Introduction to Algebraic Number Theory

William Stein

May 5, 2005

Contents

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 and Spring 2005. The textbook for the first course was chapter 1 of Swinnerton-Dyer's book [SD01]. The first draft of this book followed [SD01] closely, but the current version but adding substantial text and examples to make the mathematics accessible to advanced undergraduates. For example, chapter 1 of [SD01] is only 30 pages, whereas this book is 140 pages.

Please send any typos or corrections to `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 and 2005 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 in 2004; Mauro Braunstein, Steven Byrnes, William Fithian, Frank Kelly, Alison Miller, Nizameddin Ordulu, Corina Patrascu, Anatoly Preygel, Emily Riehl, Gary Sivek, Steven Sivek, Kaloyan Slavov, Gregory Valiant, and Yan Zhang in 2005. Also the course assistants Matt Bainbridge and Andrei Jorza made many helpful comments.

This material is based upon work supported by the National Science Foundation under Grant No. 0400386.

Chapter 1

Introduction

1.1 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/`

1.2 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.

1.2.1 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).

1.3 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:

$$\begin{aligned}
&188198812920607963838697239461650439807163563379417382700 7\ldots\\
&\ldots 6335642298885971523466548531906060650474304531738801130339\ldots\\
&\ldots 6716199692321205734031879550656996221305168759307650257059\\
&= 3980750864240649373971255005503864911990643623425267084 0\ldots\\
&\quad\ldots 6385189575946388957261768583317\\
&\qquad\times 4727721461074353025362230719730482246329146953020971 1\ldots\\
&\qquad\quad\ldots 6459852171130520711256363590397527
\end{aligned}$$

   (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?

   (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 1.3.1 (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 1.3.1 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 major open problem in arithmetic geometry is the *Birch and Swinnerton-Dyer conjecture*. Suppose X is an algebraic curve such that the set of complex points $X(\mathbf{C})$ is a topological torus. Then the conjecture of Birch and Swinnerton-Dyer gives a criterion for whether or not $X(K)$ is infinite in terms of analytic properties of the L-function $L(X, s)$.

Part I

Algebraic Number Fields

Chapter 2

Basic Commutative Algebra

The commutative algebra in this chapter will provide a solid algebraic foundation for understanding the more refined number-theoretic structures associated to number fields.

First we prove the structure theorem for finitely generated abelian groups. Then we establish the standard properties of Noetherian rings and modules, including a proof of the Hilbert basis theorem. We also observe that finitely generated abelian groups are Noetherian $\mathbf{Z}$-modules. After establishing properties of Noetherian rings, we consider rings of algebraic integers and discuss some of their properties.

2.1 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 2.1.1 (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.

For example, the group $\mathbf{Z}$ is finitely generated, since it is generated by 1.

Theorem 2.1.2 (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 2.1.3. *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 2.1.4. *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 2.1.3 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 2.1.3, $F_2 \cong \mathbf{Z}^m$, 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 2.1.5 (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 $n_1 \mid n_2 \mid \ldots \mid n_s$. Here P and Q are invertible as integer matrices, so* $\det(P)$ *and* $\det(Q)$ *are* ± 1*. The matrix A' is called the* Smith normal form *of A.*

We will see in the proof of Theorem 2.1.2 that A' is uniquely determined by A. An example of a matrix in Smith normal form is

$$A = \begin{pmatrix} 2 & 0 & 0 \\ 0 & 6 & 0 \\ 0 & 0 & 0 \end{pmatrix}.$$

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 row and column operations are as follows:

1. [**Add multiple**] Add an integer multiple of one row to another (or a multiple of one column to another).
2. [**Swap**] Interchange two rows or two columns.
3. [**Rescale**] 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. □

Example 2.1.6. The matrix $\begin{pmatrix} -1 & 2 \\ -3 & 4 \end{pmatrix}$ has Smith normal form to $\begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix}$, and the matrix $\begin{pmatrix} 1 & 4 & 9 \\ 16 & 25 & 36 \\ 49 & 64 & 81 \end{pmatrix}$ has Smith normal form $\begin{pmatrix} 1 & 0 & 0 \\ 0 & 3 & 0 \\ 0 & 0 & 72 \end{pmatrix}$. As a double check, note that the determinants of a matrix and its Smith normal form match, up to sign. This is because

$$\det(PAQ) = \det(P)\det(A)\det(Q) = \pm\det(A).$$

Theorem 2.1.2. Suppose G is a finitely generated abelian group, which we may assume is nonzero. As in the paragraph before Proposition 2.1.5, we use Corollary 2.1.4 to write G as a the cokernel of an $n \times n$ integer matrix A. By Proposition 2.1.5 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

$$G \cong (\mathbf{Z}/n_1\mathbf{Z}) \oplus (\mathbf{Z}/n_2\mathbf{Z}) \oplus \cdots \oplus (\mathbf{Z}/n_s\mathbf{Z}) \oplus \mathbf{Z}^r, \tag{2.1.1}$$

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 (2.1.1) of G as a product that n_i has this property and that no smaller positive integer does.

□

2.2 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, 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. An *ideal* in a ring R is an R-submodule $I \subset R$, where we view R as a module over itself.

Example 2.2.1. 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 $\mathrm{im}(f) = \ker(g)$.

Example 2.2.2. The sequence

$$0 \to \mathbf{Z} \xrightarrow{2} \mathbf{Z} \to \mathbf{Z}/2\mathbf{Z} \to 0$$

is an exact sequence, where the first map sends 1 to 2, and the second is the natural quotient map.

Definition 2.2.3 (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 a noetherian module M is also noetherian. Indeed, 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 2.2.4 (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 $M_n = M_{n+1} = M_{n+2} = \cdots$.

We will use the notion of maximal element below. If $\mathcal{X}$ is a set of subsets of a set S, ordered by inclusion, then a *maximal element* $A \in \mathcal{X}$ is a set so that no superset of A is contained in $\mathcal{X}$. Note that it is *not* necessary that A contain every other element of $\mathcal{X}$, and that $\mathcal{X}$ could contain many maximal elements.

Proposition 2.2.5. *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 and M_∞ is a submodule of M, 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 chain of M_i stabilizes, so 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 2.2.6. *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 2.2.7. *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 2.2.6 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 2.2.6, homomorphic images of noetherian modules are noetherian, so M is noetherian. □

Lemma 2.2.8. *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. This is an exact sequence of R-modules, where S has the R-module structure induced from φ (if $r \in R$ and $s \in S$, then $rs = \varphi(r)s$). By Lemma 2.2.6, 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 2.2.9 (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 2.2.8 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. (The leading coefficient of a polynomial is the coefficient of highest degree, or 0 if the polynomial is 0; thus $3x^7 + 5x^2 - 4$ has leading coefficient 3.) We will first show that A is an ideal of R. Suppose $a, b \in A$ 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 $a + b \in A$. Suppose $r \in R$ 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.

Since R is noetherian and A is an ideal, there exist nonzero $a_1, \ldots, a_n$ that generate A as an ideal. Since A is the set of leading coefficients of elements of I, and the a_j are in A, 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 $d \geq 1$.

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 the 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 $S_{<d}$.

We finish by proving using induction on the degree that every $g \in I$ is an $R[x]$-linear combination of $f_1, \ldots, f_n, h_1, \ldots h_m$. If $g \in I$ has degree 0, then $g \in S_{<d}$, since $d \geq 1$, so g is a linear combination of $h_1, \ldots, h_m$. Next suppose $g \in I$ has degree e, and that we have proven the statement for all elements of I of degree $< e$. If $e \leq d$, then $g \in S_{<d}$, so g is in the $R[x]$-ideal generated by $h_1, \ldots, h_m$. Next suppose that $e \geq d$. Then the leading coefficient b of g lies in the ideal A of leading coefficients of elements of I, 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. □

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.

2.2.1 The Ring Z is noetherian

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

Proposition 2.2.10. *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. □

Example 2.2.11. Let $I = (12, 18)$ be the ideal of $\mathbf{Z}$ generated by 12 and 18. If $n = 12a + 18b \in I$, with $a, b \in \mathbf{Z}$, then $6 \mid n$, since $6 \mid 12$ and $6 \mid 18$. Also, $6 = 18 - 12 \in I$, so $I = (6)$.

Proposition 2.2.7 and 2.2.10 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.

2.3 Rings of Algebraic Integers

In this section 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.

Fix an algebraic closure $\overline{\mathbf{Q}}$ of $\mathbf{Q}$. Thus $\overline{\mathbf{Q}}$ is an infinite field extension of $\mathbf{Q}$ with the property that every polynomial $f \in \mathbf{Q}[x]$ splits as a product of linear factors in $\overline{\mathbf{Q}}[x]$. One choice of $\overline{\mathbf{Q}}$ is the subfield of the complex numbers $\mathbf{C}$ generated by all roots in $\mathbf{C}$ of all polynomials with coefficients in $\mathbf{Q}$. Note that any two choices of $\overline{\mathbf{Q}}$ are isomorphic, but there will be many isomorphisms between them.

An *algebraic integer* is an element of $\overline{\mathbf{Q}}$.

Definition 2.3.1 (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 $\mathbf{Z}$.

For example, $\sqrt{2}$ is an algebraic integer, since it is a root of $x^2 - 2$, but one can prove $1/2$ is not an algebraic integer, since one can show that it is not the root of any monic polynomial over $\mathbf{Z}$. Also π and e are *not* algebraic numbers (they are *transcendental*).

The only elements of $\mathbf{Q}$ that are algebraic integers are the usual integers $\mathbf{Z}$. However, there are elements of $\overline{\mathbf{Q}}$ that have denominators when written down, but

are still algebraic integers. For example,

$$\alpha = \frac{1+\sqrt{5}}{2}$$

is an algebraic integer, since it is a root of the monic polynomial $x^2 - x - 1$.

Definition 2.3.2 (Minimal Polynomial). The *minimal polynomial* of $\alpha \in \overline{\mathbf{Q}}$ is the monic polynomial $f \in \mathbf{Q}[x]$ of least positive degree such that $f(\alpha) = 0$.

It is a consequence of Lemma 2.3.3 that the minimal polynomial α is unique. The minimal polynomial of $1/2$ is $x - 1/2$, and the minimal polynomial of $\sqrt[3]{2}$ is $x^3 - 2$.

Lemma 2.3.3. *Suppose $\alpha \in \overline{\mathbf{Q}}$. Then the minimal polynomial of α divides any polynomial h such that $h(\alpha) = 0$.*

Proof. Let f be a minimal polynomial of α. 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 monic polynomial of least positive degree with root α, so $r = 0$. □

Lemma 2.3.4. *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. Since α is an algebraic integer, there is a polynomial $g \in \mathbf{Z}[x]$ that is monic such that $g(\alpha) = 0$. By Lemma 2.3.3, we have $g = fh$, for some monic $h \in \mathbf{Q}[x]$. 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 h. Then $p^{i+j}g = (p^i f)(p^j h)$, 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. □

Proposition 2.3.5. *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 2.3.4). 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 degrees of all f_i. Then there exist integers a_i such that $\alpha^d = \sum_{i=1}^n a_i f_i(\alpha)$, hence α satisfies the monic polynomial $x^d - \sum_{i=1}^n a_i f_i(x) \in \mathbf{Z}[x]$, so α is integral. □

Example 2.3.6. 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 $G/2G = 0$. (You can see that $G/2G = 0$ implies that G is not finitely generated, by assuming that G is finitely generated, using the structure theorem to write G as a product of cyclic groups, and noting that G has nontrivial 2-torsion.)

Proposition 2.3.7. *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. □

Definition 2.3.8 (Number field). 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 2.3.9 (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 $x^2 - x - 1$. 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 2.3.10 (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 2.3.11. *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 $\alpha = a/b \in \mathbf{Q}$ in lowest terms and $b > 0$. Since α is integral, $\mathbf{Z}[a/b]$ is finitely generated as a module, so $b = 1$ (see Example 2.3.6).

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 $\mathbf{Q}\mathcal{O}_K = K$. □

2.4 Norms and Traces

In this section we develop some basic properties of norms, traces, and discriminants, and give more properties of rings of integers in the general context of Dedekind domains.

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 extension of K generated by a, which is the smallest number field that contains both K and 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 are $\sqrt{2}$ and $-\sqrt{2}$.

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

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

We know 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 $(-1)^{\deg(f)}\det(\ell_a)$, and the coefficient of $x^{\deg(f)-1}$ is $-\mathrm{tr}(\ell_a)$.

Proposition 2.4.2. *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*

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

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 and is irreducible, since it is the polynomial in $K[x]$ of least degree

that is satisfied by a and K has characteristic 0. Since f is irreducible, we have $K(a) = K[x]/(f)$, so $[K(a) : K] = \deg(f)$. Also a satisfies a polynomial if and only if ℓ_a does, so 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 **??**). □

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

Corollary 2.4.3. *Suppose $K \subset L \subset M$ is a tower of number fields, and let $a \in M$. Then*

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

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 $\sigma'\tau_1, \ldots, \sigma'\tau_d$ 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 2.4.2.

Proposition 2.4.4. *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 2.3.11 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 $x = \sum_{i=1}^n c_i a_i \in \mathcal{O}_K$ 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 $x = \sum_{i=1}^n c_i a_i \in \mathcal{O}_K$ 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, which is 0 only on the element 0. 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. □

Corollary 2.4.5. *The ring of integers $\mathcal{O}_K$ of a number field is noetherian.*

Proof. By Proposition 2.4.4, 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 Theorem 2.2.9, $\mathcal{O}_K$ is noetherian. □

Chapter 3

Unique Factorization of Ideals

Unique factorization into irreducible elements frequently fails for rings of integers of number fields. In this chapter we will deduce the most important basic property of the ring of integers $\mathcal{O}_K$ of an algebraic number, namely that every nonzero *ideal* factors uniquely as a products of prime ideals. Along the way, we will introduce fractional ideals and prove that they form a group under multiplication. The class group of $\mathcal{O}_K$ is the quotient of this group by the principal fractional ideals.

3.1 Dedekind Domains

Recall (Corollary 2.4.5) 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* $\mathrm{Frac}(R)$ of R is the field of all equivalence classes of formal quotients a/b, where $a, b \in R$ with $b \neq 0$, and $a/b \sim c/d$ if $ad = bc$. For example, the field of fractions of $\mathbf{Z}$ is $\mathbf{Q}$ and the field of fractions of $\mathbf{Z}[(1+\sqrt{5})/2]$ is $\mathbf{Q}(\sqrt{5})$. The field of fractions of the ring $\mathcal{O}_K$ of integers of a number field K is just the number field K.

Definition 3.1.1 (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 3.1.2. *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 $\alpha \in \overline{\mathbf{Q}}$ 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 $f(\alpha) = 0$. 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 $f(\alpha) = 0$, we can write α^n

as a $\mathbf{Z}[a_0, \ldots, a_{n-1}]$-linear combination of α^i for $i < n$, so the ring $\mathbf{Z}[a_0, \ldots, a_{n-1}, \alpha]$ is also finitely generated as a $\mathbf{Z}$-module. Thus $\mathbf{Z}[\alpha]$ 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 $\alpha \in K$ is integral over $\mathcal{O}_K$. Then since $\overline{\mathbf{Z}}$ is integrally closed, α is an element of $\overline{\mathbf{Z}}$, so $\alpha \in K \cap \overline{\mathbf{Z}} = \mathcal{O}_K$, as required. □

Definition 3.1.3 (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.

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. The ring $\overline{\mathbf{Z}}$ is not noetherian, but it is integrally closed in its field of fraction, and every nonzero prime ideal is maximal.

Proposition 3.1.4. *The ring of integers $\mathcal{O}_K$ of a number field is a Dedekind domain.*

Proof. By Proposition 3.1.2, the ring $\mathcal{O}_K$ is integrally closed, and by Proposition 2.4.5 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.

Definition 3.1.5 (Fractional Ideal). A *fractional ideal* is a nonzero $\mathcal{O}_K$-submodule I of 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 integral ideal $I \subset \mathcal{O}_K$.

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

Theorem 3.1.6. *The set of fractional ideals of a Dedekind domain R is an abelian group under ideal multiplication with identity element $\mathcal{O}_K$.*

Note that fractional ideals are nonzero by definition, so it's not necessary to write "nonzero fractional ideals" in the statement of the theorem. Before proving Theorem 3.1.6 we prove a lemma. For the rest of this section $\mathcal{O}_K$ is the ring of integers of a number field K.

Definition 3.1.7 (Divides for Ideals). Suppose that I, J are ideals of $\mathcal{O}_K$. Then we say that 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 3.1.8. *Suppose I is a nonzero ideal of $\mathcal{O}_K$. Then there exist prime ideals $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$ such that $\mathfrak{p}_1 \cdot \mathfrak{p}_2 \cdots \mathfrak{p}_n \subset I$, i.e., I divides a product of prime ideals.*

Proof. Let S be the set of nonzero ideals of $\mathcal{O}_K$ that do satisfy the conclusion of the lemma. The key idea is to use that $\mathcal{O}_K$ is noetherian to show that S is the empty set. If S is nonempty, then $\mathcal{O}_K$ is noetherian, so 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 we may assume that I is not prime. Thus 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, say $\mathfrak{p}_1 \cdots \mathfrak{p}_r \subset J_1$ and $\mathfrak{q}_1 \cdots \mathfrak{q}_s \subset J_2$. Then

$$\mathfrak{p}_1 \cdots \mathfrak{p}_r \cdot \mathfrak{q}_1 \cdots \mathfrak{q}_s \subset J_1 J_2 = I^2 + I(b) + (a)I + (ab) \subset I,$$

so I contains a product of primes. This is a contradiction, since we assumed $I \in S$. Thus S is empty, which completes the proof. □

We are now ready to prove the theorem.

Proof of Theorem 3.1.6. 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 all nonzero integral ideals have inverses, and finally observe that every fractional ideal has an inverse. (Note: Once we know that the set of fractional ideals is a group, it will follows that inverses are unique; until then we will be careful to write "an" instead of "the".)

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 since $\mathfrak{p}$ is maximal, 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 $d \in I$, with $d \notin \mathcal{O}_K$. Since $I\mathfrak{p} = \mathfrak{p}$, such a d would leave $\mathfrak{p}$ invariant, i.e., $d\mathfrak{p} \subset \mathfrak{p}$. Since $\mathfrak{p}$ is an $\mathcal{O}_K$-module we will see that it will follow that $d \in \mathcal{O}_K$, a contradiction.

By Lemma 3.1.8, we can choose a product $\mathfrak{p}_1, \ldots, \mathfrak{p}_m$, with m minimal, with

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

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 $\mathbf{Z}$ (because d satisfies the minimal polynomial of ℓ_d, by the Cayley-Hamilton theorem). This implies that d is integral over $\mathbf{Z}$, so $d \in \mathcal{O}_K$, since $\mathcal{O}_K$ is integrally closed by Proposition 3.1.2. (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 3.1.5, 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

$$I \subset \mathfrak{p}^{-1}I \subset \mathfrak{p}^{-1}\mathfrak{p} = \mathcal{O}_K.$$

If $I = \mathfrak{p}^{-1}I$, then arguing as in the proof that $\mathfrak{p}^{-1}$ is an 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, upon multiplying both sides by $\mathfrak{p}$, 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 J. Then $\mathfrak{p}^{-1}J$ is an inverse of I, since $(J\mathfrak{p}^{-1})I = J(\mathfrak{p}^{-1}I) = \mathcal{O}_K$. □

We can finally deduce the crucial Theorem 3.1.10, 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 ideals to mathematics over a century ago.

Theorem 3.1.9. *Suppose I is a nonzero 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.

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 3.1.6 we can cancel I from both sides of this equation to see that $\mathfrak{p}^{-1} = \mathcal{O}_K$, a contradiction. Since $\mathcal{O}_K \subset \mathfrak{p}^{-1}$, we have $I \subset I\mathfrak{p}^{-1}$, and by the above observation I is strictly contained in $I\mathfrak{p}^{-1}$. 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 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 by multiplying both sides by the inverse. Repeating this argument finishes the proof of uniqueness. □

Theorem 3.1.10. *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 3.1.10 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 3.1.10 □

Example 3.1.11. The ring of integers of $K = \mathbf{Q}(\sqrt{-6})$ is $\mathcal{O}_K = \mathbf{Z}[\sqrt{-6}]$. 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 3.1.9, however, implies that the principal ideal (6) can, however, be written uniquely as a product of prime ideals. An explicit decomposition is

$$(6) = (2, 2 + \sqrt{-6})^2 \cdot (3, 3 + \sqrt{-6})^2, \tag{3.1.1}$$

where each of the ideals $(2, 2 + \sqrt{-6})$ and $(3, 3 + \sqrt{-6})$ is prime. We will discuss algorithms for computing such a decomposition in detail in Chapter 5. 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 finite (as a set) ring $\mathcal{O}_K/p\mathcal{O}_K$.

The factorization (3.1.1) can be compute using MAGMA (see [BCP97]) as follows:

```
> R<x> := PolynomialRing(RationalField());
> K := NumberField(x^2+6);
> OK := RingOfIntegers(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 factorization (3.1.1) can also be computed using PARI (see [ABC$^+$]).

```
? k=nfinit(x^2+6);
? idealfactor(k, 6)
[[2, [0, 1]~, 2, 1, [0, 1]~] 2]
[[3, [0, 1]~, 2, 1, [0, 1]~] 2]
? k.zk
[1, x]
```

The output of PARI is a list of two prime ideals with exponent 2. A prime ideal is represented by a 5-tuple $[p, a, e, f, b]$, where the ideal is $p\mathcal{O}_K + \alpha\mathcal{O}_K$, where $\alpha = \sum a_i\omega_i$, where $\omega_1, \ldots, \omega_n$ are a basis for $\mathcal{O}_K$ (as output by `k.zk`).

Chapter 4

Computing

4.1 Algorithms for Algebraic Number Theory

The main algorithmic goals in algebraic number theory are to solve the following problems quickly:

- **Ring of integers:** Given a number field K, specified by an irreducible polynomial with coefficients in $\mathbf{Q}$, compute the ring of integers $\mathcal{O}_K$.
- **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 class group of K, i.e., 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 U_K of units of $\mathcal{O}_K$.

This chapter is about how to compute the first two using a computer.

The best overall reference for algorithms for doing basic algebraic number theory computations is [Coh93]. This chapter is not about algorithms for solving the above problems; instead is a tour of the two most popular programs for doing algebraic number theory computations, Magma and PARI. These programs are both available to use via the web page

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

The following two sections illustrate what we've done so far in this book, and a little of where we are going. First we describe Magma then PARI.

4.2 Magma

This section is a first introduction to Magma for algebraic number theory. Magma is a general purpose package for doing algebraic number theory computations, but

it is closed source and not free. Its development and maintenance at the University of Sydney is paid for by grants and subscriptions. I have visited Sydney three times to work with them, and I also wrote the modular forms parts of MAGMA.

The documentation for MAGMA is available here:

`http://magma.maths.usyd.edu.au/magma/htmlhelp/MAGMA.htm`

Much of the algebraic number theory documentation is here:

`http://magma.maths.usyd.edu.au/magma/htmlhelp/text711.htm`

4.2.1 Smith Normal Form

In Section 2.1 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 $\left(\begin{smallmatrix} 1 & 0 \\ 0 & 2 \end{smallmatrix}\right)$. 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.
```

`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 random entries between 0 and 100, 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 V2.11-10. These timings below are on an Opteron 248 server.

```
> n := 50; A := Matrix(n,n,[Random(100) : i in [1..n^2]]);
> time B := SmithForm(A);
Time: 0.020
> n := 100; A := Matrix(n,n,[Random(100) : i in [1..n^2]]);
> time B := SmithForm(A);
Time: 0.210
> n := 150; A := Matrix(n,n,[Random(100) : i in [1..n^2]]);
```

```
> time B := SmithForm(A);
Time: 1.240
> n := 200; A := Matrix(n,n,[Random(100) : i in [1..n^2]]);
> time B := SmithForm(A);
Time: 4.920
```

Remark 4.2.1. The same timings on a 1.8Ghz Pentium M notebook are `0.030, 0.410, 2.910, 10.600`, respectively, so about twice as long. On a G5 XServe (with Magma V2.11-2), they are `0.060, 0.640, 3.460, 12.270`, respectively, which is nearly three times as long as the Opteron (MAGMA seems very poorly optimized for the G5, so watch out).

