaces $|x_\infty|_\infty \leq 1/2$ and the $\mathbf{Z}_p$ for all p), hence $\mathbb{A}_{\mathbf{Q}}^{+}/\mathbf{Q}^{+}$ is also compact. □

Corollary 20.3.6. *There is a subset W of $\mathbb{A}_K$ defined by inequalities of the type $|x_v|_v \leq \delta_v$, where $\delta_v = 1$ for almost all v, such that every $\mathbf{y} \in \mathbb{A}_K$ can be put in the form*

$$\mathbf{y} = a + \mathbf{x}, \qquad a \in K, \quad \mathbf{x} \in W,$$

i.e., $\mathbb{A}_K = K + W$.

Proof. We constructed such a set for $K = \mathbf{Q}$ when proving Theorem 20.3.5. For general K the W coming from the proof determines compenent-wise a subset of $\mathbb{A}_K^{+} \cong \mathbb{A}_{\mathbf{Q}}^{+} \oplus \cdots \oplus \mathbb{A}_{\mathbf{Q}}^{+}$ that is a subset of a set with the properties claimed by the corollary. □

As already remarked, $\mathbb{A}_K^+$ is a locally compact group, so it has an invariant Haar measure. In fact one choice of this Haar measure is the product of the Haar measures on the K_v, in the sense of Definition 20.2.5.

Corollary 20.3.7. *The quotient $\mathbb{A}_K^+/K^+$ has finite measure in the quotient measure induced by the Haar measure on $\mathbb{A}_K^+$.*

Remark 20.3.8. This statement is independent of the particular choice of the multiplicative constant in the Haar measure on $\mathbb{A}_K^+$. We do not here go into the question of finding the measure $\mathbb{A}_K^+/K^+$ in terms of our explicitly given Haar measure. (See Tate's thesis, [Cp86, Chapter XV].)

Proof. This can be reduced similarly to the case of $\mathbf{Q}$ or $\mathbf{F}(t)$ which is immediate, e.g., the W defined above has measure 1 for our Haar measure.

Alternatively, finite measure follows from compactness. To see this, cover $\mathbb{A}_K/K^+$ with the translates of U, where U is a nonempty open set with finite measure. The existence of a finite subcover implies finite measure. □

Remark 20.3.9. We give an alternative proof of the product formula $\prod |a|_v = 1$ for nonzero $a \in K$. We have seen that if $x_v \in K_v$, then multiplication by x_v magnifies the Haar measure in K_v^+ by a factor of $|x_v|_v$. Hence if $\mathbf{x} = \{x_v\} \in \mathbb{A}_K$, then multiplication by $\mathbf{x}$ magnifies the Haar measure in $\mathbb{A}_K^+$ by $\prod |x_v|_v$. But now multiplication by $a \in K$ takes $K^+ \subset \mathbb{A}_K^+$ into K^+, so gives a well-defined bijection of $\mathbb{A}_K^+/K^+$ onto $\mathbb{A}_K^+/K^+$ which magnifies the measure by the factor $\prod |a|_v$. Hence $\prod |a|_v = 1$ Corollary 20.3.7. (The point is that if μ is the measure of $\mathbb{A}_K^+/K^+$, then $\mu = \prod |a|_v \cdot \mu$, so because μ is finite we must have $\prod |a|_v = 1$.)

20.4 Strong Approximation

We first prove a technical lemma and corollary, then use them to deduce the strong approximation theorem, which is an extreme generalization of the Chinese Remainder Theorem; it asserts that K^+ is dense in the analogue of the adeles with one valuation removed.

The proof of Lemma 20.4.1 below will use in a crucial way the normalized Haar measure on $\mathbb{A}_K$ and the induced measure on the compact quotient $\mathbb{A}_K^+/K^+$. Since I am not formally developing Haar measure on locally compact groups, and since I didn't explain induced measures on quotients well in the last chapter, hopefully the following discussion will help clarify what is going on.

The real numbers $\mathbf{R}^+$ under addition is a locally compact topological group. Normalized Haar measure μ has the property that $\mu([a,b]) = b - a$, where $a \leq b$ are real numbers and $[a,b]$ is the closed interval from a to b. The subset $\mathbf{Z}^+$ of $\mathbf{R}^+$ is discrete, and the quotient $S^1 = \mathbf{R}^+/\mathbf{Z}^+$ is a compact topological group, which thus has a Haar measure. Let $\overline{\mu}$ be the Haar measure on S^1 normalized so that the natural quotient $\pi : \mathbf{R}^+ \to S^1$ preserves the measure, in the sense that if $X \subset \mathbf{R}^+$ is a measurable set that maps injectively into S^1, then $\mu(X) = \overline{\mu}(\pi(X))$. This determine $\overline{\mu}$ and we have $\overline{\mu}(S^1) = 1$ since $X = [0, 1)$ is a measurable set that maps bijectively onto S^1 and has measure 1. The situation for the map $\mathbb{A}_K \to \mathbb{A}_K/K^+$ is pretty much the same.

Lemma 20.4.1. *There is a constant $C > 0$ that depends only on the global field K with the following property:*

Whenever $\mathbf{x} = \{x_v\}_v \in \mathbb{A}_K$ is such that

$$\prod_v |x_v|_v > C, \tag{20.4.1}$$

then there is a nonzero principal adele $a \in K \subset \mathbb{A}_K$ such that

$$|a|_v \le |x_v|_v \qquad \text{for all } v.$$

Proof. This proof is modelled on Blichfeldt's proof of Minkowski's Theorem in the Geometry of Numbers, and works in quite general circumstances.

First we show that (20.4.1) implies that $|x_v|_v = 1$ for almost all v. Because $\mathbf{x}$ is an adele, we have $|x_v|_v \le 1$ for almost all v. If $|x_v|_v < 1$ for infinitely many v, then the product in (20.4.1) would have to be 0. (We prove this only when K is a finite extension of $\mathbf{Q}$.) Excluding archimedean valuations, this is because the normalized valuation $|x_v|_v = |\mathrm{Norm}(x_v)|_p$, which if less than 1 is necessarily $\le 1/p$. Any infinite product of numbers $1/p_i$ must be 0, whenever p_i is a sequence of primes.

Let c_0 be the Haar measure of $\mathbb{A}_K^+/K^+$ induced from normalized Haar measure on $\mathbb{A}_K^+$, and let c_1 be the Haar measure of the set of $\mathbf{y} = \{y_v\}_v \in \mathbb{A}_K^+$ that satisfy

$$\begin{aligned} |y_v|_v &\le \frac{1}{2} && \text{if } v \text{ is real archimedean,}\\ |y_v|_v &\le \frac{1}{2} && \text{if } v \text{ is complex archimedean,}\\ |y_v|_v &\le 1 && \text{if } v \text{ is non-archimedean.} \end{aligned}$$

(As we will see, any positive real number $\le 1/2$ would suffice in the definition of c_1 above. For example, in Cassels's article he uses the mysterious $1/10$. He also doesn't discuss the subtleties of the complex archimedean case separately.)

Then $0 < c_0 < \infty$ since $\mathbb{A}_K/K^+$ is compact, and $0 < c_1 < \infty$ because the number of archimedean valuations v is finite. We show that

$$C = \frac{c_0}{c_1}$$

will do. Thus suppose $\mathbf{x}$ is as in (20.4.1).

