Algebraic Number Theory Course Notes (Fall 2006) Math 8803, Georgia Tech

Matthew Baker

E-mail address: mbaker@math.gatech.edu

School of Mathematics, Georgia Institute of Technology, Atlanta, GA 30332-0140, USA

Contents

Preface

These are the lecture notes from a graduate-level Algebraic Number Theory course taught at the Georgia Institute of Technology in Fall 2006. The notes are a revised version of those written for an Algebraic Number Theory course taught at the University of Georgia in Fall 2002.

We assume that the reader is familiar with the material covered in a one-year course on Abstract Algebra at the graduate level, including various standard facts about groups, rings, fields, vector spaces, modules, and Galois Theory. A good reference for this material is Dummitt and Foote's book "Abstract Algebra".

Our goal in designing this course was to cover as many of the fundamental ideas of Algebraic Number Theory as possible in one semester, while retaining a concrete and motivated approach to the subject. We do not claim any novelty in our approach, except perhaps in our selection and organization of the material. Algebraic Number Theory is often presented in either a very elementary way which does not take full advantage of students' backgrounds in Abstract Algebra, or in a very abstract and high-powered way which runs the danger of divorcing itself in the students' minds from the concrete origins and applications of the subject. We have tried to steer a middle ground between these approaches. In the process, we have hopefully designed a course which is at once accessible, motivated, and challenging, which fits neatly into one semester, and which gives students a solid foundation for further explorations in number theory.

We have benefitted from many different sources in assembling this material, including (but not limited to) Marcus' "Number Fields", Esmonde and Murty's "Problems in Algebraic Number Theory", Janusz's "Algebraic Number Fields", Cassels' "Local Fields", and Neukirch's "Algebraic Number Theory". We have also used some material from an Algebraic Number Theory course taught by Paul Vojta at UC Berkeley in Fall 1994.

I would like to thank Michael Guy, Sungkon Chang, Jim Blair, Paul Pollack, Xander Faber, Roy Smith, Robert Rumely, Ander Steele, Farbod Shokrieh, Ye Luo, Brad Green, Subrahmanyam Kalyanasundaram, and Yan Ding for their helpful comments on these notes.

Special thanks go to David Krumm, Elmar Grosse-Klönne, Shelly Manber, and Eugenia Rosu for providing me with detailed lists of corrections, and to Shelly Manber and Eugenia Rosu for helping to implement those corrections.

CHAPTER 1

Unique Factorization (and lack thereof) in number rings

1. UFD's, Euclidean Domains, Gaussian Integers, and Fermat's Last Theorem

We will begin by exploring the ring $\mathbb{Z}[i]$ of Gaussian integers. By definition,

$$\mathbb{Z}[i] = \{a + bi \ : \ a, b \in \mathbb{Z}\} \subset \mathbb{C}.$$

We will see later that this ring is a *unique factorization domain* (UFD), a fact which has many useful consequences.

1.1. Unique Factorization Domains. Let R be a commutative ring with a multiplicative identity element 1. (All rings in this course will be commutative with a multiplicative identity unless otherwise specified.)

A *unit* of R is an element with a multiplicative inverse.

A nonzero element $x \in R$ is called *irreducible* if x is not itself a unit, but whenever $x = ab$ with $a, b \in R$, one of a or b must be a unit. This is one way to generalize the concept of a prime number to an arbitrary ring.

Another way is with the notion of a prime element: a nonzero element $\pi \in R$ is *prime* if π is not a unit, and whenever $\pi \mid xy$ in R, we have $\pi \mid x$ or $\pi \mid y$. In an integral domain R, every prime element is irreducible, but the converse is false in general – see §1 of Appendix A for details.

Two elements $x, y \in R$ are called *associate* (written $x \sim y$) if there exists a unit $u \in R$ such that $x = uy$. It is easy to see that $\sim$ is an equivalence relation.

By definition, a ring R is a UFD if:

- R is an integral domain, i.e., $xy = 0$ in R implies that one of x, y is zero.
- Every non-zero non-unit element $x \in R$ can be written as a product $x = q_1 \cdots q_r$ of irreducible elements.
- The decomposition of x into irreducibles is unique up to units and the order of the factors; in other words, if $x = q_1 \cdots q_r$

and also $x = q_1' \cdots q_s'$, then $r = s$, and after relabeling we have $q_i \sim q_i'$ for all $i = 1, \ldots, r$.

1.2. A Diophantine Problem. We all know that $\mathbb{Z}$ is a UFD (this is the "fundamental theorem of arithmetic"). It's also true that $\mathbb{Z}[i]$ is a UFD. Let's *assume* this for the moment and see how to use this fact to find all integer solutions to a famous diophantine equation.

Problem 1: Find all $x, y \in \mathbb{Z}$ such that $x^3 - y^2 = 1$.

Remark: This is a special case of a general problem known as "Catalan's conjecture", which is that the only solution to $x^m - y^n = 1$ with x, y positive integers and $m, n \geq 2$ is $3^2 - 2^3 = 1$. In other words, the only consecutive perfect powers are 8 and 9. Catalan's conjecture was posed in 1844 and remained open until a proof was finally found in 2002 by the Swiss mathematician Preda Mihailescu. Mihailescu's proof uses the theory of cyclotomic fields, which is one of the main topics of this course, although we will not have time to go into enough detail to understand the proof of Catalan's conjecture.

Remark: The equation $y^2 = x^3 - 1$ is an example of an *elliptic curve*. Elliptic curves play an important role in modern number theory; for example, they are central to Wiles' proof of Fermat's Last Theorem.

Before solving Problem 1, we need to determine the units of $\mathbb{Z}[i]$.

LEMMA 1.1. *The units of* $\mathbb{Z}[i]$ *are* $\pm 1, \pm i$.

PROOF. It is clear that $\pm 1, \pm i$ are units. Conversely, suppose $x = a+bi$ is a unit. Then there exists $y = c+di$ such that $xy = 1$. Taking the square of the complex absolute value of each side of this equation (and using the fact that $|xy| = |x| \cdot |y|$), we find that $(a^2 + b^2)(c^2 + d^2) = 1$. Since a, b, c, d are integers, this implies that $a^2 + b^2 = 1$, and therefore that $(a, b) \in \{(\pm 1, 0), (0, \pm 1)\}$ as desired. □

Note the key role played in the proof of the lemma by the function $N : \mathbb{Z}[i] \to \mathbb{Z}$ given by $N(a + bi) = a^2 + b^2$. (We call $N(x)$ the *norm* of the Gaussian integer x.)

We see from the proof that for $x \in \mathbb{Z}[i]$, $N(x) = 1$ if and only if x is a unit. This easily leads to the following criterion for irreducibility in $\mathbb{Z}[i]$:

LEMMA 1.2. *If* $x \in \mathbb{Z}[i]$ *and* $N(x)$ *is prime, then* x *is irreducible. (Note: The converse is false!)*

PROOF. If $x = yz$ in $\mathbb{Z}[i]$ and $N(x) = N(y)N(z)$ is prime, then one of $N(y), N(z)$ must be 1, hence one of y, z is a unit. As $N(x) \neq 1$, x is not itself a unit. Therefore x is irreducible. □

Solution to Problem 1: (Assuming $\mathbb{Z}[i]$ is a UFD)

Suppose $x^3 - y^2 = 1$. We will prove in a sequence of steps that $(x, y) = (1, 0)$.

PROOF. **Step 1:** If x is even, then

$$x^3 \equiv 0 \pmod 8 \Rightarrow y^2 \equiv -1 \pmod 8.$$

But -1 is not a square mod 8. Therefore

$$x \text{ is odd and } y \text{ is even.}$$

Step 2: Factor the equation $y^2 + 1 = x^3$ in $\mathbb{Z}[i]$: we get

$$(y + i)(y - i) = x^3.$$

Step 3: We claim that $y + i$ and $y - i$ are relatively prime, i.e., a common factor of both must be a unit. Suppose, for the sake of contradiction, that there exists $\alpha \in \mathbb{Z}[i]$, α not a unit, such that $\alpha \mid y+i$ and $\alpha \mid y - i$.

Then $\alpha \mid (y+i)-(y-i) = 2i$. But $2i = (1+i)^2$, so $\alpha \mid (1+i)^2$. Now $(1 + i)$ is irreducible (since its norm is 2, which is prime). By unique factorization, since α is not a unit, we must have $(1 + i) \mid \alpha$.

But then $(1 + i) \mid (y + i)(y - i) = x^3$, and by unique factorization, $(1 + i) \mid x$. Therefore there exists $\beta \in \mathbb{Z}[i]$ such that $x = (1 + i)\beta$. Multiplying this equation by its complex conjugate, we get $x\overline{x} = (1 + i)(1 - i)\beta\overline{\beta}$, i.e., $x^2 = 2\beta\overline{\beta}$, so that $2 \mid x^2$. But then x is even, a contradiction.

We conclude that no such α exists, proving the claim.

Step 4: By unique factorization, it follows that $y + i$ and $y - i$ are each of the form $u\beta^3$ for some unit u and some $\beta \in \mathbb{Z}[i]$. As $\pm 1, \pm i$ are the only units in $\mathbb{Z}[i]$ and each is itself a perfect cube, we find that:

$$y + i, y - i \text{ are both cubes in } \mathbb{Z}[i].$$

Step 5: Write $y + i = (a + bi)^3$ with $a, b \in \mathbb{Z}$. Then

$$y + i = a^3 + 3a^2bi - 3ab^2 - b^3i = (a^3 - 3ab^2) + (3a^2b - b^3)i.$$

Comparing real and imaginary parts, we find that $y = a(a^2 - 3b^2)$ and $1 = b(3a^2 - b^2)$. From the second equation, it follows that

$$b = \pm 1.$$

Step 6: If $b = 1$, then $1 = 3a^2 - 1 \Rightarrow 3a^2 = 2$, which is impossible. If $b = -1$, then $-1 = 3a^2 - 1 \Rightarrow a = 0$.

So $a = 0$, and therefore, since $y = a(a^2 - 3b^2)$, it follows that $y = 0$. As $x^3 = y^2 + 1$, we have $x = 1$, so that

$$(x, y) = (1, 0)$$

as claimed.

□

1.3. Unique Factorization in Euclidean Domains. The solution of Problem 1 relied crucially on the fact that $\mathbb{Z}[i]$ is a UFD. In order to give a proof of this fact, we introduce the notion of a Euclidean domain.

Let R be an integral domain, and let $\phi : R \to \mathbb{Z}$ be a function such that $\phi(x) \geq 0$ for all x and $\phi(0) = 0$. (We call such a function a *norm* on R.)

We say that R is a *Euclidean domain* (with respect to ϕ) if the *division algorithm* holds: whenever we are given $x, y \in R$ with $y \neq 0$, there exist $q, r \in R$ such that $x = yq + r$ and either $r = 0$ or $\phi(r) < \phi(y)$. Note that q, r are not required to be unique.

It is a basic fact of arithmetic that $\mathbb{Z}$ is a Euclidean domain (with $\phi(x) = |x|$). Similarly, if k is any field then the polynomial ring $k[x]$ is a Euclidean domain (with $\phi(f) = \deg(f)$ for $f \neq 0$).

By Theorem A.5, every Euclidean domain is a UFD.

Let $N : \mathbb{Z}[i] \to \mathbb{Z}$ be the norm given by $N(a + bi) = a^2 + b^2$. Note that $N(x) = 0$ iff $x = 0$, which is stronger than what is required of ϕ in the definition of a Euclidean domain. We want to prove:

PROPOSITION 1.3. *If $x, y \in \mathbb{Z}[i]$ with $y \neq 0$, then there exist $q, r \in \mathbb{Z}[i]$ such that $x = yq + r$ with $N(r) < N(y)$. In particular, $\mathbb{Z}[i]$ is a Euclidean domain (and therefore also a unique factorization domain).*

PROOF. We can think of the elements of $\mathbb{Z}[i]$ as forming a lattice inside the complex plane $\mathbb{C}$. Intuitively, since q is the "quotient" in the division algorithm, q should be close to the complex number $z := \frac{x}{y}$. So we let q be any element of $\mathbb{Z}[i]$ such that $|z - q| \leq |z - q'|$ for all $q' \in \mathbb{Z}[i]$. In other words, q is the lattice point closest to $\frac{x}{y}$ (and if there is a tie for the "closest lattice point", we simply choose one). By elementary geometry, we have $|z - q| \leq \frac{1}{\sqrt{2}}$.

Now let $r = x - yq$. Then

$$N(r) = N(x - yq) = |x - yq|^2 = |y(\frac{x}{y} - q)|^2 = |y|^2|z - q|^2 \leq \frac{1}{2}N(y) < N(y)$$

as desired. □

1.4. Decomposition of rational primes in $\mathbb{Z}[i]$. In this section, we investigate how a prime number p factors into irreducibles in $\mathbb{Z}[i]$. We will see that the type of factorization depends on the congruence class of p modulo 4.

If $p = 2$, then we have $2 = -i(1+i)^2$, and $(1+i)$ is irreducible. For odd primes, we have the following proposition:

PROPOSITION 1.4. *Let p be an odd prime number. Then:*

(i) *If $p \equiv 3 \pmod 4$ then p is irreducible in $\mathbb{Z}[i]$.*
(ii) *If $p \equiv 1 \pmod 4$ then $p = \pi\overline{\pi}$ in $\mathbb{Z}[i]$, where π and $\overline{\pi}$ are irreducible.*

PROOF. We begin with some preliminary remarks. Since $N(p) = p^2$ and $N(xy) = N(x)N(y)$, we see that if π is irreducible in $\mathbb{Z}[i]$ and $\pi \mid p$, then $N(\pi) = p$ or p^2. Moreover, if $N(\pi) = p^2$ then π and p are associate, so that p is irreducible. In particular, p is irreducible if and only if $N(\pi) = p^2$.

Suppose $p \equiv 3 \pmod 4$. If some element $\pi = a + bi$ has norm p, then $a^2 + b^2 = p \equiv 3 \pmod 4$. But this is impossible, since 0 and 1 are the only squares modulo 4. So we conclude in this case that p is irreducible.

Now suppose $p \equiv 1 \pmod 4$. By elementary number theory, -1 is a square mod p, i.e., there exists an integer n such that $p \mid n^2 + 1 = (n+i)(n-i)$. Suppose p is irreducible in $\mathbb{Z}[i]$. Then since irreducible elements of $\mathbb{Z}[i]$ are prime, we must have $p \mid (n \pm i)$. However, if $p \mid (n+i)$ then it is easy to see that $p \mid (n-i)$ also, and vice-versa. It follows that p divides both $n+i$ and $n-i$. It therefore also divides $(n+i)+(n-i) = 2n$. As p is irreducible and its norm is odd, $p \nmid 2$, so $p \mid n$. This contradicts the fact that $p \mid n^2 + 1$. We conclude that p is not irreducible. Let π be an irreducible factor of p. Then we must have $N(\pi) = p$, and it is easy to see that $\overline{\pi} \mid p$ as well, and $N(\overline{\pi}) = p$. By considering norms, we conclude that $p \sim \pi\overline{\pi}$. Since p and $\pi\overline{\pi}$ are both positive real numbers and the only units of $\mathbb{Z}[i]$ are $\pm 1, \pm i$, we conclude that $p = \pi\overline{\pi}$ as desired. □

As a corollary of the proof, we obtain a famous result of Fermat:

COROLLARY 1.5. *Let p be an odd prime. Then $p = a^2 + b^2$ for some integers a, b if and only if $p \equiv 1 \pmod 4$.*

Using this result, together with the fact that $N(xy) = N(x)N(y)$, it is straightforward to deduce:

COROLLARY 1.6. *Let n be a positive integer. Then $n = a^2 + b^2$ for some integers a, b if and only if all prime divisors of n which are*

congruent to 3 (mod 4) *occur with even exponent in the factorization of* n.

1.5. Kummer and Fermat's Last Theorem. In this section, we give a brief glimpse of how the ideas discussed so far can be used to try to tackle Fermat's Last Theorem.

Let $p \geq 5$ be a prime number, and let ζ be a primitive pth root of unity. Is is a standard result from algebra that the minimal polynomial for ζ over $\mathbb{Q}$ is $\Phi_p(X) = X^{p-1} + X^{p-2} + \cdots + X + 1$. (The point here is that $\Phi_p(X)$ is irreducible; this follows, for example, from *Eisenstein's Criterion*.) Thus the set $\{1, \zeta, \zeta^2, \ldots, \zeta^{p-2}\}$ forms a basis for $\mathbb{Q}(\zeta)$ as a vector space over $\mathbb{Q}$.

Since $X^p - 1 = (X-1)(X-\zeta)\cdots(X-\zeta^{p-1})$, we have (substituting $-x/y$ for X, multiplying out the -1's, and clearing denominators)

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

So in the ring

$$\mathbb{Z}[\zeta] := \{a_0 + a_1\zeta + \cdots + a_{p-2}\zeta^{p-2} \ : \ a_i \in \mathbb{Z} \text{ for } i = 0, \ldots, p-2\},$$

with $\zeta^{p-1} = -(1 + \zeta + \cdots + \zeta^{p-2})$, the equation $x^p + y^p = z^p$ becomes

$$z^p = (x+y)(x+y\zeta)\cdots(x+y\zeta^{p-1}). \tag{1.1}$$

Suppose x, y, z are nonzero integers with $p \nmid xyz$ (this is called the "first case" of Fermat's Last Theorem). Then it is not hard to prove that the terms on the right-hand side of (1.1) are relatively prime in $\mathbb{Z}[\zeta]$. (Try this as an exercise.) Therefore, if $\mathbb{Z}[\zeta]$ were a UFD, we could conclude that $x + y\zeta = u\alpha^p$ for some $u, \alpha \in \mathbb{Z}[\zeta]$ with u a unit.

Suppose we knew further that $u = \pm\zeta^j$ for some $j \in \mathbb{Z}$. (Such elements of $\mathbb{Z}[\zeta]$ are clearly units, although we have no reason to believe that all units are of this form.) Then writing $\alpha = a_0 + a_1\zeta + \cdots + a_{p-2}\zeta^{p-2}$ with all a_i's in $\mathbb{Z}$, it follows by the binomial theorem and Fermat's little theorem that $\alpha^p \equiv a_0 + a_1 + \cdots + a_{p-2} \pmod{p}$. In particular, $\alpha^p \equiv a \pmod{p}$ for some $a \in \mathbb{Z}$. But then we would have $x + y\zeta \equiv \pm a\zeta^j \pmod{p}$ for some $0 \leq j \leq p-1$. Comparing powers of ζ on both sides, and using the relation $\zeta^{p-1} = -(1 + \zeta + \cdots + \zeta^{p-2})$, it follows from the assumption $p \geq 5$ that $xy \equiv 0 \pmod{p}$, a contradiction.

This is the starting point for the strategy used by Kummer to try to tackle Fermat's Last Theorem. However, Kummer realized that $\mathbb{Z}[\zeta]$ is hardly ever a UFD. (In fact, it turns out that $\mathbb{Z}[\zeta]$ is a UFD if and only if $p \leq 19$, but that wasn't proved until long after Kummer's time!) Moreover, when $p \geq 5$ there are always infinitely many units in

$\mathbb{Z}[\zeta]$. So the above strategy has a very small (in fact, empty) range of applicability!

Nonetheless, Kummer was able to make a lot of progress towards resolving Fermat's Last Theorem by suitably modifying this argument. First of all, he realized that even though unique factorization of elements into irreducibles often fails in $\mathbb{Z}[\zeta]$, a weaker property always holds: every *ideal* factors uniquely into a product of *prime ideals*. This discovery was really the birth of modern algebraic number theory. Kummer then initiated a careful study of the discrepancy between *ideals* of $\mathbb{Z}[\zeta]$ and *elements* of $\mathbb{Z}[\zeta]$. This involves studying the so-called *ideal class group*, as well as the *unit group*, of the number ring $\mathbb{Z}[\zeta]$. In this way, Kummer was able to sufficiently understand the units, and to recover enough of a fragment of the unique factorization property in $\mathbb{Z}[\zeta]$, to show that Fermat's Last Theorem holds for what are now called "regular primes". We will discuss all of this in more detail later in the course. In fact, it can be fairly said that understanding the ideal class group and unit group of a number ring is our primary objective in this class.

2. Rings of integers, Dedekind domains, and unique factorization of ideals

A *number field* is a field K which is a finite extension of $\mathbb{Q}$. An *algebraic number* is an element of a number field K, i.e., a root of some nonzero polynomial with rational coefficients.

We want to define what it means for an algebraic number α to be an *algebraic integer*. In particular, we will see that if K is a number field, then there is a natural subring of K called the *ring of integers* of K which consists of all algebraic integers lying in K. For example, the ring of integers in $\mathbb{Q}(i)$ is just $\mathbb{Z}[i]$. Rings of integers in number fields will be the fundamental object of study in this course.

2.1. Integral Dependence. Let A and B be rings with $A \subseteq B$. We say that an element $x \in B$ is *integral* over A if it is a root of a *monic* polynomial with coefficients in A. In other words, x is integral if it satisfies a relation of the form

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

with all a_i's in A.

It is clear that every element of A is integral over A, since $a \in A$ satisfies the relation $x - a = 0$.

We say that B is integral over A if every element of B is integral over A.

This notion of integrality is a generalization of the relationship between $\mathbb{Z}$ and $\mathbb{Q}$. In fact, we claim that $x \in \mathbb{Q}$ is integral over $\mathbb{Z}$ if and only if $x \in \mathbb{Z}$. To see this, write $x = r/s$ where $r, s \in \mathbb{Z}$ and $(r, s) = 1$. If

$$(r/s)^n + a_{n-1}(r/s)^{n-1} + \cdots + a_1(r/s) + a_0 = 0$$

with $a_i \in \mathbb{Z}$, then clearing denominators gives

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

Therefore $s \mid r^n$, which implies that $s = \pm 1$ and therefore $x \in \mathbb{Z}$.

More generally, we define an *algebraic integer* to be an algebraic number which is integral over $\mathbb{Z}$. In other words, if K is a number field, then the algebraic integers (or just integers, for brevity) in K are the elements which are roots of monic polynomials with coefficients in $\mathbb{Z}$.

Note that it is not obvious that the sum or product of two algebraic integers is again an algebraic integer. However, this is true! More generally, we will prove that the set of elements of a ring B which are integral over A forms a subring of B. The most convenient way to do this is to use modules.

Recall that an A-module M is just an abelian group M together with an action of A on M satisfying certain natural axioms generalizing those of a vector space. We say that M is a *finitely generated* A-module (or that M is finitely generated over A) if there exist $m_1, \ldots, m_r \in M$ such that every element $m \in M$ can be written as $m = a_1 m_1 + \cdots + a_r m_r$ for some $a_1, \ldots, a_r \in A$. In this case, we say that the elements $m_1, \ldots, m_r$ *generate* M as an A-module. Note that we do not require that the set of generators is unique, nor do we require that the representation of m as a linear combination of the generators is unique.

It follows from the definitions that a module M is finitely generated as a $\mathbb{Z}$-module if and only if it is finitely generated as an additive group.

The notion of being finitely generated is transitive:

LEMMA 1.7. *Let M be a B-module and let $B \supseteq A$ be a ring. Suppose that M is finitely generated as a B-module and that B is finitely generated as an A-module. Then M is finitely generated as an A-module.*

PROOF. Let $x_1, \ldots, x_m$ (resp. $y_1, \ldots, y_n$) denote a set of generators for M as a B-module (resp. for B as an A-module). Then we claim that the set of products $x_i y_j$ generates M as an A-module. To see this,

let $x \in M$, and write $x = \sum_i b_i x_i$ with $b_i \in B$. Also, for each i, write $b_i = \sum_j a_{ij} y_j$ with $a_{ij} \in A$. Then

$$x = \sum_i (\sum_j a_{ij} y_j) x_i = \sum_{i,j} a_{ij} x_i y_j,$$

so that x is a linear combination over A of the $x_i y_j$'s. □

If $x \in B$, we denote by $A[x]$ the smallest subring of B containing both A and x. In other words,

$$A[x] := \{a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0 \ : \ n \in \mathbb{N} \text{ and } a_i \in A \text{ for all } i\}$$

is the set of all polynomials in x with coefficients in A.

Under what conditions will $A[x]$ be finitely generated as an A-module? In other words, how do we determine whether or not we need to look at polynomials in x of arbitrarily large degree to obtain all of $A[x]$? The answer is closely related to integrality. To see this, we need a lemma concerning determinants of matrices over an arbitrary ring.

LEMMA 1.8. *Let B be a ring, and let M be an B-module. If $T = (a_{ij})$ is an $n \times n$ matrix with coefficients $a_{ij} \in B$, and if $Tv = 0$ for some vector v with coefficients in M, then $(\det T)v = 0$.*

PROOF. (Sketch) The key point is that if $\mathrm{adj}(T) = (b_{ij})$ is the $n \times n$ matrix whose ij^{th} entry is $(-1)^{i+j}$ times the determinant of the ji^{th} minor of T, then the identity $\mathrm{adj}(T) \cdot T = (\det T)I$ holds, where I is the $n \times n$ identity matrix. (The ji^{th} minor of T is the $(n-1) \times (n-1)$ matrix obtained by deleting the jth row and ith column from T.) You have probably seen this formula before in the context of linear algebra; this identity is valid in any ring B, and the proof is the same as the proof from linear algebra.

Given this formula, the proof of the lemma is immediate: multiply the given equation $Tv = 0$ on both sides by $\mathrm{adj}(T)$ to obtain $(\det T)v = 0$. □

THEOREM 1.9. *Let $A \subseteq B$ be rings, and let $x \in B$. The following are equivalent:*

(i) *x is integral over A*
(ii) *$A[x]$ is a finitely generated A-module*
(iii) *$A[x]$ is contained in a subring of B which is finitely generated as an A-module.*

(Note that (i) and (iii) imply (ii).)

PROOF. (i) $\Rightarrow$ (ii): If x is integral over A, then $x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 = 0$ with $a_i \in A$ for all i, so $x^n = -(a_{n-1}x^{n-1} + \cdots + a_1 x + a_0)$. It follows that $A[x]$ is generated as an A-module by $1, x, x^2, \ldots, x^{n-1}$.

(ii) $\Rightarrow$ (iii) is obvious.

(iii) $\Rightarrow$ (i): This is the trickiest direction. Suppose $A[x] \subseteq C$ with C a subring of B that is finitely generated over A. We want to show that x satisfies a monic polynomial with coefficients in A. To see this, first note that since C is a ring, we have $xC \subset C$, i.e., whenever $y \in C$ we have $xy \in C$ as well. Let $y_1, \ldots, y_n$ generate C as an A-module. If we express each product xy_i as a linear combination of the y_i's, we obtain $xy_i = \sum_j a_{ij} y_j$ for some elements $a_{ij} \in A$, $1 \leq i, j \leq n$. We can encode the a_{ij}'s in an $n \times n$ matrix T with coefficients in A, so that

$$\begin{bmatrix} xy_1 \\ \vdots \\ xy_n \end{bmatrix} = T \begin{bmatrix} y_1 \\ \vdots \\ y_n \end{bmatrix}.$$

This is equivalent to saying that

$$(xI - T) \begin{bmatrix} y_1 \\ \vdots \\ y_n \end{bmatrix} = 0,$$

where I is the $n \times n$ identity matrix and $(xI - T)$ is viewed as a matrix with coefficient in B. Since 1 is a linear combination of the y_i's, it follows from Lemma 1.8 that $\det(xI - T) = 0$. Expanding this determinant in terms of the entries of $xI - T$, we see that

$$\det(xI - T) = x^n + Q(x),$$

where $Q(x)$ is a polynomial of degree at most $n-1$ having coefficients in A. So x satisfies a monic polynomial of degree n with coefficients in A, and is therefore integral over A. □

COROLLARY 1.10 (Transitivity of integrality). *If C is integral over B and B is integral over A, then C is integral over A.*

PROOF. This follows easily from Lemma 1.7 and Theorem 1.9. □

COROLLARY 1.11. *If $x, y \in B$ are integral over A, then so are $x \pm y$ and xy. Therefore the set of elements of B which are integral over A forms a ring.*

PROOF. Since x is integral over A, it follows from Theorem 1.9 that $A[x]$ is finitely generated as an A-module. Since y is integral over A, it is in particular integral over $A[x]$, so that $A[x, y] = (A[x])[y]$ is finitely generated over $A[x]$. By Lemma 1.7, it follows that the ring $A[x, y]$

is finitely generated as an A-module. By Theorem 1.9, every element of $A[x, y]$ is therefore integral over A. In particular, $x \pm y$ and xy are integral over A. □

In particular, let K be a number field, and let $\mathcal{O}_K$ be the set of all algebraic integers in K. Then $\mathcal{O}_K$ is a subring of K. By definition, a *number ring* is a ring of the form $\mathcal{O}_K$ for some number field K.

2.2. Examples of number rings. To recognize whether a given element α of a number field K is integral (i.e., is an element of $\mathcal{O}_K$), one can use the following lemma. Recall, for the statement, that if L/K is an algebraic field extension and $\alpha \in L$, then the *minimal polynomial* of α over K is the unique monic polynomial f_α of minimal degree among all nonzero polynomials $f \in K[x]$ with $f(\alpha) = 0$. If $g \in K[x]$ is any nonzero polynomial with $g(\alpha) = 0$, then $f_\alpha \mid g$.

LEMMA 1.12. *Let α be an algebraic number, and let $f_\alpha(x) \in \mathbb{Q}[x]$ be its minimal polynomial. Then α is an algebraic integer if and only if $f_\alpha \in \mathbb{Z}[x]$.*

PROOF. One direction is obvious: if $f_\alpha \in \mathbb{Z}[x]$ then clearly α is an algebraic integer.

Now suppose α is an algebraic integer, and let $\alpha_1, \ldots, \alpha_n$ be the roots of f_α. Since α is integral over $\mathbb{Z}$, there exists a monic polynomial $h(x) \in \mathbb{Z}[x]$ with $h(\alpha) = 0$. Since $f_\alpha \mid h$, we must have $h(\alpha_i) = 0$ for all i. Therefore all of the roots of f_α are algebraic integers. Since f_α is monic, the coefficients of f_α are the elementary symmetric polynomials in the α_i's. In particular (since the set of all algebraic integers forms a ring), the coefficients of f_α are all algebraic integers. But they are also in $\mathbb{Q}$, and we have already seen that the set of algebraic integers which lie in $\mathbb{Q}$ is just $\mathbb{Z}$. Therefore $f_\alpha \in \mathbb{Z}[x]$ as desired. □

One can use the lemma to prove the following useful result:

EXERCISE 1.13. Let d be a squarefree integer. Then the ring of integers $\mathcal{O}_K$ in $K = \mathbb{Q}(\sqrt{d})$ is:

$$\begin{array}{ll} \mathbb{Z}[\sqrt{d}] & \text{if } d \equiv 2, 3 \pmod 4 \\ \mathbb{Z}[\frac{1+\sqrt{d}}{2}] & \text{if } d \equiv 1 \pmod 4. \end{array}$$

It is very important to remember that $\mathcal{O}_K$ can be strictly larger than $\mathbb{Z}[\sqrt{d}]$. A concrete example is that if $\omega = \frac{1+\sqrt{-3}}{2}$, then ω is not in $\mathbb{Z}[\sqrt{-3}]$, but ω is integral, because it satisfies the equation $x^2+x+1 = 0$.

It follows from Proposition 1.13 that if K is a quadratic field (which is common parlance for "K is a number field of degree 2 over $\mathbb{Q}$"), then

$\mathcal{O}_K$ is a free abelian group of rank 2. We will see soon that an analogous fact holds for the ring of integers in an arbitrary number field.

2.3. $\mathcal{O}_K$ is integrally closed. We begin with a simple lemma.

LEMMA 1.14. *Let α be an algebraic number. Then there exists a nonzero integer $m \in \mathbb{Z}$ such that $m\alpha$ is an algebraic integer.*

PROOF. Let $f(x) = a_n x^n + \cdots + a_1 x + a_0 \in \mathbb{Z}[x]$, $a_n \neq 0$, be a polynomial with integer coefficients which is satisfied by α. Then $a_n \cdot \alpha$ is a root of the monic polynomial

$$x^n + a_{n-1}x^{n-1} + \cdots + a_n^{n-2}a_1 x + a_n^{n-1}a_0 \in \mathbb{Z}[x] \ ,$$

and is therefore an algebraic integer. We may thus take $m = a_n$. □

Recall that if A is an integral domain, its *field of fractions* L is the smallest field containing A. Concretely, we have

$$L = \{\frac{x}{y} \ : \ x, y \in A, y \neq 0\}$$

endowed with the usual laws of addition and multiplication for fractions.

COROLLARY 1.15. *If K is a number field, then K is the field of fractions of $\mathcal{O}_K$.*

PROOF. Let L be the field of fractions of $\mathcal{O}_K$. Clearly $L \subseteq K$. On the other hand, if $\alpha \in K$, then $m\alpha = \beta \in \mathcal{O}_K$ for some nonzero integer m, and therefore $\alpha = \frac{\beta}{m}$ is in L. □

A domain R with field of fractions K is called *integrally closed* if whenever $\alpha \in K$ is integral over R, we have $\alpha \in R$.

LEMMA 1.16. *If K is a number field, then $\mathcal{O}_K$ is integrally closed.*

PROOF. Suppose $\alpha \in K$ is integral over $\mathcal{O}_K$. By definition, $\mathcal{O}_K$ is integral over $\mathbb{Z}$, and since integrality is transitive, it follows that α is integral over $\mathbb{Z}$, and therefore $\alpha \in \mathcal{O}_K$. □

2.4. Ideals of number rings and lattices. In this section, we prove the important fact that if K is a number field and $\mathcal{O}_K$ is its ring of integers, then $\mathcal{O}_K$ is a *lattice* in K. More generally, we show that any ideal I of $\mathcal{O}_K$ is a lattice in K, and we deduce from this that the quotient ring $\mathcal{O}_K/I$ is finite.

Let k be either the field $\mathbb{Q}$ of rational numbers or the field $\mathbb{R}$ of real numbers. Recall that a *complete lattice* in a finite-dimensional vector space V over k is an additive subgroup of V which is *discrete*

and *spans* V. (A subset $\Lambda \subseteq V$ is discrete if every bounded subset of V contains only finitely many points of Λ.) If $\dim_k(V) = n$, then a discrete additive subgroup Λ of V will span some subspace W of V; if $\dim_k(W) = m \leq n$, we say that Λ is a *lattice of rank* m in V.

Convention: When we say that Λ is a lattice in V, without specifying the rank, we will mean (unless otherwise noted) that Λ is a *complete lattice*.

PROPOSITION 1.17. *Let V be a finite dimensional k-vector space, and suppose $\Lambda \subseteq V$ is a $\mathbb{Z}$-module which spans V. Let $n = \dim_k(V)$. Then the following are equivalent:*

(i) *Λ is discrete.*
(ii) *Λ is generated by n elements.*
(iii) *$\Lambda \cong \mathbb{Z}^n$ as $\mathbb{Z}$-modules.*

PROOF. The equivalence of (ii) and (iii) is a consequence of the structure theorem for finitely generated abelian groups, since $\Lambda \subseteq V$ implies that Λ is torsion-free. We therefore focus on proving that (i) is equivalent to (ii).

If Λ is free, let $x_1, \ldots, x_n$ be a basis. Then every point of V can be written uniquely as $\sum \lambda_i x_i$ with $\lambda_i \in k$. Since the open neighborhood $\{\sum \lambda_i x_i \ : \ |\lambda_i| < 1 \ \forall \ i\}$ of 0 contains no non-zero element of Λ, it follows easily that Λ is discrete.

Conversely, suppose that Λ is discrete. Let $x_1, \ldots, x_n$ be elements of Λ which form a basis for V, and let Λ_0 be the $\mathbb{Z}$-module spanned by $x_1, \ldots, x_n$. Since Λ is discrete, there exists an integer $M > 0$ such that if $x = \sum \lambda_i x_i \in \Lambda$ with all $|\lambda_i| < 1/M$, then $x = 0$. Let $y_1, y_2, \ldots$ be coset representatives for Λ/Λ_0. Without loss of generality each y_i can be chosen to lie in the cube

$$C = \{x = \sum \lambda_i x_i \ : \ 0 \leq \lambda_i < 1 \ \forall \ i\} \ .$$

Cover C by M^n boxes of the form $\frac{m_i}{M} \leq \lambda_i < \frac{m_i+1}{M}$ with $m_i \in \mathbb{Z}$ and $0 \leq m_i < M$. Then $|\Lambda/\Lambda_0| \leq M^n$, or else some distinct elements y_i and y_j would lie in the same box, implying that

$$y_i - y_j \in \Lambda \cap \{\sum \lambda_i x_i \ : \ |\lambda_i| < \frac{1}{M} \ \forall \ i\} = \{0\} \ ,$$

a contradiction. Now we're done, since Λ is generated by the x_i's and the finitely many y_j's. □

For the proof of the next result, we recall the notion of *norm* for field extensions. Let $\sigma_1, \ldots, \sigma_n$ be the n distinct embeddings of a number

field K into $\mathbb{C}$, and define the norm $N_{K/\mathbb{Q}}(\gamma)$ of an element $\gamma \in K$ by the formula

$$N_{K/\mathbb{Q}}(\gamma) = \prod_i \sigma_i(\gamma) \ .$$

By field theory, we have $N_{K/\mathbb{Q}}(\gamma) \in \mathbb{Q}$, and $N_{K/\mathbb{Q}}(\gamma) = 0$ iff $\gamma = 0$. Moreover, if γ is an algebraic integer then so is $\sigma_i(\gamma)$ for each i, and therefore $N_{K/\mathbb{Q}}(\gamma) \in \mathbb{Z}$, since an algebraic integer which is also a rational number must be an (ordinary) integer.

THEOREM 1.18. *If a number field K having degree n over $\mathbb{Q}$ is identified with the vector space $\mathbb{Q}^n$, then $\mathcal{O}_K$ is a lattice in K.*

PROOF. By Lemma 1.14, there exists a basis $\alpha_1, \ldots, \alpha_n$ for $K/\mathbb{Q}$ with $\alpha_i \in \mathcal{O}_K$ for each i. Suppose $\mathcal{O}_K$ is not discrete in K. Then there are arbitrarily small $\lambda_1, \ldots, \lambda_n \in \mathbb{Q}$ such that $\alpha = \sum \lambda_i \alpha_i$ is nonzero and in $\mathcal{O}_K$. Since $\sigma(\alpha) = \sum \lambda_i \sigma(\alpha_i)$ for each embedding σ of K into $\mathbb{C}$, it follows that $N_{K/\mathbb{Q}}(\alpha) = \phi(\lambda_1, \ldots, \lambda_n)$ for some homogeneous polynomial $\phi \in \mathbb{C}[x_1, \ldots, x_n]$ of degree n. Therefore $|\phi(\lambda_1, \ldots, \lambda_n)| < 1$ if the $|\lambda_i|$ are sufficiently small. But $N_{K/\mathbb{Q}}(\alpha)$ is a nonzero integer, a contradiction. □

COROLLARY 1.19. *If I is a nonzero ideal of $\mathcal{O}_K$, then I is a sublattice of $\mathcal{O}_K$ in K.*

PROOF. Since I is a $\mathbb{Z}$-submodule of $\mathcal{O}_K$, it is discrete. Also, I contains a basis for K, since if $\alpha_1, \ldots, \alpha_n$ is a basis for K contained in $\mathcal{O}_K$, then $c\alpha_1, \ldots, c\alpha_n$ is a basis for K contained in I for any nonzero element $c \in I \cap \mathbb{Z}$. (To see that $I \cap \mathbb{Z} \neq (0)$, note for example that $N_{K/\mathbb{Q}}(\alpha) \in I \cap \mathbb{Z}$ for any nonzero element $\alpha \in I$.) Thus I is a sublattice of $\mathcal{O}_K$. □

From this, we deduce the following important result:

PROPOSITION 1.20. *If $\mathcal{O}_K$ is a number ring and I is a nonzero ideal in $\mathcal{O}_K$, then the quotient ring $\mathcal{O}_K/I$ is finite.*

PROOF. Since I is a sublattice of $\mathcal{O}_K$, we know from Proposition 1.17 that both $\mathcal{O}_K$ and I are isomorphic to $\mathbb{Z}^n$ as abelian groups. By Theorem A.11, it follows that I has finite index in $\mathcal{O}_K$. □

2.5. $\mathcal{O}_K$ is Noetherian. Recall that a ring R is called *Noetherian* if every ideal of R is finitely generated.

LEMMA 1.21. *Let R be a ring. Then the following are all equivalent to the condition that R is Noetherian:*

(i) *Every ideal of R is finitely generated.*

(ii) *If* $I_0 \subseteq I_1 \subseteq I_2 \subseteq \cdots$ *is an increasing chain of ideals in* R*, then there exists* n_0 *such that* $I_n = I_{n_0}$ *for* $n \geq n_0$*.*

(iii) *Every non-empty set* Σ *of ideals of* R *has a maximal element.*

PROOF. (i) implies (ii): Set $I = \cup_{n=0}^{\infty} I_n$; this is an ideal of R, hence is finitely generated. The generators all lie in some I_{n_0}, and therefore $I_n = I_{n_0}$ for all $n \geq n_0$.

(ii) implies (iii): If no such maximal element exists, then there must be an infinite chain $I_0 \subsetneq I_1 \subsetneq I_2 \subsetneq \cdots$ with each containment *proper*, contradicting (ii).

(iii) implies (i): For any ideal I of R, let Σ_I be the set of finitely generated ideals contained in I. Since $(0) \in \Sigma_I$, we have $\Sigma_I \neq \emptyset$. Therefore Σ_I has a maximal element I'. Suppose $I' \neq I$, let $x \in I \backslash I'$, and define $I'' = (I', x)$. Then $I'' \in \Sigma_I$ and $I' \subsetneq I''$, contradicting the maximality of I'. Therefore $I = I'$ and I is finitely generated. □

From Proposition 1.20, we deduce:

COROLLARY 1.22. *$\mathcal{O}_K$ is a Noetherian ring.*

PROOF. Let $I = I_0 \subseteq I_1 \subseteq I_2 \subseteq \cdots$ be an ascending chain of ideals in $\mathcal{O}_K$, and assume without loss of generality that $I_0 \neq 0$. By Proposition 1.20, the quotient $\mathcal{O}_K/I$ is finite. Therefore there are only finitely many ideals of $\mathcal{O}_K$ which contain I, and in particular the chain $I = I_0 \subseteq I_1 \subseteq I_2 \subseteq \cdots$ must stabilize. By Lemma 1.21, it follows that $\mathcal{O}_K$ is Noetherian. □

2.6. $\mathcal{O}_K$ has dimension 1. Let R be a ring. The (Krull) *dimension* of R is the supremum of all integers $n \geq 0$ such that there exists a chain

$$\mathfrak{p}_0 \subsetneq \mathfrak{p}_1 \subsetneq \mathfrak{p}_2 \subsetneq \cdots \subsetneq \mathfrak{p}_n$$

of prime ideals in R.

If R is an integral domain, then (0) is a prime ideal, and we have the following straightforward lemma, whose proof is left to the reader:

LEMMA 1.23. *Let R be an integral domain. Then* $\dim(R) = 0$ *iff R is a field, and* $\dim(R) \leq 1$ *iff every nonzero prime ideal of R is maximal.*

As another corollary of Proposition 1.20, we deduce:

COROLLARY 1.24. *If K is a number field, then $\mathcal{O}_K$ has dimension 1.*

PROOF. Clearly $\mathcal{O}_K$ is not a field, since $\mathcal{O}_K \cap \mathbb{Q} = \mathbb{Z}$. By Lemma 1.23, it suffices to prove that if $\mathfrak{p}$ is a nonzero prime ideal of $\mathcal{O}_K$, then $\mathcal{O}_K/\mathfrak{p}$

is a field. Since $\mathcal{O}_K/\mathfrak{p}$ is an integral domain, and is finite by Proposition 1.20, the desired result follows from the well-known fact that every finite integral domain is a field. □

2.7. Dedekind rings and Unique Factorization of Ideals. A *Dedekind ring* is a ring R satisfying the following four properties:

(1) R is an integral domain.
(2) R is Noetherian.
(3) R is integrally closed.
(4) R is 1-dimensional.

The results of the previous sections imply:

THEOREM 1.25. *If K is a number field, then $\mathcal{O}_K$ is a Dedekind ring.*

EXERCISE 1.26. Show that a PID which is not a field is a Dedekind ring.

Recall that the *product* of two ideals I, J in a ring R is defined as the smallest ideal containing all products xy with $x \in I$ and $y \in J$. If $I = (a_1, \ldots, a_m)$ and $J = (b_1, \ldots, b_n)$ are finitely generated ideals, then the product ideal IJ is generated by the products of the generators for I and J:

$$IJ = (a_i b_j \mid 1 \leq i \leq m, 1 \leq j \leq n) \ .$$

An ideal of R is called *proper* if it is not the zero ideal or the unit ideal.

We will say that a ring R admits *unique factorization of ideals* (UFI) if every proper ideal can be written uniquely as a product of prime ideals. (The uniqueness is only up to the order of the factors, of course.)

The following result is one of the most important theorems in Algebraic Number Theory, and its proof will occupy the rest of this section. It will enable us to bypass the unfortunate fact that we don't always have unique factorization of elements into irreducibles in a number ring.

THEOREM 1.27. *If R is a Dedekind ring, then R admits unique factorization of ideals.*

REMARK 1.28. Conversely, it can be shown that if R is an integral domain which admits unique factorization of ideals, then R is a Dedekind ring.

EXERCISE 1.29. Prove that $\mathbb{Z}[\sqrt{-3}]$ is not a Dedekind domain, and does not admit unique factorization of ideals.

As an illustrative example, consider the ring $R = \mathbb{Z}[\sqrt{-5}]$. We have two distinct factorizations of the element 6 into irreducibles in this ring:

$$6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5}) \ . \tag{1.2}$$

EXERCISE 1.30. Show that $2, 3, 1 \pm \sqrt{-5}$ are all irreducible and mutually non-associate. [**Hint:** Use the fact that the *norm function* defined by $N(x + y\sqrt{-5}) = x^2 + 5y^2$ is multiplicative.]

In particular, $\mathbb{Z}[\sqrt{-5}]$ is neither a PID nor a UFD.

Although $2, 3, 1 \pm \sqrt{-5}$ are all irreducible, they do not generate prime ideals. If we look on the level of ideals, then there is further splitting of the above factorizations of 6. In fact, if we let $\mathfrak{p}_1 = (2, 1 + \sqrt{-5}), \mathfrak{p}_2 = (2, 1 - \sqrt{-5}), \mathfrak{p}_3 = (3, 1 + \sqrt{-5}), \mathfrak{p}_4 = (3, 1 - \sqrt{-5})$, then:

EXERCISE 1.31. (i) $\mathfrak{p}_1, \ldots, \mathfrak{p}_4$ are all prime ideals of $\mathbb{Z}[\sqrt{-5}]$.
(ii) $(2) = \mathfrak{p}_1\mathfrak{p}_2, (3) = \mathfrak{p}_3\mathfrak{p}_4, (1 + \sqrt{-5}) = \mathfrak{p}_1\mathfrak{p}_3$, and $(1 - \sqrt{-5}) = \mathfrak{p}_2\mathfrak{p}_4$.

So there is no failure of unique factorization on the level of ideals: in terms of prime ideals, equation (1.2) becomes

$$(6) = (2) \cdot (3) = (\mathfrak{p}_1\mathfrak{p}_2)(\mathfrak{p}_3\mathfrak{p}_4) = (\mathfrak{p}_1\mathfrak{p}_3)(\mathfrak{p}_2\mathfrak{p}_4) = (1 + \sqrt{-5})(1 - \sqrt{-5}).$$

Note also that using ideals rather than elements lets us avoid having to deal with units in the statement of the unique factorization property!

We now begin preparing for the proof of Theorem 1.27. The first thing we will need are some lemmas about Noetherian rings and prime ideals.

LEMMA 1.32. *Suppose $I_1, \ldots, I_n$ are ideals of R and that $\mathfrak{p}$ is a prime ideal of R. If $I_1 \cdots I_n \subseteq \mathfrak{p}$, then $I_j \subseteq \mathfrak{p}$ for some j.*

PROOF. Suppose that for each j there exists $\alpha_j \in I_j$ which is not in $\mathfrak{p}$. Then $\alpha_1 \cdots \alpha_n \in I_1 \cdots I_n \subseteq \mathfrak{p}$, so $\alpha_1 \cdots \alpha_n \in \mathfrak{p}$. As $\mathfrak{p}$ is a prime ideal, we must have $\alpha_j \in \mathfrak{p}$ for some j, a contradiction. □

LEMMA 1.33. *If I is a nonzero ideal in a noetherian ring R, then there exist nonzero prime ideals $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ of R such that $\mathfrak{p}_1 \cdots \mathfrak{p}_r \subseteq I$.*

PROOF. Let Σ be the set of all ideals for which the conclusion of the lemma fails. If $\Sigma \neq \emptyset$, then since R is Noetherian, Σ has a maximal element J. Clearly J cannot be prime, so there exist $a, b \in R$ such that $ab \in J$ but $a, b \notin J$. Let $\mathfrak{a} := (J, a), \mathfrak{b} := (J, b)$. Then $\mathfrak{a} \supsetneq J$ and $\mathfrak{b} \supsetneq J$, so by maximality of J,

$$\mathfrak{a} \supseteq \mathfrak{p}_1 \cdots \mathfrak{p}_m, \ \mathfrak{b} \supseteq \mathfrak{q}_1 \cdots \mathfrak{q}_n,$$

where $\mathfrak{p}_i, \mathfrak{q}_j$ are nonzero prime ideals. Since $\mathfrak{ab} = (J^2, aJ, bJ, ab) \subseteq J$, it follows that $\mathfrak{p}_1 \cdots \mathfrak{p}_m \mathfrak{q}_1 \cdots \mathfrak{q}_n \subseteq J$, a contradiction. Therefore $\Sigma = \emptyset$ and the lemma is true. □

Let R be an integral domain with fraction field K, and suppose I is a nonzero ideal of R. We define I^{-1} to be

$$I^{-1} := \{x \in K \ : \ xI \subseteq R\},$$

considered as an R-submodule of K. Note that $R \subseteq I^{-1}$, and that if $I = (a)$ is principal, then $I^{-1} = Ra^{-1}$.

Note also that we can multiply two R-submodules M and N of K by defining their product MN to be the R-submodule of K generated by all products of the form xy with $x \in M$ and $y \in N$. If M, N are ideals of R, this coincides with the usual ideal-theoretic product.

Exercise 1.34. If M, M', N are R-submodules of K with $M \subseteq M'$, show that $MN \subseteq M'N$.

Proposition 1.35. *Let R be a Dedekind ring, let I be a nonzero ideal of R, and let $\mathfrak{p}$ be a nonzero prime ideal of R. Then $\mathfrak{p}^{-1}I \neq I$.*

Proof. We first consider the special case where $I = R$. In this case, we are trying to show that $\mathfrak{p}^{-1} \neq R$, so we need to find an element $x \in \mathfrak{p}^{-1}$ which is not in R. Recall that by definition, $x \in \mathfrak{p}^{-1}$ if and only if $x\mathfrak{p} \subseteq R$. An idea for finding such an element x is to take $x = a^{-1}b$ for cleverly chosen elements $a, b \in R$ so that $b\mathfrak{p} \subseteq (a)$ (i.e., $a^{-1}b \in \mathfrak{p}^{-1}$) but $b \notin (a)$ (i.e., $a^{-1}b \notin R$). Let $a \in \mathfrak{p}$ be any nonzero element of $\mathfrak{p}$; we will try to then find an appropriate element b which makes our strategy work.

By Lemma 1.33, we know that there exist nonzero prime ideals $\mathfrak{p}_i$ such that $\mathfrak{p}_1\mathfrak{p}_2 \cdots \mathfrak{p}_r \subseteq (a)$. We may assume without loss of generality that $r \geq 1$ is chosen as small as possible. Since $(a) \subseteq \mathfrak{p}$, it follows from Lemma 1.32 that one of the prime ideals $\mathfrak{p}_i$ must be contained in $\mathfrak{p}$. But R is 1-dimensional, so $\mathfrak{p}_i$ is a maximal ideal, and therefore $\mathfrak{p}_i = \mathfrak{p}$. Without loss of generality, we may assume that $i = 1$.

If $r = 1$, we conclude that $\mathfrak{p} = (a)$, and then $\mathfrak{p}^{-1} = Ra^{-1}$ cannot be equal to R (or else a would be a unit and therefore $(a) = (1)$, which is not prime).

Now assume that $r \geq 2$. As $\mathfrak{p}_2 \cdots \mathfrak{p}_r \not\subseteq (a)$ by the minimality of r, it follows that there exists $b \in \mathfrak{p}_2 \cdots \mathfrak{p}_r$ such that $b \notin (a)$. By construction, $b\mathfrak{p} = b\mathfrak{p}_1 \subseteq (a)$. As discussed above, it follows that $x := a^{-1}b$ is in $\mathfrak{p}^{-1} \backslash R$, which proves the proposition in the special case $I = R$.