4.2.2 Number Fields

To define a number field, we first define the polynomial ring over the rational numbers. The notation `R<x>` below means "the variable `x` is the generator of the polynomial ring". We then pass an irreducible polynomial ot the `NumberField` function.

```
> 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
```

4.2.3 Relative Extensions

If K is a number field, and $f(x) \in K[x]$ is an irreducible polynomial, and α is a root of f, then $L = K(\alpha) \cong K[x]/(f)$ is a *relative extension* of K. MAGMA can compute with relative extensions, and also find the corresponding absolute extension of $\mathbf{Q}$, i.e., find a polynomial g such that $K[x]/(f) \cong \mathbf{Q}[x]/(g)$.

The following illustrates defining $L = K(\sqrt{a})$, where $K = \mathbf{Q}(a)$ and $a = \sqrt[3]{2}$.

```
> R<x> := PolynomialRing(RationalField());
> K<a> := NumberField(x^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
```

4.2.4 Rings of integers

MAGMA can compute rings of integers of number fields.

```
> R<x> := PolynomialRing(RationalField());
> K<a> := NumberField(x^3-2);   // a is the image of x in Q[x]/(x^3-2)
> RingOfIntegers(K);
Maximal Equation Order with defining polynomial x^3 - 2 over ZZ
```

Sometimes the ring of integers of $\mathbf{Q}(a)$ is not $\mathbf{Z}[a]$. 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
```

Printing $\mathcal{O}_K$ gave us no real information. Instead we request a basis for $\mathcal{O}_K$:

```
> Basis(O);
[
    O.1,
    O.2
]
```

Again we get no information. To get a basis for $\mathcal{O}_K$ in terms of $a = \sqrt{3/2}$, we use MAGMA's coercion operator `!`:

```
> [K!x : x in Basis(O)];
[
    1,
    2*a
]
```

Thus the ring of integers has basis 1 and $2\sqrt{3/2} = \sqrt{6}$ as a $\mathbf{Z}$-module.

Here are some more examples, which we've reformated for publication.

```
> procedure ints(f)   // (procedures don't return anything; functions do)
      K<a> := NumberField(f);
      O := RingOfIntegers(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(&+[i*x^i + 2*x+1: i in [0..d]]);
[
    1, 10*a, ...
]
Time: 0.030
> d := 15; time ints(&+[i*x^i + 2*x+1: i in [0..d]]);
...
Time: 0.160
> d := 20; time ints(&+[i*x^i + 2*x+1: i in [0..d]]);
...
Time: 1.610
> d := 21; time ints(&+[i*x^i + 2*x+1: i in [0..d]]);
...
Time: 0.640
> d := 22; time ints(&+[i*x^i + 2*x+1: i in [0..d]]);
...
```

```
Time: 3.510
> d := 23; time ints(&+[i*x^i + 2*x+1: i in [0..d]]);
...
Time: 12.020
> d := 24; time ints(&+[i*x^i + 2*x+1: i in [0..d]]);
...
Time: 34.480
> d := 24; time ints(&+[i*x^i + 2*x+1: i in [0..d]]);
...
Time: 5.580 -- the timings very *drastically* on the same problem,
because presumably some randomized algorithms are used.
> d := 25; time ints(&+[i*x^i + 2*x+1: i in [0..d]]);
...
Time: 70.350
> d := 30; time ints(&+[i*x^i + 2*x+1: i in [0..d]]);
Time: 136.740
```

Recall that an order is a subring of $\mathcal{O}_K$ of finite index as an additive group. We can also define orders in rings of integers in MAGMA.

```
> 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 := RingOfIntegers(K);
> Index(OK,O);
8
```

4.2.5 Ideals

We can construct ideals in rings of integers of number fields in MAGMA as illustrated.

```
> R<x> := PolynomialRing(RationalField());
> K<a> := NumberField(x^2-5);
> OK := RingOfIntegers(K);
> 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]
> Generators(J);
[    [-1, 2]  ]
> K!Generators(J)[1];
a
> 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 := RingOfIntegers(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>
]
```

4.3 Using PARI

PARI is freely available (under the GPL) from

`http://pari.math.u-bordeaux.fr/`

The above website describes PARI thus:

> PARI/GP is a widely used computer algebra system designed for fast computations in number theory (factorizations, algebraic number theory, elliptic curves...), but also contains a large number of other useful functions to compute with mathematical entities such as matrices, polynomials, power series, algebraic numbers etc., and a lot of transcendental

functions. PARI is also available as a C library to allow for faster computations.

Originally developed by Henri Cohen and his co-workers (Universit Bordeaux I, France), PARI is now under the GPL and maintained by Karim Belabas (Universit Paris XI, France) with the help of many volunteer contributors.

The sections below are very similar to the MAGMA sections above, except they address PARI instead of MAGMA. We use Pari Version 2.2.9-alpha for all examples below, and all timings are on an Opteron 248.

4.3.1 Smith Normal Form

In Section 2.1 we learned about Smith normal forms of matrices. We create matrices in PARI by giving the entries of each row separated by a `;`.

```
? A = [1,2;3,4];
? A
[1 2]
[3 4]
? matsnf(A)
[2, 1]
```

The `matsnf` function computes the diagonal entries of the Smith normal form of a matrix. To get documentation about a function PARI, type `?` followed by the function name.

```
? ?matsnf
matsnf(x,{flag=0}): Smith normal form (i.e. elementary divisors)
of the matrix x, expressed as a vector d. Binary digits of flag
mean 1: returns [u,v,d] where d=u*x*v, otherwise only the diagonal d
        is returned,
     2: allow polynomial entries, otherwise assume x is integral,
     4: removes all information corresponding to entries equal
        to 1 in d.
```

Next, let's test the limits. To time code in PARI use the `gettime` function:

```
? ?gettime
gettime(): time (in milliseconds) since last call to gettime.
```

If we divide the result of `gettime` by 1000 we get the time in seconds.

We make a 10×10 integer matrix with random entries between 0 and 100, and compute its Smith normal form.

```
> n=10;A=matrix(n,n,i,j,random(101));gettime;B=matsnf(A);gettime/1000.0
%7 = 0.00100000000000000000000000000000000000000
```

Let's see how big we have to make A in order to slow down PARI 2.2.9-alpha. These timings below are on an Opteron 248 server.

```
? n=50;A=matrix(n,n,i,j,random(101));gettime;B=matsnf(A);gettime/1000.0
0.058
? n=100;A=matrix(n,n,i,j,random(101));gettime;B=matsnf(A);gettime/1000.0
1.39200000000000000000000000000000000000
? n=150;A=matrix(n,n,i,j,random(101));gettime;B=matsnf(A);gettime/1000.0
30.73100000000000000000000000000000000000
? n=200;A=matrix(n,n,i,j,random(101));gettime;B=matsnf(A);gettime/1000.0
  *** matsnf: the PARI stack overflows !
  current stack size: 8000000 (7.629 Mbytes)
  [hint] you can increase GP stack with allocatemem()
? allocatemem(); allocatemem(); allocatemem()
  *** allocatemem: Warning: doubling stack size; new stack = 16000000 (15.259 Mbytes).
? n=200;A=matrix(n,n,i,j,random(101));gettime;B=matsnf(A);gettime/1000.0
35.74200000000000000000000000000000000000
```

Remark 4.3.1. The same timings on a 1.8Ghz Pentium M notebook are `0.189, 5.489, 48.185, 170.21`, respectively. On a G5 XServe, they are `0.19, 5.70, 41.95, 153.98`, respectively.

Recall that the timings for the same computation on the Opteron under MAGMA are `0.020, 0.210, 1.240, 4.290`, which is *vastly* faster than PARI.

4.3.2 Number Fields

There are several ways to define number fields in PARI. The simplest is to give a monic integral polynomial as input to the `nfinit` function.

```
? K = nfinit(x^3-2);
```

Number fields do not print as nicely in PARI as in MAGMA:

```
? K
K
%12 = [x^3 - 2, [1, 1], -108, 1, [[1, 1.259921049894873164767210606072782283506,
 ... and tons more numbers! ...
```

Confusingly, elements of number fields can be represented in PARI in many different ways. I refer you to the documentation for PARI (§3.6). A simple way is as polymods:

```
? a = Mod(x, x^3-2)  \\ think of this as x in Q[x]/(x^3-2).
? a
Mod(x, x^3 - 2)
? a^3
Mod(2, x^3 - 2)
```

4.3.3 Rings of integers

To compute the ring of integers of a number field in PARI, use the `nfbasis` command.

```
? ?nfbasis
nfbasis(x,{flag=0},{p}): integral basis of the field Q[a], where a is
a root of the polynomial x, using the round 4 algorithm. Second and
third args are optional.   Binary digits of flag means:
   1: assume that no square of a prime>primelimit divides the
      discriminant of x,
   2: use round 2 algorithm instead.
If present, p provides the matrix of a partial factorization of the
discriminant of x, useful if one wants only an order maximal at
certain primes only.
```

For example, we compute the ring of integers of $\mathbf{Q}(\sqrt[3]{2})$.

```
? nfbasis(x^3-2)
[1, x, x^2]
? nfbasis(2*x^2-3)
[1, 2*x]
```

Here are some more examples, which we've reformated for publication.

```
> nfbasis(x^2-5)
[1, 1/2*x + 1/2]
? nfbasis(x^3-17)
[1, x, 1/3*x^2 - 1/3*x + 1/3]
? nfbasis(polcyclo(7))
[1, x, x^2, x^3, x^4, x^5]

? d=10; f=sum(i=0,d,i*x^i+2*x+1); gettime; nfbasis(f); gettime/1000.0
0.01100000000000000000000000000000000000000
? d=15; f=sum(i=0,d,i*x^i+2*x+1); gettime; nfbasis(f); gettime/1000.0
0.02700000000000000000000000000000000000000
? d=20; f=sum(i=0,d,i*x^i+2*x+1); gettime; nfbasis(f); gettime/1000.0
1.66900000000000000000000000000000000000000
? d=20; f=sum(i=0,d,i*x^i+2*x+1); gettime; nfbasis(f); gettime/1000.0
1.66400000000000000000000000000000000000000
? d=21; f=sum(i=0,d,i*x^i+2*x+1); gettime; nfbasis(f); gettime/1000.0
0.08000000000000000000000000000000000000000
? d=22; f=sum(i=0,d,i*x^i+2*x+1); gettime; nfbasis(f); gettime/1000.0
1.50000000000000000000000000000000000000000
? d=23; f=sum(i=0,d,i*x^i+2*x+1); gettime; nfbasis(f); gettime/1000.0
12.28800000000000000000000000000000000000000
```

```
? d=24; f=sum(i=0,d,i*x^i+2*x+1); gettime; nfbasis(f); gettime/1000.0
1.6380000000000000000000000000000000000000
? d=25; f=sum(i=0,d,i*x^i+2*x+1); gettime; nfbasis(f); gettime/1000.0
38.1410000000000000000000000000000000000000
? d=30; f=sum(i=0,d,i*x^i+2*x+1); gettime; nfbasis(f); gettime/1000.0
33.4230000000000000000000000000000000000000
? d=30; f=sum(i=0,d,i*x^i+2*x+1); gettime; nfbasis(f); gettime/1000.0
33.0660000000000000000000000000000000000000  \\ doesn't vary much
```

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

Recall that the timing in MAGMA for computing $\mathcal{O}_K$ for $d = 30$ was 136.740 seconds, which is four times as long as the 33 second timing of PARI.[1] Thus for the fields considered above, computation of $\mathcal{O}_K$ in PARI is faster than in MAGMA. Sometimes one system is *much* better than another, and it is not clear a priori which will be better.

4.3.4 Ideals

In PARI ideals can be represented in several ways. For example, to construct a principal ideal, give the generator. There is no ideal data type, but you can give data that defines an ideal, e.g., an alement to define a principal ideal, to functions that take ideals as input.

The following examples illustrate basic arithmetic with ideals and factorization of ideals.

```
? a = Mod(x, x^2-5)
%41 = Mod(x, x^2 - 5)
? nf = nfinit(x^2-5);
? idealadd(nf, 5*a, 10*a)
%44 =
[25 15]
[ 0  5]
```

The output of `idealadd` is a 2-column matrix, whose columns represent elements of K on the integral basis for $\mathcal{O}_K$ output by `nfbasis`. These two elements generate the ideal as an $\mathcal{O}_K$-module. We will prove later (see Prop. 6.3.2) that every ideal can be generated by 2 elements.

Note that fractional ideals are also allowed:

[1] I onced discussed timings of PARI versus MAGMA with John Cannon, who is the director of MAGMA. He commented that in some cases PARI implicitly assumes unproven conjectures, e.g., the Riemann Hypothesis, in order to get such fast algorithms, whereas the philosophy in MAGMA is to not assume conjectures unless one explicitly asks it to.

```
? idealadd(nf, a/5, 10*a)
%45 =
[1 3/5]
[0 1/5]
```

We can also factor an ideal as a product of prime ideals. The output is an arrays of pairs, a prime ideal and its exponent. These ideals are represented in yet another way, as a 5-tuple $[p, a, e, f, b]$, where a is a vector of integers. Such a tuple corresponds to the ideal $p\mathcal{O}_K + \alpha\mathcal{O}_K$, where $\alpha = \sum a_i\omega_i$, and the ω_i are the basis output by `nfbasis`. Explaining e, f, b requires ideas that we have not yet introduced (ramification, inertia degrees, etc.) Here are some examples:

```
? nf = nfinit(x^2-5);
? idealfactor(nf, 7)
%46 =
[[7, [7, 0]~, 1, 2, [1, 0]~] 1]

? idealfactor(nf, 3)
%47 =
[[3, [3, 0]~, 1, 2, [1, 0]~] 1]

? idealfactor(nf, 5)
%48 =
[[5, [1, 2]~, 2, 1, [1, 2]~] 2]

? idealfactor(nf, 11)
%49 =
[[11, [-3, 2]~, 1, 1, [5, 2]~] 1]
[[11, [5, 2]~, 1, 1, [-3, 2]~] 1]
```

We can even factor fractional ideals:

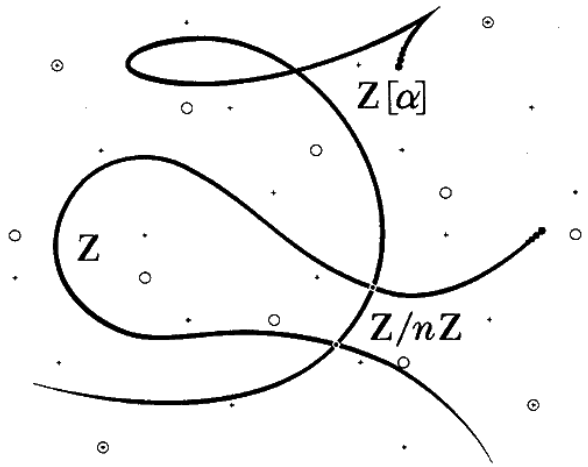
```
? idealfactor(nf, 1/11)
%50 =
[[11, [-3, 2]~, 1, 1, [5, 2]~] -1]
[[11, [5, 2]~, 1, 1, [-3, 2]~] -1]
```

Chapter 5

Factoring Primes

Let p be a prime and $\mathcal{O}_K$ the ring of integers of a number field. This chapter is about how to write $p\mathcal{O}_K$ as a product of prime ideals of $\mathcal{O}_K$. Paradoxically, computing the explicit prime ideal factorization of $p\mathcal{O}_K$ is easier than computing $\mathcal{O}_K$.

5.1 The Problem



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*, 1st ed., pg 265

Bill Gates meant[1] factoring products of two primes, which would break the RSA cryptosystem (see e.g. [Ste, §3.2]). However, perhaps he really meant what he said: then we might imagine that he meant factorization of primes of $\mathbf{Z}$ in rings of integers of number fields. For example, $2^{16}+1 = 65537$ is a "large" prime, and in $\mathbf{Z}[i]$ we have $(65537) = (65537, 2^8+i)\cdot(65537, 2^8-i)$.

5.1.1 Geomtric Intuition

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

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

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 example, if

$$\mathfrak{p} = (65537, 2^8+i) \subset \mathbf{Z}[i],$$

then $\mathfrak{p} \cap \mathbf{Z} = (65537)$. For more on this viewpoint, see [Har77] and [EH00, Ch. 2].

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 $\pi^{-1}(p\mathbf{Z})$, where the exponents e_i are the multiplicities of the fibers. Notice that the elements of $\pi^{-1}(p\mathbf{Z})$ are the prime ideals of $\mathcal{O}_K$ that contain p, i.e., the primes that divide $p\mathcal{O}_K$.

This chapter is about how to compute the $\mathfrak{p}_i$ and e_i.

5.1.2 Examples

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 $x^5+7x^4+3x^2-x+1$ and $p = 2$ and 5 (see Section 5.4 for PARI versions):

```
> R<x> := PolynomialRing(RationalField());
> K<a> := NumberField(x^5 + 7*x^4 + 3*x^2 - x + 1);
> OK := RingOfIntegers(K);
> [K!OK.i : i in [1..5]];
```

[1] This quote is on page 265 of the first edition. In the second edition, on page 303, this sentence is changed to "The obvious mathematical breakthrough that would defeat our public key encryption would be the development of an easy way to factor large numbers." This is less nonsensical; however, fast factoring is *not* known to break all commonly used public-key cryptosystem. For example, there are cryptosystems based on the difficulty of computing discrete logarithms in $\mathbf{F}_p^*$ and on elliptic curves over $\mathbf{F}_p$, which (presumably) would not be broken even if one could factor large numbers quickly.

