Algebraic Number Theory

Tom Weston

Contents

Chapter 1. Number Fields 5
1. Example : Quadratic number fields 5
2. Complex embeddings 8
3. Example : Cyclotomic fields 9
4. Galois theory of number fields 14
5. Relative extensions 17
6. Exercises 22

Chapter 2. Rings of Integers 25
1. Unique factorization 25
2. Algebraic integers 33
3. Unique factorization of ideals in Dedekind domains 43
4. Rings of integers in cyclotomic fields 47
5. Exercises 50

Chapter 3. Prime Splitting 53
1. Example : Quadratic number fields 53
2. Abstract factorization of primes 59
3. Explicit factorization of ideals 67
4. Exercises 74

Chapter 4. The Ideal Class Group 77
1. Definitions 77
2. Finiteness of the ideal class group 82
3. Ideal class groups of imaginary quadratic fields 84
4. Applications to quadratic forms 93
5. Exercises 100

Chapter 5. Fermat's Last Theorem for Regular Primes 101
1. The theorem 101
2. Regular primes 104
3. Exercises 107

Appendix A. Field Theory 109
1. Field extensions and minimal polynomials 109
2. Primitive elements 112
3. Algebraic extensions 114
4. Characteristic polynomials 116

Appendix B. Mobius Inversion 119
1. Theory over rings 119

2. Theory over groups 122

Appendix C. Factorization 123
1. Definitions 123
2. Review of ideals 124
3. Unique factorization 124
4. Principal ideal domains and Euclidean domains 126
5. Finitely generated modules 128

Appendix D. Solutions to Exercises 131
1. Chapter 1 131
2. Chapter 2 140
3. Chapter 3 151
4. Chapter 4 161
5. Chapter 5 167

Bibliography 173

CHAPTER 1

Number Fields

1. Example : Quadratic number fields

Before we consider number fields in general, let us begin with the fairly concrete case of quadratic number fields. A *quadratic number field* is an extension K of $\mathbb{Q}$ of degree 2. The fundamental examples (in fact, as we shall see in a moment the only example) are fields of the form

$$\mathbb{Q}(\sqrt{d}) = \{a + b\sqrt{d} \mid a, b \in \mathbb{Q}\}$$

where $d \in \mathbb{Q}$ is not the square of another rational number.

There is an issue that arises as soon as we write down these fields, and it is important that we deal with it immediately: what exactly do we mean by $\sqrt{d}$? There are several possible answers to this question. The most obvious is that by $\sqrt{d}$ we mean a specific choice of a complex square root of d. $\mathbb{Q}(\sqrt{d})$ is then defined as a subfield of the complex numbers. The difficulty with this is that the notation "$\sqrt{d}$" is ambiguous; d has two complex square roots, and there is no algebraic way to tell them apart.

Algebraists have a standard way to avoid this sort of ambiguity; we can simply define

$$\mathbb{Q}(\sqrt{d}) = \mathbb{Q}[x]/(x^2 - d).$$

There is no ambiguity with this notation; $\sqrt{d}$ really means x, and x behaves as a formal algebraic object with the property that $x^2 = d$.

This second definition is somehow the algebraically correct one, as there is no ambiguity and it allows $\mathbb{Q}(\sqrt{d})$ to exist completely independently of the complex numbers. However, it is far easier to think about $\mathbb{Q}(\sqrt{d})$ as a subfield of the complex numbers. The ability to think of $\mathbb{Q}(\sqrt{d})$ as a subfield of the complex numbers also becomes important when one wishes to compare fields $\mathbb{Q}(\sqrt{d_1})$ and $\mathbb{Q}(\sqrt{d_2})$ for two different numbers d_1 and d_2; the abstract algebraic fields $\mathbb{Q}[x]/(x^2 - d_1)$ and $\mathbb{Q}[y]/(y^2 - d_2)$ have no natural relation to each other, while these same fields viewed as subfields of $\mathbb{C}$ can be compared more easily.

The best approach, then, seems to be to pretend to follow the formal algebraic option, but to actually view everything as subfields of the complex numbers. We can do this through the notion of a *complex embedding*; this is simply an injection

$$\sigma : \mathbb{Q}[x]/(x^2 - d) \hookrightarrow \mathbb{C}.$$

As we have already observed, there are exactly two such maps, one for each complex square root of d.

Before we continue we really ought to decide which complex number we mean by $\sqrt{d}$. There is unfortunately no consistent way to do this, in the sense that we can not arrange to have

$$\sqrt{d_1}\sqrt{d_2} = \sqrt{d_1 d_2}$$

for all $d_1, d_2 \in \mathbb{Q}$. In order to be concrete, let us choose $\sqrt{d}$ to be the positive square root of d for all $d > 0$ and $\sqrt{d}$ to be the positive square root of $-d$ times i for all $d < 0$. (There is no real reason to prefer these choices, but since it doesn't really matter anyway we might as well fix ideas.)

With this choice, our two complex embeddings are simply

$$\sigma_1 : \mathbb{Q}[x]/(x^2 - d) \hookrightarrow \mathbb{C}$$
$$\sigma_2 : \mathbb{Q}[x]/(x^2 - d) \hookrightarrow \mathbb{C}$$

defined by

$$\sigma_1(a + bx) = a + b\sqrt{d};$$
$$\sigma_2(a + bx) = a - b\sqrt{d}.$$

Given any $a + bx \in \mathbb{Q}[x]/(x^2 - d)$, we define its *conjugates* to be the images $\sigma_1(a + bx) = a + b\sqrt{d}$ and $\sigma_2(a + bx) = a - b\sqrt{d}$.

Note that these maps have the same image. This gives us yet another way to view the ambiguity: we can take $\mathbb{Q}(\sqrt{d})$ to be the subfield $\{a + b\sqrt{d} \mid a, b \in \mathbb{Q}\}$ of $\mathbb{C}$, and we remember that $\mathbb{Q}(\sqrt{d})$ has an *automorphism*

$$a + b\sqrt{d} \mapsto a - b\sqrt{d}.$$

This is the approach we will take; that is, we will regard $\mathbb{Q}(\sqrt{d})$ as a subfield of $\mathbb{C}$ via our choice of $\sqrt{d}$, but we always remember that $\sqrt{d}$ is ambiguous, and thus that we have an automorphism of this field exchanging $\sqrt{d}$ and $-\sqrt{d}$. From this point of view, the conjugates of an element $a + b\sqrt{d}$ are $a + b\sqrt{d}$ and $a - b\sqrt{d}$.

Let us now analyze these fields $K = \mathbb{Q}(\sqrt{d})$. Note first that every $\alpha \in K$ has degree either 1 or 2 over $\mathbb{Q}$, and it has degree 1 if and only if it is actually in $\mathbb{Q}$. In particular, if $\alpha \notin \mathbb{Q}$ then we must have $K = \mathbb{Q}(\alpha)$.

Let us now compute the norms and traces from K to $\mathbb{Q}$. We take $1, \sqrt{d}$ as our basis for K over $\mathbb{Q}$. Multiplication by $\alpha = a + b\sqrt{d}$ takes 1 to $a + b\sqrt{d}$ and $\sqrt{d}$ to $bd + a\sqrt{d}$, so the matrix for the linear transformation m_α is

$$\begin{bmatrix} a & bd \\ b & a \end{bmatrix}.$$

The characteristic polynomial of this matrix is

$$x^2 - 2ax + (a^2 - bd^2).$$

Thus

$$\mathrm{N}_{K/\mathbb{Q}}(\alpha) = a^2 - bd^2$$

and

$$\mathrm{Tr}_{K/\mathbb{Q}}(\alpha) = 2a.$$

Note also that we have

$$\mathrm{N}_{K/\mathbb{Q}}(\alpha) = (a + b\sqrt{d})(a - b\sqrt{d})$$

and

$$\mathrm{Tr}_{K/\mathbb{Q}}(\alpha) = (a + b\sqrt{d}) + (a - b\sqrt{d}).$$

That is, the norm of α is the product of its conjugates and the trace of α is the sum of its conjugates. This follows immediately from the fact that the conjugates of α are the two roots of the characteristic polynomial of α.

It turns out that every quadratic field is of the form $\mathbb{Q}(\sqrt{d})$ for some $d \in \mathbb{Q}$. In fact, in the case of quadratic fields it is actually possible to give a complete classification, as described in the following theorem.

THEOREM 1.1. *Let K be a number field of degree 2. Then K is isomorphic to $\mathbb{Q}(\sqrt{d})$ for a unique squarefree integer $d \neq 1$.*

PROOF. First we will show that every extension of $\mathbb{Q}$ of degree 2 is isomorphic to one of the desired form. So let $K/\mathbb{Q}$ have degree 2 and choose a primitive element α for K, with minimal polynomial

$$f(x) = x^2 + ax + b,$$

$a, b \in \mathbb{Q}$. By the quadratic formula we have

$$\alpha = \frac{-a \pm \sqrt{a^2 - 4b}}{2};$$

put differently,

$$\bigl(2\alpha + a\bigr)^2 = a^2 - 4b.$$

Thus K contains an element $\beta = 2\alpha + a$ of square $a^2 - 4b \in \mathbb{Q}$. Note also that $a^2 - 4b$ is not a square in $\mathbb{Q}$, for otherwise $f(x)$ would not be irreducible. It follows that β has degree 2 and thus is a primitive element for K. $a^2 - 4b$ may not be a squarefree integer, but one sees easily from unique factorization in $\mathbb{Z}$ that we can find some rational number c such that $c^2(a^2 - 4b)$ is a squarefree integer. $c\beta$ still generates K over $\mathbb{Q}$, and it is now in the form we considered above. This shows that every extension of $\mathbb{Q}$ of degree 2 can be generated by the square root of a squarefree integer.

We now show that no two fields $\mathbb{Q}(\sqrt{d})$ with d a squarefree integer (other than 1) are isomorphic. So let d_1 and d_2 be distinct squarefree integers and suppose that there is an isomorphism

$$\varphi : \mathbb{Q}(\sqrt{d_1}) \xrightarrow{\cong} \mathbb{Q}(\sqrt{d_2}).$$

We will show that $d_1 = d_2$. Consider the element $\alpha = \varphi(\sqrt{d_1}) \in \mathbb{Q}(\sqrt{d_2})$. α has minimal polynomial $x^2 - d_1$, so we read off that

$$\mathrm{N}_{K_2/\mathbb{Q}}(\alpha) = -d_1$$

and

$$\mathrm{Tr}_{K_2/\mathbb{Q}}(\alpha) = 0.$$

Writing $\alpha = a + b\sqrt{d_2}$, our formulas for the norm and trace imply that $a = 0$ and $b^2 d_2 = d_1$. One now shows easily that the fact that d_1 and d_2 are squarefree integers implies that $b = 1$ and $d_1 = d_2$, as claimed. $\square$

This sort of analysis does not work for any degree other than 2; even the cubic and quartic "formulas" are too complicated to use, and beyond that there aren't any formulas at all.

2. Complex embeddings

A *number field* is a finite extension of the rational numbers $\mathbb{Q}$. (This is not quite the same as the definitions given in [**10**] and [**14**], but it seems to be the most common definition.) We define the *degree* of a number field K to be the positive integer $[K : \mathbb{Q}]$. The fundamental examples are fields of the form

$$\mathbb{Q}[x]/(f(x))$$

where $f(x) \in \mathbb{Q}[x]$ is an irreducible polynomial. In fact, Proposition A.2.3 shows that every number field K is isomorphic to one of this form: simply choose a primitive element $\alpha \in K$ with minimal polynomial $f(x) \in \mathbb{Q}[x]$. Then $K = \mathbb{Q}(\alpha)$ and Lemma A.2.1 shows that K is isomorphic to $\mathbb{Q}[x]/(f(x))$.

Let K and K' be number fields and suppose that there is a homomorphism

$$\varphi : K \to K'.$$

Then φ is automatically $\mathbb{Q}$-linear: this is because it must send 1 to 1; it follows from the fact that it is an additive homomorphism that it must be the identity on all of $\mathbb{Z}$, and it follows from the fact that it is a multiplicative homomorphism that it must be the identity on all of $\mathbb{Q}$.

We now investigate complex embeddings of arbitrary number fields. That is, for a number field K we wish to determine all of the possible injections $K \hookrightarrow \mathbb{C}$. Recall that in the quadratic case we did this by exhibiting complex square roots. We will use the same method in the general case, although of course the polynomials of interest will now have larger degree.

Fix a number field K of degree n and choose a primitive element $\alpha \in K$ with minimal polynomial $f(x) \in \mathbb{Q}[x]$. Since $\mathbb{C}$ is algebraically closed, $f(x)$ splits into n linear factors over $\mathbb{C}$; since $f(x)$ is irreducible over $\mathbb{Q}$, these linear factors must be distinct (see Problem 1.12), and thus $f(x)$ has n distinct roots $\alpha_1, \dots, \alpha_n \in \mathbb{C}$.

For each root α_i we define a (necessarily $\mathbb{Q}$-linear) map

$$\sigma_i : K \xrightarrow{\cong} \mathbb{Q}(\alpha_i) \subseteq \mathbb{C}$$

sending α to α_i; that is,

$$\sigma_i\bigl(a_0 + a_1\alpha + a_2\alpha^2 + \cdots + a_{n-1}\alpha^{n-1}\bigr) = a_0 + a_1\alpha_i + a_2\alpha_i^2 + \cdots + a_{n-1}\alpha_i^{n-1}$$

where the a_i are all in $\mathbb{Q}$. This map is well-defined since α_i satisfies $f(x)$, it is injective since all non-zero maps of fields are injective, and it is surjective since α_i generates $\mathbb{Q}(\alpha_i)$ over $\mathbb{Q}$.

We have now embedded K as a subfield of $\mathbb{C}$ in n distinct ways. (Note that we mean that the *maps* are distinct; the images of the embeddings could still be the same.) We claim that the σ_i are the only embeddings of K into $\mathbb{C}$. To see this, let $\sigma : K \hookrightarrow \mathbb{C}$ be any such map. Then $\sigma(\alpha)$ must have the same minimal polynomial $f(x)$ over $\mathbb{Q}$ as α; thus $\sigma(\alpha)$ must be one of the complex roots of $f(x)$, which are precisely the α_i. Therefore $\sigma(\alpha) = \alpha_i$ for some i, and since α generates K over $\mathbb{Q}$, this implies that $\sigma = \sigma_i$. This proves the claim.

In particular, this implies that the embeddings σ_i are independent of the choice of primitive element α, since any other choice would yield n embeddings of K into $\mathbb{C}$ which by the above argument must be the same as the σ_i. Combining all of this, we see that there are exactly n distinct embeddings of K into $\mathbb{C}$. We state this as a proposition.

PROPOSITION 2.1. *Let K be a number field of degree n. Then K has exactly n distinct complex embeddings.*

EXAMPLE 2.2. Consider the number field $\mathbb{Q}[x]/(x^3-2)$. This has degree 3 over $\mathbb{Q}$, so there should be three complex embeddings. These are determined by the three roots of x^3-2 in $\mathbb{C}$. If we let α be the real cube root of 2 and let ζ be a third root of unity in $\mathbb{C}$, then these roots are α, $\zeta\alpha$ and $\zeta^2\alpha$. The three complex embeddings are then the three maps

$$\mathbb{Q}[x]/(x^3-2) \to \mathbb{C}$$

sending x to α, $\zeta\alpha$ and $\zeta^2\alpha$ respectively. Note that in contrast to the case of $\mathbb{Q}[x]/(x^2-2)$ these maps have different images; for example, the first map has image inside of $\mathbb{R}$, while the other two do not.

Let α be an arbitrary element of K with minimal polynomial $f(x) \in \mathbb{Q}[x]$ of degree d. We define the *conjugates* of α to be the d complex roots of $f(x)$; that is, they are simply the complex numbers which behave exactly the same as α does algebraically. Alternately, if $\tau_1, \ldots, \tau_d$ are the d complex embeddings of the subfield $\mathbb{Q}(\alpha)$ of K (which is a number field since K is), the conjugates are precisely

$$\tau_1(\alpha), \ldots, \tau_d(\alpha),$$

as is clear from the above discussion. In particular, if α is a primitive element for K, then its conjugates are the n complex numbers

$$\sigma_1(\alpha), \ldots, \sigma_n(\alpha).$$

As with the quadratic case we would like to be able to think of number fields as specific subfields of the complex numbers. As we have just seen, we can do this in n different ways, where n is the degree of the number field K. In general, however, these embeddings have different images. Thus, although it is often useful to think of K in terms of these complex images, there is no single field that one can point to and say is the best choice for a complex version of K. We will always attempt to be careful about this point. For example, when we write $\mathbb{Q}(\sqrt[3]{2})$, we do not mean to single out any of the three complex versions of it; if we wish to do so, we will make it explicit.

This sets up a slightly strange situation: whenever we say "let K be a number field", we want to regard K independent of any complex embedding of K. On the other hand, our examples will usually involve specific subfields of $\mathbb{C}$ in order to fix ideas. In particular, keep in mind that a subfield of $\mathbb{C}$ can still have complex embeddings, just like any number field.

The one case where one can safely identify a number field with the images of its complex embeddings are when all of these complex embeddings are the same. In this case we will say that K is *Galois* (over $\mathbb{Q}$). We will return to the theory of Galois extensions later.

3. Example : Cyclotomic fields

3.1. Cyclotomic polynomials. Before we define cyclotomic fields abstractly, let us work with subfields of the complex numbers. Recall that a complex number ζ is an *m^{th} root of unity* if $\zeta^m = 1$; it is a *primitive m^{th} root of unity* if m is the smallest positive integer which works. The complex m^{th} roots of unity are precisely the numbers

$$e^{2\pi i k/m}$$

for $k = 0, 1, \ldots, m-1$, and the primitive m^{th} roots of unity are those for which k and m are relatively prime. In particular, there are m complex m^{th} roots of unity and $\varphi(m)$ complex primitive m^{th} roots of unity, where $\varphi(m)$ is the Euler φ-function. (See Appendix B.)

Let ζ_m be a fixed complex primitive m^{th} root of unity. ζ_m is a root of $x^m - 1$, but for $m > 1$ this can not be its minimal polynomial, as it is not irreducible. We wish to determine the minimal polynomial $f(x) \in \mathbb{Q}[x]$ of ζ_m; we will do this by determining the complex roots of $f(x)$.

PROPOSITION 3.1. *If p is a prime not dividing m, then ζ_m^p is a root of $f(x)$.*

PROOF. $f(x)$ divides $x^m - 1$ in $\mathbb{Q}[x]$; thus we can write

$$x^m - 1 = f(x)g(x)$$

for some monic $g(x) \in \mathbb{Q}[x]$, and by Exercise 1.4 we actually have $f(x), g(x) \in \mathbb{Z}[x]$. Since ζ_m^p is a root of $x^m - 1$, to show that it is a root of $f(x)$ it will suffice to show that it is not a root of $g(x)$.

So suppose that $g(\zeta_m^p) = 0$. Let $h(x) \in \mathbb{Z}[x]$ be the monic polynomial $g(x^p)$. Then $h(\zeta_m) = 0$, so $f(x)$ divides $h(x)$ in $\mathbb{Q}[x]$. Writing $h(x) = f(x)q(x)$, Exercise 1.4 again shows that $q(x)$ is actually in $\mathbb{Z}[x]$.

We now work modulo p. For any polynomial $s(x) \in \mathbb{Z}[x]$, we denote by $\bar{s}(x)$ its image in $\mathbb{F}_p[x]$ after reducing the coefficients modulo p. We have $\bar{h}(x) = \bar{f}(x)\bar{q}(x)$; also,

$$\bar{h}(x) = \bar{g}(x^p) = \bar{g}(x)^p$$

by Exercise 1.15. Thus $\bar{f}(x)$ divides $\bar{g}(x)^p$ in $\mathbb{F}_p[x]$. Since $\mathbb{F}_p[x]$ is a unique factorization domain, this implies that $\bar{f}(x)$ and $\bar{g}(x)$ have a monic common factor of positive degree, say $\bar{r}(x)$.

We have $\bar{f}(x)\bar{g}(x) = x^m - 1 \in \mathbb{F}_p[x]$, so $\bar{r}(x)^2$ divides $x^m - 1$ in $\mathbb{F}_p[x]$. By Exercise 1.11, this implies that $\bar{r}(x)$ divides mx^{m-1}. Since p does not divide m (this is the only place where we use that hypothesis), mx^{m-1} is a non-zero monomial, so $\bar{r}(x)$ must also be a non-zero monomial. But $\bar{r}(x)$ also divides $x^m - 1$; the only monic monomial with this property is 1, so $\bar{r}(x) = 1$. This contradicts the fact that $\bar{r}(x)$ has positive degree, so the initial assumption that $g(\zeta_m^p) = 0$ must be false. Thus $f(\zeta_m^p) = 0$, which completes the proof. $\square$

COROLLARY 3.2. *The conjugates of ζ_m are precisely the other primitive m^{th} roots of unity.*

PROOF. As before let $f(x)$ be the minimal polynomial of ζ_m. Let ζ_m^k be any other primitive m^{th} root of unity. Then k is relatively prime to m, so it is divisible only by primes not dividing m. Write $k = p_1 p_2 \cdots p_n$, with the p_i not necessarily distinct. Then Proposition 3.1 shows that $\zeta_m^{p_1}$ is a root of $f(x)$. In particular, $f(x)$ is also the minimal polynomial of $\zeta_m^{p_1}$. Applying Proposition 3.1 with respect to the primitive m^{th} root of unity $\zeta_m^{p_1}$ shows that $\zeta_m^{p_1 p_2}$ is also a root of $f(x)$, and continuing in this way we see that ζ_m^k is a root of $f(x)$. Thus all primitive m^{th} roots of unity are roots of $f(x)$, and therefore conjugates of ζ_m.

To complete the proof we must show that ζ_m has no other conjugates. But if α is any other conjugate of ζ_m, then there is an isomorphism of $\mathbb{Q}(\zeta_m)$ and $\mathbb{Q}(\alpha)$ sending ζ_m to α; it follows that α must also be a primitive m^{th} root of unity, as claimed. $\square$

We now define the m^{th} *cyclotomic polynomial* $\Phi_m(x) \in \mathbb{Z}[x]$ to be the minimal polynomial of the complex primitive m^{th} roots of unity. Since it is a minimal polynomial $\Phi_m(x)$ is irreducible, and our above arguments show that it has degree $\varphi(m)$.

Since we have now shown that all primitive m^{th} roots of unity are essentially "the same" from the point of view of algebraic number theory, we might as well fix specific complex values for each ζ_m. Let us take

$$\zeta_m = e^{2\pi i/m} \in \mathbb{C}$$

for all m. These roots of unity have the nice property that

$$\zeta_n^{n/m} = \zeta_m$$

whenever m divides n. (While it may appear to be true even if m doesn't divide n, one then has all sorts of multiple-valued function stuff to worry about.) More generally, any choice of ζ_m with this compatibility would be fine, but we will stick with these for concreteness.

Corollary 3.2 gives the expression

$$\Phi_m(x) = \prod_{\substack{1 \leq k < m \\ (k,m)=1}} (x - \zeta_m^k).$$

However, this formula is not very useful for actually computing the $\Phi_m(x)$ by hand. For this we have the following result, which gives an expression for $\Phi_m(x)$ entirely in terms of integer arithmetic.

PROPOSITION 3.3. *We have*

$$x^m - 1 = \prod_{d|m} \Phi_d(x)$$

and

$$\Phi_m(x) = \prod_{d|m} (x^d - 1)^{\mu(m/d)}$$

where μ *is the Mobius function.*

PROOF. The first equality is clear since each side has exactly the same complex roots; namely, each m^{th} root of unity is a root of exactly one of the $\Phi_d(x)$ with d dividing m. The second equality comes from Mobius inversion of the first. See Example B.2.5. □

Using this formula we see immediately that for any prime p,

$$\Phi_p(x) = \frac{x^p - 1}{x - 1} = x^{p-1} + x^{p-2} + + x^{p-3} \cdots + x + 1.$$

The first few cyclotomic polynomials are

$$\begin{aligned}
\Phi_1(x) &= x - 1\\
\Phi_2(x) &= x + 1\\
\Phi_3(x) &= x^2 + x + 1\\
\Phi_4(x) &= x^2 + 1\\
\Phi_5(x) &= x^4 + x^3 + x^2 + x + 1\\
\Phi_6(x) &= x^2 - x + 1\\
\Phi_7(x) &= x^6 + x^5 + x^4 + x^3 + x^2 + x + 1\\
\Phi_8(x) &= x^4 + 1
\end{aligned}$$

$$\begin{aligned}
\Phi_9(x) &= x^6 + x^3 + 1\\
\Phi_{10}(x) &= x^4 - x^3 + x^2 - x + 1\\
\Phi_{11}(x) &= x^{10} + x^9 + x^8 + x^7 + x^6 + x^5 + x^4 + x^3 + x^2 + x + 1\\
\Phi_{12}(x) &= x^4 - x^2 + 1
\end{aligned}$$

There are many patterns which can be found among the cyclotomic polynomials; we leave these to the reader. (We will at least point out that it is not true that every Φ_m has only coefficients ± 1 and 0, although Φ_{105} is the first which violates this.)

3.2. Abstract cyclotomic fields. We define the m^{th} *cyclotomic field* to be the field

$$\mathbb{Q}[x]/(\Phi_m(x))$$

where $\Phi_m(x)$ is the m^{th} cyclotomic polynomial. $\mathbb{Q}[x]/(\Phi_m(x))$ has degree $\varphi(m)$ over $\mathbb{Q}$ since $\Phi_m(x)$ has degree $\varphi(m)$. The roots of $\Phi_m(x)$ are just the primitive m^{th} roots of unity, so the complex embeddings of $\mathbb{Q}[x]/(\Phi_m(x))$ are simply the $\varphi(m)$ maps

$$\sigma_k : \mathbb{Q}[x]/(\Phi_m(x)) \hookrightarrow \mathbb{C},$$

$1 \le k < m$, $(k, m) = 1$, where

$$\sigma_k(x) = \zeta_m^k,$$

ζ_m being our fixed choice of primitive m^{th} root of unity. Note that $\zeta_m^k \in \mathbb{Q}(\zeta_m)$ for every k; it follows that $\mathbb{Q}(\zeta_m) = \mathbb{Q}(\zeta_m^k)$ for all k relatively prime to m. In particular, the images of the σ_i coincide, so $\mathbb{Q}[x]/(\Phi_m(x))$ is Galois over $\mathbb{Q}$. This means that we can write $\mathbb{Q}(\zeta_m)$ for $\mathbb{Q}[x]/(\Phi_m(x))$ without much fear of ambiguity; we will do so from now on, the identification being $\zeta_m \mapsto x$. One advantage of this is that one can easily talk about cyclotomic fields being extensions of one another, or intersections or compositums; all of these things take place considering them as subfields of $\mathbb{C}$.

We now investigate some basic properties of cyclotomic fields. The first issue is whether or not they are all distinct; to determine this, we need to know which roots of unity lie in $\mathbb{Q}(\zeta_m)$. Note, for example, that if m is odd, then $-\zeta_m$ is a $2m^{\text{th}}$ root of unity. We will show that this is the only way in which one can obtain any non-m^{th} roots of unity.

Lemma 3.4. *If m divides n, then $\mathbb{Q}(\zeta_m)$ is contained in $\mathbb{Q}(\zeta_n)$.*

Proof. Since $\zeta_n^{n/m} = \zeta_m$, we have $\zeta_m \in \mathbb{Q}(\zeta_n)$, so the result is clear. $\square$

Lemma 3.5. *If m and n are relatively prime, then*

$$\mathbb{Q}(\zeta_m, \zeta_n) = \mathbb{Q}(\zeta_{mn})$$

and

$$\mathbb{Q}(\zeta_m) \cap \mathbb{Q}(\zeta_n) = \mathbb{Q}.$$

(Recall that $\mathbb{Q}(\zeta_m, \zeta_n)$ is the compositum of $\mathbb{Q}(\zeta_m)$ and $\mathbb{Q}(\zeta_n)$.)

Proof. One checks easily that $\zeta_m\zeta_n$ is a primitive mn^{th} root of unity, so that $\mathbb{Q}(\zeta_{mn}) \subseteq \mathbb{Q}(\zeta_m, \zeta_n)$. Furthermore, by Lemma A.3.3,

$$[\mathbb{Q}(\zeta_m, \zeta_n) : \mathbb{Q}] \leq [\mathbb{Q}(\zeta_m) : \mathbb{Q}][\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \varphi(m)\varphi(n) = \varphi(mn);$$

since $[\mathbb{Q}(\zeta_{mn}) : \mathbb{Q}] = \varphi(mn)$, this implies that

$$\mathbb{Q}(\zeta_m, \zeta_n) = \mathbb{Q}(\zeta_{mn}).$$

We now have a field diagram

$$\begin{tikzcd}
& \mathbb{Q}(\zeta_m, \zeta_n) & \\
\mathbb{Q}(\zeta_m) \arrow[ur, dash] \arrow[dr, dash] \arrow[ddr, dash, "\varphi(m)"'] & & \mathbb{Q}(\zeta_n) \arrow[ul, dash] \arrow[dl, dash] \arrow[ddl, dash, "\varphi(n)"] \\
& \mathbb{Q}(\zeta_m) \cap \mathbb{Q}(\zeta_n) \arrow[d, dash] & \\
& \mathbb{Q} &
\end{tikzcd}$$

We know that $\mathbb{Q}(\zeta_m, \zeta_n)$ has degree $\varphi(mn)$ over $\mathbb{Q}$, so we must have

$$[\mathbb{Q}(\zeta_m, \zeta_n) : \mathbb{Q}(\zeta_m)] = \varphi(n)$$

and

$$[\mathbb{Q}(\zeta_m, \zeta_n) : \mathbb{Q}(\zeta_n)] = \varphi(m).$$

Now Lemma A.3.3 shows that

$$[\mathbb{Q}(\zeta_m) : \mathbb{Q}(\zeta_m) \cap \mathbb{Q}(\zeta_n)] \geq \varphi(m)$$

and thus that $\mathbb{Q}(\zeta_m) \cap \mathbb{Q}(\zeta_n) = \mathbb{Q}$. $\square$

Proposition 3.6. *For any m and n,*

$$\mathbb{Q}(\zeta_m, \zeta_n) = \mathbb{Q}(\zeta_{[m,n]})$$

and

$$\mathbb{Q}(\zeta_m) \cap \mathbb{Q}(\zeta_n) = \mathbb{Q}(\zeta_{(m,n)});$$

here $[m, n]$ and (m, n) denote the least common multiple and the greatest common divisor of m and n, respectively.