The set T of $\mathbf{t} = \{t_v\}_v \in \mathbb{A}_K^+$ such that

$$\begin{aligned} |t_v|_v &\le \frac{1}{2}\,|x_v|_v && \text{if } v \text{ is real archimedean,}\\ |t_v|_v &\le \frac{1}{2}\sqrt{|x_v|_v} && \text{if } v \text{ is complex archimedean,}\\ |t_v|_v &\le |x_v|_v && \text{if } v \text{ is non-archimedean} \end{aligned}$$

has measure

$$c_1 \cdot \prod_v |x_v|_v > c_1 \cdot C = c_0. \tag{20.4.2}$$

(Note: If there are complex valuations, then the some of the $|x_v|_v$'s in the product must be squared.)

Because of (20.4.2), in the quotient map $\mathbb{A}_K^+ \to \mathbb{A}_K^+/K^+$ there must be a pair of distinct points of T that have the same image in $\mathbb{A}_K^+/K^+$, say

$$\mathbf{t}' = \{t'_v\}_v \in T \quad \text{and} \quad \mathbf{t}'' = \{t''_v\}_v \in T$$

and

$$a = \mathbf{t}' - \mathbf{t}'' \in K^+$$

is nonzero. Then

$$|a|_v = \left|t'_v - t''_v\right|_v \leq \begin{cases} |t'_v| + |t''_v| \leq 2 \cdot \frac{1}{2} |x_v|_v \leq |x_v|_v & \text{if } v \text{ is real archimedean, or} \\ \max(|t'_v|, |t''_v|) \leq |x_v|_v & \text{if } v \text{ is non-archimedean,} \end{cases}$$

for all v. In the case of complex archimedean v, we must be careful because the normalized valuation $|\cdot|_v$ is the *square* of the usual archimedean complex valuation $|\cdot|_\infty$ on $\mathbf{C}$, so e.g., it does not satisfy the triangle inequality. In particular, the quantity $|t'_v - t''_v|_v$ is at most the square of the maximum distance between two points in the disc in $\mathbf{C}$ of radius $\frac{1}{2}\sqrt{|x_v|_v}$, where by distance we mean the usual distance. This maximum distance in such a disc is at most $\sqrt{|x_v|_v}$, so $|t'_v - t''_v|_v$ is at most $|x_v|_v$, as required. Thus a satisfies the requirements of the lemma. □

Corollary 20.4.2. *Let v_0 be a normalized valuation and let $\delta_v > 0$ be given for all $v \neq v_0$ with $\delta_v = 1$ for almost all v. Then there is a nonzero $a \in K$ with*

$$|a|_v \leq \delta_v \qquad (\textit{all } v \neq v_0).$$

Proof. This is just a degenerate case of Lemma 20.4.1. Choose $x_v \in K_v$ with $0 < |x_v|_v \leq \delta_v$ and $|x_v|_v = 1$ if $\delta_v = 1$. We can then choose $x_{v_0} \in K_{v_0}$ so that

$$\prod_{\text{all } v \text{ including } v_0} |x_v|_v > C.$$

Then Lemma 20.4.1 does what is required. □

Remark 20.4.3. The character group of the locally compact group $\mathbb{A}_K^+$ is isomorphic to $\mathbb{A}_K^+$ and K^+ plays a special role. See Chapter XV of [Cp86], Lang's [Lan64], Weil's [Wei82], and Godement's Bourbaki seminars 171 and 176. This duality lies behind the functional equation of ζ and L-functions. Iwasawa has shown [Iwa53] that the rings of adeles are characterized by certain general topologico-algebraic properties.

We proved before that K is discrete in $\mathbb{A}_K$. If one valuation is removed, the situation is much different.

Theorem 20.4.4 (Strong Approximation). *Let v_0 be any normalized nontrivial valuation of the global field K. Let $\mathbb{A}_{K,v_0}$ be the restricted topological product of the K_v with respect to the $\mathcal{O}_v$, where v runs through all normalized valuations $v \neq v_0$. Then K is dense in $\mathbb{A}_{K,v_0}$.*

Proof. This proof was suggested by Prof. Kneser at the Cassels-Frohlich conference.

Recall that if $\mathbf{x} = \{x_v\}_v \in \mathbb{A}_{K,v_0}$ then a basis of open sets about $\mathbf{x}$ is the collection of products

$$\prod_{v \in S} B(x_v, \varepsilon_v) \times \prod_{v \notin S,\ v \neq v_0} \mathcal{O}_v,$$

where $B(x_v, \varepsilon_v)$ is an open ball in K_v about x_v, and S runs through finite sets of normalized valuations (not including v_0). Thus denseness of K in $\mathbb{A}_{K,v_0}$ is equivalent to the following statement about elements. Suppose we are given (i) a finite set S of valuations $v \neq v_0$, (ii) elements $x_v \in K_v$ for all $v \in S$, and (iii) an $\varepsilon > 0$. Then there is an element $b \in K$ such that $|b - x_v|_v < \varepsilon$ for all $v \in S$ and $|b|_v \leq 1$ for all $v \notin S$ with $v \neq v_0$.

By the corollary to our proof that $\mathbb{A}_K^+/K^+$ is compact (Corollary 20.3.6), there is a $W \subset \mathbb{A}_K$ that is defined by inequalities of the form $|y_v|_v \leq \delta_v$ (where $\delta_v = 1$ for almost all v) such that ever $\mathbf{z} \in \mathbb{A}_K$ is of the form

$$\mathbf{z} = \mathbf{y} + c, \qquad \mathbf{y} \in W, \quad c \in K. \tag{20.4.3}$$

By Corollary 20.4.2, there is a nonzero $a \in K$ such that

$$\begin{aligned} |a|_v &< \frac{1}{\delta_v} \cdot \varepsilon && \text{for } v \in S, \\ |a|_v &\leq \frac{1}{\delta_v} && \text{for } v \notin S,\ v \neq v_0. \end{aligned}$$

Hence on putting $\mathbf{z} = \frac{1}{a} \cdot \mathbf{x}$ in (20.4.3) and multiplying by a, we see that every $\mathbf{x} \in \mathbb{A}_K$ is of the shape

$$\mathbf{x} = \mathbf{w} + b, \qquad \mathbf{w} \in a \cdot W, \quad b \in K,$$

where $a \cdot W$ is the set of $a\mathbf{y}$ for $\mathbf{y} \in W$. If now we let $\mathbf{x}$ have components the given x_v at $v \in S$, and (say) 0 elsewhere, then $b = \mathbf{x} - \mathbf{w}$ has the properties required. $\square$

Remark 20.4.5. The proof gives a quantitative form of the theorem (i.e., with a bound for $|b|_{v_0}$). For an alternative approach, see [Mah64].

In the next chapter we'll introduce the ideles $\mathbb{A}_K^*$. Finally, we'll relate ideles to ideals, and use everything so far to give a new interpretation of class groups and their finiteness.

Chapter 21

Ideles and Ideals

In this chapter, we introduce the ideles $\mathbb{I}_K$, and relate ideles to ideals, and use what we've done so far to give an alternative interpretation of class groups and their finiteness, thus linking the adelic point of view with the classical point of view of the first part of this course.

21.1 The Idele Group

The invertible elements of any commutative topological ring R are a group R^* under multiplication. In general R^* is not a topological group if it is endowed with the subset topology because inversion need not be continuous (only multiplication and addition on R are required to be continuous). It is usual therefore to give R^* the following topology. There is an injection

$$x \mapsto \left(x,\ \frac{1}{x}\right) \tag{21.1.1}$$

of R^* into the topological product $R \times R$. We give R^* the corresponding subset topology. Then R^* with this topology is a topological group and the inclusion map $R^* \hookrightarrow R$ is continous. To see continuity of inclusion, note that this topology is finer (has at least as many open sets) than the subset topology induced by $R^* \subset R$, since the projection maps $R \times R \to R$ are continuous.