```
[ 1, a, a^2, a^3, a^4 ]
> 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>]
```

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 5.3.2 below illustrates.) When $\mathcal{O}_K = \mathbf{Z}[a]$ it is relatively easy to factor $p\mathcal{O}_K$, at least assuming one can factor polynomials in $\mathbf{F}_p[x]$. 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:

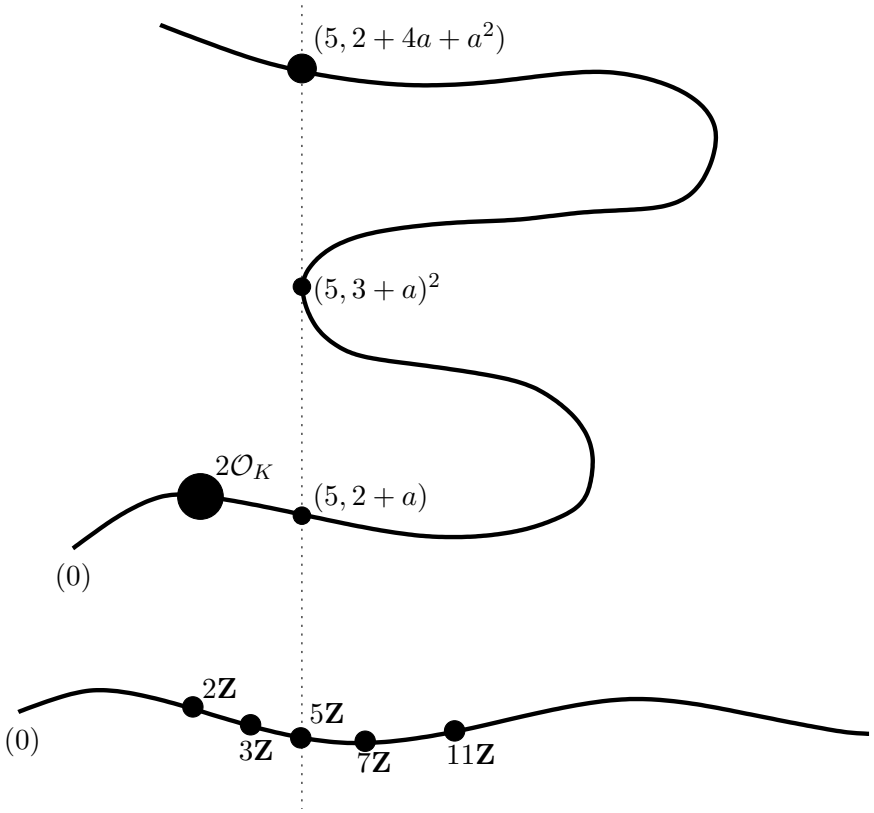


Diagram of $\mathrm{Spec}(\mathcal{O}_K) \to \mathrm{Spec}(\mathbf{Z})$

5.2 A Method for Factoring Primes that Often Works

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

$$\begin{array}{ccc} \bigcup \mathrm{Spec}(\mathcal{O}_K/\mathfrak{p}_i^{e_i}) & \hookrightarrow & \mathrm{Spec}(\mathcal{O}_K) \\ \downarrow & & \downarrow \\ \bigcup \mathrm{Spec}(\mathbf{F}_p[x]/(\overline{f}_i^{e_i})) & \hookrightarrow & \mathrm{Spec}(\mathbf{Z}[a]) \\ \downarrow & & \downarrow \\ \mathrm{Spec}(\mathbf{F}_p) & \hookrightarrow & \mathrm{Spec}(\mathbf{Z}) \end{array}$$

where $\overline{f} = \prod_i \overline{f}_i^{e_i}$ is the factorization of the image of f in $\mathbf{F}_p[x]$, and $p\mathcal{O}_K = \prod \mathfrak{p}_i^{e_i}$ is the factorization of $p\mathcal{O}_K$ in terms of prime ideals of $\mathcal{O}_K$. On the level of rings, the bottom horizontal map is the quotient map $\mathbf{Z} \to \mathbf{Z}/p\mathbf{Z} \cong \mathbf{F}_p$. The middle

horizontal map is induced by

$$\mathbf{Z}[x] \to \bigoplus_i \mathbf{F}_p[x]/(\overline{f}_i^{e_i}),$$

and the top horizontal map is induced by

$$\mathcal{O}_K \to \mathcal{O}_K/p\mathcal{O}_K \cong \bigoplus \mathcal{O}_K/\mathfrak{p}_i^{e_i},$$

where the isomorphism is by the Chinese Remainder Theorem, which we will prove in Chapter 6. The left vertical maps come from the inclusions

$$\mathbf{F}_p \hookrightarrow \mathbf{F}_p[x]/(\overline{f}_i^{e_i}) \hookrightarrow \mathcal{O}_K/\mathfrak{p}_i^{e_i},$$

and the right from the inclusions $\mathbf{Z} \hookrightarrow \mathbf{Z}[a] \hookrightarrow \mathcal{O}_K$.

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 $f(x)$, in the sense that $\mathbf{Z}[a] \cong \mathbf{Z}[x]/(f(x))$. 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 $\varphi : \mathbf{Z}[x]/(f) \to \overline{\mathbf{F}}_p$ up to automorphisms of the image, which is in turn the same as giving a root of f in $\overline{\mathbf{F}}_p$ up to automorphism, which is the same as giving an irreducible factor of the reduction of f modulo p.

Lemma 5.2.1. *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 primes that appear in the factorization of $p\mathcal{O}_K$.*

Proof. Fix a basis for $\mathcal{O}_K$ and for $\mathbf{Z}[a]$ as $\mathbf{Z}$-modules. Form the matrix A whose columns express each basis element of $\mathbf{Z}[a]$ as a $\mathbf{Z}$-linear combination of the basis for $\mathcal{O}_K$. Then

$$\det(A) = \pm[\mathcal{O}_K : \mathbf{Z}[a]]$$

is coprime to p, by hypothesis. Thus the reduction of A modulo p is invertible, so it defines an isomorphism $\mathbf{Z}[a]/p\mathbf{Z}[a] \cong \mathcal{O}_K/p\mathcal{O}_K$.

Let $\overline{\mathbf{F}}_p$ denote a fixed algebraic closure of $\mathbf{F}_p$; thus $\overline{\mathbf{F}}_p$ is an algebraically closed field of characteristic p, over which all polynomials in $\mathbf{F}_p[x]$ factor into linear factors. Any homomorphism $\mathcal{O}_K \to \overline{\mathbf{F}}_p$ send p to 0, so is the composition of a homomorphism $\mathcal{O}_K \to \mathcal{O}_K/p\mathcal{O}_K$ with a homomorphism $\mathcal{O}_K/p\mathcal{O}_K \to \overline{\mathbf{F}}_p$. Since $\mathcal{O}_K/p\mathcal{O}_K \cong \mathbf{Z}[a]/p\mathbf{Z}[a]$, the homomorphisms $\mathcal{O}_K \to \overline{\mathbf{F}}_p$ are in bijection with the homomorphisms $\mathbf{Z}[a] \to \overline{\mathbf{F}}_p$. The homomorphisms $\mathbf{Z}[a] \to \overline{\mathbf{F}}_p$ are in bijection with the roots of the reduction modulo p of the minimal polynomial of a in $\overline{\mathbf{F}}_p$. □

Remark 5.2.2. Here is a "high-brow" proof of Lemma 5.2.1. 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 $\mathbf{Z}[a] \otimes \mathbf{F}_p \cong \mathcal{O}_K \otimes \mathbf{F}_p$.

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 $\mathfrak{p} = (f(a), p)\mathbf{Z}[a]$ is a maximal ideal of $\mathbf{Z}[a]$, then the ideal $\mathfrak{p}' = (f(a), p)\mathcal{O}_K$ of $\mathcal{O}_K$ is also maximal, since

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

where $\tilde{a}$ denotes the image of a in $\mathcal{O}_K/p\mathcal{O}_K$.

We formalize the above discussion in the following theorem (note: we will not prove that the powers are e_i here):

Theorem 5.2.3. *Let $f \in \mathbf{Z}[x]$ be the minimal polynomial of a over $\mathbf{Z}$. 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 $f = x^5 + 7x^4 + 3x^2 - x + 1$. According to MAGMA, the ring of integers $\mathcal{O}_K$ has discriminant 2945785:

```
> R<x> := PolynomialRing(RationalField());
> K<a> := NumberField(x^5 + 7*x^4 + 3*x^2 - x + 1);
> Discriminant(RingOfIntegers(K));
2945785
```

The order $\mathbf{Z}[a]$ has the same discriminant as $f(x)$, which is the same as the discriminant of $\mathcal{O}_K$, so $\mathbf{Z}[a] = \mathcal{O}_K$ and we can apply the above theorem. (Here we use that the index of $\mathbf{Z}[a]$ in $\mathcal{O}_K$ is the square of the quotient of their discriminants, a fact we will prove later in Section 7.2.)

```
> 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(RingOfIntegers(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(RingOfIntegers(K));
95367431640625    // divisible by 5
> Factorization(S!f);
[   <t, 5>   ]
```

5.3 A General Method

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 5.2.3 can be used to factor 2 for K (see Example 5.3.2 below).

5.3.1 Essential Discriminant Divisors

Definition 5.3.1. A prime p is an *essential discriminant divisor* if $p \mid [\mathcal{O}_K : \mathbf{Z}[a]]$ for *every* $a \in \mathcal{O}_K$.

See Example 7.2.5 below for why is it called an essential "discriminant" instead of an essential "index divisor".

Since $[\mathcal{O}_K : \mathbf{Z}[a]]^2$ 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 5.3.2 *(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 := RingOfIntegers(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, and one sees directly from the above expressions 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 f, then $\overline{f}(x) \in \mathbf{F}_2[x]$ must be a product of three *distinct* linear factors, which is impossible, since the only linear polynomials in $\mathbf{F}_2[x]$ are x and $x+1$.

5.3.2 Remarks on Ideal Factorization in General

Recall (from Definition 2.3.10) that an *order* in $\mathcal{O}_K$ is a subring $\mathcal{O}$ of $\mathcal{O}_K$ that has finite index in $\mathcal{O}_K$. For example, if $\mathcal{O}_K = \mathbf{Z}[i]$, then $\mathcal{O} = \mathbf{Z} + 5\mathbf{Z}[i]$ is an order in $\mathcal{O}_K$, and as an abelian group $\mathcal{O}_K/\mathcal{O}$ is cyclic of order 5.

Most algebraic number theory books do not describe an algorithm for decomposing primes in the general case. Fortunately, Cohen's book [Coh93, Ch. 6] does

describe how to solve the general problem, in more than one way. The algorithms are nontrivial, and occupy a substantial part of Chapter 6 of Cohen's book. Our goal for the rest of this section is to give a hint as to what goes into them.

The general solutions to prime ideal factorization are somewhat surprising, since the algorithms are much more sophisticated than the one suggested by Theorem 5.2.3. However, these complicated algorithms all run very quickly in practice, even without assuming the maximal order is already known. In fact, they avoid computing $\mathcal{O}_K$ altogether, and instead compute only an order $\mathcal{O}$ that is *p-maximal*, i.e., is such that $p \nmid [\mathcal{O}_K : \mathcal{O}]$.

For simplicity we consider the following slightly easier problem whose solution illustrates the key ideas needed in the general case.

Problem 5.3.3. 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.

Given a prime p that we wish to factor in $\mathcal{O}_K$, we first find a p-maximal order $\mathcal{O}$. We then use a solution to Problem 5.3.3 to find the prime ideals $\mathfrak{p}$ of $\mathcal{O}$ that contain p. Second, we find the exponents e such that $\mathfrak{p}^e$ exactly divides $p\mathcal{O}$. The resulting factorization in $\mathcal{O}$ completely determines the factorization of $p\mathcal{O}_K$.

A p-maximal order can be found reasonably quickly in practice using algorithms called "round 2" and "round 4". To compute $\mathcal{O}_K$, given an order $\mathbf{Z}[\alpha] \subset \mathcal{O}_K$, one takes a sum of p-maximal orders, one for every p such that p^2 divides $\mathrm{Disc}(\mathbf{Z}[\alpha])$. The time-consuming part of this computation is finding the primes p such that $p^2 \mid \mathrm{Disc}(\mathbf{Z}[\alpha])$, not finding the p-maximal orders. This example illustrates that a fast algorithm for factoring integers would not only break the RSA cryptosystems, but would massively speed up computation of the ring of integers of a number field.

Remark 5.3.4. The MathSciNet review of [BL94] by J. Buhler contains the following:

> A result of Chistov says that finding the ring of integers $\mathcal{O}_K$ in an algebraic number field K is equivalent, under certain polynomial time reductions, to the problem of finding the largest squarefree divisor of a positive integer. No feasible (i.e., polynomial time) algorithm is known for the latter problem, and it is possible that it is no easier than the more general problem of factoring integers.

Thus it appears that computing the ring $\mathcal{O}_K$ is quite hard.

5.3.3 Finding a p-Maximal Order

Before describing the general factorization algorithm, we sketch some of the theory behind the general algorithms for computing a p-maximal order $\mathcal{O}$ in $\mathcal{O}_K$. The main input is the following theorem, whose proof can be found in [Coh93, §6.1.1].

Theorem 5.3.5 (Pohst-Zassenhaus). *Let $\mathcal{O}$ be an order in the the ring of integers $\mathcal{O}_K$ of a number field, let $p \in \mathbf{Z}$ be a prime, and let*

$$I_p = \{x \in \mathcal{O} : x^m \in p\mathcal{O} \text{ for some } m \geq 1 \} \subset \mathcal{O}$$

be the radical of $p\mathcal{O}$, which is an ideal of $\mathcal{O}$. Let

$$\mathcal{O}' = \{x \in K : xI_p \subset I_p\}.$$

Then $\mathcal{O}'$ is an order and either $\mathcal{O}' = \mathcal{O}$, in which case $\mathcal{O}$ is p-maximal, or $\mathcal{O} \subset \mathcal{O}'$ and p divides $[\mathcal{O}' : \mathcal{O}]$.

After deciding on how to represent elements of K and orders and ideals in K, one can give an efficient algorithm to compute the $\mathcal{O}'$ of the theorem. The algorithm mainly involves linear algebra over finite fields. It is complicated to describe, but efficient in practice, and is conceptually simple—just compute $\mathcal{O}'$. The trick for reducing the computation of $\mathcal{O}'$ to linear algebra is the following lemma:

Lemma 5.3.6. *Define a homomorphism map $\psi : \mathcal{O} \hookrightarrow \mathrm{End}(I_p/pI_p)$ given by sending $\alpha \in \mathcal{O}$ to left multiplication by the reduction of α modulo p. Then*

$$\mathcal{O}' = \frac{1}{p}\,\mathrm{Ker}(\psi).$$

Note that to give an algorithm one must also figure out how to compute I_p/pI_p and the kernel of this map. This is all done in [Coh93, §6.1].

5.3.4 General Factorization Algorithm

We finally give an algorithm to factor $p\mathcal{O}_K$ in general.

Algorithm 5.3.7 (General Factorization). 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 $\mathbf{Z}[a]$. For any prime $p \in \mathbf{Z}$, the following algorithm computes the set of maximal ideals of $\mathcal{O}$ that contain p.

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 using Theorem 5.2.3 we 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. Note that $p\mathcal{O} \subset I$, i.e., $I \mid p\mathcal{O}$; also I is the product of the primes that divide p, without multiplicity. Using linear algebra over the finite field $\mathbf{F}_p$, we compute a basis for $I/p\mathcal{O}$, hence I, since $p\mathcal{O} \subset I$.

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 $p\mathcal{O} \subset I$. Note that $\mathcal{O}/p\mathcal{O}$ is obtained by simply reducing the basis $w_1, \ldots, w_n$ modulo p.

4. [Decompose quotient] The ring A decomposes as a product $A \cong \prod \mathbf{F}_p[x]/(g_i(x))$ of fields. We can find such a decomposition explicitly using linear algebra.

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

Algorithm 5.3.7 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 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. Note that we do not find the powers of primes that divide p in Algorithm 5.3.7; that's left to another algorithm that we will not discuss in this book.

Algorithm 5.3.7 was invented by J. Buchmann and H. W. Lenstra, though their paper seems to have never been published; however, the algorithm is described in detail in [Coh93, §6.2.5]. Incidentally, this chapter is based on Chapters 4 and 6 of [Coh93], which is highly recommended, and goes into much more detail about these algorithms.

5.4 Appendix: The Calculations in PARI

In this section we give PARI versions of all the MAGMA calculations in the rest of this chapter.

```
? K = nfinit(x^5 + 7*x^4 + 3*x^2 - x + 1);
? idealfactor(K, 2)
[[2, [2, 0, 0, 0, 0]~, 1, 5, [1, 0, 0, 0, 0]~] 1]
? idealfactor(K, 5)
[[5, [-3, 0, 0, 1, 0]~, 2, 1, [1, 0, 2, -2, -1]~] 2]
[[5, [1, 0, 0, 1, 0]~, 1, 1, [1, 0, -2, 2, -1]~] 1]
[[5, [10, 1, 0, -8, 1]~, 1, 2, [2, 1, 1, -1, 1]~] 1]

? K.disc
2945785

? poldisc(x^5 + 7*x^4 + 3*x^2 - x + 1)
2945785

? a = Mod(x, x^5 + 7*x^4 + 3*x^2 - x + 1);
? f = charpoly(7*a)
x^5 + 49*x^4 + 1029*x^2 - 2401*x + 16807
? poldisc(f)
2350508611755109683657 85
? poldisc(f)/K.disc
79792266297612001
```

```
? factormod(f,5)
[Mod(1, 5)*x + Mod(1, 5) 2]
[Mod(1, 5)*x + Mod(4, 5) 1]
[Mod(1, 5)*x^2 + Mod(3, 5)*x + Mod(3, 5) 1]

? f = charpoly(5*a)
? factormod(f,5)
[Mod(1, 5)*x 5]

? K = nfinit(x^3 + x^2 - 2*x + 8);
? idealfactor(K,2)
[[2, [1, 0, 1]~, 1, 1, [0, 0, -1]~] 1]
[[2, [1, 1, 0]~, 1, 1, [0, 1, 0]~] 1]
[[2, [2, 1, 1]~, 1, 1, [1, 1, 1]~] 1]
```

Chapter 6

The Chinese Remainder Theorem

We prove the Chinese Remainder Theorem (CRT) for commutative rings and discuss how to compute with it explicitly in Magma and PARI. We also apply the Chinese Remainder Theorem to prove that every ideal in $\mathcal{O}_K$ is generated by two elements and determine the structure of $\mathfrak{p}^n/\mathfrak{p}^{n+1}$, where $\mathfrak{p}$ is a nonzero prime ideal of $\mathcal{O}_K$.

6.1 The Chinese Remainder Theorem

6.1.1 CRT in the Integers

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 $i = 1, \ldots, r$. Here "coprime in pairs" means that $\gcd(n_i, n_j) = 1$ whenever $i \neq j$; it does *not* mean that $\gcd(n_1, \ldots, n_r) = 1$, though it implies this. In terms of rings, the Chinese Remainder Theorem (CRT) asserts that the natural map

$$\mathbf{Z}/(n_1 \cdots n_r)\mathbf{Z} \to (\mathbf{Z}/n_1\mathbf{Z}) \oplus \cdots \oplus (\mathbf{Z}/n_r\mathbf{Z}) \tag{6.1.1}$$

that sends $a \in \mathbf{Z}$ to its reduction modulo each n_i, is an isomorphism.

This map is *not* an isomorphism if the n_i are not coprime. Indeed, the cardinality of the left hand side of (6.1.1) is $\operatorname{lcm}(n_1, \ldots, n_r)$, whereas the cardinality of the right hand side is $n_1 \cdots n_r$.

The isomorphism (6.1.1) can alternatively be viewed as asserting that any system of linear congruences

$$x \equiv a_1 \pmod{n_1}, \quad x \equiv a_2 \pmod{n_2}, \quad \cdots, x \equiv a_r \pmod{n_r}$$

with pairwise coprime moduli has a unique solution modulo $n_1 \ldots n_r$.

Before proving CRT in a general ring, we give a proof of (6.1.1). There is a natural map

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

given by projection onto each factor. It's kernel is

$$n_1\mathbf{Z} \cap \cdots \cap n_r\mathbf{Z}.$$

If n and m are integers, then $n\mathbf{Z} \cap m\mathbf{Z}$ is the set of multiples of both n and m, so $n\mathbf{Z} \cap m\mathbf{Z} = \mathrm{lcm}(n, m)\mathbf{Z}$. Since the n_i are coprime,

$$n_1\mathbf{Z} \cap \cdots \cap n_r\mathbf{Z} = n_1 \ldots n_r\mathbf{Z}.$$

Thus we have proved there is an inclusion

$$i : \mathbf{Z}/(n_1 \cdots n_r)\mathbf{Z} \hookrightarrow (\mathbf{Z}/n_1\mathbf{Z}) \oplus \cdots \oplus (\mathbf{Z}/n_r\mathbf{Z}). \tag{6.1.2}$$

This is half of the CRT; the other half is to prove that this map is surjective.

To prove the other half, note that since the n_i are coprime in pairs,

$$\gcd(n_1, n_2 \ldots n_r) = 1,$$

so there exists integers x, y such that

$$xn_1 + yn_2 \cdots n_r = 1.$$

To complete the proof, observe that $yn_2 \cdots n_r = 1 - xn_1$ is congruent to 1 modulo n_1 and 0 modulo $n_2 \cdots n_r$. Thus $(1, 0, \ldots, 0)$ is in the image of i. By a similar argument, we see that $(0, 1, \ldots, 0)$ and the other similar elements are all in the image of i, so i is surjective, which proves CRT.

Remark 6.1.1. One could also prove surjectivity of i by noting that both sides of (6.1.2) are finite of order $n_1 \ldots n_r$.

6.1.2 CRT in an Arbitrary Ring

Recall that all rings in this book are commutative with unity.

Definition 6.1.2 (Coprime). Ideals I and J are *coprime* if $I + J = (1)$.

If I and J are nonzero ideals in the ring of integers of a number field, then they are coprime precisely when the prime ideals that appear in their two (unique) factorizations are disjoint.

Lemma 6.1.3. *If I and J are coprime ideals in a ring R, then $I \cap J = IJ$.*

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 $I \cap J \subset IJ$. The other inclusion is obvious by definition of ideal. □

Lemma 6.1.4. *Suppose $I_1, \ldots, I_s$ are pairwise coprime ideals. Then I_1 is coprime to the product $I_2 \cdots I_s$.*

Proof. It suffices to prove the lemma in the case $s = 3$, since the general case then follows from induction. By assumption, there are $x_1 \in I_1, y_1 \in I_2$ and $x_2 \in I_1, y_2 \in I_3$ such

$$x_1 + y_1 = 1 \qquad \text{and} \qquad x_2 + y_2 = 1.$$

Multiplying these two relations yields

$$x_1x_2 + x_1y_2 + y_1x_2 + y_1y_2 = 1 \cdot 1 = 1.$$

The first three terms are in I_1 and the last term is in $I_2 \cap I_3 = I_2I_3$, so I_1 is coprime to I_2I_3. □

Next we prove the Chinese Remainder Theorem in a very general form. We will apply this result with $R = \mathcal{O}_K$ in the rest of this chapter.

Theorem 6.1.5 (Chinese Remainder Theorem). *Suppose $I_1, \ldots, I_r$ are nonzero ideals of a ring R such I_m and I_n are coprime for any $m \neq n$. Then the natural homomorphism $R \to \bigoplus_{n=1}^r R/I_n$ induces an isomorphism*

$$\psi : R/\prod_{n=1}^{r} I_n \to \bigoplus_{n=1}^{r} R/I_n.$$

Thus given any $a_n \in R$, for $n = 1, \ldots, r$, there exists some $a \in R$ such that $a \equiv a_n \pmod{I_n}$ for $n = 1, \ldots, r$; moreover, a is unique modulo $\prod_{n=1}^r I_n$.

Proof. Let $\varphi : R \to \bigoplus_{n=1}^r R/I_n$ be the natural map induced by reduction modulo the I_n. An inductive application of Lemma 6.1.3 implies that the kernel $\cap_{n=1}^r I_n$ of φ is equal to $\prod_{n=1}^r I_n$, so the map ψ of the theorem is injective.

Each projection $R \to R/I_n$ is surjective, so to prove that ψ is surjective, it suffices to show that $(1, 0, \ldots, 0)$ is in the image of φ, and similarly for the other factors. By Lemma 6.1.4, $J = \prod_{n=2}^r I_n$ is coprime to I_1, there exists $x \in I_1$ and $y \in J$ such that $x + y = 1$. Then $y = 1 - x$ maps to 1 in R/I_1 and to 0 in R/J, hence to 0 in R/I_n for each $n \geq 2$, since $J \subset I_n$. □

6.2 Computing Using the CRT

In order to explicitly compute an a as given by the Theorem 6.1.5, usually one first precomputes elements $v_1, \ldots, v_r \in R$ such that $v_1 \mapsto (1, 0, \ldots, 0)$, $v_2 \mapsto (0, 1, \ldots, 0)$, etc. Then given any $a_n \in R$, for $n = 1, \ldots, r$, we obtain an $a \in R$ with $a_n \equiv a \pmod{I_n}$ by taking

$$a = a_1v_1 + \cdots + a_rv_r.$$

How to compute the v_i depends on the ring R. It reduces to the following problem: Given coprimes ideals $I, J \subset R$, find $x \in I$ and $y \in J$ such that $x + y = 1$. If

R is torsion free and of finite rank as a $\mathbf{Z}$-module, so $R \approx \mathbf{Z}^n$, then I, J can be represented by giving a basis in terms of a basis for R, and finding x, y such that $x+y = 1$ can then be reduced to a problem in linear algebra over $\mathbf{Z}$. More precisely, let A be the matrix whose columns are the concatenation of a basis for I with a basis for J. Suppose $v \in \mathbf{Z}^n$ corresponds to $1 \in \mathbf{Z}^n$. Then finding x, y such that $x + y = 1$ is equivalent to finding a solution $z \in \mathbf{Z}^n$ to the matrix equation $Az = v$. This latter linear algebra problem can be solved using Hermite normal form (see [Coh93, §4.7.1]), which is a generalization of Gauss elimination.

We next describe how to use MAGMA and PARI to do CRT computations.

6.2.1 MAGMA

The MAGMA command `ChineseRemainderTheorem` implements the algorithm suggested by Theorem 6.1.5. 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 := RingOfIntegers(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);
> K!b;
-4
> b - a in I;
true
> b - 1 in J;
true
```

6.2.2 PARI

There is also a CRT algorithm for number fields in PARI, but it is more cumbersome to use. First we defined $\mathbf{Q}(\sqrt[3]{2})$ and factor the ideals (3) and (5).

```
? f = x^3 - 2;
? k = nfinit(f);
? i = idealfactor(k,3);
? j = idealfactor(k,5);
```

Next we form matrix whose rows correspond to a product of two primes, one dividing 3 and one dividing 5:

```
? m = matrix(2,2);
? m[1,] = i[1,];
? m[1,2] = 1;
? m[2,] = j[1,];
```

Note that we set `m[1,2] = 1`, so the exponent is 1 instead of 3. We apply the CRT to obtain a lift in terms of the basis for $\mathcal{O}_K$.

```
? ?idealchinese
idealchinese(nf,x,y): x being a prime ideal factorization and y
a vector of elements, gives an element b such that
v_p(b-y_p)>=v_p(x) for all prime ideals p dividing x,
and v_p(b)>=0 for all other p.
? idealchinese(k, m, [x,1])
[0, 0, -1]~
? nfbasis(f)
[1, x, x^2]
```

Thus PARI finds the lift $-(\sqrt[3]{2})^2$, and we finish by verifying that this lift is correct. I couldn't figure out how to test for ideal membership in PARI, so here we just check that the prime ideal plus the element is not the unit ideal, which since the ideal is prime, implies membership.

```
? idealadd(k, i[1,1], -x^2 - x)
[3 1 2]
[0 1 0]
[0 0 1]
? idealadd(k, j[1,1], -x^2-1)
[5 2 1]
[0 1 0]
[0 0 1]
```

6.3 Structural Applications of the CRT

The next lemma is an 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 that 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 $(a)I^{-1}$ is an integral ideal. The following lemma asserts that (a) can be chosen so the quotient $(a)I^{-1}$ is coprime to any given ideal.