In general, we can use the fact that R is Noetherian to write $I = (\alpha_1, \ldots, \alpha_n)$. Suppose for the sake of contradiction that $\mathfrak{p}^{-1}I = I$. Then for every $x \in \mathfrak{p}^{-1}$, we can write

$$x\alpha_i = \sum_{j=1}^{n} a_{ij}\alpha_j \tag{1.3}$$

with $a_{ij} \in R$. Let $A = (a_{ij})$, and define $T := xI_n - A$, where I_n is the $n \times n$ identity matrix over the fraction field K of R (which exists since R is an integral domain). Then

$$T \begin{bmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{bmatrix} = 0$$

and therefore (since (1.3) is an equation inside the field K) $\det(T) = 0$. Since $\det(T)$ is a monic polynomial in x with coefficients in R, it follows that x is integral over R. But R is integrally closed, so we must have $x \in R$. This implies that $\mathfrak{p}^{-1} = R$, contradicting the special case which was proved above. □

Corollary 1.36. *Let R be a Dedekind ring, and let $\mathfrak{p}$ be a nonzero prime ideal of R. Then $\mathfrak{p}^{-1}\mathfrak{p} = R$.*

Proof. By definition, we have $x\mathfrak{p} \subseteq R$ for all $x \in \mathfrak{p}^{-1}$. We also have $R \subseteq \mathfrak{p}^{-1}$, so that $\mathfrak{p} \subseteq \mathfrak{p}^{-1}\mathfrak{p} \subseteq R$. Note that $\mathfrak{p}^{-1}\mathfrak{p}$ is an ideal of R, and $\mathfrak{p}^{-1}\mathfrak{p} \neq \mathfrak{p}$ by Proposition 1.35. Since R is 1-dimensional, $\mathfrak{p}$ is a maximal ideal, and therefore we must have $\mathfrak{p}^{-1}\mathfrak{p} = R$ as desired. □

We now come to the proof of the main theorem of this section.

Proof of Theorem 1.27. We need to prove the existence and uniqueness of the factorization. Let's prove uniqueness first. Suppose we have

$$I = \mathfrak{p}_1\mathfrak{p}_2 \cdots \mathfrak{p}_r = \mathfrak{q}_1\mathfrak{q}_2 \cdots \mathfrak{q}_s. \tag{1.4}$$

Then $\mathfrak{q}_1\mathfrak{q}_2 \cdots \mathfrak{q}_s = \mathfrak{p}_1\mathfrak{p}_2 \cdots \mathfrak{p}_r \subseteq \mathfrak{p}_1$. Since $\mathfrak{p}_1$ is prime, we must have $\mathfrak{q}_i \subseteq \mathfrak{p}_1$ for some i by Lemma 1.32. By relabeling if necessary, we may suppose that $\mathfrak{q}_1 \subseteq \mathfrak{p}_1$. Since R is 1-dimensional, $\mathfrak{q}_1$ is maximal, so $\mathfrak{p}_1 = \mathfrak{q}_1$. Multiplying both sides of (1.4) by $\mathfrak{p}_1^{-1}$, we obtain (using Corollary 1.36) $\mathfrak{p}_2 \cdots \mathfrak{p}_r = \mathfrak{q}_2 \cdots \mathfrak{q}_s$. Continuing in this fashion, we find that $r = s$ and (after relabelling if necessary) that $\mathfrak{p}_i = \mathfrak{q}_i$ for all i.

We now prove existence, i.e., that I can be written as a product of prime ideals. The argument will be a very clever use of the noetherian property, together with Proposition 1.35. Let Σ be the set of

all proper ideals of R which cannot be written as a product of prime ideals. Suppose for the sake of contradiction that $\Sigma \neq \emptyset$. Then since R is Noetherian, there exists a maximal element J of Σ. The ideal J must be contained in a maximal ideal $\mathfrak{p}$, and the inclusion $R \subseteq \mathfrak{p}^{-1}$ gives us

$$J \subseteq J\mathfrak{p}^{-1} \subseteq \mathfrak{p}\mathfrak{p}^{-1} = R.$$

By the maximality of J, together with Proposition 1.35 (which guarantees that $J \neq J\mathfrak{p}^{-1}$), it follows that $J\mathfrak{p}^{-1} = \mathfrak{p}_1 \cdots \mathfrak{p}_r$ for some nonzero prime ideals $\mathfrak{p}_i$. Multiplying both sides of this equation by $\mathfrak{p}$, we find using Corollary 1.36 that $J = \mathfrak{p}_1 \cdots \mathfrak{p}_r\mathfrak{p}$ is a product of prime ideals, a contradiction. We conclude that the set Σ must be empty, which is what we wanted to prove. □

As an application of Theorem 1.27, the reader might wish to try the following exercise:

EXERCISE 1.37. A Dedekind ring is a UFD if and only if it is a PID.

We conclude this section with a couple of simple but important applications of Theorem 1.27.

EXERCISE 1.38. Let I be a nonzero ideal in a Dedekind ring R with factorization $I = \mathfrak{p}_1 \cdots \mathfrak{p}_r$ into prime ideals. Then:

(a) $I^{-1} = \mathfrak{p}_1^{-1} \cdots \mathfrak{p}_r^{-1}$.
(b) $II^{-1} = R$.

Let R be a ring. If $\mathfrak{a}$ and $\mathfrak{b}$ are ideals of R, we say that $\mathfrak{a}$ *divides* $\mathfrak{b}$ (written $\mathfrak{a} \mid \mathfrak{b}$) if there exists an ideal $\mathfrak{c}$ of R such that $\mathfrak{b} = \mathfrak{a}\mathfrak{c}$.

LEMMA 1.39. *If R is a Dedekind ring and $\mathfrak{a}, \mathfrak{b}$ are ideals, then $\mathfrak{a} \mid \mathfrak{b}$ if and only if $\mathfrak{a} \supseteq \mathfrak{b}$. In other words, in a Dedekind ring:*

TO CONTAIN IS TO DIVIDE.

PROOF. If $\mathfrak{a} \supseteq \mathfrak{b}$, then $\mathfrak{c} := \mathfrak{b}\mathfrak{a}^{-1} \subseteq \mathfrak{a}\mathfrak{a}^{-1} = R$. Therefore $\mathfrak{c}$ is an ideal of R and $\mathfrak{b} = \mathfrak{a}\mathfrak{c}$.

Conversely, if $\mathfrak{b} = \mathfrak{a}\mathfrak{c}$ with $\mathfrak{c}$ an ideal, then $\mathfrak{a} \supseteq \mathfrak{a}\mathfrak{c} = \mathfrak{b}$. □

3. The ideal class group

3.1. Fractional ideals and the definition of the class group. The reader will probably have noticed the important role played in the proof of Theorem 1.27 by the gadget $\mathfrak{p}^{-1}$. This is an example of what is called a *fractional ideal*.

By definition, a *fractional ideal* of an integral domain R with fraction field K is an R-submodule J of K such that $aJ \subseteq R$ for some

nonzero element $a \in R$. Note that, in this situation, aJ will automatically be an ideal of R. The element a should be thought of as a "common denominator" for the elements of J.

EXERCISE 1.40. (a) Show that a fractional ideal of R is the same thing as an additive subgroup J of K such that there exists a nonzero element $a \in R$ for which aJ is an ideal of R.
(b) Show that the product of two fractional ideals (as R-submodules of K) is again a fractional ideal.
(c) Prove that if R is noetherian, then J is a fractional ideal of R if and only if it is a finitely generated R-submodule of K.

We have the following lemma:

LEMMA 1.41. *If I is a nonzero ideal of an integral domain R, then $I^{-1} = \{x \in K \ : \ xI \subseteq R\}$ is a fractional ideal of R.*

PROOF. Let $a \in I$ be any nonzero element. Then $aI^{-1} \subseteq R$ as desired. □

LEMMA 1.42. *If R is a Dedekind domain, then the set of nonzero fractional ideals of R forms an abelian group under multiplication with identity element R.*

PROOF. The only thing which needs to be checked is the existence of inverses. Let J be a nonzero fractional ideal of R, and choose a nonzero element $a \in R$ for which $I := aJ$ is an ideal of R. Then aI^{-1} is a fractional ideal of R, and

$$J \cdot aI^{-1} = aJ \cdot I^{-1} = II^{-1} = R \ .$$

□

We denote by $I(R)$ the group of all nonzero fractional ideals of R.

A fractional ideal is called *principal* if it has the form xR for some $x \in K$. For example, the subgroup $\frac{1}{2}\mathbb{Z}$ of $\mathbb{Q}$ consisting of all half-integers is a principal fractional ideal of $\mathbb{Z}$.

EXERCISE 1.43. If R is a Dedekind ring, show that the set of all nonzero principal fractional ideals of R forms a subgroup of $I(R)$.

We denote by $P(R)$ the group of all nonzero principal fractional ideals of R.

Let R be a Dedekind ring. The *ideal class group* of R is the quotient group

$$\mathrm{Cl}(R) := I(R)/P(R) \ .$$

One can give an equivalent definition of $\mathrm{Cl}(R)$ without ever mentioning fractional ideals, as follows. We say that two ideals I, J of R are *equivalent* (and write $I \sim J$) if there exist nonzero elements a, b of R such that $aI = bJ$.

EXERCISE 1.44.
(a) Prove that $\sim$ defines an equivalence relation.
(b) If $I \sim I'$ and $J \sim J'$, show that $II' \sim JJ'$. Deduce that there is a natural group structure on the set of equivalence classes of nonzero ideals.
(c) Prove that the group of equivalence classes of nonzero ideals of R is isomorphic to the ideal class group $\mathrm{Cl}(R)$.

REMARK 1.45. Suppose K is a number field with ring of integers $\mathcal{O}_K$. By abuse of terminology, one often calls $\mathrm{Cl}(\mathcal{O}_K)$ the ideal class group of K (rather than of $\mathcal{O}_K$). We will write Cl_K instead of $\mathrm{Cl}(\mathcal{O}_K)$ when we wish to emphasize this point of view.

The ideal class group is one of the central objects of study in algebraic number theory. While it is not at all obvious, we will show the ideal class group of the ring of integers in a number field K is always a *finite* group. Note that this is a special fact about number fields, it is *not* a general fact about Dedekind domains.

Theorem 1.27 extends in a straightforward way to fractional ideals:

EXERCISE 1.46. If R is a Dedekind ring, then every fractional ideal $J \neq (0), (1)$ has a unique representation as a product

$$J = \prod_{\mathfrak{p} \in \mathrm{Max}(R)} \mathfrak{p}^{\nu_\mathfrak{p}} \ ,$$

where $\mathrm{Max}(R)$ is the set of maximal ideals of R, $\nu_\mathfrak{p} \in \mathbb{Z}$ for all $\mathfrak{p}$, and all but finitely many of the $\nu_\mathfrak{p}$ are zero. In other words, $I(R)$ is the free abelian group on the set $\mathrm{Max}(R)$.

3.2. The norm of an ideal. In this section, we define the *norm* of an ideal in a number ring, which plays an important role in proving the finiteness of the ideal class group.

Let $\mathcal{O}_K$ be the ring of integers in a number field K of degree n, and let $\mathfrak{a}$ be a nonzero ideal of $\mathcal{O}_K$. We have already seen, in the proof of Proposition 1.20, that both $\mathfrak{a}$ and $\mathcal{O}_K$ are free abelian groups of rank n, and therefore that the index $[\mathcal{O}_K : \mathfrak{a}]$ is finite. We define the *norm* of the ideal $\mathfrak{a}$ by the formula

$$N(\mathfrak{a}) = [\mathcal{O}_K : \mathfrak{a}] \ .$$

In other words, we have $N(\mathfrak{a}) = |\mathcal{O}_K/\mathfrak{a}|$. By convention, we define the norm of the zero ideal to be zero.

Recall that we already have a notion of norm for elements: if $\alpha \in K$, then $N(\alpha) := N_{K/\mathbb{Q}}(\alpha) = \sigma_1(\alpha)\cdots\sigma_n(\alpha)$, where $\sigma_1, \ldots, \sigma_n$ are the distinct embeddings of K into $\mathbb{C}$.

The reader may be concerned at this point that if $\mathfrak{a} = (\alpha)$ is a principal ideal, then we will have to write $N((\alpha))$ for the norm of the ideal (α) in order to distinguish it from the norm $N(\alpha)$ of the element α. This would be typographically irritating. Fortunately, one has the following fact:

PROPOSITION 1.47. *If $\mathfrak{a} = (\alpha)$ is principal, then $N(\mathfrak{a}) = |N(\alpha)|$.*

Before giving the proof, we need to introduce the *discriminant*, which is of independent interest and will be discussed in much more detail later on.

Let L/K be a separable field extension of degree n, and let $\alpha_1, \ldots, \alpha_n \in L$. Let $\sigma_1, \ldots, \sigma_n$ be the distinct embeddings of L into an algebraic closure $\overline{K}$ of K, and form the matrix $T = T(\alpha_1, \ldots, \alpha_n)$ whose $(i,j)^{\text{th}}$ entry is $\sigma_i(\alpha_j)$. The *discriminant* $\Delta(\alpha_1, \ldots, \alpha_n)$ is defined to be $\det(T)^2$. By standard facts about determinants, this is independent of the labelling of the α_i's and σ_j's. We clearly have $\Delta(\alpha_1, \ldots, \alpha_n) \in L$, since the images of the embeddings $\sigma_1, \ldots, \sigma_n$ is L, and we will see in a moment that in fact $\Delta(\alpha_1, \ldots, \alpha_n) \in K$.

LEMMA 1.48. *Let L/K be a separable extension of degree n, and let $\alpha_1, \ldots, \alpha_n \in L$. Then $\Delta(\alpha_1, \ldots, \alpha_n) \in K$, and $\Delta(\alpha_1, \ldots, \alpha_n) = 0$ if and only if $\alpha_1, \ldots, \alpha_n$ are linearly dependent over K.*

PROOF. Let $T := T(\alpha_1, \ldots, \alpha_n)$, and let $\Delta := \Delta(\alpha_1, \ldots, \alpha_n)$. If $\alpha_1, \ldots, \alpha_n$ are linearly dependent over K, then the columns of T are linearly dependent, and therefore $\Delta = 0$.

Conversely, assume that $\alpha_1, \ldots, \alpha_n$ form a basis for L/K. By the theorem of the primitive element, we have $L = K(\theta)$ for some $\theta \in L$. Then $1, \theta, \theta^2, \ldots, \theta^{n-1}$ is a basis for L/K, and by linear algebra there exists a matrix M with coefficients in K, having nonzero determinant, such that

$$\begin{bmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{bmatrix} = M \begin{bmatrix} 1 \\ \vdots \\ \theta^{n-1} \end{bmatrix}.$$

Applying σ_i to this equation, and using the fact that M has coefficients in K, we see that for each i we have

$$\begin{bmatrix} \sigma_i(\alpha_1) \\ \vdots \\ \sigma_i(\alpha_n) \end{bmatrix} = M \begin{bmatrix} 1 \\ \vdots \\ \sigma_i(\theta^{n-1}) \end{bmatrix}.$$

It follows that if $T' := T(1, \theta, \ldots, \theta^{n-1})$ and $\Delta' := \Delta(1, \theta, \ldots, \theta^{n-1})$, then $T = T'M^t$, so that $\Delta = \det(M)^2\Delta'$, where $\det(M)$ is a nonzero element of K.

It therefore suffices to prove that $\Delta' \in K$ and $\Delta' \neq 0$. To see this, we note that T' is a Vandermonde matrix, whose determinant (by a well-known formula from linear algebra) is

$$\prod_{1 \leq i < j \leq n} (\sigma_i(\theta) - \sigma_j(\theta)),$$

which is nonzero since the $\sigma_i(\theta)$'s are all distinct (see the proof of Proposition A.7).

Therefore

$$\Delta' := \prod_{i \neq j} (\sigma_i(\theta) - \sigma_j(\theta))$$

is nonzero. It is also a symmetric function of $\sigma_1(\theta), \ldots, \sigma_n(\theta)$, which are precisely the roots of the minimal polynomial f of θ over K. Therefore Δ' is a polynomial (with $\mathbb{Z}$-coefficients) in the coefficients of f, and hence $\Delta' \in K$ as desired. □

Proof of Proposition 1.47. Let $\omega_1, \ldots, \omega_n$ be a $\mathbb{Z}$-basis for $\mathcal{O}_K$. Since $\mathfrak{a} = (\alpha)$ is principal, $\{\alpha_1, \ldots, \alpha_n\} = \{\alpha\omega_1, \ldots, \alpha\omega_n\}$ clearly forms a $\mathbb{Z}$-basis for $\mathfrak{a}$. Write

$$\begin{bmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{bmatrix} = A \begin{bmatrix} \omega_1 \\ \vdots \\ \omega_n \end{bmatrix}$$

with A an invertible $n \times n$ matrix with integer coefficients. Then by Theorem A.11, $N(\mathfrak{a}) = |\det(A)|$.

We also have

$$\Delta(\alpha_1, \ldots, \alpha_n) = \det(A)^2 \Delta(\omega_1, \ldots, \omega_n)$$

by linear algebra.

On the other hand, it follows from the definition of the discriminant that $\Delta(\alpha\omega_1, \ldots, \alpha\omega_n)$ is the square of the determinant of the matrix

$$\begin{pmatrix} \sigma_1(\alpha\omega_1) & \cdots & \sigma_1(\alpha\omega_n) \\ \vdots & & \vdots \\ \sigma_n(\alpha\omega_1) & \cdots & \sigma_n(\alpha\omega_n) \end{pmatrix},$$

This determinant is $\sigma_1(\alpha)\cdots\sigma_n(\alpha)$ times the determinant of the matrix $(\sigma_i(\omega_j))$. In other words, we have

$$\Delta(\alpha\omega_1, \ldots, \alpha\omega_n) = N(\alpha)^2\Delta(\omega_1, \ldots, \omega_n).$$

Therefore $N(\mathfrak{a}) = |\det(A)| = |N(\alpha)|$. □

EXERCISE 1.49. Let $\alpha \in K$, and let $T_\alpha : K \to K$ be the linear transformation given by multiplication by α on K, considered as a $\mathbb{Q}$-vector space. Show that $|N(\alpha)| = |\det(T_\alpha)|$.

3.3. The norm is multiplicative. In this section, we prove the important fact that the norm function on ideals is *multiplicative*, i.e., that $N(\mathfrak{ab}) = N(\mathfrak{a})N(\mathfrak{b})$. This has some important consequences, for example Theorem 1.55 below. It will also be used in our proof that the ideal class group of a number ring is finite.

We first show that if $\mathfrak{a}$ and $\mathfrak{b}$ are relatively prime ideals in $\mathcal{O}_K$ then $N(\mathfrak{ab}) = N(\mathfrak{a})N(\mathfrak{b})$. Recall that two ideals $\mathfrak{a}, \mathfrak{b}$ in a ring R are called *relatively prime* if $\mathfrak{a} + \mathfrak{b} = (1)$. This is a natural generalization of the notion of two integers being relatively prime, since $a, b \in \mathbb{Z}$ are relatively prime iff $am+bn = 1$ for some $m, n \in \mathbb{Z}$, i.e., iff $(a)+(b) = (1)$.

We will in fact show that if $\mathfrak{a}$ and $\mathfrak{b}$ are relatively prime ideals of $\mathcal{O}_K$, then $\mathcal{O}_K/\mathfrak{ab} \cong \mathcal{O}_K/\mathfrak{a} \oplus \mathcal{O}_K/\mathfrak{b}$, from which the desired formula for norms follows. This result is a special case of the Chinese Remainder Theorem for rings, which we recall in the following form:

LEMMA 1.50. *Suppose $\mathfrak{a}_1, \ldots, \mathfrak{a}_n$ are pairwise relatively prime ideals in the ring R. Then:*

(a) *For each $x_1, \ldots, x_n \in R$, there exists $x \in R$ such that $x \equiv x_i \pmod{\mathfrak{a}_i}$ for all i.*
(b) $\mathfrak{a}_1 \cap \cdots \cap \mathfrak{a}_n = \mathfrak{a}_1 \cdots \mathfrak{a}_n$.
(c) $R/(\mathfrak{a}_1 \cdots \mathfrak{a}_n) \cong \oplus R/\mathfrak{a}_i$.

PROOF. By induction, it suffices to prove the the result when $n = 2$. Let $\mathfrak{a} = \mathfrak{a}_1, \mathfrak{b} = \mathfrak{a}_2$. For part (a), note that since $\mathfrak{a}+\mathfrak{b} = (1)$, there exist elements $a \in \mathfrak{a}, b \in \mathfrak{b}$ such that $a + b = 1$. Now take $x = ax_2 + bx_1$.

To prove (b), note that we clearly have $\mathfrak{ab} \subseteq \mathfrak{a} \cap \mathfrak{b}$. For the reverse inclusion, let $x \in \mathfrak{a} \cap \mathfrak{b}$. Then (taking a, b as above) we have $x = xa + xb \in \mathfrak{ab}$ as desired.

For part (c), note that $\mathfrak{a} \cap \mathfrak{b}$ is contained in the kernel of the natural map from R to $R/\mathfrak{a} \oplus R/\mathfrak{b}$, so there is an induced map $\phi : R/(\mathfrak{a} \cap \mathfrak{b}) \to R/\mathfrak{a} \oplus R/\mathfrak{b}$. The map ϕ is clearly injective, and surjectivity follows immediately from part (a). Now apply part (b). □

We also have:

LEMMA 1.51. *Let $\mathfrak{p}, \mathfrak{q}$ be distinct nonzero prime ideals in a 1-dimensional ring R, and let s, t be positive integers. Then $\mathfrak{p}^s$ and $\mathfrak{q}^t$ are relatively prime.*

PROOF. Let $m = \max(s, t)$. Then we claim that $(\mathfrak{p}+\mathfrak{q})^{2m} \subseteq \mathfrak{p}^s + \mathfrak{q}^t$. To see this, note that every element of $(\mathfrak{p} + \mathfrak{q})^{2m}$ is a sum of elements of the form $(x_1 + y_1)(x_2 + y_2) \cdots (x_{2m} + y_{2m})$ with $x_i \in \mathfrak{p}$ and $y_j \in \mathfrak{q}$. Furthermore, each expression $(x_1 + y_1)(x_2 + y_2) \cdots (x_{2m} + y_{2m})$ is itself a sum of terms each of which contains at least m x_i's or m y_j's. By the definition of m, all such terms are in either $\mathfrak{p}^s$ or $\mathfrak{q}^t$. This proves the claim.

Therefore it suffices to prove that $\mathfrak{p} + \mathfrak{q} = (1)$. This follows from the 1-dimensionality of R: since $\mathfrak{p} \neq \mathfrak{q}$ we have $\mathfrak{p} + \mathfrak{q} \supsetneq \mathfrak{p}$, and since $\mathfrak{p}$ is maximal this implies that $\mathfrak{p} + \mathfrak{q} = (1)$. □

If $\mathfrak{p}$ is a nonzero prime ideal of $\mathcal{O}_K$ and $\mathfrak{a}$ is any ideal, we define $\mathrm{ord}_{\mathfrak{p}}(\mathfrak{a})$ to be the largest integer m such that $\mathfrak{p}^m \mid \mathfrak{a}$, if such an m exists. Otherwise, we set $\mathrm{ord}_{\mathfrak{p}}(\mathfrak{a}) = \infty$. If $\alpha \in \mathcal{O}_K$, we set $\mathrm{ord}_{\mathfrak{p}}(\alpha) = \mathrm{ord}_{\mathfrak{p}}(\mathfrak{a})$, where $\mathfrak{a} = (\alpha)$.

EXERCISE 1.52. (a) If $\mathfrak{a} \neq (0), (1)$ is an ideal of $\mathcal{O}_K$, show that $\mathrm{ord}_{\mathfrak{p}}(\mathfrak{a})$ equals the number of copies of $\mathfrak{p}$ which appear in the factorization of $\mathfrak{a}$ into a product of nonzero prime ideals. (In particular, $\mathrm{ord}_{\mathfrak{p}}(\mathfrak{a})$ is finite.)

(b) If $\mathfrak{a}, \mathfrak{b}$ are ideals of $\mathcal{O}_K$, prove that $\mathrm{ord}_{\mathfrak{p}}(\mathfrak{ab}) = \mathrm{ord}_{\mathfrak{p}}(\mathfrak{a}) + \mathrm{ord}_{\mathfrak{p}}(\mathfrak{b})$.

We now prove:

THEOREM 1.53. *If $\mathfrak{a}, \mathfrak{b}$ are ideals of $\mathcal{O}_K$, then $N(\mathfrak{ab}) = N(\mathfrak{a})N(\mathfrak{b})$.*

PROOF. By the Chinese Remainder Theorem and the fact that $\mathfrak{p}^r$ and $\mathfrak{q}^s$ are relatively prime when $\mathfrak{p} \neq \mathfrak{q}$, it is enough (using the factorization of ideals in $\mathcal{O}_K$ into prime ideals) to prove that $N(\mathfrak{p}^m) = N(\mathfrak{p})^m$ whenever $\mathfrak{p}$ is a prime ideal.

For this, first note that we have a chain of ideals

$$\mathcal{O}_K \supset \mathfrak{p} \supset \mathfrak{p}^2 \supset \cdots \supset \mathfrak{p}^m,$$

so it is enough to prove that for each $0 \leq k \leq m-1$, $[\mathfrak{p}^k : \mathfrak{p}^{k+1}] = N(\mathfrak{p})$. (Use induction and the fact that $(\mathcal{O}_K/\mathfrak{p}^{k+1})/(\mathfrak{p}^k/\mathfrak{p}^{k+1}) \cong (\mathcal{O}_K/\mathfrak{p}^k)$ as abelian groups.)

We will prove something stronger, namely that for each k, there is an isomorphism of abelian groups $\mathcal{O}_K/\mathfrak{p} \cong \mathfrak{p}^k/\mathfrak{p}^{k+1}$. To see this, first note that there is a (non-canonical) group homomorphism

$$\phi : \mathcal{O}_K \to \mathfrak{p}^k/\mathfrak{p}^{k+1}$$

given by choosing an element $\gamma \in \mathfrak{p}^k \backslash \mathfrak{p}^{k+1}$ and sending $x \in \mathcal{O}_K$ to γx. (We know that $\mathfrak{p}^k \neq \mathfrak{p}^{k+1}$ by unique factorization, so such an element γ certainly exists). If $x \in \mathfrak{p}$, then $\gamma x \in \mathfrak{p}^{k+1}$, so ϕ induces a map (which we continue to call ϕ)

$$\phi : \mathcal{O}_K/\mathfrak{p} \to \mathfrak{p}^k/\mathfrak{p}^{k+1}.$$

We will show that this map is an isomorphism.

Claim 1: $(\gamma) + \mathfrak{p}^{k+1} = \mathfrak{p}^k$.
Given Claim 1, it follows immediately that ϕ is surjective.

Claim 2: $(\gamma) \cap \mathfrak{p}^{k+1} = \gamma\mathfrak{p}$.
Given Claim 2, it follows that if $\phi(x) = 0$, then $\gamma x \in \gamma\mathfrak{p}$ and hence $x \in \mathfrak{p}$, and thus ϕ is injective.

To prove Claim 1, let $I = (\gamma) + \mathfrak{p}^{k+1}$. Then since $\mathfrak{p}^k \mid (\gamma)$, we also have $\mathfrak{p}^k \mid I$. But $I \supsetneq \mathfrak{p}^{k+1}$, so $I \mid \mathfrak{p}^{k+1}$ and $I \neq \mathfrak{p}^{k+1}$. By unique factorization, we must have $I = \mathfrak{p}^k$ as claimed.

To prove Claim 2, let $I' = (\gamma) \cap \mathfrak{p}^{k+1}$. Since $\gamma \in \mathfrak{p}^k$, we have $\gamma\mathfrak{p} \subseteq I'$. Conversely, let $x \in I'$ and write $x = \gamma y$ with $y \in \mathcal{O}_K$ and $\gamma y \in \mathfrak{p}^{k+1}$, and note that $\mathrm{ord}_\mathfrak{p}(\gamma) + \mathrm{ord}_\mathfrak{p}(y) = \mathrm{ord}_\mathfrak{p}(\gamma y) \geq k+1$. Since $\mathrm{ord}_\mathfrak{p}(\gamma) = k$ by construction, it follows that $\mathrm{ord}_\mathfrak{p}(y) \geq 1$, i.e, $y \in \mathfrak{p}$. Therefore $x = \gamma y \in \gamma\mathfrak{p}$ as desired. □

Remark 1.54. Note that it took a bit of messy verification to prove that $\mathcal{O}_K/\mathfrak{p} \cong \mathfrak{p}^k/\mathfrak{p}^{k+1}$. In the case where $\mathfrak{p} = (\pi)$ is *principal*, this is very simple: one proves easily in that case that multiplication by π^k gives an isomorphism.

In general, there is a useful technique called *localization* which allows one to prove certain results about Dedekind domains by first reducing them to the case of a PID. We will see this in action later on. Localization is also a very useful tool in other contexts.

As an immediate corollary, we obtain another fundamental result:

Theorem 1.55. *Let K be a number field of degree n, and let p be a prime number. Write*

$$(p) = \prod_{i=1}^{r} \mathfrak{p}_i^{e_i}$$

with the $\mathfrak{p}_i$'s distinct prime ideals. Then there exist positive integers f_i such that $N(\mathfrak{p}_i) = p^{f_i}$ for all i, and we have

$$\sum_{i=1}^{r} e_i f_i = n.$$

PROOF. Since the norm is multiplicative, we have $p^n = N(p) = \prod N(\mathfrak{p}_i)^{e_i}$. Therefore $N(\mathfrak{p}_i)$ is a power of p for all i and $\sum_{i=1}^{r} e_i f_i = n$. □

We will prove a more general version of this result later on.

3.4. Finiteness of the ideal class group. In this section, we show that if K is a number field, then the ideal class group $\mathrm{Cl}(\mathcal{O}_K)$ is finite. A preliminary result in this direction is:

LEMMA 1.56. *Let K be a number field. For each $M > 0$, there are only finitely many ideals of $\mathcal{O}_K$ having norm at most M.*

PROOF. It suffices to prove that the set of ideals of norm *equal* to m is finite for each $m \geq 1$. If I is a nonzero ideal with $N(I) = |\mathcal{O}_K/I| = m$, then $mx = 0$ in $\mathcal{O}_K/I$ for all $x \in \mathcal{O}_K$, i.e., I contains the ideal $m\mathcal{O}_K$. As noted in the proof of Corollary 1.22, since $\mathcal{O}_K/m\mathcal{O}_K$ is finite, there are only finitely many ideals which contain $m\mathcal{O}_K$. Therefore there are only finitely many possibilities for I. □

Before giving the next lemma, we remark that every ideal class in $\mathrm{Cl}(\mathcal{O}_K)$ can be represented by a genuine ideal of $\mathcal{O}_K$, and not just by a fractional ideal; this follows from the definition of a fractional ideal and the fact that $[aJ] = [J]$ for every fractional ideal J and every nonzero $a \in R$.

LEMMA 1.57. *Let K be a number field. The class group $\mathrm{Cl}(\mathcal{O}_K)$ is finite if and only if there exists a constant M (depending only on K) such that every ideal class contains an ideal of norm at most M.*

PROOF. If $\mathrm{Cl}(\mathcal{O}_K)$ is finite, let $I_1, \ldots, I_h$ be ideals representing the different ideal classes, and take $M = \max_{1 \leq j \leq h} N(I_j)$. The converse follows from the previous lemma. □

THEOREM 1.58. *Let K be a number field. Then there exists a constant M such that every nonzero ideal I of $\mathcal{O}_K$ contains a nonzero element α with*

$$|N(\alpha)| \leq M \cdot N(I) \ .$$

REMARK 1.59. Note that if $\alpha \in I$, then $(\alpha) \subseteq I$ and thus $N(I) \leq |N(\alpha)|$.

REMARK 1.60. If we fix an integral basis (i.e., a $\mathbb{Z}$-basis) $\alpha_1, \ldots, \alpha_n$ for $\mathcal{O}_K$, and let $\sigma_1, \ldots, \sigma_n$ be the embeddings of K into $\mathbb{C}$, then the proof will show that M can be taken to be

$$\prod_{i=1}^{n} \sum_{j=1}^{n} |\sigma_i(\alpha_j)| = (|\sigma_1\alpha_1| + \cdots + |\sigma_1\alpha_n|) \cdots (|\sigma_n\alpha_1| + \cdots + |\sigma_n\alpha_n|)\,.$$

PROOF OF THEOREM 1.58. The idea of the proof is to use the pigeonhole principle to find an element $\alpha \in I$ whose coordinates with respect to some integral basis are small, and then the norm of α will too be small.

Take $\alpha_1, \ldots, \alpha_n$ to be an integral basis of $\mathcal{O}_K$. Let I be an ideal of $\mathcal{O}_K$ and choose $m \in \mathbb{Z}$ so that $m^n \leq N(I) < (m+1)^n$. Consider the subset Σ of elements of $\mathcal{O}_K$ defined by

$$\Sigma := \left\{ \sum_{j=1}^{n} m_j\alpha_j : 0 \leq m_j \leq m, m_j \in \mathbb{Z} \right\}.$$

Since $\#\Sigma = (m+1)^n > N(I) = |\mathcal{O}_K/I|$, it follows by the pigeonhole principle that there are two distinct elements of Σ, say x and y, which are congruent modulo I. Taking their difference to be $\alpha = x - y$, we get a nonzero element of I of the form $\alpha = \sum_{j=1}^{n} m_j\alpha_j$ with $|m_j| \leq m$ for all j. We estimate the norm of α:

$$\begin{aligned} |N(\alpha)| = \prod_{i=1}^{n} |\sigma_i\alpha| &\leq \prod_{i=1}^{n} \left(\sum_{j=1}^{n} |m_j| \cdot |\sigma_i\alpha_j| \right) \\ &\leq m^n \left(\prod_{i=1}^{n} \sum_{j=1}^{n} |\sigma_i\alpha_j| \right) \\ &\leq N(I) \cdot M. \end{aligned}$$

□

COROLLARY 1.61. *With M as in Theorem 1.58, every ideal class in $\mathcal{O}_K$ contains a nonzero ideal of norm at most M.*

PROOF. Let $c \in \mathrm{Cl}(\mathcal{O}_K)$ be an ideal class and let I be an ideal of $\mathcal{O}_K$ such that $[I] = c^{-1}$. (Here $[J]$ denotes the class of a fractional ideal J in the group $\mathrm{Cl}(\mathcal{O}_K)$.) Choose $\alpha \in I$ such that $|N(\alpha)| \leq M \cdot N(I)$. By Lemma 1.39, it follows that $I \supseteq (\alpha) \Rightarrow (\alpha) = IJ$ for some ideal J. Clearly $[J] = [I]^{-1} = c$, and multiplicativity of the norm implies that $N(J) = |N(\alpha)|/N(I) \leq M$ as desired. □

Combining this result with Lemma 1.57, we obtain the following fundamental result:

THEOREM 1.62. *If K is a number field, then $\mathrm{Cl}(\mathcal{O}_K)$ is finite.*

We also obtain the following useful criterion for $\mathcal{O}_K$ to be a PID:

PROPOSITION 1.63. *If every ideal of $\mathcal{O}_K$ of norm less than or equal to M is principal, then $\mathrm{Cl}(\mathcal{O}_K) = 1$.*

EXERCISE 1.64. Show that $\mathcal{O}_K$ is a PID if and only if every ideal I of $\mathcal{O}_K$ contains an element α with $|N(\alpha)| = N(I)$.

4. Exercises for Chapter 1

(1) Prove that the following rings are not UFD's by explicitly finding two distinct factorizations of the same element.
   (a) $\mathbb{Z}[\sqrt{-13}]$
   (b) $\mathbb{Z}[\sqrt{10}]$ (**Hint:** Factor 6 in two different ways.)

(2) Prove that the following rings are Euclidean domains (and hence UFD's).
   (a) $\mathbb{Z}[\sqrt{-2}]$ (**Hint:** For $x, y \in \mathbb{Z}[\sqrt{-2}]$ with $y \neq 0$, write $x/y = a+b\sqrt{-2}$ with $a, b \in \mathbb{Q}$, and choose $q = c+d\sqrt{-2} \in \mathbb{Z}[\sqrt{-2}]$ so that $|c - a| \leq 1/2, |d - b| \leq 1/2$.)
   (b) $\mathbb{Z}[\sqrt{2}]$ (**Hint:** Use the norm $\phi(a + b\sqrt{2}) = |a^2 - 2b^2|$.)

(3) Find all integers x, y such that $x^3 - y^2 = 2$.

(4)
   (a) Prove that every quadratic number field (a field of degree 2 over $\mathbb{Q}$) is of the form $\mathbb{Q}(\sqrt{d})$ for some square-free integer d.
   (b) Find an explicit example of a cubic number field which is not of the form $\mathbb{Q}(d^{1/3})$ for any integer d.

(5)
   (a) Determine the ring of integers in $\mathbb{Q}(\sqrt{d})$ for all square-free integers d.
   (b) Determine the unit group of the ring of integers in $\mathbb{Q}(\sqrt{d})$ for all square-free integers $d < 0$.

(6) Let $R = \mathbb{Z}[\sqrt{-5}]$, and define the following four ideals in R: $\mathfrak{p}_1 = (2, 1 + \sqrt{-5}), \mathfrak{p}_2 = (2, 1 - \sqrt{-5}), \mathfrak{p}_3 = (3, 1 + \sqrt{-5}), \mathfrak{p}_4 = (3, 1 - \sqrt{-5})$.
   (a) Show that $\mathfrak{p}_1, \ldots, \mathfrak{p}_4$ are all maximal (hence prime) ideals of R. (**Hint:** Prove in each case that the factor group $R/\mathfrak{p}_i$ is a field.)
   (b) Verify that $(2) = \mathfrak{p}_1\mathfrak{p}_2, (3) = \mathfrak{p}_3\mathfrak{p}_4, (1 + \sqrt{-5}) = \mathfrak{p}_1\mathfrak{p}_3, (1 - \sqrt{-5}) = \mathfrak{p}_2\mathfrak{p}_4$.

(7) Let $R = \mathbb{Z}[\sqrt{-3}]$, and let I be the ideal of R generated by 2 and $1 + \sqrt{-3}$.

(a) Show that $I^2 = (2)I$ but $I \neq (2)$. Conclude that proper ideals in R do not factor uniquely into products of prime ideals.
(b) Show that I is the unique prime ideal of R containing (2). Conclude that the ideal (2) cannot be written as a product of prime ideals of R.
(c) Why do parts (a) and (b) above not contradict the theorem which says that every Dedekind domain admits unique factorization of proper ideals into products of prime ideals?

(8) (a) Prove that a PID that is not a field is a Dedekind ring.
(b) Prove that a Dedekind ring is a UFD if and only if it is a PID.

(9) Let R be a Noetherian integral domain with fraction field K. Prove that an R-submodule J of K is finitely generated if and only if there is a nonzero element $a \in R$ such that $aJ \subseteq R$.

(10) If R is a Dedekind ring, prove that every fractional ideal $J \neq (0), (1)$ has a unique representation as a product

$$J = \prod_{\mathfrak{p} \in \mathrm{Max}(R)} \mathfrak{p}^{\nu_{\mathfrak{p}}}$$

where $\nu_{\mathfrak{p}} \in \mathbb{Z}$ for all $\mathfrak{p}$, and all but finitely many of the $\nu_{\mathfrak{p}}$ are zero.

(11) Which of the following are Dedekind rings?
(a) $\mathbb{C}[X, Y]/(Y^2 - X^3)$
(b) $R = \{\frac{a}{b} \in \mathbb{Q} \ : \ a, b \in \mathbb{Z},\ 3 \nmid b\}$

CHAPTER 2

Examples and Computational Methods

1. Computing the ring of integers in a number field

1.1. The discriminant of a number ring and integral bases. Let L/K be a separable field extension of degree n, and let $\alpha_1, \ldots, \alpha_n \in L$. Recall from Lemma 1.48 that $\Delta(\alpha_1, \ldots, \alpha_n) \in K$, with $\Delta(\alpha_1, \ldots, \alpha_n) = 0$ if and only if $\alpha_1, \ldots, \alpha_n$ are linearly dependent over K.

Note that in the case where L and K are number fields, if $\alpha_1, \ldots, \alpha_n$ are algebraic integers, then $\Delta_{L/K}(\alpha_1, \ldots, \alpha_n)$ is also an algebraic integer. This follows from the definition of the discriminant, together with the fact that if α is an algebraic integer, then so is $\sigma_i(\alpha)$ for all i.

In particular, if K is a number field and $\alpha_1, \ldots, \alpha_n$ are algebraic integers which form a basis for $K/\mathbb{Q}$, then $\Delta_{K/\mathbb{Q}}(\alpha_1, \ldots, \alpha_n)$ is a nonzero element of $\mathbb{Z}$.

We now use our knowledge about discriminants to say something about integral bases for rings of integers in number fields. (Recall that $\alpha_1, \ldots, \alpha_n$ is an *integral basis* for $\mathcal{O}_K$ if it is a basis for $\mathcal{O}_K$ as a $\mathbb{Z}$-module.)

PROPOSITION 2.1. *Let K be a number field of degree n, and let $\alpha_1, \ldots, \alpha_n$ be elements of $\mathcal{O}_K$ which form a basis for $K/\mathbb{Q}$. Let $d := \Delta(\alpha_1, \ldots, \alpha_n)$. Then $\mathcal{O}_K$ is contained in the $\mathbb{Z}$-module spanned by $\frac{\alpha_1}{d}, \ldots, \frac{\alpha_n}{d}$.*

PROOF. Let $\alpha \in \mathcal{O}_K$, and write $\alpha = c_1\alpha_1 + \cdots + c_n\alpha_n$ with each $c_j \in \mathbb{Q}$. We need to show that $dc_j \in \mathbb{Z}$ for all j.

Applying σ_i to the relation $\alpha = c_1\alpha_1 + \cdots + c_n\alpha_n$, we find that $\sigma_i(\alpha) = c_1\sigma_i(\alpha_1) + \cdots + c_n\sigma_i(\alpha_n)$, so that

$$\begin{bmatrix} \sigma_1(\alpha) \\ \vdots \\ \sigma_n(\alpha) \end{bmatrix} = T \begin{bmatrix} c_1 \\ \vdots \\ c_n \end{bmatrix},$$

where $T := (\sigma_i(\alpha_j))$. Note that $\sigma_i(\alpha_j)$ is an algebraic integer for any i and j, since all α_j are algebraic integers.

Multiplying this equation on both sides by the adjoint of T, and letting $\delta := \det(T)$, we obtain

$$\begin{bmatrix} \beta_1 \\ \vdots \\ \beta_n \end{bmatrix} = \delta \begin{bmatrix} c_1 \\ \vdots \\ c_n \end{bmatrix}$$

for some algebraic integers $\beta_1, \ldots, \beta_n$.

Let $m_j := \delta\beta_j$. Then since $\delta^2 = d$, we have

$$\begin{bmatrix} m_1 \\ \vdots \\ m_n \end{bmatrix} = d \begin{bmatrix} c_1 \\ \vdots \\ c_n \end{bmatrix}.$$

For any j, we see that δ and β_j are algebraic integers, and thus m_j is an algebraic integer. Furthermore c_j and d are both rational numbers, so $dc_j = m_j$ is an algebraic integer that is also in $\mathbb{Q}$. Thus dc_j is in $\mathbb{Z}$ for all j. This proves that α is in the $\mathbb{Z}$-module spanned by $\frac{\alpha_1}{d}, \ldots, \frac{\alpha_n}{d}$ as claimed. □

Note that Proposition 2.1 provides another proof of the fact that if $K/\mathbb{Q}$ is a finite extension of degree n, then $\mathcal{O}_K$ is a lattice in K. Indeed, Proposition 2.1 shows that $\mathcal{O}_K$ is contained in a finitely generated $\mathbb{Z}$-module of rank n, and therefore is itself a finitely generated $\mathbb{Z}$-module of rank at most n. Since $\mathcal{O}_K$ contains a basis for K, the rank must be exactly n.

Integral bases are not unique. However, the discriminant of every integral basis for $\mathcal{O}_K$ is the same, as the next lemma shows.

LEMMA 2.2. *If $\alpha_1, \ldots, \alpha_n$ and $\alpha'_1, \ldots, \alpha'_n$ are integral bases for $\mathcal{O}_K$, then $\Delta(\alpha_1, \ldots, \alpha_n) = \Delta(\alpha'_1, \ldots, \alpha'_n)$.*

PROOF. Let $\Delta := \Delta(\alpha_1, \ldots, \alpha_n), \Delta' := \Delta(\alpha'_1, \ldots, \alpha'_n)$. Writing each basis in terms of the other, we find that there are nonsingular $n \times n$ matrices M, M' with integer coefficients such that $\Delta = \det(M)^2\Delta'$ and $\Delta' = \det(M')^2\Delta$. The result follows easily from this. □

Because of Lemma 2.2, we may define the *discriminant of $\mathcal{O}_K$* (or, by abuse of terminology, the *discriminant of K*) to be the discriminant of any integral basis for $\mathcal{O}_K$. We write $\Delta(\mathcal{O}_K)$ or Δ_K for the discriminant of $\mathcal{O}_K$.

Using an argument similar to the proof of Proposition 1.47, we see:

LEMMA 2.3. *If $\alpha_1, \ldots, \alpha_n \in \mathcal{O}_K$ form a basis for $K/\mathbb{Q}$ and M denotes the $\mathbb{Z}$-module spanned by $\alpha_1, \ldots, \alpha_n$, then*

$$\Delta_{K/\mathbb{Q}}(\alpha_1, \ldots, \alpha_n) = |\mathcal{O}_K/M|^2 \cdot \Delta_K \ .$$

PROOF. Let $\omega_1, \ldots, \omega_n$ be an integral basis for $\mathcal{O}_K$, and write

$$\begin{bmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{bmatrix} = A \begin{bmatrix} \omega_1 \\ \vdots \\ \omega_n \end{bmatrix} .$$

By Theorem A.11, we have $|\mathcal{O}_K/M| = |\det(A)|$. The result now follows from the fact that

$$\Delta_{K/\mathbb{Q}}(\alpha_1, \ldots, \alpha_n) = \det(A)^2 \Delta(\omega_1, \ldots, \omega_n) .$$

□

COROLLARY 2.4. *If $\alpha_1, \ldots, \alpha_n \in \mathcal{O}_K$ form a basis for $K/\mathbb{Q}$ and $d = \Delta_{K/\mathbb{Q}}(\alpha_1, \ldots, \alpha_n)$ is square-free, then $\alpha_1, \ldots, \alpha_n$ form an integral basis for $\mathcal{O}_K$.*

A lemma which is useful in conjunction with Lemma 2.3 is the following:

LEMMA 2.5. (a) *If $\mathcal{O}_K/(\mathbb{Z}\cdot\alpha_1 \oplus \cdots \oplus \mathbb{Z}\cdot\alpha_n)$ is an abelian group of exponent m (i.e. each element has order dividing m), then*

$$\mathcal{O}_K \subseteq \mathbb{Z} \cdot \frac{\alpha_1}{m} \oplus \cdots \oplus \mathbb{Z} \cdot \frac{\alpha_n}{m} .$$

(b) *If $\mathcal{O}_K \neq \mathbb{Z} \cdot \alpha_1 \oplus \cdots \oplus \mathbb{Z} \cdot \alpha_n$, then $\mathcal{O}_K$ must contain some element of the form*

$$m_1 \frac{\alpha_1}{m} + \cdots + m_n \frac{\alpha_n}{m}$$

with $0 \leq m_i \leq m-1$ and not all m_i equal to zero.

PROOF. Let $M = \mathbb{Z}\cdot\alpha_1 \oplus \cdots \oplus \mathbb{Z}\cdot\alpha_n$. Part (a) follows immediately from the fact that $m\mathcal{O}_K \subset M$, and part (b) follows easily from part (a) and the fact that

$$\{m_1 \frac{\alpha_1}{m} + \cdots + m_n \frac{\alpha_n}{m} \mid 0 \leq m_i \leq m-1\}$$

forms a set of coset representatives for $\left(\frac{1}{m}M\right)/M$. □

As an application of these ideas, we determine the ring of integers $\mathcal{O}_K$ in $K = \mathbb{Q}(\sqrt{d})$ when d is a square-free integer (c.f. Exercise 1.13). Let $\theta = \sqrt{d}$, so that $\mathcal{O}_K$ contains $\mathbb{Z}[\theta]$. We will determine when equality holds, and describe $\mathcal{O}_K$ in all cases.

Let σ_1 be the identity map on K, and let $\sigma_2 : K \to \mathbb{C}$ be the map sending $\sqrt{d}$ to $-\sqrt{d}$. Then

$$\Delta_{K/\mathbb{Q}}(1, \theta) = \det \begin{pmatrix} 1 & \sqrt{d} \\ 1 & -\sqrt{d} \end{pmatrix}^2 = 4d .$$

By Lemma 2.3, we know that $|\mathcal{O}_K/\mathbb{Z}[\theta]|^2$ divides $4d$, and since d is square-free, it follows that $|\mathcal{O}_K/\mathbb{Z}[\theta]|$ equals 1 or 2. Suppose $|\mathcal{O}_K/\mathbb{Z}[\theta]| = 2$. Then by Lemma 2.5, $\mathcal{O}_K$ must contain either $\frac{1}{2}, \frac{\theta}{2}$, or $\frac{1+\theta}{2}$. The minimal polynomials of the first two elements do not have integer coefficients, so those can be ruled out. The minimal polynomial of $\frac{1+\theta}{2}$ is $X^2 - X + \frac{1-d}{4}$, so $\frac{1+\theta}{2}$ is an algebraic integer if and only if $d \equiv 1 \pmod 4$. From this, we conclude:

PROPOSITION 2.6. *Let d be a squarefree integer. Then the ring of integers in $K = \mathbb{Q}(\sqrt{d})$ is*

$$\mathcal{O}_K = \begin{cases} \mathbb{Z}[\sqrt{d}] & \text{if } d \equiv 2, 3 \pmod 4 \\ \mathbb{Z}[\frac{1+\sqrt{d}}{2}] & \text{if } d \equiv 1 \pmod 4 \ , \end{cases}$$

and the discriminant of $\mathcal{O}_K$ is $4d$ if $d \equiv 2, 3 \pmod 4$ and d if $d \equiv 1 \pmod 4$.

The following result is useful for computing discriminants.

EXERCISE 2.7. Let α be an algebraic integer of degree n, and let $f(x)$ be its minimal polynomial over $\mathbb{Q}$. Define the discriminant of α, denoted $\Delta(\alpha)$, to be the discriminant of the basis $\{1, \alpha, \ldots, \alpha^{n-1}\}$ for $\mathbb{Q}(\alpha)/\mathbb{Q}$, and let $\alpha_1, \ldots, \alpha_n$ be the conjugates of α.

(a) Show that

$$\Delta(\alpha) = (-1)^{\binom{n}{2}} \prod_{i=1}^{n} f'(\alpha_i) = (-1)^{\binom{n}{2}} N_{\mathbb{Q}(\alpha)/\mathbb{Q}}(f'(\alpha)).$$

(b) Suppose α is a root of the polynomial $f(x) = x^n + ax + b$, where $a, b \in \mathbb{Z}$ are chosen so that $f(x)$ is irreducible. Use part (a) to show that

$$\Delta(\alpha) = (-1)^{\frac{n(n-1)}{2}} \left((-1)^{n-1}(n-1)^{n-1}a^n + n^n b^{n-1}\right) \ .$$

In particular, show that if $f(x) = x^2 + ax + b$ then $\Delta(\alpha) = a^2 - 4b$, and if $f(x) = x^3 + ax + b$ then $\Delta(\alpha) = -4a^3 - 27b^2$.

EXERCISE 2.8. (a) Find an integral basis for the ring of integers of $\mathbb{Q}(\theta)$, where θ is a root of the polynomial $x^3 - 2x + 3$.

(b) Find an integral basis for the ring of integers of $\mathbb{Q}(\theta)$, where θ is a root of the polynomial $x^3 - x - 4$.

1.2. Example: The ring of integers in $\mathbb{Q}(\sqrt[3]{2})$. In order to apply Corollary 2.4 in an efficient manner, one often requires some supplemental information. The following proposition can be very useful in this context.

PROPOSITION 2.9. *Let K be a number field of degree n, and let $\alpha \in K$ be a nonzero algebraic integer of degree n. Suppose the minimal polynomial of α is* Eisenstein *with respect to the prime p. Then p does not divide $|\mathcal{O}_K/\mathbb{Z}[\alpha]|$.*

PROOF. Let $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$ be the minimal polynomial of α. Recall that $f(x)$ is *Eisenstein* at p if $p \mid a_j$ for $0 \leq j \leq n-1$ and $p^2 \nmid a_0$.

Suppose that $p \mid |\mathcal{O}_K/\mathbb{Z}[\alpha]|$. Then the quotient group $\mathcal{O}_K/\mathbb{Z}[\alpha]$ has order divisible by p, so by Cauchy's theorem there exists $\xi \in \mathcal{O}_K$ such that the class of ξ has order p. It follows that $p\xi \in \mathbb{Z}[\alpha]$ and $\xi \notin \mathbb{Z}[\alpha]$.

Write

$$p\xi = b_0 + b_1\alpha + \cdots + b_{n-1}\alpha^{n-1}.$$

Then each $b_i \in \mathbb{Z}$, and not every b_i is divisible by p. Let j be the smallest index with $0 \leq j \leq n-1$ for which $p \nmid b_j$. Then

$$\begin{aligned}\eta &:= \xi - \left(\frac{b_0}{p} + \frac{b_1}{p}\alpha + \cdots + \frac{b_{j-1}}{p}\alpha^{j-1}\right) \\ &= \frac{b_j}{p}\alpha^j + \frac{b_{j+1}}{p}\alpha^{j+1} + \cdots + \frac{b_n}{p}\alpha^n \qquad \in \mathcal{O}_K\ ,\end{aligned}$$

since both ξ and $\frac{b_0}{p} + \frac{b_1}{p}\alpha + \cdots + \frac{b_{j-1}}{p}\alpha^{j-1}$ are in $\mathcal{O}_K$.