PROOF. Write $m = p_1^{e_1} \cdots p_k^{e_k}$ and $n = p_1^{f_1} \cdots p_k^{f_k}$ where the p_i are distinct primes. (We allow e_i or f_i to be zero.) By Lemma 3.5 we have

$$\mathbb{Q}(\zeta_m) = \mathbb{Q}(\zeta_{p_1^{e_1}})\mathbb{Q}(\zeta_{p_2^{e_2}}) \cdots \mathbb{Q}(\zeta_{p_k^{e_k}})$$

and

$$\mathbb{Q}(\zeta_n) = \mathbb{Q}(\zeta_{p_1^{f_1}})\mathbb{Q}(\zeta_{p_2^{f_2}}) \cdots \mathbb{Q}(\zeta_{p_k^{f_k}}).$$

Thus

$$\begin{aligned}
\mathbb{Q}(\zeta_m, \zeta_n) &= \mathbb{Q}(\zeta_{p_1^{e_1}}) \cdots \mathbb{Q}(\zeta_{p_k^{e_k}})\mathbb{Q}(\zeta_{p_1^{f_1}}) \cdots \mathbb{Q}(\zeta_{p_k^{f_k}}) \\
&= \mathbb{Q}(\zeta_{p_1^{e_1}})\mathbb{Q}(\zeta_{p_1^{f_1}}) \cdots \mathbb{Q}(\zeta_{p_k^{e_k}})\mathbb{Q}(\zeta_{p_k^{f_k}}) \\
&= \mathbb{Q}(\zeta_{p_1^{\max\{e_1,f_1\}}}) \cdots \mathbb{Q}(\zeta_{p_k^{\max\{e_k,f_k\}}}) \\
&= \mathbb{Q}(\zeta_{p_1^{\max\{e_1,f_1\}} \cdots p_k^{\max\{e_k,f_k\}}}) \\
&= \mathbb{Q}(\zeta_{[m,n]});
\end{aligned}$$

the third equality uses Lemma 3.4, the fourth uses Lemma 3.5 and the last uses a standard expression for least common multiples. An entirely similar computation shows that $\mathbb{Q}(\zeta_m) \cap \mathbb{Q}(\zeta_n) = \mathbb{Q}(\zeta_{(m,n)})$. □

COROLLARY 3.7. *If m is even, then the only roots of unity in $\mathbb{Q}(\zeta_m)$ are the m^{th} roots of unity. If m is odd, then the only roots of unity in $\mathbb{Q}(\zeta_m)$ are the $2m^{th}$ roots of unity.*

PROOF. Suppose that $\zeta_n \in \mathbb{Q}(\zeta_m)$. Then $\zeta_m\zeta_n$ is a $[m,n]^{\text{th}}$ root of unity, so $\mathbb{Q}(\zeta_{[m,n]}) \subseteq \mathbb{Q}(\zeta_m)$. Thus

$$\varphi([m,n]) \leq \varphi(m).$$

One easily shows that this can happen only if m is odd and n divides $2m$, or if m is even and n divides m. This proves the corollary. □

COROLLARY 3.8. *If $m < n$ and $\mathbb{Q}(\zeta_m) = \mathbb{Q}(\zeta_n)$, then m is odd and $n = 2m$.*

4. Galois theory of number fields

Let K be a Galois extension of $\mathbb{Q}$ of degree n. Recall that this means that if $\sigma_1, \ldots, \sigma_n$ denote the complex embeddings of K, then the σ_i all have the same image in $\mathbb{C}$. Let us denote this image by K_0 for the remainder of this section. We wish to reinterpret the complex embeddings as automorphisms of K. To do this, fix one embedding, say $\sigma_1 : K \to K_0$. Consider the n maps

$$\sigma_1^{-1} \circ \sigma_i : K \to K.$$

These maps are all automorphisms of K (that is, isomorphisms from K to K) since the σ_i are all isomorphisms from K to K_0.

We claim that in fact these are all of the automorphisms of K. So suppose that $\sigma : K \to K$ is any automorphism of K. Then $\sigma_1 \circ \sigma : K \to K_0 \hookrightarrow \mathbb{C}$ is a complex embedding of K, and thus equals one of the σ_i. Thus $\sigma = \sigma_1^{-1} \circ \sigma_i$, as claimed.

In general, if M is any sort of object, then the set of automorphisms of M form a group with composition as the group law; this is because the composition of two automorphisms and the inverse of an automorphism are again automorphisms. We define the *Galois group* $\mathrm{Gal}(K/\mathbb{Q})$ of K over $\mathbb{Q}$ to be the group of automorphisms of K; our above arguments show that as a set $\mathrm{Gal}(K/\mathbb{Q})$ is just the maps $\sigma_1^{-1} \circ \sigma_i : K \to K$. Note in particular that

$$(\sigma_1^{-1} \circ \sigma_i) \circ (\sigma_1^{-1} \circ \sigma_j)$$

and

$$(\sigma_1^{-1} \circ \sigma_i)^{-1} = \sigma_i^{-1} \circ \sigma_1$$

are again of the form $\sigma_1^{-1} \circ \sigma_k$ for some k, although it is not at all clear which k it is.

Note that $\mathrm{Gal}(K/\mathbb{Q})$ has order n; even if K is not Galois one could still consider the automorphisms of K, but the above construction no longer works and it is somewhat harder to determine how many automorphisms there are.

When one actually computes Galois groups, it is usually much simpler to consider the fields as subfields of $\mathbb{C}$. So let K be a Galois number field which is also a subfield of $\mathbb{C}$. The automorphisms of K are now simply its complex embeddings $\sigma_i : K \to K \subseteq \mathbb{C}$. (With our earlier notation, we really are just considering the case where σ_1 is the identity map.) Note in particular that $\sigma_i \circ \sigma_j$ and σ_i^{-1} are also complex embeddings of K, although it is not immediately clear which.

To determine which, let α be a primitive element for K over $\mathbb{Q}$ and let $\alpha_1 = \alpha, \alpha_2, \ldots, \alpha_n$ be its conjugates, so that the complex embeddings of K are given by $\sigma_i(\alpha) = \alpha_i$. We can now determine $\sigma_i \circ \sigma_j$ simply by determining for which k we have

$$\sigma_i \circ \sigma_j(\alpha) = \alpha_k;$$

we then have $\sigma_i \circ \sigma_j = \sigma_k$.

Example 4.1. Let d be a squarefree integer (other than 1) and consider the field $\mathbb{Q}(\sqrt{d})$. This has the two embeddings σ_1 and σ_2 characterized by

$$\sigma_1(\sqrt{d}) = \sqrt{d}$$

and

$$\sigma_2(\sqrt{d}) = -\sqrt{d}.$$

We find that

$$\sigma_2\sigma_2(\sqrt{d}) = \sigma_2(-\sqrt{d}) = -\sigma_2(\sqrt{d}) = \sqrt{d};$$

that is, $\sigma_2^2 = \sigma_1$. This confirms that

$$\mathrm{Gal}(\mathbb{Q}(\sqrt{d})/\mathbb{Q}) \cong \mathbb{Z}/2\mathbb{Z}$$

as it must be; σ_1 is the identity element and σ_2 is the non-trivial element.

Example 4.2. Consider the field $\mathbb{Q}(\sqrt{2}, \sqrt{3})$. This field has degree 4 over $\mathbb{Q}$, with complex embeddings characterized by

$$\begin{aligned}
\sigma_1(\sqrt{2}) &= \sqrt{2},\ \sigma_1(\sqrt{3}) = \sqrt{3}\\
\sigma_2(\sqrt{2}) &= -\sqrt{2},\ \sigma_2(\sqrt{3}) = \sqrt{3}\\
\sigma_3(\sqrt{2}) &= \sqrt{2},\ \sigma_3(\sqrt{3}) = -\sqrt{3}\\
\sigma_4(\sqrt{2}) &= -\sqrt{2},\ \sigma_4(\sqrt{3}) = -\sqrt{3}
\end{aligned}$$

One computes easily that each of σ_2, σ_3 and σ_4 have square σ_1 and that the product of any two of them is the third, so that $\mathrm{Gal}(\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q})$ is isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

EXAMPLE 4.3. Consider the cyclotomic field $\mathbb{Q}(\zeta_m)$. This has $\varphi(m)$ complex embeddings σ_k (for $(k,m)=1$), where $\sigma_k(\zeta_m)=\zeta_m^k$. We compute

$$\sigma_k\sigma_j(\zeta_m)=\sigma_k(\zeta_m^j)=\sigma_k(\zeta_m)^j=\zeta_m^{jk};$$

if $jk\equiv l \pmod{m}$, then this shows that $\sigma_k\sigma_j=\sigma_l$. In particular, we obtain a map

$$\mathrm{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q})\to(\mathbb{Z}/m\mathbb{Z})^*$$

sending σ_k to the class of k in $(\mathbb{Z}/m\mathbb{Z})^*$; the above calculation shows that this is a group homomorphism. It is also clearly bijective by our characterization of the σ_k. Thus we have obtained an isomorphism

$$\mathrm{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q})\xrightarrow{\cong}(\mathbb{Z}/m\mathbb{Z})^*.$$

Note that if $\zeta=\zeta_m^i$ is any m^{th} root of unity in $\mathbb{Q}(\zeta_m)$, then

$$\sigma_k(\zeta)=\sigma_k(\zeta_m^i)=\sigma_k(\zeta_m)^i=\zeta_m^{ki}=\zeta^k.$$

This means that the above isomorphism is completely canonical, in the sense that the automorphism corresponding to $k\in(\mathbb{Z}/m\mathbb{Z})^*$ has the effect of exponentiation by k on *any* m^{th} root of unity in $\mathbb{Q}(\zeta_m)$. Note also that $\mathrm{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q})$ is abelian; in some sense this is the fact which will make all of the applications in this class work.

EXAMPLE 4.4. For a non-abelian example, let $\sqrt[4]{2}$ be the positive real fourth root of 2 and consider the field $\mathbb{Q}(\sqrt{-1},\sqrt[4]{2})$. The conjugates of $\sqrt[4]{2}$ are $\sqrt[4]{2}$, $\sqrt{-1}\sqrt[4]{2}$, $-\sqrt[4]{2}$, $-\sqrt{-1}\sqrt[4]{2}$. This field has degree 8 over $\mathbb{Q}$, with embeddings $\sigma_0,\dots,\sigma_7$ characterized by

$$\sigma_i(\sqrt[4]{2})=\sqrt{-1}^{\,i}\sqrt[4]{2}$$

and

$$\sigma_i(\sqrt{-1})=\begin{cases}\sqrt{-1} & i=0,1,2,3;\\ -\sqrt{-1} & i=4,5,6,7.\end{cases}$$

(To see that this field has degree 8, it is enough to show that $[\mathbb{Q}(\sqrt[4]{2}):\mathbb{Q}]=4$ and that $\sqrt{-1}\notin\mathbb{Q}(\sqrt[4]{2})$. The first of these follows from Exercise 1.8 and the second can be done in the same way as Exercise 1.16.)

We compute easily

$$\sigma_i\sigma_j(\sqrt{-1})=\begin{cases}\sqrt{-1} & \text{both } i,j\in\{0,1,2,3\} \text{ or both } i,j\in\{4,5,6,7\};\\ -\sqrt{-1} & \text{otherwise.}\end{cases}$$

On the other hand,

$$\begin{aligned}\sigma_i\sigma_j(\sqrt[4]{2})&=\sigma_i(\sqrt{-1}^{\,j}\sqrt[4]{2})\\ &=\sigma_i(\sqrt{-1})^j\sigma_i(\sqrt[4]{2})\\ &=\begin{cases}\sqrt{-1}^{\,j}\sqrt{-1}^{\,i}\sqrt[4]{2} & i\in\{0,1,2,3\};\\ (-\sqrt{-1})^j\sqrt{-1}^{\,i}\sqrt[4]{2} & i\in\{4,5,6,7\};\end{cases}\\ &=\begin{cases}\sqrt{-1}^{\,i+j}\sqrt[4]{2} & i\in\{0,1,2,3\};\\ \sqrt{-1}^{\,i-j}\sqrt[4]{2} & i\in\{4,5,6,7\}.\end{cases}\end{aligned}$$

For example,

$$\sigma_3\sigma_5(\sqrt{-1})=-\sqrt{1}$$

and

$$\sigma_3\sigma_5(\sqrt[4]{2}) = \sqrt{-1}^8\sqrt[4]{2} = \sqrt[4]{2},$$

so $\sigma_3\sigma_5 = \sigma_4$. On the other hand,

$$\sigma_5\sigma_3(\sqrt{-1}) = -\sqrt{-1}$$

and

$$\sigma_5\sigma_3(\sqrt[4]{2}) = \sqrt{-1}^2\sqrt[4]{2} = -\sqrt[4]{2}$$

so $\sigma_5\sigma_3 = \sigma_6$. Thus $\mathrm{Gal}(\mathbb{Q}(\sqrt[4]{2}, i)/\mathbb{Q})$ is non-abelian; with a little squinting one discovers that it is isomorphic to the dihedral group of order 8.

5. Relative extensions

5.1. Relative embeddings. Let L and K be two number fields such that $L \supseteq K$; set $n = [L : \mathbb{Q}]$, $m = [K : \mathbb{Q}]$, $d = [L : K] = n/m$. We wish to relate the complex embeddings of L to those of K. Let us fix an embedding

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

and determine how many complex embeddings of L restrict to σ on K. (Such an embedding of L is said to *extend* σ.)

Choose a primitive element α for L/K and let $f(x) \in K[x]$ be its minimal polynomial. Let $g(x) = \sigma(f(x)) \in \mathbb{C}[x]$. Since $\mathbb{C}$ is algebraically closed and $g(x)$ is irreducible in $K[x]$, $g(x)$ has d distinct roots $\alpha_1, \ldots, \alpha_d$ in $\mathbb{C}$. For each such root we can define a map

$$\tau_i : L \hookrightarrow \mathbb{C}$$

to be σ on K and to send α to α_i. This procedure yields exactly d distinct embeddings of L into $\mathbb{C}$, all of which restrict to σ on K. Explicitly, we have

$$\tau_i\big(a_0+a_1\alpha+a_2\alpha^2+\cdots+a_{n-1}\alpha^{n-1}\big) = \sigma(a_0)+\sigma(a_1)\alpha_i+\sigma(a_2)\alpha_i^2+\cdots+\sigma(a_{n-1})\alpha^{n-1}$$

where the a_i are all in K.

We can actually conclude that these are all of the embeddings of L into $\mathbb{C}$ extending σ by a counting argument. Specifically, for any of the m complex embeddings σ' of K the above procedure yields d complex embeddings of L restricting to σ' on K. In this way we can therefore obtain $md = n$ distinct complex embeddings of L. But these are then all of the n complex embeddings of L; this implies that each embedding of K has exactly d extensions to L, as if it had any more then we would obtain too many complex embeddings of L.

Summarizing our work to this point, we have shown that each complex embedding of K extends to d complex embeddings of L. In the case that $K = \mathbb{Q}$, σ must be the unique embedding of $\mathbb{Q}$ into $\mathbb{C}$, and this all reduces to our original discussion of complex embeddings.

We extend some of our earlier terminology to this situation. Given $\alpha \in L$ with minimal polynomial $f(x)$ over K of degree e, we say that the *σ-K-conjugates* of α are the e (distinct) complex roots of $\sigma(f(x))$. Continuing to let $\tau_1, \ldots, \tau_d$ be the extensions of σ to L, we find that each σ-K-conjugate of α occurs precisely d/e times among the numbers $\tau_1(\alpha), \ldots, \tau_d(\alpha)$. To see this, fix a σ-K-conjugate α_1 of α and consider the embedding $\rho : K(\alpha) \hookrightarrow \mathbb{C}$ given by σ on K and sending α to α_1. By the above discussion applied to $L/K(\alpha)$, there are exactly $[L : K(\alpha)] = d/e$ embeddings of L extending ρ, which means that there are exactly d/e embeddings of L extending σ and sending α to α_1, as claimed. In particular, in the case $K = \mathbb{Q}$

we find that each conjugate of α appears exactly d/e times among the images of α under the complex embeddings of L.

EXAMPLE 5.1. Let $K = \mathbb{Q}(\sqrt{2})$, $L = \mathbb{Q}(\sqrt{2}, \sqrt{3})$. Let $\sigma_1 : K \hookrightarrow \mathbb{C}$ be the complex embedding

$$\sigma_1(a + b\sqrt{2}) = a + b\sqrt{2}.$$

The two extensions $\tau_1, \tau_2 : L \hookrightarrow \mathbb{C}$ of σ to L are given by

$$\tau_1(a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6}) = a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6}$$
$$\tau_2(a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6}) = a + b\sqrt{2} - c\sqrt{3} - d\sqrt{6}.$$

Similarly, the two embeddings extending the other embedding σ_2 of K are

$$\tau_3(a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6}) = a - b\sqrt{2} + c\sqrt{3} - d\sqrt{6}$$
$$\tau_2(a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6}) = a - b\sqrt{2} - c\sqrt{3} + d\sqrt{6}.$$

Let $\alpha = \sqrt{2} + \sqrt{3} \in K$. The σ_1-K-conjugates of α are $\tau_1(\alpha) = \sqrt{2} + \sqrt{3}$ and $\tau_2(\alpha) = \sqrt{2} - \sqrt{3}$. The σ_2-K-conjugates of α are $\tau_3(\alpha) = -\sqrt{2} + \sqrt{3}$ and $\tau_4(\alpha) = -\sqrt{2} - \sqrt{3}$. Together these give the four conjugates of α.

5.2. Relations to characteristic polynomials. Our next goal is to relate complex embeddings to norms and traces. We first work with characteristic polynomials.

LEMMA 5.2. *Let L/K be an extension of number fields of degree d and let α be a primitive element for L/K. Let σ be a fixed complex embedding of K and let $\tau_1, \ldots, \tau_d$ be the extensions of σ to L. Let $g(x) \in K[x]$ be the characteristic polynomial (and thus the minimal polynomial) of α for L/K. Then*

$$\sigma(g(x)) = \prod_{i=1}^{d} (x - \tau_i(\alpha)) \in \mathbb{C}[x].$$

PROOF. We know that the τ_i are constructed by taking the complex roots $\alpha_1, \ldots, \alpha_d$ of $\sigma(g(x))$ and mapping α to each α_i; that is, we have $\tau_i(\alpha) = \alpha_i$. Thus the $\tau_i(\alpha)$ are precisely the complex roots of $\sigma(g(x))$, which is the statement of the lemma. □

PROPOSITION 5.3. *Let L/K be an extension of number fields of degree d and let α be an arbitrary element of L. Let σ be a fixed complex embedding of K and let $\tau_1, \ldots, \tau_d$ be the extensions of σ to L. Let $g(x)$ be the characteristic polynomial of α for L/K. Then*

$$\sigma(g(x)) = \prod_{i=1}^{d} (x - \tau_i(\alpha)).$$

PROOF. Let α have minimal polynomial $f(x)$ of degree e over K and consider the tower of fields $L/K(\alpha)/K$. Let $\rho_1, \ldots, \rho_e$ be the extensions of σ to $K(\alpha)$. By Lemma 5.2 we know that

$$\sigma(f(x)) = \prod_{i=1}^{e} (x - \rho_i(\alpha)).$$

By Corollary A.4.4 we know that $g(x) = f(x)^{d/e}$. We also know, from the discussion of the previous section, that each σ-K-conjugate $\rho_i(\alpha)$ of α occurs exactly d/e times among $\tau_1(\alpha), \ldots, \tau_d(\alpha)$. Combining all of these facts yields the proposition. □

The next result gives the fundamental connection between embeddings and norms and traces.

Corollary 5.4. *Let L/K be an extension of number fields of degree d. Let $\sigma : K \hookrightarrow \mathbb{C}$ be a complex embedding of K and let $\tau_1, \ldots, \tau_d$ be the d complex embeddings of L extending σ. Then for any $\alpha \in K$,*

$$\sigma(\mathrm{N}_{L/K}\,\alpha) = \tau_1(\alpha)\cdots\tau_d(\alpha)$$

and

$$\sigma(\mathrm{Tr}_{L/K}\,\alpha) = \tau_1(\alpha) + \cdots + \tau_d(\alpha).$$

Proof. This is immediate from Proposition 5.3 and the definitions of the norm and trace in terms of characteristic polynomials. □

For convenience, let us restate our main results in the case of an extension $K/\mathbb{Q}$.

Corollary 5.5. *Let K be a number field of degree n with complex embeddings $\sigma_1, \ldots, \sigma_n$. Let α be an element of K with characteristic polynomial $g(x)$. Then*

$$g(x) = \prod_{i=1}^{n}(x - \sigma_i(\alpha)).$$

Furthermore,

$$\mathrm{N}_{K/\mathbb{Q}}\,\alpha = \sigma_1(\alpha)\cdots\sigma_n(\alpha)$$

and

$$\mathrm{Tr}_{K/\mathbb{Q}}\,\alpha = \sigma_1(\alpha) + \cdots + \sigma_n(\alpha).$$

5.3. Relative Galois extensions. Let L/K be an extension of number fields of degree d. Fix a complex embedding σ of K with image K_0, and let $\tau_1, \ldots, \tau_d$ be the extensions of σ to L. If the τ_i all have the same image L_0 in $\mathbb{C}$, we will say that L is *Galois* over K. (We will check in a moment that this definition is independent of the choice of σ.)

Let us define the Galois group $\mathrm{Gal}(L/K)$ to be the group of K-linear automorphisms of L; that is, it is the group of automorphisms of L which fix every element of K. As with Galois groups over $\mathbb{Q}$, we can describe $\mathrm{Gal}(L/K)$ in terms of embeddings. Specifically, fix the embedding τ_1 and consider the d maps

$$\tau_1^{-1} \circ \tau_i : L \to L.$$

These are automorphisms of L, since the τ_i are all isomorphisms; furthermore, they are the identity on K, since both τ_i and τ_1 act on K as σ. Thus we have exhibited d K-linear automorphisms of L.

We claim that all K-linear automorphisms of L are of this form. So suppose that $\tau : L \to L$ is another such automorphism. Then $\tau_1 \circ \tau : L \to L_0$ is a complex embedding of L. Furthermore, it is simply σ on K, since τ is the identity on K. Thus $\tau_1 \circ \tau$ must be one of the τ_i, so that $\tau = \tau_1^{-1} \circ \tau_i$, as claimed.

Notice now that the definition of $\mathrm{Gal}(L/K)$ made no mention of σ. In particular, let $\sigma' : K \to \mathbb{C}$ be another complex embedding of K with extensions $\tau_1', \ldots, \tau_d'$. We claim that the τ_i' all have the same image. To see this, note that for every $\rho \in \mathrm{Gal}(L/K)$, $\tau_1' \circ \rho$ is a complex embedding of L which extends σ. The d different elements of $\mathrm{Gal}(L/K)$ yield d different such embeddings, all with the same image $\tau_1'(L)$; these must be nothing more than $\tau_1', \ldots, \tau_d'$, since those are all of the embeddings of L which extend σ. In particular, this shows that the property of L being Galois over K is independent of the choice of embedding of K.

As before, one can actually compute $\mathrm{Gal}(L/K)$ by considering L and K as specific subfields of $\mathbb{C}$ and then considering the action on σ-K-conjugates of generators.

EXAMPLE 5.6. Take $L = \mathbb{Q}(\sqrt{2}, \sqrt{3})$ and $K = \mathbb{Q}(\sqrt{2})$. We computed $\mathrm{Gal}(L/\mathbb{Q})$ in Example 4.2. Of the four automorphisms given there, σ_1 and σ_3 are the identity on K, so we can identify

$$\mathrm{Gal}(L/K) = \{\sigma_1, \sigma_3\} \cong \mathbb{Z}/2\mathbb{Z}.$$

Notice in particular that if $L/\mathbb{Q}$ is Galois, then $\mathrm{Gal}(L/K)$ is a subgroup of $\mathrm{Gal}(L/\mathbb{Q})$. The main theorem of Galois theory is a generalization of this fact.

THEOREM 5.7. *Let L/K be a Galois extension of number fields. There is a bijective correspondence between subgroups of $\mathrm{Gal}(L/K)$ and subfields of L, given by*

$$\begin{aligned} H \subseteq \mathrm{Gal}(L/K) &\to L^H = \{x \in L; h(x) = x \textit{ for all } h \in H\} \\ \{\sigma \in \mathrm{Gal}(L/K); \sigma|_{L'} = \mathrm{id}\} &\leftarrow L'. \end{aligned}$$

This correspondence is inclusion reversing, and L is Galois over each subfield L^H with Galois group $\mathrm{Gal}(L/L^H) = H$. Lastly, L^H is Galois over K if and only if H is a normal subgroup of $\mathrm{Gal}(L/K)$, in which case $\mathrm{Gal}(L^H/K) \cong \mathrm{Gal}(L/K)/H$.

COROLLARY 5.8. *Let L/K be a Galois extension and let α be an element of L. Then $\alpha \in K$ if and only if $\sigma(\alpha) = \alpha$ for all $\sigma \in \mathrm{Gal}(L/K)$.*

PROOF. The fact that $\sigma(\alpha) = \alpha$ for all $\alpha \in K$ and all $\sigma \in \mathrm{Gal}(L/K)$ is part of the definition of the Galois group. Conversely, by Theorem 5.7, the subfield K of L must correspond to the largest subgroup of $\mathrm{Gal}(L/K)$; that is, it corresponds to the entire group $G = \mathrm{Gal}(L/K)$, and thus by the definition of the Galois correspondence we find that $K = L^G$, as claimed. $\square$

We conclude with the promised strengthening of Lemma A.3.3.

LEMMA 5.9. *Let M/K be an extension of number fields and let L_1 and L_2 be subfields of M containing K. Suppose that L_2 is Galois over $L_1 \cap L_2$. Then L_1L_2 is Galois over L_1 and*

$$\mathrm{Gal}(L_1L_2/L_1) \cong \mathrm{Gal}(L_2/L_1 \cap L_2).$$

In particular,

$$[L_1L_2 : L_1] = [L_2 : L_1 \cap L_2]$$

and

$$[L_1L_2 : L_2] = [L_1 : L_1 \cap L_2].$$

PROOF. Set $d = [L_2 : L_1 \cap L_2]$. Let σ be an element of $\mathrm{Gal}(L_2/L_1 \cap L_2)$. We define an automorphism $\tilde{\sigma}$ of L_1L_2 to act as σ on L_2 and to be the identity on L_1; one checks easily that this is well-defined, since σ is the identity on $L_1 \cap L_2$. Applying this construction to every element of $\mathrm{Gal}(L_2/L_1 \cap L_2)$, we obtain d automorphisms of L_1L_2 fixing L_1.

Let now $\tau : L_1 \hookrightarrow \mathbb{C}$ be a complex embedding and let $\rho : L_1 L_2 \hookrightarrow \mathbb{C}$ extend τ. Then the d maps $\rho \circ \tilde{\sigma}$ are all distinct complex embeddings of $L_1 L_2$ extending τ, and they all have the same image. By Lemma A.3.3,

$$[L_1 L_2 : L_1] \leq d,$$

so the existence of these embeddings implies both that

$$[L_1 L_2 : L_1] = d$$

and that $L_1 L_2$ is Galois over L_1, since we have exhibited d automorphisms of $L_1 L_2$ over L_1.

Our map $\sigma \mapsto \tilde{\sigma}$ can now be interpreted as a map

$$\mathrm{Gal}(L_2/L_1 \cap L_2) \to \mathrm{Gal}(L_1 L_2/L_1).$$

One checks immediately that the map restricting an automorphism of $L_1 L_2$ to L_2 gives an inverse map, so they must both be isomorphisms. This proves everything but the last equality of the lemma; this follows from Lemma A.1.1 and the second to last equality. □

6. Exercises

6.1. Factorization of polynomials over $\mathbb{Z}$ and $\mathbb{Q}$.

EXERCISE 1.1. A polynomial $f(x) \in \mathbb{Z}[x]$ is said to be *primitive* if the greatest common divisor of its coefficients is 1. Show that for any non-zero $f(x) \in \mathbb{Q}[x]$ there exists a unique (up to sign) $c \in \mathbb{Q}^*$ such that $cf(x)$ is primitive.

EXERCISE 1.2. Let $f(x)$ and $g(x)$ be two primitive polynomials. Show that $f(x)g(x)$ is also primitive.

EXERCISE 1.3. Since we are not interested in constant factors of polynomials, we will say that $f(x) \in \mathbb{Z}[x]$ is *irreducible* if it does not factor as $f(x) = g(x)h(x)$ with neither $g(x)$ nor $h(x)$ a constant polynomial. (This disagrees with the usually notion of irreducible in a ring, but hopefully no confusion will result.) Show that $f(x) \in \mathbb{Z}[x]$ is irreducible in $\mathbb{Z}[x]$ if and only if it is irreducible in $\mathbb{Q}[x]$.