Lemma 6.3.1. *If I and J are nonzero integral ideals in $\mathcal{O}_K$, then there exists an $a \in I$ such that the integral ideal $(a)I^{-1}$ is coprime to J.*

Before we give the proof in general, note that the lemma is trivial when I is principal, since if $I = (b)$, just take $a = b$, and then $(a)I^{-1} = (a)(a^{-1}) = (1)$ is coprime to every ideal.

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. Since $\mathfrak{p}_n^{v_n} \neq \mathfrak{p}_n^{v_n+1}$, we can choose an element $a_n \in \mathfrak{p}_n^{v_n}$ that is not in $\mathfrak{p}_n^{v_n+1}$. By Theorem 6.1.5 applied to the $r+1$ coprime integral ideals

$$\mathfrak{p}_1^{v_1+1}, \ldots, \mathfrak{p}_r^{v_r+1}, I \cdot \left(\prod \mathfrak{p}_n^{v_n}\right)^{-1},$$

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

$$a \equiv 0 \pmod{I \cdot \left(\prod \mathfrak{p}_n^{v_n}\right)^{-1}}.$$

To complete the proof we show that $(a)I^{-1}$ is not divisible by any $\mathfrak{p}_n$, or equivalently, that each $\mathfrak{p}_n^{v_n}$ 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, since $a_n \notin \mathfrak{p}_n^{v_n+1}$. We conclude that $\mathfrak{p}_n^{v_n+1}$ does not divide (a), which completes the proof. □

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 6.3.2. *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 $I = (a, b) = \{\alpha a + \beta b : \alpha, \beta \in \mathcal{O}_K\}$.*

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 $J = (a)$. By Lemma 6.3.1, there exists $b \in I$ such that $(b)I^{-1}$ is coprime to (a). Since $a, b \in I$, we have $I \mid (a)$ and $I \mid (b)$, so $I \mid (a, b)$. Suppose $\mathfrak{p}^n \mid (a, b)$ with $\mathfrak{p}$ prime. Then $\mathfrak{p}^n \mid (a)$ and $\mathfrak{p}^n \mid (b)$, so $\mathfrak{p} \nmid (b)I^{-1}$, since $(b)I^{-1}$ is coprime to (a). We have $\mathfrak{p}^n \mid (b) = I \cdot (b)I^{-1}$ and $\mathfrak{p} \nmid (b)I^{-1}$, so $\mathfrak{p}^n \mid I$. Thus $(a, b) \mid I$, so $I = (a, b)$, as claimed. □

We can also use Theorem 6.1.5 to determine the $\mathcal{O}_K$-module structure of $\mathfrak{p}^n/\mathfrak{p}^{n+1}$.

Proposition 6.3.3. *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. [1] Since $\mathfrak{p}^n \neq \mathfrak{p}^{n+1}$, by unique factorization, there is 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 6.1.5. Suppose $c \in \mathfrak{p}^n$. By Theorem 6.1.5 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 $\mathfrak{p}^n \mid (d)$ since $d \in \mathfrak{p}^n$ and $(b)/\mathfrak{p}^n \mid (d)$ by the second displayed condition, so since $\mathfrak{p} \nmid (b)/\mathfrak{p}^n$, we have $(b) = \mathfrak{p}^n \cdot (b)/\mathfrak{p}^n \mid (d)$, hence $d/b \in \mathcal{O}_K$. Finally

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

so φ is surjective. □

[1] Proof from [SD01, pg. 13].

Chapter 7

Discrimants and Norms

In this chapter we give a geometric interpretation of the discriminant of an order in a number field. We also define norms of ideals and prove that the norm function is multiplicative. Discriminants of orders and norms of ideals will play a crucial roll in our proof of finiteness of the class group in the next chapter.

7.1 Field Embeddings

Let K be a number field of degree n. By the primitive element theorem, $K = \mathbf{Q}(\alpha)$ for some α, so we can write $K \cong \mathbf{Q}[x]/(f)$, where $f \in \mathbf{Q}[x]$ is the minimal polynomial of α. Because $\mathbf{C}$ is algebraically closed and f is irreducible, it has exactly $n = [K : \mathbf{Q}]$ complex roots. Each of these roots $z \in \mathbf{C}$ induces a homomorphism $\mathbf{Q}[x] \to \mathbf{C}$ given by $x \mapsto z$, whose kernel is (f). Thus we obtain n embeddings of $K \cong \mathbf{Q}[x]/(f)$ into $\mathbf{C}$:

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

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

Lemma 7.1.1. *Suppose $L \subset \mathbf{R}^n$ is a subgroup of the vector space $\mathbf{R}^n$. Then the induced topology on L is discrete if and only if for every $H > 0$ the set*

$$X_H = \{v \in L : \max\{|v_1|, \ldots, |v_n|\} \leq H\}$$

is finite.

Proof. If L is not discrete, then there is a point $x \in L$ such that for every $\varepsilon > 0$ there is $y \in L$ such that $0 < |x - y| < \varepsilon$. By choosing smaller and smaller ε, we find infinitely many elements $x - y \in L$ all of whose coordinates are smaller than 1. The set $X(1)$ is thus not finite. Thus if the sets X_H are all finite, L must be discrete.

Next assume that L is discrete and let $H > 0$ be any positive number. Then for every $x \in X_H$ there is an open ball B_x that contains x but no other element of L. Since X_H is closed and bounded, it is compact, so the open covering $\cup B_x$ of X_H has a finite subcover, which implies that X_H is finite, as claimed. □

Lemma 7.1.2. *If L if a free abelian group that is discrete in a finite-dimensional real vector space V and $\mathbf{R}L = V$, then the rank of L equals the dimension of V.*

Proof. If $x_1, \ldots, x_m \in L$ are a basis for $\mathbf{R}L$, then $M = \mathbf{Z}x_1 + \cdots + \mathbf{Z}x_m$ has finite index in L, since otherwise the quotient L/M would be infinite, so there would be infinitely many elements of L in a fundamental domain for M, which by Lemma 7.1.1 would contradict discreteness of L. Thus the rank of L is $m = \dim(\mathbf{R}L)$, as claimed. □

Proposition 7.1.3. *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.

Since $\sigma(\mathcal{O}_K)$ is discrete in $\mathbf{C}^n$, Lemma 7.1.2 implies that $\dim(V)$ equals the rank of $\sigma(\mathcal{O}_K)$. Since σ is injective, $\dim(V)$ is the rank of $\mathcal{O}_K$, which equals n by Proposition 2.4.4. □

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 $|\det(A)|$ is the *volume* of $V/\sigma(\mathcal{O}_K)$ (take this as the definition of volume).

Example 7.1.4. 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 $V/\sigma(\mathcal{O}_K)$ is $2\sqrt{2}$.

As the above example illustrates, the volume $V/\sigma(\mathcal{O}_K)$ need not be an integer, and it loses sign information. If we consider $\det(A)^2$ instead, we obtain a well-defined integer.

7.2 Discriminants

Suppose $w_1, \ldots, w_n$ are a basis for $\mathcal{O}_K$ as a $\mathbf{Z}$-module, 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 $\det(A)$ depends on the ordering of the w_i, and need not be an integer.

If we consider $\det(A)^2$ instead, we obtain a number that is a well-defined integer. Note that

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

so $\det(A)^2$ 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 $\det(UA)^2 = \det(U)^2\det(A)^2 = \det(A)^2$. Thus $\det(A)^2$ 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 $\det(\mathrm{Tr}(w_i w_j)) \neq 0$ hence $\det(A) \neq 0$.

Lemma 7.2.1. *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 7.2.2 (Discriminant). Suppose $a_1, \ldots, a_n$ is any $\mathbf{Q}$-basis of K. The *discriminant* of $a_1, \ldots, a_n$ is

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

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 7.2.1.

If $\alpha \in \mathcal{O}_K$ with $\mathbf{Z}[\alpha]$ of finite index in $\mathcal{O}_K$, and f is the minimal polynomial of α, then $\mathrm{Disc}(f) = \mathrm{Disc}(\mathbf{Z}[\alpha])$. To see this, note that if we choose the basis $1, \alpha, \ldots, \alpha^{n-1}$ for $\mathbf{Z}[\alpha]$, then both discriminants are the square of the same Vandermonde determinant.

Remark 7.2.3. **Warning:** In MAGMA Disc(K) is defined to be the discriminant of the polynomial you happened to use to define K.

```
> K := NumberField(x^2-5);
> Discriminant(K);
20
> Discriminant(RingOfIntegers(K));
5
```

In contrast, PARI does the right thing:

```
? k=nfinit(x^2-5);
? k.disc
5
```

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 7.2.4. *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 $|\det(C)| = [\mathcal{O}_K : \mathcal{O}]$. Then

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

□

Example 7.2.5. Let K be a number field and consider the quantity

$$D(K) = \gcd\{\mathrm{Disc}(\alpha) : \alpha \in \mathcal{O}_K \text{ and } [\mathcal{O}_K : \mathbf{Z}\alpha] < \infty\}.$$

One might hope that $D(K)$ is equal to the discriminant $\mathrm{Disc}(\mathcal{O}_K)$ of K. However it's not in general. Recall Example 5.3.2, of the field generated by a root of $f = x^3 + x^2 - 2x + 8$. In that example, the discriminant of $\mathcal{O}_K$ is coprime to 2, but for every $\alpha \in \mathcal{O}_K$, we have $2 \mid [\mathcal{O}_K : \mathbf{Z}[\alpha]]$. By Proposition 7.2.4, the discriminant of $\mathbf{Z}[\alpha]$ is divisible by 4 for all α, so $\mathrm{Disc}(\alpha)$ is also divisible by 4. This is the sense in which 2 is an "essential *discriminant* divisor".

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. A much better algorithm is to proceed exactly as just described, except use the ideas of Section 5.3.3 to find a p-maximal order for each prime divisor of f, then add these p-maximal orders together.

Example 7.2.6. 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

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

hence $\mathcal{O}$ is not maximal.

Example 7.2.7. Consider the cubic field $K = \mathbf{Q}(\sqrt[3]{2})$, and let $\mathcal{O}$ be the order $\mathbf{Z}[\sqrt[3]{2}]$. Relative to the base $1, \sqrt[3]{2}, (\sqrt[3]{2})^2$ for $\mathcal{O}$, the matrix of the trace pairing is

$$A = \begin{pmatrix} 3 & 0 & 0 \\ 0 & 0 & 6 \\ 0 & 6 & 0 \end{pmatrix}.$$

Thus

$$\mathrm{disc}(\mathcal{O}) = \det(A) = 108 = 2^2 \cdot 3^3.$$

Suppose we do not know that the ring of integers $\mathcal{O}_K$ is equal to $\mathcal{O}$. By Proposition 7.2.4, we have

$$\mathrm{Disc}(\mathcal{O}_K) \cdot [\mathcal{O}_K : \mathcal{O}]^2 = 2^2 \cdot 3^3,$$

so $3 \mid \mathrm{disc}(\mathcal{O}_K)$, and $[\mathcal{O}_K : \mathcal{O}] \mid 6$. Thus to prove $\mathcal{O} = \mathcal{O}_K$ it suffices to prove that $\mathcal{O}$ is 2-maximal and 3-maximal, which could be accomplished as described in Section 5.3.3.

7.3 Norms of Ideals

In this section we extend the notion of norm to ideals. This will be helpful in the next chapter, where 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 bound. This is enough, because as we will see below there are only finitely many ideals of bounded norm.

Definition 7.3.1 (Lattice Index). If L and M are two lattices in a 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 $A(L) = M$.

For example, if $L = 2\mathbf{Z}$ and $M = 10\mathbf{Z}$, then

$$[L : M] = [2\mathbf{Z} : 10\mathbf{Z}] = \det([5]) = 5,$$

since 5 multiples $2\mathbf{Z}$ onto $10\mathbf{Z}$.

The lattice index has the following properties:

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

$$[L : N] = [L : M] \cdot [M : N].$$

Definition 7.3.2 (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 7.3.3. *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 $[I : aI] = |\det(\ell_a)| = |\,\mathrm{Norm}_{K/\mathbf{Q}}(a)|$. □

Proposition 7.3.4. *If I and J are fractional ideals, then*

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

Proof. By Lemma 7.3.3, it suffices to prove this when I and J are integral ideals. If I and J are coprime, then Theorem 6.1.5 (the 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 6.3.3, which is a consequence of CRT, the filtration of $\mathcal{O}_K/\mathfrak{p}^n$ given by powers of $\mathfrak{p}$ has successive quotients isomorphic to $\mathcal{O}_K/\mathfrak{p}$. Thus we see that $\#(\mathcal{O}_K/\mathfrak{p}^n) = \#(\mathcal{O}_K/\mathfrak{p})^n$, which proves that $\mathrm{Norm}(\mathfrak{p}^n) = \mathrm{Norm}(\mathfrak{p})^n$. □

We will use the following proposition in the next chapter when we prove finiteness of class groups.

Proposition 7.3.5. *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. □

Chapter 8

Finiteness of the Class Group

Frequently $\mathcal{O}_K$ is not a principal ideal domain. This chapter is about a way 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 extensions of K that are Galois with abelian Galois group.

8.1 The Class Group

Definition 8.1.1 (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 fractional ideals modulo the sugroup of principal fractional ideals (a), for $a \in K$.

Note that if we let $\mathrm{Div}(\mathcal{O}_K)$ denote the group of fractional ideals, then we have an exact sequence

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

That the class group C_K is finite 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 (Proposition 7.3.5).

Theorem 8.1.2 (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 Proposition 7.3.5 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 it is the best known general bound, which doesn't depend on unproven conjectures.

The following two examples illustrate how to apply Theorem 8.1.2 to compute C_K in simple cases.

Example 8.1.3. Let $K = \mathbf{Q}[i]$. Then $n = 2$, $s = 1$, and $|d_K| = 4$, so the Minkowski bound is

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

Thus every fractional ideal is equivalent to an ideal of norm 1. Since (1) is the only ideal of norm 1, every ideal is principal, so C_K is trivial.

Example 8.1.4. Let $K = \mathbf{Q}(\sqrt{10})$. We have $\mathcal{O}_K = \mathbf{Z}[\sqrt{10}]$, so $n = 2$, $s = 0$, $|d_K| = 40$, and the Minkowski bound is

$$\sqrt{40} \cdot \left(\frac{4}{\pi}\right)^0 \cdot \frac{2!}{2^2} = 2 \cdot \sqrt{10} \cdot \frac{1}{2} = \sqrt{10} = 3.162277\ldots.$$

Theorem 8.1.2 implies that every ideal class has a representative that is an integral ideal of norm 1, 2, or 3. The ideal $2\mathcal{O}_K$ is ramified in $\mathcal{O}_K$, so

$$2\mathcal{O}_K = (2, \sqrt{10}).$$

If $(2, \sqrt{10})$ were principal, say (α), then $\alpha = a + b\sqrt{10}$ would have norm ± 2. Then the equation

$$x^2 - 10y^2 = \pm 2, \tag{8.1.1}$$

would have an integer solution. But the squares mod 5 are $0, \pm 1$, so (8.1.1) has no solutions. Thus $(2, \sqrt{10})$ defines a nontrivial element of the class group, and it has order 2 since its square is the principal ideal $2\mathcal{O}_K$. Thus $2 \mid \#C_K$.

To find the integral ideals of norm 3, we factor $x^2 - 10$ modulo 3, and see that

$$3\mathcal{O}_K = (3, 2 + \sqrt{10}) \cdot (3, 4 + \sqrt{10}).$$

If either of the prime divisors of $3\mathcal{O}_K$ were principal, then the equation $x^2 - 10y^2 = \pm 3$ would have an integer solution. Since it doesn't even have one mod 5, the prime divisors of $3\mathcal{O}_K$ are both nontrivial elements of the class group. Let

$$\alpha = \frac{4 + \sqrt{10}}{2 + \sqrt{10}} = \frac{1}{3} \cdot (1 + \sqrt{10}).$$

Then

$$(3, 2 + \sqrt{10}) \cdot (\alpha) = (3\alpha, 4 + \sqrt{10}) = (1 + \sqrt{10}, 4 + \sqrt{10}) = (3, 4 + \sqrt{10}),$$

so the classes over 3 are equal.

In summary, we now know that every element of C_K is equivalent to one of

$$(1), \quad (2, \sqrt{10}), \quad \text{or} \quad (3, 2 + \sqrt{10}).$$

Thus the class group is a group of order at most 3 that contains an element of order 2. Thus it must have order 2.

Before proving Theorem 8.1.2, we prove a few lemmas. The strategy of the proof is 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 is 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 8.1.5 (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 nonzero $Q = Q_\varepsilon \in L \cap (1+\varepsilon)S$ for arbitrarily small ε. Since S is closed, $Q \in L \cap S$. □

Lemma 8.1.6. *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 $|\det(A)| = [L_1 : L_2]$. The claimed formula then follows, since $[L_1 : L_2] = |\det(A)|$, by definition. □

Fix a number field K with ring of integers $\mathcal{O}_K$.

Let $\sigma_1, \ldots, \sigma_r$ 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. Let $\sigma : K \to V = \mathbf{R}^n$ be the embedding

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

Note that this σ is *not* the same as the one at the beginning of Section 7.2.

Lemma 8.1.7.

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

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

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

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 $d_K = \mathrm{Disc}(\mathcal{O}_K)$ in Section 7.2.

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 that now has entries $\mathrm{Re}(\sigma_{r+j}(w_i)) + i\mathrm{Im}(\sigma_{r+j}(w_i))$ to the the column with entries $-2i\mathrm{Im}(\sigma_{r+j}(w_i))$ to obtain columns $\mathrm{Re}(\sigma_{r+j}(w_i)) - i\mathrm{Im}(\sigma_{r+j}(w_i))$.

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

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

□

Lemma 8.1.8. *If I is a fractional $\mathcal{O}_K$-ideal, 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 8.1.7 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 8.1.6–8.1.7 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 8.1.2. 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 $f(\sigma(x)) = |\operatorname{Norm}_{K/\mathbf{Q}}(x)|$, and

$$f(ax_1, \ldots, ax_n) = |a|^n f(x_1, \ldots, x_n).$$

Let $S \subset V$ be any closed, bounded, convex, subset with positive volume 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 fractional ideal of $\mathcal{O}_K$. Our goal is to prove that there is an integral ideal aI with small norm. We will do this by finding an appropriate $a \in I^{-1}$. By Lemma 8.1.8,

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

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

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

so by Lemma 8.1.5 there exists $0 \neq b \in \sigma(I^{-1}) \cap \lambda S$. Let $a \in I^{-1}$ be such that $\sigma(a) = b$. Since M is the largest norm of an element of S, the largest norm of an element of $\sigma(I^{-1}) \cap \lambda S$ is at most $\lambda^n M$, so

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

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

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

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

Proof. Applying Theorem 8.1.2 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). □

A prime p ramifies in $\mathcal{O}_K$ if and only if $d \mid d_K$, so the corollary implies that every extension of $\mathbf{Q}$ is ramified at some prime.

8.2 Class Number 1

The fields of class number 1 are exactly the fields for which $\mathcal{O}_K$ is a principal ideal domain. How many such number fields are there? We still don't know.

Conjecture 8.2.1. *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 ([CL84]).

```
for d in [2..1000] do
    if IsFundamentalDiscriminant(d) then
        h := ClassNumber(NumberField(x^2-d));
        if h eq 1 then
            printf "%o, ", d;
        end if;
    end if;
end for;
5, 8, 12, 13, 17, 21, 24, 28, 29, 33, 37, 41, 44, 53, 56, 57, 61,
69, 73, 76, 77, 88, 89, 92, 93, 97, 101, 109, 113, 124, 129, 133,
137, 141, 149, 152, 157, 161, 172, 173, 177, 181, 184, 188, 193,
197, 201, 209, 213, 217, 233, 236, 237, 241, 248, 249, 253, 268,
269, 277, 281, 284, 293, 301, 309, 313, 317, 329, 332, 337, 341,
344, 349, 353, 373, 376, 381, 389, 393, 397, 409, 412, 413, 417,
421, 428, 433, 437, 449, 453, 457, 461, 472, 489, 497, 501, 508,
509, 517, 521, 524, 536, 537, 541, 553, 556, 557, 569, 573, 581,
589, 593, 597, 601, 604, 613, 617, 632, 633, 641, 649, 652, 653,
661, 664, 668, 669, 673, 677, 681, 701, 709, 713, 716, 717, 721,
737, 749, 753, 757, 764, 769, 773, 781, 789, 796, 797, 809, 813,
```

```
821, 824, 829, 844, 849, 853, 856, 857, 869, 877, 881, 889, 893,
908, 913, 917, 921, 929, 933, 937, 941, 953, 956, 973, 977, 989, 997
```

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 [-1000..-1] do
    if IsFundamentalDiscriminant(d) then
        h := ClassNumber(NumberField(x^2-d));
        if h eq 1 then
            printf "%o, ", d;
        end if;
    end if;
end for;
-163, -67, -43, -19, -11, -8, -7, -4, -3
```

It is a theorem that was proved independently and in different ways by Heegner, Stark, and Baker 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.

The function in PARI for computing the order of the class group of a quadratic field in PARI is called `qfbclassno`.