If $\eta \in \mathcal{O}_K$, then we also have

$$\eta\alpha^{n-j-1} = \frac{b_j}{p}\alpha^{n-1} + \frac{\alpha^n}{p}\left(b_{j+1} + b_{j+2}\alpha + \cdots + b_n\alpha^{n-j-2}\right) \in \mathcal{O}_K\ .$$

Since

$$\frac{\alpha^n}{p} = -(a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1})/p \in \mathcal{O}_K\ ,$$

it follows that $\frac{b_j}{p}\alpha^{n-1} \in \mathcal{O}_K$. This implies that $N_{K/\mathbb{Q}}(\frac{b_j}{p}\alpha^{n-1}) \in \mathbb{Z}$.

However,

$$N_{K/\mathbb{Q}}(\frac{b_j}{p}\alpha^{n-1}) = \frac{b_j^n N_{K/\mathbb{Q}}(\alpha)^{n-1}}{p^n} = \frac{b_j^n a_0^{n-1}}{p^n} \notin \mathbb{Z}$$

since $p \nmid b_j$ and $p^2 \nmid a_0$. This contradiction proves that $p \nmid |\mathcal{O}_K/\mathbb{Z}[\alpha]|$ as claimed. □

As an application, we now find the ring of integers in $\mathbb{Q}(\sqrt[3]{2})$.

PROPOSITION 2.10. *The ring of integers in $\mathbb{Q}(\sqrt[3]{2})$ is $\mathbb{Z}[\sqrt[3]{2}]$.*

PROOF. Let $\alpha := \sqrt[3]{2}$, and let $M = \mathbb{Z}[\alpha]$ be the $\mathbb{Z}$-submodule of $\mathcal{O}_K$ generated by $1, \alpha, \alpha^2$. Let $m = |\mathcal{O}_K/M|$. Using Lemma 2.3 and Exercise 2.7, we have

$$m^2\Delta(\mathcal{O}_K) = \Delta_{K/\mathbb{Q}}(1, \alpha, \alpha^2) = -4 \cdot 0^3 - 27 \cdot (-2)^2 = -108.$$

Since $108 = 2^2 \cdot 3^3$, the only primes that could divide m are 2 and 3.

We will use Proposition 2.9 to show that neither 2 nor 3 divides m; it follows that $m = 1$, and consequently $\mathcal{O}_K = M$.

Since $x^3 - 2$ is the minimal polynomial of α and is Eisenstein at 2, Proposition 2.9 implies that $2 \nmid m$. Now set $\beta := \alpha - 2$, so that $K = \mathbb{Q}(\alpha) = \mathbb{Q}(\beta)$. The minimal polynomial of β is $g(x) := (x+2)^3 - 2 = x^3 + 6x^2 + 12x + 6$, which is Eisenstein at both 2 and 3. Proposition 2.9 therefore tells us that $3 \nmid |\mathcal{O}_K/\mathbb{Z}[\beta]|$. But one sees easily that $\mathbb{Z}[\beta] = \mathbb{Z}[\alpha]$, and therefore $3 \nmid m$ as well. □

2. Kummer's theorem on factoring ideals

In this section, we show how to explicitly factor ideals of the form $p\mathcal{O}_K$ where p is a prime number and $\mathcal{O}_K$ is a number ring. The main result, Theorem 2.16 below, is very useful for doing computations in algebraic number theory. Before studying the general case, we begin by analyzing the special case where K is a quadratic number field.

We saw in §1.4 that if p is a prime number, then in the ring $\mathbb{Z}[i]$ of Gaussian integers we have:

(a) $(p) = \mathfrak{p}^2$ if $p = 2$, where $\mathfrak{p} = (1+i)$.
(b) $(p) = \mathfrak{p}_1\mathfrak{p}_2$ if $p \equiv 1 \pmod 4$, where $\mathfrak{p}_1, \mathfrak{p}_2$ are distinct prime ideals.
(c) (p) is prime if $p \equiv 3 \pmod 4$.

In case (a), we say that the prime ideal (p) of $\mathbb{Z}$ *ramifies* in $\mathbb{Z}[i]$. In case (b), we say that (p) *splits completely* in $\mathbb{Z}[i]$. In case (c), we say that (p) is *inert* in $\mathbb{Z}[i]$.

In case (b), we can describe $(p) = (p)\mathbb{Z}[i]$ explicitly: if we choose positive $a, b \in \mathbb{Z}$ such that $a^2+b^2 = p$, then we have $(p) = (a+bi)(a-bi)$.

Remark 2.11. When we want to emphasize that we are thinking of (p) as an ideal of $\mathbb{Z}[i]$ rather than $\mathbb{Z}$, we will usually write $p\mathbb{Z}[i]$ or $(p)\mathbb{Z}[i]$ rather than just (p).

Let's see if we can generalize these results to other quadratic extensions of $\mathbb{Q}$.

Proposition 2.12. *Let $K = \mathbb{Q}(\sqrt{d})$ with $d \in \mathbb{Z}$ squarefree. Let p be an odd prime number such that p does not divide d. Then:*

(a) *If $(\frac{d}{p}) = 1$ then $p\mathcal{O}_K$ factors into prime ideals as $(p, a+\sqrt{d})(p, a-\sqrt{d})$, where $a^2 \equiv d \pmod p$. Moreover, these prime ideals are distinct.*

(b) *If* $(\frac{d}{p}) = -1$*, then* $p\mathcal{O}_K$ *is prime.*

PROOF. For (a), note that in $\mathcal{O}_K$, we have

$$(p, a+\sqrt{d})(p, a-\sqrt{d}) = (p^2, p(a+\sqrt{d}), p(a-\sqrt{d}), a^2-d) \subseteq (p)$$

since $a^2 - d \equiv 0 \pmod{p}$. On the other hand, $(p, a+\sqrt{d})(p, a-\sqrt{d})$ contains both p^2 and $p(a+\sqrt{d}) + p(a-\sqrt{d}) = 2ap$, and therefore it contains $\gcd(p^2, 2ap) = p$. So we have $p\mathcal{O}_K = (p, a+\sqrt{d})(p, a-\sqrt{d})$.

To see that the ideals on the right hand side are prime ideals, it is enough to show that $a + \sqrt{d} \notin (p)$, for then the norm of each ideal must be p, and an ideal whose norm is prime is a prime ideal. But if $p \mid a + \sqrt{d}$, then also $p \mid a - \sqrt{d}$, so $p \mid 2a$, a contradiction.

To see that the ideals $(p, a \pm \sqrt{d})$ are distinct, note that if $a - \sqrt{d} \in (p, a+\sqrt{d})$, then we would also have $2a \in (p, a+\sqrt{d})$, so that $(1) = (p, 2a) \subseteq (p, a+\sqrt{d})$, a contradiction.

For part (b), it is enough to show that if $\mathfrak{p}$ is any prime ideal of $\mathcal{O}_K$ then $N(\mathfrak{p}) \neq p$. Equivalently, we need to show that $\mathcal{O}_K/\mathfrak{p}$ is not isomorphic to $\mathbb{Z}/p\mathbb{Z}$. For this, consider the polynomial $x^2 - d$. It has a root in $\mathcal{O}_K$ and therefore in $\mathcal{O}_K/\mathfrak{p}$. If the latter ring were isomorphic to $\mathbb{Z}/p\mathbb{Z}$, then we would have $(\frac{d}{p}) = 1$, contrary to assumption. □

EXERCISE 2.13. Work out what happens for $p = 2$ and for $p \mid d$.

We now develop a general method for factoring the ideal generated by a rational prime in a number ring which contains Proposition 2.12 as a special case. We begin with the following lemmas.

LEMMA 2.14. *Let* θ *be an algebraic integer with minimal polynomial* $m(x) \in \mathbb{Z}[x]$*. Let* p *be a prime number, let* $f(x) \in \mathbb{Z}[x]$ *be a polynomial, and let* $\overline{f(x)}$ *(resp.* $\overline{m(x)}$*) denote the reduction modulo* p *of* $f(x)$ *(resp.* $m(x)$*). Suppose* $\overline{f(x)} \mid \overline{m(x)}$ *in* $\mathbb{F}_p[x]$*. Then*

$$\mathbb{Z}[x]/\left(p, f(x)\right) \cong \mathbb{Z}[\theta]/\left(p, f(\theta)\right).$$

PROOF. Let $\psi : \mathbb{Z}[x] \to \mathbb{Z}[\theta]/\left(p, f(\theta)\right)$ be the map sending x to θ. It suffices to prove that $\ker(\psi) \subseteq (p, f(x))$ as ψ is clearly surjective and $(p, f(x)) \subseteq \ker(\psi)$.

Let $k(x) \in \ker(\psi)$, so that $k(\theta) \in (p, f(\theta))$, implying that $k(\theta) = a(\theta)\cdot p + b(\theta)f(\theta)$ for some polynomials $a(x), b(x) \in \mathbb{Z}[x]$. Define $h(x) := a(x) \cdot p + b(x)f(x) - k(x)$. Since $h(\theta) = 0$ and $m(x)$ is the minimal polynomial of θ, we have $m(x) \mid h(x)$, which implies that $h(x) = m(x)n(x)$ for some $n(x) \in \mathbb{Z}[x]$. As $m(x) \in (p, f(x))$ by assumption, we have $h(x) \in (p, f(x))$. Hence $k(x) \in (p, f(x))$ as desired. □

LEMMA 2.15. *Let $K = \mathbb{Q}(\theta)$ be a number field, where θ is an algebraic integer, and suppose that p is a prime number which does not divide $|\mathcal{O}_K/\mathbb{Z}[\theta]|$. Then $\mathcal{O}_K/p\mathcal{O}_K \cong \mathbb{Z}[\theta]/p\mathbb{Z}[\theta]$.*

PROOF. Let $\psi : \mathbb{Z}[\theta] \to \mathcal{O}_K/p\mathcal{O}_K$ be the natural map sending θ to $\theta \pmod{p\mathcal{O}_K}$. Clearly $p\mathbb{Z}[\theta] \subseteq \ker(\psi)$. Conversely, if $\alpha \in \ker(\psi)$, then $\alpha \in \mathbb{Z}[\theta] \cap p\mathcal{O}_K$. Hence $\alpha = p\beta$ for some $\beta \in \mathcal{O}_K$. Since $p\beta \in \mathbb{Z}[\theta]$, the image $\overline{\beta} \in \mathcal{O}_K/\mathbb{Z}[\theta]$ has order dividing p. Since p does not divide the order of $\mathcal{O}_K/\mathbb{Z}[\theta]$, it follows that $\overline{\beta} = 0$. Thus $\beta \in \mathbb{Z}[\theta]$, which implies that $\alpha \in p\mathbb{Z}[\theta]$. It follows that $\ker(\psi) = p\mathbb{Z}[\theta]$.

Finally, we show that ψ is surjective. For this, note that if G is any finite abelian group of order prime to p, then the multiplication by p map $[p] : G \to G$ is injective and hence surjective. So if $\gamma \in \mathcal{O}_K$, then $\overline{\gamma} \in \mathcal{O}_K/\mathbb{Z}[\theta]$ can be written as $\overline{\gamma} = p\overline{\gamma'}$ for some $\gamma' \in \mathcal{O}_K$. But then $\gamma - p\gamma' \in \mathbb{Z}[\theta]$. So $\psi(\gamma - p\gamma') = \gamma \pmod{p\mathcal{O}_K}$ as desired. □

THEOREM 2.16 (Kummer's Factorization Theorem). *Let $K = \mathbb{Q}(\theta)$ be a number field, where θ is an algebraic integer, and suppose that p is a prime number which does not divide $|\mathcal{O}_K/\mathbb{Z}[\theta]|$. Let $g(x)$ be the minimal polynomial of θ, and write*

$$g(x) \equiv g_1(x)^{e_1} \cdots g_r(x)^{e_r} \pmod{p},$$

where $g_i(x) \in \mathbb{Z}[x]$, $\overline{g_i(x)} := g_i(x) \pmod{p}$ is irreducible over $\mathbb{F}_p$, and the $\overline{g_i}$'s are pairwise distinct. Then

$$p\mathcal{O}_K = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_r^{e_r},$$

where $\mathfrak{p}_i = (p, g_i(\theta))$ is a prime ideal and $N(\mathfrak{p}_i) = p^{f_i}$ with $f_i = \deg(g_i)$. Moreover, the $\mathfrak{p}_i$'s are all distinct.

PROOF. By Lemmas 2.14 and 2.15, we have

$$\begin{aligned}
\mathcal{O}_K/\mathfrak{p}_i &= \mathcal{O}_K/(p, g_i(\theta)) \\
&\cong \mathbb{Z}[\theta]/(p, g_i(\theta)) \\
&\cong \mathbb{Z}[x]/(p, g_i(x)) \\
&\cong \mathbb{F}_p[x]/\left(\overline{g_i(x)}\right).
\end{aligned}$$

Since $\overline{g_i(x)}$ is irreducible over $\mathbb{F}_p$, we know that $\mathbb{F}_p[x]/\left(\overline{g_i(x)}\right)$ is a field of degree $f_i := \deg(g_i)$ over $\mathbb{F}_p$. Therefore $\mathfrak{p}_i$ is a prime ideal with norm p^{f_i}. Also, if $n := [K : \mathbb{Q}]$, then

$$\sum_{i=1}^{r} e_i f_i = \deg\left(\overline{g(x)}\right) = n. \tag{2.1}$$

We now prove that the $\mathfrak{p}_i$'s are distinct. Given $i \neq j$, we know that $\overline{g_i(x)}$ and $\overline{g_j(x)}$ are relatively prime in $\mathbb{F}_p[x]$. So there exist $a(x), b(x) \in \mathbb{Z}[x]$ such that $1 = \overline{a(x)} \cdot \overline{g_i(x)} + \overline{b(x)} \cdot \overline{g_j(x)}$ in $\mathbb{F}_p[x]$. But then $1 \in (p, g_i(x), g_j(x))$ in $\mathbb{Z}[x]$, from which we deduce that $1 \in (p, g_i(\theta), g_j(\theta)) \subseteq \mathcal{O}_K$. As $(p, g_i(\theta), g_j(\theta)) \subseteq (p, g_i(\theta)) + (p, g_j(\theta))$, it follows that $1 \in \mathfrak{p}_i + \mathfrak{p}_j$. So $\mathfrak{p}_i \neq \mathfrak{p}_j$ as desired.

Finally, we prove that

$$p\mathcal{O}_K = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_r^{e_r} \ .$$

A simple inductive argument, plus the fact that $g(\theta) = 0$, shows that

$$\begin{aligned} \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_r^{e_r} &= (p, g_1(\theta))^{e_1} \cdots (p, g_r(\theta))^{e_r} \\ &\subseteq (p, g_1(\theta)^{e_1} \cdots g_r(\theta)^{e_r}) = (p, g(\theta)) \\ &= p\mathcal{O}_K \ . \end{aligned}$$

Therefore $p\mathcal{O}_K \mid \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_r^{e_r}$, from which it follows that $p\mathcal{O}_K = \mathfrak{p}_1^{e_1'} \cdots \mathfrak{p}_r^{e_r'}$ with $0 \leq e_i' \leq e_i$ for all i. By Theorem 1.55 and (2.1), we know that

$$n = \sum_{i=1}^{r} e_i' f_i \leq \sum_{i=1}^{r} e_i f_i = n \ .$$

Since $e_i' \leq e_i$ for every i, it follows that all terms in the displayed inequality must be equalities. Therefore $e_i' = e_i$ for all i. □

REMARK 2.17. Kummer's Factorization Theorem applies to all primes p if $\mathcal{O}_K = \mathbb{Z}[\theta]$. More generally, we know that $p \nmid |\mathcal{O}_K/\mathbb{Z}[\theta]|$ whenever $p^2 \nmid \Delta(\theta)$, or if the minimal polynomial of θ is *Eisenstein* at p.

Unfortunately, one can find a number field K and a prime p such that p divides $|\mathcal{O}_K/\mathbb{Z}[\theta]|$ for all algebraic integers $\theta \in K$ of degree n, and in such examples Kummer's theorem does not suffice to determine the factorization of $p\mathcal{O}_K$ into prime ideals.

3. The splitting of primes

3.1. Terminology. Let $\mathcal{O}_K$ be a number ring, and let p be a rational prime. By Theorem 1.55, we know that

$$p\mathcal{O}_K = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_r^{e_r}$$

with $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ distinct prime ideals having norm $N_{K/\mathbb{Q}}(\mathfrak{p}_i) = p^{f_i}$, and that

$$\sum_{i=1}^{r} e_i f_i = n \ .$$

We call the prime ideals $\mathfrak{p}_i$ the prime ideals *lying over* (or *dividing*) p. The integer e_i is called the *ramification index* of $\mathfrak{p}_i$, and f_i is called the *residue degree* of $\mathfrak{p}_i$.

EXERCISE 2.18. Show that every nonzero prime ideal $\mathfrak{p}$ of $\mathcal{O}_K$ lies over a unique prime number p.

We say that p is *ramified* in $\mathcal{O}_K$ (or in K) if $e_i \geq 2$ for some i, i.e., if $\mathfrak{p}^2 \mid p\mathcal{O}_K$ for some nonzero prime ideal $\mathfrak{p}$ of $\mathcal{O}_K$. In addition, p is called *totally ramified* in $\mathcal{O}_K$ if $p\mathcal{O}_K = \mathfrak{p}^n$ for some prime ideal $\mathfrak{p}$.

A prime p is said to be *inert* in $\mathcal{O}_K$ if $p\mathcal{O}_K$ is a prime ideal, and p is said to *split completely* in $\mathcal{O}_K$ if $r = n$, i.e., if $p\mathcal{O}_K$ factors as a product of n distinct prime ideals, each having norm p.

As a consequence of Kummer's factorization theorem, we can deduce several useful results about the splitting behavior of rational primes in number rings:

COROLLARY 2.19. *Let θ be an algebraic integer whose minimal polynomial $g(x)$ is Eisenstein at the prime p. If $K = \mathbb{Q}(\theta)$, then p is totally ramified in $\mathcal{O}_K$.*

PROOF. We know that θ Eisenstein at p implies $p \nmid |\mathcal{O}_K/\mathbb{Z}[\theta]|$. By the preceding remarks, it suffices to note that

$$g(x) \equiv x^n \pmod{p} \Rightarrow p\mathcal{O}_K = \mathfrak{p}^n,$$

where $\mathfrak{p} = (p, \theta)$ and $[K : \mathbb{Q}] = n$. □

COROLLARY 2.20. *If $p \nmid |\mathcal{O}_K/\mathbb{Z}[\theta]|$, then p ramifies in $\mathcal{O}_K$ if and only if $p \mid \Delta_K$.*

PROOF. Let $\theta \in \mathcal{O}_K$ be a primitive element for K so that $K = \mathbb{Q}(\theta)$. Let $g(x) = \prod_{i=1}^{n}(x - \theta_i)$ be the minimal polynomial of θ, where $\theta_1, \ldots, \theta_n$ are its conjugates. Let $\Delta = \Delta(\theta)$ be the discriminant of θ. Since

$$\Delta = \prod_{i<j}(\theta_i - \theta_j)^2 \ ,$$

we know from field theory that $\overline{g(x)}$ will have a multiple root in $\overline{\mathbb{F}}_p$ if and only if $p \mid \Delta$. Moreover, it also follows from field theory that $\overline{g(x)}$ has a multiple root in $\overline{\mathbb{F}}_p$ if and only if there exists an irreducible monic polynomial $\overline{h(x)} \in \mathbb{F}_p[x]$ such that $\overline{h(x)} \mid \overline{g(x)}$ in $\mathbb{F}_p[x]$.

But if $p \nmid |\mathcal{O}_K/\mathbb{Z}[\theta]|$, then by Theorem 2.16, p ramifies in $\mathcal{O}_K$ if and only if $\overline{g(x)}$ has a multiple root in $\overline{\mathbb{F}}_p$. □

COROLLARY 2.21. *If K is a number field, then only finitely many prime numbers p ramify in K.*

PROOF. There are only finitely many primes which divide either $|\mathcal{O}_K/\mathbb{Z}[\theta]|$ or Δ_K. □

One can show that Corollary 2.20 is true for *any* number field K *without* the hypothesis that $p \nmid |\mathcal{O}_K/\mathbb{Z}[\theta]|$. We will see later that $\mathcal{O}_K$ is *not* always of the form $\mathbb{Z}[\theta]$ for some $\theta \in \mathcal{O}_K$. (If $\mathcal{O}_K = \mathbb{Z}[\theta]$, we say that $\mathcal{O}_K$ is *monogenic* over $\mathbb{Z}$.)

3.2. Examples of prime splittings.

EXAMPLE 2.22. We know that if $K = \mathbb{Q}(\sqrt[3]{2})$, then $\mathcal{O}_K = \mathbb{Z}[\sqrt[3]{2}]$. Let $p = 5$; then $x^3 - 2$ factors modulo 5 into irreducibles as

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

So the ideal $5\mathcal{O}_K$ has the prime factorization $5\mathcal{O}_K = \mathfrak{p}_1\mathfrak{p}_2$, where $f(\mathfrak{p}_1/5) = 1$ and $f(\mathfrak{p}_2/5) = 2$. Here $\mathfrak{p}_1 = (5, \sqrt[3]{2} - 3), \mathfrak{p}_2 = (5, \sqrt[3]{4} + 3\sqrt[3]{2} - 1)$. Note in particular that the f_i's are *not equal*. (We will see later that if $K/\mathbb{Q}$ is a *Galois* extension, then all of the f_i's are equal to one another.)

EXERCISE 2.23. Prove that two quadratic fields K, K' are isomorphic if and only if their discriminants are the same.

EXAMPLE 2.24. In contrast to the preceding exercise, there exist non-isomorphic cubic fields with the same discriminant.

On the one hand, let θ be a root of $g(x) = x^3 + 10x + 1$, $K = \mathbb{Q}(\theta)$. We know the discriminant of $x^3 + ax + b$ is $-4a^3 - 27b^2$. So $\Delta(\theta) = -4027$, which is prime (and hence square-free). Thus $\mathcal{O}_K = \mathbb{Z}[\theta]$. It is not hard to verify that $g(x) \pmod{17}$ is irreducible so that (17) is a prime ideal in $\mathcal{O}_K$.

On the other hand, let α be a root of $f(x) = x^3 - 8x + 15$, $L = \mathbb{Q}(\alpha)$. Then $\Delta(\alpha) = -4027$, so again $\mathcal{O}_L = \mathbb{Z}[\alpha]$. However, $f(x) \equiv (x+4)(x+6)(x+7) \pmod{17}$, so $(17) = \mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3$ splits completely in $\mathcal{O}_L$. It follows that $L \ncong K$ as fields since any field isomorphism would have to respect rings of integers and the splitting types of rational primes.

Interestingly, 17 is the smallest prime that works in this example—for all prime $p \leq 13$, $f(x)$ and $g(x)$ split the same way modulo p.

EXERCISE 2.25. Factor the ideals $(2), (3), (7)$ into prime ideals in $R = \mathbb{Z}[\sqrt[3]{2}]$.

3.3. Computing ideal class groups. Kummer's factorization theorem can also be used to determine ideal class groups. We turn now to a couple of examples which illustrate the general method.

EXAMPLE 2.26. Let $K = \mathbb{Q}(\sqrt{2})$, so that $\mathcal{O}_K$ has the integral basis $1, \sqrt{2}$. Then every ideal class contains a nonzero ideal of norm at most 5, since $M = (1+\sqrt{2})^2 = (3+2\sqrt{2}) \approx 5.8 < 6$.

Using Kummer's factorization theorem, we factor $x^2 - 2 \bmod p$ for $p = 3, 5$, and we find that both (3) and (5) remain prime in $\mathcal{O}_K$, and therefore have norms $9, 25$, respectively. So the only nonzero ideals of norm at most 5 in $\mathcal{O}_K$ are $(1), (\sqrt{2})$, and (2), all of which are principal. It follows that $\mathcal{O}_K$ is a PID.

Note that if we had used the integral basis $1, -1+\sqrt{2}$ instead, we could have obtained a better value of M, concluding that every ideal class contains a nonzero ideal of norm at most 4. This would remove the need to factor (5) in $\mathcal{O}_K$.

EXAMPLE 2.27. Let $K = \mathbb{Q}(\sqrt{-5})$, so that $\mathcal{O}_K$ has the integral basis $1, \sqrt{-5}$. We obtain $M = (1+\sqrt{5})^2 = 6 + 2\sqrt{5} < 11$, so that every ideal class in $\mathrm{Cl}(\mathcal{O}_K)$ contains a nonzero ideal of norm at most 10. Using Kummer's factorization theorem, we find that

$$\begin{array}{rcl} (2) &=& (2, 1+\sqrt{-5})^2 = \mathfrak{p}_2^2 \\ (3) &=& (3, 1+\sqrt{-5})(3, 1-\sqrt{-5}) = \mathfrak{p}_3\mathfrak{p}_3' \\ (5) &=& (\sqrt{-5})^2 = \mathfrak{p}_5^2 \\ (7) &=& (7, 3+\sqrt{-5})(7, 3-\sqrt{-5}) = \mathfrak{p}_7\mathfrak{p}_7'. \end{array}$$

Note that $\mathfrak{p}_2$ is not principal, since if it were equal to (α), then we would have $|N(\alpha)| = 2$, and therefore $N(\alpha) = \pm 2$. However, if $\alpha = a + b\sqrt{-5}$, then $N(\alpha) = a^2 + 5b^2 \neq \pm 2$, a contradiction.

Similarly, there are no elements of norm $\pm 3, \pm 7$ in $\mathcal{O}_K$, so that $\mathfrak{p}_3, \mathfrak{p}_3', \mathfrak{p}_7, \mathfrak{p}_7'$ are not principal. The prime ideal $\mathfrak{p}_5$, of course, is principal.

The nonzero ideals of norm at most 10 in $\mathcal{O}_K$ are all products of $\mathfrak{p}_2, \mathfrak{p}_3, \mathfrak{p}_3', \mathfrak{p}_5, \mathfrak{p}_7, \mathfrak{p}_7'$ to various powers between 0 and 3. Moreover, since $\mathfrak{p}_2^2 = (2)$, we have $[\mathfrak{p}_2]^2 = 1$ in $\mathrm{Cl}(\mathcal{O}_K)$. We now seek to relate the classes of $\mathfrak{p}_3$ and $\mathfrak{p}_7$ to the class of $\mathfrak{p}_2$. For this, we search for elements of K with norm divisible only by $2, 3$ (resp $2, 7$). This is simple: for example, we have $N(1+\sqrt{-5}) = 6$, from which it follows easily that $(1+\sqrt{-5}) = \mathfrak{p}_2\mathfrak{p}_3$. (Note that $1+\sqrt{-5}$ is in both $\mathfrak{p}_2$ and $\mathfrak{p}_3$, so that $\mathfrak{p}_2\mathfrak{p}_3 = \mathfrak{p}_2 \cap \mathfrak{p}_3 \subseteq (1+\sqrt{-5})$ and therefore the equality of ideals follows from the equality of the norms.) We conclude from this that

$$[\mathfrak{p}_3] = [\mathfrak{p}_2]^{-1} = [\mathfrak{p}_2],$$

where the last equality follows from the fact that $[\mathfrak{p}_2]^2 = 1$. Since $\mathfrak{p}_3\mathfrak{p}_3' = (3)$, we also have

$$[\mathfrak{p}_3'] = [\mathfrak{p}_3]^{-1} = [\mathfrak{p}_2]^{-1} = [\mathfrak{p}_2].$$

Similarly, it follows from the fact that $N(3+\sqrt{-5}) = 14$ that $[\mathfrak{p}_7] = [\mathfrak{p}_7'] = [\mathfrak{p}_2]$, and therefore every ideal class in $\mathrm{Cl}(\mathcal{O}_K)$ coincides with either 1 or $[\mathfrak{p}_2]$. We conclude that $\mathrm{Cl}(\mathcal{O}_K) \cong \mathbb{Z}/2\mathbb{Z}$. In particular, the *class number* of $\mathbb{Z}[\sqrt{-5}]$ (i.e., the order of its ideal class group) is 2.

It turns out that by using Minkowsi's theory of geometry of numbers (to be discussed later), we can dramatically reduce the value of M in the above examples. For example, with $K = \mathbb{Q}(\sqrt{-5})$, Minkowski's theory will give the bound $M = 2$ instead of $M = 10$!

Finally, we end this section with a significant generalization of Proposition 2.10.

PROPOSITION 2.28. *Let p be a prime, and let $a \notin \{0, \pm 1\}$ be a squarefree integer not divisible by p. Let $\theta = \sqrt[p]{a}$ be a pth root of a. Then $\mathcal{O}_K = \mathbb{Z}[\theta]$ if and only if $a^{p-1} \not\equiv 1 \pmod{p^2}$.*

PROOF. Let $K = \mathbb{Q}(\theta)$. Assume $a^p \not\equiv a \pmod{p^2}$. By Lemma 2.3 and Exercise 2.7, the polynomial $x^p - a$ has discriminant $\Delta(\theta) = \pm p^p a^{p-1}$ and

$$\Delta(\theta) = |\mathcal{O}_K/\mathbb{Z}[\theta]|^2 \cdot \Delta_K \ .$$

Since $x^p - a$ is Eisenstein at every prime divisor of a, it follows that $|\mathcal{O}_K/\mathbb{Z}[\theta]|$ is relatively prime to a, and thus is a power of p. Moreover, the polynomial $(x+a)^p - a$ is Eisenstein at p by hypothesis, and $\mathbb{Z}[\theta] = \mathbb{Z}[\theta - a]$. Therefore $p \nmid |\mathcal{O}_K/\mathbb{Z}[\theta]|$ by Proposition 2.9. It follows that $|\mathcal{O}_K/\mathbb{Z}[\theta]| = 1$, i.e., $\mathcal{O}_K = \mathbb{Z}[\theta]$.

Conversely, suppose $\mathcal{O}_K = \mathbb{Z}[\theta]$. Then by Kummer's factorization theorem, we have $p\mathcal{O}_K = \mathfrak{p}^p$ where $\mathfrak{p} = (p, \theta - a)$ is a prime ideal of norm p. Clearly $\theta - a \in \mathfrak{p}$, and since $p \in \mathfrak{p}^2$, we must have $\theta - a \notin \mathfrak{p}^2$. Thus

$$(\theta - a) = \mathfrak{p}\mathfrak{a}$$

for some ideal $\mathfrak{a}$ of $\mathcal{O}_K$ relatively prime to $\mathfrak{p}$. Since $\mathfrak{p}$ is the only prime ideal of $\mathcal{O}_K$ containing p, it is the only prime ideal of $\mathcal{O}_K$ whose norm is a power of p, and thus $(p, N(\mathfrak{a})) = 1$. Since the constant term of the minimal polynomial of $\theta - a$ is $a^p - a$, it follows that

$$a^p - a = |N(\theta - a)| = N(\mathfrak{p}\mathfrak{a}) = pN(\mathfrak{a}) \ ,$$

so that $p^2 \nmid a^p - a$ as desired. □

3.4. Application: The Diophantine equation $y^2 = x^3 - 5$. We now show how knowledge of the ideal class group can be of help in solving certain Diophantine equations.

Earlier on, we used the fact that $\mathbb{Z}[i]$ is a UFD to solve the equation $y^2 = x^3 - 1$ in integers. We now use arithmetic in $\mathbb{Z}[\sqrt{-5}]$ (which has class number 2) to solve the equation $y^2 = x^3 - 5$.

THEOREM 2.29. *The equation $y^2 = x^3 - 5$ has no integer solutions.*

PROOF. Suppose (x, y) is an integer solution. If x is even, then y is odd and $y^2 \equiv -1 \pmod 4$, which is impossible. Therefore x is odd.

Also, it is easy to see that x and y must be coprime, since the only possible prime dividing both is 5, but if $5 \mid x, y$ then 5^2 would divide the left-hand side but not the right-hand side of the above equation, a contradiction.

We now factor the equation in $R = \mathbb{Z}[\sqrt{-5}]$ to obtain

$$(y + \sqrt{-5})(y - \sqrt{-5}) = x^3 \ .$$

If a prime ideal $\mathfrak{p}$ of R divides both $(y+\sqrt{-5})$ and $(y-\sqrt{-5})$, then $\mathfrak{p} \mid (x^3)$ (and therefore $\mathfrak{p} \mid (x)$) and $\mathfrak{p} \mid (2y)$. Since x is odd, and $\mathfrak{p} \mid (x)$, $\mathfrak{p} \nmid (2)$, so $\mathfrak{p} \mid (y)$. This contradicts the fact that x and y are relatively prime. Therefore the ideals $(y + \sqrt{-5})$ and $(y - \sqrt{-5})$ are coprime.

It follows by unique factorization into prime ideals that $(y+\sqrt{-5}) = \mathfrak{a}^3$ and $(y - \sqrt{-5}) = \mathfrak{b}^3$ for some ideals $\mathfrak{a}, \mathfrak{b}$ of R.

As $[\mathfrak{a}]^3 = [\mathfrak{b}]^3 = 1$ in $\mathrm{Cl}(R)$, and as the class number of $\mathbb{Z}[\sqrt{-5}]$ is 2, we conclude that $\mathfrak{a}$ and $\mathfrak{b}$ are principal ideals.

Since the only units in R are ± 1, it follows in particular that

$$y + \sqrt{-5} = (a + b\sqrt{-5})^3$$

for some $a, b \in \mathbb{Z}$. This implies that $1 = 3ba^2 - 5b^3 = b(3a^2 - 5b^2)$, so that $b = \pm 1$. But then $3a^2 - 5 = \pm 1$, which is impossible.

This contradiction proves that no integral solutions (x, y) exist. □

4. Cyclotomic Fields

4.1. The cyclotomic field $\mathbb{Q}(\zeta_m)$ with m a prime power. Let $m = p^k$ be a prime power. In this section, we determine the ring of integers in $\mathbb{Q}(\zeta_m)$ and the factorization of certain ideals into products of prime ideals. The case of a general positive integer m will be dealt with in a subsequent section.

It is well-known that the polynomial

$$\Phi_m(x) = \frac{x^{p^k} - 1}{x^{p^{k-1}} - 1} = x^{(p-1)p^{k-1}} + x^{(p-2)p^{k-1}} + \cdots + x^{p^{k-1}} + 1 \tag{2.2}$$

is irreducible over $\mathbb{Z}$, and therefore is the minimal polynomial of ζ_m. This polynomial has degree $\phi(m)$, where ϕ is Euler's ϕ-function.

The irreducibility of $\Phi_m(x)$ is most conveniently proved using the fact that $\Phi_m(x+1)$ is Eisenstein at p. To see this, note that

$$\Phi_m(x+1) = \frac{(x+1)^{p^k}-1}{(x+1)^{p^{k-1}}-1} \equiv \frac{(x^{p^k}+1)-1}{(x^{p^{k-1}}+1)-1} \equiv x^{\phi(p^k)} \pmod{p},$$

and that $\Phi_m(1) = p \not\equiv 0 \pmod{p^2}$.

In particular, $\Phi_m(x+1)$, and therefore $\Phi_m(x)$, is irreducible over $\mathbb{Z}$, and $[\mathbb{Q}(\zeta_m) : \mathbb{Q}] = \phi(m)$.

More generally, for any positive integer m, the minimal polynomial $\Phi_m(x)$ of ζ_m has degree $\phi(m)$, and therefore $[\mathbb{Q}(\zeta_m) : \mathbb{Q}] = \phi(m)$. However, one cannot in general write down a simple explicit formula for $\Phi_m(x)$ as in (2.2). We will sometimes write K_m to denote the cyclotomic field $\mathbb{Q}(\zeta_m)$.

We recall for later use that $K_m/\mathbb{Q}$ is a Galois extension with Galois group isomorphic to $(\mathbb{Z}/m\mathbb{Z})^*$. The fact that $K_m/\mathbb{Q}$ is Galois follows from the fact that, by the irreducibility of $\Phi_m(x)$, $\zeta_m^t \in K_m$ is a root of $\Phi_m(x)$ whenever $1 \leq t < m$ and $\gcd(t,m) = 1$. Furthermore, the map from $(\mathbb{Z}/m\mathbb{Z})^*$ to $\mathrm{Gal}(K_m/\mathbb{Q})$ sending t to the automorphism $\sigma_t : \zeta_m \to \zeta_m^t$ is a group isomorphism.

In order to compute the ring of integers in $\mathbb{Q}(\zeta_m)$ when m is a prime-power, we will use the following lemma (which applies more generally to any positive integer m):

LEMMA 2.30. *Let m be a positive integer, and let $d = \phi(m)$ be the degree of the minimal polynomial $\Phi_m(x)$ of ζ_m over $\mathbb{Q}$. Then the discriminant $\Delta(\zeta_m)$ of ζ_m divides m^d.*

PROOF. Since $\Phi_m(x) \mid x^m - 1$, we have $x^m - 1 = \Phi_m(x)g(x)$ for some $g(x) \in \mathbb{Z}[x]$. Differentiating and setting $x = \zeta_m$, we obtain

$$m\zeta_m^{m-1} = \Phi_m'(\zeta_m)g(\zeta_m) \tag{2.3}$$

since $\Phi_m(\zeta_m) = 0$. Noting that the constant term of $\Phi_m(x)$ must be ± 1 and taking the norm of both sides of (2.3), we obtain

$$\begin{aligned} m^d &= N_{\mathbb{Q}(\zeta_m)/\mathbb{Q}}(\zeta_m) \cdot N_{\mathbb{Q}(\zeta_m)/\mathbb{Q}}(g(\zeta_m)) \\ &= \pm\Delta(\zeta_m) \cdot N_{\mathbb{Q}(\zeta_m)/\mathbb{Q}}(g(\zeta_m)) \end{aligned}$$

where the second equality comes from Exercise 2.7. As $g(\zeta_m)$ is a nonzero algebraic integer, its norm is a nonzero element of $\mathbb{Z}$. □

THEOREM 2.31. *If $m = p^k$ is a prime power and $\zeta_m = e^{2\pi i/m}$ is a primitive p^kth root of unity, then:*

(a) *The absolute value of the discriminant of $\mathbb{Q}(\zeta_m)$ is a power of p.*

(b) *The ring of integers in* $\mathbb{Q}(\zeta_m)$ *is* $\mathbb{Z}[\zeta_m]$.

PROOF. Part (a) is an immediate consequence of Lemma 2.30, since the discriminant of $\mathbb{Q}(\zeta_m)$ divides the discriminant of the basis $\{1, \zeta_m, \zeta_m^2, \ldots, \zeta_m^{\phi(m)-1}\}$ for $\mathbb{Q}(\zeta_m)/\mathbb{Q}$.

Part (b) follows from the fact that $\Phi_m(x+1)$ is Eisenstein at p, since on the one hand this implies that $p \nmid |\mathcal{O}_{K_m}/\mathbb{Z}[\zeta_m]|$, and on the other hand we have

$$\Delta(\zeta_m) = \Delta(\mathbb{Q}(\zeta_m)) \cdot |\mathcal{O}_{K_m}/\mathbb{Z}[\zeta_m]|^2 \ ,$$

which implies that $|\mathcal{O}_{K_m}/\mathbb{Z}[\zeta_m]|$ is a power of p. □

As a consequence of Kummer's factorization theorem, we obtain:

COROLLARY 2.32. (a) *If* $m = p^k$, *then* p *is totally ramified in* K_m, *and* p *is the only prime which ramifies in* K_m.

(b) *The principal ideal* $(1 - \zeta_m)$ *has norm* p, *and*

$$p\mathbb{Z}[\zeta_m] = (1 - \zeta_m)^{\phi(m)}.$$

PROOF. Part (a) follows from Theorem 2.31 using Corollary 2.19 and Corollary 2.20.

For (b), note that $\zeta_m - 1$ is a root of $\Phi_m(x+1)$, that $\mathbb{Q}(\zeta_m - 1) = \mathbb{Q}(\zeta_m)$, and that $\Phi_m(x+1) \equiv x^{\phi(m)} \pmod{p}$. Therefore $p\mathbb{Z}[\zeta_m] = (p, \zeta_m - 1)^{\phi(m)} = (\zeta_m - 1)^{\phi(m)}$, since $N(1 - \zeta_m) = \pm p$ implies that $p \in (\zeta_m - 1) = (1 - \zeta_m)$. □

4.2. The first case of Fermat's Last Theorem for regular primes. Our next goal is to establish a result concerning the units of $\mathbb{Z}[\zeta_p]$ which was used by Kummer to prove the first case of Fermat's Last Theorem for regular primes. Before stating the first of several preliminary lemmas, we remark that if the integer m is odd, then $\mathbb{Q}(\zeta_m) = \mathbb{Q}(\zeta_{2m})$.

LEMMA 2.33. *If* m *is a positive integer, the only roots of unity in* $\mathbb{Q}(\zeta_m)$ *are the* m*th roots of unity, if* m *is even, and the* $2m^{\text{th}}$ *roots of unity, if* m *is odd.*

PROOF. It is enough to prove the statement when m is even, so we assume this from now on. Let ζ be a primitive k^{th} root of 1 in $K_m = \mathbb{Q}(\zeta_m)$. We want to show that $k \mid m$, for then ζ will be an m^{th} root of unity as desired. Without loss of generality (replacing ζ by an appropriate power), we may assume that $\zeta = \zeta_k = e^{2\pi i/k}$.

Since K_m contains both ζ_k and ζ_m, we claim that it contains ζ_r, where $r = \text{lcm}(k, m)$. To see this, note that $r = km/d$, where $d = \gcd(k, m)$, and that there exist $a, b \in \mathbb{Z}$ such that $ak + bm = d$. It

follows that K_m contains $\zeta_k^b \zeta_m^a == \zeta_k^{bm/m} \zeta_m^{ak/k} = e^{2\pi i(bm+ak)/km} = \zeta_r$ as claimed.

But then $\mathbb{Q}(\zeta_r) \subseteq \mathbb{Q}(\zeta_m)$, so that $\phi(r) \leq \phi(m)$ by a consideration of degrees. Since $m \mid r$, it follows from Exercise 2.34 below that $r = m$. Therefore $k \mid m$ as desired. □

EXERCISE 2.34. If m, r are even positive integers with $m \mid r$ and $\phi(r) \leq \phi(m)$, then $m = r$.

We also note that since $\zeta_m = e^{2\pi i/m}$ has complex absolute value 1, the complex conjugation automorphism τ of $\mathrm{Gal}(K_m/\mathbb{Q})$ coincides with the automorphism $\sigma \in \mathrm{Gal}(K_m/\mathbb{Q})$ sending ζ_m to ζ_m^{-1}. And since $\mathrm{Gal}(K_m/\mathbb{Q})$ is abelian, τ commutes with σ for all $\sigma \in \mathrm{Gal}(K_m/\mathbb{Q})$. Concretely, this implies that if $\alpha \in K_m$ and $\sigma \in \mathrm{Gal}(K_m/\mathbb{Q})$, then

$$\overline{\sigma(\alpha)} = \sigma(\overline{\alpha}).$$

The following lemma is usually attributed to Kronecker.

LEMMA 2.35. *If $\alpha \in \mathbb{C}$ is a nonzero algebraic integer, all of whose conjugates have complex absolute value at most 1, then α is a root of unity.*

PROOF. Let $f(x) \in \mathbb{Z}[x]$ be the minimal polynomial of α, and let $n = \deg(f)$. Since the coefficients a_i of $f(x)$ are elementary symmetric functions of the conjugates of α, it follows from the triangle inequality that $|a_i| \leq 2^n$ for all i. Therefore there are only finitely many possibilities for the polynomial $f(x)$, and hence for α. Applying the same reasoning to α^j for each positive integer j, we see that $\{\alpha, \alpha^2, \alpha^3, \ldots\}$ is a finite set. Therefore there exist positive integers $j < k$ such that $\alpha^j = \alpha^k$, from which it follows that $\alpha^{k-j} = 1$. □

The next lemma is a simple application of the binomial theorem.

LEMMA 2.36. *If $\alpha \in \mathbb{Z}[\zeta_p]$, then there exists an element $a \in \mathbb{Z}$ such that $\alpha^p \equiv a \pmod{p}$.*

PROOF. Write $\alpha = a_0 + a_1\zeta_p + \cdots + a_{p-2}\zeta^{p-2}$. By the binomial theorem, if $\alpha_1, \alpha_2 \in \mathbb{Z}[\zeta_p]$ then $(\alpha_1 + \alpha_2)^p \equiv \alpha_1^p + \alpha_2^p \pmod{p}$. By induction, it follows that a similar statement holds for the sum of n elements for all $n \geq 2$, and in particular

$$\alpha^p \equiv a_0^p + a_1^p\zeta_p^p + \cdots + a_{p-2}^p(\zeta_p^{p-2})^p \pmod{p}.$$

Using Fermat's little theorem and the fact that $\zeta_p^p = 1$, we obtain

$$\alpha^p \equiv a_0 + a_1 + \cdots + a_{p-2} \pmod{p}.$$

Set $a := a_0 + a_1 + \cdots + a_{p-2}$. □

We can now prove the following result due to Kummer:

PROPOSITION 2.37. *Let p be an odd prime number. If $u \in \mathbb{Z}[\zeta_p]$ is a unit, then $u/\overline{u} = \zeta_p^k$ for some integer k.*

PROOF. Let $\alpha := u/\overline{u} \in \mathbb{Z}[\zeta_p] \subset \mathbb{C}$. We claim that all conjugates of α have absolute value 1. To see this, note that for all $\sigma \in \mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})$, we have

$$\overline{\sigma(\alpha)} = \sigma(\overline{\alpha}) = \sigma(\overline{u}/u) = \sigma(\alpha^{-1}) = \sigma(\alpha)^{-1}.$$

In particular,

$$|\sigma(\alpha)|^2 = \sigma(\alpha)\overline{\sigma(\alpha)} = 1$$

as claimed. By Lemma 2.35, it follows that α is a root of unity.

By Lemma 2.33, we must have $\alpha = \pm\zeta_p^k$ for some integer k. We need to show that the plus sign holds. Suppose for the sake of contradiction that $\alpha = u/\overline{u} = -\zeta_p^k$. Then (raising both sides to the pth power) we have $u^p = -\overline{u}^p$. Furthermore, we know from Lemma 2.36 that there exists an integer $a \in \mathbb{Z}$ such that $u^p \equiv a \pmod{p}$. Therefore $\overline{u}^p \equiv a \pmod{p}$ also, and we have $a \equiv -a \pmod{p}$. Since p is odd, this implies that $a \equiv 0 \pmod{p}$, so that $p \mid u^p$. This contradicts the fact that u is a unit. □

COROLLARY 2.38. *If p is an odd prime, then every unit in $\mathbb{Z}[\zeta_p]$ can be written as $r\zeta_p^j$ for some integer $0 \le j \le p-1$, where r is a real number belonging to the field $\mathbb{Q}(\zeta_p)$.*

PROOF. Let u be a unit in $\mathbb{Z}[\zeta_p]$. By Proposition 2.37, we know that $u/\overline{u} = \zeta_p^k$ for some integer k. Choose an integer $0 \le j \le p-1$ such that $2j \equiv k \pmod{p}$. Then $u\zeta_p^{-j} = \overline{u}\zeta_p^j$. Setting $r := u\zeta_p^{-j}$, we have $r = \overline{r}$, i.e., $r \in \mathbb{R}$. Therefore $u = r\zeta_p^j$ with $r \in \mathbb{R}$, as desired. □

We now turn to the "first case" of Fermat's Last Theorem for regular primes. We recall first that if p is a prime number and $\zeta_p = e^{2\pi i/p}$, then $\mathbb{Z}[\zeta_p]$ is the ring of integers in $\mathbb{Q}(\zeta_p)$. Also, since the minimal polynomial of ζ_p is $x^{p-1} + x^{p-2} + \cdots + x^2 + x + 1$, it follows that every element $\alpha \in \mathbb{Z}[\zeta_p]$ can be written *uniquely* in the form

$$\alpha = a_0 + a_1\zeta_p + \cdots + a_{p-2}\zeta_p^{p-2}$$

with $a_i \in \mathbb{Z}$.

A prime p is called *regular* if $p \nmid h_p$, where h_p is the class number of $\mathbb{Z}[\zeta_p]$. Otherwise p is called *irregular*. It can be shown that there are infinitely many irregular primes, the smallest of which is 37. However, heuristics show that "most" primes are regular.

We now prove the first case of Fermat's Last Theorem for regular primes, following Kummer. The case $p = 3$ is easy to handle directly, so we assume in the proof that $p \geq 5$.

THEOREM 2.39 (Kummer). *Suppose $p \geq 5$ is a regular prime. Then the equation $x^p + y^p = z^p$ has no solution in nonzero integers x, y, z with $p \nmid xyz$.*

PROOF. Without loss of generality, we may assume that x, y, z are pairwise relatively prime.

We factor the given equation in $\mathbb{Z}[\zeta_p]$ into ideals:

$$(x + y)(x + y\zeta_p) \cdots (x + y\zeta_p^{p-1}) = (z)^p. \tag{2.4}$$

By Exercise 2.40 below, we know that the ideals on the left-hand side of (2.4) are pairwise relatively prime. Therefore $(x + y\zeta_p) = I^p$ for some ideal I (and similarly for the other terms on the left-hand side of (2.4)). The ideal I has the property that $[I]^p = 1$ in the class group of $\mathbb{Z}[\zeta_p]$. Since p is regular, the order of the class group is not divisible by p. It follows that I is principal, so that

$$x + y\zeta_p = u\alpha^p$$

for some $\alpha \in \mathbb{Z}[\zeta_p]$ and some unit $u \in \mathbb{Z}[\zeta_p]$.

Claim: $x \equiv y \pmod{p}$.

Assume the claim for the moment. By symmetry, since we can also write $x^p + (-z)^p = (-y)^p$, it follows that $x \equiv (-z) \pmod{p}$ as well. But then

$$2x^p \equiv x^p + y^p \equiv z^p \equiv -x^p \pmod{p},$$

so that $p \mid 3x^p$, a contradiction. (We're assuming that we're in the first case, so $p \nmid x$, and also $p > 3$ by assumption.)

So we'll be done once we prove the claim. For this, we note by Lemma 2.36 that there exists $a \in \mathbb{Z}$ such that $x + y\zeta_p \equiv ua^p \pmod{p}$. Noting that $\overline{\zeta_p} = \zeta_p^{-1}$, it follows that $x + y\zeta_p^{-1} \equiv \overline{x + y\zeta_p} \equiv \overline{u}a^p \pmod{p}$. It is easy to see that $p \nmid a$, and it follows that

$$(x + y\zeta_p)\overline{u} \equiv (x + y\zeta_p^{-1})u \pmod{p}.$$

But $u/\overline{u} = \zeta^k$ for some $0 \leq k \leq p - 1$ by Corollary 2.38, so we obtain:

$$x + y\zeta_p \equiv x\zeta_p^k + y\zeta_p^{k-1} \pmod{p}. \tag{2.5}$$

Since every element α of $\mathbb{Z}[\zeta_p]$ is uniquely expressible in the form $\alpha = a_0 + a_1\zeta_p + \cdots + a_{p-2}\zeta_p^{p-2}$, it follows that $p \mid \alpha$ if and only if $p \mid a_i$ for all i.

Since $p \nmid xy$ and $p \geq 5$, it is not hard to see that (2.5) yields a contradiction unless $k = 1$, in which case $x + y\zeta_p \equiv x\zeta_p + y \pmod{p}$. (If $k = p - 1$, it is necessary to first make the substitution $\zeta_p^{p-1} = -(1 + \zeta_p + \cdots + \zeta_p^{p-2})$ in (2.5).) Thus $x \equiv y \pmod{p}$ as claimed. □

EXERCISE 2.40. Show that the ideals $(x + y\zeta_p^i)$ and $(x + y\zeta_p^j)$ are coprime in $\mathbb{Z}[\zeta_p]$ whenever i and j are distinct modulo p.

EXERCISE 2.41. Prove the first case of Fermat's last theorem in the special case $p = 3$.

We see from this argument that it is very useful to understand the structure of the unit group of a number field. A general result known as Dirichlet's unit theorem says that the unit group in a number ring is always a finitely generated abelian group. We will prove Dirichlet's unit theorem later on by utilizing Minkowski's geometry of numbers.

4.3. The cyclotomic field $\mathbb{Q}(\zeta_m)$ for arbitrary m. We seek to generalize the facts we already know concerning $\mathbb{Q}(\zeta_m)$ when m is a prime power to arbitrary positive integers m. To do this, first note that by Theorem 2.31, if $m = p^k$ and $m' = q^{k'}$, with p, q distinct primes, then the discriminants of $K_m, K_{m'}$ are relatively prime.

We will need the following result.

PROPOSITION 2.42. *Let K, K' be number fields of degrees m and m', respectively. Assume that:*

(i) *K and K' are Galois over $\mathbb{Q}$*
(ii) *$K \cap K' = \mathbb{Q}$.*
(iii) *The discriminants d and d' of K and K' are relatively prime.*

If $\alpha_1, \ldots, \alpha_m$ (resp. $\alpha'_1, \ldots, \alpha'_{m'}$) is an integral basis for $\mathcal{O}_K$ (resp. $\mathcal{O}_{K'}$), then $\alpha_i\alpha'_j$ $(1 \leq i \leq m, 1 \leq j \leq m')$ is an integral basis for $\mathcal{O}_{KK'}$.