EXERCISE 1.4. Let $f(x) \in \mathbb{Z}[x]$ be monic and suppose that $f(x)$ factors as $f(x) = g(x)h(x)$ with $g(x), h(x) \in \mathbb{Q}[x]$ and monic. Show that $g(x), h(x) \in \mathbb{Z}[x]$.

6.2. Irreducibility criteria.

Let

$$f(x) = a_n x^n + a_{n-1}x^{n-1} + a_{n-2}x^{n-2} + \cdots + a_0$$

be a polynomial in $\mathbb{Z}[x]$. We are interested in finding ways to show that $f(x)$ is irreducible in $\mathbb{Z}[x]$ (and thus in $\mathbb{Q}[x]$ by Exercise 1.3). Since constant factors are not of any importance, we may as well assume that $f(x)$ is primitive; we will do so without further comment in Exercises 1.5–1.10.

EXERCISE 1.5. Show that if $f(\alpha) = 0$ for some $\alpha \in \mathbb{Q}$, then $x - \alpha$ divides $f(x)$ in $\mathbb{Q}[x]$. Conclude that if $\deg f$ is 2 or 3, then $f(x)$ is irreducible in $\mathbb{Q}[x]$ if and only if it has no rational roots.

EXERCISE 1.6. Suppose that there is some prime p for which p does not divide a_n and $f(x)$ is irreducible modulo p; that is, in $\mathbb{F}_p[x]$. Show that $f(x)$ is irreducible in $\mathbb{Q}[x]$.

EXERCISE 1.7 (Eisenstein irreducibility criterion). Suppose that there is some prime p such that p does not divide a_n, p does divide $a_{n-1}, \ldots, a_0$, and p^2 does not divide a_0. Show that $f(x)$ is irreducible in $\mathbb{Q}[x]$. Such an $f(x)$ is called an *Eisenstein polynomial*.

EXERCISE 1.8. Use Exercise 1.7 to show that $x^n - p$ and $x^n + p$ are irreducible in $\mathbb{Q}[x]$ for all primes p and all $n \geq 2$.

EXERCISE 1.9. Show without using the results of Section 4 that for any prime p,

$$\frac{x^p - 1}{x - 1} = x^{p-1} + x^{p-2} + x^{p-3} + \cdots + 1$$

is irreducible in $\mathbb{Q}[x]$. (Hint: Make the substitution $y + 1 = x$.)

EXERCISE 1.10. Show that $x^4 - 10x^2 + 1$ is irreducible in $\mathbb{Q}[x]$. (Hint: Do it directly.)

6.3. More on minimal and irreducible polynomials.

EXERCISE 1.11. Let K be a field and let

$$f(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_0$$

be a polynomial in $K[x]$. Define the *formal derivative* $f'(x)$ of $f(x)$ to be

$$f'(x) = na_n x^{n-1} + (n-1)a_{n-1}x^{n-2} + \ldots + 2a_2 x + a_1.$$

Convince yourself that all of the usual properties of derivatives (linearity, product rule, chain rule) can be proven for formal derivatives by completely algebraic means. Then show that if $g(x)^2$ divides $f(x)$, then $g(x)$ divides $f'(x)$.

EXERCISE 1.12. Let K be a field of characteristic 0 and let L be an extension of K (not necessarily finite). Let $f(x) \in K[x]$ be an irreducible polynomial. Show that $f(x)$ has no repeated factors in $L[x]$; in particular, it has no multiple roots in L.

EXERCISE 1.13. Let $M \supseteq L \supseteq K$ be fields. Let $\alpha \in M$ be algebraic over K with minimal polynomial $f(x) \in K[x]$. Show that if $K(\alpha) \cap L = K$ and L/K is Galois, then $f(x)$ is also the minimal polynomial for α over L.

EXERCISE 1.14. Let L/K be a finite extension and let α and β be two elements of L. Explain how to compute polynomials (over K) which are satisfied by $\alpha + \beta$, $\alpha\beta$ and α^{-1}. (Hint: use linear algebra.) Give an example to show that your method does not always yield minimal polynomials. Use your method (and Exercise 1.10) to determine the minimal polynomial of $\sqrt{2} + \sqrt{3} \in \mathbb{Q}(\sqrt{2}, \sqrt{3})$.

EXERCISE 1.15. Let $f(x) \in \mathbb{F}_p[x]$. Show that $f(x^p) = f(x)^p$.

6.4. Some trace calculations.

EXERCISE 1.16. Use the following method to show that $\sqrt{3} \notin \mathbb{Q}(\sqrt[4]{2})$: Suppose that it is, so that $\sqrt{3} = a + b\sqrt[4]{2} + c\sqrt{2} + d\sqrt[4]{8}$ with $a, b, c, d \in \mathbb{Q}$. Compute the trace (from $\mathbb{Q}(\sqrt[4]{2})$ to $\mathbb{Q}$) of both sides to conclude that $a = 0$. Thus $\sqrt{3}/\sqrt[4]{2} = b + c\sqrt[4]{2} + d\sqrt{2}$. Continue the procedure to show that $b = c = 0$, and then derive a contradiction.

EXERCISE 1.17. Let $d_1, \ldots, d_n$ be pairwise relatively prime squarefree integers, all different from 1. Show that

$$\mathbb{Q}(\sqrt{d_1}, \ldots, \sqrt{d_n})$$

has degree 2^n over $\mathbb{Q}$. Conclude with an interesting fact about square roots summing to rational numbers.

EXERCISE 1.18. Show that $\cos(72°) = (\sqrt{5} - 1)/4$. (Hint: Use trigonometric identities to find some polynomial which $\cos(72°)$ satisfies. Then compare this with the minimal polynomial of $(\sqrt{5} - 1)/4$.)

EXERCISE 1.19. Compute the norm and trace maps from $\mathbb{Q}(\zeta_5)$ to $\mathbb{Q}$. (Hint: Exercise 1.18 can be used to cut down on the computations needed.)

6.5. Arithmetical functions.

EXERCISE 1.20. For any positive integer n, define $\varphi(n)$ to be the number of positive integers less than n and relatively prime to n. φ is called the *Euler φ-function*. Show that $\varphi(mn) = \varphi(m)\varphi(n)$ if m and n are relatively prime, and show that $\varphi(p^k) = p^k - p^{k-1}$ for p prime.

CHAPTER 2

Rings of Integers

1. Unique factorization

1.1. Factorization in subrings of number fields. Let K be a number field. Although there is much information which can be obtained just by considering K, answering many of the most interesting questions will require some sort of notion of factorization into primes. Factorization in K itself is not very interesting: every non-zero element is a unit, so there are no primes at all. In order to obtain these primes we must somehow define a special subring of K; this ring should have lots of primes, and factorizations in it should hopefully yield interesting arithmetic information.

EXAMPLE 1.1. As a first example of the useful of factorizations, let us solve the Diophantine equation

$$x^2 - y^2 = 105.$$

(When we speak of solving a Diophantine equation, we always mean that we are interested in solutions with $x, y \in \mathbb{Z}$, or occasionally $\mathbb{Q}$.) We can solve this equation by first factoring it as

$$(x + y)(x - y) = 105.$$

Since both $x + y$ and $x - y$ are integers, we see that we are searching for pairs of integers $d = x + y$, $e = x - y$ such that $de = 105$. The fact that x and y are integers implies that d and e must be congruent modulo 2, so we are really looking for complimentary pairs of divisors of 105 which are congruent modulo 2. These pairs (up to reordering and negation) are

$$(d, e) = (105, 1), (35, 3), (21, 5), (15, 7);$$

they yield the solutions

$$(x, y) = (53, 52), (19, 16), (13, 8), (11, 4)$$

and their negatives. This example illustrates the usefulness of factorizations for solving Diophantine equations. On the other hand, when one has an equation like $x^2+y^2 = p$ which can not be factored over $\mathbb{Z}$, it becomes necessary to add additional numbers with which to factor. In this case, $x^2 + y^2$ does factor over $\mathbb{Z}[i]$.

The question, then, is which subring. We take as our model the subring $\mathbb{Z}$ of the number field $\mathbb{Q}$. Of course, we have a very good theory of factorization in $\mathbb{Z}$: every non-zero $n \in \mathbb{Z}$ factors uniquely as a product

$$n = \pm p_1^{e_1} \cdots p_k^{e_k}$$

where the p_i are distinct positive primes and all $e_i \geq 0$. This sort of factorization actually extends to the field $\mathbb{Q}$: any non-zero rational number $\frac{m}{n} \in \mathbb{Q}$ can be uniquely written as a product

$$\frac{m}{n} = \pm p_1^{e_1} \cdots p_k^{e_k}$$

where now we allow the e_i to be negative as well. Of course, the p_i are not really prime in $\mathbb{Q}$, but so long as we remember that they come from $\mathbb{Z}$ we can still consider them as distinguished elements to be used in factorizations. In any event, note that this sort of factorization shows that we have an isomorphism

$$\mathbb{Q}^* \cong \mathbb{Z}/2\mathbb{Z} \times \bigoplus_p \mathbb{Z}$$

where the direct sum is over all positive primes p of $\mathbb{Z}$.

It is probably worth pausing a moment here to clarify the sign issue. In $\mathbb{Z}$ we have two "copies" p and $-p$ of each prime. They behave exactly the same in factorizations (the $\pm$ sign absorbing any changes), and there is no real reason to prefer one over the other. For the time being just assume that we have chosen one of them to use in factorizations; in the case of $\mathbb{Z}$, the positive primes are the natural choice, but later on, when we have rings with lots of non-trivial units, there will be no obvious natural choices. Fortunately, all of this confusion will go away as soon as we begin working with ideals rather than elements.

Returning to the previous discussion of factorization in $\mathbb{Z}$, our first requirement must be that we have some sort of good factorization theory in our special subring R of K. We shall see later that it is unreasonable to ask for unique factorization, but we would like something close.

> *First condition (vague)*: R should have a good theory of factorization.

Our second requirement should be that the factorizations in R should extend to K in some way. The easiest way to insure this is to require that K be the *field of fractions* of R; this just means that every element of K can be written as a quotient of two elements of R. In particular, the subring $\mathbb{Z}$ of K, while a wonderful ring in many ways, has field of fractions $\mathbb{Q}$, so it is not suitable for a theory of factorization in any number field larger than $\mathbb{Q}$.

> *Second condition*: The field of fractions of R should be K.

We will in fact obtain a stronger version of the second condition, and since it is easier to check we state it as well.

> *Second condition (strong form)* : Every $\alpha \in K$ can be written as α'/n where $\alpha' \in R$ and $n \in \mathbb{Z}$.

All of the above conditions amount to asking that R be "big enough"; this is clear for the second condition, while for the first we will see that in order to get a good factorization theory one must not leave out too many elements of K.

Now, it happens that $\mathbb{Q}$ has lots of subrings with all of $\mathbb{Q}$ as field of fractions. For example, for any set of primes S we have the ring.

$$S^{-1}\mathbb{Z} = \left\{ \frac{a}{b} \in \mathbb{Q} \mid \text{all prime factors of } b \text{ are in } S \right\}.$$

In terms of unique factorization in $\mathbb{Z}$, rational numbers are in $S^{-1}\mathbb{Z}$ if and only if they can be written as

$$\pm p_1^{e_1} \cdots p_k^{e_k}$$

where we allow e_i to be any integer for $p_i \in S$, but we require e_i to be positive if $p_i \notin S$. Of course, these rings seem somewhat contrived; we are really just adding some denominators to $\mathbb{Z}$. In fact, it is easy to see that all $p \in S$ are now units in $S^{-1}\mathbb{Z}$, so the primes of $S^{-1}\mathbb{Z}$ are just the primes of $\mathbb{Z}$ not in S. Thus factorizations into primes of $S^{-1}\mathbb{Z}$ contains less information than those in $\mathbb{Z}$. Somehow, then, in order to get the most information we want to choose for R the smallest subring of K which satisfies the first two conditions.

Taking advantage of our knowledge that $\mathbb{Z}$ is a good prototype for R, one possibility for this third condition is to require that $R \cap \mathbb{Q} = \mathbb{Z}$.

Third condition: $R \cap \mathbb{Q} = \mathbb{Z}$.

Our goal, then, is to find a good interpretation of the first condition, and then we will hope that there is a natural subring of K satisfying the three conditions.

1.2. First attempts. In order to help us figure out what interpretations to give to our first condition, let us begin by making some guesses. Let K be a quadratic number field. We know that we can write $K = \mathbb{Q}(\sqrt{d})$ for a unique squarefree integer d. Let us take our guess for the special subring to be

$$R = \mathbb{Z}[\sqrt{d}].$$

Now, while there are many other $d' \in \mathbb{Q}$ such that $K = \mathbb{Q}(\sqrt{d'})$, this ring R has several things recommending it. First of all, if d' is not an integer, then $d' \in \mathbb{Z}[\sqrt{d'}] \cap \mathbb{Q}$, so this intersection is larger than $\mathbb{Z}$; this would violate our third condition. Also, if d' is a non-squarefree integer, then we can write $d' = e^2 d$, so

$$\sqrt{d'} \in R$$

but

$$\sqrt{d} \notin \mathbb{Z}[\sqrt{d'}].$$

Thus $\mathbb{Z}[\sqrt{d'}]$ seems to missing the element $\sqrt{d}$ which it really ought to contain, while R does not appear to be missing anything. (Later we will see that sometimes R is missing some non-obvious elements, but let us not worry about this yet.) Considering all of this, then, $\mathbb{Z}[\sqrt{d}]$ seems to be the most natural choice for special subring R.

As a second example, take $K = \mathbb{Q}(\zeta_m)$. This time there is really only one obvious ring to write down, that being $R = \mathbb{Z}[\zeta_m]$. (Note that R is independent of the choice of primitive m^{th} root of unity ζ_m since every primitive m^{th} root of unity is a power of every other one. One can also check that if m is odd, then $\mathbb{Z}[\zeta_m] = \mathbb{Z}[\zeta_{2m}]$, so that we have defined the same ring no matter which m is used to define K.) So for lack of any better choices, we will take $R = \mathbb{Z}[\zeta_m]$ to be our guess for $\mathbb{Q}(\zeta_m)$.

The astute reader will have noticed that we have now made two different choices for the special subring of $K = \mathbb{Q}(\sqrt{-3})$. On the one hand, K is a quadratic field, so we have chosen $R = \mathbb{Z}[\sqrt{-3}]$. On the other hand, K is also a cyclotomic field: we have $K = \mathbb{Q}(\zeta_3)$, since

$$\zeta_3 = \frac{-1 + \sqrt{-3}}{2}.$$

In this case we have the choice $R' = \mathbb{Z}[\frac{-1+\sqrt{-3}}{2}]$, which is actually larger than R. Right away we see that one of these must be wrong. We will figure out which one it is a bit later.

Ignoring that issue, note that at the very least these choices all satisfy the strong form of our second condition, and one can show without too much difficulty that they satisfy the third condition. The main remaining consideration is the factorization condition.

1.3. Example : the Gaussian integers. Just to see that at least sometimes we have obtained the nice theory we were looking for, let us analyze in detail the case of $K = \mathbb{Q}(i)$ and $R = \mathbb{Z}[i]$, where $i = \sqrt{-1}$. Since $i^2 = -1$, we have

$$\mathbb{Q}(i) = \{a + bi \mid a, b \in \mathbb{Q}\}$$

and

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

We claim that $\mathbb{Z}[i]$ is a unique factorization domain. The proof of this rests upon the fact that there is a division algorithm. In order to state it we need some measure of the size of a Gaussian integer; the most natural measure is the norm $\mathrm{N}_{\mathbb{Q}(i)/\mathbb{Q}}$, which explicitly is just

$$\mathrm{N}_{\mathbb{Q}(i)/\mathbb{Q}}(a + bi) = a^2 + b^2.$$

Let us just write N for this norm for the remainder of the section; we also write $\overline{a + bi}$ for the conjugate $a - bi$ (recalling our earlier conventions, this is just the image of $a + bi$ under the other complex embedding), so that

$$\mathrm{N}(\alpha) = \alpha \cdot \bar{\alpha}$$

for all $\alpha \in \mathbb{Q}(i)$. Note also that

$$\mathrm{N}(\alpha) = \mathrm{N}(\bar{\alpha}),$$

and that if $\alpha \in \mathbb{Z}[i]$, then $\mathrm{N}(\alpha) \in \mathbb{Z}$.

Lemma 1.2. *For any $\alpha, \beta \in \mathbb{Z}[i]$ with $\beta \neq 0$, there exists $q, r \in \mathbb{Z}[i]$ such*

$$\alpha = \beta q + r$$

and

$$0 \leq \mathrm{N}(r) \leq \frac{1}{2}\,\mathrm{N}(\beta).$$

The key here is to reduce to a division problem in $\mathbb{Z}$. Specifically, the equation

$$\alpha = \beta q + r$$

is equivalent to

$$\alpha\bar{\beta} = \beta\bar{\beta}q + \bar{\beta}r,$$

and now $\beta\bar{\beta} \in \mathbb{Z}$.

Proof. Write

$$\alpha\bar{\beta} = a + bi$$

with $a, b \in \mathbb{Z}$; by division in $\mathbb{Z}$ we can write

$$a = \mathrm{N}(\beta)q_1 + r_1$$

and

$$b = \mathrm{N}(\beta)q_2 + r_2$$

with $q_1, q_2, r_1, r_2 \in \mathbb{Z}$ and $0 \leq r_1, r_2 < \mathrm{N}(\beta)$. In fact, replacing the q_i by $q_i + 1$ and the r_i by $r_i - \mathrm{N}(\beta)$, if necessary, we can obtain the stronger bound

$$0 \leq |r_1|, |r_2| \leq \frac{1}{2}\,\mathrm{N}(\beta).$$

We now have

$$\begin{aligned}
a+bi &= \mathrm{N}(\beta)(q_1+q_2 i)+(r_1+r_2 i)\\
\alpha\bar{\beta} &= \beta\bar{\beta}(q_1+q_2 i)+(r_1+r_2 i)\\
\alpha &= \beta(q_1+q_2 i)+\frac{r_1+r_2 i}{\bar{\beta}}.
\end{aligned}$$

Note that this equation implies in particular that

$$\frac{r_1+r_2 i}{\bar{\beta}} = \alpha-\beta(q_1+q_2 i)\in \mathbb{Z}[i].$$

Write $r\in\mathbb{Z}[i]$ for this quotient and set $q=q_1+q_2 i$, so that we have

$$\alpha=\beta q+r.$$

It remains to show that r satisfies the desired bound. We calculate

$$\begin{aligned}
\bar{\beta}r &= r_1+r_2 i\\
\mathrm{N}(\bar{\beta})\,\mathrm{N}(r) &= \mathrm{N}(r_1+r_2 i)\\
\mathrm{N}(r) &= \frac{\mathrm{N}(r_1+r_2 i)}{\mathrm{N}(\bar{\beta})}\\
&= \frac{r_1^2+r_2^2}{\mathrm{N}(\bar{\beta})}\\
&\le \frac{\frac{1}{4}\mathrm{N}(\beta)^2+\frac{1}{4}\mathrm{N}(\beta)^2}{\mathrm{N}(\bar{\beta})}\\
&= \frac{1}{2}\frac{\mathrm{N}(\beta)^2}{\mathrm{N}(\beta)}\\
&= \frac{1}{2}\mathrm{N}(\beta)
\end{aligned}$$

as claimed. □

Since $\mathbb{Z}[i]$ is obviously noetherian (it is a quotient of the noetherian ring $\mathbb{Z}[x]$), this shows that $\mathbb{Z}[i]$ is Euclidean. By Proposition C.4.7 we conclude that $\mathbb{Z}[i]$ is a unique factorization domain.

Before we begin actually factoring elements of $\mathbb{Z}[i]$, we should determine the units.

LEMMA 1.3. *$u\in\mathbb{Z}[i]$ is a unit if and only if $\mathrm{N}(u)=1$; in particular, the only units are ±1 and $\pm i$.*

PROOF. Suppose first that $\mathrm{N}(u)=1$. Then $u\bar{u}=1$ and $\bar{u}\in\mathbb{Z}[i]$, so u is a unit. Conversely, if $u\in\mathbb{Z}[i]$ is a unit, then there exists $v\in\mathbb{Z}[i]$ with $uv=1$. Thus $\mathrm{N}(u)\,\mathrm{N}(v)=1$. Since $\mathrm{N}(u)$ and $\mathrm{N}(v)$ are integers, this implies that $\mathrm{N}(u)=\pm1$. Since it is not possible in $\mathbb{Z}[i]$ to have $\mathrm{N}(u)=-1$, this proves the first statement of the lemma. Writing $u=x+yi$ with $x,y\in\mathbb{Z}$, the last statement of the lemma amounts to solving the equation $x^2+y^2=1$. □

The key to the determination of the primes of $\mathbb{Z}[i]$ is to use our knowledge of the primes of $\mathbb{Z}$. The connection comes from the next lemma.

LEMMA 1.4. *Let $\pi\in\mathbb{Z}[i]$ be a prime element. Then π divides (in $\mathbb{Z}[i]$) some prime p of $\mathbb{Z}$.*

Proof. Note that $\mathrm{N}(\pi) = \pi\bar{\pi} \in \mathbb{Z}$ and π divides this integer. If $\mathrm{N}(\pi)$ is prime, then the lemma is immediate. If $\mathrm{N}(\pi)$ is not prime, then factor $\mathrm{N}(\pi)$ as a product of primes of $\mathbb{Z}$; since π is prime in $\mathbb{Z}[i]$, the definition of prime implies that π must divide one of these factors. $\square$

Lemma 1.4 implies that we can determine all primes of $\mathbb{Z}[i]$ by determining how all primes of $\mathbb{Z}$ factor in $\mathbb{Z}[i]$. Later on we will see a general method for approaching this problem, but for now let us not worry about motivating our next few steps. So let p be a positive prime in $\mathbb{Z}$ such that $p \equiv 3 \pmod 4$. Suppose that p factors over $\mathbb{Z}[i]$, say as $\alpha\beta$, with α and β not units. Then

$$p^2 = \mathrm{N}(p) = \mathrm{N}(\alpha)\,\mathrm{N}(\beta),$$

so Lemma 1.3 implies that

$$\mathrm{N}(\alpha) = \mathrm{N}(\beta) = p.$$

Writing $\alpha = a + bi$, this implies that $p = a^2 + b^2$. But this is impossible, since modulo 4 all sums of two squares are congruent to 0, 1 or 2. Thus p is still prime as an element of $\mathbb{Z}[i]$.

Now let p be a positive prime such that $p \equiv 1 \pmod 4$ and suppose that p does not factor in $\mathbb{Z}[i]$. By Exercise 2.2 we have that there exists $a \in \mathbb{Z}$ such that

$$a^2 \equiv -1 \pmod p.$$

Thus p divides $a^2 + 1$ in $\mathbb{Z}$. Factoring $a^2 + 1$ as $(a + i)(a - i)$ over $\mathbb{Z}[i]$, we have that p divides the product $(a + i)(a - i)$. Our assumption that p is prime in $\mathbb{Z}[i]$ now implies that p divides one of these factors. But this is absurd, since p would then divide the coefficient of i, which is ± 1. This is a contradiction, so such a p is not prime. We summarize all of this in the next proposition.

Proposition 1.5. *Let π be a prime of $\mathbb{Z}[i]$. Then one of the three following conditions holds:*

(1) *π is associate to a positive rational prime p such that $p \equiv 3 \pmod 4$;*
(2) *$\mathrm{N}(\pi) = p$ where p is a positive rational prime such that $p \equiv 1 \pmod 4$. In this case every prime of norm p is associate to exactly one of π and $\bar{\pi}$;*
(3) *π is associate to $1 + i$.*

Proof. By Lemma 1.4 we know that π divides some rational prime p. If $p \equiv 3 \pmod 4$, then p itself is prime in $\mathbb{Z}[i]$, so π must be associate to p. The $p \equiv 1 \pmod 4$ case is Exercise 2.3. Lastly, if $p = 2$, then the fact that 2 factors as $-i(1 + i)^2$ shows that π must be associate to $1 + i$. $\square$

Example 1.6. Let us factor $\alpha = -133 - 119i \in \mathbb{Z}[i]$. We compute that

$$\mathrm{N}(\alpha) = 31850 = 2 \cdot 5^2 \cdot 7^2 \cdot 13.$$

Since 2 divides $\mathrm{N}(\alpha)$, we know that $1 + i$ divides α. Since $7 \equiv 3 \pmod 4$, we know that 7 is prime in $\mathbb{Z}[i]$, so we must have that 7 divides α. To determine what happens with the primes of norm 5 and 13 we must determine what these primes are. We have

$$5 = (2 + i)(2 - i)$$

and

$$13 = (3 + 2i)(3 - 2i).$$

To finish the factorization we simply have to figure out which of the prime factors of 13 divides α and whether one or both of the prime factors of 5 divide α. One finds that $(2+i)^2$ and $3+2i$ divide α. Up to a unit, then, the factorization of α is

$$(1+i)\cdot(2+i)^2\cdot 7\cdot(3+2i);$$

multiplying it out we find that the unit is i, so that

$$-133-119i = i\cdot(1+i)\cdot(2+i)^2\cdot 7\cdot(3+2i).$$

Our analysis of factorization in $\mathbb{Z}[i]$ seems to have suggested some connection with primes of the form x^2+y^2. In fact, using our knowledge of the arithmetic of $\mathbb{Z}[i]$, we can easily obtain the full result.

PROPOSITION 1.7. *A positive rational prime p can be written as x^2+y^2 with $x, y \in \mathbb{Z}$ if and only if p factors in $\mathbb{Z}[i]$.*

PROOF. Suppose that $p = x^2+y^2$. Then $p = (x+yi)(x-yi)$, and one easily checks that neither factor could be a unit; thus p factors in $\mathbb{Z}[i]$. Conversely, if p factors in $\mathbb{Z}[i]$, say as $\alpha\beta$, then $\mathrm{N}(\alpha) = \mathrm{N}(\beta) = p$. If $\alpha = x+yi$, then we conclude that $p = x^2+y^2$, as desired. $\square$

COROLLARY 1.8. *A positive rational prime p can be written as x^2+y^2 with $x, y \in \mathbb{Z}$ if and only if $p = 2$ or $p \equiv 1 \pmod 4$. Furthermore, this decomposition is unique up to switching x and y and negating either (or both) x or y.*

PROOF. Everything but uniqueness is immediate from Proposition 1.5 and Proposition 1.7. In fact, uniqueness also follows easily, since there are exactly 8 primes $x+yi$ dividing any $p \equiv 1 \pmod 4$ (two conjugates times four units) and these all have x and y the same up to negation and switching the factors. $\square$

1.4. Failure of unique factorization. Having given one example where everything works perfectly, let us now give several where things do not work. Before we do, we state a simple lemma which is extremely useful in factoring and finding irreducibles.

LEMMA 1.9. *Let R be a subring of a number field K such that $\mathrm{N}_{K/\mathbb{Q}}(\alpha)$ is an integer for every $\alpha \in R$. Let α and β be elements of R such that α divides β in R. Then $\mathrm{N}_{K/\mathbb{Q}}(\alpha)$ divides $\mathrm{N}_{K/\mathbb{Q}}(\beta)$ in $\mathbb{Z}$. In particular, if $\mathrm{N}_{K/\mathbb{Q}}(\alpha)$ is prime in $\mathbb{Z}$, then α is irreducible in R. Also, α is a unit only if $\mathrm{N}_{K/\mathbb{Q}}(\alpha) = \pm 1$.*

We leave the proof to the reader.

Let us begin with the field $K = \mathbb{Q}(\sqrt{-5})$ and the ring $R = \mathbb{Z}[\sqrt{-5}]$. Consider the factorization of 6 in $\mathbb{Z}[\sqrt{-5}]$. On the one hand, $6 = 2\cdot 3$. Both 2 and 3 are irreducible in R, as is easy to check using Lemma 1.9. On the other hand,

$$6 = (1+\sqrt{-5})(1-\sqrt{-5}),$$

and both of these factors are also irreducible. R has only the two units ± 1 (use Lemma 1.9 to prove this), so none of these are associates. (This could also be seen directly from the norms.) Thus R is not a UFD.

All is not lost, however. The problem, as Kummer realized, is simply that R is missing some "elements". He repaired unique factorization with his theory of ideal numbers. In modern terms, we use the somewhat simpler method of factorization into ideals. Specifically, the factorizations above are only using principal ideals, and it turns out that R is not a principal ideal domain. We need the non-principal ideals in order to solve our factorization problem.