```
?qfbclassno
 qfbclassno(x,{flag=0}): class number of discriminant x using
 Shanks's method by default. If (optional) flag is set to 1,
 use Euler products.
? for(d=2,1000, if(isfundamental(d), h=qfbclassno(d);if(h==1,print1(d,", "))))
5, 8, 12, 13, 17, 21, 24, ... 977, 989, 997,

? for(d=-1000,-1,if(isfundamental(d), h=qfbclassno(d);if(h==1,print1(d,", "))))
-163, -67, -43, -19, -11, -8, -7, -4, -3
```

PARI does the above class number computations *vastly* faster than MAGMA. However, note the following ominous warning in the PARI manual, which has been there in some form since 1997:

> **Important warning.** For $D < 0$, this function may give incorrect results when the class group has a low exponent (has many cyclic factors), because implementing Shank's method in full generality slows it down immensely. It is therefore strongly recommended to double-check results using either the version with *flag=1*, the fucntion `qfbhclassno(-D)` or the function `quadclassunit`.

8.3 More About Computing Class Groups

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 8.3.1. *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. Theorem 8.1.2 asserts 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. □

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

1. Use the algorithms of Chapter 5 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, this step can become fairly complicated.)

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 8.3.2. 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 8.3.3. 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 8.3.4. 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 9

Dirichlet's Unit Theorem

In this chapter we will prove Dirichlet's unit theorem, which is a 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 pairs of complex conjugate embeddings, then

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

where T is a finite cyclic group.

Many questions can be encoded as questions about the structure of the group of units. For example, Dirichlet's unit theorem implies that the solutions to Pell's equation $x^2 - dy^2 = 1$ form a free abelian group of rank 1.

9.1 The Group of Units

Definition 9.1.1 (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 9.1.2 (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.*

(Note that we will prove a generalization of Theorem 9.1.2 in Section 13.1 below.)

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 Blichfeld's Lemma 8.1.5.

Remark 9.1.3. Theorem 9.1.2 is due to Dirichlet who lived 1805–1859. Thomas Hirst described Dirichlet thus:

> 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 9.1.2.

Units have a simple characterization in terms of their norm.

Proposition 9.1.4. *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 $a^{-1} \in K \cap \overline{\mathbf{Z}} = \mathcal{O}_K$, which proves that a is a unit. □

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 the *log embedding*

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

by

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

(Here $|z|$ is the usual absolute value of $z = x + iy \in \mathbf{C}$, so $|z| = \sqrt{x^2 + y^2}$.)

Lemma 9.1.5. *The image of φ lies in the hyperplane*

$$H = \{(x_1, \ldots, x_{r+s}) \in \mathbf{R}^{r+s} : x_1 + \cdots + x_r + 2x_{r+1} + \cdots + 2x_{r+s} = 0\}. \quad (9.1.1)$$

Proof. If $a \in U_K$, then by Proposition 9.1.4,

$$\left(\prod_{i=1}^{r} |\sigma_i(a)|\right) \cdot \left(\prod_{i=r+1}^{r+s} |\sigma_i(a)|^2\right) = |\,\mathrm{Norm}_{K/\mathbf{Q}}(a)| = 1.$$

Taking logs of both sides proves the lemma. □

Lemma 9.1.6. *The kernel of φ is finite.*

Proof. We have

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

where X is the bounded subset of $\mathbf{R}^{r+s}$ of elements all of whose coordinates have absolute value at most 1. Since $\sigma(\mathcal{O}_K)$ is a lattice (see Proposition 2.4.4), the intersection $\sigma(\mathcal{O}_K) \cap X$ is finite, so $\mathrm{Ker}(\varphi)$ is finite. □

Lemma 9.1.7. *The kernel of φ is a finite cyclic group.*

Proof. This follows from the general fact that any finite subgroup G of the multiplicative group K^* of a field is cyclic. Indeed, if n is the exponent of G, then every element of G satisfies $x^n - 1$. A polynomial of degree n over a field has at most n roots, so G has order at most n, hence G is cyclic of order n. □

To prove Theorem 9.1.2, it suffices to prove that $\mathrm{Im}(\varphi)$ is a lattice in the hyperplane H of (9.1.1), which we view as a vector space of dimension $r + s - 1$.

Define an embedding

$$\sigma : K \hookrightarrow \mathbf{R}^n \tag{9.1.2}$$

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

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

Lemma 9.1.8. *The image $\varphi : U_K \to \mathbf{R}^{r+s}$ is discrete.*

Proof. We will show that for any bounded subset X of $\mathbf{R}^{r+s}$, the intersection $\varphi(U_K) \cap X$ is finite. If X is bounded, then for any $u \in Y = \varphi^{-1}(X) \subset U_K$ the coordinates of $\sigma(u)$ are bounded, since $|\log(x)|$ is bounded on bounded subsets of $[1, \infty)$. 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; moreover, σ is injective, so Y is finite. Thus $\varphi(U_K) \cap X \subset \varphi(Y) \cap X$ is finite. □

We will use the following lemma in our proof of Theorem 9.1.2.

Lemma 9.1.9. *Let $n \geq 2$ be an integer, suppose $w_1, \ldots, w_n \in \mathbf{R}$ are not all equal, and suppose $A, B \in \mathbf{R}$ are positive. Then there exist $d_1, \ldots, d_n \in \mathbf{R}_{>0}$ such that*

$$|w_1 \log(d_1) + \cdots + w_n \log(d_n)| > B$$

and $d_1 \cdots d_n = A$.

Proof. Order the w_i so that $w_1 \neq 0$. By hypothesis there exists a w_j such that $w_j \neq w_1$, 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 $d_1 \to \infty$. □

Proof of Theorem 9.1.2. By Lemma 9.1.8, the image $\varphi(U_K)$ is discrete, so it remains to show that $\varphi(U_K)$ spans H. Let W be the $\mathbf{R}$-span of the image $\varphi(U_K)$, and note that W is a subspace of H, by Lemma 9.1.5. We will show that $W = H$ indirectly by showing that if $v \notin H^\perp$, where $\perp$ is the orthogonal complement 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

$$f(x) = z_1 \log|\sigma_1(x)| + \cdots + z_{r+s} \log|\sigma_{r+s}(x)|. \tag{9.1.3}$$

Note that $f = 0$ if and only if $z \in W^\perp$, so 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

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

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 8.1.5, which asserts 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 (9.1.2). By Lemma 8.1.7, we have $\mathrm{Vol}(\mathbf{R}^n/L) = 2^{-s}\sqrt{|d_K|}$. To check the hypothesis of 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 $S \cap \sigma(\mathcal{O}_K)$, so there is 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

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

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

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

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

$$\frac{c_i}{|\sigma_i(a)|} \geq A \quad \text{for } i \leq r \quad \text{and} \quad \left(\frac{c_i}{|\sigma_i(a)|}\right)^2 \geq A \quad \text{for } i = r+1, \ldots, r+s. \quad (9.1.4)$$

Our overall 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 $|\operatorname{Norm}_{K/\mathbf{Q}}(a)| \leq A$, we have $(a) = (b_j)$, for some j, so there is a unit $u \in \mathcal{O}_K$ such that $a = ub_j$.

Let

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

and recall $f : K^* \to \mathbf{R}$ defined in (9.1.3) above. We first show that

$$|f(u) - t| \leq B = |f(b_j)| + \log(A) \cdot \left(\sum_{i=1}^{r} |z_i| + \frac{1}{2} \cdot \sum_{i=r+1}^{s} |z_i|\right). \quad (9.1.5)$$

We have

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

In the last step we use (9.1.4).

A wonderful property of (9.1.5) is that the bound B on the right hand side does not depend on our choice of c_i. For example, if we can choose positive real numbers c_i such that

$$\begin{aligned}
c_1 \cdots c_r \cdot (c_{r+1} \cdots c_{r+s})^2 &= A \\
|t(c_1, \ldots, c_{r+s})| &> B,
\end{aligned}$$

then $|f(u) - t| \leq B$ would imply that $|f(u)| > 0$, which is exactly what we aimed to prove. 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 $r + s > 1$. It is possible to choose such c_i such that $|f(u) - t| > B$, using Lemma 9.1.9. Write

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

where $w_i = z_i$ and $d_i = c_i$ for $i \leq r$, and $w_i = \frac{1}{2} z_i$ and $d_i = c_i^2$ for $r < i \leq r + s$, 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 $\prod_{i=1}^{r+s} d_i = A$. But this is exactly what Lemma 9.1.9 shows. It is thus possible to find a unit u such that $|f(u)| > 0$. Thus $z \notin W^\perp$, so $W^\perp \subset Z^\perp$, whence $Z \subset W$, which finishes the proof Theorem 9.1.2. □

9.2 Examples with MAGMA

9.2.1 Pell's Equation

The Pell's equation problem 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

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

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 Pell's equation $x^2 - 5y^2 = 1$ with $d = 5$ by finding the units of a field using MAGMA:

```
> 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
```

The MathSciNet review of [Len02] 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."

The simplest solutions to Pell's equation can be huge, even when d is quite small. Read Lenstra's paper for some examples from over two thousand years ago.

```
K<a> := NumberField(x^2-NextPrime(10^7));
> G, phi := UnitGroup(K);
> K!phi(G.2);
    16358025988034632822559223812109462549914267769314291550674725 30\
    00340064100365767872890438816249271266423998175030309436575 6\
    10631639272377601680603795883791477817611974184075445702823 7\
    89975945910042889569323816504809803 9*a +
    51728669288581496747017067236834679830362903437357520297507 5\
    60505871495808089399127442790344809864383651287835122785626 9\
    08685667907830497932104776503107334525990262271205916496900 8\
    63360360364033117566345622041829362222409 30
```

9.2.2 Examples with Various Signatures

In this section we give examples for various (r, s) pairs. 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
```

The `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.

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));
[ -0.259921049894873164767210607278228350570251464700999999999995,
1.629960524947436582383605303639114175285125732351384392310 4 -
1.091123635971721403560072614189808881325873338740185473705 60*i,
1.629960524947436582383605303639114175285125732351384392310 4 +
```

```
1.09112363597172140356007261418980888132587333874018547370560*i ]
> Logs(K!phi(G.2));   // image of infinite order unit -- generates a lattice
[ -1.34737734832938410091818789144565304628306227332099999999989\
, 0.67368867416469205045909394572282652314153113666032889999999 ]
> 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);
[ 1.65022945678458847118947727496822281521549484215899999999997,
-2.09638539134527779532491660083370951943382108902299999999997,
0.44615593456068932413543932586548670421832624686433469999994 ]
```

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);
[ 1.16761574692758757159598251863681302946987760474899999999995,
-0.39284872458139826129179862583435951875841422643044369999996,
-0.77476702234618931030418389280245351071146337831817669999998 ]
> Logs(u2);
[ 0.64354294622886187738518172276864672577579540244630819999999,
-1.64022415032231714691015055517008505755834642266699999999999,
0.99668120409345526952496883240143833178255102022054989999998 ]
```