REMARK 2.43. Let L be an overfield containing both K' and K, and let KK' be the compositum of K and K' in L (i.e., the smallest subfield of L containing both K and K'). Then by Galois theory, the hypothesis $K' \cap K = \mathbb{Q}$ implies that:

(a) KK' is Galois and $[KK' : \mathbb{Q}] = mm'$. In fact, there is a natural isomorphism $\mathrm{Gal}(KK'/\mathbb{Q}) \cong \mathrm{Gal}(K/\mathbb{Q}) \times \mathrm{Gal}(K'/\mathbb{Q})$.
(b) The mm' elements $\alpha_i\alpha'_j$ form a basis for $KK'/\mathbb{Q}$.
(c) There are natural isomorphisms $\mathrm{Gal}(K'/\mathbb{Q}) \cong \mathrm{Gal}(KK'/K)$ and $\mathrm{Gal}(K/\mathbb{Q}) \cong \mathrm{Gal}(KK'/K')$. In particular, $[KK' : K] = m'$ and $[KK' : K'] = m$,
(d) If $\mathrm{Gal}(KK'/K) = \{\sigma'_1, \ldots, \sigma'_{m'}\}$ and $\mathrm{Gal}(KK'/K') = \{\sigma_1, \ldots, \sigma_m\}$, then $\mathrm{Gal}(KK'/\mathbb{Q}) = \{\sigma_k\sigma'_l\}$ $(1 \leq k \leq m, 1 \leq l \leq m')$.

REMARK 2.44. One can show under the hypotheses of the proposition that the discriminant of KK' is $d^{m'}d'^{m}$.

PROOF. Let $\alpha \in \mathcal{O}_{KK'}$ be arbitrary, and write

$$\alpha = \sum_{i,j} a_{ij}\alpha_i\alpha'_j,\ a_{ij} \in \mathbb{Q}.$$

We want to show that each $a_{ij} \in \mathbb{Z}$. We claim first that $da_{ij} \in \mathbb{Z}$ for all i, j.

Assuming the claim for the moment, we show how to conclude. By symmetry (switching the roles of K, K'), we also have $d'a_{ij} \in \mathbb{Z}$ for all i, j. But we are assuming that d and d' are relatively prime, so there exist $s, t \in \mathbb{Z}$ such that $sd + td' = 1$. Therefore $a_{ij} = sda_{ij} + td'a_{ij} \in \mathbb{Z}$ as desired.

We now prove the claim. Set $\beta_j = \sum_{i=1}^{m'} a_{ij}\alpha'_i$ for $j = 1, \ldots, m$ and let T be the $m \times m$ matrix whose $(\ell, j)^{\text{th}}$ entry is $\sigma_\ell(\alpha_j)$, where $\{\sigma_1, \ldots, \sigma_m\} = \mathrm{Gal}(KK'/K')$. Also, set

$$a := \begin{bmatrix} \sigma_1\alpha \\ \vdots \\ \sigma_m(\alpha) \end{bmatrix}, \quad b := \begin{bmatrix} \beta_1 \\ \vdots \\ \beta_m \end{bmatrix}.$$

By Galois theory, the m embeddings of K into $\mathbb{C}$ are just the restrictions of the embeddings $\sigma_1, \ldots, \sigma_n$ to K. Therefore we have $d = \det(T)^2$. Also, we have $a = Tb$. Indeed, the ℓth row of Tb is

$$\begin{aligned} \sum_{j=1}^{m} \sigma_\ell(\alpha_j)\beta_j &= \sum_{\substack{i=1,\ldots,m' \\ j=1,\ldots,m}} \sigma_\ell(\alpha_j)a_{ij}\alpha'_i \\ &= \sum_{\substack{i=1,\ldots,m' \\ j=1,\ldots,m}} \sigma_\ell(\alpha_j a_{ij}\alpha'_i) \\ &= \sigma_\ell(\sum_{i,j} a_{ij}\alpha_j\alpha'_i) \\ &= \sigma_\ell(\alpha) \end{aligned}$$

since $\sigma_\ell \in \mathrm{Gal}(KK'/K')$ fixes K'. Multiplying both sides of this identity by $\mathrm{adj}(T)$, we obtain $\mathrm{adj}(T)a = \det(T)b$. Therefore $\det(T)\mathrm{adj}(T)a = db$. Since the entries of T, $\mathrm{adj}(T)$, and a are all algebraic integers, it follows that the entries of db are also algebraic integers, i.e.,

$$d\beta_j = \sum_i da_{ij}\alpha'_i \in \mathcal{O}_{K'}\ \forall\ j.$$

As the set $\{\alpha_i'\}$ forms an integral basis for $\mathcal{O}_{K'}$, it follows that $da_{ij} \in \mathbb{Z}$ for all i, j, as claimed.

□

We can now prove:

THEOREM 2.45. *Let $m > 1$ be a positive integer and let $K_m = \mathbb{Q}(\zeta_m)$. Let the prime factorization of m be $m = p_1^{k_1} \cdots p_s^{k_s}$. Then:*

(a) *The field K_m is the compositum of the fields $K_{p_i^{k_i}}$ for all i.*
(b) *$[K_m : \mathbb{Q}] = \phi(m)$ and $K_m/\mathbb{Q}$ is Galois with Galois group isomorphic to $(\mathbb{Z}/m\mathbb{Z})^*$.*
(c) *Δ_{K_m} is divisible only by the primes p_i.*
(d) *The ring of integers of K_m is $\mathbb{Z}[\zeta_m]$.*

PROOF. Parts (a) and (b) are proved in Section 14.5 of Dummit and Foote's "Abstract Algebra", along with the fact that if $m = m'm''$ with $m'' = p^k$ and $p \nmid m'$, and if $K' = K_{m'}$ and $K'' = K_{p^k}$, then $K' \cap K'' = \mathbb{Q}$. We refer to Dummit and Foote for those facts, or leave them as exercises for the reader.

Part (c) follows from Lemma 2.30, and in particular, this shows that the discriminants of K' and K'' above are relatively prime. Part (d) now follows by induction from Theorem 2.31 and Proposition 2.42, since

$$\{\zeta_{m'}^i \zeta_{m''}^j\}_{\substack{0 \le i \le \phi(m')-1 \\ 0 \le j \le \phi(m'')-1}} = \{\zeta_m^k\}_{0 \le k \le \phi(m)-1}$$

by the Chinese remainder theorem. □

5. Exercises for Chapter 2

For some of these problems, you may wish to use the following theorem of Minkowski, which will be proved in the next chapter:

Theorem: Let K be a number field. Then every ideal class in $\mathcal{O}_K$ contains a nonzero ideal of norm at most M_K, where

$$M_K := \frac{n!}{n^n}\left(\frac{4}{\pi}\right)^{r_2}\sqrt{|\Delta_K|}$$

is *Minkowski's constant*. (Here $n = [K : \mathbb{Q}]$, Δ_K is the discriminant of K, and r_2 is one-half the number of *complex embeddings* of K. An embedding $\sigma : K \hookrightarrow \mathbb{C}$ is called *real* if $\sigma(K) \subseteq \mathbb{R}$, and *complex* otherwise.)

(1) Let K be a number field, let $\alpha \in K$, and let $T_\alpha : K \to K$ be the linear transformation from the $\mathbb{Q}$-vector space K to itself corresponding to multiplication by α. Show that $\det(T_\alpha) = N_{K/\mathbb{Q}}(\alpha)$.

(2) Let α be an algebraic integer of degree n, and let $f(x)$ be its minimal polynomial over $\mathbb{Q}$. Define the discriminant of α, denoted $\Delta(\alpha)$, to be the discriminant of the basis $\{1, \alpha, \ldots, \alpha^{n-1}\}$ for $\mathbb{Q}(\alpha)/\mathbb{Q}$, and let $\alpha_1, \ldots, \alpha_n$ be the conjugates of α.
   (a) Show that

$$\Delta(\alpha) = (-1)^{\binom{n}{2}} \prod_{i=1}^{n} f'(\alpha_i) = (-1)^{\binom{n}{2}} N_{\mathbb{Q}(\alpha)/\mathbb{Q}}(f'(\alpha)).$$

   (b) Use part (a) to compute the discriminant of α if α is a root of the polynomial $f(x) = x^n + ax + b$, where $a, b \in \mathbb{Z}$ are chosen so that $f(x)$ is irreducible.
   (c) Find an integral basis for the ring of integers of $\mathbb{Q}(\theta)$, where θ is a root of the polynomial $x^3 - 2x + 3$.
   (d) Find an integral basis for the ring of integers of $\mathbb{Q}(\theta)$, where θ is a root of the polynomial $x^3 - x - 4$.

(3) Let K be a number field of degree n, let $\alpha_1, \ldots, \alpha_n \in \mathcal{O}_K$, and let $d = \Delta_{K/\mathbb{Q}}(\alpha_1, \ldots, \alpha_n)$. Show that $d \equiv 0$ or $1 \pmod 4$. In particular, this implies that the discriminant of a number field is congruent to 0 or 1 (mod 4). (**Hint:** Let $\sigma_1, \ldots, \sigma_n$ be as usual. Then the determinant of $(\sigma_i(\alpha_j))$ is a sum of $n!$ terms, one for each permutation of $\{1, \ldots, n\}$. Let P (resp. N) be the sum of the terms corresponding to even (resp. odd) permutations, so that $d = (P - N)^2$. Show that $P + N$ and PN are in $\mathbb{Z}$.)

(4) Let I be a non-zero ideal in a Dedekind ring R. Show that I can be generated by 2 elements. (**Hint:** Let $\alpha \in I$ be arbitrary, and write $I = \prod \mathfrak{p}_i^{a_i}$. Show that $(\alpha) = (\prod \mathfrak{p}_i^{b_i}) \prod \mathfrak{q}_j^{c_j}$ for some $b_i \geq a_i$ and $c_j \geq 1$, and use the Chinese Remainder Theorem to show that there exists $\beta \in R$ such that $\beta \in \mathfrak{p}_i^{a_i} \backslash \mathfrak{p}_i^{a_i+1}$ and $\beta \notin \mathfrak{q}_j$ for all i, j.)

(5) (a) Prove that a Dedekind ring with only finitely many prime ideals is a PID. (**Hint:** Use the Chinese Remainder Theorem to prove that every prime ideal is principal.)
   (b) Deduce from this and the fact that $\mathbb{Z}[\sqrt{-5}]$ is not a UFD an incredibly indirect proof of the fact that there are infinitely many prime numbers in $\mathbb{Z}$.

(6) Factor the ideals $(2), (3), (7), (29)$, and (31) into prime ideals in $R = \mathbb{Z}[\sqrt[3]{2}]$.

(7) Let $K = \mathbb{Q}(\theta)$, where θ is a root of $f(x) = x^3 - 2x - 2$.
   (a) Show that $[K : \mathbb{Q}] = 3$ and that $\mathbb{Z}[\theta]$ is the ring of integers in K.

(b) Show that $\mathrm{Cl}(\mathcal{O}_K)$ is trivial.

(8) Let $K = \mathbb{Q}(\sqrt{-6})$. Determine which rational primes p split, ramify, and remain inert in K. Your answer should be expressed in terms of congruence conditions on p. (**Hint:** Use quadratic reciprocity.)

(9) Let p be a prime, and let a be a squarefree integer which is relatively prime to p. Let $K = \mathbb{Q}(\theta)$, where $\theta = \sqrt[p]{a}$. Show that $\mathcal{O}_K = \mathbb{Z}[\theta]$ if and only if $a^{p-1} \not\equiv 1 \pmod{p^2}$.

(10) Determine the ideal class group of $\mathbb{Z}[\sqrt[3]{2}]$.

(11) Determine the ideal class groups (not just their orders) of:

(a) $\mathbb{Z}[\sqrt{-14}]$.

(b) $\mathbb{Z}[\sqrt{-21}]$.

CHAPTER 3

Geometry of numbers and applications

1. Minkowski's geometry of numbers

1.1. Embedding the ring of integers as a lattice in $\mathbb{R}^n$. In order to enable more efficient computation of the ideal class group, we now introduce a new technique for studying number fields due to Minkowski. It will be a very powerful tool, which will also help us better understand topics as diverse as the discriminant, the group of units, and the zeta function of a number field.

Minkowski's idea is to view the ring of integers in a number field as a lattice in a suitable Euclidean space. Minkowski's lattice embedding is slightly different from the one which we studied earlier. We now explain in detail how this works.

Let K be a number field of degree n with ring of integers $\mathcal{O}_K$. An important role will be played by the n embeddings $\sigma_1, \ldots, \sigma_n$ of K into $\mathbb{C}$. In particular, it is important to divide these embeddings into two categories: the *real embeddings* (those for which $\sigma(K) \subset \mathbb{R}$) and the *complex embeddings* (those for which $\sigma(K) \not\subset \mathbb{R}$). Note that the complex embeddings come in conjugate pairs: if σ is a complex embedding then so is $\overline{\sigma}$. Following the traditional notation, we let r_1 denote the number of real embeddings and r_2 the number of *pairs* of complex embeddings, so that $r_1 + 2r_2 = n$.

Furthermore, we label the embeddings so that $\sigma_1, \ldots, \sigma_{r_1}$ are real, and we let $\tau_1, \ldots, \tau_{r_2}$ consist of one representative from each pair of complex conjugate embeddings.

The basic fact, which will be established below, is that if we embed K into the vector space $\mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$ by the map

$$\alpha \mapsto (\sigma_1(\alpha), \ldots, \sigma_{r_1}(\alpha), \tau_1(\alpha), \ldots, \tau_{r_2}(\alpha))$$

and then identify $\mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$ with $\mathbb{R}^n$ using the isomorphism $\mathbb{C} \cong \mathbb{R}^2$ given by

$$z \mapsto (\mathrm{Re}(z), \mathrm{Im}(z)),$$

then the image of $\mathcal{O}_K$ in $\mathbb{R}^n$ is a *lattice* of rank n.

Recall that a *lattice* of rank n in $\mathbb{R}^n$ is the $\mathbb{Z}$-span of a vector space basis for $\mathbb{R}^n$. (More generally, Λ is a lattice of rank m in $\mathbb{R}^n$ if it can be written as $\Lambda = \mathbb{Z}\beta_1 \oplus \cdots \oplus \mathbb{Z}\beta_m$ with $\beta_1, \ldots, \beta_m$ linearly independent over $\mathbb{R}$.)

Before proving that the image of $\mathcal{O}_K$ in $\mathbb{R}^n$ under the embedding $\iota : K \hookrightarrow \mathbb{R}^n$ described above is a lattice of maximal rank, we first explain why we chose to distinguish one embedding from each complex conjugate pair. Had we not done this, we could have defined a map $\iota' : K \to \mathbb{R}^{r_1} \times \mathbb{C}^{2r_2} \cong \mathbb{R}^{r_1+4r_2} = \mathbb{R}^{n+2r_2}$, but the image of $\mathcal{O}_K$ would clearly not be a lattice of maximal rank, since if $\tau_j(\alpha) = x_j + iy_j$, the coordinates of $\iota'(\alpha)$ would be

$$(\cdots, x_j, y_j, \cdots, x_j, -y_j, \cdots)$$

and therefore $\iota'(K)$ would lie in a linear subspace of codimension $2r_2$ in $\mathbb{R}^{n+2r_2}$.

We now prove:

PROPOSITION 3.1. *The image $\iota(\mathcal{O}_K)$ of $\mathcal{O}_K$ in $\mathbb{R}^n$ is a lattice of rank n.*

PROOF. It suffices to prove that if $\alpha_1, \ldots, \alpha_n$ is an integral basis for $\mathcal{O}_K$, then $\iota(\alpha_1), \ldots, \iota(\alpha_n)$ is a basis for $\mathbb{R}^n$, since the image of $\mathcal{O}_K$ is clearly the $\mathbb{Z}$-span of $\{\iota(\alpha_1), \ldots, \iota(\alpha_n)\}$.

For this, we need to show that the $n \times n$ matrix A obtained by writing out the n column vectors $\{\iota(\alpha_1), \ldots, \iota(\alpha_n)\}$ in terms of their coordinates in $\mathbb{R}^n$ has nonzero determinant.

Explicitly, the determinant of the matrix A is

$$\begin{Vmatrix} \sigma_1(\alpha_1) & \cdots & \sigma_1(\alpha_n) \\ \vdots & & \vdots \\ \sigma_{r_1}(\alpha_1) & \cdots & \sigma_{r_1}(\alpha_n) \\ \mathrm{Re}(\tau_1(\alpha_1)) & \cdots & \mathrm{Re}(\tau_1(\alpha_n)) \\ \mathrm{Im}(\tau_1(\alpha_1)) & \cdots & \mathrm{Im}(\tau_1(\alpha_n)) \\ \vdots & & \vdots \\ \mathrm{Re}(\tau_{r_2}(\alpha_1)) & \cdots & \mathrm{Re}(\tau_{r_2}(\alpha_n)) \\ \mathrm{Im}(\tau_{r_2}(\alpha_1)) & \cdots & \mathrm{Im}(\tau_{r_2}(\alpha_n)) \end{Vmatrix}.$$

By elementary row operations, and viewing A as an $n \times n$ matrix over $\mathbb{C}$, we can relate $\det(A)$ to the discriminant of $\mathcal{O}_K$ as follows.

First, we add $i\mathrm{Im}(\tau_i(\alpha_j))$ to $\mathrm{Re}(\tau_i(\alpha_j))$ to find that $\det(A)$ equals

$$\begin{Vmatrix} \sigma_1(\alpha_1) & \cdots & \sigma_1(\alpha_n) \\ \vdots & & \vdots \\ \sigma_{r_1}(\alpha_1) & \cdots & \sigma_{r_1}(\alpha_n) \\ \tau_1(\alpha_1) & \cdots & \tau_1(\alpha_n) \\ \mathrm{Im}(\tau_1(\alpha_1)) & \cdots & \mathrm{Im}(\tau_1(\alpha_n)) \\ \vdots & & \vdots \\ \tau_{r_2}(\alpha_1) & \cdots & \tau_{r_2}(\alpha_n) \\ \mathrm{Im}(\tau_{r_2}(\alpha_1)) & \cdots & \mathrm{Im}(\tau_{r_2}(\alpha_n)) \end{Vmatrix}.$$

Next, we multiply $\mathrm{Im}(\tau_i(\alpha_j))$ by $-2i$ to find that $(-2i)^{r_2}\det(A)$ equals

$$\begin{Vmatrix} \sigma_1(\alpha_1) & \cdots & \sigma_1(\alpha_n) \\ \vdots & & \vdots \\ \sigma_{r_1}(\alpha_1) & \cdots & \sigma_{r_1}(\alpha_n) \\ \tau_1(\alpha_1) & \cdots & \tau_1(\alpha_n) \\ -2i\mathrm{Im}(\tau_1(\alpha_1)) & \cdots & -2i\mathrm{Im}(\tau_1(\alpha_n)) \\ \vdots & & \vdots \\ \tau_{r_2}(\alpha_1) & \cdots & \tau_{r_2}(\alpha_n) \\ -2i\mathrm{Im}(\tau_{r_2}(\alpha_1)) & \cdots & -2i\mathrm{Im}(\tau_{r_2}(\alpha_n)) \end{Vmatrix}.$$

Finally, we add $\tau_i(\alpha_j)$ to $-2i\mathrm{Im}(\tau_i(\alpha_j))$ and find that $(-2i)^{r_2}\det(A)$ equals

$$\begin{Vmatrix} \sigma_1(\alpha_1) & \cdots & \sigma_1(\alpha_n) \\ \vdots & & \vdots \\ \sigma_{r_1}(\alpha_1) & \cdots & \sigma_{r_1}(\alpha_n) \\ \tau_1(\alpha_1) & \cdots & \tau_1(\alpha_n) \\ \overline{\tau_1}(\alpha_1) & \cdots & \overline{\tau_1}(\alpha_n) \\ \vdots & & \vdots \\ \tau_{r_2}(\alpha_1) & \cdots & \tau_{r_2}(\alpha_n) \\ \overline{\tau_{r_2}}(\alpha_1) & \cdots & \overline{\tau_{r_2}}(\alpha_n) \end{Vmatrix},$$

which equals $\pm|\Delta_K|^{1/2}$, where Δ_K is the discriminant of $\mathcal{O}_K$.

Since $\Delta_K \neq 0$, we find that $|\det(A)| = 2^{-r_2}|\Delta_K|^{1/2} \neq 0$ as desired. □

Given a lattice Λ in $\mathbb{R}^n$ of rank n, we define a *fundamental domain* for Λ to be a set of the form

$$F := \{\sum_{j=1}^{n} a_j v_j \ : \ a_j \in \mathbb{R}, 0 \leq a_j < 1\},$$

where $v_1, \ldots, v_n$ is a $\mathbb{Z}$-basis for Λ. It is easy to see that given any $x \in \mathbb{R}^n$, there exists a unique point $x' \in F$ such that $x - x' \in \Lambda$. In other words, there is a unique translate of x by a lattice point which lies in the given fundamental domain.

Since F is always a a parallelotope in $\mathbb{R}^n$, it follows from multivariable calculus that the n-dimensional Euclidean volume of F is the absolute value of the determinant formed by the coordinates of $v_1, \ldots, v_n$. Moreover, it follows from linear algebra that any two $\mathbb{Z}$-bases for Λ give rise to the same determinant (up to ± 1). Therefore it makes sense to define the *covolume* of a lattice Λ, written $\mathrm{covol}(\Lambda)$ or $\mathrm{vol}(\mathbb{R}^n/\Lambda)$, to be the volume of any fundamental domain for Λ.

As a corollary of the above proof, we note the following important calculation:

COROLLARY 3.2. *If $\Lambda = \iota(\mathcal{O}_K)$, then* $\mathrm{vol}(\mathbb{R}^n/\Lambda) = 2^{-r_2}\sqrt{|\Delta_K|}$.

If Λ is a rank n lattice in $\mathbb{R}^n$ and Λ' is a $\mathbb{Z}$-submodule of Λ of rank n, then it is easy to see that Λ' is also a rank n lattice in $\mathbb{R}^n$, and by the structure theorem for finitely generated abelian groups (Theorem A.11),

$$\mathrm{vol}(\mathbb{R}^n/\Lambda') = [\Lambda : \Lambda']\mathrm{vol}(\mathbb{R}^n/\Lambda).$$

Applying these remarks to the image in $\mathbb{R}^n$ of an ideal I of $\mathcal{O}_K$, we find:

COROLLARY 3.3. *If I is an ideal of $\mathcal{O}_K$, then*

$$\mathrm{vol}(\mathbb{R}^n/\iota(I)) = 2^{-r_2}\sqrt{|\Delta_K|}N(I).$$

Now recall from §3.4 that the key to proving the finiteness of the class number is to find a constant M such that every ideal I of $\mathcal{O}_K$ contains an element α such that $|N(\alpha)| \leq M \cdot N(I)$. Moreover, the smaller the value of M the better for the purpose of estimating the class number of $\mathcal{O}_K$.

With our new geometric picture in mind, we see that if we define a norm function on $\mathbb{R}^n = \mathbb{R}^{r_1+2r_2}$ by setting

$$N(a_1, a_2, \ldots, a_{r_1}, x_1, y_1, x_2, y_2, \ldots, x_{r_2}, y_{r_2}) = \\ a_1 a_2 \cdots a_{r_1}(x_1^2 + y_1^2)(x_2^2 + y_2^2)\cdots(x_{r_2}^2 + y_{r_2}^2),$$

then for all $\alpha \in K$, we have $N_{K/\mathbb{Q}}(\alpha) = N(\iota(\alpha))$. In other words, the function N on $\mathbb{R}^n$ is compatible with the norm function on K under the embedding ι.

This allows us to view the norm on $\mathcal{O}_K$ geometrically in terms of the function N restricted the lattice Λ. Minkowski's brilliant idea was to prove a general result (the convex body lemma) about lattices in

Euclidean space which implies a much sharper version of the key result used for proving the finiteness of the class number. We will discuss this result and its applications next.

1.2. Minkowski's convex body theorem. Let S be a subset of $\mathbb{R}^n$. We say that S is *convex* if whenever $x, y \in S$, all points on the line segment joining x and y are also in S. More formally, S is convex if $x, y \in S$ implies $\lambda x + (1-\lambda)y \in S$ for all real numbers $\lambda \in [0,1]$.

We call S *symmetric* if it is symmetric with respect to reflection across the origin. In other words, S is symmetric if $x \in S$ implies $-x \in S$.

We will need to use some properties of volumes of convex sets in $\mathbb{R}^n$. For our purposes, we just need to know that every convex set is *measurable*, i.e., it has a well-defined volume. The reader who is not familiar with measure theory should take on faith the following facts:

There is a large class $\mathbf{M}$ of bounded subsets of $\mathbb{R}^n$, called (Lebesgue) *measurable* sets, containing all convex sets, such that:

- If $A \in M$ then the volume $\mathrm{vol}(A)$ is well-defined.
- If A is a convex set, then the volume of A coincides with the volume as defined by the Riemann integral.
- If A is a finite (or more generally countable) disjoint union of measurable sets A_i, then A is measurable and $\mathrm{vol}(A) = \sum \mathrm{vol}(A_i)$.
- If $A \subseteq B$ are measurable sets, then $\mathrm{vol}(A) \leq \mathrm{vol}(B)$.

Let $S \subset \mathbb{R}^n$ be a bounded measurable set. We say that $T : S \to \mathbb{R}^n$ is *piecewise volume-preserving* if S can be written as a finite disjoint union of measurable subsets S_i such that $\mathrm{vol}(T(S_i)) = \mathrm{vol}(S_i)$ for all i.

The following result is a geometric analogue of the pigeonhole principle:

LEMMA 3.4. *Let $S \subset \mathbb{R}^n$ be a bounded measurable set, and suppose that $T : S \to \mathbb{R}^n$ is piecewise volume-preserving. If $\mathrm{vol}(S) > \mathrm{vol}(T(S))$, then T is not injective.*

PROOF. If T is injective, then $T(S)$ is the disjoint union of the sets $T(S_i)$, and therefore

$$\mathrm{vol}(T(S)) = \sum_i \mathrm{vol}(T(S_i)) = \sum_i \mathrm{vol}(S_i) = \mathrm{vol}(S).$$

□

EXERCISE 3.5. Let F be a fundamental domain for a lattice Λ in $\mathbb{R}^n$, and consider the map $T : \mathbb{R}^n \to F$ which sends $z \in \mathbb{R}^n$ to the unique

point $T(z) \in F$ such that $z - T(z) \in \Lambda$. Show that T is a piecewise translation, and in particular T is piecewise volume-preserving.

The following famous result of Minkowski gives conditions which guarantee the existence of nonzero elements of a given lattice Λ inside a given convex symmetric set S.

THEOREM 3.6 (Minkowski's Convex Body Theorem). *Let $\Lambda \subset \mathbb{R}^n$ be a rank n lattice, and let $S \subset \mathbb{R}^n$ be a bounded, convex, symmetric set. If*

$$\operatorname{vol}(S) > 2^n \operatorname{vol}(\mathbb{R}^n/\Lambda),$$

then S contains a nonzero element of Λ. If S is compact, then the same conclusion holds with the weaker hypothesis

$$\operatorname{vol}(S) \geq 2^n \operatorname{vol}(\mathbb{R}^n/\Lambda).$$

REMARK 3.7. The constant 2^n in the lemma is sharp, as shown by the example of the standard lattice $\mathbb{Z}^n$ in $\mathbb{R}^n$ spanned by $e_1, \ldots, e_n$ together with $S = \{a_1 e_1 + \cdots + a_n e_n \ : \ a_j \in (-1, 1)\}$.

PROOF. We will prove just the first part, and leave the proof of the second part of the theorem (the compact case) as an exercise.

Suppose that $\operatorname{vol}(S) > 2^n \operatorname{vol}(\mathbb{R}^n/\Lambda)$. Consider the lattice

$$\Lambda' = 2\Lambda = \{2x \in \mathbb{R}^n \ : \ x \in \Lambda\} \subset \Lambda.$$

By our previous remarks, we have $\operatorname{vol}(\mathbb{R}^n/\Lambda') = 2^n \operatorname{vol}(\mathbb{R}^n/\Lambda)$.

Let F' be a fixed fundamental domain for Λ', and consider the map $T : \mathbb{R}^n \to F'$ which sends $z \in \mathbb{R}^n$ to the unique point $T(z) \in F'$ such that $z - T(z) \in \Lambda'$. By Exercise 3.5, the map T is a piecewise volume-preserving.

Since $\operatorname{vol}(S) > \operatorname{vol}(F') \geq \operatorname{vol}(T(S))$ by hypothesis, it follows from Lemma 3.4 that the restriction of T to the set S is not injective. Therefore there exist distinct points $x', y' \in S$ such that $T(x') = T(y')$.

In particular, it follows that $P' := x' - y'$ is a nonzero element of Λ'. Write $P' = 2P$ with P a nonzero element of Λ. Since S is symmetric, $-y'$ is in S, and since S is convex, we find that $P = \frac{1}{2}P' = \frac{1}{2}x' + \frac{1}{2}(-y')$ is also in S. Therefore P is a nonzero element of $S \cap \Lambda$, as desired. $\square$

EXERCISE 3.8. Let $\Lambda \subset \mathbb{R}^n$ be a rank n lattice, and let $S \subset \mathbb{R}^n$ be a compact, convex, and symmetric set. If

$$\operatorname{vol}(S) \geq 2^n \operatorname{vol}(\mathbb{R}^n/\Lambda).$$

prove that S contains a nonzero element of Λ.

We would like to apply Minkowski's theorem to the study of ideal classes in $\mathcal{O}_K$. For this, we want to find a symmetric, convex, compact set S contained in the set $\{x \in \mathbb{R}^n \ : \ |N(x)| \leq 1\}$, where N is the norm function on $\mathbb{R}^n$ defined above. If we do that, then we can apply Minkowski's theorem to the homogeneously expanding region $\{tS \ : \ t > 0\}$ as follows:

PROPOSITION 3.9. *Suppose S is a symmetric, convex, compact set contained in $\{x \in \mathbb{R}^n \ : \ |N(x)| \leq 1\}$. Then for each nonzero ideal I in $\mathcal{O}_K$, there exists a nonzero element $\alpha \in I$ such that*

$$|N(\alpha)| \leq \frac{2^n 2^{-r_2}\sqrt{|\Delta_K|}}{\mathrm{vol}(S)} N(I) \ .$$

PROOF. Consider the region tS for real $t > 0$; it is bounded, symmetric, and convex, its volume is $t^n \,\mathrm{vol}(S)$, and since $N(tx) = t^n N(x)$, tS is contained in the set $\{x \in \mathbb{R}^n \ : \ |N(x)| \leq t^n\}$. If we choose the real number t so that $t^n \,\mathrm{vol}(S) = 2^n \,\mathrm{vol}(\mathbb{R}^n/\iota(I))$, then by Minkowski's theorem tS contains a nonzero element of $\iota(I)$. It follows that there exists a nonzero element $\alpha \in I$ such that $|N(\alpha)| \leq t^n$. Since $\mathrm{vol}(\mathbb{R}^n/\iota(I)) = 2^{-r_2}\sqrt{|\Delta_K|}N(I)$, this gives the desired upper bound for $|N(\alpha)|$. $\square$

It is pretty clear that such a set S exists: for example, take S to be any sufficiently small closed ball around the origin in $\mathbb{R}^n$. This already gives another proof of the finiteness of the class number. However, for applications we would like to find a set S as above having as large a volume as possible. The first obvious candidate for a set contained in $H := \{x \in \mathbb{R}^n \ : \ |N(x)| \leq 1\}$ is the set H itself. Explicitly, we have:

$$H = \{x = (a_1, \ldots, a_{r_1}, x_1, y_1, \ldots, x_{r_2}, y_{r_2}) \in \mathbb{R}^n \ : \\ |a_1 \cdots a_{r_1}(x_1^2 + y_1^2) \cdots (x_{r_2}^2 + y_{r_2}^2)| \leq 1\}.$$

Unfortunately, however, the set H is in general neither bounded nor convex. For example, consider the case where K is a real quadratic field. Then $r_1 = 2, r_2 = 0$, and $H = \{(a, b) \in \mathbb{R}^2 \ : \ |ab| \leq 1\}$. This is the region in $\mathbb{R}_2$ bounded by the hyperbolas $xy = 1$ and $xy = -1$, which is clearly not bounded or convex. However, the diamond-shaped region $D := \{(a, b) \in \mathbb{R}^2 \ : \ |a| + |b| \leq 2\}$ is contained in H, and it **is** bounded and convex! Geometrically, this is clear if you graph the two regions that $D \subseteq H$. To see this algebraically, we can use the inequality between the geometric and arithmetic means: since $\sqrt{xy} \leq (x + y)/2$ for all nonnegative real numbers x, y, we have (for $(a, b) \in D$):

$$|ab| \leq \frac{(|a| + |b|)^2}{4} \leq \frac{4}{4} = 1.$$

We can use a similar idea in general to produce a suitable region S. In fact, define

$$S = \{x = (a_1, \dots, a_{r_1}, x_1, y_1, \dots, x_{r_2}, y_{r_2}) \in \mathbb{R}^n \ : \\ |a_1| + \cdots + |a_{r_1}| + 2(\sqrt{x_1^2 + y_1^2} + \cdots + \sqrt{x_{r_2}^2 + y_{r_2}^2}) \leq n\}.$$

The set S is clearly symmetric and compact. In addition:

EXERCISE 3.10. Show that S is convex.

Since for all $x \in S$ the average of

$$|a_1|, \dots, |a_{r_1}|, \sqrt{x_1^2 + y_1^2}, \sqrt{x_1^2 + y_1^2}, \dots, \sqrt{x_{r_2}^2 + y_{r_2}^2}, \sqrt{x_{r_2}^2 + y_{r_2}^2}$$

is at most 1, it follows by the arithmetic-geometric mean inequality that $|N(x)| \leq 1$ for all $x \in S$ as desired.

It remains to use some basic tools from multivariable calculus to compute the volume of S:

LEMMA 3.11. *The volume of S is*

$$\frac{n^n}{n!} 2^{r_1} (\frac{\pi}{2})^{r_2}.$$

Assuming this calculation, we state the big final result as follows.

THEOREM 3.12. *Let K be a number field. Then every ideal class in $\mathcal{O}_K$ contains a nonzero ideal of norm at most M_K, where*

$$M_K := \frac{n!}{n^n} (\frac{4}{\pi})^{r_2} \sqrt{|\Delta_K|}.$$

is Minkowski's constant.

PROOF. We calculate that

$$\frac{2^n 2^{-r_2} \sqrt{|\Delta_K|}}{\frac{n^n}{n!} 2^{r_1} (\frac{\pi}{2})^{r_2}} = \frac{n!}{n^n} (\frac{4}{\pi})^{r_2} \sqrt{|\Delta_K|},$$

and then apply Proposition 3.9. □

Theorem 3.12 is an extremely useful result, primarily because $\frac{n!}{n^n} (\frac{4}{\pi})^{r_2}$ goes to zero rapidly as n increases. The constant M_K, obtained by geometric methods, represents a substantial improvement over the previous value of M obtained using the pigeonhole principle applied to linear combinations of an integral basis. For example, if $K = \mathbb{Q}(\sqrt{-5})$, we previously showed that every ideal class contains a nonzero ideal of norm at most 10, and by working with the primes above $2, 3, 5, 7$, we

were able to show that K has class number 2. Applying the Minkowski bound instead, we find that

$$M_K = \frac{2!}{2^2}(\frac{4}{\pi})\sqrt{|20|} = \frac{4\sqrt{5}}{\pi} < 3,$$

so every ideal class contains a nonzero ideal of norm at most 2. It follows that we only have to check that the prime above 2 is non-principal (which is simple) in order to conclude that K has class number 2.

We conclude this section with another useful consequence of Theorem 3.12. Since every nonzero ideal in a number ring has norm at least 1, Minkowski's constant M_K must be at least 1, and thus we can deduce from Theorem 3.12 the following result:

COROLLARY 3.13 (Minkowski's discriminant bound). *If K is a number field, then*

$$\sqrt{|\Delta_K|} \geq (\frac{\pi}{4})^{r_2}\frac{n^n}{n!} \ .$$

An elementary induction argument shows that $r_2 \leq n/2$ and $n^n/n! \geq 2^{n-1}$ for all $n \geq 2$. Therefore for $n \geq 2$ we have

$$\sqrt{|\Delta_K|} \geq (\frac{\pi}{4})^{n/2}2^{n-1} = \pi^{n/2}/2 \geq \pi/2 > 1 \ ,$$

from which we can deduce:

COROLLARY 3.14. *If $K \neq \mathbb{Q}$ is a number field, then $|\Delta_K| \geq 2$.*

One can show that $p \mid \Delta_K$ iff p is ramified in $\mathcal{O}_K$. (This was proved in the special case where $\mathcal{O}_K$ is monogenic in Corollary 2.20.) Therefore Corollary 3.14 implies the important fact that in any number field $K \neq \mathbb{Q}$, there is some prime number p which ramifies in $\mathcal{O}_K$.

1.3. A volume computation. We now finish the proof of Theorem 3.12 by establishing Lemma 3.11.

PROOF. It suffices to prove that if

$$S_{r_1,r_2} := \{x = (a_1, \ldots, a_{r_1}, x_1, y_1, \ldots, x_{r_2}, y_{r_2}) \in \mathbb{R}^n \ : \\ |a_1| + \cdots + |a_{r_1}| + 2(\sqrt{x_1^2 + y_1^2} + \cdots + \sqrt{x_{r_2}^2 + y_{r_2}^2}) \leq 1\},$$

then

$$V_{r_1,r_2} := \mathrm{vol}(S_{r_1,r_2}) = \frac{2^{r_1}}{n!}(\frac{\pi}{2})^{r_2}.$$

For this, we note that

$$V_{r_1,r_2} = \int_{R_1} da_1 \cdots da_{r_1} dx_1 dy_1 \cdots dx_{r_2} dy_{r_2},$$

where

$$R_1 := \{|a_1| + \cdots + |a_{r_1}| + 2(\sqrt{x_1^2 + y_1^2} + \cdots + \sqrt{x_{r_2}^2 + y_{r_2}^2}) \leq 1\}.$$

We now change each pair (x_j, y_j) to polar coordinates (u_j, θ_j) with $0 \leq \theta_j \leq 2\pi$ and $u_j \geq 0$ to obtain

$$\begin{aligned} V_{r_1,r_2} &= \int_{R_2} u_1 \cdots u_{r_2} da_1 \cdots da_{r_1} du_1 \cdots du_{r_2} d\theta_1 \cdots d\theta_{r_2} \\ &= (2\pi)^{r_2} \int_{R_2} u_1 \cdots u_{r_2} da_1 \cdots da_{r_1} du_1 \cdots du_{r_2}, \end{aligned}$$

where

$$R_2 := \{|a_1| + \cdots + |a_{r_1}| + 2u_1 + \cdots + 2u_{r_2} \leq 1,\ u_j \geq 0\ \forall j\}.$$

If we change the region of integration to

$$R_3 := \{a_1 + \cdots + a_{r_1} + 2u_1 + \cdots + 2u_{r_2} \leq 1,\ a_j, u_j \geq 0\ \forall j\},$$

so that the a_j's are required to be positive, then the integral over R_2 is 2^{r_1} times the integral over R_3. If we furthermore make the change of variables $2u_j = w_j$ for $j = 1, \ldots, r_2$ (so that $u_j = (1/2)w_j$ and $du_j = (1/2)dw_j$), then we obtain

$$V_{r_1,r_2} = 2^{r_1} 4^{-r_2} (2\pi)^{r_2} W_{r_1,r_2}(1),$$

where

$$W_{r_1,r_2}(t) = \int_{R_4(t)} w_1 \cdots w_{r_2} da_1 \cdots da_{r_1} dw_1 \cdots dw_{r_2}$$

and

$$R_4(t) := \{a_1 + \cdots + a_{r_1} + w_1 + \cdots + w_{r_2} \leq t,\ a_j, w_j \geq 0\ \forall j\}.$$

It suffices, then, to show that $W_{r_1,r_2}(1) = \frac{1}{n!}$.

Note that by homogeneity, $W_{r_1,r_2}(t) = t^{r_1+2r_2} W_{r_1,r_2}(1)$. If $r_1 > 0$ then as a_1 ranges from 0 to 1 in $R_4(1)$, the sum $a_2 + \cdots + a_{r_1} + w_1 + \cdots + w_{r_2}$ ranges from 0 to $1 - a_1$. Therefore

$$W_{r_1,r_2}(1) = \int_0^1 W_{r_1-1,r_2}(1 - u_1) du_1,$$

which by homogeneity is

$$W_{r_1-1,r_2}(1) \int_0^1 (1 - u_1)^{r_1+2r_2-1} du_1 = \frac{1}{r_1 + 2r_2} W_{r_1-1,r_2}(1).$$

By induction, we obtain (letting $n = r_1 + 2r_2$)

$$W_{r_1,r_2}(1) = \frac{1}{n(n-1)\cdots(n - r_1 + 1)} W_{0,r_2}(1).$$

Similarly, we have

$$\begin{aligned} W_{0,r_2}(1) &= \int_0^1 W_{0,r_2-1}(1-u_1)u_1 du_1 \\ &= W_{0,r_2-1}(1)\int_0^1 (1-u_1)^{2r_2-2}u_1 du_1 \\ &= \frac{1}{(2r_2)(2r_2-1)} W_{0,r_2-1}(1), \end{aligned}$$

so that by induction we find

$$W_{0,r_2}(1) = \frac{1}{(2r_2)!}W_{0,0}(1) = \frac{1}{(2r_2)!}.$$

Therefore

$$W_{r_1,r_2}(1) = \frac{1}{n(n-1)\cdots(n-r_1+1)}\frac{1}{(2r_2)!} = \frac{1}{n!}$$

as desired. □

1.4. Application: Representing integers as the sum of four squares. Our goal in this section is to use Minkowski's theorem to prove a famous theorem of Lagrange which asserts that every positive integer is a sum of four integer squares. As a warm-up, we give a new proof of Fermat's theorem that every prime congruent to 1 modulo 4 is a sum of two squares.

THEOREM 3.15. *If $p \equiv 1 \pmod 4$ is prime, then there exist $a, b \in \mathbb{Z}$ such that $a^2 + b^2 = p$.*

PROOF. From elementary number theory, we know that the equation $x^2 \equiv -1 \pmod p$ has an integer solution u. Let $\Lambda \subset \mathbb{Z}^2$ be the lattice in $\mathbb{R}^2$ consisting of all pairs $(a, b) \in \mathbb{Z}$ such that $b \equiv au \pmod p$. An easy computation (see Exercise 3.18(a) below) shows that $\mathrm{covol}(\Lambda) = p$. By Minkowski's theorem, if $\pi r^2 = 4p$ then the closed disk of radius r centered at the origin in $\mathbb{R}^2$ contains a nonzero element of Λ. So there exists a point $(a, b) \in \Lambda$ such that

$$0 \neq a^2 + b^2 \leq r^2 = \frac{4}{\pi}p < 2p\ .$$

Since

$$a^2 + b^2 \equiv a^2 + a^2u^2 \equiv 0 \pmod p\ ,$$

it follows that $a^2 + b^2 = p$ as desired. □

We now apply a similar argument to prove Lagrange's theorem. We begin with the following lemma:

LEMMA 3.16. *If p is an odd prime, then the congruence $x^2+y^2 \equiv -1 \pmod p$ has a solution $(u, v) \in \mathbb{Z}^2$.*

PROOF. Counting 0, there are $(p+1)/2$ squares in $\mathbb{F}_p$. Letting $A = \{1 + x^2 : x \in \mathbb{F}_p\}$ and $B = \{-y^2 : y \in \mathbb{F}_p\}$, we have $|A| + |B| = p + 1 > p$, and therefore $A \cap B \neq \emptyset$. □

THEOREM 3.17. *Every positive integer n is a sum of four integer squares.*

PROOF. It suffices to consider the case where $n = p$ is prime, thanks to the identity

$$\begin{aligned}(a^2+b^2+c^2+d^2)(A^2+B^2+C^2+D^2)\\ = (aA-bB-cC-dD)^2 + (aB+bA+cD-dC)^2\\ +(aC-bD+cA+dB)^2 + (aD+bC-cB+dA)^2\ .\end{aligned}$$

(Conceptually, this identity comes from the fact that the norm of a product of two Hamilton quaternions is the product of their norms.)

Since $2 = 1^2 + 1^2 + 0^2 + 0^2$, we may assume that p is odd. By Lemma 3.16, we may choose $(u, v) \in \mathbb{Z}^2$ such that $u^2 + v^2 \equiv -1 \pmod{p}$. Let $\Lambda \subset \mathbb{Z}^4$ be the lattice in $\mathbb{R}^4$ consisting of all $(a, b, c, d) \in \mathbb{Z}^4$ such that

$$c \equiv ua + vb \quad d \equiv ub - va \qquad (\text{mod } p)\ .$$

By Exercise 3.18(b), we have $\text{covol}(\Lambda) = p^2$. If B_r is the 4-dimensional closed ball of radius r centered around the origin in $\mathbb{R}^4$, then by Exercise 3.18(c) we have $\text{vol}(B_r) = \pi^2 r^4/2$. By Minkowski's theorem, if r is chosen so that $\pi^2 r^4/2 = 16p^2$, then B_r contains a nonzero element (a, b, c, d) of Λ. Since

$$0 \neq a^2 + b^2 + c^2 + d^2 \leq r^2 = \frac{4\sqrt{2}}{\pi} p < 2p$$

and

$$a^2 + b^2 + c^2 + d^2 \equiv a^2 + b^2 + (ua + vb)^2 + (ub - va)^2 \equiv 0 \pmod{p}\ ,$$

it follows as before that $a^2 + b^2 + c^2 + d^2 = p$. □

EXERCISE 3.18. Let p be a prime number.

(a) Let u be an integer relatively prime to p, and define $\Lambda \subset \mathbb{Z}^2$ to be the lattice in $\mathbb{R}^2$ consisting of all pairs $(a, b) \in \mathbb{Z}^2$ such that $b \equiv au \pmod{p}$. Show that $\text{covol}(\Lambda) = p$.

(b) Let $\Lambda \subset \mathbb{Z}^4$ be the lattice in $\mathbb{R}^4$ consisting of all $(a, b, c, d) \in \mathbb{Z}^4$ such that

$$c \equiv ua + vb \quad d \equiv ub - va \qquad (\text{mod } p)\ .$$

Show that $\text{covol}(\Lambda) = p^2$.

(c) Show that the volume of a ball of radius r in $\mathbb{R}^4$ is $\pi^2 r^4/2$.

2. Dirichlet's Unit Theorem

2.1. Statement of Dirichlet's theorem. Dirichlet's unit theorem tells us the structure of the unit group in a general number field. Recall that if K is a number field, then r_1 (resp. r_2) denotes the number of real (resp. half the number of complex) embeddings of K into $\mathbb{C}$. Dirichlet's result is the following:

THEOREM 3.19 (Dirichlet's Unit Theorem). *Let K be a number field, and let $\mathcal{O}_K^*$ be the group of units in $\mathcal{O}_K$. Then $\mathcal{O}_K^*$ is a finitely generated abelian group. More precisely, let W_K denote the group of roots of unity contained in K. Then W_K is a finite cyclic group, and $\mathcal{O}_K^* \cong W_K \times \mathbb{Z}^{r-1}$, where $r = r_1 + r_2$.*

We give some concrete examples of Dirichlet's theorem.

EXAMPLE 3.20. If K is an imaginary quadratic field, then $r_1 = 0, r_2 = 1$, so that $r - 1 = 0$ and therefore $\mathcal{O}_K^* = W_K$ is a finite group.

This agrees with what we already know from studying the norm function on K: the unit group in an imaginary quadratic field $K = \mathbb{Q}(\sqrt{d})$, with $d < 0$ a squarefree integer, is:

$$\begin{array}{ll} \mathcal{O}_K^* = \{\pm 1, \pm i\} & d = -1 \\ \mathcal{O}_K^* = \{\pm 1, \pm\omega, \pm\omega^2\} & d = -3 \\ \mathcal{O}_K^* = \{\pm 1\} & d \leq -5 \end{array}$$

EXAMPLE 3.21. If K is a real quadratic field, then we must have $W = \{\pm 1\}$, since ± 1 are the only roots of unity in $\mathbb{R}$. Also, we have $r_1 = 2, r_2 = 0$, so that $r - 1 = 1$. Therefore Dirichlet's theorem implies that $\mathcal{O}_K^* = \{\pm 1\} \times \mathbb{Z}$. In particular, there exists a unit $u \in \mathcal{O}_K^*$ such that $\mathcal{O}_K^* = \{\pm u^m \ : \ m \in \mathbb{Z}\}$. If we fix an embedding of K into $\mathbb{R}$, then u is uniquely determined by requiring that $u > 1$. This generator of $\mathcal{O}_K^*$ is called the *fundamental unit* of K.

For example, let $K = \mathbb{Q}(\sqrt{2})$. (By thinking of $\sqrt{2}$ as the *positive* square root of 2, we have secretly fixed an embedding of K into $\mathbb{R}$.) We claim that the fundamental unit of K is then $u = 1 + \sqrt{2}$, so that every element of $\mathcal{O}_K^*$ can be written uniquely as $\pm u^k$ with $k \in \mathbb{Z}$.

It is clear that u is a unit of $\mathcal{O}_K$, since $\sqrt{2} - 1$ is an inverse for u. It is also clear that u is not a root of unity, since (for example) it does not have absolute value 1. It remains to show that every positive unit in $\mathcal{O}_K$ is a power of u. Assuming Dirichlet's unit theorem, it is easily checked that this is equivalent to proving that if v is any unit of $\mathcal{O}_K$ with $v > 1$ then $v \geq u$.

For this, suppose $v > 1$ is a unit, and write $v = a + b\sqrt{2}$ with $a, b \in \mathbb{Z}$. Let $\tau : K \to \mathbb{R}$ be the embedding sending $\sqrt{2}$ to $-\sqrt{2}$. Then

$a^2 - 2b^2 = (a + b\sqrt{2})(a - b\sqrt{2}) = \pm 1$. Suppose that $a^2 - 2b^2 = 1$. Then we must have $0 < \tau(v) = a - b\sqrt{2} < 1$. Since $a + b\sqrt{2} > 1$ and $a - b\sqrt{2} > 0$, it follows that $a \geq 1$. And since $a - b\sqrt{2} < 1$, we must have $b \geq 1$, and thus $v \geq u$.

Similarly suppose $a^2 + 2b^2 = -1$. Then $-1 < a - b\sqrt{2} < 0$. The inequalities $a - b\sqrt{2} > -1$ and $a + b\sqrt{2} > 1$ imply that $a \geq 1$, and then $a - b\sqrt{2} < 0$ implies that $b \geq 1$. So again, we must have $v \geq u = 1 + \sqrt{2}$, as claimed.

EXERCISE 3.22. If $K = \mathbb{Q}(\sqrt{d})$ is a real quadratic field with d squarefree, show that the units of K are in bijection with the set of integer solutions to the *Pell equation*

$$\begin{aligned} a^2 - db^2 &= \pm 1 \quad d \equiv 2, 3 \pmod 4 \\ a^2 - db^2 &= \pm 4 \quad d \equiv 1 \pmod 4. \end{aligned}$$

By the previous exercise, Dirichlet's unit theorem gives us information about the solutions to Pell equations. For example, it follows from Dirichlet's theorem that $a^2 - db^2 = 1$ is always solvable in integers when $d \equiv 2, 3 \pmod 4$ is a positive squarefree integer. In addition, Dirichlet's theorem tells us that every solution to this equation can be derived in a simple way from a single fundamental solution. Note, however, that Dirichlet's theorem by itself does not provide us with a way to determine, for example, whether or not the equation $a^2 - db^2 = -1$ has a solution. The rules which govern whether the fundamental unit in K has norm $+1$ or -1 turn out to be rather subtle.

EXAMPLE 3.23. If $K = \mathbb{Q}(\zeta_m)$ is a cyclotomic field, then we have already determined W_K; it consists of the group of all m^{th} roots of unity when m is even, and the group of all $2m^{\text{th}}$ roots of unity when m is odd. The field K clearly has no real embeddings when $m > 2$, so we have $r_1 = 0, r_2 = \phi(m)/2$. Therefore the rank of the unit group of K is $r - 1 = \phi(m)/2 - 1$. Where do all these units come from?

Suppose, for simplicity, that $m = p^k$ is a prime power, and consider the subgroup C of $\mathcal{O}_K^*$ generated by W_K and

$$\{\frac{1 - \zeta_m^a}{1 - \zeta_m},\ 1 \leq a \leq (p-1), (a, p) = 1\}.$$

We leave it as an exercise to show that the elements of C are indeed units. It is not hard to show that C is a finitely generated abelian group of rank at most $\phi(m)/2 - 1$, called the group of *cyclotomic units* in K. What is in fact true, but is harder to prove, is that C has rank exactly $\phi(m)/2 - 1$, so that C in fact has finite index in $\mathcal{O}_K^*$. In general, one has $[\mathcal{O}_K^* : C] > 1$, which is an indication that units in cyclotomic fields are

rather complicated objects. A lot of beautiful and deep mathematics has been developed to try to understand the situation more completely – see, for example, Larry Washington's book "Cyclotomic Fields".