The ideals we want (we will see later how to compute them) are

$$\mathfrak{a}_1 = \bigl(2, 1+\sqrt{-5}\bigr)$$
$$\mathfrak{a}_2 = \bigl(3, 1+\sqrt{-5}\bigr)$$
$$\mathfrak{a}_3 = \bigl(3, 1-\sqrt{-5}\bigr).$$

Note that we can also write

$$\mathfrak{a}_1 = \bigl(2, 1-\sqrt{-5}\bigr)$$

since $2 \in \mathfrak{a}_1$. We now find that

$$\begin{aligned}\mathfrak{a}_1^2 &= \bigl(2\cdot 2, 2\cdot(1-\sqrt{-5}), (1+\sqrt{-5})\cdot 2, (1+\sqrt{-5})\cdot(1-\sqrt{-5})\bigr)\\ &= \bigl(4, 2-2\sqrt{-5}, 2+2\sqrt{-5}, 6\bigr)\\ &= \bigl(2\bigr)\end{aligned}$$

since $2 = 6-4 \in \mathfrak{a}_1^2$ and every generator is divisible by 2. Similarly, one finds that

$$\mathfrak{a}_1\mathfrak{a}_2 = \bigl(1+\sqrt{-5}\bigr)$$
$$\mathfrak{a}_1\mathfrak{a}_3 = \bigl(1-\sqrt{-5}\bigr)$$
$$\mathfrak{a}_2\mathfrak{a}_3 = \bigl(3\bigr).$$

In particular,

$$\bigl(6\bigr) = \bigl(2\bigr)\bigl(3\bigr) = (\mathfrak{a}_1\mathfrak{a}_1)(\mathfrak{a}_2\mathfrak{a}_3)$$

and

$$\bigl(6\bigr) = \bigl(1+\sqrt{-5}\bigr)\bigl(1-\sqrt{-5}\bigr) = (\mathfrak{a}_1\mathfrak{a}_2)(\mathfrak{a}_1\mathfrak{a}_3)$$

are really the same factorization in terms of ideals. The two different factorizations in terms of elements comes from regrouping the non-principal factors in two different ways. (Before it becomes too confusing let us acknowledge the fact that it can often be difficult to tell in an equation when symbols like (2) are ideals or simply elements. We will usually try to write principal ideals with slightly large parentheses, like $\bigl(2\bigr)$, if there is any chance of confusion. Fortunately, it rarely matters very much whether one is working with principal ideals or with actual elements, and hopefully whenever it does matter it will be clear which is being done.)

So, then, while we do not have unique factorization of elements in $\mathbb{Z}[\sqrt{5}]$, we can still hope that we have unique factorization of ideals. This is not perfect, but it is a pretty good substitute.

Let us now consider $K = \mathbb{Q}(\zeta)$ and $R = \mathbb{Z}[\zeta]$ where $\zeta = \zeta_{23}$. Here things are much more complicated (K has degree 22 over $\mathbb{Q}$), but we should at least state Kummer's famous counterexample to unique factorization. He found that

$$(1+\zeta^2+\zeta^4+\zeta^5+\zeta^6+\zeta^{10}+\zeta^{11})(1+\zeta+\zeta^5+\zeta^6+\zeta^7+\zeta^9+\zeta^{11})$$

is divisible by 2. (Work it out. It's not nearly as bad as it looks. You will need to use the identity

$$\zeta^{22} = -1-\zeta-\zeta^2-\cdots-\zeta^{21},$$

which is just the statement that $\Phi_{23}(\zeta) = 0$.) He also showed that 2 is irreducible in R (a non-trivial fact in this situation), and that 2 doesn't divide either factor. Thus R can not possibly be a UFD.

Here again one can show that unique factorization is restored if factorizations are considered as factorizations of ideals. We will not even attempt to write them down, however. (One might ask why we went all the way up to $\mathbb{Q}(\zeta_{23})$ to give our counterexample. The answer is fairly remarkable: for $m \leq 22$, every ring $\mathbb{Z}[\zeta_m]$ is a UFD.)

Let us consider one last example. Take $K = \mathbb{Q}(\sqrt{-3})$ and $R = \mathbb{Z}[\sqrt{-3}]$. Recall that for this field we already suspected that something was wrong, as we had another possible choice for R. It turns out that in this ring things go very wrong. First of all, we have

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

and 2, $1+\sqrt{-3}$ and $1-\sqrt{-3}$ are all easily checked to be irreducible. Thus R is not a UFD.

This time, however, we do not even have unique factorization of ideals. Let $\mathfrak{a}$ be the ideal $\bigl(2, 1+\sqrt{-3}\bigr)$. Then we compute

$$\begin{aligned} \mathfrak{a}^2 &= \bigl(4, 2+2\sqrt{-3}, (1+\sqrt{-3})^2\bigr) \\ &= \bigl(4, 2+2\sqrt{-3}, -2+2\sqrt{-3}\bigr) \\ &= \bigl(4, 2+2\sqrt{-3}\bigr) \\ &= \bigl(2\bigr)\bigl(2, 1+\sqrt{-3}\bigr) \\ &= \bigl(2\bigr)\mathfrak{a}. \end{aligned}$$

But $\mathfrak{a} \neq (2)$, since $1+\sqrt{-3} \notin (2)$. Thus we have an example of non-unique factorization of ideals.

Luckily, we did have another choice for this ring. In fact, the ring $R' = \mathbb{Z}[\frac{-1+\sqrt{-3}}{2}]$ not only has unique factorization of ideals, it is actually a UFD. (See Exercise 2.5. Note that in this ring,

$$\bigl(2, 1+\sqrt{-3}\bigr) = \bigl(2\bigr)$$

since now 2 does divide $1+\sqrt{-3}$.) Thus it is certainly a much better choice than R. The problem with R is that it is missing certain elements; we will see the full solution in the next section.

2. Algebraic integers

2.1. Integrally closed rings. The key to our search for the right special subring of a number field K is the "good factorization theory" condition. As we have seen, it is unreasonable to expect unique factorization, although there is still some hope that we may be able to get unique factorization of ideals. What we need, then, is some condition which is weaker than UFD but still strong enough to eliminate the problem case of $\mathbb{Z}[\sqrt{3}]$. The correct condition turns out to be the following.

DEFINITION 2.1. Let R be an integral domain contained in some field K. An element $\alpha \in K$ is said to be *integral over* R if it satisfies some monic polynomial in $R[x]$. R is said to be *integrally closed in* K if every element in K which is integral over R actually lies in R.

Note that the definition says nothing about monic polynomials in $R[x]$ actually having roots in K; it says only that if they do have roots in K, then these roots lie in R. Note also that there is nothing about the minimal polynomial of α in the definition; any monic polynomial at all will do, irreducible or not.

Example 2.2. Let $R = \mathbb{Z}$ and $K = \mathbb{Q}$. Suppose that there is some $\frac{r}{s} \in \mathbb{Q}$ (with r and s assumed to be relatively prime) satisfying some monic polynomial

$$x^n + a_{n-1}x^{n-1} + \cdots + a_0 \in \mathbb{Z}[x].$$

Then

$$\left(\frac{r}{s}\right)^n + a_{n-1}\left(\frac{r}{s}\right)^{n-1} + \cdots + a_0 = 0,$$

so

$$r^n + a_{n-1}sr^{n-1} + \cdots + a_0s^n = 0$$
$$s(-a_{n-1}r^{n-1} - sa_{n-2}r^{n-2} - \cdots - a_0s^{n-1}) = r^n.$$

Thus s divides r^n. Since r and s were assumed to be relatively prime, this implies that $s = 1$. Thus $\frac{r}{s} \in \mathbb{Z}$. This shows that if a monic polynomial with integer coefficients has a rational root, then the root is actually an integer; in other words, $\mathbb{Z}$ is integrally closed in $\mathbb{Q}$.

The exact same proof works for any UFD R with field of fractions K, thus yielding the desired connection between integrally closed rings and UFDs.

Proposition 2.3. *Let R be a UFD with field of fractions K. Then R is integrally closed in K.*

Example 2.4. The converse of Proposition 2.3 is false. For example, it is not too hard to show that $\mathbb{Z}[\sqrt{-5}]$ is integrally closed in $\mathbb{Q}(\sqrt{-5})$ (we will do this soon), but as we saw before $\mathbb{Z}[\sqrt{-5}]$ is not a UFD.

Example 2.5. Proposition 2.3 does not hold if K is replaced with a larger field. For example, take $R = \mathbb{Z}$ and $K = \mathbb{Q}(i)$. Then the element $i \in \mathbb{Q}(i)$ satisfies the monic polynomial $x^2 + 1 \in \mathbb{Z}[x]$, but $i \notin \mathbb{Z}$; thus $\mathbb{Z}$ is not integrally closed in $\mathbb{Q}(i)$.

Example 2.6. Let $R = \mathbb{Z}[\sqrt{-3}]$ and $K = \mathbb{Q}(\sqrt{-3})$. Consider the polynomial

$$x^2 + x + 1 \in R[x].$$

By the quadratic formula this has roots

$$\alpha = \frac{-1 \pm \sqrt{-3}}{2} \in K.$$

These roots are not in R, so R is not integrally closed in K. On the other hand, $R' = \mathbb{Z}[\frac{-1+\sqrt{-3}}{2}]$ is integrally closed in K, as we will show shortly. We have therefore found a way to distinguish between these two choices for special subring of K.

Note that as promised the property of being integrally closed corresponds to R being "large enough" in K; that is, R can not leave out any elements of K which are integral over R. What we are looking for, then, is a ring R which has K as its field of fractions, which is integrally closed in K, and which is as small as possible given the first two conditions. That such a ring exists is not immediately clear; we will show that it does and give a more concrete description of it in the next section. In order to do this we first should define the notion of integral closure of a ring in a field.

Definition 2.7. Let R be a subring of a field K. The *integral closure of R in K* is defined to the subset of K of elements which are integral over R.

Note that it is not at all clear that the integral closure R' of R is even a ring, let alone integrally closed if it is. (R' contains all elements which are roots of monic polynomials with coefficients in R, but what about monic polynomials with coefficients in R'?)

2.2. Rings of integers. Let K be a number field. We define the *ring of integers* $\mathcal{O}_K$ of K to be the integral closure of $\mathbb{Z}$ in K. Thus $\mathcal{O}_K$ consists of all elements of K which satisfy monic polynomials in $\mathbb{Z}[x]$. (While every element of K satisfies a monic polynomial with rational coefficients and also satisfies a not necessarily monic polynomial with integral coefficients, it is not true that every element of K satisfies a monic polynomial with integer coefficients.) An element of $\mathcal{O}_K$ will be called an *algebraic integer*. Note that by Example 2.2, we have $\mathcal{O}_{\mathbb{Q}} = \mathbb{Z}$. From now on, in order to avoid confusion we will refer to elements of $\mathbb{Z}$ as *rational integers*.

EXAMPLE 2.8. Let $K = \mathbb{Q}(\sqrt{d})$ with d a squarefree integer. Then $\sqrt{d} \in \mathcal{O}_K$, since it satisfies the monic polynomial $x^2 - d \in \mathbb{Z}[x]$. More generally, if $a, b \in \mathbb{Z}$, then $a + b\sqrt{d} \in \mathcal{O}_K$, as it satisfies the polynomial

$$x^2 - 2ax + (a^2 - db^2) \in \mathbb{Z}[x].$$

Thus $\mathbb{Z}[\sqrt{d}] \subseteq \mathcal{O}_K$. We will see later that this is the entire ring of integers if $d \equiv 2, 3 \pmod 4$, but that there are more integers if $d \equiv 1 \pmod 4$.

Our first goal is to prove that $\mathcal{O}_K$ really is a ring. To do this we must find analogues for algebraic integers and $\mathbb{Z}$-modules of the fundamental relations between algebraic numbers and $\mathbb{Q}$-vector spaces. Recall that a $\mathbb{Z}$-module A is said to be *finitely generated* if there is some finite set $a_1, \dots, a_m \in A$ such that every element of A can be written as a $\mathbb{Z}$-linear combination of the a_i.

PROPOSITION 2.9. *Let K be a number field. For any $\alpha \in K$, the following are equivalent:*

1. *α is an algebraic integer;*
2. *The minimal polynomial of α has coefficients in $\mathbb{Z}$;*
3. *The ring $\mathbb{Z}[\alpha]$ is a finitely generated $\mathbb{Z}$-module;*
4. *α is contained in some subring A of K which is a finitely generated $\mathbb{Z}$-module;*
5. *There is some finitely generated $\mathbb{Z}$-submodule A of K such that $\alpha A \subseteq A$.*

PROOF. We show first that each statement implies the next. For (1) implies (2), suppose that α is an algebraic integer, so that it satisfies some monic polynomial $f(x) \in \mathbb{Z}[x]$. Let $g(x) \in \mathbb{Q}[x]$ be the minimal polynomial of α. Then $g(x)$ divides $f(x)$ in $\mathbb{Q}[x]$. By Exercise 1.4, $g(x)$ actually lies in $\mathbb{Z}[x]$, as claimed.

To show that (2) implies (3), note that

$$\mathbb{Z}[x]/(g(x)) \cong \mathbb{Z}[\alpha]$$

where $g(x)$ is the minimal polynomial of α. (Just consider the map sending x to α, which is easily seen to be an isomorphism.) Since $g(x)$ is monic, the elements $1, x, \dots, x^{n-1}$ (where n is the degree of $g(x)$) are a $\mathbb{Z}$-basis for $\mathbb{Z}[x]/(g(x))$. (This is certainly not true if $g(x)$ is not monic, since then, while some multiple of x^n can be written in terms of $1, x, \dots, x^{n-1}$, the power x^n itself can not be. For an example, compare $\mathbb{Z}[x]/(x^2+1)$, which is generated as a $\mathbb{Z}$-module by 1 and x, with $\mathbb{Z}[x]/(2x-1)$, which requires infinitely many $\mathbb{Z}$-generators.) Thus $1, \alpha, \dots, \alpha^{n-1}$ is a $\mathbb{Z}$-basis for $\mathbb{Z}[\alpha]$, so $\mathbb{Z}[\alpha]$ is a finitely generated $\mathbb{Z}$-module. That (3) implies (4) and (4) implies (5) is clear.

It remains to show that (5) implies (1). So suppose that there exists a finitely generated $\mathbb{Z}$-submodule A of K such that $\alpha A \subseteq A$. Since A is a submodule of K and K is $\mathbb{Z}$-torsion-free (being a field of characteristic 0), A is also torsion-free. Since A is finitely generated by hypothesis, it follows that it is a free $\mathbb{Z}$-module of finite rank. (See Appendix C, Section 5.) Let $a_1, \ldots, a_m$ be a $\mathbb{Z}$-basis for A. Since multiplication by α maps A to itself we can view it as a map

$$m_\alpha : A \to A;$$

expressing this in terms of the $\mathbb{Z}$-basis $a_1, \ldots, a_m$, we can represent m_α as an $m \times m$ matrix M with coefficients in $\mathbb{Z}$. Let $f(x)$ be the characteristic polynomial of m_α, which is just the determinant of $xI - M$. The Cayley-Hamilton theorem shows that $f(M) = 0$ (if you are uncomfortable with the Cayley-Hamilton theorem over rings, note that for this calculation we can consider M as a matrix over the rationals and apply Cayley-Hamilton there); since the map $f(M) : A \to A$ is just multiplication by $f(\alpha)$ and A is torsion free, this implies that $f(\alpha) = 0$. But $f(x)$ is clearly a monic polynomial with coefficients in $\mathbb{Z}$ (every characteristic polynomial is monic, and $f(x)$ has integer coefficients since M has integer entries), so α is an algebraic integer, as claimed. □

From this proposition it is easy to obtain the fundamental properties of $\mathcal{O}_K$. Note first that the fact that the minimal polynomial of an algebraic integer has rational integer coefficients implies that its norm and trace are rational integers. In particular, Lemma 1.9 applies. The next lemma is just the strong form of our second condition on the special subring.

Lemma 2.10. *Let $\alpha \in K$. Then there is some $a \in \mathbb{Z}$ such that $a\alpha \in \mathcal{O}_K$.*

Proof. Let $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0 \in \mathbb{Q}[x]$ be the minimal polynomial of α. Let $a \in \mathbb{Z}$ be some integer such that $af(x) \in \mathbb{Z}[x]$. (Such an a clearly exists.) Let $g(x)$ be the monic polynomial

$$x^n + aa_{n-1}x^{n-1} + a^2a_{n-2}x^{n-2} + \cdots + a^n a_0,$$

which is in $\mathbb{Z}[x]$ since $af(x)$ is. We have

$$g(a\alpha) = a^n\alpha^n + a^n a_{n-1}x^{n-1} + \cdots + a^n a_0 = a^n f(\alpha) = 0.$$

Thus $a\alpha$ satisfies a monic polynomial with integral coefficients, and therefore lies in $\mathcal{O}_K$. □

We next show that $\mathcal{O}_K$ really is a ring. The proof of this is quite similar to the proof that the set of algebraic elements of a field form a field.

Lemma 2.11. *Let α, β be elements of $\mathcal{O}_K$. Then $\mathbb{Z}[\alpha, \beta]$ is a finitely generated $\mathbb{Z}$-submodule of K. More generally, if $\alpha_1, \ldots, \alpha_m$ are elements of $\mathcal{O}_K$, then $\mathbb{Z}[\alpha_1, \ldots, \alpha_m]$ is a finitely generated $\mathbb{Z}$-submodule of K.*

Proof. If $a_1, \ldots, a_m$ are $\mathbb{Z}$-generators of $\mathbb{Z}[\alpha]$ and $b_1, \ldots, b_n$ are $\mathbb{Z}$-generators of $\mathbb{Z}[\beta]$, one shows easily that the products a_ib_j are $\mathbb{Z}$-generators of $\mathbb{Z}[\alpha, \beta]$. The general case is similar. □

Proposition 2.12. *The sum and product of algebraic integers of K are again algebraic integers of K. In particular, $\mathcal{O}_K$ is a ring.*

PROOF. Let α, β be in $\mathcal{O}_K$. By Lemma 2.11 the ring $\mathbb{Z}[\alpha, \beta]$ is a finitely-generated $\mathbb{Z}$-module. This ring contains $\alpha + \beta$ and $\alpha\beta$; it now follows from Proposition 2.9 that $\alpha + \beta$ and $\alpha\beta$ are algebraic integers, and therefore that $\mathcal{O}_K$ is a ring. □

Next we show that $\mathcal{O}_K$ is integrally closed in K; this is our first condition.

LEMMA 2.13. *Let $f(x)$ be a monic polynomial with coefficients in $\mathcal{O}_K$. Let $\alpha \in K$ be a root of $f(x)$. Then $\alpha \in \mathcal{O}_K$. In particular, $\mathcal{O}_K$ is integrally closed in K.*

PROOF. Let $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0$ with $a_i \in \mathcal{O}_K$. Let S be the ring $\mathbb{Z}[a_0, \ldots, a_{n-1}]$; Lemma 2.11 show that S is a finitely generated $\mathbb{Z}$-module. Now, since $f(x)$ is monic with coefficients in S, the ring $S' = S[\alpha]$ will be finitely generated over S, with generators $1, \alpha, \ldots, \alpha^{n-1}$ (not necessarily a basis). Thus S' is finitely generated over S, which in turn is finitely generated over $\mathbb{Z}$; it follows easily that S' is finitely generated over $\mathbb{Z}$. Since $\alpha \in S'$, we now conclude by Proposition 2.9 that α is an algebraic integer. □

The last thing we need to show is that $\mathcal{O}_K$ satisfies the third condition.

LEMMA 2.14. $\mathcal{O}_K \cap \mathbb{Q} = \mathbb{Z}$.

PROOF. Let α be a rational number which is integral over $\mathbb{Z}$. Then by Proposition 2.9 the minimal polynomial $x - \alpha$ has coefficients in $\mathbb{Z}$; that is, $\alpha \in \mathbb{Z}$. □

More generally, we have the following.

LEMMA 2.15. *Let K and L be number fields such that $K \subseteq L$. Then*

$$\mathcal{O}_K = \mathcal{O}_L \cap K.$$

PROOF. $\mathcal{O}_L$ is the subset of L of elements which satisfy monic integer polynomials. Therefore, $\mathcal{O}_L \cap K$ is just the set of elements of K which satisfy monic integer polynomials; in other words, $\mathcal{O}_K$. □

We have seen, then, that $\mathcal{O}_K$ satisfies all of the conditions which we had set down. In the next section we give the fundamental algebraic description of $\mathcal{O}_K$.

2.3. Integral bases. Let K be a number field of degree n. Recall that K is a $\mathbb{Q}$-vector space of dimension n. A natural question is whether or not a similar statement can be made about $\mathcal{O}_K$ as a $\mathbb{Z}$-module. Remarkably, it turns out that the strongest analogue of the $\mathbb{Q}$-statement is true: $\mathcal{O}_K$ is a free $\mathbb{Z}$-module of rank n. We will prove this fact in this section. (Note that if we knew that $\mathcal{O}_K$ was a finitely-generated $\mathbb{Z}$-module, then the fact that it was a free $\mathbb{Z}$-module would follow immediately from the fact that it was torsion-free. However, the fact that $\mathcal{O}_K$ is a finitely-generated $\mathbb{Z}$-module is not immediately clear. Even if we knew it was, and thus that A is a free $\mathbb{Z}$-module, it still would not be obvious that it actually had rank n.)

To begin with, let $\alpha_1, \ldots, \alpha_n$ be a $\mathbb{Q}$-basis for K. Further assume that the α_i are all algebraic integers; this can be done by applying Lemma 2.10 to any $\mathbb{Q}$-basis for K. Since the α_i satisfy no linear dependence with $\mathbb{Q}$-coefficients, they certainly satisfy no linear dependence with $\mathbb{Z}$-coefficients; thus

$$\mathbb{Z}\alpha_1 + \mathbb{Z}\alpha_2 + \cdots + \mathbb{Z}\alpha_n$$

is a free $\mathbb{Z}$-module of rank n. Furthermore, it is clearly contained in $\mathcal{O}_K$; thus $\mathcal{O}_K$ contains a free $\mathbb{Z}$-module of rank n. To complete the proof we will just need to find some free $\mathbb{Z}$-module of rank n which contains $\mathcal{O}_K$.

This direction requires a bit more care. Our basic strategy is the following: let $\alpha_1, \dots, \alpha_n$ be a $\mathbb{Q}$-basis for K consisting entirely of algebraic integers. Then any $\alpha \in K$ can be written uniquely as

$$a_1\alpha_1 + \cdots + a_n\alpha_n$$

for some $a_i \in \mathbb{Q}$. We want to find some bound on the possible denominators for the a_i in the case that α is an algebraic integer; the desired result will follow easily from this. The bound in question is a number which comes up very often in algebraic number theory.

Definition 2.16. Let K be a number field of degree n with complex embeddings $\sigma_1, \dots, \sigma_n$. Let $\alpha_1, \dots, \alpha_n$ be elements of K. The *discriminant* $\Delta(\alpha_1, \dots, \alpha_n)$ of this n-tuple is defined to be the square of the determinant of the $n \times n$ matrix

$$\big(\sigma_i(\alpha_j)\big).$$

Example 2.17. Take $K = \mathbb{Q}(\sqrt{2})$ and $\alpha_1 = 1$, $\alpha_2 = \sqrt{2}$. Then

$$\Delta(1, \sqrt{2}) = \det \begin{pmatrix} 1 & \sqrt{2} \\ 1 & -\sqrt{2} \end{pmatrix}^2 = (-\sqrt{2} - \sqrt{2})^2 = 8.$$

Note that the squaring kills any -1 factors coming from changing the order of the α_i, so that $\Delta(\alpha_1, \dots, \alpha_n)$ depends only on the numbers themselves and not on the order. The discriminant has a second fundamental expression.

Lemma 2.18. *Let K be a number field as above and let $\alpha_1, \dots, \alpha_n$ be elements of K. Then $\Delta(\alpha_1, \dots, \alpha_n)$ is equal to the determinant of the $n \times n$ matrix*

$$\big(\mathrm{Tr}_{K/\mathbb{Q}}(\alpha_i\alpha_j)\big).$$

Proof. Let $A = (\sigma_i(\alpha_j))$. Since $\det A^t = \det A$ (where A^t is the transpose of A), we see that $\Delta(\alpha_1, \dots, \alpha_n)$ is equal to the determinant of $A^t \cdot A$. The ij entry of this matrix is

$$\sum_{k=1}^{n} \sigma_k(\alpha_i)\sigma_k(\alpha_j) = \sum_{k=1}^{n} \sigma_k(\alpha_i\alpha_j) = \mathrm{Tr}_{K/\mathbb{Q}}(\alpha_i\alpha_j)$$

by Corollary I.5.5. This proves the lemma. □

Corollary 2.19. $\Delta(\alpha_1, \dots, \alpha_n) \in \mathbb{Q}$*; if the α_i are all algebraic integers, then* $\Delta(\alpha_1, \dots, \alpha_n) \in \mathbb{Z}$.

Proof. This follows immediately from Lemma 2.18 and the corresponding results for the trace. □

Example 2.20. We will use Lemma 2.18 to recompute the discriminant of Example 2.17. We have $\mathrm{Tr}_{\mathbb{Q}(\sqrt{2})/\mathbb{Q}}(a + b\sqrt{2}) = 2a$, so

$$\Delta(1, \sqrt{2}) = \det \begin{pmatrix} \mathrm{Tr}(1) & \mathrm{Tr}(\sqrt{2}) \\ \mathrm{Tr}(\sqrt{2}) & \mathrm{Tr}(2) \end{pmatrix} = \det \begin{pmatrix} 2 & 0 \\ 0 & 4 \end{pmatrix} = 8$$

as before.

The first use of the discriminant is in determining if a collection of elements of K is a basis; that is, $\alpha_1, \dots, \alpha_n$ is a $\mathbb{Q}$-basis for K if and only if $\Delta(\alpha_1, \dots, \alpha_n)$ is non-zero. (See Exercise 2.20.) The second use of the discriminant is the following result.

PROPOSITION 2.21. *Let K be a number field of degree n and let $\alpha_1, \dots, \alpha_n$ be a $\mathbb{Q}$-basis for K consisting entirely of algebraic integers. Set $\Delta = \Delta(\alpha_1, \dots, \alpha_n)$. Fix $\alpha \in \mathcal{O}_K$ and write*

$$\alpha = a_1\alpha_1 + \cdots + a_n\alpha_n$$

with each $a_i \in \mathbb{Q}$. Then $\Delta a_i \in \mathbb{Z}$ for all i.

PROOF. Note that by Corollary 2.19 and Exercise 2.20 Δ is a non-zero integer, so the statement of the proposition makes sense. To prove the proposition, apply the embedding σ_i to the expression for α, yielding

$$\sigma_i(\alpha) = a_1\sigma_i(\alpha_1) + \cdots + a_n\sigma_i(\alpha_n).$$

This can be considered to be a system of n linear equations in the n "unknowns" $a_1, \dots, a_n$; that is, we have the matrix equation

$$\begin{pmatrix} \sigma_1(\alpha) \\ \sigma_2(\alpha) \\ \vdots \\ \sigma_n(\alpha) \end{pmatrix} = \begin{pmatrix} \sigma_1(\alpha_1) & \sigma_1(\alpha_2) & \cdots & \sigma_1(\alpha_n) \\ \sigma_2(\alpha_1) & \sigma_2(\alpha_2) & \cdots & \sigma_2(\alpha_n) \\ \vdots & \vdots & & \vdots \\ \sigma_n(\alpha_1) & \sigma_n(\alpha_2) & \cdots & \sigma_n(\alpha_n) \end{pmatrix} \begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_n \end{pmatrix}$$

By Cramer's rule, this has the unique solution

$$a_i = \gamma_i/\delta$$

where δ is the determinant of $A = (\sigma_i(\alpha_j))$ (so that $\delta^2 = \Delta$; in particular, the solution is unique since $\Delta \neq 0$) and γ_i is the determinant of the matrix obtained from A by replacing the i^{th} column by $(\sigma_j(\alpha))$. Note that both γ_i and δ are algebraic integers, since each entry in each matrix is. Since $\delta^2 = \Delta$, we have

$$\Delta a_i = \delta\gamma_i.$$

The left-hand side is rational and the right-hand side is an algebraic integer, so both sides must be rational integers by Lemma 2.14. This proves the proposition. □

THEOREM 2.22. *Let K be a number field with ring of integers $\mathcal{O}_K$. Let $n = [K : \mathbb{Q}]$. Then $\mathcal{O}_K$ is a free $\mathbb{Z}$-module of rank n.*

PROOF. Let $\alpha_1, \dots, \alpha_n$ be a $\mathbb{Q}$-basis for K consisting entirely of algebraic integers. We have

$$\mathbb{Z}\alpha_1 + \cdots \mathbb{Z}\alpha_n \subseteq \mathcal{O}_K,$$

and by Proposition 2.21 we have

$$\mathcal{O}_K \subseteq \frac{1}{\Delta}\left(\mathbb{Z}\alpha_1 + \cdots \mathbb{Z}\alpha_n\right)$$

where $\Delta = \Delta(\alpha_1, \dots, \alpha_n)$. Thus we have shown that $\mathcal{O}_K$ lies between two free $\mathbb{Z}$-modules of rank n; it follows from Appendix C, Section 5 that $\mathcal{O}_K$ itself is free of rank n. □

COROLLARY 2.23. *Let K be a number field with ring of integers $\mathcal{O}_K$. Then $\mathcal{O}_K$ is noetherian.*

PROOF. By Theorem 2.22 we can find a $\mathbb{Z}$-basis $\alpha_1, \dots, \alpha_n$ for $\mathcal{O}_K$. Thus, in particular,

$$\mathcal{O}_K = \mathbb{Z}[\alpha_1, \dots, \alpha_n].$$

(This is far weaker than Theorem 2.22, but it is all that we need at the moment.) This allows us to define a surjective homomorphism

$$\mathbb{Z}[x_1, \dots, x_n] \twoheadrightarrow \mathcal{O}_K$$

sending x_i to α_i. Since $\mathbb{Z}[x_1, \dots, x_n]$ is noetherian (see Example C.3.2) and quotients of noetherian rings are noetherian (see Exercise 2.8), this implies that $\mathcal{O}_K$ is noetherian. $\square$

A $\mathbb{Z}$-basis for $\mathcal{O}_K$ is called an *integral basis*. In contrast to the situation with number fields, it is not always possible to find an integral basis of the form $1, \alpha, \alpha^2, \dots, \alpha^{n-1}$; that is, one can not always write $\mathcal{O}_K = \mathbb{Z}[\alpha]$ for some α. This tends to complicate things quite a bit; fortunately, in the situations we will be most interested in we will always have an expression of this form.

We conclude with one last definition. We define the *discriminant* Δ_K of the number field K to be the discriminant of any integral bases of K; that this is independent of the choice of integral basis is Exercise 2.21. The discriminant is an extremely useful invariant of the number field, although we will not make much use of it in this course.