Example 21.1.1. This is a "non-example". The inverse map on $\mathbf{Z}_p^*$ is continuous with respect to the p-adic topology. If $a, b \in \mathbf{Z}_p^*$, then $|a| = |b| = 1$, so if $|a - b| < \varepsilon$, then

$$\left|\frac{1}{a} - \frac{1}{b}\right| = \left|\frac{b-a}{ab}\right| = \frac{|b-a|}{|ab|} < \frac{\varepsilon}{1} = \varepsilon.$$

Definition 21.1.2 (Idele Group). The *idele group* $\mathbb{I}_K$ of K is the group $\mathbb{A}_K^*$ of invertible elements of the adele ring $\mathbb{A}_K$.

We shall usually speak of $\mathbb{I}_K$ as a subset of $\mathbb{A}_K$, and will have to distinguish between the $\mathbb{I}_K$ and $\mathbb{A}_K$-topologies.

Example 21.1.3. For a rational prime p, let $\mathbf{x}_p \in \mathbb{A}_{\mathbf{Q}}$ be the adele whose pth component is p and whose vth component, for $v \neq p$, is 1. Then $\mathbf{x}_p \to 1$ as $p \to \infty$ in $\mathbb{A}_{\mathbf{Q}}$, for the following reason. We must show that if U is a basic open set that contains the adele $1 = \{1\}_v$, the $\mathbf{x}_p$ for all sufficiently large p are contained in U. Since U contains 1 and is a basic open set, it is of the form

$$\prod_{v \in S} U_v \times \prod_{v \notin S} \mathbf{Z}_v,$$

where S if a finite set, and the U_v, for $v \in S$, are arbitrary open subsets of $\mathbf{Q}_v$ that contain 1. If q is a prime larger than any prime in S, then $\mathbf{x}_p$ for $p \geq q$, is in U. This proves convergence. If the inverse map were continuous on $\mathbb{I}_K$, then the sequence of $\mathbf{x}_p^{-1}$ would converge to $1^{-1} = 1$. However, if U is an open set as above about 1, then for sufficiently large p, *none* of the adeles $\mathbf{x}_p$ are contained in U.

Lemma 21.1.4. *The group of ideles $\mathbb{I}_K$ is the restricted topological project of the K_v^* with respect to the units $U_v = \mathcal{O}_v^* \subset K_v$, with the restricted product topology.*

We omit the proof of Lemma 21.1.4, which is a matter of thinking carefully about the definitions. The main point is that inversion is continuous on $\mathcal{O}_v^*$ for each v. (See Example 21.1.1.)

We have seen that K is naturally embedded in $\mathbb{A}_K$, so K^* is naturally embedded in $\mathbb{I}_K$.

Definition 21.1.5 (Principal Ideles). We call K^*, considered as a subgroup of $\mathbb{I}_K$, the *principal ideles.*

Lemma 21.1.6. *The principal ideles K^* are discrete as a subgroup of $\mathbb{I}_K$.*

Proof. For K is discrete in $\mathbb{A}_K$, so K^* is embedded in $\mathbb{A}_K \times \mathbb{A}_K$ by (21.1.1) as a discrete subset. (Alternatively, the subgroup topology on $\mathbb{I}_K$ is finer than the topology coming from $\mathbb{I}_K$ being a subset of $\mathbb{A}_K$, and K is already discrete in $\mathbb{A}_K$.) $\square$

Definition 21.1.7 (Content of an Idele). The *content* of $\mathbf{x} = \{x_v\}_v \in \mathbb{I}_K$ is

$$c(\mathbf{x}) = \prod_{\text{all } v} |x_v|_v \in \mathbf{R}_{>0}.$$

Lemma 21.1.8. *The map $\mathbf{x} \to c(\mathbf{x})$ is a continuous homomorphism of the topological group $\mathbb{I}_K$ into $\mathbf{R}_{>0}$, where we view $\mathbf{R}_{>0}$ as a topological group under multiplication. If K is a number field, then c is surjective.*

Proof. That the content map c satisfies the axioms of a homomorphisms follows from the multiplicative nature of the defining formula for c. For continuity, suppose (a, b) is an open interval in $\mathbf{R}_{>0}$. Suppose $\mathbf{x} \in \mathbb{I}_K$ is such that $c(\mathbf{x}) \in (a, b)$. By considering small intervals about each non-unit component of $\mathbf{x}$, we find an open neighborhood $U \subset \mathbb{I}_K$ of $\mathbf{x}$ such that $c(U) \subset (a, b)$. It follows the $c^{-1}((a, b))$ is open.

For surjectivity, use that each archimedean valuation is surjective, and choose an idele that is 1 at all but one archimedean valuation. $\square$

Remark 21.1.9. Note also that the $\mathbb{I}_K$-topology is that appropriate to a group of operators on $\mathbb{A}_K^+$: a basis of open sets is the $S(C,U)$, where $C, U \subset \mathbb{A}_K^+$ are, respectively, $\mathbb{A}_K$-compact and $\mathbb{A}_K$-open, and S consists of the $\mathbf{x} \in \mathbb{I}_J$ such that $(1-\mathbf{x})C \subset U$ and $(1-\mathbf{x}^{-1})C \subset U$.

Definition 21.1.10 (1-Ideles). The subgroup $\mathbb{I}_K^1$ of 1-*ideles* is the subgroup of ideles $\mathbf{x} = \{x_v\}$ such that $c(\mathbf{x}) = 1$. Thus $\mathbb{I}_K^1$ is the kernel of c, so we have an exact sequence

$$1 \to \mathbb{I}_K^1 \to \mathbb{I}_K \xrightarrow{c} \mathbf{R}_{>0} \to 1,$$

where the surjectivity on the right is only if K is a number field.

Lemma 21.1.11. *The subset $\mathbb{I}_K^1$ of $\mathbb{A}_K$ is closed as a subset, and the $\mathbb{A}_K$-subset topology on $\mathbb{I}_K^1$ coincides with the $\mathbb{I}_K$-subset topology on $\mathbb{I}_K^1$.*

Proof. Let $\mathbf{x} \in \mathbb{A}_K$ with $\mathbf{x} \notin \mathbb{I}_K^1$. To prove that $\mathbb{I}_K^1$ is closed in $\mathbb{A}_K$, we find an $\mathbb{A}_K$-neighborhood W of $\mathbf{x}$ that does not meet $\mathbb{I}_K^1$.

1st Case. Suppose that $\prod_v |x_v|_v < 1$ (possibly $= 0$). Then there is a finite set S of v such that

1. S contains all the v with $|x_v|_v > 1$, and
2. $\prod_{v \in S} |x_v|_v < 1$.

Then the set W can be defined by

$$\begin{aligned} |w_v - x_v|_v &< \varepsilon \qquad v \in S \\ |w_v|_v &\leq 1 \qquad v \notin S \end{aligned}$$

for sufficiently small ε.