A field with $r = 0$ is called totally complex. For example, the *cyclotomic fields* $\mathbf{Q}(\zeta_n)$ are totally complex, where ζ_n is a primitive nth root of unity. 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);
[ -1.25656632417872848745322215929976803991663080388899999999969,
0.65179689403314000797179238846850991828232844023032739999999,
-0.18533004655986214094922163920197221556431542171819269999999,
0.52028498203007493933069857341185075513889550652722369999998,
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.
```

Chapter 10

Decomposition and Inertia Groups

In this chapter we will study extra structure in the case when K is Galois over $\mathbf{Q}$. 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 attach L-function to representations of $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$.

10.1 Galois Extensions

In this section we give a survey without proofs of the basic facts about Galois extensions of $\mathbf{Q}$ that will be needed in the rest of this chapter.

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 10.1.1 (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 $\mathrm{Gal}(K/L) = \operatorname{Aut}(K/L)$.

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.

If $K \subset \mathbf{C}$ 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

the field generated by all 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 an embedding of $\mathrm{Gal}(K^{\mathrm{gc}}/\mathbf{Q})$ into the group of permutations of the conjugates of a. If a has n conjugates, then this is an embedding $\mathrm{Gal}(K^{\mathrm{gc}}/\mathbf{Q}) \hookrightarrow S_n$, 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 one can prove that 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.

One can show that the 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, $[K : \mathbf{Q}] = \varphi(n)$, so this map is an isomorphism. (Remark: Taking a limit 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 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 $\mathrm{Cl}(K)$, is also of great interest.

10.2 Decomposition of Primes: $efg = n$

If $I \subset \mathcal{O}_K$ is any ideal in the ring of integers of a Galois extension K of $\mathbf{Q}$ and $\sigma \in \mathrm{Gal}(K/\mathbf{Q})$, then

$$\sigma(I) = \{\sigma(x) : x \in I\}$$

is also an ideal of $\mathcal{O}_K$.

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 10.2.1 (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 10.2.2. *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 $\mathfrak{P}_i$. Moreover,*

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

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 6.1.5) 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

$$I = \prod_{\sigma \in G} \sigma((a)/\mathfrak{p}) = \prod_{\sigma \in G} \frac{(\sigma(a))\mathcal{O}_K}{\sigma(\mathfrak{p})} = \frac{(\mathrm{Norm}_{K/\mathbf{Q}}(a))\mathcal{O}_K}{\prod_{\sigma \in G} \sigma(\mathfrak{p})} \tag{10.2.1}$$

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 (10.2.1) 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 (10.2.1) must also be divisibly by $p\mathcal{O}_K$ in order to cancel the $p\mathcal{O}_K$ in the numerator. Thus we have shown that for any i,

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

By unique factorization, since every $\mathfrak{p}_j$ appears in the left hand side, we must have that for each j there is a σ with $\sigma(\mathfrak{p}_i) = \mathfrak{p}_j$.

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 and using unique factorization, 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, upon apply CRT, that

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

which completes the proof. □

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

10.2.1 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 possibilities:

- **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, 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. It is a nontrivial theorem that this happens half of the time, 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 half of the time.

For example, let $K = \mathbf{Q}(\sqrt{5})$, so $\mathcal{O}_K = \mathbf{Z}[\gamma]$, where $\gamma = (1+\sqrt{5})/2$. Then $p = 5$ is ramified, since $5\mathcal{O}_K = (\sqrt{5})^2$. 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. It is a theorem of Dirichlet, which was massively generalized by Chebotarev, that $p \equiv \pm 1$ half the time and $p \equiv \pm 2$ the other half the time.

10.2.2 The Cube Root 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 $f = g = 1$. 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 $g = 2$. Thus when K is not Galois we need not have that the f_i are all equal.

10.3 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 10.3.1 (Decomposition group). The *decomposition group* of $\mathfrak{p}$ is the subgroup

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

It also makes sense to define decomposition groups for relative extensions K/L, but for simplicity and to fix ideas in this section we only define decomposition groups for a Galois extension $K/\mathbf{Q}$.

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

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

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 $D_\mathfrak{p} \to \mathrm{Gal}(k_\mathfrak{p}/\mathbf{F}_p)$ 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 from Theorem 10.2.2 that G acts transitively 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 cardinality of the orbit of $\mathfrak{p}$, which by Theorem 10.2.2 equals the number g of primes lying over p, so $[G : D_\mathfrak{p}] = g$.

Lemma 10.3.2. *The decomposition subgroups $D_\mathfrak{p}$ corresponding to primes $\mathfrak{p}$ lying over a given p are all conjugate as subgroups of G.*

Proof. We have

$$\tau^{-1}\sigma\tau\mathfrak{p} = \mathfrak{p} \iff \sigma\tau\mathfrak{p} = \tau\mathfrak{p},$$

so

$$\sigma \in D_{\tau\mathfrak{p}} \iff \tau^{-1}\sigma\tau \in D_\mathfrak{p}.$$

Thus

$$\sigma \in D_\mathfrak{p} \iff \tau\sigma\tau^{-1} \in D_{\tau\mathfrak{p}}.$$

Thus $\tau D_\mathfrak{p}\tau^{-1} = D_{\tau\mathfrak{p}}$. □

The decomposition group is 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.

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

Proposition 10.3.3. *The fixed field*

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

of D is the smallest subfield $L \subset K$ such that $\mathfrak{p} \cap \mathcal{O}_L$ such that $g(K/L) = 1$.

Proof. First suppose $L = K^D$, and note that by Galois theory $\mathrm{Gal}(K/L) \cong D$, and by Theorem 10.2.2, the group D acts transitively on the primes of K lying over $\mathfrak{p} \cap \mathcal{O}_L$. One of these primes is $\mathfrak{p}$, and D fixes $\mathfrak{p}$ by definition, so there is only one prime of K lying over $\mathfrak{p} \cap \mathcal{O}_L$, i.e., $g = 1$. Conversely, if $L \subset K$ is such that $\mathfrak{p} \cap \mathcal{O}_L$ has $g = 1$, then $\mathrm{Gal}(K/L)$ fixes $\mathfrak{p}$ (since it is the only prime over $\mathfrak{p} \cap \mathcal{O}_L$), 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 10.3.4. *Fix a Galois number field K of $\mathbf{Q}$, let $\mathfrak{p}$ be a prime lying over p with decomposition group D, and set $L = K^D$. Let $e = e(L/\mathbf{Q}), f = f(L/\mathbf{Q}), g = g(L/\mathbf{Q})$ be for $L/\mathbf{Q}$ and p. Then $e = f = 1$, $g = [L : \mathbf{Q}]$, $e(K/\mathbf{Q}) = e(K/L)$ and $f(K/\mathbf{Q}) = f(K/L)$.*

Proof. As mentioned right after Definition 10.3.1, the orbit-stabilizer theorem implies that $g(K/\mathbf{Q}) = [G : D]$, and by Galois theory $[G : D] = [L : \mathbf{Q}]$. Thus by Proposition 10.3.3 $g(K/L) = 1$, so by Theorem 10.2.2,

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

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 $f(K/\mathbf{Q}) = f(K/L) \cdot f(L/\mathbf{Q})$, it follows that $f(L/\mathbf{Q}) = f(L/\mathbf{Q}) = 1$. □

10.3.1 Galois groups of finite fields

Each $\sigma \in D = D_{\mathfrak{p}}$ acts in a well-defined way on the finite field $k_{\mathfrak{p}} = \mathcal{O}_K/\mathfrak{p}$, 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 general properties of Galois groups for finite fields. Let $f = [k_{\mathfrak{p}} : \mathbf{F}_p]$.

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

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

The group $k_{\mathfrak{p}}^*$ is cyclic (see proof of Lemma 9.1.7), so there is an element $a \in k_{\mathfrak{p}}^*$ of order $p^f - 1$, and $k_{\mathfrak{p}} = \mathbf{F}_p(a)$. 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 $k_{\mathfrak{p}}/\mathbf{F}_p$ is Galois, with group $\mathrm{Gal}(\mathbf{F}_{\mathfrak{p}}/\mathbf{F}_p)$ cyclic of order f generated by Frob_p. (Another 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.)

10.3.2 The Exact Sequence

Because $D_{\mathfrak{p}}$ preserves $\mathfrak{p}$, there is a natural reduction homomorphism

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

Theorem 10.3.5. *The homomorphism φ is surjective.*

Proof. Let $\tilde{a} \in k_{\mathfrak{p}}$ be an element such that $k_{\mathfrak{p}} = \mathbf{F}_p(a)$. 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 10.3.4 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 $\widetilde{\sigma(a)}$, 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 $\mathrm{Gal}(k_{\mathfrak{p}}/\mathbf{F}_p)$ is in the image of φ, which proves the theorem. □

Definition 10.3.6 (Inertia Group). The *inertia group* is the kernel $I_{\mathfrak{p}}$ of $D_{\mathfrak{p}} \to \mathrm{Gal}(k_{\mathfrak{p}}/\mathbf{F}_p)$.

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

$$1 \to I_{\mathfrak{p}} \to D_{\mathfrak{p}} \to \mathrm{Gal}(k_{\mathfrak{p}}/\mathbf{F}_p) \to 1. \tag{10.3.1}$$

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

Corollary 10.3.7. *We have $\#I_{\mathfrak{p}} = e(\mathfrak{p}/p)$, where $\mathfrak{p}$ is a prime of K over p.*

Proof. The sequence (10.3.1) implies that $\#I_{\mathfrak{p}} = (\#D_{\mathfrak{p}})/f(K/\mathbf{Q})$. Applying Propositions 10.3.3–10.3.4, 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. □

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

Proposition 10.3.8. *Let $K/\mathbf{Q}$ be a Galois extension with group G, and let $\mathfrak{p}$ be a prime of $\mathcal{O}_K$ 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 $\sigma(a) \not\equiv a \pmod{\mathfrak{p}}$. If $\sigma \notin D_{\mathfrak{p}}$, then $\sigma^{-1} \notin D_{\mathfrak{p}}$, so $\sigma^{-1}(\mathfrak{p}) \neq \mathfrak{p}$. 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 $\sigma(a) \not\equiv a \pmod{\mathfrak{p}}$. □

10.4 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 10.3.5 is a canonical isomorphism $D_{\mathfrak{p}} \cong \mathrm{Gal}(k_{\mathfrak{p}}/\mathbf{F}_p)$. By Section 10.3.1, the group $\mathrm{Gal}(k_{\mathfrak{p}}/\mathbf{F}_p)$ 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 10.3.8.) Just as the primes $\mathfrak{p}$ and decomposition groups $D_{\mathfrak{p}}$ are all conjugate, the Frobenius elements corresponding to primes $\mathfrak{p} \mid p$ are all conjugate as elements of G.

Proposition 10.4.1. *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 $\mathrm{Frob}_{\mathfrak{p}}(\sigma^{-1}(a)) - \sigma^{-1}(a)^p \in \mathfrak{p}$. Applying σ to both sides, we see that $\sigma\,\mathrm{Frob}_{\mathfrak{p}}(\sigma^{-1}(a)) - a^p \in \sigma\mathfrak{p}$, so $\sigma\,\mathrm{Frob}_{\mathfrak{p}}\,\sigma^{-1} = \mathrm{Frob}_{\sigma\mathfrak{p}}$. □

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 homomorphism from the free abelian group on unramified primes p to G. 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 is 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 $(\mathbf{Z}/n\mathbf{Z})^*$, so giving an abelian extension K of $\mathbf{Q}$ is *exactly the same* as giving an integer n and a subgroup of $H \subset (\mathbf{Z}/n\mathbf{Z})^*$. The Artin reciprocity map $p \mapsto \left(\frac{K/\mathbf{Q}}{p}\right)$ is then $p \mapsto [p] \in (\mathbf{Z}/n\mathbf{Z})^*/H$.

10.5 Galois Representations, L-series 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 much of 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 10.5.1. 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 if K is the fixed field of $\mathrm{Ker}(\rho)$, then $K/\mathbf{Q}$ is finite Galois. We have a diagram

$$\begin{array}{ccc} \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) & \xrightarrow{\quad\rho\quad} & \mathrm{GL}_n(\mathbf{C}) \\ & \searrow \quad \nearrow_{\rho'} & \\ & \mathrm{Gal}(K/\mathbf{Q}) & \end{array}$$

Remark 10.5.2. Continuous implies that the image of ρ is finite, but the converse is not true. Using Zorn's lemma, one can show that there are homomorphisms $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \to \{\pm 1\}$ with image of order 2 that are not continuous, since they do not factor through the Galois group of any finite Galois extension.

Fix a Galois representation ρ and let K be the fixed field of $\ker(\rho)$, so 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 $F_p(x) \in \mathbf{C}[x]$ of $\rho'(\mathrm{Frob}_p)$ is a well-defined invariant of p and ρ. Let

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

be the polynomial obtain by reversing the order of the coefficients of F_p. Following E. Artin [Art23, Art30], set

$$L(\rho, s) = \prod_{p \text{ unramified}} \frac{1}{R_p(p^{-s})}. \tag{10.5.1}$$

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 10.5.3 (Artin). *The L-function 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 is known 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 image of ρ in $\mathrm{PGL}_2(\mathbf{C})$ is not solvable, the only possibility is that the projective image is isomorphic to the alternating group A_5. Because A_5 is the symmetry group of the icosahedron, these representations are called *icosahedral*. In this case, Joe Buhler's Harvard Ph.D. thesis [Buh78] gave the first example in which ρ was shown to satisfy Conjecture 10.5.3. There is a book [Fre94], which proves Artin's conjecture for 7 icosahedral representation (none of which are twists of each other). Kevin Buzzard and the author proved the conjecture for 8 more examples [BS02]. Subsequently, Richard Taylor, Kevin Buzzard, Nick Shepherd-Barron, and Mark Dickinson proved the conjecture for an infinite class of icosahedral Galois representations (disjoint from the examples) [BDSBT01]. The general problem for $n = 2$ is still open, but Taylor and others are making amazing progress toward it.

Chapter 11

Elliptic Curves, Galois Representations, and L-functions

The rest of this book is about elliptic curves and their interplay with algebraic number theory. Our approach will be less systematic and more a survey than the first part of this book. The goal is to take you to the forefront of research, but assuming many basic facts that can be found, e.g., in [Sil92].

11.1 Groups Attached to Elliptic Curves

Definition 11.1.1 (Elliptic Curve). An *elliptic curve* over a field K is a genus one curve E over K equipped with a point $\mathcal{O} \in E(K)$ defined over K.

We will not define genus in this book, except to note that a nonsingular curve over K has genus one if and only if over $\overline{K}$ it can be realized as a nonsingular plane cubic curve. Moreover, one can show (using the Riemann-Roch formula) that a genus one curve with a rational point can always be defined by a projective cubic

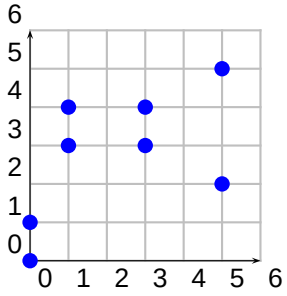


Figure 11.1.1: The Elliptic Curve $y^2 = x^3 + x$ over $\mathbf{Z}/7\mathbf{Z}$

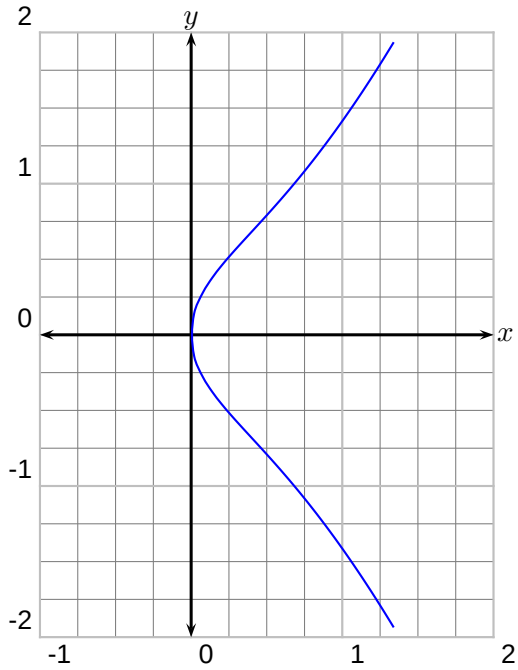


Figure 11.1.2: The Elliptic Curve $y^2 = x^3 + x$ over $\mathbf{R}$

equation of the form

$$Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3.$$

In affine coordinates this becomes

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6. \tag{11.1.1}$$

Thus one presents an elliptic curve by giving a *Weierstrass equation* (11.1.1).

Figure 11.1.1 contains the graph of an elliptic curve over $\mathbf{F}_7$, and Figure 11.1.2 contains a graph of the real points on an elliptic curve defined over $\mathbf{Q}$.

11.1.1 Abelian Groups Attached to Elliptic Curves

If E is an elliptic curve over K, then we give the set $E(K)$ of all K-rational points on E the structure of abelian group with identity element $\mathcal{O}$. If we embed E in the projective plane, then this group is determined by the condition that three points sum to the zero element $\mathcal{O}$ if and only if they lie on a common line. See Figure 11.1.3 for an example, in which $(0, 2)$ and $(1, 0)$ add to $(3, 4)$ in the group law.

That the above condition defines an abelian group structure on $E(K)$ is not obvious (the trickiest part is seeing that the operation is associative). The best way to understand the group operation on $E(K)$ is to view $E(K)$ as a class group, very similar to class groups of number fields. Let $\mathrm{Div}(E/K)$ be the free abelian group on the points of E, which is analogous to the group of fractional ideals of a number

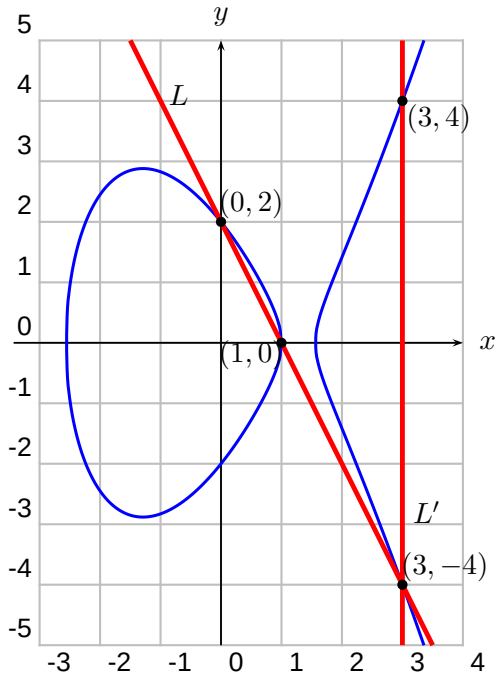


Figure 11.1.3: The Group Law: $(1,0)+(0,2)=(3,4)$ on $y^2=x^3-5x+4$

field. We call the elements of $\mathrm{Div}(E/K)$ *divisors*. Let $\mathrm{Pic}(E/K)$ be the quotient of $\mathrm{Div}(E/K)$ by the principal divisors, i.e., the divisors associted to rational functions $f \in K(E)^*$ via

$$f \mapsto (f) = \sum_P \mathrm{ord}_P(f)[P].$$

Note that the principal divisor associated to f is analogous to the principal fractional ideal associated to a nonzero element of a number field. The definition of $\mathrm{ord}_P(f)$ is analogous to the "power of P that divides the principal ideal generated by f". Define the class group $\mathrm{Pic}(E/K)$ to be the quotient of the divisors by the principal divisors, so we have an exact sequence:

$$0 \to K(E)^*/K^* \to \mathrm{Div}(E/K) \to \mathrm{Pic}(E/K) \to 0.$$

A key difference between elliptic curves and algebraic number fields is that the principal divisors in the context of elliptic curves all have degree 0, i.e., the sum of the coefficients of the divisor (f) is always 0. This might be a familiar fact to you: the number of zeros of a nonzero rational function on a projective curve equals the number of poles, counted with multiplicity. If we let $\mathrm{Div}^0(E/K)$ denote the subgroup of divisors of degree 0, then we have an exact sequence

$$0 \to K(E)^*/K^* \to \mathrm{Div}^0(E/K) \to \mathrm{Pic}^0(E/K) \to 0.$$

To connect this with the group law on $E(K)$, note that there is a natural map

$$E(K) \to \mathrm{Pic}^0(E/K), \qquad P \mapsto [P - \mathcal{O}].$$

Using the Riemann-Roch theorem, one can prove that this map is a bijection, which is moreover an isomorphism of abelian groups. Thus really when we discuss the group of K-rational points on an E, we are talking about the class group $\mathrm{Pic}^0(E/K)$.

Recall that we proved (Theorem 8.1.2) that the class group $\mathrm{Cl}(\mathcal{O}_K)$ of a number field is finite. The group $\mathrm{Pic}^0(E/K) = E(K)$ of an elliptic curve can be either finite (e.g., for $y^2 + y = x^3 - x + 1$) or infinite (e.g., for $y^2 + y = x^3 - x$), and determining which is the case for any particular curve is one of the central unsolved problems in number theory.

Also, if L/K is an arbitrary extension of fields, and E is an elliptic curve over K, then there is a natural inclusion homomorphism $E(K) \hookrightarrow E(L)$. Thus instead of just obtaining one group attached to an elliptic curve, we obtain a whole collection, one for each extension of L. Even more generally, if S/K is an arbitrary scheme, then $E(S)$ is a group, and the association $S \mapsto E(S)$ defines a functor from the category of schemes to the category of groups.

11.1.2 A Formula for Adding Points

We close this section with an explicit formula for adding two points in $E(K)$. If E is an elliptic curve over a field K, given by an equation $y^2 = x^3 + ax + b$, then we can compute the group addition using the following algorithm.

Algorithm 11.1.2 (Elliptic Curve Group Law). Given $P_1, P_2 \in E(K)$, this algorithm computes the sum $R = P_1 + P_2 \in E(K)$.

1. [One Point $\mathcal{O}$] If $P_1 = \mathcal{O}$ set $R = P_2$ or if $P_2 = \mathcal{O}$ set $R = P_1$ and terminate. Otherwise write $P_i = (x_i, y_i)$.

2. [Negatives] If $x_1 = x_2$ and $y_1 = -y_2$, set $R = \mathcal{O}$ and terminate.

3. [Compute λ] Set $\lambda = \begin{cases} (3x_1^2 + a)/(2y_1) & \text{if } P_1 = P_2, \\ (y_1 - y_2)/(x_1 - x_2) & \text{otherwise.} \end{cases}$
   Note: If $y_1 = 0$ and $P_1 = P_2$, output $\mathcal{O}$ and terminate.

4. [Compute Sum] Then $R = \big(\lambda^2 - x_1 - x_2, -\lambda x_3 - \nu\big)$, where $\nu = y_1 - \lambda x_1$ and x_3 is the x coordinate of R.

11.1.3 Other Groups

There are other abelian groups attached to elliptic curves, such as the torsion subgroup $E(K)_{\mathrm{tor}}$ of elements of $E(K)$ of finite order. When K is a number field, there is a mysterious group called the Shafarevich-Tate group $Ш(E/K)$ attached to E. It's definition involves Galois cohomology, so we wait until Chapter 12 to define it. There are also component groups attached to E, one for each prime of $\mathcal{O}_K$. These groups all come together in the Birch and Swinnerton-Dyer conjecture (see Conjecture **??**).

11.2 Galois Representations Attached to Elliptic Curves

Let E be an elliptic curve over a number field K. In this section we attach representations of $G_K = \mathrm{Gal}(\overline{K}/K)$ to E, and use them to define the L-function $L(E, s)$.

Fix an integer n. The group structure on E is defined by algebraic formulas with coefficients that are elements of K, so the subgroup

$$E[n] = \{R \in E(\overline{K}) : nR = \mathcal{O}\}$$

is invariant under the action of G_K. We thus obtain a homomorphism

$$\overline{\rho}_{E,n} : G_K \to \mathrm{Aut}(E[n]).$$

It is a fact, which we will not prove in this book, that for any positive integer n, the group $E[n]$ is isomorphic as an abstract abelian group to $(\mathbf{Z}/n\mathbf{Z})^2$. There are various related ways to see why this is true. One is to use the Weierstrass $\wp$-theory to parametrize $E(\mathbf{C})$ by the the complex numbers, i.e., to find an isomorphism $\mathbf{C}/\Lambda \cong E(\mathbf{C})$, where Λ is a lattice in $\mathbf{C}$ and the isomorphism is given by $z \mapsto (\wp(z), \wp'(z))$ with respect to an appropriate choice of coordinates on $E(\mathbf{C})$. It is then an easy exercise to verify that $(\mathbf{C}/\Lambda)[n] \cong (\mathbf{Z}/n\mathbf{Z})^2$.

Another way to understand $E[n]$ is to use that $E(\mathbf{C})_{\mathrm{tor}}$ is isomorphic to the quotient

$$\mathrm{H}_1(E(\mathbf{C}), \mathbf{Q})/\,\mathrm{H}_1(E(\mathbf{C}), \mathbf{Z})$$

of homology groups and that the homology of a curve of genus g is isomorphic to $\mathbf{Z}^{2g}$. Then

$$E[n] \cong (\mathbf{Q}/\mathbf{Z})^2[n] = (\mathbf{Z}/n\mathbf{Z})^2.$$