2.4. Integers in quadratic fields. Let $K = \mathbb{Q}(\sqrt{d})$ be a quadratic field, where d is a squarefree integer distinct from 1. In this section we will determine the ring of integers $\mathcal{O}_K$.

Lemma 2.14 tells us that $\mathcal{O}_K \cap \mathbb{Q} = \mathbb{Z}$, so we need only consider $\alpha \in K$ which do not lie in $\mathbb{Q}$. We can write such an α as $\alpha = a + b\sqrt{d}$ with $b \neq 0$. Since α is automatically a primitive element for K, its minimal polynomial is the same as its characteristic polynomial. This we computed in Section I.3; it is just

$$x^2 - 2ax + (a^2 - b^2 d).$$

By Proposition 2.9, α is an algebraic integer if and only if

$$2a \in \mathbb{Z} \text{ and } a^2 - b^2 d \in \mathbb{Z}.$$

It is immediately clear from this that $\mathbb{Z}[\sqrt{d}] \subseteq \mathcal{O}_K$, as then both $a, b \in \mathbb{Z}$; however, it is still possible that there are additional integral elements.

Suppose first that $a \in \mathbb{Z}$. Then $a^2 \in \mathbb{Z}$, so $b^2 d \in \mathbb{Z}$. Since d is squarefree this implies that $b \in \mathbb{Z}$; thus we do not get any additional integers in this case.

The other case is that $a = a_1/2$, where $a_1 \in \mathbb{Z}$ is odd. Since

$$\frac{a_1^2}{4} - b^2 d \in \mathbb{Z}$$

we must have $b = b_1/2$ where b_1 in $\mathbb{Z}$ is also odd. Substituting this in, we find that

$$a_1^2 - b_1^2 d \equiv 0 \pmod 4,$$

this being an ordinary congruence over the integers. Now, since a_1 and b_1 are both odd,

$$a_1^2 \equiv b_1^2 \equiv 1 \pmod 4.$$

Substituting these in, we find that

$$1 - d \equiv a_1^2 - b_1^2 d \equiv 0 \pmod 4,$$

so

$$d \equiv 1 \pmod 4.$$

Thus in the case that $d \equiv 2, 3 \pmod 4$ there are no algebraic integers with a half an odd integer; if $d \equiv 1 \pmod 4$, then there are additional integers of the form

$$\frac{a_1 + b_1\sqrt{d}}{2}$$

where a_1 and b_1 are odd. (Note that $d \equiv 0 \pmod 4$ can not happen since d is squarefree.) We summarize this in the following proposition.

Proposition 2.24. *Let $K = \mathbb{Q}(\sqrt{d})$ be a quadratic field with d a squarefree integer. If $d \equiv 2, 3 \pmod 4$, then $\mathcal{O}_K = \mathbb{Z}[\sqrt{d}] \cong \mathbb{Z}[x]/(x^2 - d)$ and $\mathcal{O}_K$ is free of rank 2 over $\mathbb{Z}$ with basis $1, \sqrt{d}$. If $d \equiv 1 \pmod 4$, then $\mathcal{O}_K = \mathbb{Z}[\frac{1+\sqrt{d}}{2}] \cong \mathbb{Z}[x]/(x^2 - x + \frac{1-d}{4})$ and $\mathcal{O}_K$ is free of rank 2 over $\mathbb{Z}$ with basis $1, \frac{1+\sqrt{d}}{2}$.*

Proof. The previous discussion makes the proposition clear in the case that $d \equiv 2, 3 \pmod 4$; it is easy to see that $\mathbb{Z}[\sqrt{d}]$ is free of rank 2 over $\mathbb{Z}$ with the asserted basis. If $d \equiv 1 \pmod 4$, then we have

$$\mathcal{O}_K = \left\{a + b\sqrt{d} \mid a, b \in \mathbb{Z}\right\} \cup \left\{\frac{a + b\sqrt{d}}{2} \mid a, b \in \mathbb{Z},\ a, b \text{ odd}\right\}.$$

One can then check that $\mathcal{O}_K = \mathbb{Z}[\frac{1+\sqrt{d}}{2}]$ by direct computation; we leave this to the reader. The minimal polynomial of $\frac{1+\sqrt{d}}{2}$ is $x^2 - x + \frac{1-d}{4}$, which yields the other expression for $\mathcal{O}_K$. $\square$

2.5. More examples of rings of integers. Given an arbitrary number field K it is a difficult computational task to determine the ring of integers. There are several very clever algorithms available; see [**5**]. We will content ourselves with stating a few more examples.

We first consider the case of biquadratic fields; these are fields of the form $K = \mathbb{Q}(\sqrt{d}, \sqrt{e}) = \mathbb{Q}[x, y]/(x^2 - d, y^2 - e)$ where d and e are distinct squarefree integers. That such a field has degree 4 was (pretty much) shown in Exercise 1.17. Note first that K contains the square root of one other squarefree integer: $f = de/(d, e)^2$. Note also that if one starts with e and f, the third integer computed is d, and similarly if one starts with d and e.

Proposition 2.25. *Let $K = \mathbb{Q}(\sqrt{d}, \sqrt{e}, \sqrt{f})$ be a biquadratic field as above. Then we have the following possibilities for the ring of integers $\mathcal{O}_K$:*

(1) *If $d \equiv 3 \pmod 4$ and $e, f \equiv 2 \pmod 4$, then*

$$1, \sqrt{d}, \sqrt{e}, \frac{\sqrt{e} + \sqrt{f}}{2}$$

is an integral basis for $\mathcal{O}_K$.

(2) *If $d \equiv 1 \pmod 4$ and $e, f \equiv 2$ or $3 \pmod 4$, then*

$$1, \frac{1 + \sqrt{d}}{2}, \sqrt{e}, \frac{\sqrt{e} + \sqrt{f}}{2}$$

is an integral basis for $\mathcal{O}_K$.

(3) *If* $d, e, f \equiv 1 \pmod 4$, *then*

$$1, \frac{1+\sqrt{d}}{2}, \frac{1+\sqrt{e}}{2}, \left(\frac{1+\sqrt{d}}{2}\right)\left(\frac{1+\sqrt{f}}{2}\right)$$

is an integral basis for $\mathcal{O}_K$.

PROOF. See Exercise 2.11 for the case of $\mathbb{Q}(\sqrt{2}, \sqrt{3})$. The general case is similar. Note that despite appearances the cases listed cover all possible cases, up to re-ordering of d, e, f. $\square$

Next we consider the case of a *pure cubic field* $K = \mathbb{Q}(\sqrt[3]{d}) \cong \mathbb{Q}[x]/(x^3 - d)$ where d is a cubefree integer. (In contrast to the quadratic case, not all cubic fields are of this form.) Write $d = ef^2$ where e and f are squarefree and relatively prime; this amounts to grouping all of the p such that p^2 divides d into f and putting the rest in e.

PROPOSITION 2.26. *Let* $K = \mathbb{Q}(\sqrt[3]{d})$ *be a pure cubic field as above. Then we have the following possibilities for the ring of integers* $\mathcal{O}_K$.

(1) *If* $d \equiv 0, 2, 3, 4, 5, 6, 7 \pmod 9$, *then*

$$1, \sqrt[3]{d}, \frac{\sqrt[3]{d}^2}{f}$$

is an integral basis for $\mathcal{O}_K$.

(2) *If* $d \equiv 1 \pmod 9$, *then*

$$1, \sqrt[3]{d}, \frac{\sqrt[3]{d}^2 + f^2\sqrt[3]{d} + f^2}{3f}$$

is an integral basis for $\mathcal{O}_K$.

(3) *If* $d \equiv 8 \pmod 9$, *then*

$$1, \sqrt[3]{d}, \frac{\sqrt[3]{d}^2 - f^2\sqrt[3]{d} + f^2}{3f}$$

is an integral basis for $\mathcal{O}_K$.

PROOF. We omit the proof. For a sketch see [**14**, Chapter 2, Exercise 41]. $\square$

As a final example we consider cyclotomic fields. In this case, thankfully, things work out to be somewhat simpler.

PROPOSITION 2.27. *Let* $K = \mathbb{Q}(\zeta_m)$ *be the* m^{th} *cyclotomic field. Then* $\mathcal{O}_K = \mathbb{Z}[\zeta_m]$; *thus* $\mathcal{O}_K$ *has integral basis*

$$1, \zeta_m, \ldots, \zeta_m^{\varphi(m)-1}.$$

We will prove this proposition in the case that m is a prime (which is the only case we will need in the applications) in Section 4.

3. Unique factorization of ideals in Dedekind domains

3.1. Dedekind domains. Our next goal is to prove that rings of integers of number fields have unique factorization into ideals. The proof we will give works for a larger class of rings called *Dedekind domains*; as is often the case in algebra, the proof becomes somewhat easier to follow when abstracted to the appropriate axiomatic setting.

DEFINITION 3.1. Let R be an integral domain with field of fractions K. R is said to be a *Dedekind domain* if it has the following three properties.

(1) R is noetherian;
(2) R is integrally closed in K;
(3) Every non-zero prime ideal of R is a maximal ideal. (R is said to have *dimension* ≤ 1.)

Of course, in order for this to be useful to us we must show that rings of integers are Dedekind domains. We will need the following useful lemma in the proof.

LEMMA 3.2. *Let K be a number field and let $\mathfrak{a}$ be a non-zero ideal of $\mathcal{O}_K$. Then $\mathfrak{a} \cap \mathbb{Z}$ is non-zero; that is, $\mathfrak{a}$ contains some non-zero integer.*

PROOF. Let α be any non-zero element of $\mathfrak{a}$; in particular, α is an algebraic integer. We claim that $\mathrm{N}_{K/\mathbb{Q}}(\alpha) \in \mathfrak{a}$; since it is a rational integer, this will prove the lemma.

In order to prove this we will need to consider K as a subfield of the complex numbers. So let $\sigma : K \hookrightarrow \mathbb{C}$ be some fixed complex embedding of K. Let $\alpha_1, \ldots, \alpha_n$ be the images of α under the different complex embeddings of K, ordered so that $\alpha_1 = \sigma(\alpha)$. By Corollary I.5.5 we have

$$\mathrm{N}_{K/\mathbb{Q}}(\alpha) = \alpha_1 \cdots \alpha_n.$$

Set $\alpha' = \alpha_2 \cdots \alpha_n$. α' is an algebraic integer since it is a product of algebraic integers, and it is in $\sigma(K)$ since

$$\alpha' = \frac{\mathrm{N}_{K/\mathbb{Q}}(\alpha)}{\alpha_1}$$

and both factors on the right are in $\sigma(K)$. Thus α' is in $\sigma(\mathcal{O}_K)$. Let $\alpha'' \in \mathcal{O}_K$ be such that $\sigma(\alpha'') = \alpha'$. Since $\mathfrak{a}$ is an ideal and $\alpha \in \mathfrak{a}$ we have

$$\alpha''\alpha \in \mathfrak{a};$$

since $\alpha''\alpha = \mathrm{N}_{K/\mathbb{Q}}(\alpha)$ this completes the proof. □

PROPOSITION 3.3. *Let K be a number field. Then the ring of integers $\mathcal{O}_K$ is a Dedekind domain.*

PROOF. That $\mathcal{O}_K$ is noetherian is Corollary 2.23, and that it is integrally closed in K is Lemma 2.13. Thus it remains to show that every non-zero prime ideal of $\mathcal{O}_K$ is maximal. So let $\mathfrak{p}$ be a non-zero prime ideal of $\mathcal{O}_K$. By Lemma 3.2 there is some non-zero rational integer m in $\mathfrak{p}$. (We will see later that m could be taken to be a prime number, but we don't need this at the moment.) Thus there is a natural surjection

$$\mathcal{O}_K/\big(m\big) \twoheadrightarrow \mathcal{O}_K/\mathfrak{p}.$$

Now, by Theorem 2.22, $\mathcal{O}_K$ is a free $\mathbb{Z}$-module of rank $n = [K : \mathbb{Q}]$. It follows easily that $\mathcal{O}_K/(m)$ is finite and has size m^n. Since this ring surjects onto $\mathcal{O}_K/\mathfrak{p}$, it follows that $\mathcal{O}_K/\mathfrak{p}$ is finite. Finally, since $\mathfrak{p}$ is prime $\mathcal{O}_K/\mathfrak{p}$ is an integral domain; since it is also finite, Exercise 2.6 implies that it is actually a field, so that $\mathfrak{p}$ is a maximal ideal, as claimed. $\square$

There are other examples of Dedekind domains that come up in mathematics (for example, the local ring of a nonsingular point on an algebraic curve is a Dedekind domain), but we will not take the time to consider them here.

Before we begin the proof of unique factorization into ideals, let us consider briefly some of the peculiarities of ideal arithmetic. The main issue is that everything seems to happen backwards. For example, let (m) and (n) be ideals in $\mathbb{Z}$. Then the ideal $(m)(n) = (mn)$ is smaller (as a set) than either of the ideals (m) and (n), although the integer mn is larger in absolute value than either m or n. Thus the larger the number, the smaller the ideal. The same sort of behavior holds in arbitrary Dedekind domains, and one must always remember to take it into account. In particular, in a Dedekind domain the prime ideals are the largest ideals even though one would usually think of them as being the "smallest" elements.

3.2. Invertible ideals. Let R be a Dedekind domain with field of fractions K and let $\mathfrak{a}$ be a non-zero ideal of R. The key step in the proof of unique factorization of ideals is to show that there is some other ideal $\mathfrak{b}$ of R such that $\mathfrak{ab}$ is principal; after we prove this result, the remainder of the proof is pretty easy, as it is easy to do manipulations with principal ideals.

We will eventually need to prove that every ideal of R equals a product of prime ideals. We begin with a weaker statement.

LEMMA 3.4. *Let $\mathfrak{a}$ be a non-zero ideal of R. Then there exist (not necessarily distinct) non-zero prime ideals $\mathfrak{p}_1, \ldots, \mathfrak{p}_k$ of R such that*

$$\mathfrak{a} \supseteq \mathfrak{p}_1 \cdots \mathfrak{p}_k.$$

PROOF. Let $\mathcal{S}$ be the set of non-zero ideals of R which do not contain a product of non-zero prime ideals. Suppose that $\mathcal{S}$ is non-empty. Since R is noetherian $\mathcal{S}$ has a maximal element, say $\mathfrak{a}$. $\mathfrak{a}$ is certainly not prime, since then it would contain a product of prime ideals (namely, itself). Thus there exist $\alpha, \beta \in \mathcal{O}_K$ such that $\alpha, \beta \notin \mathfrak{a}$ but $\alpha\beta \in \mathfrak{a}$. Consider now the ideals $\mathfrak{a} + (\alpha)$ and $\mathfrak{a} + (\beta)$, which are strictly larger than $\mathfrak{a}$ and thus not in $\mathcal{S}$. Therefore $\mathfrak{a} + (\alpha)$ and $\mathfrak{a} + (\beta)$ both contain a product of non-zero prime ideals, by the definition of $\mathcal{S}$. But then the same is true of

$$\big(\mathfrak{a} + (\alpha)\big)\big(\mathfrak{a} + (\beta)\big) = \mathfrak{a} \cdot \mathfrak{a} + \alpha\mathfrak{a} + \beta\mathfrak{a} + \alpha\beta \subseteq \mathfrak{a}.$$

This is a contradiction, so $\mathcal{S}$ is empty; this proves the lemma. $\square$

Note that the proof of this lemma is very similar to the proof of Proposition C.3.3.

The next step is to show that pairs of ideals of R can be distinguished from each other by a single element of K, even though the ideals themselves may not be principal. We will only need this at the moment in the case that one of the ideals is all of R, so we prove only this version.

LEMMA 3.5. *Let $\mathfrak{a}$ be a non-zero ideal of R such that $\mathfrak{a} \neq R$. Then there exists $\gamma \in K$ such that $\gamma \notin R$ and $\gamma\mathfrak{a} \subseteq R$.*

The lemma just says that $\mathfrak{a}$ is significantly distinct from R in the sense that there is some non-integral element of K we can multiply it by which will not cause the ideal to become non-integral. R itself certainly does not have this property, for example.

PROOF. Fix any non-zero α in $\mathfrak{a}$. By Lemma 3.4 the principal ideal (α) contains some product of non-zero prime ideals; choose (not necessarily distinct) primes $\mathfrak{p}_1, \ldots, \mathfrak{p}_k$ such that

$$(\alpha) \supseteq \mathfrak{p}_1 \cdots \mathfrak{p}_k$$

and k is as small as possible. Since R is noetherian, it is also true that $\mathfrak{a}$ is contained in some maximal ideal $\mathfrak{p}$. (Some might claim that this statement is true independent of whether or not R is noetherian.) Thus

$$\mathfrak{p} \supseteq \mathfrak{a} \supseteq (\alpha) \supseteq \mathfrak{p}_1 \cdots \mathfrak{p}_k.$$

It follows from Exercise 2.9 that $\mathfrak{p}$ contains one of the $\mathfrak{p}_i$; we assume without loss of generality that it is $\mathfrak{p}_1$. Since R is Dedekind, $\mathfrak{p}_1$ is a maximal ideal, and thus $\mathfrak{p} = \mathfrak{p}_1$.

Now, since (α) contains no product of $k-1$ prime ideals, there must exist some $\beta \in \mathfrak{p}_2 \cdots \mathfrak{p}_k$ such that $\beta \notin (\alpha)$. Set $\gamma = \beta/\alpha$. We claim that γ satisfies the conditions of the lemma. First of all, $\gamma \notin R$ since $\beta \notin (\alpha)$. For the other part, if $\alpha' \in \mathfrak{a}$, then

$$\gamma\alpha' = \frac{\beta\alpha'}{\alpha}.$$

But $\alpha' \in \mathfrak{a} \subseteq \mathfrak{p} = \mathfrak{p}_1$, so

$$\beta\alpha' \in \mathfrak{p}_1\mathfrak{p}_2 \cdots \mathfrak{p}_k \subseteq (\alpha);$$

thus $\gamma\alpha' = \beta\alpha'/\alpha \in R$, as claimed. □

We are now in a position to prove that every ideal of R is "invertible", using the above two lemmas and the fact that R is integrally closed in K. (Note that we used the fact that R is noetherian very explicitly in Lemma 3.4 and the fact that R has dimension ≤ 1 in Lemma 3.5.)

PROPOSITION 3.6. *Let R be a Dedekind domain and let $\mathfrak{a}$ be a non-zero ideal of R. Then there is some non-zero ideal $\mathfrak{b}$ of R such that $\mathfrak{ab}$ is principal.*

PROOF. Fix any non-zero $\alpha \in \mathfrak{a}$ and set

$$\mathfrak{b} = \{\beta \in R \mid \beta\mathfrak{a} \subseteq (\alpha)\}.$$

One checks easily that $\mathfrak{b}$ is a non-zero ideal, and by definition we have $\mathfrak{ab} \subseteq (\alpha)$. We will prove that we have equality.

To do this, we consider

$$\mathfrak{c} = \frac{1}{\alpha}\mathfrak{ab}.$$

One checks immediately that $\mathfrak{c}$ is an ideal of R, and to show that $\mathfrak{ab} = (\alpha)$ is visibly the same as to show that $\mathfrak{c} = R$. So suppose that $\mathfrak{c} \neq R$. Then by Lemma 3.5 we can find $\gamma \in K$ such that $\gamma \notin R$ and $\gamma\mathfrak{c} \subseteq R$. We will show that γ is satisfies a monic polynomial with coefficients in R; since R is integrally closed in K, this will imply that $\gamma \in R$, which is a contradiction.

We want to apply the methods of Proposition 2.9 (5) $\Rightarrow$ (1). At the moment we have a submodule $\mathfrak{c}$ of K such that $\gamma\mathfrak{c} \subseteq R$, which isn't quite good enough. Note, however, that $\mathfrak{b} \subseteq \mathfrak{c}$ since $\alpha \in \mathfrak{a}$. Thus

$$\gamma\mathfrak{b} \subseteq \gamma\mathfrak{c} \subseteq R.$$

We will show that $\gamma\mathfrak{b} \subseteq \mathfrak{b}$.

So, take an arbitrary element $\beta \in \mathfrak{b}$. We want to show that $\gamma\beta \in \mathfrak{b}$. To do this we will show that for all $\alpha' \in \mathfrak{a}$, we have

$$\gamma\beta\alpha' \in \big(\alpha\big);$$

this will imply that $\gamma\beta \in \mathfrak{b}$ by the definition of $\mathfrak{b}$. (Note that $\gamma\beta \in R$ since $\gamma\beta \in \gamma\mathfrak{b} \subseteq \gamma\mathfrak{c} \subseteq R$.) So fix $\alpha' \in \mathfrak{a}$. Then $\beta\alpha' \in \big(\alpha\big)$ by definition of $\mathfrak{b}$, so we can write $\beta\alpha' = \alpha\delta$ for some $\delta \in R$. Now, visibly $\delta \in \mathfrak{c}$, so $\gamma\delta \in \gamma\mathfrak{c} \subseteq R$. So, finally,

$$\gamma\beta\alpha' = (\gamma\delta)\alpha \in \big(\alpha\big).$$

Thus $\gamma\beta \in \mathfrak{b}$; since this is true for all $\beta \in b$, we have $\gamma\mathfrak{b} \subseteq \mathfrak{b}$. But $\mathfrak{b}$ is an ideal of R, and thus finitely generated over R. We can not directly apply Proposition 2.9, since that requires that $\mathfrak{b}$ be finitely generated over $\mathbb{Z}$, but the same method as used there constructs a monic polynomial with coefficients in R which γ satisfies. Specifically, let $b_1, \ldots, b_k$ be a finite R-generating set for $\mathfrak{b}$ (we do not require that they are a basis; this is important, since $\mathfrak{b}$ need not be free), and let A be the matrix for multiplication by γ with respect to this basis. The Cayley-Hamilton theorem still applies to show that γ satisfies the characteristic polynomial of this matrix, which is a monic polynomial with coefficients in R. (Convince yourself that it doesn't matter that the b_i are not a basis.) Since R is integrally closed, this implies That $\gamma \in R$, which is the desired contradiction. $\square$

3.3. Factorizations of ideals. With Proposition 3.6 in hand it will not be difficult to prove unique factorization of ideals. We first give some useful preliminary results. We continue to let R be a Dedekind domain with field of fractions K.

LEMMA 3.7. *Let $\mathfrak{a}, \mathfrak{b}, \mathfrak{c}$ be ideals of R. Suppose that $\mathfrak{a}\mathfrak{b} = \mathfrak{a}\mathfrak{c}$. Then $\mathfrak{b} = \mathfrak{c}$.*

PROOF. Let $\mathfrak{a}'$ be an ideal of R such that $\mathfrak{a}\mathfrak{a}'$ is principal; $\mathfrak{a}'$ exists by Proposition 3.6. Let α be a generator of $\mathfrak{a}\mathfrak{a}'$. Then

$$\mathfrak{a}'\mathfrak{a}\mathfrak{b} = \mathfrak{a}'\mathfrak{a}\mathfrak{c}$$
$$\alpha\mathfrak{b} = \alpha\mathfrak{c}$$

which implies that $\mathfrak{b} = \mathfrak{c}$. $\square$

This lemma is not true if R is not a Dedekind domain; see the case of $\mathbb{Z}[\sqrt{-3}]$ in Section 1.4.

If $\mathfrak{a}$ and $\mathfrak{b}$ are ideals of R, we say that $\mathfrak{b}$ *divides* $\mathfrak{a}$ if there is some third ideal $\mathfrak{c}$ such that $\mathfrak{a} = \mathfrak{b}\mathfrak{c}$. Note in particular that this implies that $\mathfrak{b} \supseteq \mathfrak{a}$; in Dedekind domains these statements are actually equivalent.

LEMMA 3.8. *Let $\mathfrak{a}$ and $\mathfrak{b}$ be ideals of R. Then $\mathfrak{b}$ divides $\mathfrak{a}$ if and only if $\mathfrak{b} \supseteq \mathfrak{a}$.*

PROOF. We have already seen one direction, so suppose that $\mathfrak{b} \supseteq \mathfrak{a}$. Let $\mathfrak{b}'$ be such that $\mathfrak{b}\mathfrak{b}'$ is principal, say $\mathfrak{b}\mathfrak{b}' = \big(\beta\big)$. One verifies easily that $\mathfrak{c} = \frac{1}{\beta}\mathfrak{b}'\mathfrak{a}$ is an ideal of R (using the fact that $\mathfrak{b} \supseteq \mathfrak{a}$). We compute

$$\mathfrak{b}\mathfrak{c} = \frac{1}{\beta}\mathfrak{b}\mathfrak{b}'\mathfrak{a} = \frac{1}{\beta}\big(\beta\big)\mathfrak{a} = \mathfrak{a},$$

so $\mathfrak{b}$ divides $\mathfrak{a}$, as claimed. $\square$

We now prove the unique factorization theorem. We will say that an ideal $\mathfrak{a}$ of R *factors into primes* if we can write

$$\mathfrak{a} = \mathfrak{p}_1 \dots \mathfrak{p}_k$$

where the $\mathfrak{p}_i$ are non-zero prime ideals of R. We will say that $\mathfrak{a}$ *factors uniquely into primes* if any two such factorizations are the same up to rearrangement of the factors. (Note that the whole business of units and associates does not enter into these definitions since units are irrelevant on the level of ideals and associates generate the same ideal.)

THEOREM 3.9. *Let R be a Dedekind domain. Then every non-zero ideal of R factors uniquely into prime ideals.*

PROOF. We first show that every non-zero ideal of R actually factors into primes. Let $\mathcal{S}$ be the set of non-zero ideals of R which do not factor into primes. Suppose that $\mathcal{S}$ is non-empty. Since R is noetherian, $\mathcal{S}$ has a maximal element, say $\mathfrak{a}$. We know that $\mathfrak{a}$ is contained in some maximal ideal $\mathfrak{p}$; by Lemma 3.8 this implies that $\mathfrak{a} = \mathfrak{p}\mathfrak{b}$ for some ideal $\mathfrak{b}$. Lemma 3.8 now implies that $\mathfrak{b} \supseteq \mathfrak{a}$; in fact, we also have $\mathfrak{b} \neq \mathfrak{a}$ since if it did, Lemma 3.7 would imply that $R = \mathfrak{p}$, which it does not. Thus $\mathfrak{b} \notin \mathcal{S}$, since $\mathfrak{a}$ is a maximal element of $\mathcal{S}$, so it factors into primes; now so does $\mathfrak{a} = \mathfrak{p}\mathfrak{b}$, which is a contradiction. Thus $\mathcal{S}$ is empty, so every non-zero ideal of R factors into primes.

We now show that this factorization is unique. Let $\mathfrak{a}$ be an ideal with two factorizations, say

$$\mathfrak{p}_1 \cdots \mathfrak{p}_r = \mathfrak{a} = \mathfrak{q}_1 \cdots \mathfrak{q}_s.$$

Lemma 3.8 shows that $\mathfrak{p}_1 \supseteq \mathfrak{q}_1 \dots \mathfrak{q}_s$, and now Exercise 2.9 implies that $\mathfrak{p}_1 \supseteq \mathfrak{q}_i$ for some i. Reordering the $\mathfrak{q}_j$ if necessary, we assume that $\mathfrak{p}_1 \supseteq \mathfrak{q}_1$. Since every non-zero prime of R is maximal, this implies that $\mathfrak{p}_1 = \mathfrak{q}_1$. Using Lemma 3.7 we can cancel $\mathfrak{p}_1 = \mathfrak{q}_1$ from both sides, leaving us with

$$\mathfrak{p}_2 \cdots \mathfrak{p}_r = \mathfrak{q}_2 \cdots \mathfrak{q}_s.$$

Continuing in this way we find that $r = s$ and that the factors on each side are identical. This proves the theorem. $\square$

4. Rings of integers in cyclotomic fields

Let p be a rational prime and let $K = \mathbb{Q}(\zeta_p)$. We write ζ for ζ_p for this section. Recall that K has degree $\varphi(p) = p - 1$ over $\mathbb{Q}$. We wish to show that $\mathcal{O}_K = \mathbb{Z}[\zeta]$. Note that ζ is a root of $x^p - 1$, and thus is an algebraic integer; since $\mathcal{O}_K$ is a ring we have that $\mathbb{Z}[\zeta] \subseteq \mathcal{O}_K$. We need to show the other inclusion.

Following [**15**], we give a proof without assuming unique factorization of ideals. We begin with some norm and trace computations. Let j be any integer. If j is not divisible by p, then ζ^j is a primitive p^{th} root of unity, and thus its conjugates are $\zeta, \zeta^2, \dots, \zeta^{p-1}$. Therefore

$$\mathrm{Tr}_{K/\mathbb{Q}}(\zeta^j) = \zeta + \zeta^2 + \cdots + \zeta^{p-1} = \Phi_p(\zeta) - 1 = -1.$$

If p does divide j, then $\zeta^j = 1$, so it has only the one conjugate 1, and

$$\mathrm{Tr}_{K/\mathbb{Q}}(\zeta^j) = p - 1.$$

By linearity of the trace, we find that

$$\operatorname{Tr}_{K/\mathbb{Q}}(1-\zeta) = \operatorname{Tr}_{K/\mathbb{Q}}(1-\zeta^2) = \cdots = \operatorname{Tr}_{K/\mathbb{Q}}(1-\zeta^{p-1}) = p.$$

We also need to compute the norm of $1-\zeta$. For this, we use the factorization

$$x^{p-1} + x^{p-2} + \cdots + 1 = \Phi_p(x) = (x-\zeta)(x-\zeta^2)\cdots(x-\zeta^{p-1});$$

plugging in $x = 1$ shows that

$$p = (1-\zeta)(1-\zeta^2)\cdots(1-\zeta^{p-1}).$$

Since the $1-\zeta^j$ are the conjugates of $1-\zeta$, this shows that

$$\mathrm{N}_{K/\mathbb{Q}}(1-\zeta) = p.$$

The key result for determining the ring of integers $\mathcal{O}_K$ is the following.