2nd Case. Suppose that $C := \prod_v |x_v|_v > 1$. Then there is a finite set S of v such that

1. S contains all the v with $|x_v|_v > 1$, and
2. if $v \notin S$ an inequality $|w_v|_v < 1$ implies $|w_v|_v < \frac{1}{2C}$. (This is because for a non-archimedean valuation, the largest absolute value less than 1 is $1/p$, where p is the residue characteristic. Also, the upper bound in Cassels's article is $\frac{1}{2}C$ instead of $\frac{1}{2C}$, but I think he got it wrong.)

We can choose ε so small that $|w_v - x_v|_v < \varepsilon$ (for $v \in S$) implies $1 < \prod_{v \in S} |w_v|_v < 2C$. Then W may be defined by

$$\begin{aligned} |w_v - x_v|_v &< \varepsilon \qquad v \in S \\ |w_v|_v &\leq 1 \qquad v \notin S. \end{aligned}$$

This works because if $\mathbf{w} \in W$, then either $|w_v|_v = 1$ for all $v \notin S$, in which case $1 < c(\mathbf{w}) < 2c$, so $\mathbf{w} \notin \mathbb{I}_K^1$, or $|w_{v_0}|_{v_0} < 1$ for some $v_0 \notin S$, in which case

$$c(\mathbf{w}) = \left(\prod_{v \in S} |w_v|_v\right) \cdot |w_{v_0}| \cdots < 2C \cdot \frac{1}{2C} \cdots < 1,$$

so again $\mathbf{w} \notin \mathbb{I}_K^1$.

We next show that the $\mathbb{I}_K$- and $\mathbb{A}_K$-topologies on $\mathbb{I}_K^1$ are the same. If $\mathbf{x} \in \mathbb{I}_K^1$, we must show that every $\mathbb{A}_K$-neighborhood of $\mathbf{x}$ contains an $\mathbb{A}_K$-neighborhood and vice-versa.

Let $W \subset \mathbb{I}_K^1$ be an $\mathbb{A}_K$-neighborhood of $\mathbf{x}$. Then it contains an $\mathbb{A}_K$-neighborhood of the type

$$|w_v - x_v|_v < \varepsilon \qquad v \in S \tag{21.1.2}$$
$$|w_v|_v \leq 1 \qquad v \notin S \tag{21.1.3}$$

where S is a finite set of valuations v. This contains the $\mathbb{I}_K$-neighborhood in which $\leq$ in (21.1.2) is replaced by $=$.

Next let $H \subset \mathbb{I}_K^1$ be an $\mathbb{I}_K$-neighborhood. Then it contains an $\mathbb{I}_K$-neighborhood of the form

$$|w_v - x_v|_v < \varepsilon \qquad v \in S \tag{21.1.4}$$
$$|w_v|_v = 1 \qquad v \notin S, \tag{21.1.5}$$

where the finite set S contains at least all archimedean valuations v and all valuations v with $|x_v|_v \neq 1$. Since $\prod |x_v|_v = 1$, we may also suppose that ε is so small that (21.1.4) implies

$$\prod_v |w_v|_v < 2.$$

Then the intersection of (21.1.4) with $\mathbb{I}_K^1$ is the same as that of (21.1.2) with $\mathbb{I}_K^1$, i.e., (21.1.4) defines an $\mathbb{A}_K$-neighborhood. $\square$

By the product formula we have that $K^* \subset \mathbb{I}_K^1$. The following result is of vital importance in class field theory.

Theorem 21.1.12. *The quotient $\mathbb{I}_K^1/K^*$ with the quotient topology is compact.*

Proof. After the preceeding lemma, it is enough to find an $\mathbb{A}_K$-compact set $W \subset \mathbb{A}_K$ such that the map

$$W \cap \mathbb{I}_K^1 \to \mathbb{I}_K^1/K^*$$

is surjective. We take for W the set of $\mathbf{w} = \{w_v\}_v$ with

$$|w_v|_v \leq |x_v|_v\,,$$

where $\mathbf{x} = \{x_v\}_v$ is any idele of content greater than the C of Lemma 20.4.1.

Let $\mathbf{y} = \{y_v\}_v \in \mathbb{I}_K^1$. Then the content of $\mathbf{x}/\mathbf{y}$ equals the content of $\mathbf{x}$, so by Lemma 20.4.1 there is an $a \in K^*$ such that

$$|a|_v \leq \left|\frac{x_v}{y_v}\right|_v \qquad \text{all } v.$$

Then $a\mathbf{y} \in W$, as required. $\square$

Remark 21.1.13. The quotient $\mathbb{I}_K^1/K^*$ is totally disconnected in the function field case. For the structure of its connected component in the number field case, see papers of Artin and Weil in the "Proceedings of the Tokyo Symposium on Algebraic Number Theory, 1955" (Science Council of Japan) or [AT90]. The determination of the character group of $\mathbb{I}_K/K^*$ is global class field theory.

21.2 Ideals and Divisors

Suppose that K is a finite extension of $\mathbf{Q}$. Let F_K be the the free abelian group on a set of symbols in bijection with the non-archimedean valuation v of K. Thus an element of F_K is a formal linear combination

$$\sum_{v \text{ non arch.}} n_v \cdot v$$

where $n_v \in \mathbf{Z}$ and all but finitely many n_v are 0.

Lemma 21.2.1. *There is a natural bijection between F_K and the group of nonzero fractional ideals of $\mathcal{O}_K$. The correspondence is induced by*

$$v \mapsto \wp_v = \{x \in \mathcal{O}_K : v(x) < 1\},$$

where v is a non-archimedean valuation.

Endow F_K with the discrete topology. Then there is a natural continuous map $\pi : \mathbb{I}_K \to F_K$ given by

$$\mathbf{x} = \{x_v\}_v \mapsto \sum_v \mathrm{ord}_v(x_v) \cdot v.$$

This map is continuous since the inverse image of a valuation v (a point) is the product

$$\pi^{-1}(v) = \pi\mathcal{O}_v^* \quad \times \prod_{w \text{ archimedean}} K_w^* \quad \times \prod_{w \neq v \text{ non-arch.}} \mathcal{O}_w^*,$$

which is an open set in the restricted product topology on $\mathbb{I}_K$. Moreover, the image of K^* in F_K is the group of nonzero principal fractional ideals.

Recall that the *class group* C_K of the number field K is by definition the quotient of F_K by the image of K^*.

Theorem 21.2.2. *The class group C_K of a number field K is finite.*

Proof. We first prove that the map $\mathbb{I}_K^1 \to F_K$ is surjective. Let ∞ be an archimedean valuation on K. If v is a non-archimedean valuation, let $\mathbf{x} \in \mathbb{I}_K^1$ be a 1-idele such that $x_w = 1$ at ever valuation w except v and ∞. At v, choose $x_v = \pi$ to be a generator for the maximal ideal of $\mathcal{O}_v$, and choose x_∞ to be such that $|x_\infty|_\infty = 1/|x_v|_v$. Then $\mathbf{x} \in \mathbb{I}_K$ and $\prod_w |x_w|_w = 1$, so $\mathbf{x} \in \mathbb{I}_K^1$. Also $\mathbf{x}$ maps to $v \in F_K$.

Thus the group of ideal classes is the continuous image of the compact group $\mathbb{I}_K^1/K^*$ (see Theorem 21.1.12), hence compact. But a compact discrete group is finite. □

21.2.1 The Function Field Case

When K is a finite separable extension of $\mathbf{F}(t)$, we define the divisor group D_K of K to be the free abelian group on all the valuations v. For each v the number of elements of the residue class field $\mathbf{F}_v = \mathcal{O}_v/\wp_v$ of v is a power, say q^{n_v}, of the number q of elements in $\mathbf{F}_v$. We call n_v the degree of v, and similarly define $\sum n_v d_v$ to be the degree of the divisor $\sum n_v \cdot v$. The divisors of degree 0 form a group D_K^0. As before, the principal divisor attached to $a \in K^*$ is $\sum \mathrm{ord}_v(a) \cdot v \in D_K$. The following theorem is proved in the same way as Theorem 21.2.2.