If $n = p$ is a prime, then upon chosing a basis for the two-dimensional $\mathbf{F}_p$-vector space $E[p]$, we obtain an isomorphism $\mathrm{Aut}(E[p]) \cong \mathrm{GL}_2(\mathbf{F}_p)$. We thus obtain a two-dimensional representation

$$\overline{\rho}_{E,p} : G_K \to \mathrm{GL}_2(\mathbf{F}_p),$$

which is continuous if $\mathrm{GL}_2(\mathbf{F}_p)$ has the discrete topology, because the field

$$K(E[p]) = \{x, y : (x, y) \in E[p]\}$$

is a Galois extension of K of finite degree.

In order to attach an L-function to E, one could try to embed $\mathrm{GL}_2(\mathbf{F}_p)$ into $\mathrm{GL}_2(\mathbf{C})$ and use the construction of Artin L-functions from Section 10.5, but this approach depends on the choice of p, and does not "capture the essence" of E, in that there can be many elliptic curves with exactly the same mod p representation (though I think for $p \geq 23$ there are conjecturally only finitely many). Instead, we pass to a p-adic limit as follows. For each power p^n of p, we have a Galois representation ρ_{E,p^n}. The inverse limit of these representations is a continuous homomorphism

$$\rho_{E,p} : G_K \to \mathrm{Aut}(\varprojlim E[p^n]) \cong \mathrm{GL}_2(\mathbf{Z}_p),$$

where $\mathbf{Z}_p$ is the ring of p-adic integers. The composition of this homomorphism with the reduction map $\mathrm{GL}_2(\mathbf{Z}_p) \to \mathrm{GL}_2(\mathbf{F}_p)$ is the representation $\overline{\rho}_{E,p}$, which we defined above, which is why we denoted it by $\overline{\rho}_{E,p}$. We next try to mimic the construction of $L(\rho, s)$ from Section 10.5 in the context of a p-adic Galois representation $\rho_{E,p}$.

Definition 11.2.1 (Tate module). The p-adic Tate module of E is

$$T_p(E) = \varprojlim E[p^n].$$

Let M be the fixed field of $\ker(\rho_{E,p})$. The image of $\rho_{E,p}$ is infinite, so M is an infinite extension of K. Fortunately, one can prove that M is ramified at only finitely many primes (the primes of bad reduction for E and p). If ℓ is a prime of K, let D_ℓ be a choice of decomposition group for some prime $\mathfrak{p}$ of M lying over ℓ, and let I_ℓ be the inertia group. We haven't defined inertia and decomposition groups for infinite Galois extensions, but the definitions are almost the same: choose a prime of $\mathcal{O}_M$ over ℓ, and let D_ℓ be the subgroup of $\mathrm{Gal}(M/K)$ that leaves $\mathfrak{p}$ invariant. Then the submodule $T_p(E)^{I_\ell}$ of inertia invariants is a module for D_ℓ and the characteristic polynomial $F_\ell(x)$ of Frob_ℓ on $T_p(E)^{I_\ell}$ is well defined (since inertia acts trivially). Let $R_\ell(x)$ be the polynomial obtained by reversing the coefficients of $F_\ell(x)$. One can prove that $R_\ell(x) \in \mathbf{Z}[x]$ and that $R_\ell(x)$, for $\ell \neq p$ does not depend on the choice of p. Define $R_\ell(x)$ for $\ell = p$ using a different prime $q \neq p$, so the definition of $R_\ell(x)$ does not depend on the choice of p.

Definition 11.2.2. The L-series of E is

$$L(E, s) = \prod_\ell \frac{1}{R_\ell(\ell^{-s})}.$$

A prime $\mathfrak{p}$ of $\mathcal{O}_K$ is a prime of *good reduction* for E if there is an equation for E such that $E \mod \mathfrak{p}$ is an elliptic curve over $\mathcal{O}_K/\mathfrak{p}$.

If $K = \mathbf{Q}$ and ℓ is a prime of good reduction for E, then one can show that that $R_\ell(\ell^{-s}) = 1 - a_\ell \ell^{-s} + \ell^{1-2s}$, where $a_\ell = \ell + 1 - \#\tilde{E}(\mathbf{F}_\ell)$ and $\tilde{E}$ is the reduction of a local minimal model for E modulo ℓ. (There is a similar statement for $K \neq \mathbf{Q}$.)

One can prove using fairly general techniques that the product expression for $L(E, s)$ defines a holomorphic function in some right half plane of $\mathbf{C}$, i.e., the product converges for all s with $\mathrm{Re}(s) > \alpha$, for some real number α.

Conjecture 11.2.3. *The function $L(E, s)$ extends to a holomorphic function on all $\mathbf{C}$.*

11.2.1 Modularity of Elliptic Curves over Q

Fix an elliptic curve E over $\mathbf{Q}$. In this section we will explain what it means for E to be modular, and note the connection with Conjecture 11.2.3 from the previous section.

First, we give the general definition of modular form (of weight 2). The complex *upper half plane* is $\mathfrak{h} = \{z \in \mathbf{C} : \mathrm{Im}(z) > 0\}$. A *cuspidal modular form f* of level N

(of weight 2) is a holomorphic function $f : \mathfrak{h} \to \mathbf{C}$ such that $\lim_{z \to i\infty} f(z) = 0$ and for every integer matrix $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ with determinant 1 and $c \equiv 0 \pmod{N}$, we have

$$f\left(\frac{az+b}{cz+d}\right) = (cz+d)^{-2} f(z).$$

For each prime number ℓ of good reduction, let $a_\ell = \ell + 1 - \#\tilde{E}(\mathbf{F}_\ell)$. If ℓ is a prime of bad reduction let $a_\ell = 0, 1, -1$, depending on how singular the reduction $\tilde{E}$ of E is over $\mathbf{F}_\ell$. If $\tilde{E}$ has a cusp, then $a_\ell = 0$, and $a_\ell = 1$ or -1 if $\tilde{E}$ has a node; in particular, let $a_\ell = 1$ if and only if the tangents at the cusp are defined over $\mathbf{F}_\ell$.

Extend the definition of the a_ℓ to a_n for all positive integers n as follows. If $\gcd(n, m) = 1$ let $a_{nm} = a_n \cdot a_m$. If p^r is a power of a prime p of good reduction, let

$$a_{p^r} = a_{p^{r-1}} \cdot a_p \; - \; p \cdot a_{p^{r-2}}.$$

If p is a prime of bad reduction let $a_{p^r} = (a_p)^r$.

Attach to E the function

$$f_E(z) = \sum_{n=1}^{\infty} a_n e^{2\pi i z}.$$

It is an extremely deep theorem that $f_E(z)$ is actually a cuspidal modular form, and not just some random function.

The following theorem is called the modularity theorem for elliptic curves over $\mathbf{Q}$. Before it was proved it was known as the Taniyama-Shimura-Weil conjecture.

Theorem 11.2.4 (Wiles, Brueil, Conrad, Diamond, Taylor). *Every elliptic curve over $\mathbf{Q}$ is modular, i.e, the function $f_E(z)$ is a cuspidal modular form.*

Corollary 11.2.5 (Hecke). *If E is an elliptic curve over $\mathbf{Q}$, then the L-function $L(E, s)$ has an analytic continuous to the whole complex plane.*

Chapter 12

Galois Cohomology

12.1 Group Cohomology

12.1.1 Group Rings

Let G be a finite group. The group ring $\mathbf{Z}[G]$ of G is the free abelian group on the elements of G equipped with multiplication given by the group structure on G. Note that $\mathbf{Z}[G]$ is a commutative ring if and only if G is commutative.

For example, the group ring of the cyclic group $C_n = \langle a \rangle$ of order n is the free $\mathbf{Z}$-module on $1, a, \ldots, a^{n-1}$, and the multiplication is induced by $a^i a^j = a^{i+j} = a^{i+j \pmod n}$ extended linearly. For example, in $\mathbf{Z}[C_3]$ we have

$$(1+2a)(1-a^2) = 1 - a^2 + 2a - 2a^3 = 1 + 2a - a^2 - 2 = -1 + 2a - a^2.$$

You might think that $\mathbf{Z}[C_3]$ is isomorphic to the ring $\mathbf{Z}[\zeta_3]$ of integers of $\mathbf{Q}(\zeta_3)$, but you would be wrong, since the ring of integers is isomorphic to $\mathbf{Z}^2$ as abelian group, but $\mathbf{Z}[C_3]$ is isomorphic to $\mathbf{Z}^3$ as abelian group. (Note that $\mathbf{Q}(\zeta_3)$ is a quadratic extension of $\mathbf{Q}$.)

12.2 Modules and Group Cohomology

Let A be a G module. This means that A is an abelian group equipped with a left action of G, i.e., a group homomorphism $G \to \mathrm{Aut}(A)$, where $\mathrm{Aut}(A)$ denotes the group of bijections $A \to A$ that preserve the group structure on A. Alternatively, A is a module over the ring $\mathbf{Z}[G]$ in the usual sense of module. For example, $\mathbf{Z}$ with the trivial action is a module over any group G, as is $\mathbf{Z}/m\mathbf{Z}$ for any positive integer m. Another example is $G = (\mathbf{Z}/n\mathbf{Z})^*$, which acts via multiplication on $\mathbf{Z}/n\mathbf{Z}$.

For each integer $n \geq 0$ there is an abelian group $\mathrm{H}^n(G, A)$ called the *nth cohomology group of G acting on A*. The general definition is somewhat complicated, but the definition for $n \leq 1$ is fairly concrete. For example, the *0th cohomology group*

$$\mathrm{H}^0(G, A) = \{x \in A : \sigma x = x \text{ for all } \sigma \in G\} = G^A$$

is the subgroup of elements of A that are fixed by every element of G.

The *first cohomology group*

$$\mathrm{H}^1(G, A) = C^1(G, A)/B^1(G, A)$$

is the group of 1-cocycles modulo 1-coboundaries, where

$$C^1(G, A) = \{f : G \to A \text{ such that } f(\sigma\tau) = f(\sigma) + \sigma f(\tau)\}$$

and if we let $f_a : G \to A$ denote the set-theoretic map $f_a(\sigma) = \sigma(a) - a$, then

$$B^1(G, A) = \{f_a : a \in A\}.$$

There are also explicit, and increasingly complicated, definitions of $\mathrm{H}^n(G, A)$ for each $n \geq 2$ in terms of certain maps $G \times \cdots \times G \to A$ modulo a subgroup, but we will not need this.

For example, if A has the trivial action, then $B^1(G, A) = 0$, since $\sigma a - a = a - a = 0$ for any $a \in A$. Also, $C^1(G, A) = \mathrm{Hom}(G, A)$. If $A = \mathbf{Z}$, then since G is finite there are no nonzero homomorphisms $G \to \mathbf{Z}$, so $\mathrm{H}^1(G, \mathbf{Z}) = 0$.

If X is any abelian group, then

$$A = \mathrm{Hom}(\mathbf{Z}[G], X)$$

is a G-module. We call a module constructed in this way *co-induced*.

The following theorem gives three properties of group cohomology, which uniquely determine group cohomology.

Theorem 12.2.1. *Suppose G is a finite group. Then*

1. *We have $\mathrm{H}^0(G, A) = A^G$.*
2. *If A is a co-induced G-module, then $\mathrm{H}^n(G, A) = 0$ for all $n \geq 1$.*
3. *If $0 \to A \to B \to C \to 0$ is any exact sequence of G-modules, then there is a long exact sequence*

$$0 \to \mathrm{H}^0(G, A) \to \mathrm{H}^0(G, B) \to \mathrm{H}^0(G, C) \to \mathrm{H}^1(G, A) \to \cdots$$

$$\cdots \to \mathrm{H}^n(G, A) \to \mathrm{H}^n(G, B) \to \mathrm{H}^n(G, C) \to \mathrm{H}^{n+1}(G, A) \to \cdots$$

Moreover, the functor $\mathrm{H}^n(G, -)$ is uniquely determined by these three properties.

We will not prove this theorem. For proofs see [Cp86, Atiyah-Wall] and [Ser79, Ch. 7]. The properties of the theorem uniquely determine group cohomology, so one should in theory be able to use them to deduce anything that can be deduced about cohomology groups. Indeed, in practice one frequently proves results about higher cohomology groups $\mathrm{H}^n(G, A)$ by writing down appropriate exact sequences, using explicit knowledge of H^0, and chasing diagrams.

Remark 12.2.2. Alternatively, we could view the defining properties of the theorem as the definition of group cohomology, and could state a theorem that asserts that group cohomology exists.

Remark 12.2.3. For those familiar with commutative and homological algebra, we have

$$\mathrm{H}^n(G, A) = \mathrm{Ext}^n_{\mathbf{Z}[G]}(\mathbf{Z}, A),$$

where $\mathbf{Z}$ is the trivial G-module.

Remark 12.2.4. One can interpret $\mathrm{H}^2(G, A)$ as the group of equivalence classes of extensions of G by A, where an extension is an exact sequence

$$0 \to A \to M \to G \to 1$$

such that the induced conjugation action of G on A is the given action of G on A. (Note that G acts by conjugation, as A is a normal subgroup since it is the kernel of a homomorphism.)

12.2.1 Example Application of the Theorem

For example, let's see what we get from the exact sequence

$$0 \to \mathbf{Z} \xrightarrow{m} \mathbf{Z} \to \mathbf{Z}/m\mathbf{Z} \to 0,$$

where m is a positive integer, and $\mathbf{Z}$ has the structure of trivial G module. By definition we have $\mathrm{H}^0(G, \mathbf{Z}) = \mathbf{Z}$ and $\mathrm{H}^0(G, \mathbf{Z}/m\mathbf{Z}) = \mathbf{Z}/m\mathbf{Z}$. The long exact sequence begins

$$0 \to \mathbf{Z} \xrightarrow{m} \mathbf{Z} \to \mathbf{Z}/m\mathbf{Z} \to \mathrm{H}^1(G, \mathbf{Z}) \xrightarrow{m} \mathrm{H}^1(G, \mathbf{Z}) \to \mathrm{H}^1(G, \mathbf{Z}/m\mathbf{Z}) \to \mathrm{H}^2(G, \mathbf{Z}) \xrightarrow{m} \mathrm{H}^2(G, \mathbf{Z}) \to \cdots$$

From the first few terms of the sequence and the fact that $\mathbf{Z}$ surjects onto $\mathbf{Z}/m\mathbf{Z}$, we see that $[m]$ on $\mathrm{H}^1(G, \mathbf{Z})$ is injective. This is consistent with our observation above that $\mathrm{H}^1(G, \mathbf{Z}) = 0$. Using this vanishing and the right side of the exact sequence we obtain an isomorphism

$$\mathrm{H}^1(G, \mathbf{Z}/m\mathbf{Z}) \cong \mathrm{H}^2(G, \mathbf{Z})[m].$$

As we observed above, when a group acts trivially the H^1 is Hom, so

$$\mathrm{H}^2(G, \mathbf{Z})[m] \cong \mathrm{Hom}(G, \mathbf{Z}/m\mathbf{Z}). \tag{12.2.1}$$

One can prove that for any $n > 0$ and any module A that the group $\mathrm{H}^n(G, A)$ has exponent dividing $\#G$ (see Remark 12.3.4). Thus (12.2.1) allows us to understand $\mathrm{H}^2(G, \mathbf{Z})$, and this comprehension arose naturally from the properties that determine H^n.

12.3 Inflation and Restriction

Suppose H is a subgroup of a finite group G and A is a G-module. For each $n \geq 0$, there is a natural map

$$\mathrm{res}_H : \mathrm{H}^n(G, A) \to \mathrm{H}^n(H, A)$$

called restriction. Elements of $\mathrm{H}^n(G, A)$ can be viewed as classes of n-cocycles, which are certain maps $G \times \cdots \times G \to A$, and the restriction maps restricts these cocycles to $H \times \cdots \times H$.

If H is a normal subgroup of G, there is also an inflation map

$$\mathrm{inf}_H : \mathrm{H}^n(G/H, A^H) \to \mathrm{H}^n(G, A),$$

given by taking a cocycle $f : G/H \times \cdots \times G/H \to A^H$ and precomposing with the quotient map $G \to G/H$ to obtain a cocycle for G.

Proposition 12.3.1. *Suppose H is a normal subgroup of G. Then there is an exact sequence*

$$0 \to \mathrm{H}^1(G/H, A^H) \xrightarrow{\mathrm{inf}_H} \mathrm{H}^1(G, A) \xrightarrow{\mathrm{res}_H} \mathrm{H}^1(H, A).$$

Proof. Our proof follows [Ser79, pg. 117] closely.

We see that $\mathrm{res} \circ \mathrm{inf} = 0$ by looking at cochains. It remains to prove that inf_H is injective and that the image of inf_H is the kernel of res_H.

1. *That* inf_H *is injective:* Suppose $f : G/H \to A^H$ is a cocycle whose image in $\mathrm{H}^1(G, A)$ is equivalent to 0 modulo coboundaries. Then there is an $a \in A$ such that $f(\sigma) = \sigma a - a$, where we identify f with the map $G \to A$ that is constant on the costs of H. But f depends only on the costs of σ modulo H, so $\sigma a - a = \sigma\tau a - a$ for all $\tau \in H$, i.e., $\tau a = a$ (as we see by adding a to both sides and multiplying by σ^{-1}).Thus $a \in A^H$, so f is equivalent to 0 in $\mathrm{H}^1(H, A^H)$.

2. *The image of* inf_H *contains the kernel of* res_H*:* Suppose $f : G \to A$ is a cocycle whose restriction to H is a coboundary, i.e., there is $a \in A$ such that $f(\tau) = \tau a - a$ for all $\tau \in H$. Subtracting the coboundary $g(\sigma) = \sigma a - a$ for $\sigma \in G$ from f, we may assume $f(\tau) = 0$ for all $\tau \in H$. Examing the equation $f(\sigma\tau) = f(\sigma) + \sigma f(\tau)$ with $\tau \in H$ shows that f is constant on the cosets of H. Again using this formula, but with $\sigma \in H$ and $\tau \in G$, we see that

   $$f(\tau) = f(\sigma\tau) = f(\sigma) + \sigma f(\tau) = \sigma f(\tau),$$

   so the image of f is contained in A^H. Thus f defines a cocycle $G/H \to A^H$, i.e., is in the image of inf_H.

□

This proposition will be useful when proving the weak Mordell-Weil theorem.

Example 12.3.2. The sequence of Proposition 12.3.1 need not be surjective on the right. For example, suppose $H = A_3 \subset S_3$, and let S_3 act trivially on the cyclic group $C = \mathbf{Z}/3\mathbf{Z}$. Using the Hom interpretation of H^1, we see that $\mathrm{H}^1(S_3/A_3, C) = \mathrm{H}^1(S_3, C) = 0$, but $\mathrm{H}^1(A_3, C)$ has order 3.

Remark 12.3.3. On generalization of Proposition 12.3.1 is to a more complicated exact sequence involving the "transgression map" tr:

$$0 \to \mathrm{H}^1(G/H, A^H) \xrightarrow{\inf_H} \mathrm{H}^1(G, A) \xrightarrow{\mathrm{res}_H} \mathrm{H}^1(H, A)^{G/H} \xrightarrow{\mathrm{tr}} \mathrm{H}^2(G/H, A^H) \to \mathrm{H}^2(G, A).$$

Another generalization of Proposition 12.3.1 is that if $\mathrm{H}^m(H, A) = 0$ for $1 \leq m < n$, then there is an exact sequence

$$0 \to \mathrm{H}^n(G/H, A^H) \xrightarrow{\inf_H} \mathrm{H}^n(G, A) \xrightarrow{\mathrm{res}_H} \mathrm{H}^n(H, A).$$

Remark 12.3.4. If H is a not-necessarily-normal subgroup of G, there are also maps

$$\mathrm{cores}_H : \mathrm{H}^n(H, A) \to \mathrm{H}^n(G, A)$$

for each n. For $n = 0$ this is the trace map $a \mapsto \sum_{\sigma \in G/H} \sigma a$, but the definition for $n \geq 1$ is more involved. One has $\mathrm{cores}_H \circ \mathrm{res}_H = [\#(G/H)]$. Taking $H = 1$ we see that for each $n \geq 1$ the group $\mathrm{H}^n(G, A)$ is annihilated by $\#G$.

12.4 Galois Cohomology

Suppose L/K is a finite Galois extension of fields, and A is a module for $\mathrm{Gal}(L/K)$. Put

$$\mathrm{H}^n(L/K, A) = \mathrm{H}^n(\mathrm{Gal}(L/K), A).$$

Next suppose A is a module for the group $\mathrm{Gal}(K^{\mathrm{sep}}/K)$ and for any extension L of K, let

$$A(L) = \{x \in A : \sigma(x) = x \text{ all } \sigma \in \mathrm{Gal}(K^{\mathrm{sep}}/L)\}.$$

We think of $A(L)$ as the group of elements of A that are "defined over L". For each $n \geq 0$, put

$$\mathrm{H}^n(L/K, A) = \mathrm{H}^n(\mathrm{Gal}(L/K), A(L)).$$

Also, put

$$\mathrm{H}^n(K, A) = \varinjlim_{L/K} \mathrm{H}^n(L/K, A(L)),$$

where L varies over all finite Galois extensions of K. (Recall: Galois means normal and separable.)

Example 12.4.1. The following are examples of $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$-modules:

$$\overline{\mathbf{Q}}, \quad \overline{\mathbf{Q}}^*, \quad \overline{\mathbf{Z}}, \quad \overline{\mathbf{Z}}^*, \quad E(\overline{\mathbf{Q}}), \quad E(\overline{\mathbf{Q}})[n], \quad \mathrm{Tate}_\ell(E),$$

where E is an elliptic curve over $\mathbf{Q}$.

Theorem 12.4.2 (Hilbert 90). *We have* $\mathrm{H}^1(K, \overline{K}^*) = 0$.

Proof. See [Ser79]. The main input to the proof is linear independence of automorphism and a clever little calculation. □

Chapter 13

The Weak Mordell-Weil Theorem

13.1 Kummer Theory of Number Fields

Suppose K is a number field and fix a positive integer n. Consider the exact sequence

$$1 \to \mu_n \to \overline{K}^* \xrightarrow{n} \overline{K}^* \to 1.$$

The long exact sequence is

$$1 \to \mu_n(K) \to K^* \xrightarrow{n} K^* \to \mathrm{H}^1(K, \mu_n) \to \mathrm{H}^1(K, \overline{K}^*) = 0,$$

where $\mathrm{H}^1(K, \overline{K}^*) = 0$ by Theorem 12.4.2.

Assume now that the group μ_n of nth roots of unity is contained in K. Using Galois cohomology we obtain a relatively simple classification of all abelian extensions of K with Galois group cyclic of order dividing n. Moreover, since the action of $\mathrm{Gal}(\overline{K}/K)$ on μ_n is trivial, by our hypothesis that $\mu_n \subset K$, we see that

$$\mathrm{H}^1(K, \mu_n) = \mathrm{Hom}(\mathrm{Gal}(\overline{K}/K), \mu_n).$$

Thus we obtain an exact sequence

$$1 \to \mu_n \to K^* \xrightarrow{n} K^* \to \mathrm{Hom}(\mathrm{Gal}(\overline{K}/K), \mu_n) \to 1,$$

or equivalently, an isomorphism

$$K^*/(K^*)^n \cong \mathrm{Hom}(\mathrm{Gal}(\overline{K}/K), \mu_n),$$

By Galois theory, homomorphisms $\mathrm{Gal}(\overline{K}/K) \to \mu_n$ (up to automorphisms of μ_n) correspond to cyclic abelian extensions of K with Galois group a subgroup of the cyclic group μ_n of order n. Unwinding the definitions, what this says is that every cyclic abelian extension of K of degree dividing n is of the form $K(a^{1/n})$ for some element $a \in K$.

One can prove via calculations with discriminants, etc. that $K(a^{1/n})$ is unramified outside n and and the primes that divide $\mathrm{Norm}(a)$. Moreover, and this is a much bigger result, one can combine this with facts about class groups and unit groups to prove the following theorem:

Theorem 13.1.1. *Suppose K is a number field with $\mu_n \subset K$, where n is a positive integer. Then the maximal abelian exponent n extension L of K unramified outside a finite set S of primes is of finite degree.*

Sketch of Proof. We may enlarge S, because if an extension is unramified outside a set larger than S, then it is unramified outside S.

We first argue that we can enlarge S so that the ring

$$\mathcal{O}_{K,S} = \{a \in K^* : \mathrm{ord}_{\mathfrak{p}}(a\mathcal{O}_K) \geq 0 \text{ all } \mathfrak{p} \notin S\} \cup \{0\}$$

is a principal ideal domain. Note that for any S, the ring $\mathcal{O}_{K,S}$ is a Dedekind domain. Also, the condition $\mathrm{ord}_{\mathfrak{p}}(a\mathcal{O}_K) \geq 0$ means that in the prime ideal factorization of the fractional ideal $a\mathcal{O}_K$, we have that $\mathfrak{p}$ occurs to a nonnegative power. Thus we are allowing denominators at the primes in S. Since the class group of $\mathcal{O}_K$ is finite, there are primes $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ that generate the class group as a group (for example, take all primes with norm up to the Minkowski bound). Enlarge S to contain the primes $\mathfrak{p}_i$. Note that the ideal $\mathfrak{p}_i\mathcal{O}_{K,S}$ is the unit ideal (we have $\mathfrak{p}_i^m = (\alpha)$ for some $m \geq 1$; then $1/\alpha \in \mathcal{O}_{K,S}$, so $(\mathfrak{p}_i\mathcal{O}_{K,S})^m$ is the unit ideal, hence $\mathfrak{p}_i\mathcal{O}_{K,S}$ is the unit ideal by unique factorization in the Dedekind domain $\mathcal{O}_{K,S}$.) Then $\mathcal{O}_{K,S}$ is a principal ideal domain, since every ideal of $\mathcal{O}_{K,S}$ is equivalent modulo a principal ideal to a product of ideals $\mathfrak{p}_i\mathcal{O}_{K,S}$. Note that we have used that *the class group of $\mathcal{O}_K$ is finite*.

Next enlarge S so that all primes over $n\mathcal{O}_K$ are in S. Note that $\mathcal{O}_{K,S}$ is still a PID. Let

$$K(S,n) = \{a \in K^*/(K^*)^n : n \mid \mathrm{ord}_{\mathfrak{p}}(a) \text{ all } \mathfrak{p} \notin S\}.$$

Then a refinement of the arguments at the beginning of this section show that L is generated by all nth roots of the elements of $K(S,n)$. It thus sufficies to prove that $K(S,n)$ is finite.

There is a natural map

$$\phi : \mathcal{O}_{K,S}^* \to K(S,n).$$

Suppose $a \in K^*$ is a representative of an element in $K(S,n)$. The ideal $a\mathcal{O}_{K,S}$ has factorization which is a product of nth powers, so it is an nth power of an ideal. Since $\mathcal{O}_{K,S}$ is a PID, there is $b \in \mathcal{O}_{K,S}$ and $u \in \mathcal{O}_{K,S}^*$ such that

$$a = b^n \cdot u.$$

Thus $u \in \mathcal{O}_{K,S}^*$ maps to $[a] \in K(S,n)$. Thus ϕ is surjective.

Recall that we proved *Dirichlet's unit theorem* (see Theorem 9.1.2), which asserts that the group $\mathcal{O}_K^*$ is a finitely generated abelian group of rank $r + s - 1$. More

generally, we now show that $\mathcal{O}_{K,S}^*$ is a finitely generated abelian group of rank $r+s+\#S-1$. Once we have shown this, then since $K(S,n)$ is torsion group that is a quotient of a finitely generated group, we will conclude that $K(S,n)$ is finite, which will prove the theorem.