Lemma 4.1.

$$(1-\zeta)\mathcal{O}_K \cap \mathbb{Z} = p\mathbb{Z}.$$

Proof. We saw above that p is a multiple of $1-\zeta$ in $\mathcal{O}_K$, so the inclusion

$$(1-\zeta)\mathcal{O}_K \cap \mathbb{Z} \supseteq p\mathbb{Z}$$

is immediate. Suppose now that the inclusion is strict. Since $(1-\zeta)\mathcal{O}_K \cap \mathbb{Z}$ is an ideal of $\mathbb{Z}$ (check the definition) containing $p\mathbb{Z}$ and $p\mathbb{Z}$ is a maximal ideal of $\mathbb{Z}$, we must have

$$(1-\zeta)\mathcal{O}_K \cap \mathbb{Z} = \mathbb{Z}.$$

Thus we can write

$$1 = \alpha(1-\zeta)$$

for some $\alpha \in \mathcal{O}_K$. That is, $1-\zeta$ is a unit in $\mathcal{O}_K$. But this is impossible by Lemma 1.9, since we know that $1-\zeta$ has norm p, while units have norm ± 1. This is a contradiction, which proves the lemma. □

Corollary 4.2. *For any $\alpha \in \mathcal{O}_K$,*

$$\operatorname{Tr}_{K/\mathbb{Q}}\big((1-\zeta)\alpha\big) \in p \cdot \mathbb{Z}.$$

Proof. We have

$$\begin{aligned}\operatorname{Tr}_{K/\mathbb{Q}}\big((1-\zeta)\alpha\big) &= \sigma_1((1-\zeta)\alpha) + \cdots + \sigma_{p-1}((1-\zeta)\alpha)\\ &= \sigma_1(1-\zeta)\sigma_1(\alpha) + \cdots + \sigma_{p-1}(1-\zeta)\sigma_{p-1}(\alpha)\\ &= (1-\zeta)\sigma_1(\alpha) + \cdots + (1-\zeta^{p-1})\sigma_{p-1}(\alpha)\end{aligned}$$

where the σ_i are the complex embeddings of K (which we are really viewing as automorphisms of K) with the usual ordering. Furthermore, by Exercise 2.12 $1-\zeta^j$ is a multiple of $1-\zeta$ in $\mathcal{O}_K$ for every $j \neq 0$. Thus

$$\operatorname{Tr}_{K/\mathbb{Q}}\big(\alpha(1-\zeta)\big) \in (1-\zeta)\mathcal{O}_K.$$

Since the trace is also a rational integer, Lemma 4.1 completes the proof. □

Proposition 4.3. *Let p be a prime number and let $K = \mathbb{Q}(\zeta_p)$ be the p^{th} cyclotomic field. Then*

$$\mathcal{O}_K = \mathbb{Z}[\zeta_p] \cong \mathbb{Z}[x]/(\Phi_p(x));$$

thus $1, \zeta_p, \ldots, \zeta_p^{p-2}$ is an integral basis for $\mathcal{O}_K$.

PROOF. Let $\alpha \in \mathcal{O}_K$ and write

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

with $a_i \in \mathbb{Q}$. Then

$$\alpha(1-\zeta) = a_0(1-\zeta) + a_1(\zeta - \zeta^2) + \cdots + a_{p-2}(\zeta^{p-2} - \zeta^{p-1}).$$

By the linearity of the trace and our above calculations we find that

$$\mathrm{Tr}_{K/\mathbb{Q}}\big(\alpha(1-\zeta)\big) = pa_0.$$

By Corollary 4.2 we also have

$$\mathrm{Tr}_{K/\mathbb{Q}}\big(\alpha(1-\zeta)\big) \in p\mathbb{Z},$$

so $a_0 \in \mathbb{Z}$.

Next consider the algebraic integer

$$(\alpha - a_0)\zeta^{-1} = a_1 + a_2\zeta + \cdots + a_{p-2}\zeta^{p-3};$$

this is an algebraic integer since $\zeta^{-1} = \zeta^{p-1}$ is. The same argument as above shows that $a_1 \in \mathbb{Z}$, and continuing in this way we find that all of the a_i are in $\mathbb{Z}$. This completes the proof. □

One can use an almost identical proof in the case where ζ is a p^k-root of unity for some k. The case of ζ_m where m has multiple prime factors is usually handled by a general lemma on rings of integers in compositums of number fields (see [**14**, Chapter 2, Theorem 12]).

5. Exercises

5.1. A Diophantine equation.

Exercise 2.1. Determine all right triangles with integer sides and one leg of length 21.

5.2. Problems on $\mathbb{Z}[i]$, $\mathbb{Z}[\sqrt{-2}]$ and $\mathbb{Z}[\zeta_3]$.

Exercise 2.2. Let p be a positive prime in $\mathbb{Z}$. Show that -1 is a square modulo p if and only if $p = 2$ or $p \equiv 1 \pmod 4$. Can you give any sort of explicit expression for $\sqrt{-1}$ in this case?

Exercise 2.3. Complete the analysis of the factorization of primes congruent to 1 modulo 4 in Proposition 1.5.

Exercise 2.4. Show that $\mathbb{Z}[\sqrt{-2}]$ is Euclidean and analyze the factorization of rational primes in this ring. What can you conclude about primes of the form $x^2 + 2y^2$?

Exercise 2.5. Show that $\mathbb{Z}[\zeta_3]$ is Euclidean and analyze the factorization of rational primes in this ring. About what quadratic form do we obtain information this time?

5.3. Problems on ideals.

Exercise 2.6. Show that every finite commutative integral domain is a field.

Exercise 2.7. Let R be a commutative ring. Show that the following properties are equivalent.

(1) Every ideal of R is finitely generated; that is, if I is an ideal, then there exist $a_1, \ldots, a_n \in I$ such that
$$I = \{r_1 a_1 + \cdots + r_n a_n \mid r_i \in R\}.$$
(2) Every increasing sequence of ideals of R eventually stabilizes; that is, if
$$I_1 \subseteq I_2 \subseteq \cdots \subseteq I_n \subseteq \cdots$$
then there exists an N such that for all $n, n' > N$, $I_n = I_{n'}$.
(3) Every non-empty set $\mathcal{S}$ of ideals of R contains a maximal element. (Recall that this means that there is an ideal $I \in \mathcal{S}$ such that $\mathcal{S}$ contains no ideal strictly containing I. Note that a set can have many maximal elements.)

If R satisfies the above equivalent conditions, then R is said to be *noetherian*.

Exercise 2.8. Let R be a noetherian ring and let I be an ideal of R. Show that R/I is noetherian.

Exercise 2.9. Let R be a ring, let $\mathfrak{p}$ be a prime ideal and let $I_1, \ldots, I_n$ be ideals of R. Suppose that
$$\mathfrak{p} \supseteq I_1 \cdots I_n.$$
Show that $\mathfrak{p} \supseteq I_i$ for some i.

5.4. Problems on rings of integers.

Exercise 2.10. Show that a Dedekind domain is a UFD if and only if it is a PID. (This is not true in general.)

EXERCISE 2.11. Compute the ring of integers in $K = \mathbb{Q}(\sqrt{2}, \sqrt{3})$. (Hint: Note that $\sqrt{6} \in K$. First show that $\alpha \in K$ is an algebraic integer if and only if $\mathrm{Tr}_{K/\mathbb{Q}(\sqrt{2})}(\alpha)$ and $\mathrm{N}_{K/\mathbb{Q}(\sqrt{2})}(\alpha)$ are algebraic integers. Next show that the same is true if $\sqrt{2}$ is replaced by $\sqrt{3}$ or $\sqrt{6}$. Now consider an arbitrary element

$$\alpha = a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6} \in K$$

with $a, b, c, d \in \mathbb{Q}$, and use the trace conditions to restrict a, b, c, d when α is an integer. Use norms to finish the analysis.)

5.5. Problems on cyclotomic fields.

EXERCISE 2.12. Show that $1 - \zeta_p^i$ and $1 - \zeta_p^j$ are associates in $\mathbb{Z}[\zeta_p]$ for any i and j which are not divisible by p.

EXERCISE 2.13. Show that the ideal $\bigl(1 - \zeta_p\bigr)$ is a prime in $\mathbb{Z}[\zeta_p]$. Conclude that the ideal (p) factors as $(1 - \zeta_p)^{p-1}$.

EXERCISE 2.14. Redo exercises 2.12 and 2.13 for ζ_{p^n}. Specifically, show that $1 - \zeta_{p^n}^i$ and $1 - \zeta_{p^n}^j$ are associates in $\mathbb{Z}[\zeta_{p^n}]$ for any i and j which are not divisible by p; show that $\bigl(1 - \zeta_{p^n}\bigr)$ is a prime ideal in $\mathbb{Z}[\zeta_{p^n}]$; and show that $\bigl(p\bigr)$ factors as $\bigl(1 - \zeta_{p^n}\bigr)^{\varphi(p^n)}$.

EXERCISE 2.15. Show that $1 - \zeta_m$ is a unit in $\mathbb{Z}[\zeta_m]$ if and only if m is not a prime power.

EXERCISE 2.16. Let K be a number field with complex embeddings $\sigma_1, \ldots, \sigma_n$. Let $\alpha \in K$ be an algebraic integer such that $\sigma_i(\alpha)$ has absolute value 1 for every i. Show that α is a root of unity. (Hint: Show that there are only finitely many such α in K.)

EXERCISE 2.17. Let u be a unit in $\mathbb{Z}[\zeta_p]$ Show that $u/\bar{u}$ is a power of ζ_p. Here $\bar{u}$ is the complex conjugate of u.

EXERCISE 2.18. For $m \geq 2$, let $\mathbb{Q}(\zeta_m)^+$ be the subfield of $\mathbb{Q}(\zeta_m)$ corresponding to the subgroup $\{\pm 1\}$ of $\mathrm{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q}) \cong (\mathbb{Z}/m\mathbb{Z})^*$. Show that $\mathbb{Q}(\zeta_m)^+ = \mathbb{Q}(\zeta_m + \zeta_m^{-1})$ and that every complex embedding of $\mathbb{Q}(\zeta_m)^+$ has image in $\mathbb{R}$. $\mathbb{Q}(\zeta_m)^+$ is called the *maximal real subfield of* $\mathbb{Q}(\zeta_m)$.

EXERCISE 2.19. Show that the ring of integers of $\mathbb{Q}(\zeta_m)^+$ is $\mathbb{Z}[\zeta_m + \zeta_m^{-1}]$.

5.6. Problems on discriminants.

EXERCISE 2.20. Let K be a number field of degree n and let $\alpha_1, \ldots, \alpha_n$ be elements of K. Show that the α_i form a basis for K if and only if $\Delta(\alpha_1, \ldots, \alpha_n) \neq 0$.

EXERCISE 2.21. Let K be a number field with ring of integers $\mathcal{O}_K$. Suppose that we have two integral bases $\alpha_1, \ldots, \alpha_n$ and $\alpha_1', \ldots, \alpha_n'$ of $\mathcal{O}_K$. Show that

$$\Delta(\alpha_1, \ldots, \alpha_n) = \Delta(\alpha_1', \ldots, \alpha_n').$$

EXERCISE 2.22. Let $K = \mathbb{Q}(\sqrt{d})$ be a quadratic number field with d a squarefree integer. Show that

$$\Delta_K = \begin{cases} d & d \equiv 1 \pmod 4; \\ 4d & d \equiv 2, 3 \pmod 4. \end{cases}$$

CHAPTER 3

Prime Splitting

In this chapter we will investigate how to explicitly factor ideals in rings of integers of number fields. A common theme will be considering ideals of one ring in another. Specifically, we will often have the following situation: K and L will be number fields with $K \subseteq L$ (so $\mathcal{O}_K \subseteq \mathcal{O}_L$), $\mathfrak{a}$ will be an ideal of $\mathcal{O}_K$, and we will consider the ideal $\mathfrak{a}\mathcal{O}_L$ of $\mathcal{O}_L$ generated by $\mathfrak{a}$. We will be especially interested in the case where $\mathfrak{a} = \mathfrak{p}$ is a prime of $\mathcal{O}_K$; determining how $\mathfrak{p}\mathcal{O}_L$ factors into primes of $\mathcal{O}_K$ (even though $\mathfrak{p}$ is prime in $\mathcal{O}_K$, it doesn't still have to be prime in $\mathcal{O}_L$) will be the key to our factorization results.

One other construction which is sometimes useful is to take a prime $\mathfrak{P}$ of $\mathcal{O}_L$ and to consider the ideal $\mathfrak{P} \cap \mathcal{O}_K$ of $\mathcal{O}_L$; this ideal is necessarily prime since there is an injection

$$\mathcal{O}_K/\mathfrak{P} \cap \mathcal{O}_K \hookrightarrow \mathcal{O}_L/\mathfrak{P}$$

and subrings of integral domains are again integral domains.

Very often we will be considering the case of an extension $K/\mathbb{Q}$, in which case the relevant ideals are of the form $p\mathcal{O}_K$ for rational primes p. Note that we could also write these ideals as (p), assuming that the ring the principal ideal is formed in is clear from context.

1. Example : Quadratic number fields

1.1. The prime ideals. Before we restrict to the case of quadratic number fields, we prove the following useful fact about prime ideals.

Lemma 1.1. *Let K be a number field and let $\mathfrak{p}$ be a non-zero prime ideal of $\mathcal{O}_K$. Then $\mathfrak{p}$ contains a rational prime.*

Proof. By Lemma II.3.2 we know that $\mathfrak{p}$ contains a non-zero integer. Let n be the smallest positive integer in $\mathfrak{p}$; n is not 1 since $\mathfrak{p} \neq \mathcal{O}_K$. Suppose that n is not prime in $\mathbb{Z}$. Then n factors as ab for some $a, b \in \mathbb{Z}^+$; since $\mathfrak{p}$ is a prime ideal it must contain at least one of a and b. But both of these factors are smaller than n, which contradicts the definition of n. Thus n must be prime, which proves the lemma. □

Lemma 1.1 tells us that every prime of $\mathcal{O}_K$ contain a rational prime; it then follows from Lemma II.3.8 that all non-zero primes of $\mathcal{O}_K$ divide an ideal of the form $p\mathcal{O}_K$ for some prime p of $\mathbb{Z}$. In particular, we can determine all primes of $\mathcal{O}_K$ simply by determining the factorization of these ideals $p\mathcal{O}_K$. Our main results will be explicit determinations of these factorizations.

In the calculations below we will be working with polynomials both in $\mathbb{Z}[x]$ and in $\mathbb{F}_p[x]$. We will write $\bar{g}(x)$ for polynomials in $\mathbb{F}_p[x]$, and we will then let $g(x)$

denote some choice of a polynomial in $\mathbb{Z}[x]$ reducing modulo p to $\bar{g}(x)$; the precise choice of $g(x)$ will never matter.

We now restrict to the case of quadratic number fields. Let $K = \mathbb{Q}(\sqrt{d})$ be a quadratic number field, where d is a squarefree integer. Set $\alpha = \sqrt{d}$ if $d \equiv 2, 3 \pmod 4$ and $\alpha = \frac{1+\sqrt{d}}{2}$ if $d \equiv 1 \pmod 4$, so that $\mathcal{O}_K = \mathbb{Z}[\alpha]$. Let $f(x)$ be the minimal polynomial of α, so that $f(x) = x^2 - d$ if $d \equiv 2, 3 \pmod 4$ and $f(x) = x^2 - x + \frac{1-d}{4}$ if $d \equiv 1 \pmod 4$.

Let p be a rational prime. To determine the factorization of the ideal $p\mathcal{O}_K$ in $\mathcal{O}_K$ we will compute in an easier setting. Specifically, $p\mathcal{O}_K$ is the kernel of the map

$$\mathcal{O}_K \to \mathcal{O}_K/p\mathcal{O}_K,$$

and we will find a second expression for this kernel. To do this, recall that $\mathcal{O}_K \cong \mathbb{Z}[x]/(f(x))$, where under the isomorphism α corresponds to x. We now have

$$\mathcal{O}_K/p\mathcal{O}_K \cong \big(\mathbb{Z}[x]/f(x)\big)/p \cong \mathbb{Z}[x]/(p, f(x)).$$

This last ring is isomorphic to

$$\mathbb{F}_p[x]/(\bar{f}(x)),$$

and here we can finally compute easily.

There are three possibilities for the factorization of $\bar{f}(x)$ in $\mathbb{F}_p[x]$. First of all, $\bar{f}(x)$ could be irreducible. Second, $\bar{f}(x)$ could factor as a product of distinct, monic linear (and therefore irreducible) polynomials. Third, $\bar{f}(x)$ could factor as the square of a single monic linear polynomial. We will consider all three cases separately.

Suppose first that $\bar{f}(x)$ is irreducible in $\mathbb{F}_p[x]$. Then $\mathbb{F}_p[x]/(\bar{f}(x))$ is a field, so $\mathcal{O}_K/p\mathcal{O}_K$ is as well. $\mathfrak{p}\mathcal{O}_K$ is therefore a prime ideal of $\mathcal{O}_K$, by the definition of prime ideal, so it does not factor any further.

Before we do the next case, let us determine exactly what all of these maps are, since this will be important in determining the kernel. The sequence of maps is

$$\begin{tikzcd}
\mathcal{O}_K \arrow[r] \arrow[d, "\cong"] & \mathcal{O}_K/p\mathcal{O}_K \arrow[d, "\cong"] & \\
\mathbb{Z}[x]/(f(x)) \arrow[r] & \mathbb{Z}[x]/(p, f(x)) \arrow[r, "\cong"] & \mathbb{F}_p[x]/(\bar{f}(x))
\end{tikzcd}$$

Both of the horizontal maps of the square are the natural quotient maps, and the two vertical isomorphisms send α to x. The last horizontal isomorphism simply sends x to x. (All maps always send 1 to 1, of course, which determines what happens to all of $\mathbb{Z}$.) The ideal $p\mathcal{O}_K$ has now been expressed as the kernel of the map

$$\mathcal{O}_K \to \mathbb{F}_p[x]/(\bar{f}(x))$$

sending α to x.

Suppose now that $\bar{f}(x)$ factors as $\bar{g}(x)\bar{h}(x)$ in $\mathbb{F}_p[x]$, where $\bar{g}(x)$ and $\bar{h}(x)$ are distinct, monic, linear polynomials. Then the Chinese remainder theorem (see Exercise 3.5) gives an isomorphism

$$\mathbb{F}_p[x]/(\bar{f}(x)) \xrightarrow{\cong} \mathbb{F}_p[x]/(\bar{g}(x)) \times \mathbb{F}_p[x]/(\bar{h}(x))$$

sending x to (x, x). Note that both of these factors are fields since $\bar{g}(x)$ and $\bar{h}(x)$ are irreducible in $\mathbb{F}_p[x]$; in fact, they are both isomorphic to $\mathbb{F}_p$.

Consider now the composite map

$$\mathcal{O}_K \to \mathbb{F}_p[x]/(\bar{g}(x)) \times \mathbb{F}_p[x]/(\bar{h}(x))$$

sending α to (x, x), which still has kernel $p\mathcal{O}_K$. The kernel into the first factor is the ideal $\big(p, g(\alpha)\big)$ of $\mathcal{O}_K$ (since α maps to x in this factor), and the kernel into the second factor is $\big(p, h(\alpha)\big)$. Thus the kernel of the map (which by construction is just $p\mathcal{O}_K$) can also be written as

$$\big(p, g(\alpha)\big) \cap \big(p, h(\alpha)\big);$$

however, these ideals are easily seen to be relatively prime (see Exercise 3.3), so Exercise 3.4 shows that

$$\big(p, g(\alpha)\big) \cap \big(p, h(\alpha)\big) = \big(p, g(\alpha)\big)\big(p, h(\alpha)\big).$$

Furthermore, both of these ideals are prime, since as we saw above

$$\mathcal{O}_K/(p, g(\alpha)) \cong \mathbb{F}_p[x]/(\bar{g}(x)),\ \ \mathcal{O}_K/(p, h(\alpha)) \cong \mathbb{F}_p[x]/(\bar{h}(x))$$

are fields. Thus we have determined the prime factorization

$$p\mathcal{O}_K = \big(p, g(\alpha)\big)\big(p, h(\alpha)\big)$$

of $p\mathcal{O}_K$. (Note that it does not matter which lifts of $\bar{g}(x)$ and $\bar{h}(x)$ are chosen, since any two lifts differ by multiples of p and p lies in these ideals.)

The last case is the case where $\bar{f}(x) = \bar{g}(x)^2$ for some monic, linear polynomial $\bar{g}(x) \in \mathbb{F}_p[x]$. In this case the above analysis does not quite work since the Chinese remainder theorem does not apply. However, it suggests strongly that

$$p\mathcal{O}_K = \big(p, g(\alpha)\big)^2,$$

and this we can check directly. We check the case where $d \equiv 2, 3 \pmod 4$ and $p \neq 2$; the other cases are similar. We have that $\bar{f}(x) = x^2 - d$ is a square in $\mathbb{F}_p[x]$. One checks easily that this implies that p divides d (since $p \neq 2$), so we can take $g(x) = x$. Thus the claim is that

$$p\mathcal{O}_K = \big(p, \alpha\big)^2.$$

To check this, we simply compute

$$\big(p, \alpha\big)\big(p, \alpha\big) = \big(p^2, p\alpha, \alpha^2\big).$$

Since $\alpha^2 = d$ is divisible by p, every generator of the ideal is divisible by p. Furthermore, since d is squarefree, p^2 does not divide d; it follows that p is a linear combination of p^2 and d, so that p lies in the ideal. Thus the ideal is simply $p\mathcal{O}_K$ as claimed.

We summarize our results in a proposition.

Proposition 1.2. *Let $K = \mathbb{Q}(\sqrt{d})$ be a quadratic number field with d a squarefree integer and let*

$$f(x) = \begin{cases} x^2 - d & d \equiv 2, 3 \pmod 4; \\ x^2 - x + \frac{1-d}{4} & d \equiv 1 \pmod 4. \end{cases}$$

Let p be a rational prime and let

$$\bar{f}(x) = \bar{g}_1(x)^{e_1} \cdots \bar{g}_r(x)^{e_r}$$

be the factorization of $\bar{f}(x)$ in $\mathbb{F}_p[x]$. (Of course, we have $r = 1$ or 2 and $e_i = 1$ or 2.) Then the factorization of $p\mathcal{O}_K$ into primes of $\mathcal{O}_K$ is

$$p\mathcal{O}_K = \big(p, g_1(\alpha)\big)^{e_1} \cdots \big(p, g_r(\alpha)\big)^{e_r}.$$

We will say that $p\mathcal{O}_K$ is *inert* in K if it is a prime ideal in $\mathcal{O}_K$; that it *splits* in K if it is a product of distinct prime ideals in $\mathcal{O}_K$; and that it *ramifies* in K if it is the square of a prime ideal. Our above results show that $p\mathcal{O}_K$ is inert if and only if $f(x)$ is irreducible modulo p; it splits if and only if $f(x)$ factors into distinct linear factors; and it ramifies if and only if $f(x)$ is the square of a linear polynomial. Determination of the ramification in a number field turns out to be of great importance, and our above analysis yields the following result.

Corollary 1.3. *Let $K = \mathbb{Q}(\sqrt{d})$ be a quadratic number field with d a square-free integer. If $d \equiv 1 \pmod 4$, then a prime of $\mathbb{Z}$ is ramified in $\mathcal{O}_K$ if and only if it divides d. If $d \equiv 2, 3 \pmod 4$, then a prime of $\mathbb{Z}$ is ramified in $\mathcal{O}_K$ if and only if it is 2 or it divides d.*

Proof. First take $d \equiv 2, 3 \pmod 4$. Modulo 2 we have

$$x^2 - d \equiv (x - d)^2 \pmod 2,$$

so $p = 2$ is always ramified. It was shown above that otherwise ramification occurs if and only if p divides d, which completes the analysis in this case.

When $d \equiv 1 \pmod 4$, $x^2 - x + \frac{1-d}{4}$ is never a square modulo 2, since all squares have no linear term. Thus $p = 2$ never ramifies. The fact that all p dividing d do ramify follows from the determination of the roots of $x^2 - x + \frac{1-d}{4}$ by the quadratic formula; we leave the details to the reader. $\square$

Example 1.4. Let $K = \mathbb{Q}(\sqrt{-5})$ and $\mathcal{O}_K = \mathbb{Z}[\sqrt{-5}]$. Let us factor the first few primes. First take $p = 2$. Then

$$x^2 + 5 \equiv (x + 1)^2 \pmod 2,$$

so $2\mathcal{O}_K$ ramifies:

$$2\mathcal{O}_K = \big(2, \sqrt{-5} + 1\big)^2.$$

For $p = 3$, we have

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

so $3\mathcal{O}_K$ splits as

$$3\mathcal{O}_K = \big(3, \sqrt{-5} + 1\big)\big(3, \sqrt{-5} + 2\big).$$

(Note that these factorizations agree with those in Chapter 2, Section 1.4.) For $p = 5$,

$$x^2 + 5 \equiv x^2 \pmod 5,$$

so

$$5\mathcal{O}_K = \big(5, \sqrt{-5}\big)^2.$$

Note that the second ideal is just the principal ideal $\big(\sqrt{-5}\big)$, since $\sqrt{-5}$ divides 5 in $\mathbb{Z}[\sqrt{-5}]$. This illustrates the general fact that the above algorithm does not tell you whether or not the factors are principal ideals. Note also that $2\mathcal{O}_K$ and $5\mathcal{O}_K$ are the only primes which ramify in K, as we proved above that in this case that either $p = 2$ or p divides $d = -5$.

Continuing,

$$x^2 + 5 \equiv (x + 3)(x + 4) \pmod 7,$$

so

$$7\mathcal{O}_K = \big(7, \sqrt{-5}+3\big)\big(7, \sqrt{-5}+4\big).$$

Next, x^2+5 is irreducible in $\mathbb{F}_{11}[x]$, so $11\mathcal{O}_K$ is still a prime ideal in $\mathbb{Z}[\sqrt{-5}]$. For a final example, take $p = 29$. Then

$$x^2+5 = (x+13)(x+16) \pmod{29},$$

so

$$29\mathcal{O}_K = \big(29, \sqrt{-5}+13\big)\big(29, \sqrt{-5}+16\big).$$

In this case, however, we also find the element factorization

$$29 = (3-2\sqrt{-5})(3+2\sqrt{-5}).$$

One can show with a little calculation that

$$\big(29, \sqrt{-5}+13\big) = \big(3-2\sqrt{-5}\big)$$

$$\big(29, \sqrt{-5}+16\big) = \big(3+2\sqrt{-5}\big),$$

so we actually have the ideal factorization

$$\big(29\big) = \big(3-2\sqrt{-5}\big)\big(3+2\sqrt{-5}\big)$$

of $\big(29\big)$ into principal ideals.

1.2. Quadratic forms. There are many deep and important connections between quadratic forms and the splitting of primes in quadratic fields. In this section we investigate some of the simplest; for more information on this subject, see [**7**].

We begin by refining our results of the previous section. Let $K = \mathbb{Q}(\sqrt{d})$ and let p be a a rational prime. Recall that the behavior of the prime ideal $p\mathcal{O}_K$ was determined by the factorization of a certain polynomial in $\mathbb{F}_p[x]$. The various behaviors of $p\mathcal{O}_K$ are captured well by the Legendre symbol.

Definition 1.5. Let p be an odd prime. We define the *Legendre symbol*

$$\left(\frac{\cdot}{p}\right) : \mathbb{Z}/p\mathbb{Z} \to \{0, \pm 1\}$$

by

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{if } a \text{ is a non-zero square modulo } p; \\ 0 & \text{if } a \equiv 0 \pmod{p}; \\ -1 & \text{if } a \text{ is not a square modulo } p. \end{cases}$$

By abuse of notation we use the same symbol for $a \in \mathbb{Z}$.

The fundamental properties of the Legendre symbol are in Exercise 3.9 and Exercise 3.10. It is possible to extend the definition of the Legendre symbol to include the case $p = 2$, but we will not do so here.

Proposition 1.6. *Let $K = \mathbb{Q}(\sqrt{d})$ be a quadratic number field and let p be an odd rational prime. Then the prime ideal $p\mathcal{O}_K$ splits in K if and only if $\left(\frac{d}{p}\right) = 1$; it ramifies in K if and only if $\left(\frac{d}{p}\right) = 0$; and it is inert in K if and only if $\left(\frac{d}{p}\right) = -1$.*

Proof. First suppose that $d \equiv 2, 3 \pmod 4$. Then the behavior of $p\mathcal{O}_K$ is determined by the factorization of the polynomial $x^2 - d$ in $\mathbb{F}_p[x]$. If $d \equiv 0 \pmod p$, then this polynomial has the repeated factor x, so $p\mathcal{O}_K$ ramifies; if d is a non-zero square modulo p, then it splits into distinct linear factors, so $p\mathcal{O}_K$ splits; and if d is not a square modulo p, then it does not factor, so $p\mathcal{O}_K$ is inert. This is precisely the statement of the proposition in this case.