2.2. Lattices and logarithmic space. In order to prove Dirichlet's unit theorem, we need to establish a geometric setting for the problem to which Minkowski's convex body theorem will apply. Our previous method of embedding $\mathcal{O}_K$ as a lattice in the "Minkowski space" $\mathbb{R}^n$ is very beautiful, but it sheds no direct light on the structure of the unit group. This is because we were embedding $\mathcal{O}_K$ as a subgroup of the *additive group* of K into Minkowski space, but the unit group $\mathcal{O}_K^*$ is a subgroup of the *multiplicative group* of K. Therefore, in order to apply geometric methods to the current problem, we need to find a multiplicative analogue of our previous embedding.

This is accomplished as follows. As before, let $\sigma_1, \ldots, \sigma_{r_1}$ denote the real embeddings of K into $\mathbb{C}$, and let $\tau_1, \ldots, \tau_{r_2}$ be complex embeddings, consisting of one representative from each complex conjugate pair. We define a map $L : K^* \to \mathbb{R}^r$ by

$$L(\alpha) := (\log|\sigma_1(\alpha)|, \ldots, \log|\sigma_{r_1}(\alpha)|, \log|\tau_1(\alpha)|^2, \ldots, \log|\tau_{r_2}(\alpha)|^2).$$

It is easy to verify that L is a group homomorphism. We call the image space $\mathbb{R}^r$ "logarithmic space" (as opposed to Minkowski space). The reason for squaring the absolute values of the $\tau_j(\alpha)$'s is that it implies the following identity:

$$\log|N(\alpha)| = S(L(\alpha)),$$

where $S : \mathbb{R}^r \to \mathbb{R}$ is the linear transformation defined by $S(x_1, \ldots, x_r) := x_1 + \cdots + x_r$.

Let $G = L(\mathcal{O}_K^*)$ be the image of the unit group of K under the homomorphism L, so that G is an additive subgroup of $\mathbb{R}^r$. Unlike the "analogous" situation in Minkowski space, G does not contain enough linearly independent vectors to span logarithmic space. This follows from the simple observation that since $N(u) = \pm 1$ for every unit $u \in \mathcal{O}_K^*$, every $x = (x_1, \ldots, x_r) \in G$ satisfies the relation $S(x) = 0$. In other words, G lies in the hyperplane (i.e., $r-1$-dimensional subspace) H of $\mathbb{R}^r$ defined by $x_1 + \cdots + x_r = 0$. Our main goal in the next section will be to prove that G is in fact a lattice of maximal rank $r-1$ in H.

2.3. Proof of Dirichlet's theorem. We start out by characterizing the group W_K in terms of the map L.

LEMMA 3.24. *The kernel of the restriction of L to $\mathcal{O}_K^*$ is finite, and is precisely the group W_K of roots of unity contained in K^*.*

PROOF. If we fix an embedding of K into $\mathbb{C}$, then it is easy to see that the kernel of L (restricted to $\mathcal{O}_K^*$) consists of the set of $u \in \mathcal{O}_K^*$ such that all conjugates of u have absolute value 1. By Lemma 2.35, the set of such u is finite, and consists precisely of the set of roots of unity contained in K. □

REMARK 3.25. Since W_K is a finite subgroup of the multiplicative group of K, it must be cyclic.

REMARK 3.26. A word of caution: if we do not restrict at least to $\mathcal{O}_K$, then there are many more elements in the kernel of L. For example, let $K = \mathbb{Q}(i)$, and let (a, b, c) be any Pythagorean triple. Then both conjugates of $\alpha := (a/c) + (b/c)i$ have absolute value 1, so that α is in the kernel of L. It is easy to see that infinitely many distinct α's arise in this way. (The point, of course, is that these α's are not algebraic integers, so in particular they are not units!)

By the structure theorem for finitely generated abelian groups, to prove Dirichlet's theorem it suffices to prove that $G = L(\mathcal{O}_K^*)$ is a lattice of rank $r - 1$ in $\mathbb{R}^r$. Since G is an additive subgroup of the hyperplane H, it suffices to prove that:

(D1) G is discrete.
(D2) G contains $r - 1$ vectors which are linearly independent over $\mathbb{R}$.

For once we know that G is discrete, it follows by Proposition 1.17 that G is a lattice of rank at most $r-1$. If, moreover, G contains $r-1$ vectors which are linearly independent over $\mathbb{R}$, then the rank must be exactly $r - 1$.

The discreteness part is easy, and follows from the following simple lemma (compare with Lemma 2.35):

LEMMA 3.27. *Let $M > 0$, and for each $n \geq 1$ define $S_M(n)$ to be the set of all algebraic integers of degree n whose conjugates all have complex absolute value at most M. Then $S_M(n)$ is a finite set.*

PROOF. Suppose $\alpha \in S_M$, and let $f(x) \in \mathbb{Z}[x]$ be the minimal polynomial of α, so that $\deg(f) = n$. Since the coefficients a_i of $f(x)$ are elementary symmetric functions of the conjugates of α, it follows from the triangle inequality that $|a_i| \leq 2^n M$ for all i. Therefore there are only finitely many possibilities for the polynomial $f(x)$, and hence for α. □

Property (D1) now follows:

COROLLARY 3.28. *G is a discrete subset of $\mathbb{R}^r$.*

PROOF. Let $M > 1$ be any real number; it suffices to show that the intersection S of G and the closed ball $B_{\log M}(0)$ of radius $\log M$ around 0 in $\mathbb{R}^r$ is finite. Note that if $\alpha \in \mathcal{O}_K^*$ maps to an element of S, then all conjugates of α have absolute value bounded by M. Therefore $(L)^{-1}(S)$ is contained in the finite set $S_M(n)$ defined in the statement of Lemma 3.27. It follows that S is finite. □

It remains to prove (D2). Our strategy for obtaining this result will be based on the following elementary lemma:

LEMMA 3.29. *Let $A = (a_{ij})$ be an $r \times r$ matrix with coefficients in $\mathbb{R}$ such that:*

(i) *The entries in every row of A sum to zero.*
(ii) *The diagonal entries of A are all positive.*
(iii) *The off-diagonal entries of A are all negative.*

Then A has rank $r - 1$.

PROOF. It suffices to prove that the first $r-1$ columns of A are linearly independent. Suppose for the sake of contradiction that $\sum_{j=1}^{r-1} c_j v_j = 0$, where v_j is the jth column of A and $c_j \in \mathbb{R}$ are not all 0. By rescaling, we may assume that there is an index k with $1 \leq k \leq r-1$ such that $c_k = 1$ and $c_j \leq 1$ for all $j \neq k$. Since $a_{kj} < 0$ for all $j \neq k$, we have $c_j a_{jk} \geq a_{jk}$ for such j. Similarly, since $k < r$ we must have

$$\sum_{j=1}^{r-1} a_{kj} > \sum_{j=1}^{r} a_{kj}.$$

Just by focusing in on the kth row of A, we therefore see that

$$0 = \sum_{j=1}^{r-1} c_j a_{kj} \geq \sum_{j=1}^{r-1} a_{kj} > \sum_{j=1}^{r} a_{kj} = 0 \ ,$$

a contradiction. □

Now comes the crucial step in which we use Minkowski's convex body theorem. For this, we will use the fact that the Minkowski space $\mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$ and logarithmic space are related in the following way. Recall that the embedding $\iota : \mathcal{O}_K \to \mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$ is given by

$$\iota(\alpha) = (\sigma_1(\alpha), \ldots, \sigma_{r_1}(\alpha), \tau_1(\alpha), \ldots, \tau_{r_2}(\alpha)).$$

If we define $\pi : \mathbb{R}^{r_1} - \{0\} \times \mathbb{C}^{r_2} - \{0\} \to \mathbb{R}^r$ to be the map given by

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

then it follows from the definitions that for $\alpha \in \mathcal{O}_K^*$, we have $L(\alpha) = \pi \circ \iota(\alpha)$.

LEMMA 3.30. *Fix any integer k with $1 \leq k \leq r$. There is a constant C (depending only on K) such that given any $\alpha \in \mathcal{O}_K$, $\alpha \neq 0$ there exists $\beta \in \mathcal{O}_K$, $\beta \neq 0$, satisfying the following two properties:*

(i) $|N(\beta)| \leq C$.
(ii) *If $L(\alpha) = (a_1, \ldots, a_r)$ and $L(\beta) = (b_1, \ldots, b_r)$, then $b_i < a_i$ for all $i \neq k$.*

PROOF. We will work in the Minkowski space $\mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$, and for simplicity of notation, we will write a point $x \in \mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$ as $(x_1, \ldots, x_r)$.

We claim that we can take the constant C to be $(\frac{2}{\pi})^{r_2}\sqrt{|\Delta_K|}$. Let $n = [K : \mathbb{Q}]$, and for $1 \leq i \leq r = r_1 + r_2$, define ϵ_i to be 1 if $1 \leq i \leq r_1$ and 2 if $r_1 + 1 \leq i \leq r$. Choose real numbers $a_1', \ldots, a_r'$ such that $a_i' < a_i$ for all $i = 1, \ldots, r$. Define E to be the subset of $\mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$ defined by inequalities of the form

$$|x_i|^{\epsilon_i} \leq C_i,$$

where $C_i = e^{a_i'}$ for $i \neq k$ and C_k is chosen so that $\prod_i C_i = C$. It is easy to see that E is symmetric, compact, and convex. Moreover, a straightforward computation shows that

$$\begin{aligned} \operatorname{vol}(E) = 2^{r_1}\pi^{r_2}\textstyle\prod_i C_i &= 2^{r_1}\pi^{r_2}(\tfrac{2}{\pi})^{r_2}\sqrt{|\Delta_K|} \\ &= 2^{r_1+2r_2}(2^{-r_2}\sqrt{|\Delta_K|}) \\ &= 2^n \operatorname{vol}(\mathbb{R}^n/\iota(\mathcal{O}_K)). \end{aligned}$$

By Minkowski's convex body theorem, E must contain a nonzero element of $\iota(\mathcal{O}_K)$. The lemma is proved by taking β to be the corresponding element of $\mathcal{O}_K$. □

REMARK 3.31. The exact value of the constant C is irrelevant if we just want to prove Dirichlet's theorem as stated (though it becomes relevant if we are interested in finding "small" generators for the unit group). The qualitative version of the argument we have just given is as follows. The region E is a product of lines and circles in $\mathbb{R}^n$ in which all but one of the coordinates is constrained to lie in a thin strip. The other (k^{th}) coordinate is constrained linearly in terms of the constant C. By choosing C sufficiently large, we can make the volume of E as big as we like. In particular, for sufficiently large C, Minkowski's theorem implies that E contains a nonzero lattice point.

We now prove Dirichlet's unit theorem.

PROOF. By Lemma 3.29, we see that to prove (D2) (and hence Dirichlet's theorem), it suffices to prove that for any given integer k with $1 \leq k \leq r$, there exists a unit $u \in \mathcal{O}_K^*$ such that $L(u) =$

$(a_1, \ldots, a_r)$ with $a_k > 0$ and $a_i < 0$ for $i \neq k$. For this, we use Lemma 3.30.

Let $\alpha_0 \in \mathcal{O}_K$ be any nonzero element. Applying Lemma 3.30 repeatedly, we produce a sequence of elements $\alpha_j \in \mathcal{O}_K$, $\alpha_j \neq 0$ such that for all $j = 1, 2, \ldots$, we have (letting $L(\alpha_j) = (a_1(j), \ldots, a_r(j))$):

(i) $|N(\alpha_j)| \leq C$.
(ii) $a_i(j) < a_i(j-1)$ for all $i \neq k$.

Since there are only finitely many ideals of norm at most C, there must be distinct positive integers $j_1 > j_2$ such that $(\alpha_{j_1}) = (\alpha_{j_2})$. Let

$$u := \alpha_{j_1}/\alpha_{j_2}.$$

Since α_{j_1} and α_{j_2} generate the same ideal, it follows that u is a unit. Moreover, since $a_i(j_1) < a_i(j_2)$ for all $i \neq k$, it follows that

$$L(u) = (a_1, \ldots, a_r)$$

with $a_i < 0$ for $i \neq k$. Finally, we must have $a_k > 0$, since $\sum_{i=1}^{r} a_i = 0$. □

EXERCISE 3.32. Choose a basis $\epsilon_1, \ldots, \epsilon_{r_1+r_2-1}$ for the free abelian group $\mathcal{O}_K^*/W_K$, and let M be the $(r_1+r_2-1) \times (r_1+r_2)$ matrix whose j^{th} row is

$$(\log|\sigma_1(\epsilon_j)|, \ldots, \log|\sigma_{r_1}(\epsilon_j)|, 2\log|\tau_1(\epsilon_j)|, \ldots, 2\log|\tau_{r_2}(\epsilon_j)|) \ .$$

Let M' be the $(r_1+r_2-1) \times (r_1+r_2)$ matrix obtained by deleting any column of M. Show that $|\det(M')|$, which is called the *regulator* of K, is independent of which particular column is deleted, and is a nonzero real number which depends only on the field K. [**Hint:** Use the fact that the columns of M add up to zero.]

It is not hard to see that the regulator of K, defined in Exercise 3.32, is the covolume of the lattice $\mathcal{O}_K^*$ under its logarithmic embedding into the Euclidean space $H \cong \mathbb{R}^{r-1} \subset \mathbb{R}^r$. It is therefore the "multiplicative" version of the quantity $2^{-r_2}\sqrt{|\Delta_K|}$, which is the covolume of $\mathcal{O}_K$ under its embedding ι into Minkowski space.

2.4. Units in real quadratic fields. The most efficient procedure for finding the fundamental unit in a real quadratic field is to use *continued fractions*. We state the relevant results mostly without proof (see, for example, §9.3–9.5 of Koch's book "Number Theory: Algebraic Numbers and Functions" for details). [1]

[1]Our exposition here is based on H. Koch's book and on J. S. Milne's online "Algebraic Number Theory" lecture notes.

A *continued fraction* is an expression of the form

$$a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 + \cfrac{1}{a_4 + \cdots}}} \tag{3.1}$$

where $a_1, a_2, \ldots$ are positive integers called the *successive quotients*. For typographical reasons, we abbreviate (3.1) by the expression

$$[a_1, a_2, a_3, a_4, \ldots] \ .$$

The truncated expression

$$[a_1, a_2, \ldots, a_n] = a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 + \cdots + \cfrac{1}{a_n}}}$$

is called the n^{th} *convergent* to the continued fraction, and the *value* of the continued fraction is $\lim_{n\to\infty}[a_1, a_2, \ldots, a_n]$, which one can show always exists.

It is known from elementary number theory that every irrational real number $\alpha > 1$ has a *unique* continued fraction expansion, and this expansion is *periodic* if and only if $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 2$. (See, for example, Chapter X of Hardy and Wright's "An Introduction to the Theory of Numbers".)

To obtain the continued fraction expansion of a real number $\alpha > 1$, one proceeds inductively as follows. Set $\alpha_1 = \alpha$, and $a_1 = [\alpha]$ (where $[\cdot]$ denotes the greatest integer function). If $\alpha \in \mathbb{Z}$, the continued fraction terminates at this point. Otherwise, continue inductively by setting

$$\alpha_{n+1} = \frac{1}{\alpha_n - a_n} \ , \qquad a_{n+1} = [\alpha_{n+1}] \ .$$

If $\alpha_{n+1} \in \mathbb{Z}$ for some n, then the continued fraction expansion of α terminates with $a_{n+1} = \alpha_{n+1}$; otherwise, one obtains an infinite sequence $a_1, a_2, a_3, \ldots$. The numbers α_n are called the *successive remainders*.

Exercise 3.33. Show that the continued fraction expansion of α terminates if and only if α is rational.

Define a sequence $P_0, P_1, \ldots$ of 2×2 matrices with positive integer coefficients by setting, for $n \geq 1$:

$$A_n = \begin{pmatrix} a_n & 1 \\ 1 & 0 \end{pmatrix}$$

and

$$P_0 = \begin{pmatrix} p_0 & p_{-1} \\ q_0 & q_{-1} \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \ , \qquad P_n = \begin{pmatrix} p_n & p_{n-1} \\ q_n & q_{n-1} \end{pmatrix} = A_1 A_2 \cdots A_n \ .$$

Then one checks easily that $p_{n+1} = a_{n+1}p_n + p_{n-1}$ and $q_{n+1} = a_{n+1}q_n + q_{n-1}$ for all $n \geq 0$, and from the relation

$$p_n q_{n-1} - p_{n-1}q_n = \det P_n = \prod_{i=1}^{n}(-1) = (-1)^n \ ,$$

one finds that $\gcd(p_n, q_n) = 1$ for all $n \geq 1$. Moreover, it is clear that

$$0 < p_1 < p_2 < \cdots \ , \qquad 0 < q_1 < q_2 < \cdots \ .$$

From this, one shows easily that if $\alpha > 1$ is irrational, then

$$|\alpha - \frac{p_n}{q_n}| < \frac{1}{q_n^2} \ .$$

In particular, it follows that $\alpha = \lim_{n\to\infty} \frac{p_n}{q_n}$. More precisely, one has the formula

$$[a_1, \ldots, a_n] = \frac{p_n}{q_n} \ ,$$

and therefore

$$\lim_{n\to\infty} [a_1, \ldots, a_n] = \lim_{n\to\infty} \frac{p_n}{q_n} = \alpha \ .$$

The main theorem connecting continued fractions and units of quadratic fields is:

THEOREM 3.34. *Let d be a square-free positive integer with $d \equiv 2, 3 \pmod 4$, and let $\epsilon > 1$ be the fundamental unit for $\mathbb{Q}(\sqrt{d})$. Let k be the period of the continued fraction expansion for $\sqrt{d}$. Then*

$$\epsilon = p_k + q_k\sqrt{d} \ .$$

COROLLARY 3.35. *With notation as in Theorem 3.34, if d is a square-free positive integer with $d \equiv 2, 3 \pmod 4$, then all solutions to the Pell equation $x^2 - dy^2 = \pm 1$ are given by*

$$x + y\sqrt{d} = \pm(p_k + q_k\sqrt{d})^m$$

with $m \in \mathbb{Z}$.

In general (if d is not necessarily congruent to 2 or 3 (mod 4)), one can proceed as follows. An irrational number $\theta > 1$ is said to be *reduced* if

$$-\frac{1}{\theta'} > 1 \ ,$$

where θ' denotes the conjugate of θ. According to a theorem of Galois, the continued fraction expansion of θ is *purely periodic* if and only if θ is reduced. (Purely periodic means that

$$\alpha = [\overline{a_1, a_2, \ldots, a_k}]$$

for some integer $k \geq 1$; the minimal such k is called the *period* of the continued fraction expansion of α.) Then:

THEOREM 3.36. *Let D be the discriminant of $K = \mathbb{Q}(\sqrt{d})$, let θ be a reduced element of K having discriminant D, and let $[\overline{a_1, a_2, \ldots, a_k}]$ be the continued fraction expansion of θ, with period k. Then the fundamental unit of $\mathcal{O}_K$ is*

$$\epsilon = q_{k-1} + q_k\theta \ .$$

In applying this theorem, the following exercise is useful:

EXERCISE 3.37. If

$$\omega = \begin{cases} \frac{1+\sqrt{d}}{2} & \text{if } d \equiv 1 \pmod 4 \\ \sqrt{d} & \text{if } d \equiv 2, 3 \pmod 4 \ , \end{cases}$$

show that the *second successive remainder*

$$\theta = \alpha_2 = \frac{1}{\omega - [\omega]}$$

of ω is reduced.

The advantage of Theorem 3.36 over Theorem 3.34 is that it applies even when $d \equiv 1 \pmod 4$. We illustrate both theorems with the following example.

EXAMPLE 3.38. Let $K = \mathbb{Q}(\sqrt{19})$. Then one computes that

$$\sqrt{19} = [4, \overline{2, 1, 3, 1, 2, 8}] \ ,$$

and the period of this continued fraction is 6. We have

$$(p_{-1}, p_0, p_1, p_2, p_3, p_4, p_5, p_6) = (0, 1, 4, 9, 13, 48, 61, 170) \ ,$$
$$(q_{-1}, q_0, q_1, q_2, q_3, q_4, q_5, q_6) = (1, 0, 1, 2, 3, 11, 14, 39)$$

and therefore, by Theorem 3.34, we have

$$\epsilon = p_6 + q_6\sqrt{19} = 170 + 39\sqrt{19} \ .$$

On the other hand, we have

$$\theta = \frac{1}{\sqrt{19} - 4} = [\overline{2, 1, 3, 1, 2, 8}] \ ,$$

and for this continued fraction we get

$$(q_{-1}, q_0, q_1, q_2, q_3, q_4, q_5, q_6) = (1, 0, 1, 1, 4, 5, 14, 117) \ .$$

By Theorem 3.36, the fundamental unit ϵ of K is

$$q_5 + q_6\theta = 14 + 117 \cdot \frac{1}{\sqrt{19} - 4} = 170 + 39\sqrt{19} \ .$$

REMARK 3.39. The coefficients of the fundamental unit can be quite large, even when d is small. For example, using the above procedure one checks that the fundamental unit of $\mathbb{Q}(\sqrt{94})$ is

$$\epsilon = 2143295 + 221064\sqrt{94} \ ,$$

and the constant coefficient of the fundamental unit of $\mathbb{Q}(\sqrt{9199})$ has 88 decimal digits.

2.5. The fundamental unit in cubic fields with negative discriminant. We begin with a result which explains the meaning of the sign of the discriminant.

EXERCISE 3.40. If K is a number field, show that the sign of Δ_K is $(-1)^{r_2}$.

Therefore a cubic field has negative discriminant if and only if it has precisely one real embedding. For example, every 'pure' cubic field of the form $\mathbb{Q}(\sqrt[3]{d})$ has this property. By Dirichlet's unit theorem, such fields have a unit group of rank one (and the torsion subgroup is just $\{\pm 1\}$). It therefore makes sense to define the *fundamental unit* of a cubic field with negative discriminant as in the quadratic case: If we identify K with a subfield of $\mathbb{R}$ via the unique real embedding, then $\mathcal{O}_K^* = \{\pm\epsilon^m\}$ for a unique unit $\epsilon > 1$, called the *fundamental unit* of K. [2]

LEMMA 3.41. *If K is a cubic field with negative discriminant, then the fundamental unit ϵ of K satisfies the inequality*

$$\epsilon > \sqrt[3]{\frac{|\Delta_K| - 24}{4}} \ .$$

PROOF. It is easy to check that $K = \mathbb{Q}(\epsilon)$ (since $[K : \mathbb{Q}] = 3$ is prime) and that $N_{K/\mathbb{Q}}(\epsilon) = 1$, since if ϵ_2, ϵ_3 denote the other conjugates of $\epsilon = \epsilon_1$, then $\epsilon_3 = \overline{\epsilon}_2$. Write $\epsilon = u^2$ with $u > 1$, and since $|\epsilon_2|^2 = 1/u^2$, we may assume without loss of generality that $\epsilon_2 = u^{-1}e^{i\theta}$ with $0 \leq \theta \leq \pi$. A determinant calculation and some trigonometry shows that

$$|\Delta(\epsilon)|^{1/2} = 2i(u^3 + u^{-3} - 2\cos\theta)\sin\theta \ .$$

Setting $2a = u^3 + u^{-3}$, we obtain

$$|\Delta(\epsilon)|^{1/2} = 4(a - \cos\theta)\sin\theta \ ,$$

which by calculus is maximized (for a given value of u) when

$$a\cos\theta = \cos^2\theta - \sin^2\theta = 2\cos^2\theta - 1 \ .$$

[2]The statement and proof of the next lemma are adapted from J. S. Milne's online Algebraic Number Theory lecture notes.

If we substitute $x = \cos\theta$ and let $g(x) = 2x^2 - ax - 1$, then we are trying to solve the equation $g(x) = 0$ for some x with $|x| \leq 1$. Since $u > 1$, we have $a > 1$ and therefore $g(1) = 1 - a < 0$. As $g(x) > 0$ for x sufficiently large, it follows that $g(x)$ has a root bigger than 1. Also, $g(-\frac{1}{2u^3}) = \frac{3}{4}(u^{-6} - 1) < 0$ and $g(-1) = 1 + a > 0$. It follows that $g(x)$ has exactly one root $x_0 \in [-1, -\frac{1}{2u^3}]$. Therefore

$$|\Delta(\epsilon)|^{1/2} \leq 4(a - x_0)(1 - x_0^2)^{1/2}$$

which, in view of the fact that $ax_0 = 2x_0^2 - 1$ and $a^2x_0^2 = 4x_0^4 - 4x_0^2 + 1$, yields

$$\begin{aligned} |\Delta(\epsilon)| &\leq 16(a^2 - 2ax_0 + x_0^2)(1 - x_0^2) \\ &= 16(a^2 - a^2x_0^2 - 5x_0^2 + 3x_0^4 + 2) \\ &= 16(a^2 + 1 - x_0^2 - x_0^4) \\ &= 4u^6 + 24 + 4(u^{-6} - 4x_0^2 - 4x_0^4) \\ &< 4u^6 + 24 \\ &= 4\epsilon^3 + 24 \ . \end{aligned}$$

Since $|\Delta_K| \leq |\Delta(\epsilon)|$, we are done. □

EXAMPLE 3.42. Let $\alpha = \sqrt[3]{2}$. We can use Lemma 3.41 to show that the fundamental unit ϵ in the field $K = \mathbb{Q}(\alpha)$ is $u = 1 + \alpha + \alpha^2$. This is indeed a unit, since $1/u = -1 + \alpha \in \mathcal{O}_K$, and it is clearly not a root of unity, since $u > 1$ is real. Since $\alpha < 2$, we have $1 < u < 7 < 21^{2/3}$, and since $\Delta_K = -108$, it follows from Lemma 3.41 that

$$\epsilon^3 > \frac{108 - 24}{4} = 21 \ ,$$

and therefore

$$1 < u < 21^{2/3} < \epsilon^2 \ . \tag{3.2}$$

But we know that $u = \pm\epsilon^m$ for some $m \in \mathbb{Z}$, and since $u > 1$, we must in fact have $u = \epsilon^m$ with $m \geq 1$. By (3.2), it follows that $m = 1$ as desired.

EXAMPLE 3.43. Let $K = \mathbb{Q}(\alpha)$ with α the real root of $X^3 + 10X + 1$, which has discriminant -4027. Since 4027 is prime, we know that $\mathcal{O}_K = \mathbb{Z}[\alpha]$. By Lemma 3.41, the fundamental unit ϵ of K satisfies

$$\epsilon > \sqrt[3]{\frac{4027 - 24}{4}} \approx 10.002499\ldots$$

Since $N_{K/\mathbb{Q}}(\alpha) = -1$, it follows that α is a unit. A calculation shows that $\beta := -\alpha^{-1} \approx 10.00998\ldots$, so that $1 < \beta < \epsilon^2$, and as in the previous example it follows that $\epsilon = \beta$.

Knowledge of the fundamental unit is often of great utility when trying to compute the ideal class group. We illustrate this in the following example taken from Cassels' book "Local Fields".

EXAMPLE 3.44. We now calculate the group of units in the field $K = \mathbb{Q}(\sqrt[3]{11})$, and use this information to compute the ideal class group of $\mathcal{O}_K$.

Let $\alpha = \sqrt[3]{11}$. Since $11^2 \not\equiv 1 \pmod 9$, it follows from Proposition 2.28 that $\mathcal{O}_K = \mathbb{Z}[\alpha]$.

The discriminant of K is $\Delta_K = -3^3 \cdot 11^2$, and the Minkowski constant of K is

$$M_K = \frac{3!}{3^3}(\frac{4}{\pi})\sqrt{3^3 \cdot 11^2} < 17 \ ,$$

so we need to see how $2, 3, 5, 7, 11$, and 13 factor in $\mathcal{O}_K$. Using Kummer's factorization theorem, we find that:

$$x^3 - 11 \equiv \begin{cases} (x-1)(x^2+x+1) & \pmod 2 \\ (x+1)^3 & \pmod 3 \\ (x-1)(x^2+x+1) & \pmod 5 \\ x^3 - 4 & \pmod 7 \\ x^3 & \pmod{11} \\ x^3 + 2 & \pmod{13} \ . \end{cases}$$

Letting $(2) = \mathfrak{p}_2\mathfrak{p}_2'$ with $N(\mathfrak{p}_2) = 2$, $(3) = \mathfrak{p}_3^3$, $(5) = \mathfrak{p}_5\mathfrak{p}_5'$ with $N(\mathfrak{p}_5) = 5$, and noting that $(11) = \mathfrak{p}_{11}^3$ with $\mathfrak{p}_{11} = (\alpha)$ principal, it follows that $\mathrm{Cl}(\mathcal{O}_K)$ is generated by $[\mathfrak{p}_2], [\mathfrak{p}_3]$, and $[\mathfrak{p}_5]$.

We now find some relations between these generators by searching for elements of $\mathcal{O}_K$ with small norm. For $t \in \mathbb{Z}$, the minimal polynomial of $\alpha - t$ is $(x+t)^3 - 11$, and therefore $N(\alpha - t) = -t^3 - 11$. Plugging in various small values of t gives the following information:

$$(\alpha) = \mathfrak{p}_{11} \ , (\alpha - 1) = \mathfrak{p}_2\mathfrak{p}_5 \ , (\alpha - 2) = \mathfrak{p}_3 \ , (\alpha + 1) = \mathfrak{p}_2^2\mathfrak{p}_3 \ .$$

This tells us that $[\mathfrak{p}_3] = 1, [\mathfrak{p}_5] = [\mathfrak{p}_2]^{-1}$, and $[\mathfrak{p}_2]^2 = 1$. Thus $\mathrm{Cl}(\mathcal{O}_K) = \{0\}$ if $[\mathfrak{p}_2] = 1$ and $\mathrm{Cl}(\mathcal{O}_K) \cong \mathbb{Z}/2\mathbb{Z}$ if $[\mathfrak{p}_2] \neq 1$. So the computation of $\mathrm{Cl}(\mathcal{O}_K)$ boils down to the question: is the ideal $\mathfrak{p}_2$ principal? To answer this question, we need to first calculate the *unit group* of K.

First, we try to find *some* nontrivial unit of $\mathcal{O}_K$. We do this by looking at principal ideals whose factorizations involve only $\mathfrak{p}_2$ and $\mathfrak{p}_3$. We have already seen that $\mathfrak{p}_3 = (\alpha - 2)$ and $\mathfrak{p}_2^2\mathfrak{p}_3 = (\alpha + 1)$. We have also seen that $\mathfrak{p}_2^2 = (\beta)$ for some $\beta \in \mathcal{O}_K$, and we know that

$$(\beta)(\alpha - 2) = (\alpha + 1) \ ,$$

so we can take

$$\beta = \frac{\alpha+1}{\alpha-2} = \alpha^2 + 2\alpha + 5 \ .$$

We also have $(\beta)^2 = \mathfrak{p}_2^4 = (\alpha - 3)$, since $N(\alpha - 3) = 16$ and $(\alpha - 3) \neq \mathfrak{p}_2^2\mathfrak{p}_2'$ or else we would have $2 \mid \alpha - 3$, which is clearly not the case. Therefore

$$u = -\frac{\beta^2}{\alpha - 3} = 18\alpha^2 + 40\alpha + 89 \approx 266.9889\ldots$$

is a unit in $\mathcal{O}_K$.

Let ϵ be the fundamental unit of K. By Lemma 3.41, we have

$$\epsilon > \sqrt[3]{\frac{3267 - 24}{4}} \approx 9.3437\ldots$$

and thus

$$\epsilon^2 > 87 \ , \qquad \epsilon^3 > 815 \ ,$$

from which it follows that $u = \epsilon$ or $u = \epsilon^2$.

We rule out $u = \epsilon^2$ by constructing a homomorphism from $\mathbb{Z}[\alpha]$ to $\mathbb{F}_p$ for which the image of u is not a square in $\mathbb{F}_p$. Since $\mathfrak{p}_5 = (5, \alpha - 1)$ has norm 5, reduction modulo $\mathfrak{p}_5$ gives a homomorphism $\psi : \mathbb{Z}[\alpha] \to \mathbb{F}_5$ sending α to 1. As $\psi(u) = 2$ and 2 is not a square in $\mathbb{F}_5$, we win.

We conclude that $\epsilon = u$ and that $\mathcal{O}_K^* = \{\pm u^m\}$. We note that the unit group modulo ± 1 is also generated by $v = 1/u = -2\alpha^2 + 4\alpha + 1$, which is a bit simpler to work with algebraically.

We now show that $\mathfrak{p}_2$ is not principal. Recall that $\mathfrak{p}_2^2 = (\beta)$, where $\beta = \alpha^2 + 2\alpha + 5$. Suppose for the sake of contradiction that $\mathfrak{p}_2 = (\gamma)$ is principal. Then we would have

$$\mathfrak{p}_2^2 = (\beta) = (\gamma^2)$$

and thus

$$\pm v^m \beta = \gamma^2$$

for some $\gamma \in \mathbb{Z}[\alpha]$. Without loss of generality, we may assume (after multiplying by the appropriate power of v^{-2}) that $m = 0$ or 1. We therefore conclude that either (a) β, (b) $-\beta$, (c) $v\beta$, or (d) $-v\beta$ is a square in $\mathbb{Z}[\alpha]$.

We rule these possibilities out by again using a cleverly chosen homomorphism from $\mathbb{Z}[\alpha]$ to a finite field. In this case, using Kummer's factorization theorem, we see that 19 splits completely in K, and the cube roots of 11 in $\mathbb{F}_{19}$ are $5, -3, -2$. Therefore there is a homomorphism $\psi_1 : \mathbb{Z}[\alpha] \to \mathbb{F}_{19}$ sending α to 5. A simple calculation shows that $\psi_1(\beta) = 2$ and $\psi_1(v\beta) = -1$, both of which are non-squares in $\mathbb{F}_{19}$. This rules out (a) and (c).

The other elements $-\beta$ and $-v\beta$ must go to squares under ψ_1, since $19 \equiv 3 \pmod 4$. However, sending α to -2 gives a different homomorphism $\psi_2 : \mathbb{Z}[\alpha] \to \mathbb{F}_{19}$, and we calculate that $\psi_2(-\beta) = -5$ and $\psi_2(-v\beta) = -1$, both of which are non-squares in $\mathbb{F}_{19}$. This rules out (b) and (d)!

We conclude that $\mathfrak{p}_2$ is not principal, and therefore that $\mathrm{Cl}(\mathcal{O}_K) \cong \mathbb{Z}/2\mathbb{Z}$.

3. Exercises for Chapter 3

(1) Let m be a nonzero integer.
   (a) Let $t \in \mathbb{Z}$ and define $\Lambda \subset \mathbb{Z}^2$ to be the lattice in $\mathbb{R}^2$ consisting of all pairs $(a, b) \in \mathbb{Z}$ such that $b \equiv at \pmod m$. Show that $\mathrm{covol}(\Lambda) = m$.
   (b) Let $u, v \in \mathbb{Z}$, and let $\Lambda \subset \mathbb{Z}^4$ be the lattice in $\mathbb{R}^4$ consisting of all $(a, b, c, d) \in \mathbb{Z}^4$ such that
   $$c \equiv ua + vb \ , \quad d \equiv ub - va \qquad (\mathrm{mod}\ m) \ .$$
   Show that $\mathrm{covol}(\Lambda) = m^2$.

(2) (a) Show that the volume of a ball of radius r in $\mathbb{R}^4$ is $\pi^2 r^4/2$.
   (b) A *quaternion* is an expression of the form $a + bi + cj + dk$, where i, j, k are formal symbols satisfying $i^2 = j^2 = k^2 = -1$ and $ij = -k$. Quaternions can be added componentwise (like complex numbers). They can also be multiplied, but unlike with complex numbers, multiplication of quaternions is associative but not commutative. If $z = a + bi + cj + dk$ is a quaternion, its conjugate $\overline{z}$ is given by $a - bi - cj - dk$. Show that $z\overline{z}$ is always a positive real number, so that we can define the norm of z to be $\sqrt{z\overline{z}}$. Prove that the norm of a product of two quaternions is the product of their norms.

(3) Let $\Lambda \subset \mathbb{R}^n$ be a rank n lattice, and let $S \subset \mathbb{R}^n$ be a compact, convex, and symmetric set. If
   $$\mathrm{vol}(S) \geq 2^n \mathrm{vol}(\mathbb{R}^n/\Lambda).$$
   prove that S contains a nonzero element of Λ.

(4) For $x = (x_1, \ldots, x_n) \in \mathbb{R}^n$, let
   $$L_i(x) = \sum_{j=1}^{n} a_{ij} x_j \ , \quad 1 \leq i \leq n$$
   be n linear forms with coefficients $a_{ij} \in \mathbb{R}$. If $\lambda_1, \ldots, \lambda_n$ are positive real numbers for which $\lambda_1 \cdots \lambda_n \geq |\det(a_{ij})| > 0$,

prove that there exist integers $y_1, \ldots, y_n \in \mathbb{Z}$, not all zero, such that $|L_i(y_1, \ldots, y_n)| \leq \lambda_i$ for all $i = 1, \ldots, n$. (Bonus: Does the conclusion still hold if $\det(a_{ij}) = 0$?)

(5) Let p be a prime number which is congruent to 5 modulo 12. If $p > 3^n$, show that the ideal class group of $K = \mathbb{Q}(\sqrt{-p})$ contains an element of order greater than n. In particular, it follows from Dirichlet's theorem on primes in arithmetic progressions that the class number of an imaginary quadratic field can be arbitrarily large. (**Hint:** Factor (3) in $\mathcal{O}_K$.)

(6) Let d be a square-free even positive integer, and suppose $d = a^n - 1$ for some integers $a, n \geq 2$.
   (a) Show that $(1 + \sqrt{-d}) = \mathfrak{a}^n$ for some ideal $\mathfrak{a}$ of $\mathbb{Z}[\sqrt{-d}]$.
   (b) Show that the class of $\mathfrak{a}$ has order exactly equal to n in the ideal class group of $\mathbb{Q}(\sqrt{-d})$.

(7) Let $k > 0$ be a squarefree positive integer such that:
   (i) $k \equiv 1, 2 \pmod 4$.
   (ii) $k \neq 3a^2 \pm 1$ for any integer a.
   (iii) 3 does not divide the class number of $\mathbb{Q}(\sqrt{-k})$.
   (a) Prove that the Diophantine equation $y^2 = x^3 - k$ has no integral solution.
   (b) Find two integers k which satisfy the above 3 hypotheses.
   (c) Show that all 3 hypotheses are necessary. (**Hint:** For hypothesis (iii), consider $k = 61$.)

(8) (a) If $p = 4n - 1 \geq 11$ is a prime number, show that $\mathbb{Q}(\sqrt{-p})$ has class number 1 if and only if $x^2 + x + n$ is prime whenever $0 \leq x \leq n - 2$.
   (b) Find a monic quadratic polynomial $f(x) \in \mathbb{Z}[x]$ which has prime values at 40 consecutive integers.

(9) Choose a basis $\epsilon_1, \ldots, \epsilon_{r_1+r_2-1}$ for the free abelian group $\mathcal{O}_K^*/W_K$, and let M be the $(r_1 + r_2 - 1) \times (r_1 + r_2)$ matrix whose j^{th} row is

$$(\log|\sigma_1(\epsilon_j)|, \ldots, \log|\sigma_{r_1}(\epsilon_j)|, 2\log|\tau_1(\epsilon_j)|, \ldots, 2\log|\tau_{r_2}(\epsilon_j)|) \ .$$

Let M' be the $(r_1 + r_2 - 1) \times (r_1 + r_2 - 1)$ matrix obtained by deleting any column of M. Show that $|\det(M')|$, which is called the *regulator* of K, is independent of which particular column is deleted, and is a nonzero real number which depends only on the field K. [**Hint:** Use the fact that the columns of M add up to zero.]

(10) Let $K = \mathbb{Q}(\sqrt{223})$.
   (a) Find the group of units of K.
   (b) Show that the ideal class group of $\mathcal{O}_K$ is cyclic of order 3.

(11) Which of the following Diophantine equations have integer solutions?
   (a) $X^2 - 223Y^2 = \pm 11$.
   (b) $X^2 - 223Y^2 = \pm 11^3$.
   (c) $X^2 - 223Y^2 = \pm 11^{19}$.

(12) (a) If $\alpha \in K$ is a root of a monic polynomial $f \in \mathbb{Z}[x]$, and if $f(r) = \pm 1$ with $r \in \mathbb{Z}$, show that $\alpha - r$ is a unit of $\mathcal{O}_K$.
   (b) Find the fundamental unit in $\mathbb{Q}(\sqrt[3]{7})$.

(13) Show that $1 - \zeta_m$ is a unit in $\mathbb{Z}[\zeta_m]$ if and only if m is not a prime power.

(14) Let $K = \mathbb{Q}(\zeta_p)$, where p is an odd prime.
   (a) Show that the ring of integers in $\mathbb{Q}(\zeta_p + \zeta_p^{-1})$ is $\mathbb{Z}[\zeta_p + \zeta_p^{-1}]$.
   (b) Show that the unit group of $\mathcal{O}_K$ is the direct product of the cyclic group generated by ζ_p and the unit group of $\mathbb{Z}[\zeta_p + \zeta_p^{-1}]$.

CHAPTER 4

Relative extensions

1. Localization

1.1. Introduction to localization. We now introduce the technique of *localization*. This is a way of starting with one ring R and constructing from it a ring R' in which some of the prime ideals of R have been "removed". Frequently, if R is a Dedekind ring, we can arrange for the localized ring to be a PID.

An example you already know of localization is the field of fractions K of an integral domain R. This is a ring in which all nonzero prime ideals of R have been deleted! The process of adding *all* nonzero elements of R as denominators is a bit too drastic, since K does not retain much arithmetic information about the original ring R. So the idea is to invert some, but not all, elements of R, to form a ring R' which is intermediate between R and K. This ring will hopefully be close enough to K to be simple, but also close enough to R to still contain interesting information about R.

When we are interested in studying quantities related to a particular prime ideal $\mathfrak{p}$ of R, such as the ramification index or residue degree of $\mathfrak{p}$, localization allows us to focus on $\mathfrak{p}$ without letting the other prime ideals make our view too "hazy".

That was probably sufficiently vague — now let's actually define localization and prove some of its important properties.

For simplicity, let R be an integral domain with field of fractions K. (You should be aware that one can define localization in a more general context.) Let S be a *multiplicative subset* of R, which we define to mean a subset which is closed under multiplication and contains 1 but not 0. One of the main examples to keep in mind is where S is the complement of a prime ideal $\mathfrak{p}$. Note that $R\backslash\mathfrak{p}$ is indeed a multiplicative subset of R, since if $x \notin \mathfrak{p}$ and $y \notin \mathfrak{p}$, then $xy \notin \mathfrak{p}$ by the definition of a prime ideal.

The *localization* $S^{-1}R$ is the subring of K given by

$$S^{-1}R := \{\frac{r}{s} \ : \ r \in R, s \in S\}.$$

The fact that S is closed under multiplication guarantees that $S^{-1}R$ is closed under the usual addition and multiplication of fractions, and therefore $S^{-1}R$ is indeed a ring.

When $S = R\backslash\mathfrak{p}$ for some prime ideal $\mathfrak{p}$, we will often write $R_\mathfrak{p}$ for $S^{-1}R$. We call $R_\mathfrak{p}$ the localization of R at the prime ideal $\mathfrak{p}$.

Note that by definition, the field of fractions K is just $R_{(0)}$, the localization of R at the prime ideal (0). In general we always have $R \subseteq S^{-1}R \subseteq K$.

The most important thing to know about localization is its effect on prime ideals. We denote by $\mathrm{Spec}(R)$ the set of prime ideals of a ring R.

PROPOSITION 4.1. *The prime ideals of $R' := S^{-1}R$ are in bijection with the prime ideals of R which are disjoint from S.*

PROOF. The correspondence is as follows: we associate to any $\mathfrak{q} \in \mathrm{Spec}(R)$ disjoint from S the ideal $S^{-1}\mathfrak{q} = \mathfrak{q}R' = \{\frac{q}{s} \,:\, q \in \mathfrak{q}, s \in S\}$ in R', and to any $\mathfrak{q}' \in \mathrm{Spec}(R')$ the ideal $\mathfrak{q}' \cap R$ in R. We need to check that these associations establish the claimed bijection.

Suppose first that $\mathfrak{q} \in \mathrm{Spec}(R)$ is disjoint from S. We claim that the ideal $S^{-1}\mathfrak{q}$ of R' is prime. Indeed (with the obvious notation), suppose $x = \frac{r_1}{s_1}, y = \frac{r_2}{s_2} \in R'$ and $xy \in \mathfrak{q}R'$. Then $\frac{r_1 r_2}{s_1 s_2} = \frac{q}{s}$, so clearing denominators we have $r_1 r_2 s \in \mathfrak{q}$. But $s \notin \mathfrak{q}$ since $S \cap \mathfrak{q} = \emptyset$, so $r_1 \in \mathfrak{q}$ or $r_2 \in \mathfrak{q}$, which implies that $x \in S^{-1}\mathfrak{q}$ or $y \in S^{-1}\mathfrak{q}$. We also need to check that $S^{-1}\mathfrak{q} \neq R'$, but this is easy: we cannot have $\frac{q}{s} = 1$ with $q \in \mathfrak{q}$ and $s \in S$ since $\mathfrak{q} \cap S = \emptyset$.

Next suppose that $\mathfrak{q}' \in \mathrm{Spec}(R')$. We claim that $\mathfrak{q}' \cap R$ is a prime ideal which is disjoint from S. The fact that it is a prime ideal is clear. To see disjointness, suppose $s \in S \cap \mathfrak{q}'$. Then $1 = \frac{1}{s}s \in \mathfrak{q}'$, a contradiction.

Finally, we verify that the maps $\mathfrak{q} \mapsto S^{-1}\mathfrak{q}$ and $\mathfrak{q}' \mapsto \mathfrak{q}' \cap R$ are inverse to one another, i.e.:

(a) $S^{-1}\mathfrak{q} \cap R = \mathfrak{q}$
(b) $S^{-1}(\mathfrak{q}' \cap R) = \mathfrak{q}'$.

For (a), it suffices to show that $S^{-1}\mathfrak{q} \cap R \subseteq \mathfrak{q}$, since the other direction is clear. If $x = \frac{q}{s} \in S^{-1}\mathfrak{q} \cap R$, then $sx \in \mathfrak{q}$, and since $s \notin \mathfrak{q}$, we must have $x \in \mathfrak{q}$ as desired.

For (b), it suffices to show that $\mathfrak{q}' \subseteq S^{-1}(\mathfrak{q}' \cap R)$, since the other containment follows directly from the fact that $\mathfrak{q}'$ is an ideal. If $x \in \mathfrak{q}'$, we can write $x = \frac{r}{s}$ with $r \in R, s \in S$. Then $r = sx \in \mathfrak{q}' \cap R$ and therefore $x \in S^{-1}(\mathfrak{q}' \cap R)$. □

EXERCISE 4.2. Prove that every ideal of $S^{-1}R$ is of the form $S^{-1}I$ for some ideal I of R.

COROLLARY 4.3. *The prime ideals of the ring $R_\mathfrak{p}$ are in bijection with the prime ideals of R contained in $\mathfrak{p}$.*

PROOF. If $S = R\backslash\mathfrak{p}$, then $\mathfrak{q} \cap S = \emptyset$ iff $\mathfrak{q} \subseteq \mathfrak{p}$. □

In particular, the corollary shows that $R_\mathfrak{p}$ is a *local ring*, i.e., a ring having just one maximal ideal. The proof of Proposition 4.1 shows that the unique maximal ideal of $R_\mathfrak{p}$ is just $\mathfrak{p}R_\mathfrak{p}$. For notational convenience, we will sometimes write $\mathfrak{m}_\mathfrak{p}$ instead of $\mathfrak{p}R_\mathfrak{p}$.

For example, the ring $R' = \mathbb{Z}_{(2)}$ consists of all rational numbers which, when written in reduced form, have odd denominator. The unique maximal ideal M' in this ring is the set of all rational numbers with even numerator and odd denominator. Note that every element of $R'\backslash M'$ is a unit in R'. Also, since the difference of any two elements of $R'\backslash M'$ is in M', we see that the quotient ring R'/M' is isomorphic to $\mathbb{Z}/2\mathbb{Z}$.

We generalize some of these observations.

LEMMA 4.4. *Let R be a local ring with maximal ideal $\mathfrak{m}$. Then every element of $R\backslash\mathfrak{m}$ is a unit in R.*

PROOF. This is clear, since every non-unit element of a ring is contained in some maximal ideal. □

LEMMA 4.5. *Let $\mathfrak{m}$ be a maximal ideal in a ring R. If $s \in R\backslash\mathfrak{m}$ then $\mathfrak{m}^n + (s) = (1)$ for all $n \geq 1$, i.e., $\overline{s}$ is a unit in $R/\mathfrak{m}^n$.*

PROOF. This is clear when $n = 1$ by maximality of $\mathfrak{m}$. For general n it follows by induction:

$$(1) = \mathfrak{m}^{n-1} + (s) \Rightarrow \mathfrak{m} = \mathfrak{m}(\mathfrak{m}^{n-1} + (s)) \subsetneq \mathfrak{m}^n + (s).$$

By maximality of $\mathfrak{m}$, it follows that $\mathfrak{m}^n + (s) = (1)$ as desired. □

LEMMA 4.6. *If R is an integral domain and $\mathfrak{p}$ is a maximal ideal of R, then for each $n \geq 1$ the natural map*

$$\phi : R/\mathfrak{p}^n \cong R_\mathfrak{p}/\mathfrak{m}_\mathfrak{p}^n.$$

is an isomorphism of rings. In particular, the residue fields $R/\mathfrak{p}$ and $R_\mathfrak{p}/\mathfrak{m}_\mathfrak{p}$ are isomorphic.

PROOF. To see that ϕ is injective, let $x \in R$ be such that $x \in \mathfrak{m}_\mathfrak{p}^n$, i.e., $x = \frac{y}{s}$ with $y \in \mathfrak{p}^n$ and $s \notin \mathfrak{p}$. By Lemma 4.5, $\overline{s}$ is a unit in $R/\mathfrak{p}^n$. On the other hand, since $sx = y \in \mathfrak{p}^n$, we have $\overline{sx} = 0$ in $R/\mathfrak{p}^n$. Therefore $\overline{x} = 0$ in $R/\mathfrak{p}^n$, i.e., $x \in \mathfrak{p}^n$ as desired.

To see that ϕ is surjective, let $\frac{r}{s} \in R_{\mathfrak{p}}$ with $r \in R, s \notin \mathfrak{p}$. By Lemma 4.5, there exists $r' \in R$ such that $r \equiv r's \pmod{\mathfrak{p}^n}$. But then $\frac{r}{s} \equiv r' \pmod{\mathfrak{m}_{\mathfrak{p}}^n}$, so that $\phi(r') = \frac{r}{s} + \mathfrak{m}_{\mathfrak{p}}^n$. □

Next, we will show that any localization of a Dedekind ring is again a Dedekind ring (or a field), and that the localization of a Dedekind ring at a nonzero prime ideal is a PID.

We start with a couple of easy lemmas. In the statements, R will denote an integral domain, and S will be a multiplicative subset of R.

LEMMA 4.7. *If R is a noetherian integral domain, then so is $S^{-1}R$.*

PROOF. As noted in Exercise 4.2, every ideal of $S^{-1}R$ is of the form $S^{-1}I$ for some ideal I of R. If $x_1, \ldots, x_n$ generate I, then it is easy to see that $x_1, \ldots, x_n$ also generate $S^{-1}I$. □

LEMMA 4.8. *If R is integrally closed, then so is $S^{-1}R$.*

PROOF. Suppose $x = \frac{a}{b} \in K$ satisfies a monic polynomial relation $x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 = 0$ with coefficients $a_i = \frac{r_i}{s_i} \in S^{-1}R$. Then letting $s = s_0 s_1 \cdots s_{n-1} \in S$ and multiplying through by s^n to clear denominators, we find that

$$(sx)^n + a_{n-1}s(sx)^{n-1} + \cdots + a_1 s^{n-1}(sx) + a_0 s^n = 0.$$

Since $sa_i \in R$ for all i, this shows that sx is integral over R. As R is integrally closed, we must have $sx \in R$, and therefore $x \in S^{-1}R$ as desired. □

PROPOSITION 4.9. *If R is a Dedekind ring and S is a multiplicative subset of R, then $S^{-1}R$ is either a field or a Dedekind ring.*

PROOF. It is clear that $S^{-1}R$ is an integral domain, since it is a subring of the fraction field K of R. The two lemmas above show that $S^{-1}R$ is noetherian and integrally closed. Finally, note that since the prime ideals of $S^{-1}R$ are in bijection with the primes ideals of R disjoint from S, and since this bijection is inclusion-preserving, it follows that $S^{-1}R$ has dimension at most 1. This implies the desired result. □

COROLLARY 4.10. *If R is a Dedekind ring, then $R_{\mathfrak{p}}$ is a PID for every nonzero prime ideal $\mathfrak{p}$ of R.*

PROOF. We know that $R_{\mathfrak{p}}$ is a local Dedekind ring whose only prime ideals are (0) and $\mathfrak{m}_{\mathfrak{p}}$. Since every nonzero ideal in a Dedekind ring is a product of prime ideals, it follows that every nonzero ideal of $R_{\mathfrak{p}}$ is a power of $\mathfrak{m}_{\mathfrak{p}}$. Therefore to show that $R_{\mathfrak{p}}$ is a PID, it suffices to show that $\mathfrak{m}_{\mathfrak{p}}$ is principal. For this, choose any element $\pi \in \mathfrak{p} \backslash \mathfrak{p}^2$. We claim that $\mathfrak{m}_{\mathfrak{p}} = \pi R_{\mathfrak{p}}$. To see this, note that we must have $\pi R_{\mathfrak{p}} = \mathfrak{m}_{\mathfrak{p}}^k$ for

some $k \geq 1$. If $k \geq 2$ then $\pi \in \mathfrak{m}_{\mathfrak{p}}^2 \cap R = \mathfrak{p}^2$, a contradiction. Therefore $k = 1$ as desired. □

REMARK 4.11. A *discrete valuation ring* (DVR) is by definition a local PID. The name comes from the fact that every element x of such a ring R can be written as $x = u\pi^n$ for some integer $n \geq 0$, where u is a unit and π generates the maximal ideal of R. The function $v(u\pi^n) = n$ is an example of a *discrete valuation*; it has the property that $(a) = (\pi)^{v(a)}$ for all nonzero elements $a \in R$. The valuation v extends naturally to a function $v : \mathrm{Frac}(R)^* \to \mathbb{Z}$ by setting $v(a/b) = v(a) - v(b)$.