Thus it remains to prove that $\mathcal{O}_{K,S}^*$ has rank $r+s-1+\#S$. Let $\mathfrak{p}_1,\ldots,\mathfrak{p}_n$ be the primes in S. Define a map $\phi : \mathcal{O}_{K,S}^* \to \mathbf{Z}^n$ by

$$\phi(u) = (\mathrm{ord}_{\mathfrak{p}_1}(u),\ldots,\mathrm{ord}_{\mathfrak{p}_n}(u)).$$

First we show that $\mathrm{Ker}(\phi) = \mathcal{O}_K^*$. We have that $u \in \mathrm{Ker}(\phi)$ if and only if $u \in \mathcal{O}_{K,S}^*$ and $\mathrm{ord}_{\mathfrak{p}_i}(u) = 0$ for all i; but the latter condition implies that u is a unit at each prime in S, so $u \in \mathcal{O}_K^*$. Thus we have an exact sequence

$$1 \to \mathcal{O}_K^* \to \mathcal{O}_{K,S}^* \xrightarrow{\phi} \mathbf{Z}^n.$$

Next we show that the image of ϕ has finite index in $\mathbf{Z}^n$. Let h be the class number of $\mathcal{O}_K$. For each i there exists $\alpha_i \in \mathcal{O}_K$ such that $\mathfrak{p}_i^h = (\alpha_i)$. But $\alpha_i \in \mathcal{O}_{K,S}^*$ since $\mathrm{ord}_{\mathfrak{p}}(\alpha_i) = 0$ for all $\mathfrak{p} \notin S$ (by unique factorization). Then

$$\phi(\alpha_i) = (0,\ldots,0,h,0,\ldots,0).$$

It follows that $(h\mathbf{Z})^n \subset \mathrm{Im}(\phi)$, so the image of ϕ has finite index in $\mathbf{Z}^n$. It follows that $\mathcal{O}_{K,S}^*$ has rank equal to $r+s-1+\#S$. □

13.2 Proof of the Weak Mordell-Weil Theorem

Suppose E is an elliptic curve over a number field K, and fix a positive integer n. Just as with number fields, we have an exact sequence

$$0 \to E[n] \to E \xrightarrow{n} E \to 0.$$

Then we have an exact sequence

$$0 \to E[n](K) \to E(K) \xrightarrow{n} E(K) \to \mathrm{H}^1(K,E[n]) \to \mathrm{H}^1(K,E)[n] \to 0.$$

From this we obtain a short exact sequence

$$0 \to E(K)/nE(K) \to \mathrm{H}^1(K,E[n]) \to \mathrm{H}^1(K,E)[n] \to 0. \tag{13.2.1}$$

Now assume, in analogy with Section 13.1, that $E[n] \subset E(K)$, i.e., all n-torsion points are defined over K. Then

$$\mathrm{H}^1(K,E[n]) = \mathrm{Hom}(\mathrm{Gal}(\overline{K}/K),(\mathbf{Z}/n\mathbf{Z})^2),$$

and the sequence (13.2.1) induces an inclusion

$$E(K)/nE(K) \hookrightarrow \mathrm{Hom}(\mathrm{Gal}(\overline{K}/K),(\mathbf{Z}/n\mathbf{Z})^2). \tag{13.2.2}$$

Explicitly, this homomorphism sends a point P to the homomorphism defined as follows: Choose $Q \in E(\overline{K})$ such that $nQ = P$; then send each $\sigma \in \mathrm{Gal}(\overline{K}/K)$ to $\sigma(Q) - Q \in E[n] \cong (\mathbf{Z}/n\mathbf{Z})^2$. Given a point $P \in E(K)$, we obtain a homomorphism $\varphi : \mathrm{Gal}(\overline{K}/K) \to (\mathbf{Z}/n\mathbf{Z})^2$, whose kernel defines an abelian extension L of K that has exponent n. The amazing fact is that L can be ramified at most at the primes of bad reduction for E and the primes that divide n. Thus we can apply theorem 13.1.1 to see that there are only finitely many such L.

Theorem 13.2.1. *If $P \in E(K)$ is a point, then the field L obtained by adjoining to K all coordinates of all choices of $Q = \frac{1}{n}P$ is unramified outside n and the primes of bad reduction for E.*

Sketch of Proof. First one proves that if $\mathfrak{p} \nmid n$ is a prime of good reduction for E, then the natural reduction map $\pi : E(K)[n] \to \tilde{E}(\mathcal{O}_K/\mathfrak{p})$ is injective. The argument that π is injective uses "formal groups", whose development is outside the scope of this course. Next, as above, $\sigma(Q) - Q \in E(K)[n]$ for all $\sigma \in \mathrm{Gal}(\overline{K}/K)$. Let $I_\mathfrak{p} \subset \mathrm{Gal}(L/K)$ be the inertia group at $\mathfrak{p}$. Then by definition of interia group, $I_\mathfrak{p}$ acts trivially on $\tilde{E}(\mathcal{O}_K/\mathfrak{p})$. Thus for each $\sigma \in I_\mathfrak{p}$ we have

$$\pi(\sigma(Q) - Q) = \sigma(\pi(Q)) - \pi(Q) = \pi(Q) - \pi(Q) = 0.$$

Since π is injective, it follows that $\sigma(Q) = Q$ for $\sigma \in I_\mathfrak{p}$, i.e., that Q is fixed under all $I_\mathfrak{p}$. This means that the subfield of L generated by the coordinates of Q is unramified at $\mathfrak{p}$. Repeating this argument with all choices of Q implies that L is unramified at $\mathfrak{p}$. □

Theorem 13.2.2 (Weak Mordell-Weil). *Let E be an elliptic curve over a number field K, and let n be any positive integer. Then $E(K)/nE(K)$ is finitely generated.*

Proof. First suppose all elements of $E[n]$ have coordinates in K. Then the homomorphism (13.2.2) provides an injection of $E(K)/nE(K)$ into

$$\mathrm{Hom}(\mathrm{Gal}(\overline{K}/K), (\mathbf{Z}/n\mathbf{Z})^2).$$

By Theorem 13.2.1, the image consists of homomorphisms whose kernels cut out an abelian extension of K unramified outside n and primes of bad reduction for E. Since this is a finite set of primes, Theorem 13.1.1 implies that the homomorphisms all factor through a finite quotient $\mathrm{Gal}(L/K)$ of $\mathrm{Gal}(\overline{\mathbf{Q}}/K)$. Thus there can be only finitely many such homomorphisms, so the image of $E(K)/nE(K)$ is finite. Thus $E(K)/nE(K)$ itself is finite, which proves the theorem in this case.

Next suppose E is an elliptic curve over a number field, but do *not* make the hypothesis that the elements of $E[n]$ have coordinates in K. Since the group $E[n](\mathbf{C})$ is finite and its elements are defined over $\overline{\mathbf{Q}}$, the extension L of K got by adjoining to K all coordinates of elements of $E[n](\mathbf{C})$ is a finite extension. It is also Galois, as we saw when constructing Galois representations attached to elliptic curves. By Proposition 12.3.1, we have an exact sequence

$$0 \to \mathrm{H}^1(L/K, E[n](L)) \to \mathrm{H}^1(K, E[n]) \to \mathrm{H}^1(L, E[n]).$$

The kernel of the restriction map $\mathrm{H}^1(K, E[n]) \to \mathrm{H}^1(L, E[n])$ is finite, since it is isomorphic to the finite group cohomology group $\mathrm{H}^1(L/K, E[n](L))$. By the argument of the previous paragraph, the image of $E(K)/nE(K)$ in $\mathrm{H}^1(L, E[n])$ under

$$E(K)/nE(K) \hookrightarrow \mathrm{H}^1(K, E[n]) \xrightarrow{\mathrm{res}} \mathrm{H}^1(L, E[n])$$

is finite, since it is contained in the image of $E(L)/nE(L)$. Thus $E(K)/nE(K)$ is finite, since we just proved the kernel of res is finite. □

Chapter 14

Exercises

1. Let $A = \begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 7 & 8 & 9 \end{pmatrix}$.
   (a) Find the Smith normal form of A.
   (b) Prove that the cokernel of the map $\mathbf{Z}^3 \to \mathbf{Z}^3$ given by multiplication by A is isomorphic to $\mathbf{Z}/3\mathbf{Z} \oplus \mathbf{Z}$.
2. Show that the minimal polynomial of an algebraic number $\alpha \in \overline{\mathbf{Q}}$ is unique.
3. Which of the following rings have infinitely many prime ideals?
   (a) The integers $\mathbf{Z}$.
   (b) The ring $\mathbf{Z}[x]$ of polynomials over $\mathbf{Z}$.
   (c) The quotient ring $\mathbf{C}[x]/(x^{2005} - 1)$.
   (d) The ring $(\mathbf{Z}/6\mathbf{Z})[x]$ of polynomials over the ring $\mathbf{Z}/6Z$.
   (e) The quotient ring $\mathbf{Z}/n\mathbf{Z}$, for a fixed positive integer n.
   (f) The rational numbers $\mathbf{Q}$.
   (g) The polynomial ring $\mathbf{Q}[x, y, z]$ in three variables.
4. Which of the following numbers are algebraic integers?
   (a) The number $(1 + \sqrt{5})/2$.
   (b) The number $(2 + \sqrt{5})/2$.
   (c) The value of the infinite sum $\sum_{n=1}^{\infty} 1/n^2$.
   (d) The number $\alpha/3$, where α is a root of $x^4 + 54x + 243$.
5. Prove that $\overline{\mathbf{Z}}$ is not noetherian.
6. Prove that the ring $\overline{\mathbf{Z}}$ is not noetherian, but it is integrally closed in its field of fraction, and every nonzero prime ideal is maximal. Thus $\overline{\mathbf{Z}}$ is not a Dedekind domain.

7. Let K be a field.
   (a) Prove that the polynomial ring $K[x]$ is a Dedekind domain.
   (b) Is $\mathbf{Z}[x]$ a Dedekind domain?

8. Let $\mathcal{O}_K$ be the ring of integers of a number field. Let F_K denote the abelian group of fractional ideals of $\mathcal{O}_K$.
   (a) Prove that F_K is torsion free.
   (b) Prove that F_K is not finitely generated.
   (c) Prove that F_K is countable.
   (d) Conclude that if K and L are number fields, then there exists an isomorphism of groups $F_K \approx F_L$.

9. From basic definitions, find the rings of integers of the fields $\mathbf{Q}(\sqrt{11})$ and $\mathbf{Q}(\sqrt{13})$.

10. Factor the ideal (10) as a product of primes in the ring of integers of $\mathbf{Q}(\sqrt{11})$. You're allowed to use a computer, as long as you show the commands you use.

11. Let $\mathcal{O}_K$ be the ring of integers of a number field K, and let $p \in \mathbf{Z}$ be a prime number. What is the cardinality of $\mathcal{O}_K/(p)$ in terms of p and $[K : \mathbf{Q}]$, where (p) is the ideal of $\mathcal{O}_K$ generated by p?

12. Give an example of each of the following, with proof:
   (a) A non-principal ideal in a ring.
   (b) A module that is not finitely generated.
   (c) The ring of integers of a number field of degree 3.
   (d) An order in the ring of integers of a number field of degree 5.
   (e) The matrix on K of left multiplication by an element of K, where K is a degree 3 number field.
   (f) An integral domain that is not integrally closed in its field of fractions.
   (g) A Dedekind domain with finite cardinality.
   (h) A fractional ideal of the ring of integers of a number field that is not an integral ideal.

13. Let $\varphi : R \to S$ be a homomorphism of (commutative) rings.
   (a) Prove that if $I \subset S$ is an ideal, then $\varphi^{-1}(I)$ is an ideal of R.
   (b) Prove moreover that if I is prime, then $\varphi^{-1}(I)$ is also prime.

14. Let $\mathcal{O}_K$ be the ring of integers of a number field. The Zariski topology on the set $X = \mathrm{Spec}(\mathcal{O}_K)$ of all prime ideals of $\mathcal{O}_K$ has closed sets the sets of the form
$$V(I) = \{\mathfrak{p} \in X : \mathfrak{p} \mid I\},$$
where I varies through *all* ideals of $\mathcal{O}_K$, and $\mathfrak{p} \mid I$ means that $I \subset \mathfrak{p}$.

    (a) Prove that the collection of closed sets of the form $V(I)$ is a topology on X.

    (b) Let Y be the subset of nonzero prime ideals of $\mathcal{O}_K$, with the induced topology. Use unique factorization of ideals to prove that the closed subsets of Y are exactly the finite subsets of Y along with the set Y.

    (c) Prove that the conclusion of (a) is still true if $\mathcal{O}_K$ is replaced by an order in $\mathcal{O}_K$, i.e., a subring that has finite index in $\mathcal{O}_K$ as a $\mathbf{Z}$-module.

15. Explicitly factor the ideals generated by each of 2, 3, and 5 in the ring of integers of $\mathbf{Q}(\sqrt[3]{2})$. (Thus you'll factor 3 separate ideals as products of prime ideals.) You may assume that the ring of integers of $\mathbf{Q}(\sqrt[3]{2})$ is $\mathbf{Z}[\sqrt[3]{2}]$, but do *not* simply use a computer command to do the factorizations.

16. Let $K = \mathbf{Q}(\zeta_{13})$,where ζ_{13} is a primitive 13th root of unity. Note that K has ring of integers $\mathcal{O}_K = \mathbf{Z}[\zeta_{13}]$.

    (a) Factor 2, 3, 5, 7, 11, and 13 in the ring of integers $\mathcal{O}_K$. You may use a computer.

    (b) For $p \neq 13$, find a conjectural relationship between the number of prime ideal factors of $p\mathcal{O}_K$ and the order of the reduction of p in $(\mathbf{Z}/13\mathbf{Z})^*$.

    (c) Compute the minimal polynomial $f(x) \in \mathbf{Z}[x]$ of ζ_{13}. Reinterpret your conjecture as a conjecture that relates the degrees of the irreducible factors of $f(x) \pmod p$ to the order of p modulo 13. Does your conjecture remind you of quadratic reciprocity?

17. (a) Find by hand and with proof the ring of integers of each of the following two fields: $\mathbf{Q}(\sqrt{5})$, $\mathbf{Q}(i)$.

    (b) Find the ring of integers of $\mathbf{Q}(x^5 + 7x + 1)$ using a computer.

18. Let p be a prime. Let $\mathcal{O}_K$ be the ring of integers of a number field K, and suppose $a \in \mathcal{O}_K$ is such that $[\mathcal{O}_K : \mathbf{Z}[a]]$ is finite and coprime to p. Let $f(x)$ be the minimal polynomial of a. We proved in class that if the reduction $\overline{f} \in \mathbf{F}_p[x]$ of f factors as
$$\overline{f} = \prod g_i^{e_i},$$
where the g_i are distinct irreducible polynomials in $\mathbf{F}_p[x]$, then the primes appearing in the factorization of $p\mathcal{O}_K$ are the ideals $(p, g_i(a))$. In class, we did not prove that the exponents of these primes in the factorization of $p\mathcal{O}_K$ are the e_i. Prove this.

19. Let $a_1 = 1 + i$, $a_2 = 3 + 2i$, and $a_3 = 3 + 4i$ as elements of $\mathbf{Z}[i]$.

    (a) Prove that the ideals $I_1 = (a_1)$, $I_2 = (a_2)$, and $I_3 = (a_3)$ are coprime in pairs.

    (b) Compute $\#\mathbf{Z}[i]/(I_1 I_2 I_3)$.

    (c) Find a single element in $\mathbf{Z}[i]$ that is congruent to n modulo I_n, for each $n \leq 3$.

20. Find an example of a field K of degree at least 4 such that the ring $\mathcal{O}_K$ of integers of K is not of the form $\mathbf{Z}[a]$ for any $a \in \mathcal{O}_K$.

21. Let $\mathfrak{p}$ be a prime ideal of $\mathcal{O}_K$, and suppose that $\mathcal{O}_K/\mathfrak{p}$ is a finite field of characteristic $p \in \mathbf{Z}$. Prove that there is an element $\alpha \in \mathcal{O}_K$ such that $\mathfrak{p} = (p, \alpha)$. This justifies why PARI can represent prime ideals of $\mathcal{O}_K$ as pairs (p, α). (More generally, if I is an ideal of $\mathcal{O}_K$, we can choose one of the elements of I to be *any* nonzero element of I.)

22. (*) Give an example of an order $\mathcal{O}$ in the ring of integers of a number field and an ideal I such that I cannot be generated by 2 elements as an ideal. Does the Chinese Remainder Theorem hold in $\mathcal{O}$? [The (*) means that this problem is more difficult than usual.]

23. For each of the following three fields, determining if there is an order of discriminant 20 contained in its ring of integers:

$$K = \mathbf{Q}(\sqrt{5}), \quad K = \mathbf{Q}(\sqrt[3]{2}), \quad \text{and} \ldots$$

    K any extension of $\mathbf{Q}$ of degree 2005. [Hint: for the last one, apply the exact form of our theorem about finiteness of class groups to the unit ideal to show that the discriminant of a degree 2005 field must be large.]

24. Prove that the quantity $C_{r,s}$ in our theorem about finiteness of the class group can be taken to be $\left(\frac{4}{\pi}\right)^s \frac{n!}{n^n}$, as follows (adapted from [SD01, pg. 19]): Let S be the set of elements $(x_1, \ldots, x_n) \in \mathbf{R}^n$ such that

$$|x_1| + \cdots |x_r| + 2 \sum_{v=r+1}^{r+s} \sqrt{x_v^2 + x_{v+s}^2} \leq 1.$$

    (a) Prove that S is convex and that $M = n^{-n}$, where

$$M = \max\{|x_1 \cdots x_r \cdot (x_{r+1}^2 + x_{(r+1)+s}^2) \cdots (x_{r+s}^2 + x_n^2)| : (x_1, \ldots, x_n) \in S\}.$$

    [Hint: For convexity, use the triangle inequality and that for $0 \leq \lambda \leq 1$, we have

$$\lambda\sqrt{x_1^2 + y_1^2} + (1-\lambda)\sqrt{x_2^2 + y_2^2} \geq \sqrt{(\lambda x_1 + (1-\lambda)x_2)^2 + (\lambda y_1 + (1-\lambda)y_2)^2}$$

for $0 \leq \lambda \leq 1$. In polar coordinates this last inequality is

$$\lambda r_1 + (1-\lambda) r_2 \geq \sqrt{\lambda^2 r_1^2 + 2\lambda(1-\lambda) r_1 r_2 \cos(\theta_1 - \theta_2) + (1-\lambda)^2 r_2^2},$$

which is trivial. That $M \leq n^{-n}$ follows from the inequality between the arithmetic and geometric means.

(b) Transforming pairs x_v, x_{v+s} from Cartesian to polar coordinates, show also that $v = 2^r (2\pi)^s D_{r,s}(1)$, where

$$D_{\ell,m}(t) = \int \cdots \int_{\mathcal{R}_{\ell,m}(t)} y_1 \cdots y_m dx_1 \cdots dx_\ell dy_1 \cdots dy_m$$

and $\mathcal{R}_{\ell,\Updownarrow}(t)$ is given by $x_\rho \geq 0$ $(1 \leq \rho \leq \ell)$, $y_\rho \geq 0$ $(1 \leq \rho \leq m)$ and

$$x_1 + \cdots + x_\ell + 2(y_1 + \cdots + y_m) \leq t.$$

(c) Prove that

$$D_{\ell,m}(t) = \int_0^t D_{\ell-1,m}(t-x)dx = \int_0^{t/2} D_{\ell,m-1}(t-2y) y dy$$

and deduce by induction that

$$D_{\ell,m}(t) = \frac{4^{-m} t^{\ell+2m}}{(\ell+2m)!}$$

25. Let K vary through all number fields. What torsion subgroups $(U_K)_{\mathrm{tor}}$ actually occur?

26. If $U_K \approx \mathbf{Z}^n \times (U_K)_{\mathrm{tor}}$, we say that U_K has rank n. Let K vary through all number fields. What ranks actually occur?

27. Let K vary through all number fields such that the group U_K of units of K is a finite group. What finite groups U_K actually occur?

28. Let $K = \mathbf{Q}(\zeta_5)$.

    (a) Show that $r = 0$ and $s = 2$.

    (b) Find explicit generators for the group of units of U_K.

    (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.

29. Let K be a number field. Prove that $p \mid d_K$ if and only if p ramifies in K. (Note: This fact is proved in many books.)

30. 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. [Hint: The extension $\mathbf{Q}(\sqrt{d}, d \in \mathbf{Q}^*/(\mathbf{Q}^*)^2)$ is an extension of $\mathbf{Q}$ with Galois group $X \approx \prod \mathbf{F}_2$. The index-two open subgroups of X correspond to the quadratic extensions of $\mathbf{Q}$. However, Zorn's lemma implies that X contains many index-two subgroups that do not correspond to quadratic extensions of $\mathbf{Q}$.]

31. (a) Give an example of a finite nontrivial Galois extension K of $\mathbf{Q}$ and a prime ideal $\mathfrak{p}$ such that $D_{\mathfrak{p}} = \mathrm{Gal}(K/\mathbf{Q})$.
    (b) Give an example of a finite nontrivial Galois extension K of $\mathbf{Q}$ and a prime ideal $\mathfrak{p}$ such that $D_{\mathfrak{p}}$ has order 1.
    (c) Give an example of a finite Galois extension K of $\mathbf{Q}$ and a prime ideal $\mathfrak{p}$ such that $D_{\mathfrak{p}}$ is not a normal subgroup of $\mathrm{Gal}(K/\mathbf{Q})$.
    (d) Give an example of a finite Galois extension K of $\mathbf{Q}$ and a prime ideal $\mathfrak{p}$ such that $I_{\mathfrak{p}}$ is not a normal subgroup of $\mathrm{Gal}(K/\mathbf{Q})$.

32. 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 (32a) 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 $p = 5, 7, 11, 13$.

33. Look up the Riemann-Roch theorem in a book on algebraic curves.
    (a) Write it down in your own words.
    (b) Let E be an elliptic curve over a field K. Use the Riemann-Roch theorem to deduce that the natural map
    $$E(K) \to \mathrm{Pic}^0(E/K)$$
    is an isomorphism.

34. Suppose G is a finite group and A is a finite G-module. Prove that for any q, the group $\mathrm{H}^q(G, A)$ is a torsion abelian group of exponent dividing the order $\#A$ of A.

35. Let $K = \mathbf{Q}(\sqrt{5})$ and let $A = U_K$ be the group of units of K, which is a module over the group $G = \mathrm{Gal}(K/\mathbf{Q})$. Compute the cohomology groups $\mathrm{H}^0(G, A)$ and $\mathrm{H}^1(G, A)$. (You shouldn't use a computer, except maybe to determine U_K.)

36. Let $K = \mathbf{Q}(\sqrt{-23})$ and let C be the class group of $\mathbf{Q}(\sqrt{-23})$, which is a module over the Galois group $G = \mathrm{Gal}(K/\mathbf{Q})$. Determine $\mathrm{H}^0(G, C)$ and $\mathrm{H}^1(G, C)$.

37. Let E be the elliptic curve $y^2 = x^3 + x + 1$. Let $E[2]$ be the group of points of order dividing 2 on E. Let

$$\overline{\rho}_{E,2} : \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \to \mathrm{Aut}(E[2])$$

be the mod 2 Galois representation associated to E.

(a) Find the fixed field K of $\ker(\overline{\rho}_{E,2})$.

(b) Is $\overline{\rho}_{E,2}$ surjective?

(c) Find the group $\mathrm{Gal}(K/\mathbf{Q})$.

(d) Which primes are ramified in K?

(e) Let I be an inertia group above 2, which is one of the ramified primes. Determine $E[2]^I$ explicitly for your choice of I. What is the characteristic polynomial of Frob_2 acting on $E[2]^I$.

(f) What is the characteristic polynomial of Frob_3 acting on $E[2]$?

(g) Let K be a number field. Prove that there is a finite set S of primes of K such that

$$\mathcal{O}_{K,S} = \{a \in K^* : \mathrm{ord}_{\mathfrak{p}}(a\mathcal{O}_K) \geq 0 \text{ all } \mathfrak{p} \notin S\} \cup \{0\}$$

is a prinicipal ideal domain. The condition $\mathrm{ord}_{\mathfrak{p}}(a\mathcal{O}_K) \geq 0$ means that in the prime ideal factorization of the fractional ideal $a\mathcal{O}_K$, we have that $\mathfrak{p}$ occurs to a nonnegative power.

(h) Let $a \in K$ and n a positive integer. Prove that $L = K(a^{1/n})$ is unramified outside the primes that divide n and the norm of a. This means that if $\mathfrak{p}$ is a prime of $\mathcal{O}_K$, and $\mathfrak{p}$ is coprime to $n\,\mathrm{Norm}_{L/K}(a)\mathcal{O}_K$, then the prime factorization of $\mathfrak{p}\mathcal{O}_L$ involves no primes with exponent bigger than 1.

(i) Write down a proof of Hilbert's Theorem 90, formulated as the statement that for any number field K, we have

$$\mathrm{H}^1(K, \overline{K}^*) = 0.$$

Bibliography

[ABC$^+$] B. Allombert, K. Belabas, H. Cohen, X. Roblot, and I. Zakharevitch, `PARI/GP`, `http://pari.math.u-bordeaux.fr/`.

[Art23] E. Artin, *Über eine neue Art von L-reihen*, Abh. Math. Sem. Univ. Hamburg **3** (1923), 89–108.

[Art30] E Artin, *Zur Theorie der L-Reihen mit allgemeinen Gruppencharakteren*, Abh. math. Semin. Univ. Hamburg **8** (1930), 292–306.

[Art91] M. Artin, *Algebra*, Prentice Hall Inc., Englewood Cliffs, NJ, 1991. MR 92g:00001

[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

[BDSBT01] Kevin Buzzard, Mark Dickinson, Nick Shepherd-Barron, and Richard Taylor, *On icosahedral Artin representations*, Duke Math. J. **109** (2001), no. 2, 283–318. MR MR1845181 (2002k:11078)

[BL94] J. A. Buchmann and H. W. Lenstra, Jr., *Approximating rings of integers in number fields*, J. Théor. Nombres Bordeaux **6** (1994), no. 2, 221–260. MR MR1360644 (96m:11092)

[BS02] K. Buzzard and W. A. Stein, *A mod five approach to modularity of icosahedral Galois representations*, Pacific J. Math. **203** (2002), no. 2, 265–282. MR 2003c:11052

[Buh78] J. P. Buhler, *Icosahedral Galois representations*, Springer-Verlag, Berlin, 1978, Lecture Notes in Mathematics, Vol. 654.

[Cas67] J. W. S. Cassels, *Global fields*, Algebraic Number Theory (Proc. Instructional Conf., Brighton, 1965), Thompson, Washington, D.C., 1967, pp. 42–84.

[CL84] H. Cohen and H. W. Lenstra, Jr., *Heuristics on class groups of number fields*, Number theory, Noordwijkerhout 1983 (Noordwijkerhout, 1983), Lecture Notes in Math., vol. 1068, Springer, Berlin, 1984, pp. 33–62. MR MR756082 (85j:11144)

[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

[Har77] R. Hartshorne, *Algebraic Geometry*, Springer-Verlag, New York, 1977, Graduate Texts in Mathematics, No. 52.

[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

[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

[Ser79] J-P. Serre, *Local fields*, Springer-Verlag, New York, 1979, Translated from the French by Marvin Jay Greenberg.

[Sil92] J. H. Silverman, *The arithmetic of elliptic curves*, Springer-Verlag, New York, 1992, Corrected reprint of the 1986 original.

[Ste] W. A. Stein, *Elementary Number Theory,* `http://modular.fas.harvard.edu/ent/`.