Theorem 21.2.3. *The quotient of D_K^0 modulo the principal divisors is a finite group.*

21.2.2 Jacobians of Curves

For those familiar with algebraic geometry and algebraic curves, one can prove Theorem 21.2.3 from an alternative point of view. There is a bijection between nonsingular geometrically irreducible projective curves over $\mathbf{F}$ and function fields K over $\mathbf{F}$ (which we assume are finite separable extensions of $\mathbf{F}(t)$ such that $\overline{\mathbf{F}} \cap K = \mathbf{F}$). Let X be the curve corresponding to K. The group D_K^0 is in bijection with the divisors of degree 0 on X, a group typically denoted $\mathrm{Div}^0(X)$. The quotient of $\mathrm{Div}^0(X)$ by principal divisors is denoted $\mathrm{Pic}^0(X)$. The *Jacobian* of X is an abelian variety $J = \mathrm{Jac}(X)$ over the finite field $\mathbf{F}$ whose dimension is equal to the genus of X. Moreover, assuming X has an $\mathbf{F}$-rational point, the elements of $\mathrm{Pic}^0(X)$ are in natural bijection with the $\mathbf{F}$-rational points on J. In particular, with these hypothesis, the class group of K, which is isomorphic to $\mathrm{Pic}^0(X)$, is in bijection with the group of $\mathbf{F}$-rational points on an algebraic variety over a finite field. This gives an alternative more complicated proof of finiteness of the degree 0 class group of a function field.

Without the degree 0 condition, the divisor class group won't be finite. It is an extension of $\mathbf{Z}$ by a finite group.

$$0 \to \mathrm{Pic}^0(X) \to \mathrm{Pic}(X) \xrightarrow{\deg} n\mathbf{Z} \to 0,$$

where n is the greatest common divisor of the degrees of elements of $\mathrm{Pic}(X)$, which is 1 when X has a rational point.

Chapter 22

Exercises

1. Let $A = \begin{pmatrix} 4 & 7 & 2 \\ 2 & 4 & 6 \\ 0 & 0 & 0 \end{pmatrix}$.

   (a) Find invertible integer matrices P and Q such that PAQ is in Smith normal form.

   (b) What is the group structure of the cokernel of the map $\mathbf{Z}^3 \to \mathbf{Z}^3$ defined by multiplication by A?

2. Let G be the abelian group generated by x, y, z with relatoins $2x + y = 0$ and $x - y + 3z = 0$. Find a product of cyclic groups that is isomorphic to G.

3. Prove that each of the following rings have infinitely many prime ideals:

   (a) The integers $\mathbf{Z}$. [Hint: Euclid gave a famous proof of this long ago.]

   (b) The ring $\mathbf{Q}[x]$ of polynomials over $\mathbf{Q}$.

   (c) The ring $\mathbf{Z}[x]$ of polynomials over $\mathbf{Z}$.

   (d) The ring $\overline{\mathbf{Z}}$ of all algebraic integers. [Hint: Use Zorn's lemma, which implies that every ideal is contained in a maximal ideal. See, e.g., Prop 1.12 on page 589 of Artin's *Algebra*.]

4. (This problem was on the graduate qualifying exam on Tuesday.) Let $\overline{\mathbf{Z}}$ denote the subset of all elements of $\overline{\mathbf{Q}}$ that satisfy a monic polynomial with coefficients in the ring $\mathbf{Z}$ of integers. We proved in class that $\overline{\mathbf{Z}}$ is a ring.

   (a) Show that the ideals (2) and $(\sqrt{2})$ in $\overline{\mathbf{Z}}$ are distinct.

   (b) Prove that $\overline{\mathbf{Z}}$ is not Noetherian.

5. Show that neither $\mathbf{Z}[\sqrt{-6}]$ nor $\mathbf{Z}[\sqrt{5}]$ is a unique factorization domain. [Hint: Consider the factorization into irreducible elements of 6 in the first case and 4 in the second. A nonzero element a in a ring R is an *irreducible element* if it is not a unit and if whenever $a = qr$, then one of q or r is a unit.]

6. Find the ring of integers of each of the following number fields:
   (a) $\mathbf{Q}(\sqrt{-3})$,
   (b) $\mathbf{Q}(\sqrt{3})$, and
   (c) $\mathbf{Q}(\sqrt[3]{2})$.

   Do not use a computer for the first two.

7. Find the discriminants of the rings of integers of the numbers fields in the previous problem. (Do not use a computer.)

8. Let R be a finite integral domain. Prove that R is a field. [Hint: Show that if x is a nonzero element, then x has an inverse by considering powers of x.]

9. Suppose $K \subset L \subset M$ is a tower of number fields and let $\sigma : L \hookrightarrow \overline{\mathbf{Q}}$ be a field embedding of L into $\overline{\mathbf{Q}}$ that fixes K elementwise. Show that σ extends in exactly $[M : L]$ ways to a field embedding $M \hookrightarrow \overline{\mathbf{Q}}$.

10. (a) Suppose I and J are principal ideals in a ring R. Show that the set $\{ab : a \in I,\, b \in J\}$ is an ideal.
    (b) Give an example of ideals I and J in the polynomial ring $\mathbf{Q}[x, y]$ in two variables such that $\{ab : a \in I,\, b \in J\}$ is not an ideal. Your example illustrates why it is necessary to define the product of two ideals to be the ideal generated by $\{ab : a \in I,\, b \in J\}$.
    (c) Give an example of a ring of integers $\mathcal{O}_K$ of a number field, and ideals I and J such that $\{ab : a \in I,\, b \in J\}$ is not an ideal.

11. (a) Let k be a field. Prove that $k[x]$ is a Dedekind domain.
    (b) (Problem 1.12 from Swinnerton-Dyer) Let x be an indeterminate. Show that the ring $\mathbf{Z}[x]$ is Noetherian and integrally closed in its field of fractions, but is not a Dedekind domain.

12. Use Magma to write each of the following (fractional) ideals as a product of explicitly given prime ideals:
    (a) The ideal (2004) in $\mathbf{Q}(\sqrt{-1})$.
    (b) The ideals $I = (7)$ and $J = (3)$ in the ring of integers of $\mathbf{Q}(\zeta_7)$, where ζ_7 is a root of the irreducible polynomial $x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$. (The field $\mathbf{Q}(\zeta_7)$ is called the 7th cyclotomic field.)
    (c) The principal fractional ideal $(3/8)$ in $\mathbf{Q}(\sqrt{5})$.

13. Suppose R is an order in the ring $\mathcal{O}_K$ of integers of a number field. (Recall that an order is a subring of finite index in $\mathcal{O}_K$.) For each of the following questions, either explain why the answer is yes for any possible order R in any $\mathcal{O}_K$, or find one specific counterexample:

(a) Is R necessarily Noetherian?

(b) Is R necessarily integrally closed in its field of fractions?

(c) Is every nonzero prime ideal of R necessarily maximal?

(d) Is it always possible to write every ideal of R uniquely as a product of prime ideals of R?