With this terminology, Corollary 4.10 says that if R is a Dedekind ring, then $R_{\mathfrak{p}}$ is a DVR for all nonzero prime ideals $\mathfrak{p}$ of R.

EXAMPLE 4.12. The localization of $\mathbb{Z}$ at the prime ideal $p\mathbb{Z}$ is the ring

$$\mathbb{Z}_{(p)} = \{\frac{a}{b} \in \mathbb{Q} \ : \ a, b \in \mathbb{Z}, \ p \nmid b\} \ .$$

The unique maximal ideal $p\mathbb{Z}_{(p)}$ of this ring consists of all rational numbers a/b (written in lowest terms) such that $p \mid a$ and $p \nmid b$, and the unit group $\mathbb{Z}_{(p)}^*$ consists of all a/b such that $p \nmid a, p \nmid b$. The associated valuation $v_p : \mathbb{Q}^* \to \mathbb{Z}$ is called the *p-adic valuation*, and has the property that if $x = p^k \frac{a}{b} \in \mathbb{Q}^*$ with $k \in \mathbb{Z}$ and a, b relatively prime to p, then $v_p(x) = k$.

We now prove a converse to Corollary 4.10. We begin with the following lemma. In the statement, $\mathrm{Max}(R)$ denotes the set of maximal ideals of R.

LEMMA 4.13. *If R is an integral domain, then*

$$R = \cap_{\mathfrak{p} \in \mathrm{Spec}(R)} R_{\mathfrak{p}} = \cap_{\mathfrak{p} \in \mathrm{Max}(R)} R_{\mathfrak{p}} \ .$$

PROOF. It suffices to prove that $\cap_{\mathfrak{p} \in \mathrm{Max}(R)} R_{\mathfrak{p}} \subseteq R$. Suppose $\frac{a}{b} \in \cap_{\mathfrak{p}} R_{\mathfrak{p}}$ with $a, b \in R$. Define $I = \{y \in R \ : \ ay \in bR\}$. Then I is an ideal of R. Let $\mathfrak{p}$ be a maximal ideal of R. Then by assumption, we have

$$\frac{a}{b} \in R_{\mathfrak{p}} \Rightarrow \frac{a}{b} = \frac{x}{y} \text{ with } x \in R \text{ and } y \notin \mathfrak{p} \ .$$

But then $ya = xb$ and thus $y \in I \backslash \mathfrak{p}$. It follows that I is not contained in any maximal ideal $\mathfrak{p}$ of R, and hence that $I = R$. But then $a = 1 \cdot a \in bR$, i.e., $\frac{a}{b} \in R$. □

THEOREM 4.14. *If R is a Noetherian integral domain which is not a field, then R is a Dedekind ring if and only if $R_{\mathfrak{p}}$ is a PID for all nonzero prime ideals $\mathfrak{p}$ of R.*

PROOF. We already know that if R is Dedekind then $R_{\mathfrak{p}}$ is a PID for all $\mathfrak{p}$. Conversely, suppose $R_{\mathfrak{p}}$ is a PID for all nonzero $\mathfrak{p} \in \mathrm{Spec}(R)$. It follows from Proposition 4.1 that every nonzero prime ideal of R is maximal, since this is true in each $R_{\mathfrak{p}}$. So it suffices to prove that R is integrally closed. But each $R_{\mathfrak{p}}$ is a PID, hence integrally closed, and therefore $\cap_{\mathfrak{p}} R_{\mathfrak{p}} = R$ is integrally closed as well. □

1.2. Rings of S-integers, S-units, and the S-class group. Let R be an integral domain with field of fractions K. It is easy to see from the definition of a prime ideal that if S is any set of prime ideals of R, then the set

$$T := \{x \in R \ : \ x \notin \cup_{\mathfrak{p} \notin S} \mathfrak{p}\}$$

is a multiplicative subset of R.

For the rest of this section, let S be a *finite* subset of $\mathrm{Spec}(R)$. Define

$$R^S := T^{-1}R = \{\frac{x}{y} \in K \ : \ x, y \in R \text{ and } y \notin \mathfrak{p} \text{ for all } \mathfrak{p} \notin S\} \ .$$

If R is a Dedekind ring, then R^S consists of all elements of K which can be written as x/y with (y) divisible only by the prime ideals in S. It follows from Proposition 4.9 that R^S is also a Dedekind ring.

EXAMPLE 4.15. If $R = \mathbb{Z}$ and $S = \{(2), (3)\}$, then

$$R^S := \{\frac{x}{y} \in \mathbb{Q} \ : \ x, y \in \mathbb{Z} \text{ and } y = \pm 2^a 3^b \text{ for some integers } a, b \geq 0\} \ .$$

The relationship between the ideal class groups and unit groups of R and R^S is encoded by the following exercise:

EXERCISE 4.16. Let K be a number field with ring of integers R, and let S be a finite subset of nonzero prime ideals of R. Show that there is a canonical exact sequence of abelian groups

$$1 \to R^* \to (R^S)^* \to \oplus_{\mathfrak{p} \in S} \left(K^*/R_{\mathfrak{p}}^*\right) \to \mathrm{Cl}(R) \to \mathrm{Cl}(R^S) \to 1 \ ,$$

and that $K^*/R_{\mathfrak{p}}^* \cong \mathbb{Z}$ for each $\mathfrak{p} \in S$. [**Hint:** Use Lemma 4.13 to show that $R^* = \cap_{\mathfrak{p}} R_{\mathfrak{p}}^*$.]

When $R = \mathcal{O}_K$ is the ring of integers in a number field K, then $\mathcal{O}_K^S$ is called the *ring of S-integers* in K, the group $\mathrm{Cl}_K^S := \mathrm{Cl}(\mathcal{O}_K^S)$ is called the *S-class group* of K, and $K^S := (\mathcal{O}_K^S)^*$ is called the group of *S-units* of K.

It follows from Exercise 4.16 and the finiteness of $\mathrm{Cl}(\mathcal{O}_K)$ that the S-class group of a number field K is finite. Moreover, from Dirichlet's unit theorem and Exercise 4.16 we see that the torsion subgroup of K^S

is the group W_K of roots of unity contained in K, and (since Cl_K^S is finite) that K^S is finitely generated of rank

$$\mathrm{rank}(K^S) = \mathrm{rank}(\mathcal{O}_K^*) + \mathrm{rank}(\oplus_{\mathfrak{p}\in S}\mathbb{Z}) = |S| + r_1 + r_2 - 1 \ .$$

In summary, we have:

PROPOSITION 4.17. *If K is a number field and S is a finite subset of nonzero prime ideals of $\mathcal{O}_K$, then Cl_K^S is finite and*

$$K^S \cong W_K \times \mathbb{Z}^{|S|+r_1+r_2-1} \ .$$

The latter half of this proposition is sometimes known as *Dirichlet's S-unit theorem.*

EXERCISE 4.18. Let $\overline{\mathbb{Q}}$ denote an algebraic closure of $\mathbb{Q}$. Show that a subgroup G of $\overline{\mathbb{Q}}^*$ is finitely generated if and only if $G \subseteq K^S$ for some number field K and some finite set $S \subset \mathrm{Spec}(\mathcal{O}_K)$.

The main utility of rings of S-integers is that if S is large enough, then $\mathcal{O}_K^S$ is always a PID, as the following result shows:

PROPOSITION 4.19. *If K is a number field, then there exists a finite set S of nonzero prime ideals of $\mathcal{O}_K$ such that $\mathcal{O}_K^S$ is a PID.*

PROOF. By Exercise 4.16, for every S the natural map $\rho : \mathrm{Cl}(\mathcal{O}_K) \to \mathrm{Cl}(\mathcal{O}_K^S)$ given by sending the class of $\mathfrak{a}$ to the class of $\mathfrak{a}\mathcal{O}_K^S$ is surjective. (The surjectivity comes from the fact that the prime ideals of $\mathcal{O}_K^S$ are in bijection with the prime ideals $\mathfrak{p} \notin S$, and $\mathrm{Cl}(\mathcal{O}_K^S)$ is generated by the classes of such prime ideals.) Let $\mathfrak{a}_1, \ldots, \mathfrak{a}_t$ be nonzero ideals of $\mathcal{O}_K$ whose classes generate the finite group $\mathrm{Cl}(\mathcal{O}_K)$, and let S consist of the set of all nonzero prime ideals of $\mathcal{O}_K$ dividing some $\mathfrak{a}_i$. For $\mathfrak{p} \in S$, we have $\mathfrak{p}\mathcal{O}_K^S = (1)$, from which it follows easily that $\rho([\mathfrak{a}_i]) = 1$ for all i. Therefore $\rho(\mathrm{Cl}(\mathcal{O}_K)) = \{1\}$, from which it follows that $\mathrm{Cl}(\mathcal{O}_K^S)$ is trivial. This is equivalent to the statement that $\mathcal{O}_K^S$ is a PID. □

The reader should note that the ring $\mathcal{O}_K^S$ is much "closer" to $\mathcal{O}_K$ than the ring $(\mathcal{O}_K)_{\mathfrak{p}}$, since we have inverted many fewer elements. Thus Proposition 4.19 is a stronger result than Corollary 4.10 in the context of number rings.

1.3. Siegel's theorem and the S-unit equation. This section can be skipped without any loss of continuity. The purpose is to illustrate how to use Proposition 4.19 in practice to prove interesting things.

We begin by stating the following theorem, whose proof is beyond the scope of this course.

THEOREM 4.20 (Siegel, Mahler). *Let K be a number field, let S be a finite set of nonzero prime ideals in $\mathcal{O}_K$, and let $K^S = (\mathcal{O}_K^S)^*$ be the group of S-units in K. Then the equation $x + y = 1$ has only finitely many solutions with $x, y \in K^S$.*

The equation $x + y = 1$ with $x, y \in K^S$ is called the *S-unit equation*. Theorem 4.20 can be proved using methods from the theory of *Diophantine approximation*, for example Roth's theorem. See §D.8 of Hindry and Silverman's book "Diophantine Geometry: An Introduction" for details.

Our goal in the rest of this section is to show that Theorem 4.20 implies a famous theorem of Siegel's which says that there are only finitely many integral points on an elliptic (or more generally hyperelliptic) curve. Without defining these terms, we show more concretely that Theorem 4.20 implies the following result:

THEOREM 4.21 (Siegel). *Let K be a number field, and let S be a finite set of nonzero prime ideals of $\mathcal{O}_K$. Let $f(x) \in K[x]$ be a polynomial of degree at least 3 with distinct roots in $\overline{K}$. Then the equation*

$$Y^2 = f(X)$$

has only finitely many solutions (x, y) with $x, y \in \mathcal{O}_K^S$ (and in particular only finitely many solutions with $x, y \in \mathcal{O}_K$).

REMARK 4.22. Even if one is only interested in proving the finiteness of solutions with $x, y \in \mathcal{O}_K$, the argument we give below requires working in $\mathcal{O}_K^S$ for a sufficiently large finite set S, and it turns out to be no harder to prove the more general result which we have stated.

PROOF. Without loss of generality, we may replace K by a finite extension in order to assume that

$$f(X) = a(X - \alpha_1) \cdots (X - \alpha_n)$$

with $a, \alpha_1, \ldots, \alpha_n \in K$, $a \neq 0$. By hypothesis, we have $n \geq 3$ and the α_i's are all distinct.

We may also clearly enlarge S if we wish. By doing so, we may assume that:

1. $a \in K^S$ and $\alpha_1, \ldots, \alpha_n \in \mathcal{O}_K^S$.
2. $\alpha_i - \alpha_j \in K^S$ for all $i \neq j$.
3. $\mathcal{O}_K^S$ is a PID.

Let L be the compositum (inside a fixed algebraic closure $\overline{K}$ of K) of the fields $K(\sqrt{u})$ for all $u \in K^S$. Since K^S is finitely generated (by Dirichlet's S-unit theorem), the group $K^S/(K^S)^2$ is finite, and therefore L is a *finite* extension of K.

Let T be the set of prime ideals of $\mathcal{O}_L$ containing some element of S, and let $\mathcal{O}_L^T$ be the ring of T-integers in L.

Now suppose that $y^2 = f(x)$ with $x, y \in \mathcal{O}_K^S$.

If $\mathfrak{p}$ is a prime ideal of $\mathcal{O}_K^S$ and $\mathfrak{p} \mid (x - \alpha_i)$, then for $j \neq i$ we have

$$x - \alpha_j = (x - \alpha_i) + (\alpha_i - \alpha_j) \equiv \alpha_i - \alpha_j \not\equiv 0 \pmod{\mathfrak{p}},$$

so that $\mathfrak{p}$ divides *at most one* term $x - \alpha_i$.

Since

$$(x - \alpha_1) \cdots (x - \alpha_n) = a^{-1} y^2$$

and $a \in K^S$, it follows by unique factorization in the Dedekind ring $\mathcal{O}_K^S$ that every prime ideal dividing the ideal $(x - \alpha_i)$ divides it to an even power. Therefore there exist ideals $\mathfrak{a}_i$ of $\mathcal{O}_K^S$ such that $(x - \alpha_i) = \mathfrak{a}_i^2$ for $1 \leq i \leq n$.

As $\mathcal{O}_K^S$ is a PID, we have $\mathfrak{a}_i = (a_i)$ for some $a_i \in \mathcal{O}_K^S$, so that there exist S-units $u_i \in K^S$ with

$$x - \alpha_i = u_i a_i^2$$

for all i.

Furthermore, we can write $u_i = v_i^2$ with $v_i \in L^T$. Therefore

$$x - \alpha_i = v_i^2 a_i^2 = w_i^2$$

with $w_i \in \mathcal{O}_L^T$.

All of this work so far has been to show that $x - \alpha_i$ is a perfect square in the ring $\mathcal{O}_L^T$ for all i. The key point here is that the ring $\mathcal{O}_L^T$ is independent of x. We now show that this unusual situation places such limitations on x that there are only finitely many choices for it!

We have

$$\alpha_j - \alpha_i = w_i^2 - w_j^2 = (w_i - w_j)(w_i + w_j).$$

Since $\alpha_j - \alpha_i \in K^S$, it follows that $w_i - w_j$ and $w_i + w_j$ are in L^T for all $i \neq j$.

We now use the fact that $n \geq 3$ (we have to use this somewhere!) to write down *Siegel's identities*, which are very useful and completely trivial to prove:

$$\frac{w_1 - w_2}{w_1 - w_3} + \frac{w_2 - w_3}{w_1 - w_3} = 1$$

and

$$\frac{w_1 + w_2}{w_1 - w_3} - \frac{w_2 + w_3}{w_1 - w_3} = 1.$$

By Theorem 4.20, the equation $A + B = 1$ with A, B lying in the finitely generated group L^T has only finitely many solutions.

Therefore there are only finitely many choices for

$$\left(\frac{w_1 - w_2}{w_1 - w_3}\right)\left(\frac{w_1 + w_2}{w_1 - w_3}\right) = \frac{\alpha_2 - \alpha_1}{(w_1 - w_3)^2},$$

and hence only finitely many choices for $w_1 - w_3$.

Therefore there are only finitely many choices for

$$w_1 + w_3 = \frac{\alpha_3 - \alpha_1}{w_1 - w_3}$$

and hence only finitely many choices for

$$w_1 = \frac{1}{2}\left((w_1 - w_3) + (w_1 + w_3)\right).$$

It follows that there are only finitely many choices for

$$x = \alpha_1 + w_1^2.$$

Finally, since $y^2 = f(x)$, we see that for any given value of x, there are at most 2 possibilities for y. □

2. Galois theory and prime decomposition

2.1. Relative extensions. We first recall the statement of Theorem 1.55: Let K be a number field of degree n, and let p be a prime number. Write $p\mathcal{O}_K = \prod_{i=1}^r \mathfrak{p}_i^{e_i}$ with the $\mathfrak{p}_i$'s distinct prime ideals of $\mathcal{O}_K$. Then there exist positive integers f_i such that $N(\mathfrak{p}_i) = p^{f_i}$ for all i, and $\sum_{i=1}^r e_i f_i = n$.

In this section we will prove a more general version of this result for relative extensions where the base field is not necessarily $\mathbb{Q}$. We will use localization to simplify the otherwise more laborious proof.

To state the result, we first need to introduce some notation and definitions. Suppose L/K is a finite extension of fields, and that $B \supseteq A$ are Dedekind rings whose fraction fields are L, K respectively. Assume, moreover, that B is a finitely generated A-module. (For example, if L and K are number fields and $B = \mathcal{O}_L, A = \mathcal{O}_K$, then B is a finitely generated A-module, since it is even finitely generated as a $\mathbb{Z}$-module.) Recall that this implies that B is integral over A.

Note in this situation that $B \cap K = A$. This is because every element of B is integral over A, and A is assumed to be integrally closed in its fraction field K.

Remark 4.23. One can show that if L/K is a finite extension of fields, and if A is a Dedekind ring with field of fractions K, then the integral closure B of A in L is again a Dedekind ring, and B is finitely generated as an A-module. When L/K is *separable*, this can be proved

using the fact that the bilinear form $\langle x, y\rangle = \mathrm{Tr}_{L/K}(xy)$ on the K-vector space L is non-degenerate if L/K is separable. The general case requires some additional facts from the theory of purely inseparable field extensions.

Now suppose $\mathfrak{p}$ is a nonzero prime ideal of A. The field $A/\mathfrak{p}$ is called the *residue field* of $\mathfrak{p}$. We say that a prime ideal $\mathfrak{q}$ of B *lies over* $\mathfrak{p}$ (or that $\mathfrak{p}$ *lies under* $\mathfrak{q}$) if $\mathfrak{q}$ contains $\mathfrak{p}$. This is equivalent to saying that $\mathfrak{q}$ divides the ideal $\mathfrak{p}B$ of B, which by definition is the smallest ideal of B containing $\mathfrak{p}$. (The ideal $\mathfrak{p}B$ may of course not be a prime ideal in B).

LEMMA 4.24. *A prime ideal $\mathfrak{q}$ of B lies over $\mathfrak{p}$ if and only if $\mathfrak{q} \cap A = \mathfrak{p}$.*

PROOF. If $\mathfrak{q} \cap A = \mathfrak{p}$ then certainly $\mathfrak{q} \supseteq \mathfrak{p}$, i.e., $\mathfrak{q}$ lies over $\mathfrak{p}$. Conversely, if $\mathfrak{q} \supseteq \mathfrak{p}$ then $\mathfrak{q} \cap A$ is a prime ideal of A containing $\mathfrak{p}$. Since A is 1-dimensional, $\mathfrak{p}$ is maximal, so we conclude that $\mathfrak{q} \cap A = \mathfrak{p}$ as desired. □

Let $\mathfrak{q}_1, \ldots, \mathfrak{q}_r$ be the prime ideals of B lying over $\mathfrak{p}$, which are exactly the prime ideals appearing in the factorization of the ideal $\mathfrak{p}B$. This is well-defined because of the following lemma.

LEMMA 4.25. *If $\mathfrak{p}$ is a nonzero prime ideal of A, then $\mathfrak{p}B \neq B$.*

PROOF. Let $\pi \in \mathfrak{p} \backslash \mathfrak{p}^2$, so that $\pi A = \mathfrak{p}\mathfrak{a}$ with $\mathfrak{p}$ not dividing $\mathfrak{a}$. Then $\mathfrak{p}$ and $\mathfrak{a}$ are relatively prime in A, so we can write $1 = b + a$ with $b \in \mathfrak{p}$ and $a \in \mathfrak{a}$. If $\mathfrak{p}B = B$, then we would have $aB = a\mathfrak{p}B \subseteq \pi B$. But then $a = \pi x$ for some $x \in B$. As $x = \frac{a}{\pi} \in K$, we have $x \in B \cap K = A$ and therefore $a \in \pi A \subseteq \mathfrak{p}$. But then $1 = b + a \in \mathfrak{p}$, a contradiction. □

EXERCISE 4.26. Show that the residue field $B/\mathfrak{q}_i$ is a finite-dimensional vector space over the residue field $A/\mathfrak{p}$. (Note that if $R \subseteq S$ are rings, I is an ideal of R, and J is an ideal of S containing I, then S/J is naturally an R/I-module.)

Let $f_i = f(\mathfrak{q}_i/\mathfrak{p}) := [B/\mathfrak{q}_i : A/\mathfrak{p}]$ be the *residue degree* of $\mathfrak{q}_i$ over $\mathfrak{p}$. Also, write the prime ideal factorization of $\mathfrak{p}B$ as

$$\mathfrak{p}B = \mathfrak{q}_1^{e_1}\mathfrak{q}_2^{e_2} \cdots \mathfrak{q}_r^{e_r} \ .$$

We call $e_i = e(\mathfrak{q}_i/\mathfrak{p})$ the *ramification index* of $\mathfrak{q}_i$ over $\mathfrak{p}$.

With this terminology, we have:

THEOREM 4.27. *Let L/K be a finite extension of fields. Let $B \supseteq A$ be a finitely generated extension of Dedekind rings with fraction fields*

L, K respectively. Let $\mathfrak{q}_1, \ldots, \mathfrak{q}_r$ be the prime ideals of B lying over the nonzero prime ideal $\mathfrak{p}$ of A. Then

$$\sum_{i=1}^{r} e(\mathfrak{q}_i/\mathfrak{p}) f(\mathfrak{q}_i/\mathfrak{p}) = [L : K].$$

PROOF. Let $S := A \backslash \mathfrak{p}$. We claim that in order to prove the desired formula, we may replace A by $A' = S^{-1}A$, B by $B' = S^{-1}B$, $\mathfrak{p}$ by $\mathfrak{p}' = \mathfrak{p}A'$, and each $\mathfrak{q}_i$ by $\mathfrak{q}_i' = \mathfrak{q}_i B'$. A few remarks are in order to justify this claim:

(i) Since S is a multiplicative subset of A, it is also a multiplicative subset of B. Therefore $S^{-1}B$ is well-defined.
(ii) By Proposition 4.9, A' and B' are both Dedekind rings.
(iii) Since B is finitely generated over A, it follows that B' is finitely generated over A' (use the same set of generators).
(iv) The f_i's don't change after localization. To see this, first note that $\mathfrak{p}'$ is a maximal ideal in A' and $A/\mathfrak{p} \cong A'/\mathfrak{p}'$ by Lemma 4.6. Similarly, since $\mathfrak{q}_i \cap A = \mathfrak{p}$, we have $\mathfrak{q}_i \cap S = \emptyset$, and therefore $\mathfrak{q}_i'$ is a maximal ideal of B'. In addition, we have $B/\mathfrak{q}_i \cong B'/\mathfrak{q}_i'$.
(v) The e_i's don't change after localization. Indeed, it is straightforward to check that after localizing both sides of the equation $\mathfrak{p}B = \mathfrak{q}_1^{e_1} \cdots \mathfrak{q}_r^{e_r}$, we obtain the factorization $\mathfrak{p}B' = (\mathfrak{q}_1')^{e_1} \cdots (\mathfrak{q}_r')^{e_r}$.

For simplicity of notation, we now write A instead of A', etc. What has this localization accomplished? Well, we have reduced to the case where A is a PID! This simplifies the rest of the argument. (Note that B is not necessarily a PID, since Corollary 4.10 only applies to localization at a prime ideal.)

Since A is a PID and B is a finitely generated torsion-free A-module, the structure theorem for finitely generated modules over a PID tells us that B is a free A-module of finite rank. By Exercise 4.28 below, the rank of B over A must be $n = [L : K]$, and $[B/\mathfrak{p}B : A/\mathfrak{p}] = n$ as well.

We have $\mathfrak{p}B = \mathfrak{q}_1^{e_1}\mathfrak{q}_2^{e_2} \cdots \mathfrak{q}_r^{e_r}$, so by the Chinese Remainder Theorem, there is a ring isomorphism

$$B/\mathfrak{p}B \cong \oplus_{i=1}^{r} B/\mathfrak{q}_i^{e_i} \ .$$

It therefore suffices to prove that $\dim_k(B/\mathfrak{q}_i^{e_i}) = e_i f_i$ for each i, where $k = A/\mathfrak{p}$.

As in the proof of Theorem 1.53, by considering the chain of ideals

$$B \supset \mathfrak{q}_i \supset \mathfrak{q}_i^2 \supset \cdots$$

it is enough by induction to prove that $\dim_k(\mathfrak{q}_i^m/\mathfrak{q}_i^{m+1}) = f_i$ for each $m \geq 0$. And for this, it suffices to prove the stronger fact that there is an isomorphism $B/\mathfrak{q}_i \cong \mathfrak{q}_i^m/\mathfrak{q}_i^{m+1}$ for each $m \geq 0$.

This can be verified as in the proof of Theorem 1.53. Alternatively, since $B/\mathfrak{q}_i^m \cong B_{\mathfrak{q}_i}/(\mathfrak{q}_i B_{\mathfrak{q}_i})^m$ for each m, we may without loss of generality replace B by $B_{\mathfrak{q}_i}$ and assume that B is a PID. Writing $\mathfrak{q}_i = (\pi_i)$, the map $B/\mathfrak{q}_i \to \mathfrak{q}_i^m/\mathfrak{q}_i^{m+1}$ given by multiplication by π_i^m is then easily checked to be an isomorphism. □

EXERCISE 4.28. In the proof of Theorem 4.27, assuming that A is a PID, show that the rank of B over A is $n = [L : K]$, and that the dimension of $B/\mathfrak{p}B$ over $A/\mathfrak{p}$ is also n. [**Hint:** For the first part, show that if $x_1, \ldots, x_n$ is a basis for B as an A-module, then it is also a basis for L as a K-vector space. For the second part, show that $\overline{x}_1, \ldots, \overline{x}_n$ gives a basis for $B/\mathfrak{p}B$ as a vector space over $A/\mathfrak{p}$.]

If L/K is a Galois extension, then we can say more about the e_i's and f_i's.

LEMMA 4.29. *If in the setting of Theorem 4.27 the extension L/K is Galois, then the Galois group G of L/K acts transitively on the set of prime ideals of B lying over $\mathfrak{p}$.*

PROOF. Let $\mathfrak{q}_i, \mathfrak{q}_j$ be distinct prime ideals of B lying over $\mathfrak{p}$. Suppose $\sigma\mathfrak{q}_i \neq \mathfrak{q}_j$ for all $\sigma \in G$. Then by the Chinese Remainder Theorem, there exists $x \in B$ such that $x \equiv 0 \pmod{\mathfrak{q}_j}$ and $x \equiv 1 \pmod{\sigma\mathfrak{q}_i}$ for all $\sigma \in G$. It is easy to see that $N_{L/K}(x) = \prod_{\sigma \in G} \sigma x$ lies in $B \cap K = A$, and in fact lies in $\mathfrak{q}_j \cap A = \mathfrak{p}$. But $x \notin \sigma^{-1}\mathfrak{q}_i$ for all $\sigma \in G$, so $\sigma x \notin \mathfrak{q}_i$ for all $\sigma \in G$. This contradicts the fact that $\prod_{\sigma \in G} \sigma x$ belongs to the prime ideal $\mathfrak{p}$. □

COROLLARY 4.30. *If in Theorem 4.27 the extension L/K is Galois, then $e_1 = e_2 = \cdots = e_r$ and $f_1 = f_2 = \cdots = f_r$. Therefore, letting e (resp. f) denote the common value of the e_i's (resp. the f_i's), we have $ref = [L : K]$.*

PROOF. Since the Galois group G of L/K acts transitively on the $\mathfrak{q}_i$'s, given i, j we can find $\sigma \in G$ mapping $\mathfrak{q}_i$ to $\mathfrak{q}_j$. Then applying σ to both sides of the relation

$$\mathfrak{p}B = \mathfrak{q}_1^{e_1}\mathfrak{q}_2^{e_2} \cdots \mathfrak{q}_r^{e_r} \ ,$$

we get

$$\mathfrak{p}B = (\sigma\mathfrak{q}_1)^{e_1}(\sigma\mathfrak{q}_2)^{e_2} \cdots (\sigma\mathfrak{q}_r)^{e_r} \ .$$

As $\sigma\mathfrak{q}_i = \mathfrak{q}_j$, it follows from unique factorization that $e_i = e_j$. Moreover, it is easy to see that σ induces an isomorphism of residue fields

$$\sigma : B/\mathfrak{q}_i \xrightarrow{\sim} B/\mathfrak{q}_j \ ,$$

so that $f_i = f_j$ as desired. □

EXERCISE 4.31. Prove that e and f are multiplicative in towers, in the sense that if $\mathfrak{p}_1 \subset \mathfrak{p}_2 \subset \mathfrak{p}_3$ are nonzero prime ideals contained in the Dedekind rings $A_1 \subset A_2 \subset A_3$, then $e(\mathfrak{p}_3/\mathfrak{p}_1) = e(\mathfrak{p}_3/\mathfrak{p}_2) \cdot e(\mathfrak{p}_2/\mathfrak{p}_1)$ and $f(\mathfrak{p}_3/\mathfrak{p}_1) = f(\mathfrak{p}_3/\mathfrak{p}_2) \cdot f(\mathfrak{p}_2/\mathfrak{p}_1)$.

2.2. Decomposition and inertia groups. For simplicity, we suppose throughout this section that L/K is a *Galois extension of number fields*, [1] and we let $\mathfrak{p}$ be a nonzero prime ideal of $\mathcal{O}_K$.

We have already seen that the action of the Galois group $G = \mathrm{Gal}(L/K)$ on the set of prime ideals of $\mathcal{O}_L$ lying over $\mathfrak{p}$ is transitive. Our goal now is to understand some of the finer structure associated with this action. This investigation will have a number of payoffs. For example, we will be soon able to:

- Describe how rational primes factor in the ring of integers of a cyclotomic field.
- Give examples of number rings which are not monogenic.
- Give a short and insightful proof of Gauss' law of quadratic reciprocity.

Let S be the set of prime ideals of $\mathcal{O}_L$ lying over $\mathfrak{p}$, and fix a particular prime ideal $\mathfrak{q} \in S$. Since the action of G on S is transitive, it follows from group theory that the stabilizer of $\mathfrak{q}$ is a subgroup of G of order $n/r = ef$, where $e = e(\mathfrak{q}/\mathfrak{p})$ and $f = f(\mathfrak{q}/\mathfrak{p})$ are independent of $\mathfrak{q}$, and $n := [L : K]$. We denote this stabilizer by $D_{\mathfrak{q}/\mathfrak{p}}$ (or simply by $D_{\mathfrak{q}}$ when $\mathfrak{p}$ is understood), and call it the *decomposition group* of $\mathfrak{q}$. As we will see later, the decomposition group is so named because it is closely related to the factorization of $\mathfrak{p}$ in $\mathcal{O}_L$. By definition, we have

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

In order to understand the decomposition group better, we now introduce an important homomorphism. Let k (resp. ℓ) denote the residue field $\mathcal{O}_K/\mathfrak{p}$ (resp. $\mathcal{O}_L/\mathfrak{q}$). Then ℓ/k is an extension of finite fields of characteristic p, where $p\mathbb{Z} = \mathfrak{p} \cap \mathbb{Z}$. By definition, we have $f := f(\mathfrak{q}/\mathfrak{p}) = [\ell : k]$.

[1] In principle, everything we are doing here works in the more general context where L/K is a Galois extension of Dedekind domains, all of whose residue fields are finite.

It follows from the theory of finite fields that ℓ/k is a Galois extension. Moreover, the Galois group $\mathrm{Gal}(\ell/k)$ is cyclic, with a natural generator given by the *Frobenius automorphism* of ℓ. (Recall that the Frobenius automorphism is the map which sends x to $x^{|k|}$ for all $x \in \ell$.)

An important observation is the fact that every $\sigma \in D_{\mathfrak{q}/\mathfrak{p}}$ induces an automorphism $\overline{\sigma}$ of $\mathrm{Gal}(\ell/k)$ in a natural way. Indeed, if $\overline{x} \in \ell$, we can lift it to some element $x \in \mathcal{O}_L$, and then we can define $\overline{\sigma}(\overline{x})$ to be the class of $\sigma(x)$ mod $\mathfrak{q}$. We claim that the map $\sigma \mapsto \overline{\sigma}$ is well-defined (independent of the choice of a lifting of $\overline{x}$). Assuming this, it follows easily that this map gives us a natural homomorphism from $D_{\mathfrak{q}/\mathfrak{p}}$ to $\mathrm{Gal}(\ell/k)$.

To see that the map $\sigma \mapsto \overline{\sigma}$ is well-defined, suppose x, x' are both lifts in $\mathcal{O}_L$ of $\overline{x}$, so that $x \equiv x' \pmod{\mathfrak{q}}$. We need to show that $\sigma(x), \sigma(x')$ are congruent modulo $\mathfrak{q}$. But this follows directly from the fact that $\sigma \in D_{\mathfrak{q}/\mathfrak{p}}$, since $x - x' \in \mathfrak{q}$ implies that

$$\sigma(x) - \sigma(x') \in \sigma(\mathfrak{q}) = \mathfrak{q} \ .$$

The next proposition has numerous applications.

PROPOSITION 4.32. *The natural homomorphism $D_{\mathfrak{q}/\mathfrak{p}} \to \mathrm{Gal}(\ell/k)$ sending σ to $\overline{\sigma}$ is surjective.*

PROOF. As ℓ/k is separable, there exists a primitive element $\overline{\alpha}$ for this extension. Since an element of $\mathrm{Gal}(\ell/k)$ is uniquely determined by what it does to $\overline{\alpha}$, it suffices to prove that every conjugate of $\overline{\alpha}$ is of the form $\overline{\sigma}(\overline{\alpha})$ for some $\sigma \in D_{\mathfrak{q}/\mathfrak{p}}$.

Let $\alpha \in \mathcal{O}_L$ be a lift of $\overline{\alpha}$ such that $\alpha \in \mathfrak{q}'$ for all $\mathfrak{q}' \neq \mathfrak{q}$ lying over $\mathfrak{p}$. We can find such an α by the Chinese Remainder Theorem, since this is equivalent to solving the system of congruences

$$\alpha \equiv \overline{\alpha} \pmod{\mathfrak{q}}, \ \alpha \equiv 0 \pmod{\mathfrak{q}'} \ .$$

Let $f(x) \in \mathcal{O}_K[x]$ be the minimal polynomial of α over K, and let $\overline{g}(x) \in k[x]$ be the minimal polynomial of $\overline{\alpha}$ over k. Since every root of $f(x)$ is a Galois conjugate of α, there exists a subset H of G such that

$$f(x) = \prod_{\sigma \in H} (x - \sigma(\alpha)) \ .$$

Let $H' = H \cap D_{\mathfrak{q}/\mathfrak{p}}$. Note that if $\sigma \in G$ and $\sigma \notin D_{\mathfrak{q}/\mathfrak{p}}$, then $\sigma^{-1} \notin D_{\mathfrak{q}/\mathfrak{p}}$. Therefore $\sigma^{-1}\mathfrak{q} \neq \mathfrak{q}$, so that $\alpha \in \sigma^{-1}\mathfrak{q}$ by our choice of α. Equivalently, we have $\sigma(\alpha) \in \mathfrak{q}$ whenever $\sigma \in G \backslash D_{\mathfrak{q}/\mathfrak{p}}$. Therefore, if we

use a bar to denote reduction modulo $\mathfrak{q}$, then we have

$$\begin{aligned}\overline{f}(x) &= \prod_{\sigma\in H}(x-\overline{\sigma(\alpha)}) \\ &= \prod_{\sigma\in H'}(x-\overline{\sigma(\alpha)})\prod_{\sigma\notin H'}(x-\overline{\sigma(\alpha)}) \\ &= x^m\prod_{\sigma\in H'}(x-\overline{\sigma}(\overline{\alpha}))\end{aligned}$$

for some positive integer m.

In particular, all nonzero roots of $\overline{f}(x)$ are of the form $\overline{\sigma}(\overline{\alpha})$ with $\sigma\in D_{\mathfrak{q}/\mathfrak{p}}$. But $\overline{f}(\overline{\alpha})=\overline{f(\alpha)}=0$, so $\overline{g}(x)\mid\overline{f}(x)$. Since 0 is not a root of $\overline{g}(x)$, we must have

$$\overline{g}(x)\mid\prod_{\sigma\in H'}(x-\overline{\sigma}(\overline{\alpha}))\ .$$

Therefore every conjugate of $\overline{\alpha}$ is of the form $\overline{\sigma}(\overline{\alpha})$ for some $\sigma\in D_{\mathfrak{q}/\mathfrak{p}}$, as desired. □

The kernel of the natural map $D_{\mathfrak{q}/\mathfrak{p}}\to\mathrm{Gal}(\ell/k)$ is called the *inertia group* of $\mathfrak{q}$ in G, and is denoted $I_{\mathfrak{q}/\mathfrak{p}}$, or simply $I_{\mathfrak{q}}$ when $\mathfrak{p}$ is understood. Explicitly, we have:

$$I_{\mathfrak{q}}:=\{\sigma\in G\ :\ \sigma(x)\equiv x\ (\mathrm{mod}\ \mathfrak{q})\ \forall x\in\mathcal{O}_L\}\ .$$

Proposition 4.32 implies that $D_{\mathfrak{q}/\mathfrak{p}}/I_{\mathfrak{q}/\mathfrak{p}}\cong\mathrm{Gal}(\ell/k)$. In particular, since the cardinality of $D_{\mathfrak{q}}$ is $e(\mathfrak{q}/\mathfrak{p})f(\mathfrak{q}/\mathfrak{p})$ and the cardinality of $\mathrm{Gal}(\ell/k)$ is $f(\mathfrak{q}/\mathfrak{p})$, we obtain the following:

COROLLARY 4.33. *The inertia group $I_{\mathfrak{q}/\mathfrak{p}}$ has cardinality equal to $e(\mathfrak{q}/\mathfrak{p})$. In particular, $\mathfrak{q}/\mathfrak{p}$ is unramified if and only if $I_{\mathfrak{q}/\mathfrak{p}}=1$.*

Similarly, we deduce the following important result:

COROLLARY 4.34. *The quotient group $D_{\mathfrak{q}/\mathfrak{p}}/I_{\mathfrak{q}/\mathfrak{p}}$ is cyclic of order $f(\mathfrak{q}/\mathfrak{p})$, and there is a canonical element $\mathrm{Frob}_{\mathfrak{q}/\mathfrak{p}}\in D_{\mathfrak{q}/\mathfrak{p}}/I_{\mathfrak{q}/\mathfrak{p}}$ having the property that its image in $\mathrm{Gal}(\ell/k)$ is the Frobenius automorphism. In particular, if $\mathfrak{q}/\mathfrak{p}$ is unramified, then $\mathrm{Frob}_{\mathfrak{q}/\mathfrak{p}}$ is well-defined as an element of the decomposition group $D_{\mathfrak{q}/\mathfrak{p}}$.*

2.3. Decomposition and inertia fields. We will now use Galois theory to study the fixed fields of the groups $D_{\mathfrak{q}/\mathfrak{p}}$ and $I=I_{\mathfrak{q}/\mathfrak{p}}$ defined in the previous section.

We will maintain the basic setup from the previous section. To simplify notation, we fix a prime $\mathfrak{q}$ over $\mathfrak{p}$ and write $D=D_{\mathfrak{q}/\mathfrak{p}}$ and $I=I_{\mathfrak{q}/\mathfrak{p}}$. We also write $e=e(\mathfrak{q}/\mathfrak{p})$ and $f=f(\mathfrak{q}/\mathfrak{p})$. If H is any subgroup of G, we denote by L^H the fixed field of H. By Galois theory, $\mathrm{Gal}(L/L^H)=H$.

We now introduce some common sense terminology: the fixed field L^D of the decomposition group is called the *decomposition field* of $\mathfrak{q}/\mathfrak{p}$,

and the fixed field L^I of the inertia group is called the *inertia field* of $\mathfrak{q}/\mathfrak{p}$. We have the following chain of inclusions:

$$K \subseteq L^D \subseteq L^I \subseteq L.$$

If K' is any intermediate field between K and L, we let $\mathfrak{p}'$ be the prime ideal $\mathfrak{q} \cap \mathcal{O}_{K'}$ of $\mathcal{O}_{K'}$, and we let D' (resp. I') be the decomposition group (resp. the inertia group) of $\mathfrak{q}/\mathfrak{p}'$, which is a subgroup of $\mathrm{Gal}(L/K')$.

LEMMA 4.35. *Let H be a subgroup of G and let $K' := L^H$. Then $D' = D \cap H$ and $I' = I \cap H$.*

PROOF. This follows immediately from the definitions: D is the stabilizer of $\mathfrak{q}$ in G, while D' is the stabilizer of $\mathfrak{q}$ in H, so $D' = D \cap H$. Similarly, I is the kernel of $D \to \mathrm{Gal}(\ell/k)$ and I' is the kernel of $D' \to \mathrm{Gal}(\ell/k') \subseteq \mathrm{Gal}(\ell/k)$, so $I' = I \cap D' = I \cap H$. □

We note that, by Galois theory, if H and H' are subgroups of G, then $L^{H \cap H'} = L^H L^{H'}$. Using this fact, we will see that the decomposition and inertia fields have the following pleasant (and useful) characterizations:

PROPOSITION 4.36. (i) *L^D is the largest intermediate field K' for which $e(\mathfrak{p}'/\mathfrak{p}) = f(\mathfrak{p}'/\mathfrak{p}) = 1$.*
(ii) *L^I is the largest intermediate field K' for which $e(\mathfrak{p}'/\mathfrak{p}) = 1$.*

PROOF. First, we claim that if $K' = L^D$ then $e(\mathfrak{p}'/\mathfrak{p}) = f(\mathfrak{p}'/\mathfrak{p}) = 1$. To see this, note that by Lemma 4.35, we have $D' = D$, so that $e(\mathfrak{q}/\mathfrak{p}')f(\mathfrak{q}/\mathfrak{p}') = e(\mathfrak{q}/\mathfrak{p})f(\mathfrak{q}/\mathfrak{p})$. By the multiplicativity of e and f in towers (Exercise 4.31), we must have $e(\mathfrak{p}'/\mathfrak{p}) = f(\mathfrak{p}'/\mathfrak{p}) = 1$ as claimed. Similarly, if $K' = L^I$, then $I' = I$ and we deduce that $e(\mathfrak{p}'/\mathfrak{p}) = 1$.

We now prove that if K' is any intermediate field between K and L with $e(\mathfrak{p}'/\mathfrak{p}) = f(\mathfrak{p}'/\mathfrak{p}) = 1$, then $K' \subseteq L^D$. For this, write $K' = L^H$ for some subgroup H, and note that since $D' = D \cap H$, we have $L^{D'} = L^D K'$. The hypothesis $e(\mathfrak{p}'/\mathfrak{p}) = f(\mathfrak{p}'/\mathfrak{p}) = 1$ implies, using multiplicativity of e and f in towers, that $|D'| = e(\mathfrak{q}/\mathfrak{p}')f(\mathfrak{q}/\mathfrak{p}') = e(\mathfrak{q}/\mathfrak{p})f(\mathfrak{q}/\mathfrak{p}) = |D|$. Therefore $D' = D$ and $L^D = L^{D'} = L^D K'$, so that $K' \subseteq L^D$ as desired.

Similarly, suppose $K' = L^H$ is any intermediate field between K and L with $e(\mathfrak{p}'/\mathfrak{p}) = 1$. Then on one hand we have $L^{I'} = L^I K'$, and on the other hand (by multiplicativity of ramification indices) we have $|I'| = e(\mathfrak{q}/\mathfrak{p}') = e(\mathfrak{q}/\mathfrak{p}) = |I|$, so that $I' = I$. Therefore $L^I = L^{I'} = L^I K'$, so that $K' \subseteq L^I$ as desired. □

EXERCISE 4.37. Let L/K be a Galois extension of number fields. Suppose $\mathfrak{q}$ is a nonzero prime ideal of $\mathcal{O}_L$ lying over the nonzero prime ideal $\mathfrak{p}$ of $\mathcal{O}_K$. Let $D = D_{\mathfrak{q}/\mathfrak{p}}$ and $I = I_{\mathfrak{q}/\mathfrak{p}}$. Show that:

(i) L^D is the smallest intermediate field K' such that $\mathfrak{q}$ is the only prime ideal of $\mathcal{O}_L$ lying over $\mathfrak{p}' = \mathcal{O}_{K'} \cap \mathfrak{q}$.

(ii) L^I is the smallest intermediate field K' such that $\mathfrak{q}$ is totally ramified over $\mathfrak{p}' = \mathcal{O}_{K'} \cap \mathfrak{q}$.

We have the following useful corollary of Proposition 4.36:

COROLLARY 4.38. *Suppose L_1, L_2 are finite extensions of the number field K, and let $\mathfrak{p}$ be a nonzero prime ideal of $\mathcal{O}_K$. Then $\mathfrak{p}$ is unramified (resp. splits completely) in both L_1 and L_2 if and only if $\mathfrak{p}$ is unramified (resp. splits completely) in L_1L_2.*

PROOF. We will treat the unramified case; the case where $\mathfrak{p}$ splits completely works exactly the same.

If $\mathfrak{p}$ is unramified in L_1L_2, then $\mathfrak{p}$ is unramified in both L_1 and L_2 by multiplicativity of the ramification index in towers. Conversely, suppose $\mathfrak{p}$ is unramified in L_1 and L_2. Let $\mathfrak{p}'$ be a prime of $\mathcal{O}_{L_1L_2}$ lying over $\mathfrak{p}$. Let M be a Galois extension of K containing L_1L_2, and let $\mathfrak{q}$ be a prime ideal of $\mathcal{O}_M$ lying over $\mathfrak{p}'$. Let $I = I_{\mathfrak{q}/\mathfrak{p}}$, and let M^I be the corresponding inertia field. Then M^I contains both L_1 and L_2, since $\mathfrak{q} \cap \mathcal{O}_{L_1}$ and $\mathfrak{q} \cap \mathcal{O}_{L_2}$ are unramified over $\mathfrak{p}$. Therefore $M^I \supseteq L_1L_2$, which implies that $\mathfrak{q} \cap \mathcal{O}_{L_1L_2} = \mathfrak{p}'$ is unramified over $\mathfrak{p}$. □

COROLLARY 4.39. *Suppose L is a finite extension of the number field K, and let M be the Galois closure of L/K. Let $\mathfrak{p}$ be a nonzero prime ideal of $\mathcal{O}_K$. Then $\mathfrak{p}$ is unramified (resp. splits completely) in L if and only if $\mathfrak{p}$ is unramified (resp. splits completely) in M.*

PROOF. If $\mathfrak{p}$ is unramified in L/K, then clearly $\mathfrak{p}$ is also unramified in $\sigma(L)/K$ for each embedding σ of L into $\mathbb{C}$ which fixes K. Since M is the compositum of all such fields $\sigma(L)$, the result follows by induction from Corollary 4.38. (Again, the case where $\mathfrak{p}$ splits completely follows from the exact same argument.) □

2.4. A number ring which is not monogenic. In this section, we apply Corollary 4.38 to give examples of number fields K whose rings of integers are not *monogenic*, i.e., are not of the form $\mathbb{Z}[\alpha]$ for any $\alpha \in \mathcal{O}_K$.

Note that we have already shown that the ring of integers in every quadratic and cyclotomic field is monogenic, so we will have to look elsewhere to find our examples.

Let d_1, d_2 be distinct squarefree integers (different from 1). Define $K_1 = \mathbb{Q}(\sqrt{d_1})$, $K_2 = \mathbb{Q}(\sqrt{d_2})$, and $K = K_1K_2$.

EXERCISE 4.40. Show that $[K : \mathbb{Q}] = 4$.

Suppose now that $\mathcal{O}_K = \mathbb{Z}[\alpha]$ for some $\alpha \in \mathcal{O}_K$. Let $f(x)$ be the minimal polynomial of α over $\mathbb{Q}$. According to Kummer's decomposition theorem, a rational prime p splits completely in K if and only if $f(x)$ splits into four distinct linear factors mod p. If $p = 3$, for example, then this is impossible, since the field $\mathbb{Z}/p\mathbb{Z}$ contains only 3 distinct elements. In particular, 3 can never split completely in K.

By Corollary 4.38, we will have a contradiction if 3 splits completely in both K_1 and K_2, since this would imply that 3 splits completely in K. By Kummer's decomposition theorem, 3 splits completely in $\mathbb{Q}(\sqrt{d})$ if and only if $d \equiv 1 \pmod 3$. We have therefore proved:

THEOREM 4.41. *Let $d_1, d_2 \neq 1$ be distinct squarefree integers congruent to 1 mod 3, and let $K = \mathbb{Q}(\sqrt{d_1}, \sqrt{d_2})$. Then $\mathcal{O}_K$ is not monogenic.*

As a concrete example, the ring of integers in $\mathbb{Q}(\sqrt{7}, \sqrt{10})$ is not monogenic.

REMARK 4.42. In fact, we have proved more: the argument just given shows that under the hypotheses of Theorem 4.41, we have $3 \mid |\mathcal{O}_K/\mathbb{Z}[\alpha]|$ for any $\alpha \in \mathcal{O}_K$ such that $K = \mathbb{Q}(\alpha)$.

2.5. Frobenius elements in $\mathrm{Gal}(L/K)$**.** Suppose that L/K is a Galois extension of number fields with Galois group G, and let $\mathfrak{p}$ be a nonzero prime ideal of $\mathcal{O}_K$. The first question which we address in this section is how the decomposition groups $D_{\mathfrak{q}/\mathfrak{p}}$ and $D_{\mathfrak{q}'/\mathfrak{p}}$ (resp. the inertia groups) are related when $\mathfrak{q}, \mathfrak{q}'$ are distinct primes of $\mathcal{O}_L$ lying over $\mathfrak{p}$.

LEMMA 4.43. *Suppose $\mathfrak{q}, \mathfrak{q}'$ are distinct primes of $\mathcal{O}_L$ lying over $\mathfrak{p}$, and write $\mathfrak{q}' = \sigma\mathfrak{q}$ with $\sigma \in G$. (This is always possible by Lemma 4.29.) Then*

$$D_{\mathfrak{q}'/\mathfrak{p}} = \sigma D_{\mathfrak{q}/\mathfrak{p}} \sigma^{-1}$$

and

$$I_{\mathfrak{q}'/\mathfrak{p}} = \sigma I_{\mathfrak{q}/\mathfrak{p}} \sigma^{-1}.$$

PROOF. We give a proof for the decomposition group, and leave the corresponding fact for the inertia group as an exercise.

$$\begin{aligned} D_{\mathfrak{q}'} &= \{\tau \in G \,:\, \tau\mathfrak{q}' = \mathfrak{q}'\} \\ &= \{\tau \in G \,:\, \tau\sigma\mathfrak{q} = \sigma\mathfrak{q}\} \\ &= \{\tau \in G \,:\, \sigma^{-1}\tau\sigma\mathfrak{q} = \mathfrak{q}\} \\ &= \{\sigma\tau\sigma^{-1} \in G \,:\, \tau\mathfrak{q} = \mathfrak{q}\} \\ &= \sigma\{\tau \in G \,:\, \tau\mathfrak{q} = \mathfrak{q}\}\sigma^{-1} \\ &= \sigma D_{\mathfrak{q}}\sigma^{-1}. \end{aligned}$$

□

COROLLARY 4.44. *If L/K is abelian (i.e., if L/K is Galois and the group $\mathrm{Gal}(L/K)$ is an abelian group), then the groups $D_{\mathfrak{q}/\mathfrak{p}}$ and $I_{\mathfrak{q}/\mathfrak{p}}$ depend only on $\mathfrak{p}$, and not on the chosen prime $\mathfrak{q}$ above $\mathfrak{p}$.*

Because of this corollary, when L/K is abelian we frequently write $D_{\mathfrak{p}}$ instead of $D_{\mathfrak{q}/\mathfrak{p}}$ or $D_{\mathfrak{q}}$, and similarly for inertia groups.

Assume now that L/K is Galois and that $\mathfrak{p}$ is a prime ideal of $\mathcal{O}_K$ which is unramified in $\mathcal{O}_L$. This is equivalent to assuming that $I_{\mathfrak{q}/\mathfrak{p}}$ is trivial for all $\mathfrak{q}$ lying over $\mathfrak{p}$.

Fix a prime ideal $\mathfrak{q}$ lying over $\mathfrak{p}$, and let ℓ/k be the corresponding extension of residue fields. As discussed in Section 2.2, there is then a canonical generator $\mathrm{Frob}_{\mathfrak{q}} = \mathrm{Frob}_{\mathfrak{q}/\mathfrak{p}}$ of $D_{\mathfrak{q}}$. It is the unique element of $D_{\mathfrak{q}}$ which maps to the Frobenius automorphism in $\mathrm{Gal}(\ell/k)$. Equivalently, $\mathrm{Frob}_{\mathfrak{q}}$ can be characterized as the unique automorphism σ in $D_{\mathfrak{q}}$ such that

$$\sigma(x) \equiv x^{N(\mathfrak{p})} \pmod{\mathfrak{q}} \; \forall x \in \mathcal{O}_L, \tag{4.1}$$

since $N(\mathfrak{p}) = |k|$ by definition.