Now take $d \equiv 1 \pmod 4$. This time the behavior is determined by the factorization of the polynomial $x^2 - x + \frac{1-d}{4}$ in $\mathbb{F}_p[x]$. By the quadratic formula (which applies since $p \neq 2$), this polynomial has roots

$$\frac{1 \pm \sqrt{d}}{2},$$

from which the same analysis as above proves the proposition. $\square$

We now turn to quadratic forms. Recall that in the cases of $\mathbb{Q}(i)$,$\mathbb{Q}(\sqrt{-2})$ and $\mathbb{Q}(\zeta_3) = \mathbb{Q}(\sqrt{-3})$ the natural quadratic form to study were the "norm forms" $x^2 + y^2$, $x^2 + 2y^2$ and $x^2 - xy + y^2$. If $d \equiv 2, 3 \pmod 4$, then the appropriate quadratic form is

$$\mathrm{N}_{K/\mathbb{Q}}(x + y\sqrt{d}) = x^2 - dy^2,$$

while if $d \equiv 1 \pmod 4$, then it is

$$\mathrm{N}_{K/\mathbb{Q}}\left(x + y\frac{1+\sqrt{d}}{2}\right) = x^2 + xy + \frac{1-d}{4}y^2.$$

(We get a different quadratic form for $\mathbb{Q}(\sqrt{-3})$ here because we are using a different generator of the field; we nevertheless will obtain an equivalent result.) Write $q_K(x, y)$ for the quadratic form attached to K. Then an integer n can be written as $q_K(x, y)$ if and only if n is the norm of some element of $\mathcal{O}_K$.

Note in particular that we can not at the moment study "natural" quadratic forms like x^2+3y^2; the correct quadratic form for $\mathbb{Q}(\sqrt{-3})$ is x^2+xy+y^2. To study other quadratic forms one must work in certain subrings of $\mathcal{O}_K$, where factorization is more complicated; we won't go into it here.

The basic result is the following.

Proposition 1.7. *Let $K = \mathbb{Q}(\sqrt{d})$ be a quadratic number field and let $q_K(x, y)$ be its norm quadratic form. Let p be a positive rational prime number. Then (at least) one of $\pm p$ is of the form $q_K(x_0, y_0)$ for some $x_0, y_0 \in \mathbb{Z}$ if and only if p splits (or ramifies) in K into principal ideals. If $d < 0$, then it is always p which is of this form, and never $-p$.*

Proof. Suppose first that p factors into principal ideals in $\mathcal{O}_K$, say $p\mathcal{O}_K = (\pi)(\pi')$. Then $\pi\pi'$ is an associate of p, say $\pi\pi' = up$ for some unit u. Thus

$$\mathrm{N}(\pi)\,\mathrm{N}(\pi') = \mathrm{N}(u)\,\mathrm{N}(p) = \pm p^2$$

by Lemma II.1.9. It follows that $\mathrm{N}(\pi) = \pm\,\mathrm{N}(\pi') = \pm p$, which gives the desired expression for p.

Now suppose that $\pm p$ is of the form $q_K(x_0, y_0)$ for some $x_0, y_0 \in \mathbb{Z}$. By the definition of $q_K(x, y)$,

$$\pm p = \mathrm{N}_{K/\mathbb{Q}}(x_0 + y_0\alpha),$$

where α is $\sqrt{d}$ or $\frac{1+\sqrt{d}}{2}$, as appropriate. This implies that

$$p\mathcal{O}_K = \bigl(x_0 + y_0\alpha\bigr)\bigl(x_0 + y_0\bar{\alpha}\bigr),$$

where $\bar{\alpha}$ is the conjugate of α. Furthermore, each of these ideals is easily seen to be prime. Thus $p\mathcal{O}_K$ splits (or possibly ramifies) into principal ideals. The fact that p must be positive for $d < 0$ follows immediately from the fact that $q_K(x, y)$ is positive definite in that case. □

COROLLARY 1.8. *With the above notation,* $\pm p = q_K(x_0, y_0)$ *for some* $x_0, y_0 \in \mathbb{Z}$ *only if* $\left(\frac{d}{p}\right) = 0$ *or* 1*. The converse is also true if* $\mathcal{O}_K$ *is a PID.*

In non-PID cases our answer is still far from complete. We will return to this question and give some surprising results in the next chapter.

2. Abstract factorization of primes

2.1. Factorization of rational primes. Before we extend the methods of Section 1 to more general number fields, it will be useful to give the abstract factorization results. We begin with the factorization of rational primes in number fields. Let K be a number field of degree n. If $\mathfrak{p}$ is a prime ideal of $\mathcal{O}_K$ and p is a rational prime, we say that $\mathfrak{p}$ *lies above* p if $\mathfrak{p} \cap \mathbb{Z} = p\mathbb{Z}$. It is clear from Lemma 1.1 that every non-zero prime of $\mathcal{O}_K$ lies above a unique prime of $\mathbb{Z}$, and it follows from Lemma II.3.8 that the primes of $\mathcal{O}_K$ lying above p are precisely those ideals occurring in the prime factorization of $p\mathcal{O}_K$.

Let $\mathfrak{p}$ be a prime of $\mathcal{O}_K$ lying over $p \in \mathbb{Z}$. Let e be the exact power of $\mathfrak{p}$ dividing $p\mathcal{O}_K$. We call e the *ramification index* of $\mathfrak{p}/p$ and write it as $e(\mathfrak{p}/p)$. The factorization of $p\mathcal{O}_K$ is thus

$$p\mathcal{O}_K = \prod_{\mathfrak{p}\cap\mathbb{Z}=p\mathbb{Z}} \mathfrak{p}^{e(\mathfrak{p}/p)}.$$

We will also need a way to measure the relative "sizes" of ideals. The most natural way to do this is to consider the residue field $\mathcal{O}_K/\mathfrak{p}$, which we proved earlier is a finite field. Since it clearly has characteristic p, it must have order p^f for some f. We define the *inertial degree* $f(\mathfrak{p}/p)$ of $\mathfrak{p}/p$ to be this integer f.

EXAMPLE 2.1. Take $K = \mathbb{Q}(\sqrt{-5})$. Our calculations in Example 1.4 yield the following values for e and f:

$$\begin{array}{lcllcl}
e\bigl((2,\sqrt{-5}+1)/2\bigr) & = & 2 & \qquad f\bigl((2,\sqrt{-5}+1)/2\bigr) & = & 1\\
e\bigl((3,\sqrt{-5}+1)/3\bigr) & = & 1 & \qquad f\bigl((3,\sqrt{-5}+1)/3\bigr) & = & 1\\
e\bigl((3,\sqrt{-5}+2)/3\bigr) & = & 1 & \qquad f\bigl((3,\sqrt{-5}+2)/3\bigr) & = & 1\\
e\bigl((5,\sqrt{-5})/5\bigr) & = & 2 & \qquad f\bigl((5,\sqrt{-5})/5\bigr) & = & 1\\
e\bigl((7,\sqrt{-5}+3)/7\bigr) & = & 1 & \qquad f\bigl((7,\sqrt{-5}+4)/7\bigr) & = & 1\\
e\bigl((11)/11\bigr) & = & 1 & \qquad f\bigl((11)/11\bigr) & = & 2
\end{array}$$

The values of f can be computed using expressions for quotients of $\mathbb{F}_p[x]$; for example,

$$\mathcal{O}_K/\bigl(3,\sqrt{-5}+1\bigr) \cong \mathbb{F}_3[x]/\bigl(x+1\bigr) \cong \mathbb{F}_3.$$

It is useful to have a notion of the size of an ideal for non-prime ideals. Since in this case we can no longer isolate a specific rational prime of interest, we define the *norm* $\mathrm{N}'_{K/\mathbb{Q}}(\mathfrak{a})$ of an ideal $\mathfrak{a}$ to be the size of the quotient ring $\mathcal{O}_K/\mathfrak{a}$; that this is finite follows easily from Lemma II.3.2 and Theorem II.2.22. (We will prove later that the ideal norm agrees with the absolute value of the usual element norm in the case that $\mathfrak{a}$ is a principal ideal; hopefully this notation should cause no confusion until then.) It follows immediately from the definition of inertial degree that if $\mathfrak{p}$ is a prime of $\mathcal{O}_K$ such that $\mathfrak{p} \cap \mathbb{Z} = p\mathbb{Z}$, then

$$\mathrm{N}'_{K/\mathbb{Q}}(\mathfrak{p}) = p^{f(\mathfrak{p}/p)}.$$

A first indication that the ideal norm behaves like the usual norm is given by the following lemma.

LEMMA 2.2. *The ideal norm is multiplicative; that is,*

$$\mathrm{N}'_{K/\mathbb{Q}}(\mathfrak{a}\mathfrak{b}) = \mathrm{N}'_{K/\mathbb{Q}}(\mathfrak{a})\,\mathrm{N}'_{K/\mathbb{Q}}(\mathfrak{b})$$

for any non-zero ideals $\mathfrak{a}, \mathfrak{b}$ *of* $\mathcal{O}_K$.

PROOF. Suppose first that $\mathfrak{a}$ and $\mathfrak{b}$ are relatively prime. Then by the Chinese remainder theorem (see Exercise 3.5) we have

$$\mathcal{O}_K/\mathfrak{a}\mathfrak{b} \cong \mathcal{O}_K/\mathfrak{a} \times \mathcal{O}_K/\mathfrak{b},$$

from which the lemma follows immediately. It will therefore be enough to prove that for any prime $\mathfrak{p}$ of $\mathcal{O}_K$ we have

$$\mathrm{N}'_{K/\mathbb{Q}}(\mathfrak{p}^m) = \mathrm{N}'_{K/\mathbb{Q}}(\mathfrak{p})^m;$$

the lemma will then follow from unique factorization of ideals and the relatively prime case.

Note that it is immediate from elementary group theory that

$$\mathrm{N}'_{K/\mathbb{Q}}(\mathfrak{p}^m) = \#(\mathcal{O}_K/\mathfrak{p}^m) = \#(\mathcal{O}_K/\mathfrak{p}) \cdot \#(\mathfrak{p}/\mathfrak{p}^2) \cdot \#(\mathfrak{p}^2/\mathfrak{p}^3) \cdots \#(\mathfrak{p}^{m-1}/\mathfrak{p}^m).$$

(All quotients here are simply as abelian groups.) Thus it will suffice to show that

$$\#(\mathfrak{p}^k/\mathfrak{p}^{k+1}) = \#(\mathcal{O}_K/\mathfrak{p})$$

for any k. To do this let γ be any element of $\mathfrak{p}^k$ which does not lie in $\mathfrak{p}^{k+1}$; such a γ must exist since if the containment $\mathfrak{p}^k \supseteq \mathfrak{p}^{k+1}$ were an equality it would violate unique factorization of ideals. We claim that the map

$$\begin{aligned} \mathcal{O}_K/\mathfrak{p} &\longrightarrow \mathfrak{p}^k/\mathfrak{p}^{k+1} \\ \alpha &\longmapsto \gamma\alpha \end{aligned}$$

is an isomorphism; we leave the details to the reader. □

We can now give the fundamental relationship between the numbers $e(\mathfrak{p}/p)$, $f(\mathfrak{p}/p)$ and the degree n of $K/\mathbb{Q}$.

PROPOSITION 2.3. *Let* K *be a number field of degree* n *and let* p *be a rational prime. Let*

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

be the factorization of $p\mathcal{O}_K$ *into primes of* $\mathcal{O}_K$. *(Thus* $e_i = e(\mathfrak{p}_i/p)$.*) Set* $f_i = f(\mathfrak{p}_i/p)$. *Then*

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

PROOF. Both $p\mathcal{O}_K$ and $\mathfrak{p}_1^{e_1}\cdots\mathfrak{p}_r^{e_r}$ have the same norm, so by Lemma 2.2

$$\begin{aligned}\mathrm{N}'_{K/\mathbb{Q}}(p\mathcal{O}_K) &= \mathrm{N}'_{K/\mathbb{Q}}(\mathfrak{p}_1)^{e_1}\cdots\mathrm{N}'_{K/\mathbb{Q}}(\mathfrak{p}_r)^{e_r}\\ &= p^{f_1e_1}\cdots p^{f_re_r}\\ &= p^{f_1e_1+\cdots+f_re_r}.\end{aligned}$$

On the other hand, we know that $\mathcal{O}_K/p\mathcal{O}_K$ has p^n elements, since $\mathcal{O}_K$ is a free $\mathbb{Z}$-module of rank n. Thus $\mathrm{N}'_{K/\mathbb{Q}}(p\mathcal{O}_K) = p^n$ and the proposition follows immediately. $\square$

EXAMPLE 2.4. Let K be a quadratic number field and let p be a rational prime. We saw that there were three possibilities for the factorization of p: first of all, $p\mathcal{O}_K$ could still be prime, in which case $f(p\mathcal{O}_K/p) = 2$ and $e(p\mathcal{O}_K/p) = 1$. Next, $p\mathcal{O}_K$ could factor as $\mathfrak{p}_1\mathfrak{p}_2$ where $f(\mathfrak{p}_1/p) = f(\mathfrak{p}_2/p) = 1$ and $e(\mathfrak{p}_1/p) = e(\mathfrak{p}_2/p) = 1$. Lastly, $p\mathcal{O}_K$ could ramify as $\mathfrak{p}^2$, in which case $f(\mathfrak{p}/p) = 1$ and $e(\mathfrak{p}/p) = 2$. In all three cases we do indeed have the equality of Proposition 2.3.

2.2. Localizations of integer rings. Before we extend the above results to the case of relative extensions we will need to introduce an additional piece of machinery. Very often in algebraic number theory it is convenient to work "one prime at a time". More precisely, given a number field K with ring of integers $\mathcal{O}_K$ and given a prime $\mathfrak{p}$, we would like to find a larger subring of K in which the only non-zero prime ideal is $\mathfrak{p}$. We will construct such a ring in this section.

The definition of the ring is actually fairly simple. We define the *local ring of* $\mathcal{O}_K$ *at* $\mathfrak{p}$ to be the ring

$$\mathcal{O}_{K,\mathfrak{p}} = \left\{\frac{\alpha}{\beta} \in K \mid \alpha \in \mathcal{O}_K, \beta \in \mathcal{O}_K - \mathfrak{p}\right\}.$$

That is, $\mathcal{O}_{K,\mathfrak{p}}$ consists of all elements of K which can be written as ratios of integers with the denominator not in $\mathfrak{p}$. (The terminology here is influenced by algebraic geometry. In fact, in a suitably general setting one can think of a ring of integers $\mathcal{O}_K$ as a curve, where the points are the non-zero prime ideals. In this setting the ring $\mathcal{O}_{K,\mathfrak{p}}$ really is the ring of regular functions on the curve $\mathcal{O}_K$ at the point $\mathfrak{p}$.) One can check easily that $\mathcal{O}_{K,\mathfrak{p}}$ is actually a ring.

EXAMPLE 2.5. Let $K = \mathbb{Q}$. Then the local ring $\mathbb{Z}_{(p)}$ is simply the subring of $\mathbb{Q}$ of rational numbers with denominator relatively prime to p. (We considered such rings in Chapter 2, Section 1.) Note that this ring $\mathbb{Z}_{(p)}$ is not the ring $\mathbb{Z}_p$ of p-adic integers; to get $\mathbb{Z}_p$ one must *complete* $\mathbb{Z}_{(p)}$, which is a process which we will not go into here.

The usefulness of $\mathcal{O}_{K,\mathfrak{p}}$ comes from the fact that it has a particularly simple ideal structure. Let $\mathfrak{a}$ be any proper ideal of $\mathcal{O}_{K,\mathfrak{p}}$ and consider the ideal $\mathfrak{a}\cap\mathcal{O}_K$ of $\mathcal{O}_K$. We claim that

$$\mathfrak{a} = (\mathfrak{a}\cap\mathcal{O}_K)\mathcal{O}_{K,\mathfrak{p}};$$

that is, that $\mathfrak{a}$ is generated by the elements of $\mathfrak{a}$ in $\mathfrak{a}\cap\mathcal{O}_K$. It is clear from the definition of an ideal that $\mathfrak{a} \supseteq (\mathfrak{a}\cap\mathcal{O}_K)\mathcal{O}_{K,\mathfrak{p}}$. To prove the other inclusion, let α be any element of $\mathfrak{a}$. Then we can write $\alpha = \beta/\gamma$ where $\beta \in \mathcal{O}_K$ and $\gamma \notin \mathfrak{p}$. In particular, $\beta \in \mathfrak{a}$ (since $\beta/\gamma \in \mathfrak{a}$ and $\mathfrak{a}$ is an ideal), so $\beta \in \mathfrak{a}\cap\mathcal{O}_K$. Since $1/\gamma \in \mathcal{O}_{K,\mathfrak{p}}$, this implies that $\alpha = \beta/\gamma \in (\mathfrak{a}\cap\mathcal{O}_K)\mathcal{O}_{K,\mathfrak{p}}$, as claimed.

We can use this fact to determine all of the ideals of $\mathcal{O}_{K,\mathfrak{p}}$. Let $\mathfrak{a}$ be any ideal of $\mathcal{O}_{K,\mathfrak{p}}$ and consider the ideal factorization of $\mathfrak{a} \cap \mathcal{O}_K$ in $\mathcal{O}_K$. Write it as

$$\mathfrak{a} \cap \mathcal{O}_K = \mathfrak{p}^n \mathfrak{b}$$

for some n and some ideal $\mathfrak{b}$, relatively prime to $\mathfrak{p}$. We claim first that $\mathfrak{b}\mathcal{O}_{K,\mathfrak{p}} = \mathcal{O}_{K,\mathfrak{p}}$. To see this, note that $\mathfrak{b}$ is not contained in $\mathfrak{p}$ since $\mathfrak{b}$ is assumed to be relatively prime to $\mathfrak{p}$, and thus is not divisible by it. In particular, $\mathfrak{b}$ contains elements of $\mathcal{O}_K - \mathfrak{p}$; these are units in $\mathcal{O}_{K,\mathfrak{p}}$, so $\mathfrak{b}\mathcal{O}_{K,\mathfrak{p}} = \mathcal{O}_{K,\mathfrak{p}}$.

We now find that

$$\mathfrak{a} = (\mathfrak{a} \cap \mathcal{O}_K)\mathcal{O}_{K,\mathfrak{p}} = \mathfrak{p}^n \mathfrak{b}\mathcal{O}_{K,\mathfrak{p}} = \mathfrak{p}^n \mathcal{O}_{K,\mathfrak{p}}$$

since $\mathfrak{b}\mathcal{O}_{K,\mathfrak{p}} = \mathcal{O}_{K,\mathfrak{p}}$. Thus every ideal of $\mathcal{O}_{K,\mathfrak{p}}$ has the form $\mathfrak{p}^n\mathcal{O}_{K,\mathfrak{p}}$ for some n; it follows immediately that $\mathcal{O}_{K,\mathfrak{p}}$ is noetherian.

It is also now clear that $\mathfrak{p}\mathcal{O}_{K,\mathfrak{p}}$ is the unique non-zero prime ideal in $\mathcal{O}_{K,\mathfrak{p}}$. Furthermore, the inclusion $\mathcal{O}_K \hookrightarrow \mathcal{O}_{K,\mathfrak{p}}$ induces an injection

$$\mathcal{O}_K/\mathfrak{p} \hookrightarrow \mathcal{O}_{K,\mathfrak{p}}/\mathfrak{p}\mathcal{O}_{K,\mathfrak{p}}$$

since $\mathfrak{p}\mathcal{O}_{K,\mathfrak{p}} \cap \mathcal{O}_K = \mathfrak{p}$, as the reader can easily check. This map is also a surjection, since the residue class of $\alpha/\beta \in \mathcal{O}_{K,\mathfrak{p}}$ (with $\alpha \in \mathcal{O}_K$ and $\beta \notin \mathfrak{p}$) is the image of $\alpha\beta^{-1}$ in $\mathcal{O}_K/\mathfrak{p}$, which makes sense since β is invertible in $\mathcal{O}_K/\mathfrak{p}$. Thus the map is an isomorphism. In particular, it is now abundantly clear that every non-zero prime ideal of $\mathcal{O}_{K,\mathfrak{p}}$ is maximal.

To show that $\mathcal{O}_{K,\mathfrak{p}}$ is a Dedekind domain, it remains to show that it is integrally closed in K. So let $\gamma \in K$ be a root of a polynomial with coefficients in $\mathcal{O}_{K,\mathfrak{p}}$; write this polynomial as

$$x^m + \frac{\alpha_{m-1}}{\beta_{m-1}}x^{m-1} + \cdots + \frac{\alpha_0}{\beta_0}$$

with $\alpha_i \in \mathcal{O}_K$ and $\beta_i \in \mathcal{O}_K - \mathfrak{p}$. Set $\beta = \beta_0\beta_1 \cdots \beta_{m-1}$. Multiplying by β^m we find that $\beta\gamma$ is the root of a monic polynomial with coefficients in $\mathcal{O}_K$. Thus $\beta\gamma \in \mathcal{O}_K$; since $\beta \notin \mathfrak{p}$, we have $\beta\gamma/\beta = \gamma \in \mathcal{O}_{K,\mathfrak{p}}$ Thus $\mathcal{O}_{K,\mathfrak{p}}$ is integrally closed in K.

Let us summarize our results in a proposition.

PROPOSITION 2.6. *Let K be a number field and let $\mathfrak{p}$ be a non-zero prime of $\mathcal{O}_K$. Then $\mathcal{O}_{K,\mathfrak{p}}$ is a Dedekind domain and every ideal of $\mathcal{O}_{K,\mathfrak{p}}$ has the form $\mathfrak{p}^n\mathcal{O}_{K,\mathfrak{p}}$ for some $n \geq 0$. In particular, $\mathfrak{p}\mathcal{O}_{K,\mathfrak{p}}$ is the only prime ideal of $\mathcal{O}_{K,\mathfrak{p}}$.*

We have now shown that $\mathcal{O}_{K,\mathfrak{p}}$ is a Dedekind domain with a unique non-zero prime ideal. Such a ring is called a *discrete valuation ring* or a *DVR*. These rings will be useful to us for the following reason.

PROPOSITION 2.7. *Let R be a discrete valuation ring. Then R is a principal ideal domain.*

PROOF. Let $\mathfrak{p}$ be the unique non-zero prime ideal of R. By unique factorization of ideals, every ideal of R has the form $\mathfrak{p}^n$ for some n; thus it will suffice to show that $\mathfrak{p}$ itself is principal. Let π be any element in $\mathfrak{p}$ but not in $\mathfrak{p}^2$. By unique factorization of ideals, we have $\pi R = \mathfrak{p}^n$ for some $n \geq 1$. But we can not have $n \geq 2$, since then π would lie in $\mathfrak{p}^2$. Thus $\pi R = \mathfrak{p}$, so $\mathfrak{p}$ is indeed principal. $\square$

A generator of the unique non-zero prime ideal of a DVR R is called a *uniformizer*. R has a particularly simple sort of unique factorization: every $\alpha \in R$ can be written as $u\pi^n$, where $u \in R^*$ and $n \geq 0$.

The usefulness of $\mathcal{O}_{K,\mathfrak{p}}$ comes from the fact that it has all of the information about the prime $\mathfrak{p}$, but it has no other prime ideals to clutter things up. This makes $\mathcal{O}_{K,\mathfrak{p}}$ much simpler than $\mathcal{O}_K$, but also still useful for studying the prime $\mathfrak{p}$.

EXAMPLE 2.8. Let p be a rational prime and consider the ring $\mathbb{Z}_{(p)}$. The units of this ring are

$$\mathbb{Z}_{(p)}^* = \left\{ \frac{m}{n} \mid (m,p) = (n,p) = 1 \right\}.$$

The unique prime ideal of $\mathbb{Z}_{(p)}$ is $\big(p\big)$, and every $\alpha \in \mathbb{Z}_{(p)}$ can be written uniquely as

$$\alpha = up^n$$

where $u \in \mathbb{Z}_{(p)}^*$ and $n \geq 0$.

Now let L/K be an extension of number fields of degree n. Let $\mathfrak{p}$ be a prime ideal of $\mathcal{O}_K$; denote by $\mathcal{O}_{L,\mathfrak{p}}$ the ring

$$\left\{ \frac{\alpha}{\beta} \in L \mid \alpha \in \mathcal{O}_L, \beta \in \mathcal{O}_K - \mathfrak{p} \right\}.$$

$\mathcal{O}_{L,\mathfrak{p}}$ is not quite a discrete valuation ring, since we allow only denominators in $\mathcal{O}_K - \mathfrak{p}$, but it will suffice for our purposes. We will need to know two key facts about $\mathcal{O}_{L,\mathfrak{p}}$. First of all, note that $\mathfrak{p}\mathcal{O}_{L,\mathfrak{p}} \cap \mathcal{O}_L = \mathfrak{p}\mathcal{O}_L$. Thus the natural inclusion $\mathcal{O}_L \hookrightarrow \mathcal{O}_{L,\mathfrak{p}}$ induces an injection

$$\mathcal{O}_L/\mathfrak{p}\mathcal{O}_L \hookrightarrow \mathcal{O}_{L,\mathfrak{p}}/\mathfrak{p}\mathcal{O}_{L,\mathfrak{p}}.$$

We claim that this map is an isomorphism. So let α/β represent a residue class in the range, where $\alpha \in \mathcal{O}_L$ and $\beta \in \mathcal{O}_K - \mathfrak{p}$. We know that $\mathcal{O}_K/\mathfrak{p}$ injects into $\mathcal{O}_L/\mathfrak{p}\mathcal{O}_L$; thus β is invertible in $\mathcal{O}_L/\mathfrak{p}\mathcal{O}_L$. It follows that the element $\alpha\beta^{-1}$ is well-defined in $\mathcal{O}_L/\mathfrak{p}\mathcal{O}_L$, and it maps to α/β. Thus the map is surjective, and therefore an isomorphism.

The second fact we need is that $\mathcal{O}_{L,\mathfrak{p}}$ is a free $\mathcal{O}_{K,\mathfrak{p}}$-module of rank n. The proof of this fact is exactly the same as the proof that $\mathcal{O}_L$ is a free $\mathcal{O}_K$-module of rank n. One begins with a basis $\alpha_1, \ldots, \alpha_n$ for L/K with each $\alpha_i \in \mathcal{O}_{L,\mathfrak{p}}$. Next, the discriminant $\Delta = \Delta(\alpha_1, \ldots, \alpha_n)$ lies in $\mathcal{O}_{K,\mathfrak{p}}$ (using Lemma II.2.18). The same proof as in Proposition II.2.21 shows that

$$\mathcal{O}_{L,\mathfrak{p}} \subseteq \frac{1}{\Delta}(\mathcal{O}_{K,\mathfrak{p}}\alpha_1 + \cdots + \mathcal{O}_{K,\mathfrak{p}}\alpha_n),$$

and we obviously have

$$\mathcal{O}_{K,\mathfrak{p}}\alpha_1 + \cdots + \mathcal{O}_{K,\mathfrak{p}}\alpha_n \subseteq \mathcal{O}_{L,\mathfrak{p}}.$$

Since $\mathcal{O}_{K,\mathfrak{p}}$ is a PID, these two facts combine to show that $\mathcal{O}_{L,\mathfrak{p}}$ is a free $\mathcal{O}_{K,\mathfrak{p}}$-module of rank n. (See Appendix C, Section 5.)

The fact we actually need from all of this is contained in the next proposition.

PROPOSITION 2.9. *Let L/K be an extension of number fields of degree n and let $\mathfrak{p}$ be a non-zero prime of $\mathcal{O}_K$. Then*

$$\#(\mathcal{O}_L/\mathfrak{p}\mathcal{O}_L) = \big(\#(\mathcal{O}_K/\mathfrak{p}\mathcal{O}_K)\big)^n.$$

PROOF. We saw above that $\mathcal{O}_{L,\mathfrak{p}}$ is a free $\mathcal{O}_{K,\mathfrak{p}}$-module of rank n. Thus $\mathcal{O}_{L,\mathfrak{p}}/\mathfrak{p}\mathcal{O}_{L,\mathfrak{p}}$ is a free $\mathcal{O}_{K,\mathfrak{p}}/\mathfrak{p}\mathcal{O}_{K,\mathfrak{p}}$-module of rank n as well. Therefore

$$\#(\mathcal{O}_{L,\mathfrak{p}}/\mathfrak{p}\mathcal{O}_{L,\mathfrak{p}}) = \#(\mathcal{O}_{K,\mathfrak{p}}/\mathfrak{p}\mathcal{O}_{K,\mathfrak{p}})^n.$$

But these residue rings are isomorphic to $\mathcal{O}_L/\mathfrak{p}\mathcal{O}_L$ and $\mathcal{O}_K/\mathfrak{p}\mathcal{O}_K$ respectively, so the proposition follows. □

COROLLARY 2.10. *Let L/K be an extension of number fields of degree n and let $\mathfrak{a}$ be a nonzero ideal of $\mathcal{O}_K$. Then*

$$\mathrm{N}'_{L/\mathbb{Q}}(\mathfrak{a}\mathcal{O}_L) = \mathrm{N}'_{K/\mathbb{Q}}(\mathfrak{a})^n.$$

PROOF. Since each side of the desired equality is multiplicative in $\mathfrak{a}$, it will suffice to prove the result in the case that $\mathfrak{a} = \mathfrak{p}$ is a prime of $\mathcal{O}_K$. In this case the corollary is precisely Proposition 2.9. □

COROLLARY 2.11. *Let K be a number field of degree n and let α be in $\mathcal{O}_K$. Then*

$$\mathrm{N}'_{K/\mathbb{Q}}(\alpha\mathcal{O}_K) = |\,\mathrm{N}_{K/\mathbb{Q}}(\alpha)|.$$

PROOF. We assume a bit more Galois theory than usual for this proof. Assume first that $K/\mathbb{Q}$ is Galois. Let σ be an element of $\mathrm{Gal}(K/\mathbb{Q})$. It is clear that $\sigma(\mathcal{O}_K)/\sigma(\alpha) \cong \mathcal{O}_K/\alpha$; since $\sigma(\mathcal{O}_K) = \mathcal{O}_K$, this shows that

$$\mathrm{N}'_{K/\mathbb{Q}}(\sigma(\alpha)\mathcal{O}_K) = \mathrm{N}'_{K/\mathbb{Q}}(\alpha\mathcal{O}_K).$$

Taking the product over all $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$, we have

$$\mathrm{N}'_{K/\mathbb{Q}}(\mathrm{N}_{K/\mathbb{Q}}(\alpha)\mathcal{O}_K) = \mathrm{N}'_{K/\mathbb{Q}}(\alpha\mathcal{O}_K)^n.$$

Since $\mathrm{N}_{K/\mathbb{Q}}(\alpha)$ is a rational integer and $\mathcal{O}_K$ is a free $\mathbb{Z}$-module of rank n,

$$\mathcal{O}_K/\,\mathrm{N}_{K/\mathbb{Q}}(\alpha)\mathcal{O}_K$$

will have order $\mathrm{N}_{K/\mathbb{Q}}(\alpha)^n$; therefore

$$\mathrm{N}'_{K/\mathbb{Q}}(\mathrm{N}_{K/\mathbb{Q}}(\alpha)\mathcal{O}_K) = \mathrm{N}_{K/\mathbb{Q}}(\alpha)^n,$$

which completes the proof.