14. Let $\mathcal{O}_K$ be the ring of integers of a number field K. Prove that the group of fractional ideals of $\mathcal{O}_K$, under multiplication is (non-canonically) isomorphic to the group of positive rational numbers under multiplication.

15. (a) Suppose K is a number field of degree 2. Prove that $\mathcal{O}_K = \mathbf{Z}[a]$ for some $a \in \mathcal{O}_K$.

    (b) Prove that if K and K' are two number fields of degree 2 and $\mathrm{Disc}(\mathcal{O}_K) = \mathrm{Disc}(\mathcal{O}_{K'})$ then $K = K'$.

16. (*) Does there exist a number field K of degree 4 such that $\mathcal{O}_K \neq \mathbf{Z}[a]$ for all $a \in \mathcal{O}_K$? If so, give an explicit example.

17. Let K be the quintic number field generated by a root of $x^5+7x^4+3x^2-x+1$. Draw a diagram (be creative) that illustrates the factorization of every prime $p \in \mathbf{Z}$, with $p < 100$, in $\mathcal{O}_K$.

18. (Problem 1.9 in Swinnerton-Dyer) Show that the only solutions $x, y \in \mathbf{Z}$ to $y^2 = x^3 - 13$ are given by $x = 17, y = \pm 70$, as follows. Factor the equation $y^2 + 13 = x^3$ in the number field $\mathbf{Q}(\sqrt{-13})$, which has class number 2. Show that if x, y is an integer solution then the ideal $(y + \sqrt{-13})$ must be the cube of an ideal, and hence $y + \sqrt{-13} = (a + b\sqrt{-13})^3$; thus $1 = b(3a^2 - 13b^2)$.

19. Suppose I and J are ideals in the ring $\mathcal{O}_K$ of integers of a number field K. Does $IJ = I \cap J$? Prove or give a counterexample.

20. Let $\mathcal{O}_K$ be the ring of integers $\mathbf{Q}(\sqrt{5})$, and let

$$I = (5, 2 + \sqrt{5}) \qquad \text{and} \qquad J = (209, (389 + \sqrt{5})/2)$$

be integral ideals of $\mathcal{O}_K$.

(a) Find an element of $\mathcal{O}_K$ that is congruent to $\sqrt{5}$ modulo I and is congruent to $1 - \sqrt{5}$ modulo J.

(b) What is the cardinality of $(\mathcal{O}_K/I) \oplus (\mathcal{O}_K/J)$?

(c) Find an element $a \in I$ such that $(a)/I$ is coprime to J.

21. Let $\mathcal{O}_K$ be the ring of integers of a number field K, and suppose K has exactly $2s$ complex embeddings. Prove that the sign of $\mathrm{Disc}(\mathcal{O}_K)$ is $(-1)^s$.

22. (*) Suppose $\mathcal{O}$ is an order in the ring of integers $\mathcal{O}_K$ of a number field. Is every ideal in $\mathcal{O}$ necessarily generated by two elements? (Answer: No. Challenge: Given an example.)

23. Find representative ideals for each element of the class group of $\mathbf{Q}(\sqrt{-23})$. Illustrate how to use the Minkowski bound to prove that your list of representatives is complete.

24. Suppose $\mathcal{O}$ is an order in the ring of integers $\mathcal{O}_K$ of a number field. Is every ideal in $\mathcal{O}$ necessarily generated by two elements?

25. Let K be a number field of degree $n > 1$ with s pairs of complex conjugate embeddings. Prove that
$$\left(\frac{\pi}{4}\right)^s \cdot \frac{n^n}{n!} > 1.$$

26. Do the exercise on page 19 of Swinnerton-Dyer, which shows that the quantity $C_{r,s}$ in the finiteness of class group theorem can be taken to be $\left(\frac{4}{\pi}\right)^s \frac{n!}{n^n}$.

27. Let α denote a root of $x^3 - x + 2$ and let $K = \mathbf{Q}(\alpha)$. Show that $\mathcal{O}_K = \mathbf{Z}[\alpha]$ and that K has class number 1 (don't just read this off from the output of the MAGMA commands `MaximalOrder` and `ClassNumber`). [Hint: consider the square factors of the discriminant of $x^3 - x + 2$ and show that $\frac{1}{2}(a + b\alpha + c\alpha^2)$ is an algebra integer if and only if a, b, and c are all even.]

28. If S is a closed, bounded, convex, symmetric set in $\mathbf{R}^n$ with $\mathrm{Vol}(S) \geq m2^n$, for some positive integer m, show that S contains at least $2m$ nonzero points in $\mathbf{Z}^n$.

29. Prove that any finite subgroup of the multiplicative group of a field is cyclic.

30. For a given number field K, which seems more difficult for MAGMA to compute, the class groups or explicit generators for the group of units? It is very difficult (but not impossible) to not get full credit on this problem. Play around with some examples, see what seems more difficult, and *justify* your response with examples. (This problem might be annoying to do using the MAGMA web page, since it kills your MAGMA job after 30 seconds. Feel free to request a binary of MAGMA from me, or an account on MECCAH (Mathematics Extreme Computation Cluster at Harvard).)

31. (a) Prove that there is no number field K such that $U_K \cong \mathbf{Z}/10\mathbf{Z}$.
    (b) Is there a number field K such that $U_K \cong \mathbf{Z} \times \mathbf{Z}/6\mathbf{Z}$?

32. Prove that the rank of U_K is unbounded as K varies over all number fields.

33. Let $K = \mathbf{Q}(\zeta_5)$.
    (a) Show that $r = 0$ and $s = 2$.

(b) Find explicitly generators for the group of units of U_K (you can use MAGMA for this).

(c) Draw an illustration of the log map $\varphi : U_K \to \mathbf{R}^2$, including the hyperplane $x_1+x_2 = 0$ and the lattice in the hyperplane spanned by the image of U_K.

34. Find the group of units of $\mathbf{Q}(\zeta_n)$ as an abstract group as a function of n. (I.e., find the number of cyclic factors and the size of the torsion subgroup. You do not have to find explicit generators!)

35. Let $K = \mathbf{Q}(a)$, where a is a root $x^3 - 3x + 1$.

    (a) Show that $r = 3$.

    (b) Find explicitly the log embedding of U_K into a 2-dimensional hyperplane in $\mathbf{R}^3$, and draw a picture.

36. Prove that if K is a quadratic field and the torsion subgroup of U_K has order bigger than 2, then $K = \mathbf{Q}(\sqrt{-3})$ or $K = \mathbf{Q}(\sqrt{-1})$.

37. A *Salem number* is a real algebraic integer, greater than 1, with the property that all of its conjugates lie on or within the unit circle, and at least one conjugate lies on the unit circle. By any method (including "google"), give two examples of Salem numbers.

38. Let $p \in \mathbf{Z}$ and let K be a number field. Show that $\mathrm{Norm}_{K/\mathbf{Q}}(p\mathcal{O}_K) = p^{[K:\mathbf{Q}]}$.

39. A totally real number field is a number field in which all embeddings into $\mathbf{C}$ have image in $\mathbf{R}$. Prove there are totally real number fields of degree p, for every prime p. [Hint: Let ζ_n denote a primitive nth root of unity. For $n \geq 3$, show that $\mathbf{Q}(\zeta_n + 1/\zeta_n)$ is totally real of degree $\varphi(n)/2$. Now prove that $\varphi(n)/2$ can be made divisible by any prime.]

40. Give an example of a number field $K/\mathbf{Q}$ and a prime p such that the e_i in the factorization of $p\mathcal{O}_K$ are not all the same.