In fact, $\mathrm{Frob}_{\mathfrak{q}}$ is the unique element of the Galois group G with this property, since (4.1) clearly implies that $\sigma\mathfrak{q} = \mathfrak{q}$ and hence $\sigma \in D_{\mathfrak{q}}$.

This is important enough of an observation to state it as a proposition:

PROPOSITION 4.45. $\mathrm{Frob}_{\mathfrak{q}}$ *is the unique element $\sigma \in G$ such that*

$$\sigma(x) \equiv x^{N(\mathfrak{p})} \pmod{\mathfrak{q}} \; \forall x \in \mathcal{O}_L.$$

The importance of $\mathrm{Frob}_{\mathfrak{q}}$ can partly be seen in the fact that its order in G is precisely $f(\mathfrak{q}/\mathfrak{p})$. We will exploit this fact in the next section.

Next, we would like to know how $\mathrm{Frob}_{\mathfrak{q}}$ depends on $\mathfrak{q}$. The answer is not surprising, in view of Lemma 4.43, and we leave it as an exercise to supply a proof.

EXERCISE 4.46. Let L/K be a Galois extension of number fields with Galois group G. Suppose $\mathfrak{q}, \mathfrak{q}'$ are prime ideals of $\mathcal{O}_L$ lying over

$\mathfrak{p}$, and assume that $\mathfrak{p}$ is unramified in L. If $\mathfrak{q}' = \sigma\mathfrak{q}$ with $\sigma \in G$, show that

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

REMARK 4.47. We see, in particular, that if L/K is *abelian*, then the Frobenius element $\mathrm{Frob}_{\mathfrak{q}/\mathfrak{p}}$ of G depends only on $\mathfrak{p}$, and not on the choice of a particular prime $\mathfrak{q}$ lying over $\mathfrak{p}$.

In general, there is at least a well-defined *conjugacy class* $\mathrm{Frob}_{\mathfrak{p}}$ in G (depending only on $\mathfrak{p}$) whenever $\mathfrak{p}$ is unramified.

If L/K is abelian and $\mathfrak{p}$ is unramified in L, then $\mathrm{Frob}_{\mathfrak{p}}$ satisfies (4.1) for all $\mathfrak{q} \mid \mathfrak{p}$. Since $\mathfrak{p}\mathcal{O}_L$ is the product of all the prime ideals of $\mathcal{O}_L$ lying over it, we conclude by the Chinese Remainder Theorem that:

PROPOSITION 4.48. *If L/K is abelian and $\mathfrak{p}$ is a nonzero prime ideal of $\mathcal{O}_K$ unramified in $\mathcal{O}_L$, then $\mathrm{Frob}_{\mathfrak{p}}$ is the unique element $\sigma \in \mathrm{Gal}(L/K)$ such that*

$$\sigma(x) \equiv x^{N(\mathfrak{p})} \pmod{\mathfrak{p}\mathcal{O}_L} \ \forall x \in \mathcal{O}_L.$$

2.6. Factorization in cyclotomic fields. Suppose $K_m = \mathbb{Q}(\zeta_m)$ is a cyclotomic field, with ζ_m a primitive mth root of unity for some positive integer m. Since $\mathcal{O}_{K_m} = \mathbb{Z}[\zeta_m]$ by Theorem 2.45(d), we know that to find the prime factorization of a rational prime p in $\mathcal{O}_{K_m}$, it suffices by Kummer's criterion to factor the minimal polynomial $\Phi_m(x)$ of ζ_m mod p. *A priori*, it is not obvious that there is a simple rule governing how $\Phi_m(x)$ factors mod p. But in fact, there is a simple and elegant way to determine this factorization. The rule is as follows (where for simplicity, we stick to the case $p \nmid m$).

THEOREM 4.49. *Let m be a positive integer, and let p be a prime not dividing m. Let f be the order of p in $(\mathbb{Z}/m\mathbb{Z})^*$. Then the factorization of (p) into distinct prime ideals in $\mathbb{Z}[\zeta_m]$ has the form $(p) = \mathfrak{p}_1 \cdots \mathfrak{p}_r$, where $f(\mathfrak{p}_i/p) = f$ for all i and $r = \phi(m)/f$.*

COROLLARY 4.50. *With m, p, f, r as above, the cyclotomic polynomial $\Phi_m(x)$ splits into r distinct irreducible factors mod p, each of which has degree f.*

Before proving the theorem, we need to study Frobenius elements in cyclotomic fields.

Note that since $p \nmid m$ by assumption, it follows from Corollary 2.20 and Theorem 2.45(c) that the prime p is unramified in K_m. Therefore $I_{\mathfrak{p}/p} = 1$ for all $\mathfrak{p} \mid p$. Also, $K_m/\mathbb{Q}$ is abelian, so it follows from Remark 4.47 that Frob_p is well-defined as an element of $\mathrm{Gal}(K_m/\mathbb{Q})$. The following lemma identifies the Frobenius element Frob_p explicitly; for

the statement, recall that $\mathrm{Gal}(K_m/\mathbb{Q})$ consists of the elements σ_t for $(t,m)=1$, where $\sigma_t(\zeta_m)=\zeta_m^t$.

LEMMA 4.51. *If $K_m=\mathbb{Q}(\zeta_m)$, p is a prime with $p\nmid m$, and $\mathfrak{p}$ is a prime ideal of $\mathbb{Z}[\zeta_m]$ lying over p, then* $\mathrm{Frob}_p=\sigma_p$.

PROOF. Let $n=\phi(m)$. By Proposition 4.48, Frob_p is the unique element σ of $G=\mathrm{Gal}(K_m/\mathbb{Q})$ such that $\sigma(x)\equiv x^p \pmod p$ for all $x\in\mathbb{Z}[\zeta_m]$. But the automorphism σ_p has this property, since

$$\begin{aligned}\sigma_p(a_0+a_1\zeta_m+\cdots+a_{n-1}\zeta_m^{n-1}) &= a_0+a_1\zeta_m^p+\cdots+a_{n-1}\zeta_m^{(n-1)p}\\ &\equiv (a_0+a_1\zeta_m+\cdots+a_{n-1}\zeta_m^{n-1})^p\end{aligned}$$

modulo p by the binomial formula and Fermat's Little Theorem. Therefore $\mathrm{Frob}_p=\sigma_p$. □

For future use, we note the following corollary:

COROLLARY 4.52. *Let m be a positive integer, and let p be a prime number with $p\nmid m$. If we identify the Galois group G of $K_m/\mathbb{Q}$ with $(\mathbb{Z}/m\mathbb{Z})^*$, then the decomposition group at any prime above p is identified with the cyclic subgroup $\langle p\rangle\subseteq(\mathbb{Z}/m\mathbb{Z})^*$ generated by p.*

We can now prove Theorem 4.49.

PROOF. We know already that $p\nmid m$ implies that p is unramified in K. Also, since $K_m/\mathbb{Q}$ is Galois, we know that $f(\mathfrak{p}_1/p)=\cdots=f(\mathfrak{p}_r/p)=f'$ for some f'. We also know that $rf'=[K_m:\mathbb{Q}]=\phi(m)$. It therefore suffices to prove that $f'=f$.

We do this by showing that if $\mathfrak{p}$ is a fixed prime ideal of $\mathcal{O}_{K_m}$ lying over p, the decomposition group D of $\mathfrak{p}/p$ has order f. (Note that since $e(\mathfrak{p}/p)=1$, the decomposition group has order $f(\mathfrak{p}/p)=f'$).

For this, we recall from above that D is cyclic of order f', and is generated by the Frobenius element $\mathrm{Frob}_p=\sigma_p$ inside G taking ζ_m to ζ_m^p. Since $(\sigma_p)^t=\sigma_{p^t}$, the order f' of the automorphism Frob_p is clearly the smallest positive integer t such that $p^t\equiv 1 \pmod m$. In other words, $f'=f$ as desired. □

As an example, let's see how the prime ideals (2) and (31) factor in the ring $\mathbb{Z}[\zeta_{15}]$.

Since the order of 2 mod 15 is 4 and $\phi(15)=8$, we find that $(2)=\mathfrak{p}_1\mathfrak{p}_2$ with $\mathfrak{p}_1,\mathfrak{p}_2$ distinct prime ideals of norm 16.

On the other hand, the order of 31 mod 15 is 1, so that $(31)=\mathfrak{q}_1\cdots\mathfrak{q}_8$ in $\mathbb{Z}[\zeta_{31}]$, where the $\mathfrak{q}_i$'s are distinct prime ideals of norm 31.

The polynomial counterpart of these results is as follows. Let $\Phi_{15}(x)=x^8-x^7+x^5-x^4+x^3-x+1$ be the minimal polynomial of the primitive 15th roots of unity. Kummer's decomposition theorem

tells us that over $\mathbb{F}_2$, $\Phi_{15}(x)$ splits into 2 distinct irreducible factors of degree 4, and that over $\mathbb{F}_{31}$, $\Phi_{15}(x)$ splits into 8 distinct linear factors. Indeed, according to MAPLE [2] we have

$$\begin{aligned}\Phi_{15}(x) &\equiv (x^4+x^3+1)(x^4+x+1) \pmod 2\\ \Phi_{15}(x) &\equiv (x+3)(x+11)(x+12)(x+13)(x+17)\cdots\\ &\quad (x+21)(x+22)(x+24) \pmod{31}.\end{aligned}$$

As an immediate consequence of Theorem 4.49, we obtain the following important result:

COROLLARY 4.53. *The rational primes which split completely in* $\mathbb{Z}[\zeta_m]$ *are exactly the primes congruent to* 1 *mod* m.

Finally, we mention that one can formulate the following more general version of Theorem 4.49, which deals with the ramified primes as well. We leave this stronger formulation as an exercise for the reader:

EXERCISE 4.54. Let m be a positive integer, and let p be a prime number. Let p^ν be the largest power of p dividing m, let $m' = m/p^\nu$, and let f be the order of p in $(\mathbb{Z}/m'\mathbb{Z})^*$. Then the factorization of (p) into distinct prime ideals in $\mathbb{Z}[\zeta_m]$ has the form $(p) = (\mathfrak{p}_1 \cdots \mathfrak{p}_r)^{\phi(p^\nu)}$, where $f(\mathfrak{p}_i/p) = f$ for all i and $r = \phi(m')/f$.

2.7. Gauss' law of quadratic reciprocity. In this section, we will give a proof of Gauss' celebrated law of quadratic reciprocity. This result is almost certainly in the top five (along with the "Big Kahuna" – Fermat's Last Theorem) in terms of its historical impact on the development of Algebraic Number Theory. First, though, we need some background material on subfields of cyclotomic fields.

Let p be an odd prime, and let $K_p = \mathbb{Q}(\zeta_p)$. The extension $K_p/\mathbb{Q}$ is Galois, with Galois group isomorphic to $(\mathbb{Z}/p\mathbb{Z})^* \cong \mathbb{Z}/(p-1)\mathbb{Z}$. Since a cyclic group of order m has exactly one subgroup of every order dividing m, it follows by Galois theory that K_p contains a unique subfield of order m for all $m \mid p-1$. In particular, K_p contains a unique quadratic subfield L, which we will now determine explicitly.

The "abstract" way to determine L is to use ramification. We know that p is the only rational prime which ramifies in K_p, and it is totally ramified. Since ramification indices are multiplicative, it follows that p is the unique prime which ramifies in L. But for quadratic fields (which are necessarily monogenic), we know that a rational prime ℓ ramified

[2] To obtain these results, use the Maple commands:
with(numtheory); Phi(x) := cyclotomic(15,x); Factor(Phi(x)) mod 2; Factor(Phi(x)) mod 31;

in L if and only if $\ell \mid \Delta_L$. Furthermore, if $L = \sqrt{d}$ with d squarefree, then $\Delta_L = d$ (resp. $4d$) if $d \equiv 1 \pmod 4$ (resp. $d \equiv 2, 3 \pmod 4$). Therefore the only quadratic field in which p is the unique prime which ramifies is $L = \mathbb{Q}(\sqrt{p^*})$, where $p^* = (-1)^{\frac{p-1}{2}} p$. This is because $p^* \equiv 1 \pmod 4$, so that $|\Delta_{\mathbb{Q}(\sqrt{p^*})}| = p$, whereas $|\Delta_{\mathbb{Q}(\sqrt{-p^*})}| = 4p$.

In summary, we have proved:

PROPOSITION 4.55. *Let p be a prime number, and let $p^* = (-1)^{\frac{p-1}{2}} p$. Then the cyclotomic field K_p contains a unique quadratic subfield L, and L is isomorphic to $\mathbb{Q}(\sqrt{p^*})$.*

REMARK 4.56. A more constructive proof of Proposition 4.55 will be given in §2.8.

We have the following alternative characterization of the unique quadratic subfield of K_p.

LEMMA 4.57. *Let p be a prime, and identify the Galois group of $K_p/\mathbb{Q}$ with $(\mathbb{Z}/p\mathbb{Z})^*$. Let L be the unique quadratic subfield of K_p. Then $L = K_p^H$, where H is the index 2 subgroup of $(\mathbb{Z}/p\mathbb{Z})^*$ consisting of all elements which are squares.*

PROOF. It is clear from group theory that H has index 2 in $(\mathbb{Z}/p\mathbb{Z})^*$. By Galois theory, K_p^H has degree 2 over $\mathbb{Q}$, and must therefore coincide with L. □

Combining our two different characterizations of L (as K_p^H on the one hand and $\mathbb{Q}(\sqrt{p^*})$ on the other), we obtain:

THEOREM 4.58 (Gauss' Law of Quadratic Reciprocity). *Let p, q be distinct odd primes. Then*

$$(\frac{p}{q}) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}} (\frac{q}{p}).$$

PROOF. Since $(\frac{-1}{q}) = (-1)^{\frac{q-1}{2}}$ by elementary considerations, quadratic reciprocity is equivalent to the assertion

$$(\frac{p^*}{q}) = (\frac{q}{p}) \ .$$

Now note that on one hand, since $L = \mathbb{Q}(\sqrt{p^*})$, it follows by Kummer's criterion that q splits completely in L if and only if $x^2 - p^*$ factors into linear factors modulo q, i.e., if and only if $(\frac{p^*}{q}) = 1$.

On the other hand, let $D = \langle q \rangle \subseteq (\mathbb{Z}/p\mathbb{Z})^*$ be the decomposition group at any prime ideal $\mathfrak{q}$ lying over q in $K_p/\mathbb{Q}$, and recall that K_p^D is the largest subfield of K_p in which q splits completely. Since $L = K_p^H$,

where H is the subgroup of squares in $(\mathbb{Z}/p\mathbb{Z})^*$, we find by Galois theory that

$$q \text{ splits completely in } L \Leftrightarrow L = K_p^H \subseteq K_p^D \Leftrightarrow D = \langle q \rangle \subseteq H \Leftrightarrow (\frac{q}{p}) = 1.$$

□

Although there are many more elementary proofs of quadratic reciprocity, this proof we have just given is arguably the most important and most insightful one. It guided E. Artin to formulate and prove a deep result now known as Artin's Reciprocity Law, which is one of the cornerstones of Class Field Theory and generalizes all previously known reciprocity laws.

2.8. Gauss sums. In this section, we give a more constructive proof of Proposition 4.55 using *Gauss sums*. We also use Gauss sums to give another proof of the law of quadratic reciprocity.

Let $\zeta_p = e^{2\pi i/p}$ as usual, and let

$$g := \sum_{t \in (\mathbb{Z}/p\mathbb{Z})^*} (\frac{t}{p}) \zeta_p^t \in \mathbb{Z}[\zeta_p] \ .$$

We need:

LEMMA 4.59. *Let $b \in \mathbb{Z}$. Then*

$$\sum_{t \in (\mathbb{Z}/p\mathbb{Z})} \zeta_p^{bt} = \begin{cases} 0 & b \not\equiv 0 \pmod{p} \\ p & b \equiv 0 \pmod{p}. \end{cases}$$

PROOF. This follows easily from the fact that if $b \not\equiv 0 \pmod{p}$, then

$$\sum_{t \in (\mathbb{Z}/p\mathbb{Z})} \zeta_p^{bt} = \frac{\zeta_p^{bp} - 1}{\zeta_p^b - 1} = 0.$$

□

PROPOSITION 4.60. *In $\mathbb{Z}[\zeta_p]$, we have the relation $g^2 = p^*$.*

REMARK 4.61. In particular, this gives an independent proof of the fact that K_p contains the quadratic field $\mathbb{Q}(\sqrt{p^*})$.

PROOF. For $a \in (\mathbb{Z}/p\mathbb{Z})$, define $g_a = \sum_{t \in (\mathbb{Z}/p\mathbb{Z})^*} (\frac{t}{p}) \zeta_p^{at}$. We claim that $g_a = (\frac{a}{p}) g$. If $a = 0$, this formula follows from the fact that the number of squares in $(\mathbb{Z}/p\mathbb{Z})^*$ equals the number of nonsquares.

Otherwise, if $a \in (\mathbb{Z}/p\mathbb{Z})^*$ then multiplication by a is an automorphism of $(\mathbb{Z}/p\mathbb{Z})^*$, and therefore

$$(\frac{a}{p})g_a = \sum_{t\in(\mathbb{Z}/p\mathbb{Z})^*} (\frac{at}{p})\zeta_p^{at} = \sum_{b\in(\mathbb{Z}/p\mathbb{Z})^*} (\frac{b}{p})\zeta_p^{b} = g,$$

which proves the claim.

We now prove the proposition by evaluating the sum

$$\sum_{a\in(\mathbb{Z}/p\mathbb{Z})} g_a g_{-a}$$

in two different ways.

On one hand, the claim implies that

$$g_a g_{-a} = (\frac{a}{p})(\frac{-a}{p})g^2 = \begin{cases} 0 & a = 0 \\ (\frac{-1}{p})g^2 & a \neq 0. \end{cases}$$

Therefore

$$\sum_{a\in(\mathbb{Z}/p\mathbb{Z})} g_a g_{-a} = \sum_{a\in(\mathbb{Z}/p\mathbb{Z})^*} (\frac{-1}{p})g^2 = (p-1)(\frac{-1}{p})g^2.$$

On the other hand, we have

$$g_a g_{-a} = \sum_{x,y\in(\mathbb{Z}/p\mathbb{Z})^*} (\frac{x}{p})(\frac{y}{p})\zeta_p^{ax}\zeta_p^{-ay} = \sum_{x,y\in(\mathbb{Z}/p\mathbb{Z})^*} (\frac{xy}{p})\zeta_p^{a(x-y)}.$$

Using Lemma 4.59, we therefore have

$$\sum_{a\in(\mathbb{Z}/p\mathbb{Z})} g_a g_{-a} = \sum_{x,y\in(\mathbb{Z}/p\mathbb{Z})^*} (\frac{xy}{p}) \sum_{a\in(\mathbb{Z}/p\mathbb{Z})} \zeta_p^{a(x-y)} = p(p-1).$$

The result follows. □

We conclude this section with a second proof of the law of quadratic reciprocity.

PROOF. Let p, q be odd primes, and let $g = \sum_{t=0}^{p-1}(\frac{t}{p})\zeta_p^t$. By the binomial theorem and Lemma 4.59, we have

$$g^q \equiv \sum_{t=0}^{p-1}(\frac{t}{p})\zeta_p^{tq} = g_q = (\frac{q}{p})g \pmod{q\mathbb{Z}[\zeta_p]}.$$

By Proposition 4.60, if we multiply both sides of this congruence by g, we obtain

$$p^* \cdot (p^*)^{\frac{q-1}{2}} \equiv (\frac{q}{p})p^* \pmod{q\mathbb{Z}[\zeta_p]}$$

and therefore (since p and q are relatively prime)

$$(p^*)^{\frac{q-1}{2}} \equiv (\frac{q}{p}) \pmod{q\mathbb{Z}[\zeta_p]}. \tag{4.2}$$

On the other hand, Euler's criterion from elementary number theory implies that

$$(p^*)^{\frac{q-1}{2}} \equiv (\frac{p^*}{q}) \pmod{q\mathbb{Z}[\zeta_p]} \ . \tag{4.3}$$

Combining (4.2) and (4.3), and using the fact that q is odd, yields the desired equality

$$(\frac{p^*}{q}) = (\frac{q}{p}) \ .$$

□

3. Exercises for Chapter 4

(1) Let A be an integral domain, and let S be a multiplicative subset of A.
   (a) Prove that every ideal of $S^{-1}A$ is of the form $S^{-1}I$ for some ideal I of A.
   (b) Let $g : A \to B$ be a ring homomorphism such that $g(s)$ is a unit in B for all $s \in S$. Prove that there is a unique ring homomorphism $h : S^{-1}A \to B$ such that $g = h \circ f$, where $f : A \to S^{-1}A$ is the natural inclusion.

(2) Let K be a number field with ring of integers R, and let S be a finite subset of nonzero prime ideals of R.
   (a) Prove that $R^* = \cap_{\mathfrak{p}} R^*_{\mathfrak{p}}$.
   (b) Show that there is a canonical exact sequence of abelian groups

$$1 \to R^* \to (R^S)^* \to \oplus_{\mathfrak{p} \in S} \left(K^*/R^*_{\mathfrak{p}}\right) \to \mathrm{Cl}(R) \to \mathrm{Cl}(R^S) \to 1 \ .$$

   (c) Prove that $K^*/R^*_{\mathfrak{p}} \cong \mathbb{Z}$ for each $\mathfrak{p} \in S$.
   (d) If K is a number field and $R = \mathcal{O}_K$, use Dirichlet's unit theorem to show that

$$(R^S)^* \cong W_K \times \mathbb{Z}^{r_1+r_2-1+|S|} \ .$$

(3) Let $\overline{\mathbb{Q}}$ denote an algebraic closure of $\mathbb{Q}$. Show that a subgroup G of $\overline{\mathbb{Q}}^*$ is finitely generated if and only if $G \subseteq (\mathcal{O}_K^S)^*$ for some number field K and some finite set S of nonzero prime ideals of $\mathcal{O}_K$.

(4) Prove that e and f are multiplicative in towers, in the sense that if $\mathfrak{p}_1 \subset \mathfrak{p}_2 \subset \mathfrak{p}_3$ are nonzero prime ideals contained in the number rings $A_1 \subset A_2 \subset A_3$, then $e(\mathfrak{p}_3/\mathfrak{p}_1) = e(\mathfrak{p}_3/\mathfrak{p}_2) \cdot e(\mathfrak{p}_2/\mathfrak{p}_1)$ and $f(\mathfrak{p}_3/\mathfrak{p}_1) = f(\mathfrak{p}_3/\mathfrak{p}_2) \cdot f(\mathfrak{p}_2/\mathfrak{p}_1)$.

(5) Find a prime number p and quadratic extensions K and L of $\mathbb{Q}$ illustrating each of the following:

(a) p can be totally ramified in K and L without being totally ramified in KL.
(b) K and L can each contain unique primes lying over p while KL does not.
(c) p can be inert in K and L without being inert in KL.
(d) The residue degrees of p in K and L can be 1 without being 1 in KL.

(6) Let L/K be a Galois extension of number fields with Galois group G. Suppose $\mathfrak{q}, \mathfrak{q}'$ are prime ideals of $\mathcal{O}_L$ lying over $\mathfrak{p}$, and assume that $\mathfrak{p}$ is unramified in L. If $\mathfrak{q}' = \sigma\mathfrak{q}$ with $\sigma \in G$, show that

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

(7) Let L/K be a Galois extension of number fields. Suppose $\mathfrak{q}$ is a nonzero prime ideal of $\mathcal{O}_L$ lying over the nonzero prime ideal $\mathfrak{p}$ of $\mathcal{O}_K$. Let $D = D_{\mathfrak{q}/\mathfrak{p}}$ and $I = I_{\mathfrak{q}/\mathfrak{p}}$. Show that:
(a) L^D is the smallest intermediate field K' such that $\mathfrak{q}$ is the only prime ideal of $\mathcal{O}_L$ lying over $\mathfrak{p}' = \mathcal{O}_{K'} \cap \mathfrak{q}$.
(b) L^I is the smallest intermediate field K' such that $\mathfrak{q}$ is totally ramified over $\mathfrak{p}' = \mathcal{O}_{K'} \cap \mathfrak{q}$.

CHAPTER 5

Introduction to completions

1. The field $\mathbb{Q}_p$

We now turn to the study of absolute values on number fields, and the corresponding completions. The idea is to generalize the well-known construction of the real numbers as equivalence classes of Cauchy sequences of rational numbers to a wider context. This opens up the door to many new techniques for studying number fields.

Before we give formal definitions, we describe the prototypical example (other than $\mathbb{R}$) of a completion, namely the field $\mathbb{Q}_p$ of p-adic numbers. Because of the large number of details which need to be checked, we proceed in this section mostly without proof. The motivated reader should be able to fill in most of the details herself without too much trouble.

For many more details, and for a number of examples and applications, see e.g. the book "p-adic Numbers" by Fernando Gouvea.

Let p be a prime number, and for $x \in \mathbb{Z}$, $x \neq 0$, let $v_p(x) = \mathrm{ord}_p(x)$ be the maximum power of p dividing x. We can extend v_p to $\mathbb{Q}$ in a natural way by setting $v_p(x/y) = v_p(x) - v_p(y)$ when $x, y \in \mathbb{Z}$ and $y \neq 0$. We also set $v_p(0) = +\infty$ by convention.

For $x \in \mathbb{Q}$, define the *p-adic absolute value* $|x|_p$ of x to be $p^{-\mathrm{ord}_p(x)}$, where by convention we have $|0|_p = 0$. The intuition is that x and y are "p-adically close" when $x - y$ is divisible by a large positive power of p. So for example, $|29-2|_3 = \frac{1}{27}$ and $|3-2|_3 = 1$, which means that 2 and 29 are closer 3-adically than 2 and 3. It is easy to check that $\mathbb{Q}$, together with the function $|\cdot|_p$, defines a normed vector space, and in particular that $\mathbb{Q}$ together with the distance function $d(x, y) = |x - y|_p$ defines a metric space. In fact, the p-adic absolute value satisfies stronger properties than those required to define a metric. More precisely, it is easy to verify that for $x, y \in \mathbb{Q}$ we have:

(1) $|x|_p = 0$ iff $x = 0$.
(2) $|xy|_p = |x|_p \cdot |y|_p$
(3) $|x - y|_p \leq \max\{|x|_p, |y|_p\}$.

The third of these properties goes by various names such as the *ultrametric inequality* or the *non-archimedean triangle inequality*. The point is that it is much stronger than the usual triangle inequality

$$|x - y| \leq |x| + |y|.$$

We want to consider the completion $\mathbb{Q}_p$ of $\mathbb{Q}$ with respect to the absolute value $|\cdot|_p$. Recall that a sequence of elements $\{x_n\}$ in a metric space X is a *Cauchy sequence* with respect to the metric $|\cdot|$ if given $\epsilon > 0$, there exists N such that for $m, n \geq N$, we have $|x_m - x_n| < \epsilon$. We put an equivalence relation on the set of such Cauchy sequences by declaring that $\{x_n\} \sim \{y_n\}$ if $\lim_{n\to\infty} |x_n - y_n| = 0$. By definition, the *completion* of X with respect to $|\cdot|$ is the set of equivalence classes of Cauchy sequences in X.

EXERCISE 5.1. Verify that the completion $\mathbb{Q}_p$ of $\mathbb{Q}$ with respect to the p-adic absolute value is naturally a field.

We call the field $\mathbb{Q}_p$ described in Exercise 5.1 the *field of p-adic numbers*.

EXERCISE 5.2. Show that the absolute value $|\cdot|_p$ extends in a natural way to $\mathbb{Q}_p$, and that this extension still satisfies properties (1)-(3) above for $x, y \in \mathbb{Q}_p$.

The key property possessed by $\mathbb{Q}_p$ which $\mathbb{Q}$ does not have is that it is *complete*, i.e., every Cauchy sequence in $\mathbb{Q}_p$ converges. In fact, $\mathbb{Q}_p$ is the *completion* of $\mathbb{Q}$ with respect to $|\cdot|_p$, in the sense that it is the unique field L (up to isomorphism) containing $\mathbb{Q}$ for which:

- There is an absolute value on L satisfying (1)-(3) above which extends $|\cdot|_p$ on $\mathbb{Q}$.
- $\mathbb{Q}$ is dense in L (with respect to the topology induced by $|\cdot|_p$).
- L is complete with respect to $|\cdot|_p$.

Inside $\mathbb{Q}_p$, there is the important subring $\mathbb{Z}_p$ of p-adic integers, which can be defined as the completion of $\mathbb{Z}$ with respect to $|\cdot|_p$, or as

$$\mathbb{Z}_p = \{x \in \mathbb{Q}_p \ : \ |x|_p \leq 1\} \ .$$

EXERCISE 5.3. Show that

$$p\mathbb{Z}_p := \{x \in \mathbb{Z}_p \ : \ |x|_p < 1\}$$

is the unique maximal ideal of $\mathbb{Z}_p$. In particular, $\mathbb{Z}_p$ is a *local ring*.

EXERCISE 5.4. Show that there is a natural isomorphism

$$\mathbb{Z}_p/p\mathbb{Z}_p \cong \mathbb{Z}/p\mathbb{Z} \ .$$

We rarely think of $\mathbb{R}$ in terms of Cauchy sequences, and the same is true for $\mathbb{Q}_p$. In fact, there are several alternate ways to think of $\mathbb{Q}_p$. For simplicity, we give the descriptions for $\mathbb{Z}_p$, and simply note that $\mathbb{Q}_p$ can then be described as the field of fractions of $\mathbb{Z}_p$. One concrete way to think of $\mathbb{Z}_p$ is in terms of coherent sequences of integers modulo p^n, as follows.

For every integer $n \geq 1$, suppose we are given elements $a_n \in \mathbb{Z}$ such that $0 \leq a_n \leq p^n - 1$ and $a_n \equiv a_{n-1} \pmod{p^{n-1}}$. We call such a sequence $\{a_n\}$ a *coherent (p-adic) sequence*. For example, if $p = 3$, then $\{1, 4, 22, \ldots\}$ is the beginning of a coherent sequence, since $4 \equiv 1 \mod 3$ and $22 \equiv 4 \mod 9$.

We claim that there is a bijection between coherent sequences and elements of $\mathbb{Z}_p$. For on one hand, it is easy to see that a coherent sequence is Cauchy with respect to $|\cdot|_p$, so defines an element of $\mathbb{Z}_p$. Conversely, if $x \in \mathbb{Z}_p$, then it is not hard to show that there exists a unique coherent sequence which converges to x.

Algebraically, this means that the ring $\mathbb{Z}_p$ is the *inverse limit* of the rings $\mathbb{Z}/p^n\mathbb{Z}$.

Using this characterization of elements of $\mathbb{Z}_p$, one can then form "p-adic expansions" analogous to the decimal expansion of real numbers:

THEOREM 5.5. *Every p-adic integer $x \in \mathbb{Z}_p$ can be written uniquely in the form*

$$x = b_0 + b_1 p + \cdots + b_n p^n + \cdots$$

with $b_n \in \{0, 1, 2, \ldots, p-1\}$ for all n.

The proof just comes down to the fact that the sequence of partial sums

$$\{b_0, b_0 + b_1 p, b_0 + b_1 p + b_2 p^2, \ldots\}$$

is a coherent sequence, and conversely every coherent sequence can be written uniquely in this way.

EXERCISE 5.6. Show that a p-adic integer $b = b_0 + b_1 p + b_2 p^2 + \cdots$ is a unit in the ring $\mathbb{Z}_p$ if and only if $b_0 \neq 0$.

Similarly:

THEOREM 5.7. *Every $x \in \mathbb{Q}_p$ can be written uniquely in the form*

$$x = b_{-k} p^{-k} + b_{-k+1} p^{-k+1} + \cdots + b_0 + b_1 p + \cdots + b_n p^n + \cdots$$

for some integer k, where $b_{-k} \neq 0$ and $0 \leq b_n \leq p - 1$ for all n.

EXERCISE 5.8. Show that $v_p(x) = -k$, so that $|x|_p = p^k$.

Arithmetic in $\mathbb{Q}_p$ is done in the "obvious" way. For example, suppose $p = 3$ and

$$x = 1 + 1 \cdot 3 + 2 \cdot 3^2 + 2 \cdot 3^4 + O(3^5),$$
$$y = 1 \cdot 3 + 2 \cdot 3^2 + 1 \cdot 3^4 + O(3^5),$$

where $O(3^5)$ means that all remaining terms are divisible by 3^5, and so are 3-adically "small".

Then we have, for example,

$$x + y = 1 + 2 \cdot 3 + 1 \cdot 3^2 + 1 \cdot 3^3 + O(3^5),$$

which we obtain by adding componentwise and "carrying" the remainders to the right, so for example

$$2 \cdot 3^2 + 2 \cdot 3^2 = 4 \cdot 3^2 = (1 + 3) \cdot 3^2 = 1 \cdot 3^2 + 1 \cdot 3^3.$$

EXERCISE 5.9. Devise a similar algorithm for multiplication of p-adic expansions.

EXERCISE 5.10. Verify the following identities in $\mathbb{Z}_p$:

(1) $\frac{1}{1-p} = 1 + p + p^2 + \cdots + p^n + \cdots$
(2) $-1 = (p-1) + (p-1)p + \cdots + (p-1)p^n + \cdots$

An important property of p-adic numbers is described by the following result:

PROPOSITION 5.11. *A polynomial $F(x) \in \mathbb{Z}[x]$ has a root in $\mathbb{Z}_p$ if and only if $F(x)$ has a root modulo p^n for all $n \geq 1$.*

PROOF. If $F(x)$ has a root in $\mathbb{Z}_p$, then from the natural map $\mathbb{Z}_p \twoheadrightarrow \mathbb{Z}/p^n\mathbb{Z}$ we see that $F(x)$ has a root modulo p^n for all n. Conversely, suppose $F(x)$ has a root modulo p^n for all n. Let (x_n) be a sequence of integers such that $F(x_n) \equiv 0 \pmod{p^n}$ for $n = 1, 2, \ldots$. Since $\mathbb{Z}/p\mathbb{Z}$ is finite, there are infinitely many terms x_n which reduce to the same element $y_1 \in \mathbb{Z}/p\mathbb{Z}$. Therefore there is a subsequence $x_n^{(1)}$ of x_n for which

$$x_n^{(1)} \equiv y_1 \pmod{p} \text{ and } F(x_n^{(1)}) \equiv 0 \pmod{p}$$

for all n. Continuing inductively, we find that for each $k \geq 1$ there is a subsequence $x_n^{(k)}$ of $x_n^{(k-1)}$ for which

$$x_n^{(k)} \equiv y_k \pmod{p^k} \text{ and } F(x_n^{(k)}) \equiv 0 \pmod{p^k}$$

for some $y_k \in \mathbb{Z}/p^k\mathbb{Z}$ such that $y_k \equiv y_{k-1} \pmod{p^{k-1}}$. Then $(y_k)_{k \geq 1}$ forms a coherent sequence, and hence defines an element $y \in \mathbb{Z}_p$ for which $F(y_k) \equiv 0 \pmod{p^k}$ for all k, i.e., for which $F(y) = 0$. □

EXERCISE 5.12. Show that the equation $x^2 = 2$ has two solutions in $\mathbb{Z}_7$, and no solutions in $\mathbb{Z}_3$.

EXERCISE 5.13. Extend Proposition 5.11 to the multivariable case by showing that $F(x_1, \ldots, x_m) \in \mathbb{Z}[x_1, \ldots, x_m]$ has a root modulo p^n for all $n \geq 1$ iff $F(x_1, \ldots, x_m)$ has a root in $(\mathbb{Z}_p)^m$.

2. Absolute values

2.1. Absolute values on a field. Our goal in this section is to present the abstract notion of an absolute value on a field K, and to classify such objects in the case where K is a number field. We continue to omit most proofs for the time being, in order to give an overview of what completions and absolute values are all about.

Let K be a field. An *absolute value* on K is a function $|\cdot| : K \to \mathbb{R}$ such that for all $x, y \in K$:

(1) $|x| \geq 0$, and $|x| = 0$ iff $x = 0$.
(2) $|xy| = |x| \cdot |y|$.
(3) $|x + y| \leq |x| + |y|$.

If $|\cdot|$ satisfies the stronger inequality

(3′) $|x + y| \leq \max\{|x|, |y|\}$,

then it is called a *non-archimedean* (or *ultrametric*) absolute value. Otherwise, $|\cdot|$ is called *archimedean*.

If $|\cdot|$ is an absolute value, the function $v : x \mapsto -\log|x|$ (or any scalar multiple of this function) is called a *valuation*. For example, $|\cdot|_p$ is an absolute value on $\mathbb{Q}$, and $v_p = -\log_p |x|_p$ is the corresponding valuation.

An absolute value makes K into a metric space using the rule $d(x, y) = |x - y|$. If two absolute values $|\cdot|, |\cdot|'$ define the same underlying topology on K (i.e., if $(K, |\cdot|)$ and $(K, |\cdot|')$ have the same open sets), then we call them *equivalent* and write $|\cdot| \sim |\cdot|'$.

The *trivial absolute value* on K is the function sending $x \in K$ to 1 if $x \neq 0$ and 0 if $x = 0$. Every other absolute value on K is called non-trivial.

A *place* of K is an equivalence class of nontrivial absolute values on K. We are typically interested only in those properties of an absolute value which depend only on the underlying place. For example, it is not hard to see that whether or not an absolute value is archimedean depends only on the underlying place. Archimedean places are also called *infinite places*, and the non-archimedean ones *finite places*.

LEMMA 5.14. *Let $|\cdot|, |\cdot|'$ be absolute values on K. Then the following are equivalent:*

(1) *$|\cdot|, |\cdot|'$ are equivalent.*
(2) *$|x| < 1 \Leftrightarrow |x|' < 1$.*
(3) *There is a constant $s > 0$ such that $|x|' = |x|^s$ for all $x \in K$.*

PROOF. If $|\cdot|' = |\cdot|^s$ with $s > 0$, then $|\cdot|$ and $|\cdot|'$ are clearly equivalent. Also, $|x| < 1$ if and only if the sequence (x^n) converges to zero, so if $|\cdot|, |\cdot|'$ are equivalent then $|x| < 1 \Leftrightarrow |x|' < 1$. It remains to show that if $|x| < 1 \Leftrightarrow |x|' < 1$, then there is a constant $s > 0$ such that $|x|' = |x|^s$ for all $x \in K$. For this, fix a nonzero element $y \in K$ with $|y| < 1$. If x is a nonzero element of K, then $|x| = |y|^\alpha$ for some $\alpha \in \mathbb{R}$. Let $\frac{m_i}{n_i}$ be a sequence of rational numbers with $n_i > 0$ converging to α from above. Then $|x| = |y|^\alpha < |y|^{\frac{m_i}{n_i}}$, and therefore $|\frac{x^{n_i}}{y^{m_i}}| < 1$, which implies that $|\frac{x^{n_i}}{y^{m_i}}|' < 1$. This in turn shows that $|x|' \leq (|y|')^\alpha$. Using a sequence $\frac{m_i}{n_i}$ converging to α from below shows that $|x|' \geq (|y|')^\alpha$, and thus $|x|' = (|y|')^\alpha$. It follows that for all nonzero $x \in K$, we have

$$\frac{\log |x|'}{\log |x|} = s \ ,$$

where

$$s = \frac{\log |y|'}{\log |y|} \ ,$$

and thus $|x|' = |x|^s$. Since $|y| < 1$ implies $|y|' < 1$, we must have $s > 0$. □

LEMMA 5.15. *Let $|\cdot|$ be an absolute value on K, and suppose there exists $N > 0$ such that $|n| \leq N$ for all $n \in \mathbb{N}$. Then $|\cdot|$ is non-archimedean.*

PROOF. If $x, y \in K$, then by the binomial theorem and the triangle inequality, we have

$$|x + y|^n \leq N(n + 1) \max\{|x|, |y|\}^n$$

for all $n \geq 1$. Taking n^{th} roots and letting $n \to \infty$ gives

$$|x + y| \leq \max\{|x|, |y|\}$$

as desired. □

We have the following famous theorem describing all places of $\mathbb{Q}$:

THEOREM 5.16 (Ostrowski). *Every archimedean absolute value on $\mathbb{Q}$ is equivalent to the usual absolute value $|\cdot|_\infty$ on $\mathbb{R}$, and every non-trivial non-archimedean absolute value on $\mathbb{Q}$ is equivalent to the p-adic absolute value $|\cdot|_p$ for some prime number p.*

PROOF. Let $|\cdot|$ be a non-trivial absolute value on $\mathbb{Q}$. Suppose first that $|\cdot|$ is non-archimedean. Then $|n| \leq 1$ for all integers $n \geq 1$, and there exists a prime p such that $|p| < 1$ (or else $|\cdot|$ would be trivial). The set $I = \{n \in \mathbb{Z} \ : \ |n| < 1\}$ is an ideal of $\mathbb{Z}$ containing p, and since $|1| = 1$, we have $1 \notin I$. Therefore $I = p\mathbb{Z}$. If $n = mp^k \in \mathbb{Z}$ with $(m, p) = 1$, then $m \notin I$, so $|m| = 1$ and $|n| = |p|^k = |n|_p^s$, where $s = -\log_p |p|$. Therefore $|\cdot|$ is equivalent to $|\cdot|_p$.

Now suppose that $|\cdot|$ is archimedean, and fix integers $n, m > 1$ with n large enough so that $|n| > 1$. Write m in base n as $m = a_0 + a_1 n + \cdots + a_k n^k$ with $a_i \in \{0, 1, \ldots, n-1\}$. Then $k \leq \log_n m$ and $|a_i| \leq a_i |1| < n$, so that

$$|m| \leq \sum |a_i| \cdot |n|^k \leq (1 + \log_n m)\, n \cdot |n|^{\log_n m} \ .$$

(Here we have used the fact that $|n| > 1$ implies $|n|^i \leq |n|^k$ for $i \leq k$.) Substituting m^t for m, taking the t^{th} root of both sides, and letting $t \to \infty$ gives $|m| \leq |n|^{\log_n m}$. Switching the roles of m and n and rearranging the terms gives

$$|m|^{1/\log m} = |n|^{1/\log n} \tag{5.1}$$

whenever $|m|, |n| > 1$. Let $s = \log |n| / \log n$, which by (5.1) is independent of n. Since $|n| > 1$ by assumption, we have $s > 0$. For every positive rational number x, we can write $x = m/n$ with m, n large enough so that $|m|, |n| > 1$, and it follows that

$$|x|_\infty^s = e^{s \log x} = e^{s \log m} / e^{s \log n} = e^{\log |m|} / e^{\log |n|} = |m| / |n| = |x| \ .$$

Since $|-1| = |1|$, it follows that $|x|_\infty^s = |x|$ for all $x \in K$, and therefore $|x|$ is equivalent to $|x|_\infty$. □

In summary, $\mathbb{Q}$ has one archimedean place, corresponding to the "usual" absolute value, and it has one non-archimedean place for each prime number p.

We let $M_{\mathbb{Q}}$ denote the set of places of $\mathbb{Q}$, and for $v \in M_{\mathbb{Q}}$, we let $|\cdot|_v$ be the usual absolute value on $\mathbb{Q}$ if v is archimedean, and the normalized p-adic absolute value $|\cdot|_p$ if v corresponds to a prime number p. We have the following simple but extremely useful result:

PROPOSITION 5.17 (The product formula for $\mathbb{Q}$). *For every nonzero rational number $x \in \mathbb{Q}$, we have*

$$\prod_{v \in M_{\mathbb{Q}}} |x|_v = 1 \ .$$

We leave the (almost trivial) proof to the reader.

We conclude this section with one more useful general result about absolute values, due to Artin and Whaples, which is known as the *Weak Approximation Theorem*. It should be thought of as a valuation-theoretic analogue of the Chinese Remainder theorem.

THEOREM 5.18 (Weak Approximation Theorem). *Let $|\cdot|_1, \ldots, |\cdot|_n$ be pairwise inequivalent absolute values on a field K, and let $a_1, \ldots, a_n \in K$ be arbitrary. Then for every $\epsilon > 0$, there exists $x \in K$ such that $|x - a_i|_i < \epsilon$ for all $1 \leq i \leq n$.*

PROOF. Since $|\cdot|_1$ and $|\cdot|_n$ are not equivalent, it follows from Lemma 5.14 that there exists $\alpha \in K$ such that $|\alpha|_1 < 1$ and $|\alpha|_n \geq 1$. Similarly, there exists $\beta \in K$ such that $|\beta|_n < 1$ and $|\beta|_1 \geq 1$. Setting $y = \beta/\alpha$, we have $|y|_1 > 1$ and $|y|_n < 1$. We claim that there exists $z \in K$ such that $|z|_1 > 1$ and $|z|_j < 1$ for $j = 2, \ldots, n$. We prove this by induction on n. We have just proved this for the base case $n = 2$, and if $|w|_1 > 1$ and $|w|_j < 1$ for $j = 2, \ldots, n-1$, then either $|w|_n \leq 1$, in which case we can set $z = w^m y$ for m sufficiently large, or else $|w|_n > 1$, in which case we can set $z = \frac{w^m}{1+w^m} y$ for m sufficiently large. This proves the claim.

Finally, since $\frac{z^m}{1+z^m}$ converges to 1 with respect to $|\cdot|_1$ and to 0 with respect to $|\cdot|_j$ for $2 \leq j \leq n$, for each $1 \leq i \leq n$ we can (by symmetry) find an element $z_i \in K$ which is arbitrarily close to 1 with respect to $|\cdot|_i$ and arbitrarily close to 0 with respect to $|\cdot|_j$ for $j \neq i$. The element

$$x = a_1 z_1 + \cdots + a_n z_n$$

will then have $|x - a_i|_i < \epsilon$ for all $1 \leq i \leq n$. □

2.2. Absolute values on number fields and their completions. Suppose now that K is a number field. Let $\mathcal{O}_K$ be the ring of integers of K, and let $\mathfrak{p}$ be a nonzero prime ideal of $\mathcal{O}_K$. Then $\mathfrak{p}$ defines an absolute value $|\cdot|_\mathfrak{p}$ on K as follows. Set $|0|_\mathfrak{p} = 0$, and if $\alpha \in K$ is nonzero, define $v_\mathfrak{p}(\alpha) = \mathrm{ord}_\mathfrak{p}(\alpha)$ to be the power of $\mathfrak{p}$ appearing in the factorization of the fractional ideal (α) into prime ideals. Now define

$$|\alpha|_\mathfrak{p} = (N\mathfrak{p})^{-v_\mathfrak{p}(\alpha)} \ . \tag{5.2}$$

(The reason for this normalization will become apparent when we state the product formula for K below.) Then it is easy to verify that $|\cdot|_\mathfrak{p}$ is a non-archimedean absolute value. The completion $K_\mathfrak{p}$ of K with respect to $|\cdot|_\mathfrak{p}$ is easily verified to be a field containing K, and $|\cdot|_\mathfrak{p}$ induces an absolute value on $K_\mathfrak{p}$ which extends the given one on K. Furthermore,

K is dense in $K_\mathfrak{p}$, $K_\mathfrak{p}$ is complete with respect to the induced absolute value, and $K_\mathfrak{p}$ is in fact the unique field with these properties.

We denote by $\hat{\mathcal{O}}_\mathfrak{p}$ the corresponding completion of $\mathcal{O}_K$, which is a subring of $K_\mathfrak{p}$. It is not hard to see that

$$\hat{\mathcal{O}}_\mathfrak{p} = \{x \in K_\mathfrak{p} \ : \ |x|_\mathfrak{p} \leq 1\} \ .$$

Moreover, the set

$$\hat{\mathfrak{m}}_\mathfrak{p} := \{x \in K_\mathfrak{p} \ : \ |x|_\mathfrak{p} < 1\}$$

is clearly an ideal in $\hat{\mathcal{O}}_\mathfrak{p}$. In fact, $\hat{\mathcal{O}}_\mathfrak{p}$ is a local ring and $\hat{\mathfrak{m}}_\mathfrak{p}$ is its unique maximal ideal, since if $x \in \hat{\mathcal{O}}_\mathfrak{p} \backslash \hat{\mathfrak{m}}_\mathfrak{p}$ then $|x^{-1}|_\mathfrak{p} = 1$ and thus $x^{-1} \in \hat{\mathcal{O}}_\mathfrak{p}$.

Note that the *value group*

$$|K^*| = \{|x|_\mathfrak{p} \ : \ x \in K^*\} = \{(N\mathfrak{p})^k \ : \ k \in \mathbb{Z}\}$$

is discrete in $\mathbb{R}^*$. The maximal ideal $\hat{\mathfrak{m}}_\mathfrak{p}$ of $\hat{\mathcal{O}}_\mathfrak{p}$ is therefore principal; this follows from the following more general result:

LEMMA 5.19. *Let $|\cdot|$ be a non-archimedean absolute value on a field K, let $\hat{K}$ be the corresponding completion, let $A = \{x \in K \ : \ |x| \leq 1$ be the valuation ring of $\hat{K}$, and let $\mathfrak{m} = \{x \in A \ : \ |x| < 1\}$ be the unique maximal ideal of A. Then $\mathfrak{m}$ is principal if and only if $|K^*|$ is discrete.*

PROOF. Suppose $|K^*|$ is discrete, and let $\pi \in \mathfrak{m}$ have maximal absolute value. We claim that $\mathfrak{m} = \pi A$. Indeed, if $x \in \mathfrak{m}$, then $|x/\pi| \leq 1$ and thus $x/\pi \in A$, so that $x \in \pi A$. Conversely, suppose $\mathfrak{m} = \pi A$ is principal. Then every $x \in K^*$ can be written as $u \cdot \pi^t$ with $t \in \mathbb{Z}$ and $u \in A^*$, and therefore $|K^*| = \{|\pi|^t \ : \ t \in \mathbb{Z}$, which is a discrete set. □

EXERCISE 5.20. With the notation of the preceding lemma, show that $|K^*| = |(\hat{K})^*|$.

The quotient $\hat{\mathcal{O}}_\mathfrak{p}/\hat{\mathfrak{m}}_\mathfrak{p}$ is canonically isomorphic to the residue field $\mathcal{O}_K/\mathfrak{p}$, which one sees by an argument similar to the proof of Lemma 4.6. More generally, the natural map

$$\psi : \mathcal{O}_K/\mathfrak{p}^n \to \hat{\mathcal{O}}_\mathfrak{p}/\hat{\mathfrak{m}}_\mathfrak{p}^n \tag{5.3}$$

is an isomorphism for all $n \geq 1$.

We sketch a topological proof of (5.3). Since every $x \in \mathcal{O}_K \cap \hat{\mathfrak{m}}_\mathfrak{p}^n$ is a limit of elements of $\mathfrak{p}^n$, and since $\mathfrak{p}^n = \{x \in \mathcal{O}_K \ : \ |x|_\mathfrak{p} \leq 1/(N\mathfrak{p})^n\}$ is closed in the $\mathfrak{p}$-adic topology on $\mathcal{O}_K$, it follows that ψ is injective. Similarly, since $\mathcal{O}_K$ is dense in $\hat{\mathcal{O}}_\mathfrak{p}$, everything in $\hat{\mathcal{O}}_\mathfrak{p}$ is

congruent modulo $\hat{\mathfrak{m}}_{\mathfrak{p}}^n$ to an element of $\mathcal{O}_K$, which means that ψ is injective.

As with $\mathbb{Q}_p$, elements of $K_{\mathfrak{p}}$ have '$\mathfrak{p}$-adic expansions" of the following type. Let π be a *uniformizer* in $\mathcal{O}_K$, i.e., an element of $\mathfrak{p}\backslash\mathfrak{p}^2$. Let S be coset representatives in $\mathcal{O}_K$ for the $N(\mathfrak{p})$ distinct residue classes $\mathcal{O}_K/\mathfrak{p}$. Then we have:

THEOREM 5.21. *Every element $x \in K_{\mathfrak{p}}$ can be written uniquely in the form*

$$x = \sum_{m=-n}^{\infty} a_m \pi^m, \tag{5.4}$$

where $a_m \in S$ for all m and $a_{-n} \not\equiv 0 \mod \mathfrak{p}$. Moreover, we have $n = v_{\mathfrak{p}}(x)$ and $|x|_{\mathfrak{p}} = N(\mathfrak{p})^n$.