41. Let K be a number field. Give the "simplest" proof you can think of that there are only finitely many primes that ramify (i.e., have some $e_i > 1$) in K. [The meaning of "simplest" is a matter of taste.]

42. Give examples to show that for $K/\mathbf{Q}$ a Galois extension, the quantity e can be arbirarily large and f can be arbitrarily large.

43. Suppose $K/\mathbf{Q}$ is Galois and p is a prime such that $p\mathcal{O}_K$ is also prime (i.e., p is inert in K). Show that $\mathrm{Gal}(K/\mathbf{Q})$ is a cyclic group.

44. (Problem 7, page 116, from Marcus *Number Fields*) For each of the following, find a prime p and quadratic extensions K and L of $\mathbf{Q}$ that illustrates the assertion:

(a) The prime p can be totally ramified in K and L without being totally ramified in KL.

(b) The fields K and L can each contain unique primes lying over p while KL does not.

(c) The prime p can be inert in K and L without being inert in KL.

(d) The residue field extensions of $\mathbf{F}_p$ can be trivial for K and L without being trivial for KL.

45. Let S_3 by the symmetric group on three symbols, which has order 6.

    (a) Observe that $S_3 \cong D_3$, where D_3 is the dihedral group of order 6, which is the group of symmetries of an equilateral triangle.

    (b) Use (45a) to write down an explicit embedding $S_3 \hookrightarrow \mathrm{GL}_2(\mathbf{C})$.

    (c) Let K be the number field $\mathbf{Q}(\sqrt[3]{2}, \omega)$, where $\omega^3 = 1$ is a nontrivial cube root of unity. Show that K is a Galois extension with Galois group isomorphic to S_3.

    (d) We thus obtain a 2-dimensional irreducible complex Galois representation

    $$\rho : \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \to \mathrm{Gal}(K/\mathbf{Q}) \cong S_3 \subset \mathrm{GL}_2(\mathbf{C}).$$

    Compute a representative matrix of Frob_p and the characteristic polynomial of Frob_p for $p = 5, 7, 11, 13$.

46. Let $K = \mathbf{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5}, \sqrt{7})$. Show that K is Galois over $\mathbf{Q}$, compute the Galois group of K, and compute Frob_{37}.

47. Let k be any field. Prove that the only nontrivial valuations on $k(t)$ which are trivial on k are equivalent to the valuation (15.3.3) or (15.3.4) of page 115.

48. A field with the topology induced by a valuation is a topological field, i.e., the operations sum, product, and reciprocal are continuous.

49. Give an example of a non-archimedean valuation on a field that is not discrete.

50. Prove that the field $\mathbf{Q}_p$ of p-adic numbers is uncountable.

51. Prove that the polynomial $f(x) = x^3 - 3x^2 + 2x + 5$ has all its roots in $\mathbf{Q}_5$, and find the 5-adic valuations of each of these roots. (You might need to use Hensel's lemma, which we don't discuss in detail in this book. See [Cas67, App. C].)

52. In this problem you will compute an example of weak approximation, like I did in the Example 16.3.3. Let $K = \mathbf{Q}$, let $|\cdot|_7$ be the 7-adic absolute value, let $|\cdot|_{11}$ be the 11-adic absolute value, and let $|\cdot|_\infty$ be the usual archimedean absolute value. Find an element $b \in \mathbf{Q}$ such that $|b - a_i|_i < \frac{1}{10}$, where $a_7 = 1$, $a_{11} = 2$, and $a_\infty = -2004$.

53. Prove that -9 has a cube root in $\mathbf{Q}_{10}$ using the following strategy (this is a special case of Hensel's Lemma, which you can read about in an appendix to Cassel's article).

    (a) Show that there is an element $\alpha \in \mathbf{Z}$ such that $\alpha^3 \equiv 9 \pmod{10^3}$.

    (b) Suppose $n \geq 3$. Use induction to show that if $\alpha_1 \in \mathbf{Z}$ and $\alpha^3 \equiv 9 \pmod{10^n}$, then there exists $\alpha_2 \in \mathbf{Z}$ such that $\alpha_2^3 \equiv 9 \pmod{10^{n+1}}$. (Hint: Show that there is an integer b such that $(\alpha_1 + b \cdot 10^n)^3 \equiv 9 \pmod{10^{n+1}}$.)

    (c) Conclude that 9 has a cube root in $\mathbf{Q}_{10}$.

54. Compute the first 5 digits of the 10-adic expansions of the following rational numbers:
$$\frac{13}{2}, \quad \frac{1}{389}, \quad \frac{17}{19}, \qquad \text{the 4 square roots of 41.}$$

55. Let $N > 1$ be an integer. Prove that the series
$$\sum_{n=1}^{\infty} (-1)^{n+1} n! = 1! - 2! + 3! - 4! + 5! - 6! + \cdots .$$
converges in $\mathbf{Q}_N$.

56. Prove that -9 has a cube root in $\mathbf{Q}_{10}$ using the following strategy (this is a special case of "Hensel's Lemma").

    (a) Show that there is $\alpha \in \mathbf{Z}$ such that $\alpha^3 \equiv 9 \pmod{10^3}$.

    (b) Suppose $n \geq 3$. Use induction to show that if $\alpha_1 \in \mathbf{Z}$ and $\alpha^3 \equiv 9 \pmod{10^n}$, then there exists $\alpha_2 \in \mathbf{Z}$ such that $\alpha_2^3 \equiv 9 \pmod{10^{n+1}}$. (Hint: Show that there is an integer b such that $(\alpha_1 + b10^n)^3 \equiv 9 \pmod{10^{n+1}}$.)

    (c) Conclude that 9 has a cube root in $\mathbf{Q}_{10}$.

57. Let $N > 1$ be an integer.

    (a) Prove that $\mathbf{Q}_N$ is equipped with a natural ring structure.

    (b) If N is prime, prove that $\mathbf{Q}_N$ is a field.

58. (a) Let p and q be distinct primes. Prove that $\mathbf{Q}_{pq} \cong \mathbf{Q}_p \times \mathbf{Q}_q$.

    (b) Is $\mathbf{Q}_{p^2}$ isomorphic to either of $\mathbf{Q}_p \times \mathbf{Q}_p$ or $\mathbf{Q}_p$?

59. Prove that every finite extension of $\mathbf{Q}_p$ "comes from" an extension of $\mathbf{Q}$, in the following sense. Given an irreducible polynomial $f \in \mathbf{Q}_p[x]$ there exists an irreducible polynomial $g \in \mathbf{Q}[x]$ such that the fields $\mathbf{Q}_p[x]/(f)$ and $\mathbf{Q}_p[x]/(g)$ are isomorphic. [Hint: Choose each coefficient of g to be sufficiently close to the corresponding coefficient of f, then use Hensel's lemma to show that g has a root in $\mathbf{Q}_p[x]/(f)$.]

60. Find the 3-adic expansion to precision 4 of each root of the following polynomial over $\mathbf{Q}_3$:

$$f = x^3 - 3x^2 + 2x + 3 \in \mathbf{Q}_3[x].$$

Your solution should conclude with three expressions of the form

$$a_0 + a_1 \cdot 3 + a_2 \cdot 3^2 + a_3 \cdot 3^3 + O(3^4).$$

61. (a) Find the normalized Haar measure of the following subset of $\mathbf{Q}_7^+$:

$$U = B\left(28, \frac{1}{50}\right) = \left\{x \in \mathbf{Q}_7 : |x - 28| < \frac{1}{50}\right\}.$$

(b) Find the normalized Haar measure of the subset $\mathbf{Z}_7^*$ of $\mathbf{Q}_7^*$.

62. Suppose that K is a finite extension of $\mathbf{Q}_p$ and L is a finite extension of $\mathbf{Q}_q$, with $p \neq q$ and assume that K and L have the same degree. Prove that there is a polynomial $g \in \mathbf{Q}[x]$ such that $\mathbf{Q}_p[x]/(g) \cong K$ and $\mathbf{Q}_q[x]/(g) \cong L$. [Hint: Combine your solution to 59 with the weak approximation theorem.]

63. Prove that the ring C defined in Section 9 really is the tensor product of A and B, i.e., that it satisfies the defining universal mapping property for tensor products. Part of this problem is for you to look up a functorial definition of tensor product.

64. Find a zero divisor pair in $\mathbf{Q}(\sqrt{5}) \otimes_{\mathbf{Q}} \mathbf{Q}(\sqrt{5})$.

65. (a) Is $\mathbf{Q}(\sqrt{5}) \otimes_{\mathbf{Q}} \mathbf{Q}(\sqrt{-5})$ a field?

(b) Is $\mathbf{Q}(\sqrt[4]{5}) \otimes_{\mathbf{Q}} \mathbf{Q}(\sqrt[4]{-5}) \otimes_{\mathbf{Q}} \mathbf{Q}(\sqrt{-1})$ a field?

66. Suppose ζ_5 denotes a primitive 5th root of unity. For any prime p, consider the tensor product $\mathbf{Q}_p \otimes_{\mathbf{Q}} \mathbf{Q}(\zeta_5) = K_1 \oplus \cdots \oplus K_{n(p)}$. Find a simple formula for the number $n(p)$ of fields appearing in the decomposition of the tensor product $\mathbf{Q}_p \otimes_{\mathbf{Q}} \mathbf{Q}(\zeta_5)$. To get full credit on this problem your formula must be correct, but you do *not* have to prove that it is correct.

67. Suppose $\|\cdot\|_1$ and $\|\cdot\|_2$ are equivalent norms on a finite-dimensional vector space V over a field K (with valuation $|\cdot|$). Carefully prove that the topology induced by $\|\cdot\|_1$ is the same as that induced by $\|\cdot\|_2$.

68. Suppose K and L are number fields (i.e., finite extensions of $\mathbf{Q}$). Is it possible for the tensor product $K \otimes_{\mathbf{Q}} L$ to contain a nilpotent element? (A nonzero element a in a ring R is *nilpotent* if there exists $n > 1$ such that $a^n = 0$.)

69. Let K be the number field $\mathbf{Q}(\sqrt[5]{2})$.

(a) In how many ways does the 2-adic valuation $|\cdot|_2$ on $\mathbf{Q}$ extend to a valuation on K?

(b) Let $v = |\cdot|$ be a valuation on K that extends $|\cdot|_2$. Let K_v be the completion of K with respect to v. What is the residue class field $\mathbf{F}$ of K_v?

70. Prove that the product formula holds for $\mathbf{F}(t)$ similar to the proof we gave in class using Ostrowski's theorem for $\mathbf{Q}$. You may use the analogue of Ostrowski's theorem for $\mathbf{F}(t)$, which you had on a previous homework assignment. (Don't give a measure-theoretic proof.)

71. Prove Theorem 20.3.5, that "The global field K is discrete in $\mathbb{A}_K$ and the quotient $\mathbb{A}_K^+/K^+$ of additive groups is compact in the quotient topology." in the case when K is a finite extension of $\mathbf{F}(t)$, where $\mathbf{F}$ is a finite field.

Bibliography

[ABC$^+$] B. Allombert, K. Belabas, H. Cohen, X. Roblot, and I. Zakharevitch, `PARI/GP`, `http://pari.math.u-bordeaux.fr/`.

[Art59] E. Artin, *Theory of algebraic numbers*, Notes by Gerhard Würges from lectures held at the Mathematisches Institut, Göttingen, Germany, in the Winter Semester, vol. 1956/7, George Striker, Schildweg 12, Göttingen, 1959. MR 24 #A1884

[Art91] M. Artin, *Algebra*, Prentice Hall Inc., Englewood Cliffs, NJ, 1991. MR 92g:00001

[AT90] E. Artin and J. Tate, *Class field theory*, second ed., Advanced Book Classics, Addison-Wesley Publishing Company Advanced Book Program, Redwood City, CA, 1990. MR 91b:11129

[BCP97] W. Bosma, J. Cannon, and C. Playoust, *The Magma algebra system. I. The user language*, J. Symbolic Comput. **24** (1997), no. 3-4, 235–265, Computational algebra and number theory (London, 1993). MR 1 484 478

[Cas67] J. W. S. Cassels, *Global fields*, Algebraic Number Theory (Proc. Instructional Conf., Brighton, 1965), Thompson, Washington, D.C., 1967, pp. 42–84.

[Cas91] ———, *Lectures on elliptic curves*, London Mathematical Society Student Texts, vol. 24, Cambridge University Press, Cambridge, 1991. MR 92k:11058

[Coh93] H. Cohen, *A course in computational algebraic number theory*, Springer-Verlag, Berlin, 1993. MR 94i:11105

[Cp86] J. W. S. Cassels and A. Fröhlich (eds.), *Algebraic number theory*, London, Academic Press Inc. [Harcourt Brace Jovanovich Publishers], 1986, Reprint of the 1967 original.

[EH00] D. Eisenbud and J. Harris, *The geometry of schemes*, Springer-Verlag, New York, 2000. MR 2001d:14002

[Fre94] G. Frey (ed.), *On Artin's conjecture for odd 2-dimensional representations*, Springer-Verlag, Berlin, 1994, 1585. MR 95i:11001

[Iwa53] K. Iwasawa, *On the rings of valuation vectors*, Ann. of Math. (2) **57** (1953), 331–356. MR 14,849a

[Lan64] S. Lang, *Algebraic numbers*, Addison-Wesley Publishing Co., Inc., Reading, Mass.-Palo Alto-London, 1964. MR 28 #3974

[Lan80] R. P. Langlands, *Base change for* GL(2), Princeton University Press, Princeton, N.J., 1980.

[Len02] H. W. Lenstra, Jr., *Solving the Pell equation*, Notices Amer. Math. Soc. **49** (2002), no. 2, 182–192. MR 2002i:11028

[LL93] A. K. Lenstra and H. W. Lenstra, Jr. (eds.), *The development of the number field sieve*, Springer-Verlag, Berlin, 1993. MR 96m:11116

[Mah64] K. Mahler, *Inequalities for ideal bases in algebraic number fields*, J. Austral. Math. Soc. **4** (1964), 425–448. MR 31 #1243

[SD01] H. P. F. Swinnerton-Dyer, *A brief guide to algebraic number theory*, London Mathematical Society Student Texts, vol. 50, Cambridge University Press, Cambridge, 2001. MR 2002a:11117

[Ser73] J-P. Serre, *A Course in Arithmetic*, Springer-Verlag, New York, 1973, Translated from the French, Graduate Texts in Mathematics, No. 7.

[Wei82] A. Weil, *Adeles and algebraic groups*, Progress in Mathematics, vol. 23, Birkhäuser Boston, Mass., 1982, With appendices by M. Demazure and Takashi Ono. MR 83m:10032

Index