PROOF. Let $A = \hat{\mathcal{O}}_{\mathfrak{p}}$ and let $\mathfrak{m} = \hat{\mathfrak{m}}_{\mathfrak{p}}$ be its unique maximal ideal. We have just seen that $\mathfrak{m} = \pi A$. For any sequence $(a_m)_{m \geq -n}$ with $a_m \in S$, let $S_M = \sum_{m=-n}^{M} a_m \pi^m$, and choose $N > M$. Then $|S_M - S_N| \leq |\pi|^{M+1}$, from which one deduces that (S_M) is a Cauchy sequence. This shows that series of the form (5.4) are convergent in $\hat{K} = K_{\mathfrak{p}}$. Conversely, suppose $a \in \hat{K}$. Since $|\hat{K}| = |K|$, we can write $\alpha = u \cdot \pi^n$ with $u \in A^*$. By the definition of S and the isomorphism (5.3), there exists $a_0 \in S$ such that $u - a_0 \in \mathfrak{m}$. As $(u - a_0)/\pi \in A$, there exists $a_1 \in S$ with $\frac{u-a_0}{\pi} - a_1 \in \mathfrak{m}$, i.e., $\pi(u - (a_0 + a_1\pi)) \in \mathfrak{m}^2$. Continuing in this way, we find a sequence $a_1, a_2, \ldots$ for which

$$u = a_0 + a_1\pi + a_2\pi^2 + \cdots$$

and therefore

$$\alpha = \pi^n(a_0 + a_1\pi + a_2\pi^2 + \cdots) .$$

We leave the uniqueness part, as well as the other assertions of the theorem, to the reader. □

The same proof shows that if A is any complete discrete valuation ring with maximal ideal $\mathfrak{m} = \pi A$, then every element $x \in A$ can be written uniquely in the form

$$\sum_{m=0}^{\infty} a_m \pi^m$$

with $a_m \in S$, where S is any fixed set of coset representatives for $A/\pi A$.

EXERCISE 5.22. Prove that $\hat{\mathcal{O}}_{\mathfrak{p}}$ is isomorphic to the inverse limit of $\mathcal{O}_K/\mathfrak{p}^n$ as $n \to \infty$.

The generalized version of Ostrowski's theorem (Theorem 5.16), whose proof we omit, gives a complete description of the places of a number field K:

THEOREM 5.23. *Every archimedean absolute value on K is equivalent to the restriction to K of the usual absolute value on $\mathbb{C}$ for some embedding of K into $\mathbb{C}$, and every non-archimedean absolute value on K is equivalent to the $\mathfrak{p}$-adic absolute value $|\cdot|_{\mathfrak{p}}$ for some nonzero prime ideal $\mathfrak{p}$ of $\mathcal{O}_K$. More precisely, there are bijections:*

$$\{\textit{non-archimedean places of } K\} \leftrightarrow \{\textit{nonzero prime ideals } \mathfrak{p} \textit{ of } \mathcal{O}_K\}$$

$$\begin{aligned}\{\textit{archimedean places of } K\} \leftrightarrow \{&\textit{real embeddings } K \hookrightarrow \mathbb{R}\} \cup \\ &\{\textit{conjugate pairs of complex embeddings } K \hookrightarrow \mathbb{C}\} \ .\end{aligned}$$

The product formula (Proposition 5.17) can be generalized to number fields as follows. Let M_K denote the set of places of K. If v corresponds to a nonzero prime ideal $\mathfrak{p}$ of $\mathcal{O}_K$, define $|x|_v = |x|_{\mathfrak{p}}$ to be the corresponding $\mathfrak{p}$-adic absolute value, as defined in (5.2). If v correponds to an embedding $\sigma : K \hookrightarrow \mathbb{R}$, define $|x|_v = |\sigma(x)|_\infty$, where $|\cdot|_\infty$ denotes the usual absolute value on $\mathbb{R}$. Finally, if v correponds to a complex embedding $\sigma : K \hookrightarrow \mathbb{C}$, define $|x|_v = |\sigma(x)|_\infty^2$, where $|\cdot|_\infty$ denotes the usual absolute value on $\mathbb{C}$. (In this last case, note that $|\cdot|_v$ is not itself an absolute value, since $|\cdot|_\infty^2$ doesn't satisfy the triangle inequality.) With these normalizations, we have the following fundamental result, whose proof we omit:

THEOREM 5.24 (Product formula for number fields). *For every nonzero element $x \in K$, we have*

$$\prod_{v \in M_K} |x|_v = 1 \ .$$

We also state without proof the following theorem, which illustrates one of the many uses for completions in algebraic number theory:

THEOREM 5.25. *If K is a number field and $\mathfrak{p}$ is a nonzero prime ideal of $\mathcal{O}_K$ lying over the rational prime p, then $K_{\mathfrak{p}}$ is a finite extension of $\mathbb{Q}_p$ of degree*

$$[K_{\mathfrak{p}} : \mathbb{Q}_p] = e(\mathfrak{p}/p) \cdot f(\mathfrak{p}/p) \ .$$

Moreover, if $K/\mathbb{Q}$ is Galois, then so is $K_{\mathfrak{p}}/\mathbb{Q}_p$, and

$$\mathrm{Gal}(K_{\mathfrak{p}}/\mathbb{Q}_p) \cong D_{\mathfrak{p}/(p)} \ .$$

3. Hensel's Lemma

Consider the following two examples.

EXAMPLE 5.26. 2 is not a square in $\mathbb{Q}_5$. Indeed, suppose that $\alpha \in \mathbb{Q}_5$ satisfies $\alpha^2 = 2$. Then $|\alpha|_5 = 1$, since $|2|_5 = 1$, and in particular $\alpha \in \mathbb{Z}_5$. Let $\overline{\alpha}$ denote the image of α in the residue field $\mathbb{Z}_5/5\mathbb{Z}_5$; then $\overline{\alpha}^2 = \overline{2}$. But since $\mathbb{Z}_5/5\mathbb{Z}_5 \cong \mathbb{Z}/5\mathbb{Z}$, this would imply that 2 is a square modulo 5, which it is not.

On the other hand:

EXAMPLE 5.27. -1 is a square in $\mathbb{Q}_5$. More precisely, we claim that the equation $x^2 = -1$ has 2 solutions in $\mathbb{Z}_5$, one congruent to 2 and one congruent to 3 modulo 5. To see this, we will find the 5-adic expansions of these numbers explicitly. Write $\alpha = a_0 + a_1 \cdot 5 + a_2 \cdot 5^2 + \cdots$ with $a_i \in \{0, 1, 2, 3, 4\}$, and suppose that $\alpha^2 + 1 = 0$. Since

$$\alpha^2 + 1 = (a_0^2 + 1) + 2a_0a_1 \cdot 5^1 + (2a_0a_2 + a_1^2) \cdot 5^2 + O(5^3) \ ,$$

it follows in particular that $a_0^2 + 1 \equiv 0 \pmod 5$, and therefore $a_0 \equiv \pm 2 \pmod 5$. Suppose $a_0 = 2$ (the other case works the same way). Then the equation $\alpha^2 + 1 \equiv 0 \pmod{5^2}$ implies that

$$(2 + a_1 \cdot 5^1)^2 + 1 \equiv 0 \pmod{5^2} \ ,$$

so that $5 + 20a_1 \equiv 0 \pmod{5^2}$, which implies that $a_1 \equiv 1 \pmod 5$, so that $a_1 = 1$. Similarly, suppose that we have found $c_n = a_0 + a_1 \cdot 5^1 + \cdots + a_n \cdot 5^n$ such that $c_n^2 + 1 \equiv 0 \pmod{5^{n+1}}$, and we want to find a_{n+1} such that

$$(a_0 + a_1 \cdot 5^1 + \cdots + a_n \cdot 5^n + a_{n+1} \cdot 5^{n+1})^2 + 1 \equiv 0 \pmod{5^{n+2}} \ .$$

Then we need to solve the equation

$$(c_n + a_{n+1} \cdot 5^{n+1})^2 + 1 \equiv 0 \pmod{5^{n+1}} \ ,$$

which simplifies to

$$2c_n a_{n+1} \equiv \frac{-1 - c_n^2}{5^{n+1}} \pmod 5 \ ,$$

which means (since $c_n \equiv 2 \pmod 5$ and $4 \equiv -1 \pmod 5$) that

$$a_{n+1} \equiv \frac{1 + c_n^2}{5^{n+1}} \pmod 5 \ .$$

This allows us to inductively solve for all the coefficients of α.

The same argument which was used in the last example can be used to prove a general result called *Hensel's lemma*. A closer look reveals that what actually made the previous argument work was the fact that 2 is a *simple root* of $f(x) = x^2 + 1$ modulo 5.

PROPOSITION 5.28 (Hensel's Lemma). *Let A be a complete discrete valuation ring with maximal ideal $\mathfrak{m} = \pi A$. Let $f(x) \in A[x]$, and let α_0 be a simple root of $f(x)$ modulo π, i.e., $f(\alpha_0) \equiv 0 \pmod{\pi}$ and $f'(\alpha_0) \not\equiv 0 \pmod{\pi}$. Then there exists a unique root $\alpha \in A$ of $f(x)$ with $\alpha \equiv \alpha_0 \pmod{\pi}$.*

PROOF. We prove by induction on n that for each $n \geq 0$, there is an element $\alpha_n \in A$ such that $f(\alpha_n) \equiv 0 \pmod{\pi^{n+1}}$, and such that $\alpha_n \equiv \alpha_{n-1}$ for $n \geq 1$. The base case $n = 0$ is obvious. Suppose we have constucted α_n with the required properties, and write $\alpha_{n+1} = \alpha_n + a\pi^{n+1}$ for some $a \in A$ to be determined. The condition on a is that

$$f(\alpha_{n+1}) = f(\alpha_n + a\pi^{n+1}) \equiv 0 \pmod{\pi^{n+2}} ,$$

which by Taylor's expansion is equivalent to

$$f(\alpha_n) + f'(\alpha_n)(b\pi^{n+1}) \equiv 0 \pmod{\pi^{n+2}} .$$

By hypothesis, this equation has the unique solution

$$b \equiv -\frac{f(\alpha_n)}{\pi^{n+1} f'(\alpha_n)} \pmod{\pi} ,$$

which makes sense because $\pi^{n+1} \mid f(\alpha_n)$ and $f'(\alpha_n) \equiv f'(\alpha_0) \not\equiv 0 \pmod{\pi}$. □

EXAMPLE 5.29. As an application of Proposition 5.28, since $x^p - x$ splits into linear factors over $\mathbb{F}_p$ and has derivative -1, we see that $\mathbb{Z}_p$ contains $p-1$ distinct $(p-1)^{\text{st}}$ roots of unity, one in each nonzero residue class modulo p.

Hensel's lemma can be viewed as a p-adic version of *Newton's method* from calculus for approximating roots of polynomials. Indeed, the proof we have just given can be generalized to show:

PROPOSITION 5.30 (Hensel's Lemma, Version II). *Let K be a field which is complete with respect to a non-archimedean absolute value $|\cdot|$, and let $A = \{x \in K \ : \ |x| \leq 1\}$ be the valuation ring of K. Let $f(x) \in A[x]$, and suppose there exists $\alpha_0 \in A$ with $|f(\alpha_0)| < |f'(\alpha_0)|^2$. Then the sequence defined inductively by*

$$\alpha_{n+1} = \alpha_n - \frac{f(\alpha_n)}{f'(\alpha_n)}$$

converges to a root α of $f(x)$ in A, and

$$|\alpha - \alpha_0| \leq |\frac{f(\alpha_0)}{f'(\alpha_0)^2}| < 1 .$$

Hensel's Lemma can be generalized in many different ways. We give one more version here:

PROPOSITION 5.31 (Hensel's Lemma, Version III). *Let K be a field which is complete with respect to a non-archimedean absolute value $|\cdot|$, and let $A = \{x \in K \ : \ |x| \leq 1\}$ be the valuation ring of K, with maximal ideal $\mathfrak{m}$. Let $f(x) \in A[x]$ be a* primitive *polynomial, meaning that $\overline{f}(x) \in (A/\mathfrak{m})[x]$ is nonzero, and suppose that*

$$\overline{f}(x) = \overline{g}(x) \cdot \overline{h}(x)$$

with $\overline{g}(x), \overline{h}(x) \in (A/\mathfrak{m})[x]$ relatively prime polynomials. Then there exist polynomials $g(x), h(x) \in A[x]$ with $\deg(g) = \deg(\overline{g})$ such that

$$g(x) \equiv \overline{g}(x) \pmod{\mathfrak{m}} \text{ and } h(x) \equiv \overline{h}(x) \pmod{\mathfrak{m}} \ .$$

EXERCISE 5.32. Let p be an odd prime. Show that an element $x \in \mathbb{Q}_p$ is a square if and only if $x = p^{2n}y^2$ for some $n \in \mathbb{Z}$ and $y \in \mathbb{Z}_p^*$. What happens for $p = 2$?

4. Introductory p-adic analysis

Let K be a field which is complete with respect to a non-archimedean absolute value $|\cdot|$, and let A denote the valuation ring of K. In this section, we will investigate some basic properties of power series with coefficients in K. Applications to Diophantine equations and linear recurrence sequences will be given in the next section. In both this section and the next, we follow rather closely the exposition from J.W.S. Cassels' book "Local Fields".

Perhaps the most basic fact in p-adic analysis is the following result, which we leave as a simple exercise to the reader:

EXERCISE 5.33. A series $\sum_{n=0}^{\infty} a_n$ with $a_n \in K$ converges if and only if $|a_n| \to 0$. In particular, a power series $f(x) = \sum_{n=0}^{\infty} a_n x^n \in K[[x]]$ converges for all $x \in A$ if and only if $|a_n| \to 0$.

Note that the corresponding statements over $\mathbb{R}$ are utterly false, despite the beliefs of many Calculus II students.

The *radius of convergence* of a power series $f(x) = \sum_{n=0}^{\infty} a_n x^n \in K[[x]]$ is defined as in the real or complex case to be

$$R = \frac{1}{\limsup_n |a_n|^{1/n}} \in [0, +\infty] \ .$$

EXERCISE 5.34. Let

$$D = \{x \in K \ : \ \sum_{n=0}^{\infty} a_n x^n \text{ converges } \}$$

be the *domain of convergence* of f. Then:

(1) If $R = 0$, then $D = \{0\}$.
(2) If $R = \infty$, then $D = K$.
(3) If $0 < R < \infty$ and $|a_n|R^n$ tends to 0, then $D = \{x \in K \ : |x| \leq R\}$.
(4) If $0 < R < \infty$ and $|a_n|R^n$ does not tend to 0, then $D = \{x \in K \ : \ |x| < R\}$.

EXERCISE 5.35. Show that a power series $f(x) = \sum_{n=0}^{\infty} a_n x^n \in K[[x]]$ is continuous on its domain of convergence.

The following result, concerning rearrangement of double series, is another result whose real or complex analogue is much more delicate:

EXERCISE 5.36. Let $b_{ij} \in K$ for $i, j = 0, 1, 2, \ldots$ Suppose that for every $\epsilon > 0$, there exists M such that $|b_{ij}| < \epsilon$ whenever $\max(i, j) \geq M$. Then the series

$$\sum_i \left(\sum_j b_{ij} \right) \ , \ \sum_j \left(\sum_i b_{ij} \right)$$

both converge, and their sums are equal.

The next result again has no real or complex analogue, and is one of the most useful facts in p-adic analysis:

THEOREM 5.37 (Strassmann's theorem). *Let $f(x) = \sum_{n=0}^{\infty} a_n x^n$ with $a_n \in K$, and suppose that $|a_n| \to 0$ (i.e., $f(x)$ converges for all x in the unit disc A). Suppose furthermore that not all of the coefficients a_n are zero. Define the nonnegative integer $N = N(f)$ by*

$$|a_N| = \max_n |a_n| \ , \ |a_n| < |a_N| \text{ for } n > N \ .$$

Then $f(x)$ has at most N zeroes in A.

PROOF. The proof is by induction on N. For the base case $N = 0$, note that if $f(\alpha) = 0$ for some $\alpha \in A$, then

$$|a_0| = |-\sum_{n \geq 1} a_n \alpha^n| \leq \max_{n \geq 1} |a_n \alpha^n| \leq \max_{n \geq 1} |a_n| < |a_0| \ ,$$

a contradiction. Now suppose that $N \geq 1$, and suppose $f(\alpha) = 0$ with $\alpha \in A$. Then for any $\beta \in A$, we have

$$f(\beta) = f(\beta) - f(\alpha) = \sum_{n \geq 1} a_n(\beta^n - \alpha^n) = (\beta - \alpha) \sum_{n \geq 1} \sum_{j=0}^{n-1} a_n \beta^j \alpha^{n-1-j} \ .$$

By Exercise 5.36, we have $f(\beta) = (\beta - \alpha)g(\beta)$ with

$$g(x) = \sum_{j=0}^{\infty} b_j x^j \ , \ b_j = \sum_{t=0}^{\infty} a_{j+1+t} \alpha^t \ .$$

It is easy to check that $N(g) = N(f) - 1$, and therefore by induction we may assume that $g(x)$ has at most $N-1$ zeros in A. Since $f(\beta) = 0$ iff $\beta = \alpha$ or $g(\beta) = 0$, it follows that $f(x)$ has at most N zeros in A, as desired. □

We conclude our very brief introduction to p-adic analysis with a p-adic version of the binomial theorem.

For $t \in \mathbb{Q}_p$ and n a positive integer, define the *binomial coefficient* $\binom{t}{n}$ by

$$\binom{t}{n} = \begin{cases} \frac{t(t-1)\cdots(t-n+1)}{n!} & n \neq 0 \\ 1 & n = 0. \end{cases}$$

LEMMA 5.38. *If $t \in \mathbb{Z}_p$, then $\binom{t}{n} \in \mathbb{Z}_p$ for all integers $n \geq 0$.*

PROOF. If $t \in \mathbb{Z}$, then it is well-known that $\binom{t}{n} \in \mathbb{Z}$. For fixed n, the map $t \mapsto \binom{t}{n}$ is continuous in the p-adic topology on $\mathbb{Z}_p$, and $|\binom{t}{n}|_p \leq 1$ for all $t \in \mathbb{Z}$. Since $\mathbb{Z}$ is dense in $\mathbb{Z}_p$, it follows that $|\binom{t}{n}|_p \leq 1$ for all $t \in \mathbb{Z}_p$. □

EXERCISE 5.39. (1) If $n \in \mathbb{N}$ and p is a prime, prove that $|n!|_p = p^{-M}$, where

$$M = v_p(n!) = [n/p] + [n/p^2] + [n/p^3] + \cdots$$

(Here $[\cdot]$ denotes the greatest integer function.)

(2) Let s be the sum of the digits in the base p expansion of n. Show that

$$v_p(n) = \frac{n-s}{p-1} \ .$$

(3) In particular, show that $|n!|_p > p^{-\frac{n}{p-1}}$.

The p-adic binomial theorem has two parts; the first is analogous to the usual binomial theorem, and the second is unique to p-adic analysis in that it expands $(1+x)^t$ *as a power series in* t, rather than in x.

THEOREM 5.40 (The p-adic binomial theorem). *Let p be an odd prime.*

1. *If t is a nonnegative integer, then*

$$(1+x)^t = \sum_{n=0}^{t} \binom{t}{n} x^n \tag{5.5}$$

for all $x \in p\mathbb{Z}_p$.

2. *If $x \in p\mathbb{Z}_p$, then there exists a power series*

$$\Phi_x(t) = \sum_{n=0}^{\infty} \gamma_n t^n \in \mathbb{Q}_p[[t]]$$

converging for all $t \in \mathbb{Z}_p$ such that

$$\Phi_x(t) = (1+x)^t$$

for all $t \in \mathbb{Z}$.

REMARK 5.41. With slight modifications, the statement and proof can be modified to work for $p = 2$, and more generally for any finite extension K of $\mathbb{Q}_p$.

PROOF. Since $|\binom{t}{n}|_p \leq 1$ for all t, n, the right-hand side of (5.5) converges and is continuous for all $x \in p\mathbb{Z}_p$. The left-hand side of (5.5) is continuous for all $x \in \mathbb{Q}_p$, since it's a polynomial in x. Also, if $x \in \mathbb{Z}$, then (5.5) holds by the usual binomial theorem. As $p\mathbb{Z}$ is dense in $p\mathbb{Z}_p$, it follows that (5.5) holds for all $x \in p\mathbb{Z}_p$. This proves (1).

To prove (2), suppose first that $t \geq 0$. We use the fact that $\binom{t}{n} = 0$ when $n > t$ to write (5.5) as

$$(1+x)^t = \sum_{n=0}^{\infty} t(t-1)\cdots(t-n+1)\frac{x^n}{n!}\ . \tag{5.6}$$

Since $|x|_p \leq \frac{1}{p}$ by assumption, it follows from Exercise 5.39 that $|\frac{x^n}{n!}|_p \to 0$ as $n \to \infty$. By Exercise 5.36, we may therefore rearrange the terms of (5.6) according to powers of t. Doing so, we obtain a power series representation

$$(1+x)^t = \sum_{n=0}^{\infty} \gamma_n t^n \tag{5.7}$$

where each $\gamma_n \in \mathbb{Q}_p$ is independent of t and $|\gamma_n|_p \to 0$ as $n \to \infty$. This proves the desired result for $t \geq 0$.

Now suppose $t < 0$. Then $p^m + t > 0$ for m sufficiently large, and applying (5.7) with t replaced by $p^m + t$ gives

$$(1+x)^{p^m+t} = \sum_{n=0}^{\infty} \gamma_n (p^m + t)^n \ . \tag{5.8}$$

As $m \to \infty$ (in the usual sense), it follows from (5.7) that $(1+x)^{p^m} \to 1$ in the p-adic topology, and therefore the left-hand side of (5.8) tends to $(1+x)^t$. The right-hand side of (5.8) tends to $\sum \gamma_n t^n$, since $p^m \to 0$ and a power series is continuous in its domain of convergence by Exercise 5.35. Therefore (5.7) holds for $t < 0$ as well. □

EXERCISE 5.42. If p is an odd prime, show that $v_p(n!) \leq n-2$, and conclude that for $x \in p\mathbb{Z}_p$ and $t \in \mathbb{Z}_p$, we have

$$\Phi_x(t) \equiv 1 + tx \pmod{p^2} \ .$$

EXERCISE 5.43. Using Lemma 5.38, we see that if p is an odd prime, $t \in \mathbb{Z}_p$, and $x \in p\mathbb{Z}_p$, then the binomial series

$$B(t,x) = \sum_{n=0}^{\infty} \binom{t}{n} x^n \tag{5.9}$$

converges p-adically. Show that the right-hand side of (5.9) with $p = 7$, $t = 1/2$, and $x = 7/9$ converges to $4/3$ in $\mathbb{R}$ and to a 7-adic number $\alpha \neq 4/3$ in $\mathbb{Q}_7$.

EXERCISE 5.44.

(1) Show that the power series

$$\log_p(x) = \sum_{n=1}^{\infty} (-1)^{n+1} \frac{(x-1)^n}{n}$$

(called the *p-adic logarithm*) converges if and only if $|x-1|_p < 1$.

(2) Show that the power series

$$\exp_p(x) = \sum_{n=0}^{\infty} \frac{x^n}{n!}$$

(called the *p-adic exponential*) converges if and only if $|x|_p < p^{-1/(p-1)}$.

5. Applications to Diophantine equations

5.1. The Diophantine equation $x^3 - 11y^3 = 1$. In this section, we illustrate the utility of p-adic analysis by finding all integer solutions to the Diophantine equation $x^3 - 11y^3 = 1$.

We begin with the observation that if x, y are integers for which $x^3 - 11y^3 = 1$, then $x - y\sqrt[3]{11}$ is a unit of norm 1 in the cubic field $K = \mathbb{Q}(\sqrt[3]{11})$. Let $\alpha = \sqrt[3]{11}$. Recall from Example 3.44 that the fundamental unit in K is

$$u = 18\alpha^2 + 40\alpha + 89 \ ,$$

and that $v = 1/u = -2\alpha^2 + 4\alpha + 1$. A short calculation shows that both of these units have norm 1. Since every unit in $\mathcal{O}_K$ has the form $\pm v^n$ ($n \in \mathbb{Z}$), and since $N_{K/\mathbb{Q}}(-1) = -1$, it follows that every unit of norm 1 in K can be written as v^n for some integer n. We will now show that $x - y\sqrt[3]{11} = v^n$ implies that $n = 0$.

PROPOSITION 5.45. *If $x - y\sqrt[3]{11} = v^n$ with $x, y, n \in \mathbb{Z}$, then $n = 0$.*

PROOF. As noted in Example 3.44, the prime 19 splits completely in K. Equivalently, there are three distinct roots in $\mathbb{F}_{19}$ to the equation $x^3 - 11 = 0$. By Hensel's Lemma, there are three distinct solutions $\alpha_1, \alpha_2, \alpha_3$ to $x^3 - 11 = 0$ in $\mathbb{Q}_{19}$, and a short computation shows that, after relabelling if necessary, we have

$$\begin{aligned}
\alpha_1 &= -3 + 5 \cdot 19 + O(19^2) \\
\alpha_2 &= -2 + 8 \cdot 19 + O(19^2) \\
\alpha_3 &= 5 + 6 \cdot 19 + O(19^2)
\end{aligned}$$

The three different cube roots of 11 in $\mathbb{Q}_{19}$ correspond to three different embeddings ψ_1, ψ_2, ψ_3 of K into $\mathbb{Q}_{19}$. A calculation shows that, letting $v_i = \psi_i(v) \in \mathbb{Q}_{19}$, we have:

$$\begin{aligned}
v_1 &= 9 + 2 \cdot 19 + O(19^2) \\
v_2 &= 4 + 0 \cdot 19 + O(19^2) \\
v_3 &= 9 + 6 \cdot 19 + O(19^2)
\end{aligned}$$

Since $x - y\sqrt[3]{11} = v^n$ in K, we have $x - y\alpha_i = v_i^n$ in $\mathbb{Q}_{19}$ for $i = 1, 2, 3$. In particular, noting that

$$\begin{aligned}
\alpha_1 + \alpha_2 + \alpha_3 &= -\{ \text{ coefficient of } x^2 \text{ in } x^3 - 11\} = 0 \ , \\
\alpha_1^2 + \alpha_2^2 + \alpha_3^2 &= -\{ \text{ coefficient of } x^2 \text{ in } x^3 - 11^2\} = 0 \ ,
\end{aligned}$$

it follows that

$$\alpha_1 v_1^n + \alpha_2 v_2^n + \alpha_3 v_3^n = 0 \ . \tag{5.10}$$

The advantage of (5.10), of course, is that we have eliminated the unknown quantities x and y. We would like to use the p-adic binomial theorem to expand the left-hand side of (5.10) as a power series in n. Unfortunately, we cannot do this directly, since v_1, v_2, v_3 are not

congruent to 1 modulo 19. However, with a bit of manipulation, we can rewrite (5.10) in such a way that the p-adic binomial theorem will apply.

Since $N_{K/\mathbb{Q}}(v) = 1$, it follows as above that $v_1 v_2 v_3 = 1$ Multiplying both sides of (5.10) by $v_2^n v_3^n$, we obtain

$$\alpha_1 + \alpha_2 \beta_2^n + \alpha_3 \beta_3^n = 0 \tag{5.11}$$

with $\beta_2 = v_2^2 v_3 \equiv 11 \pmod{19}$ and $\beta_3 = v_2 v_3^2 \equiv 1 \pmod{19}$. In particular,

$$2 - 2 \cdot 11^n \equiv 0 \pmod{19} ,$$

which means that $11^n \equiv 1 \pmod{19}$, i.e., $n \equiv 0 \pmod{3}$. Writing $n = 3m$, expressing (5.11) as

$$\alpha_1 + \alpha_2 (\beta_2^3)^m + \alpha_3 (\beta_3^3)^m = 0 , \tag{5.12}$$

and noting that

$$\begin{aligned} \beta_2^3 &= 1 + 7 \cdot 19 + O(19^2) \\ \beta_3^3 &= 1 + 11 \cdot 19 + O(19^2) , \end{aligned}$$

it follows from the p-adic binomial theorem that we can express (5.12) in power series form as

$$\sum_{i=1}^{\infty} \gamma_i m^i = 0 \tag{5.13}$$

with $\gamma_i \in \mathbb{Q}_{19}$. Moreover, the *proof* of the p-adic binomial theorem allows us to explicitly calculate the coefficients γ_j. In particular, by Exercise 5.42 we have

$$\begin{aligned} (\beta_2^3)^m &\equiv (1 + 7 \cdot 19)^m \equiv 1 + (7 \cdot 19)m && \pmod{19^2} \\ (\beta_3^3)^m &\equiv (1 + 11 \cdot 19)^m \equiv 1 + (11 \cdot 19)m && \pmod{19^2} \\ \alpha_1 + \alpha_2 (\beta_2^3)^m + \alpha_3 (\beta_3^3)^m &\equiv (-2 \cdot 7 + 5 \cdot 11) \cdot 19 \cdot m && \pmod{19^2}, \end{aligned}$$

from which it follows that $|\gamma_1|_{19} = \frac{1}{19}$ and $|\gamma_j|_{19} \leq \frac{1}{19^2}$ for $j \geq 2$. By Strassmann's theorem, we conclude that $m = 0$ is the only solution to (5.13) in $\mathbb{Z}_{19}$. In particular, $m = 0$ is the only solution to (5.13) in $\mathbb{Z}$, and therefore $n = 3 \cdot 0 = 0$ is the only solution to (5.10). □

As a consequence, we find:

COROLLARY 5.46. *The only integer solution to* $x^3 - 11y^3 = 1$ *is* $(x, y) = (1, 0)$.

5.2. The Diophantine equation $2x^2+1 = 3^m$. The Diophantine equation

$$2x^2 + 1 = 3^m \tag{5.14}$$

with x, m nonnegative integers, clearly has the solutions $(x, m) = (0, 1), (1, 1), (2, 2)$, and $(11, 5)$. Are there any others? We will answer this question by once again employing p-adic methods.

Let $K = \mathbb{Q}(\sqrt{-2})$, and let $\alpha = 1 + x\sqrt{-2} \in \mathcal{O}_K = \mathbb{Z}[\sqrt{-2}]$. Then letting $N = N_{K/\mathbb{Q}}$ and $\overline{\alpha} = 1 - x\sqrt{-2}$, the equation (5.14) becomes

$$N\alpha = 3^m \ .$$

Since $N\alpha = \alpha\overline{\alpha}$ and $3 = \beta_1\beta_2$ with $\beta_1 = 1 + \sqrt{-2}$ and $\beta_2 = 1 - \sqrt{-2}$ both irreducible, and since $\mathbb{Z}[\sqrt{-2}]$ is a PID, it follows that

$$\alpha = \pm\beta_1^{m_1}\beta_2^{m_2}$$

with m_1, m_2 nonnegative integers. Without loss of generality, we may assume that $m_1 \leq m_2$. Since $\mathrm{Tr}(\alpha) = \alpha + \overline{\alpha} = 2$, we have

$$\beta_1^{m_1}\beta_2^{m_2} + \beta_2^{m_1}\beta_1^{m_2} = \pm 2 \ .$$

Factoring out $\beta_1^{m_1}\beta_2^{m_1}$ gives

$$3^{m_1}\left(\beta_2^{m_2-m_1} + \beta_1^{m_2-m_1}\right) = \pm 2$$

in $\mathcal{O}_K$, which by unique factorization implies that $m_1 = 0$. Therefore (setting $n = m_2$), we have

$$\beta_1^n + \beta_2^n = \pm 2 \ ,$$

where $\beta_1, \beta_2 \in \mathbb{Q}(\sqrt{-2})$ are the two roots of the polynomial $f(x) = x^2 - 2x + 3 \in \mathbb{Z}[x]$.

So we will be finished once we establish the following result:

PROPOSITION 5.47. *There are at most 4 integer values of n for which*

$$\beta_1^n + \beta_2^n = \pm 2 \ , \tag{5.15}$$

where $\beta_1, \beta_2 \in \mathbb{Q}(\sqrt{-2})$ are the roots of the polynomial $f(x) = x^2 - 2x + 3$.

PROOF. By Hensel's lemma, there are two roots of $f(x) = x^2 - 2x + 3$ in $\mathbb{Z}_{11}$, and this allows us to define two embeddings of $K = \mathbb{Q}(\sqrt{-2})$ into $\mathbb{Q}_{11}$. Identifying K with a subfield of $\mathbb{Q}_{11}$ via one of these embeddings, we may identify the two roots of $f(x)$ in $\mathbb{Q}_{11}$ with β_1 and β_2, respectively. Without loss of generality, we have $\beta_1 \equiv 9$

(mod 11) and $\beta_2 \equiv 4 \pmod{11}$. Since $\beta_i^5 \equiv 1 \pmod{11}$ for $i = 1, 2$, if we let $\lambda_i = \beta_i^5 - 1 \in 11\mathbb{Z}_{11}$, we have (writing $n = k + 5t$ with $0 \leq k \leq 4$):

$$\beta_1^k(1+\lambda_1)^t + \beta_2^k(1+\lambda_2)^t = \pm 2 \ . \tag{5.16}$$

Looking at this equation modulo 11, we see that we need only consider $k = 0, 1, 2$.

For example, consider $k = 0$. Then (5.16) reduces to

$$(1+\lambda_1)^t + (1+\lambda_2)^t = 2 \ , \tag{5.17}$$

since the left-hand-side cannot be congruent to -2 modulo 11. We now use the p-adic binomial theorem to expand

$$\Phi_0(t) = (1+\lambda_1)^t + (1+\lambda_2)^t - 2$$

as a power series in t. Doing so, we obtain

$$\begin{aligned}
\Phi_0(t) &= 0 + (\lambda_1 + \lambda_2)t + (\lambda_1^2 + \lambda_2^2)\binom{t}{2} + \cdots \\
&= (7 \cdot 11^2 + 10 \cdot 11^3 + 10 \cdot 11^4)\frac{t(t-1)}{2} + 8 \cdot 11^4 \cdot \binom{t}{4} + O(11^5) \\
&= \gamma_1 t + \gamma_2 t^2 + \gamma_3 t^3 + \cdots
\end{aligned}$$

with $|\gamma_1|_{11} = 11^{-2}$, $|\gamma_2|_{11} = 11^{-2}$, and $|\gamma_n|_{11} \leq 11^{-4}$ for $n \geq 3$. It follows by Strassmann's theorem that there are at most 2 roots of $\Phi_0(t)$ in $\mathbb{Z}_{11}$, and in particular there are at most two solutions to (5.16) in $\mathbb{Z}$ when $k = 0$.

Similarly, when $k = 1$ we find at most 1 solution to (5.16) in $\mathbb{Z}_{11}$, and when $k = 2$ we also find at most 1 solution in $\mathbb{Z}_{11}$. All together, this shows that there are at most 4 integer solutions to (5.15), as claimed. □

COROLLARY 5.48. *The only solutions to (5.14) with x, m nonnegative integers are $(x, m) = (0, 1), (1, 1), (2, 2)$, and $(11, 5)$.*

Note that (5.15) is equivalent to the equation $a_n = \pm 2$, where a_n is the linear recurrence sequence defined by $a_0 = 2$, $a_1 = 2$, and $a_{n+2} = 2a_{n+1} - 3a_n$ for $n \geq 2$. Therefore we have proved:

COROLLARY 5.49. *Let a_n be the linear recurrence defined by $a_0 = 2$, $a_1 = 2$, and $a_{n+2} = 2a_{n+1} - 3a_n$ for $n \geq 2$. Then $a_n = \pm 2$ only for $n = 0, 1, 2, 5$.*

The p-adic method used to prove Proposition 5.47 is the main idea behind the proof of the following beautiful general theorem:

THEOREM 5.50 (The Skolem-Mahler-Lech Theorem). *Let a_n be a sequence of elements in a field K of characteristic zero satisfying a linear recurrence relation over K, and let $c \in K$. Then either $a_n = c$ for at most finitely many n, or else $a_n = c$ for all n in some arithmetic progression.*

REMARK 5.51. Theorem 5.50 is false if K has characteristic p, as the following example shows. Let $K = \mathbb{F}_p(t)$, and define a_n by $a_n = (t+1)^n - t^n$. Then $a_n = 1$ iff n is a power of p.

The idea behind the proof of Theorem 5.50 is the following (see §5.5 of Cassels' "Local Fields" for further details). If $F(x) \in K[x]$ denotes the generating polynomial for the linear recurrence, then

$$a_n = \sum_j P_j(n)\theta_j^n$$

with $\theta_j \in L$ and $P_j(x) \in L[x]$ for some field L which is finitely generated over $\mathbb{Q}$. The *Cassels-Lech Embedding Theorem* (see Theorem 1.1 in Chapter 5 of Cassels' "Local Fields") asserts that if $k/\mathbb{Q}$ is a finitely generated field extension and C is a finite set of nonzero elements of k, then there are infinitely many primes p for which there is a field embedding $\alpha : k \hookrightarrow \mathbb{Q}_p$ such that $|\alpha(c)|_p = 1$ for all $c \in C$. Applying this result to the situation at hand, we see that there exists a prime $p > 2$ and an embedding $\psi : L \hookrightarrow \mathbb{Q}_p$ such that $|\psi(\theta_j)|_p = 1$ for all j. Setting $\lambda_j = \psi(\theta_j^{p-1} - 1)$, it follows from Fermat's Little Theorem that $|\lambda_j|_p \leq \frac{1}{p}$. Writing $n = r + (p-1)s$ with $0 \leq r < p-1$, for each fixed r we can use the p-adic binomial theorem to develop

$$a_{r+(p-1)s} - c = -c + \sum_j P_j(r + (p-1)s)\theta_j^r(1+\lambda_j)^s$$

as a power series $\Phi_r(s)$ in s which converges for all $s \in \mathbb{Z}_p$. If $\Phi_r(s) \equiv 0$ for some r, then $a_n = c$ for all $n \equiv r \pmod{p-1}$. Otherwise, Strassmann's theorem ensures that each $\Phi_r(s)$ vanishes for at most finitely many $s \in \mathbb{Z}_p$, which gives the desired result.

APPENDIX A

Some background results from abstract algebra

1. Euclidean Domains are UFD's

In this section, we show that every Euclidean domain is a UFD (unique factorization domain). See §1.1 and §1.3 for the definition of a UFD and a Euclidean domain, respectively. The usual way to do this is to show that every Euclidean domain is a PID, and every PID is a UFD. Here, we give a somewhat more direct argument.

Recall that a nonzero element $\pi \in R$ which is not a unit is called *prime* if whenever $\pi \mid xy$ in R, we have $\pi \mid x$ or $\pi \mid y$, and is called *irreducible* if whenever $\pi = ab$ with $a, b \in R$, one of a or b must be a unit.

LEMMA A.1. *In any integral domain R, every prime element is irreducible.*

PROOF. Suppose π is prime, and that $\pi = xy$ for some $x, y \in R$. By the definition of primality, we have $\pi \mid x$ or $\pi \mid y$. Suppose WLOG that $\pi \mid y$, so that $y = \pi\beta$ for some $\beta \in R$. Then $\pi = \pi x\beta$ in R. Since R is an integral domain and $\pi \neq 0$, we must have $x\beta = 1$, which implies that x is a unit. Therefore π is irreducible. □

The converse of the above lemma is false. Here is an example, which also gives an example of a ring of the form $\mathbb{Z}[\sqrt{d}]$ which is not a UFD.

Example: Consider the ring $\mathbb{Z}[\sqrt{-5}]$. By considering the norm function $N(a + b\sqrt{-5}) = a^2 + 5b^2$, one shows easily that ± 1 are the only units in $\mathbb{Z}[\sqrt{-5}]$, and that $N(x) = 1$ iff x is a unit. Note that we have the identity

$$6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5}).$$

We claim that $2, 3, 1 \pm \sqrt{-5}$ are all irreducible. To see this, it suffices to note that there are no elements of norm 2 or 3 in $\mathbb{Z}[\sqrt{5}]$, and $N(2) = 4, N(3) = 9, N(1 \pm \sqrt{-5}) = 6$.

Note also that 2 is not associate to either $1 + \sqrt{-5}$ or $1 - \sqrt{-5}$. This is clear, since associate elements must have the same norm. We therefore have two genuinely distinct factorizations of 6 into irreducible

elements in $\mathbb{Z}[\sqrt{-5}]$. Also, 2 is an example of an irreducible element which is not prime, for we have $2 \mid (1+\sqrt{-5})(1-\sqrt{-5})$, but we cannot have $2 \mid 1 \pm \sqrt{-5}$ or else (taking norms), we would have $4 \mid 6$, a contradiction. (If $x \mid y$ then $y = x\beta$ for some β, so $\overline{y} = \overline{x}\overline{\beta}$ and therefore $|y|^2 = |x|^2|\beta|^2$ and $N(x) \mid N(y)$.)

We need a few simple lemmas before being able to prove that Euclidean domains are UFD's. The first concerns elements of norm zero in a Euclidean domain.

LEMMA A.2. *Let R be a Euclidean domain and suppose that x is a nonzero element of R with $\phi(x) = 0$. Then x is a unit.*

PROOF. Use the division algorithm to write $1 = xq + r$ with $r = 0$ or $\phi(r) < \phi(x)$. The latter is impossible since $\phi(x) = 0$ and $\phi(r) \geq 0$. Therefore $1 = xq$ and x is a unit. □

We need the notion of a least common multiple in an integral domain R. Let $a, b, m \in R$, $a, b, m \neq 0$. We say that m is a *least common multiple* (LCM) of a and b if a and b both divide m, and if $m \mid M$ for every other common multiple M of a and b.

LEMMA A.3. *If R is a Euclidean domain, then any two nonzero elements $a, b \in R$ have a least common multiple.*

PROOF. Let $S = \{M \in R \ : \ a \mid M, b \mid M\}$. Then $ab \in S$, so $S \neq \emptyset$. Choose a nonzero element $m \in S$ of least possible norm. We claim that m is an LCM of a and b. To see this, suppose that $M \in S$ is any common multiple of a and b, and write $M = mq + r$ with $r = 0$ or $\phi(r) < \phi(m)$. Since $r = M - mq$, we have $r \in S$, and since $\phi(m)$ is minimal among all nonzero elements of S, we must have $r = 0$, so that $m \mid M$ as desired. □

The following lemma is the key to proving that Euclidean domains are UFD's.

LEMMA A.4. *If R is a Euclidean domain, then every irreducible element is prime.*

PROOF. Let p be an irreducible element of R and suppose $p \mid ab$ with $a, b \neq 0$. Suppose p does not divide a; we claim that $p \mid b$. Let m be an LCM of a and p. Then $m \mid ap$, so $x = \frac{ap}{m}$ is in R. As $a \mid m$, we have $p = x\frac{m}{a}$. Since p is irreducible, either x or $\frac{m}{a}$ is a unit. If $\frac{m}{a}$ is a unit, then $m \sim a$, and since $p \mid m$ we would have $p \mid a$, a contradiction. Therefore x is a unit, so $m \sim ap$. As ab is a multiple of both a and p, we have $m \mid ab$, and therefore $ap \mid ab$. This implies that $p \mid b$, so we are done. □

We can now prove the main theorem of this section.

THEOREM A.5. *A Euclidean domain is a UFD.*

PROOF. To show that every element of the Euclidean domain R has (at least one) factorization into irreducibles, it suffices by induction to prove that up to multiplication by units, every element of R has only finitely many divisors. (Convince yourself that this suffices!)

In other words, it suffices to prove:

Claim: If $x \in R$ then there exist $x_1, \ldots, x_n$ such that if $y \mid x$ then $y \sim x_i$ for some i.

To prove this, suppose $y \mid x$, and write $y = qx + r$ with $r = 0$ or $\phi(r) < \phi(x)$. If $r = 0$ then $x \mid y$, and it follows easily that $y \sim x$. Now suppose $\phi(r) < \phi(x)$. Then by induction on $\phi(x)$, we can assume that there exist $r_1, \ldots, r_m$ such that every divisor of r is associate to one of $r_1, \ldots, r_m$. (If $\phi(x) = 0$ then x is a unit and we're done, which establishes the base case of the induction). But $y = qx + r$ and $y \mid x$, so $y \mid r$, and therefore y is associate to one of $r_1, \ldots, r_m$. So we can take $\{x_1, \ldots, x_n\} = \{x, r_1, \ldots, r_m\}$.

For uniqueness, suppose that $f_1 \cdots f_m = g_1 \cdots g_n$ with each f_i, g_i irreducible. Since f_1 is irreducible and R is Euclidean, f_1 is prime. Since $f_1 \mid g_1 \cdots g_n$, it follows that $f_1 \mid g_i$ for some i. As g_i is irreducible and f_1 is not a unit, we must have $f_1 \sim g_i$.

After relabeling, we may assume WLOG that $i = 1$, so that $f_1 = g_1$. We find that $f_1(f_2 \cdots f_m - g_2 \cdots g_n) = 0$, and since R is an integral domain, this implies that $f_2 \cdots f_m = g_2 \cdots g_n$. We are now finished by induction on the number of factors. □

In particular, this theorem gives us a proof of the Fundamental Theorem of Arithmetic.

2. The theorem of the primitive element and embeddings into algebraic closures

Let K be a field, and fix an algebraically closed field $\overline{K}$ containing K.

Recall that a field extension L/K is *separable* if the minimal polynomial over K of every element $\alpha \in L$ has distinct roots in $\overline{K}$. This does not depend on the choice of $\overline{K}$. We recall the following basic results from field theory. The first is often proved as a consequence of Galois theory, but one does not really need Galois theory in order to prove it.

THEOREM A.6 (Theorem of the primitive element). *If L/K is a separable field extension of degree n, then there exists an element $\theta \in L$ of degree n.*

PROOF. If K is a finite field, then the result follows from the fact that the multiplicative group of a finite field is cyclic. We therefore assume that K is infinite. By induction, it suffices to prove that if $L = K(\alpha, \beta)$, then in fact $L = K(\theta)$ for some $\theta \in L$.

Let f and g be the minimal polynomials over K of α and β, respectively. Suppose that f and g factor over $\overline{K}$ as

$$f(x) = (x - \alpha_1) \cdots (x - \alpha_s),\ g(x) = (x - \beta_1) \cdots (x - \beta_t),$$

with $\alpha_1 = \alpha$ and $\beta_1 = \beta$. Note that the α_i's are distinct (since L/K is separable), as are the β_j's.

In particular, the fact that the β_j's are distinct implies that for each i and each $k \neq 1$, there is at most one element $\gamma' \in K$ such that

$$\alpha_i + \gamma'\beta_k = \alpha + \gamma'\beta.$$

There are only finitely many such equations, and K is infinite, so we can find an element $\gamma \in K$ such that for each i and for each $k \neq 1$,

$$\alpha_i + \gamma\beta_k \neq \alpha + \gamma\beta.$$

Define $\theta := \alpha + \gamma\beta$, and note that by construction, θ is not of the form $\alpha_i + \gamma\beta_k$ for any $(i, k) \neq (1, 1)$.

We claim that $L = K(\theta)$. Clearly $K(\theta) \subseteq L$, and since $\gamma \in K$ and $\alpha = \theta - \gamma\beta$, it suffices to prove that $\beta \in K(\theta)$.

Let $L' := K(\theta)$. Since $f(\theta - \gamma\beta) = f(\alpha) = 0$, if we define $h(x) := f(\theta - \gamma x) \in L'[x]$, then $h(\beta) = 0$. We claim that β is the only common zero of $g(x)$ and $h(x)$ in $\overline{K}$, so that the GCD in $\overline{K}[x]$ of $g(x)$ and $h(x)$ is $(x - \beta)$. Indeed, if $\lambda \in \overline{K}$ and $g(\lambda) = h(\lambda) = 0$, then λ is one of the β_j's and $\theta - \gamma\lambda$ is one of the α_i's. By our choice of θ, this implies that $\lambda = \beta$ as claimed.

Let $G(x)$ be the minimal polynomial of β over L'. Then $G(x)$ divides both $g(x)$ and $h(x)$, so it divides their GCD. But then we must have $G(x) = (x - \beta)$, and in particular $\beta \in L'$ as desired. □

The following is a standard result in Galois theory, but can also be proved directly using the primitive element theorem as follows.

PROPOSITION A.7. *If L/K is a separable extension of degree n, then there are precisely n distinct embeddings of L into $\overline{K}$ which fix every element of K.*

PROOF. By the theorem of the primitive element, there exists an element $\theta \in L$ of degree n. Let $\theta_1, \ldots, \theta_n \in \overline{K}$ be the conjugates of θ. By basic field theory, there exists a unique embedding (i.e., injective field homomorphism) $\sigma_i : L \to \overline{K}$ which fixes K and sends θ to θ_i. Let f_θ be the minimal polynomial of θ over K. If σ is any embedding of L into $\overline{K}$ fixing K, then $f_\theta(\sigma(\theta)) = \sigma(f_\theta(\theta)) = 0$, so that $\sigma(\theta) = \theta_i$ for some i. Therefore $\sigma = \sigma_i$ for some i. □

COROLLARY A.8. *Let L/K be a finite separable extension, and let $\sigma_1, \ldots, \sigma_n$ denote the embeddings of L into $\overline{K}$. If $\beta \in L$ is fixed by σ_i for all $i = 1, \ldots, n$, then $\beta \in K$.*

PROOF. Let $d = [K(\beta) : K]$. Then there are exactly d embeddings, call them $\tau_1, \ldots, \tau_d$, of $K(\beta)$ into $\overline{K}$ which fix K, and they are given by sending β to each of its conjugates over K. Note that we can extend each τ_i to L. If α is a primitive element for L/K, so that $L = K(\alpha)$, then each τ_i must send α to one of its conjugates over K, and therefore must equal σ_j for some j. Since the σ_j's all fix β, we conclude that $d = 1$, i.e., $\beta \in K$. □

3. Free modules over a PID

Let R be a commutative ring with 1. An R-module M is called *torsion-free* if $m \in M$, $r \in R$, and $rm = 0$ imply that either $m = 0$ or $r = 0$. A module M is *free of rank n* if there is a generating set $m_1, \ldots, m_n$ with the property that $r_1 m_1 + \cdots + r_n m_n = 0$ if and only if $r_i = 0$ for all i. In this case, M is isomorphic to a direct sum of n copies of R, and the set $\{m_1, \ldots, m_n\}$ is called a *free basis* for M.

The following result is proved as Theorem B.3 of Appendix B in [Janusz].

THEOREM A.9. *Suppose R is a PID, and let M be a finitely generated, torsion-free R module which can be generated by n elements but no fewer. Then M is free of rank n, and any generating set of n elements gives a free basis of M.*

COROLLARY A.10. *If K is the quotient field of the PID R and L/K is a finite field extension, then every finitely generated R-submodule of L is free of rank at most $[L : K]$.*

PROOF. Since R is a subring of the field L, any R-submodule M of L must be torsion-free. By Theorem A.9, M is free of rank n for some n. By clearing denominators, one shows easily that the elements of a free basis of M over R are linearly independent over K. Therefore the rank of M is at most $[L : K]$. □

We will also use the fundamental theorem for finitely generated abelian groups, in the following (slightly non-standard) form.

THEOREM A.11. *Let G be a free $\mathbb{Z}$-module of rank n, and let H be a subgroup of G. Then:*

(a) *H is free of rank $m \leq n$.*
(b) *There exists a basis $\alpha_1, \ldots, \alpha_n$ for G and positive integers $c_1, \ldots, c_m$ such that $c_1\alpha_1, \ldots, c_m\alpha_m$ forms a basis for H.*
(c) *The index $[G : H]$ is finite if and only if $m = n$. In this case, let $x_1, \ldots, x_n$ (resp. $y_1, \ldots, y_n$) be any basis for G (resp. H), and write*

$$\begin{bmatrix} y_1 \\ \vdots \\ y_n \end{bmatrix} = A \begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix}$$

with $A \in M_n(\mathbb{Z})$. Then $[G : H] = |\det(A)|$.

PROOF. (Sketch) Although part (a) follows from Theorem A.9, we sketch a direct proof by induction on n. If $n = 1$ then $H = a\mathbb{Z}$ for some $a \in \mathbb{Z}$ and therefore H is free of rank 1 (if $a \neq 0$) or 0 (if $a = 0$). In general, we identify G with $\mathbb{Z}^n$ and let $\pi : \mathbb{Z}^n \to \mathbb{Z}$ be projection onto the last coordinate. Let $H' = \ker(\pi) \cap H$ and let $H'' = \pi(H)$. Then by induction H' is free of rank $\leq n-1$ (since H' is isomorphic to a subgroup of $\mathbb{Z}^{n-1}$) and H'' is free of rank at most 1. If $H'' = (0)$ then $H = H'$ and we are done. Otherwise, $H'' = a\mathbb{Z}$ is free of rank 1. Choose $x \in H$ such that $\pi(x) = a$. Then π maps $G'' := x\mathbb{Z}$ isomorphically onto H'', so to prove (a) it suffices to prove that $H = H' \oplus G''$. This is straightforward and we leave it to the reader.

We assume $m = n$ and prove (b) and (c) at the same time. (We leave the case $m < n$ to the reader). Let $x = [x_1, \ldots, x_n]^t$ (resp. $y = [y_1, \ldots, y_n]^t$) be a basis for G (resp. H), and write $y = Ax$ with $A \in M_n(\mathbb{Z})$. The reader can verify that multiplying A on the right by a unimodular matrix T (i.e., an element of $M_n(\mathbb{Z})$ with determinant ± 1) corresponds to replacing x by another basis x'. Similarly, multiplying A on the left by a unimodular matrix T' corresponds to replacing y by another basis y'. Therefore, it is enough to prove that by performing elementary row and column operations on A, we can change it into a diagonal matrix. (Convince yourself that this is enough).

For this, it is enough by symmetry and induction to use elementary row operations to obtain a matrix A' with $a'_{i1} = 0$ for all $i > 1$. This can be done using the division algorithm and induction on $M := \max\{|a_i| : i > 1\}$: Let $\phi(x) = |x|$ and swap two rows if necessary so that $\phi(a_{11}) \leq$

$\phi(a_{i1})$ for $i > 1$. Then add a suitable integer multiple of row 1 to row i for each $i > 1$ so that M is decreased. □

REMARK A.12. The theorem is in fact valid when $\mathbb{Z}$ is replaced by any PID R. The proof we have given works whenever R is a Euclidean domain.