In the general case, let L be the Galois closure of K and set $[L:K] = m$. The above argument shows that

$$\mathrm{N}'_{L/\mathbb{Q}}(\alpha\mathcal{O}_L) = \mathrm{N}_{L/\mathbb{Q}}(\alpha).$$

By Corollary 2.10 the first term is equal to $\mathrm{N}'_{K/\mathbb{Q}}(\alpha\mathcal{O}_K)^m$, and it is easy to see that the second term is just $\mathrm{N}_{K/\mathbb{Q}}(\alpha)^m$. This establishes the corollary. □

From now on we will often write $\mathrm{N}_{K/\mathbb{Q}}$ for both the ideal norm and the element norm; no confusion should result.

2.3. Relative factorizations. We now extend our earlier factorization results to arbitrary extensions of number fields. Let L/K be an extension of number fields of degree n. We first need to extend the notion of a prime of $\mathcal{O}_L$ lying over a prime of $\mathcal{O}_K$.

LEMMA 2.12. *Let $\mathfrak{p}$ a non-zero prime of $\mathcal{O}_K$ and let $\mathfrak{P}$ be a non-zero prime of $\mathcal{O}_L$. The following five conditions are equivalent.*

(1) $\mathfrak{P}$ *divides* $\mathfrak{p}\mathcal{O}_L$;
(2) $\mathfrak{P} \supseteq \mathfrak{p}\mathcal{O}_L$;
(3) $\mathfrak{P} \supseteq \mathfrak{p}$;
(4) $\mathfrak{P} \cap \mathcal{O}_K = \mathfrak{p}$;
(5) $\mathfrak{P} \cap K = \mathfrak{p}$.

Furthermore, if any of the above are satisfied, then $\mathfrak{p} \cap \mathbb{Z} = \mathfrak{P} \cap \mathbb{Z}$.

PROOF. See Exercise 3.7. □

If $\mathfrak{p}$ and $\mathfrak{P}$ satisfy any of the equivalent conditions of Lemma 2.12, we say that $\mathfrak{P}$ *lies over* $\mathfrak{p}$ and that $\mathfrak{p}$ *lies under* $\mathfrak{P}$. Exercise 3.8 shows that every prime of $\mathcal{O}_L$ lies over a unique prime of $\mathcal{O}_K$, and that every prime of $\mathcal{O}_K$ lies under at least one prime of $\mathcal{O}_L$. Note also that by Lemma II.3.8 the primes lying over $\mathfrak{p}$ are precisely the primes occurring in the ideal factorization of $\mathfrak{p}\mathcal{O}_L$.

Now, let $\mathfrak{p}$ and $\mathfrak{P}$ be as above and suppose that $\mathfrak{P}$ lies over $\mathfrak{p}$. We denote by $e(\mathfrak{P}/\mathfrak{p})$ the exact power of $\mathfrak{P}$ dividing $\mathfrak{p}\mathcal{O}_L$; it is called the *ramification index* of $\mathfrak{P}/\mathfrak{p}$. Thus we can write

$$\mathfrak{p}\mathcal{O}_L = \prod_{\mathfrak{P}\cap\mathcal{O}_K=\mathfrak{p}} \mathfrak{P}^{e(\mathfrak{P}/\mathfrak{p})}.$$

Next, let p be the unique positive rational prime contained in $\mathfrak{p}$ and $\mathfrak{P}$. Then $\mathcal{O}_K/\mathfrak{p}$ and $\mathcal{O}_L/\mathfrak{P}$ are finite fields of characteristic $\mathfrak{p}$. Furthermore, the natural injection $\mathcal{O}_K \hookrightarrow \mathcal{O}_L$ induces an injection

$$\mathcal{O}_K/\mathfrak{p} \hookrightarrow \mathcal{O}_L/\mathfrak{P},$$

since $\mathfrak{P}\cap\mathcal{O}_K = \mathfrak{p}$ by Lemma 2.12. Thus $\mathcal{O}_L/\mathfrak{P}$ is an extension field of $\mathcal{O}_K/\mathfrak{p}$. We define the *inertial degree* $f(\mathfrak{P}/\mathfrak{p})$ to be the degree $[\mathcal{O}_L/\mathfrak{P} : \mathcal{O}_K/\mathfrak{p}]$ of this extension. Note that

$$\mathrm{N}_{L/K}(\mathfrak{P}) = \mathrm{N}_{K/\mathbb{Q}}(\mathfrak{p})^{f(\mathfrak{P}/\mathfrak{p})}.$$

We can now state and prove our fundamental result.

THEOREM 2.13. *Let L/K be an extension of number fields of degree n and let $\mathfrak{p}$ be a prime of $\mathcal{O}_K$. Let*

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

be the factorization of $\mathfrak{p}\mathcal{O}_L$ into primes of $\mathcal{O}_L$. Set $f_i = f(\mathfrak{P}_i/\mathfrak{p})$. Then

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

PROOF. Taking ideal norms of both sides of the factorization of $\mathfrak{p}\mathcal{O}_L$, we find that

$$\begin{aligned}\mathrm{N}_{L/\mathbb{Q}}(\mathfrak{p}\mathcal{O}_L) &= \mathrm{N}_{L/\mathbb{Q}}(\mathfrak{P}_1)^{e_1}\cdots\mathrm{N}_{L/\mathbb{Q}}(\mathfrak{P}_r)^{e_r}\\ &= \mathrm{N}_{K/\mathbb{Q}}(\mathfrak{p})^{f_1e_1}\cdots\mathrm{N}_{K/\mathbb{Q}}(\mathfrak{p})^{f_re_r}\end{aligned}$$

by the definition of the f_i. By Corollary 2.10 we know that $\mathrm{N}_{L/\mathbb{Q}}(\mathfrak{p}\mathcal{O}_L) = \mathrm{N}_{K/\mathbb{Q}}(\mathfrak{p})^n$, from which the theorem now follows immediately. □

Let us finish this section with some additional facts and terminology. First of all, let $M/L/K$ be number fields, let $\mathfrak{p}_K$ be a prime of $\mathcal{O}_K$, let $\mathfrak{p}_L$ be a prime of $\mathcal{O}_L$ lying over $\mathfrak{p}_K$, and let $\mathfrak{p}_M$ be a prime of $\mathcal{O}_M$ lying over $\mathfrak{p}_L$. Then clearly $\mathfrak{p}_M$ lies over $\mathfrak{p}_K$, and it follows immediately from the definitions that we have

$$e(\mathfrak{p}_M/\mathfrak{p}_K) = e(\mathfrak{p}_M/\mathfrak{p}_L)e(\mathfrak{p}_L/\mathfrak{p}_K)$$

and

$$f(\mathfrak{p}_M/\mathfrak{p}_K) = f(\mathfrak{p}_M/\mathfrak{p}_L)f(\mathfrak{p}_L/\mathfrak{p}_K).$$

Next return to the case of an extension L/K of degree n and let $\mathfrak{p}$ be a prime of $\mathcal{O}_K$. Let

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

be the factorization of $\mathfrak{p}\mathcal{O}_L$ into primes of $\mathcal{O}_L$. Set $f_i = f(\mathfrak{P}_i/\mathfrak{p})$. If any of the e_i are not equal to 1, then we say that $\mathfrak{p}$ *ramifies* in L/K. (It is an important fact that only finitely many primes ramify in an extension, and which primes these are and how badly they ramify is an essential invariant of the extension.) If $r = 1$ and $e_1 = n$ (so that $f_1 = 1$), then $\mathfrak{p}$ is said to be *totally ramified* in L/K:

$$\mathfrak{p}\mathcal{O}_L = \mathfrak{P}^n.$$

If $r = 1$ and $e_1 = 1$ (so that $f_1 = n$), we say that $\mathfrak{p}$ is *inert* or *remains primes* in L/K; this is the case where $\mathfrak{p}\mathcal{O}_L$ is still prime. Lastly, if $e_i = f_i = 1$ for all i, we say that $\mathfrak{p}$ *splits completely* in L/K:

$$\mathfrak{p}\mathcal{O}_L = \mathfrak{P}_1 \cdots \mathfrak{P}_n.$$

2.4. Factorization in Galois extensions. Let L/K be a Galois extension. The presence of automorphisms of K causes factorizations to behave much more regularly than in arbitrary extensions, for the simple reason that if two primes are mapped to each other by an element of $\mathrm{Gal}(L/K)$, then the primes must have isomorphic residue fields. The key fact is the following.

LEMMA 2.14. *Let L/K be a Galois extension and let $\mathfrak{p}$ be a prime of $\mathcal{O}_K$. Let $\mathfrak{P}_1, \ldots, \mathfrak{P}_r$ be the primes of L lying over $\mathfrak{p}$. Then $\mathrm{Gal}(L/K)$ acts transitively on this set of primes; that is, for any i and j, there exists $\sigma \in \mathrm{Gal}(L/K)$ such that $\sigma(\mathfrak{P}_i) = \mathfrak{P}_j$.*

PROOF. Fix distinct primes $\mathfrak{P}$ and $\mathfrak{P}'$ lying over $\mathfrak{p}$. Suppose that

$$\sigma(\mathfrak{P}) \neq \mathfrak{P}'$$

for all $\sigma \in \mathrm{Gal}(L/K)$. Using this hypothesis, by the Chinese remainder theorem (see Exercise 3.6), we can find $\alpha \in \mathcal{O}_L$ such that

$$\alpha \equiv 0 \pmod{\mathfrak{P}'}$$

and

$$\alpha \equiv 1 \pmod{\sigma(\mathfrak{P})}$$

for all $\sigma \in \mathrm{Gal}(L/K)$. Consider

$$\mathrm{N}_{L/K}(\alpha) = \prod_{\sigma \in \mathrm{Gal}(L/K)} \sigma(\alpha) \in \mathcal{O}_K.$$

Since $\alpha \in \mathfrak{P}'$, this norm must lie in $\mathfrak{P}' \cap \mathcal{O}_K = \mathfrak{p}$.

On the other hand, since $\alpha \equiv 1 \pmod{\sigma(\mathfrak{P})}$ for all σ, we also have $\alpha \notin \sigma(\mathfrak{P})$; thus

$$\sigma^{-1}(\alpha) \notin \mathfrak{P}$$

for any $\sigma \in \mathrm{Gal}(L/K)$. Since as σ runs through $\mathrm{Gal}(L/K)$, σ^{-1} also runs through $\mathrm{Gal}(L/K)$, we find that

$$\mathrm{N}_{L/K}(\alpha) = \prod_{\sigma \in \mathrm{Gal}(L/K)} \sigma^{-1}(\alpha).$$

Since none of the factors lie in $\mathfrak{P}$ and $\mathfrak{P}$ is prime, this implies that $\mathrm{N}_{L/K}(\alpha) \notin \mathfrak{P}$. Thus $\mathrm{N}_{L/K}(\alpha) \notin \mathfrak{P} \cap \mathcal{O}_K = \mathfrak{p}$. But thus is a contradiction, which proves the lemma. $\square$

COROLLARY 2.15. *Let L/K be a Galois extension of degree n and let $\mathfrak{p}$ be a prime of $\mathcal{O}_K$. Let*

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

be the factorization of $\mathfrak{p}$ in $\mathcal{O}_L$, and set $f_i = f(\mathfrak{P}_i/\mathfrak{p})$. Then

$$f_1 = f_2 = \cdots = f_r$$

and

$$e_1 = e_2 = \cdots = e_r.$$

In particular, $re_if_i = n$ for all i.

PROOF. If $r = 1$ then the corollary is trivial, so we assume that $r \geq 2$. We will prove that $e_1 = e_2$ and $f_1 = f_2$; the general case is the same. By Lemma 2.14 we can find $\sigma \in \mathrm{Gal}(L/K)$ such that $\sigma(\mathfrak{P}_1) = \mathfrak{P}_2$. Applying σ to our factorization, and using the fact that $\sigma(\mathfrak{p}) = \mathfrak{p}$ since σ fixes K, we find that

$$\begin{aligned}\mathfrak{p}\mathcal{O}_L &= \sigma(\mathfrak{P}_1)^{e_1}\sigma(\mathfrak{P}_2)^{e_2} \cdots \sigma(\mathfrak{P}_r)^{e_r} \\ &= \mathfrak{P}_2^{e_1}\sigma(\mathfrak{P}_2)^{e_2} \cdots \sigma(\mathfrak{P}_r)^{e_r}.\end{aligned}$$

Furthermore, if $\sigma(\mathfrak{P}_i) = \mathfrak{P}_2$, then $\mathfrak{P}_i = \sigma^{-1}(\mathfrak{P}_2) = \mathfrak{P}_1$; thus $\sigma(\mathfrak{P}_i) \neq \mathfrak{P}_2$ for $i \neq 1$. Therefore $\mathfrak{P}_2^{e_1}$ is the only factor of $\mathfrak{P}_2$ occurring in this factorization of $\mathfrak{p}\mathcal{O}_K$; by unique factorization of ideals we now see that e_1 must equal e_2.

The fact that $f_1 = f_2$ is immediate from the fact that σ induces an isomorphism

$$\mathcal{O}_L/\mathfrak{P}_1 \cong \mathcal{O}_L/\mathfrak{P}_2.$$

□

3. Explicit factorization of ideals

3.1. Factorization of primes. Let K be a number field of degree n. For this section we make the additional hypothesis that $\mathcal{O}_K = \mathbb{Z}[\alpha]$ for some $\alpha \in \mathcal{O}_K$, with minimal polynomial $f(x) \in \mathbb{Z}[x]$. (We have in mind the case $K = \mathbb{Q}(\zeta_m)$, in which case this hypothesis is satisfied.) The general case is somewhat more complicated and we will not treat it here. Let p be a prime of $\mathbb{Z}$. We wish to explicitly determine the factorization of the ideal $p\mathcal{O}_K$ of $\mathcal{O}_K$.

We will mimic the method we used in the quadratic case. Let

$$\bar{f}(x) = \bar{g}_1(x)^{e_1} \cdots \bar{g}_r(x)^{e_r}$$

be the factorization of $\bar{f}(x)$ into irreducibles in $\mathbb{F}_p[x]$. (As usual we will write $g_i(x)$ for any lift of $\bar{g}_i(x)$ to $\mathbb{Z}[x]$.) Let f_i be the degree of $\bar{g}_i(x)$; we have $\sum e_if_i = n$.

We claim that each ideal

$$\mathfrak{p}_i = \big(p, g_i(\alpha)\big)$$

of $\mathcal{O}_K$ is prime, and that

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

We further claim that

$$f(\mathfrak{p}_i/p) = f_i.$$

Some of these assertions are immediate. First of all,

$$\begin{aligned}\mathcal{O}_K/\mathfrak{p}_i &= \mathbb{Z}[\alpha]/(p, g_i(\alpha))\\ &\cong \mathbb{Z}[x]/(f(x), p, g_i(x))\\ &\cong \mathbb{F}_p[x]/(\bar{f}(x), \bar{g}_i(x))\\ &\cong \mathbb{F}_p[x]/(\bar{g}_i(x))\end{aligned}$$

since $\bar{g}_i(x)$ divides $\bar{f}(x)$ in $\mathbb{F}_p[x]$. Since $\bar{g}_i(x)$ is an irreducible polynomial of degree f_i, $\mathbb{F}_p[x]/(\bar{g}_i(x))$ is a field of order p^{f_i}, which shows both that $\mathfrak{p}_i$ is prime and that $f(\mathfrak{p}_i/p) = f_i$. Note also that it follows from Exercise 3.3 that the $\mathfrak{p}_i$ are relatively prime.

Let us now relate these to the factorization of $p\mathcal{O}_K$. We will determine the kernel of the quotient map

$$\mathcal{O}_K \to \mathcal{O}_K/p\mathcal{O}_K,$$

which of course is just $p\mathcal{O}_K$, in a different way. Note that

$$\mathcal{O}_K/p\mathcal{O}_K = \mathbb{Z}[\alpha]/p\mathbb{Z}[\alpha] \cong \mathbb{Z}[x]/(p, f(x)) \cong \mathbb{F}_p[x]/(\bar{f}(x)).$$

The Chinese remainder theorem shows that

$$\mathbb{F}_p[x]/(\bar{f}(x)) \cong \mathbb{F}_p[x]/(\bar{g}_1(x)^{e_1}) \times \cdots \times \mathbb{F}_p[x]/(\bar{g}_r(x)^{e_r});$$

thus we can consider the map $\mathcal{O}_K \to \mathcal{O}_K/p\mathcal{O}_K$ as the map

$$\mathcal{O}_K \to \mathbb{F}_p[x]/(\bar{g}_1(x)^{e_1}) \times \cdots \times \mathbb{F}_p[x]/(\bar{g}_r(x)^{e_r}$$

sending α to $(x, \dots, x)$. The kernel into each factor is just $\big(p, g_i(\alpha)\big)$, so the kernel of the map (which is just $\mathfrak{p}\mathcal{O}_K$) is

$$\big(p, g_1(\alpha)^{e_1}\big) \cap \cdots \cap \big(p, g_r(\alpha)^{e_r}\big).$$

Furthermore, Exercise 3.3 shows that all of these ideals are pairwise relatively prime, so that by Exercise 3.4 the kernel is just the product

$$\big(p, g_1(\alpha)^{e_1}\big) \cdots \big(p, g_r(\alpha)^{e_r}\big).$$

This shows that

$$p\mathcal{O}_K = \big(p, g_1(\alpha)^{e_1}\big) \cdots \big(p, g_r(\alpha)^{e_r}\big).$$

However, these factors are not yet primes for any i such that $e_i > 1$.

It remains to "pull out" the e_i. First, $(p, g_i(\alpha)^{e_i})$ divides $\mathfrak{p}_i^{e_i}$. To see this, note that every generator of

$$\mathfrak{p}_i^{e_i} = \big(p, g_i(\alpha)\big)^{e_i}$$

is divisible by p except for $g_i(\alpha)^{e_i}$. This shows that every generator of $\mathfrak{p}_i^{e_i}$ lies in $\big(p, g_i(\alpha)^{e_i}\big)$, so $\mathfrak{p}_i^{e_i}$ itself is contained in $\big(p, g_i(\alpha)^{e_i}\big)$. Lemma II.3.8 now gives the asserted division.

Since the ideals $(p, g_i(\alpha)^{e_i})$ are all relatively prime, we now know that $p\mathcal{O}_K$ divides $\mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_r^{e_r}$ divides $p\mathcal{O}_K$. The norm of the second term is

$$p^{f_1 e_1} \cdots p^{f_r e_r} = p^n;$$

this is also the norm of $p\mathcal{O}_K$. This implies that the two ideals must be equal, since if one ideal contains another and has the same norm they must be equal. This completes the proof of the explicit factorization of $p\mathcal{O}_K$.

Example 3.1. Let α be a root of the polynomial $f(x) = x^3 + 2x + 1$ and let $K = \mathbb{Q}(\alpha)$. Exercise 3.18 shows that $\mathcal{O}_K = \mathbb{Z}[\alpha]$, so we may apply the methods of this section. Let us factor some small rational primes. Note that factoring $f(x)$ modulo primes is easy, since if $f(x)$ has any factors then it will have roots; this is no longer true for degree 4 and higher.

When $p = 2$, we find that

$$x^3 + 2x + 1 \equiv (x+1)(x^2+x+1) \pmod{2},$$

so

$$2\mathcal{O}_K = \bigl(2, \alpha+1\bigr)\bigl(2, \alpha^2+\alpha+1\bigr).$$

Here the first factor has inertial degree 1 and the second factor has inertial degree 2. For $p = 3$, $f(x)$ is irreducible in $\mathbb{F}_3[x]$, so $3\mathcal{O}_K$ factors as $\bigl(3, f(\alpha)\bigr) = (3)$; that is, $3\mathcal{O}_K$ remains prime. The reader can easily check that $5\mathcal{O}_K$ and $7\mathcal{O}_K$ also remain prime. For $p = 11$, we find that

$$x^3 + 2x + 1 \equiv (x+2)(x^2-2x+6) \pmod{11},$$

so

$$11\mathcal{O}_K = \bigl(11, \alpha+2\bigr)\bigl(11, \alpha^2-2\alpha+6\bigr).$$

$13\mathcal{O}_K$ also remains prime, while

$$x^3 + 2x + 1 \equiv (x-3)(x-5)(x-9) \pmod{17},$$

so $17\mathcal{O}_K$ splits completely as

$$17\mathcal{O}_K = \bigl(17, \alpha-3\bigr)\bigl(17, \alpha-5\bigr)\bigl(17, \alpha-9\bigr).$$

Since K has discriminant -59, Exercise 3.16 shows that 59 will be the only prime which ramifies. One finds that

$$x^3 + 2x + 1 \equiv (x-14)^2(x-31) \pmod{59},$$

so

$$59\mathcal{O}_K = \bigl(59, \alpha-14\bigr)^2\bigl(59, \alpha-31\bigr).$$

3.2. Factoring cyclotomic polynomials. The methods of the previous section give us a computational procedure for determining prime splitting in many number fields, but it becomes difficult to carry out in practice as soon as the degree of the number field becomes large. Luckily, in the important case of cyclotomic fields we can give a good description of the factorization of cyclotomic polynomials, even if it is difficult to write down the actual factors. The key result is the following lemma, which says that the m^{th} cyclotomic polynomial is the "universal" polynomial for testing if an element of a field is a primitive m^{th} root of unity.

Lemma 3.2. *Let m be a positive integer and let K be a field of characteristic not dividing m. Let α be an element of K. Then $\Phi_m(\alpha) = 0$ if and only if α is a primitive m^{th} root of unity.*

Proof. Recall that

$$x^m - 1 = \prod_{d \mid m} \Phi_d(x).$$

Since this factorization is in $\mathbb{Z}[x]$, it also makes sense in $K[x]$. Note also that $x^m - 1$ has no multiple roots in K, as follows immediately from the derivative test. (This is the only place where we will use the assumption on the characteristic of K.)

Suppose first that α is a primitive m^{th} root of unity. Then α is a root of $x^m - 1$, so it must be a root of some $\Phi_d(x)$ with d dividing m. Suppose that α is a root of $\Phi_d(x)$ with $d < m$. Then, since $\Phi_d(x)$ divides $x^d - 1$, $\alpha^d = 1$. This contradicts the fact that α is a primitive m^{th} root of unity, so α must be a root of $\Phi_m(x)$.

Conversely, suppose that $\Phi_m(\alpha) = 0$. Since $\Phi_m(x)$ divides $x^m - 1$, this implies that $\alpha^m = 1$; that is, α is an m^{th} root of unity. Suppose that α is actually a primitive d^{th} root of unity for some divisor d of m with $d < m$. Then the argument in the first half of the proof shows that $\Phi_d(\alpha) = 0$. But then α would be a double root of $x^m - 1$, which is a contradiction since $x^m - 1$ does not have multiple roots. Thus α is a primitive m^{th} root of unity. $\square$

Let $K = \mathbb{Q}(\zeta_m)$ be a cyclotomic field and let p be a rational prime. Let $\mathfrak{p}$ be any prime of $\mathcal{O}_K = \mathbb{Z}[\zeta_m]$ lying over p. We wish to determine $e = e(\mathfrak{p}/p)$ and $f = f(\mathfrak{p}/p)$. Note that by Corollary 2.15 these numbers are independent of the choice of prime $\mathfrak{p}$. Put differently, in $\mathbb{F}_p[x]$ $\Phi_m(x)$ factors as

$$\Phi_m(x) = \big(g_1(x) \cdots g_r(x)\big)^e$$

where $\deg g_i = f$ for all i and $efr = \varphi(m)$.

We begin with the case that p does not divide m. Since $x^m - 1$ has no repeated factors in $\mathbb{F}_p[x]$, $\Phi_m(x)$ doesn't either; in particular, we must have $e = 1$. Thus we are left to determine f and r. Before we do the general case, we examine the case $f = 1$ to illustrate the idea. If $f = 1$, then $\Phi_m(x)$ splits into linear factors in $\mathbb{F}_p[x]$; thus $\Phi_m(x)$ has roots in $\mathbb{F}_p$. By Lemma 3.2, this implies that $\mathbb{F}_p$ has primitive m^{th} roots of unity. But $\mathbb{F}_p^*$ is a cyclic group of order $p - 1$, so it has elements of exact order m if and only if m divides $p - 1$; that is, if and only if

$$p \equiv 1 \pmod{m}.$$

The above argument is reversible, so we have shown that a rational prime p splits completely in $\mathbb{Q}(\zeta_m)$ if and only if p does not divide m and $p \equiv 1 \pmod{m}$.

In the general case we must go to an extension of $\mathbb{F}_p$ to find a primitive m^{th} root of unity. Let $g(x)$ be one of the irreducible factors of $\Phi_m(x)$ in $\mathbb{F}_p[x]$; $g(x)$ has degree f. Let α be a root of $g(x)$ and set $F = \mathbb{F}_p(\alpha) \cong \mathbb{F}_p[x]/(g(x))$; this is an extension of $\mathbb{F}_p$ of degree f. Note that α is a primitive m^{th} root of unity since it satisfies $g(x)$ and thus $\Phi_m(x)$. Furthermore, F is clearly the smallest extension of $\mathbb{F}_p$ containing a primitive m^{th} root of unity (since it is just $\mathbb{F}_p$ adjoined a m^{th} root of unity), so we have shown that f is the degree of the smallest extension of $\mathbb{F}_p$ containing a primitive m^{th} root of unity.

Let us now determine this extension in another way. Let F_i be the unique extension of $\mathbb{F}_p$ of degree i. Then F_i^* is cyclic of order $p^i - 1$, so it contains a primitive m^{th} root of unity if and only if m divides $p^i - 1$. Thus the smallest extension of $\mathbb{F}_p$ containing a primitive m^{th} root of unity will be F_i, where i is the smallest positive integer such that

$$p^i \equiv 1 \pmod{m};$$

that is, i is the order of p in $(\mathbb{Z}/m\mathbb{Z})^*$. Combining this with our earlier arguments, we obtain the following result.

Proposition 3.3. *Let p be a rational prime not dividing m and let $\mathfrak{p}$ be a prime of $\mathbb{Z}[\zeta_m]$ lying over p. Then $e(\mathfrak{p}/p) = 1$, $f(\mathfrak{p}/p)$ is the order of p in $(\mathbb{Z}/m\mathbb{Z})^*$, and there are exactly $\varphi(m)/f(\mathfrak{p}/p)$ primes of $\mathbb{Z}[\zeta_m]$ lying over p.*

EXAMPLE 3.4. Let $K = \mathbb{Q}(\zeta_5)$. The behavior of a rational prime p in $\mathcal{O}_K$ is determined entirely by the residue class of p in $(\mathbb{Z}/5\mathbb{Z})^*$. If $p \equiv 1 \pmod 5$ (for example, $p = 11$), then p splits completely in $\mathcal{O}_K$. If $p \equiv 4 \pmod 5$, then p splits into 2 prime factors, each with inertial degree 2. If $p \equiv 2, 3 \pmod 5$, then p remains prime in $\mathcal{O}_K$.

For some explicit examples, we consider the primes $3, 7, 11, 19$. For $p = 3, 7$ the above argument shows that $\Phi_5(x) = x^4 + x^3 + x^2 + x + 1$ is irreducible modulo p, so $3\mathcal{O}_K$ and $7\mathcal{O}_K$ are both prime ideals of $\mathcal{O}_K$. For $p = 19$, we find that

$$x^4 + x^3 + x^2 + x + 1 \equiv (x^2 + 5x + 1)(x^2 + 15x + 1) \pmod{19},$$

so

$$\bigl(19\bigr) = \bigl(19, \zeta_5^2 + 5\zeta_5 + 1\bigr)\bigl(19, \zeta_5^2 + 15\zeta_5 + 1\bigr).$$

Lastly, modulo 11 we have

$$x^4 + x^3 + x^2 + x + 1 = (x + 2)(x + 6)(x + 7)(x + 8) \pmod{11},$$

so

$$\bigl(11\bigr) = \bigl(11, \zeta_5 + 2\bigr)\bigl(11, \zeta_5 + 6\bigr)\bigl(11, \zeta_5 + 7\bigr)\bigl(11, \zeta_5 + 8\bigr).$$

The ramified case works out somewhat differently. We will only consider the case of the splitting of $p\mathcal{O}_K$ in $\mathbb{Q}(\zeta_p)$, which is by far the most important.

We must determine the factorization of

$$\Phi_p(x) = \frac{x^p - 1}{x - 1} = x^{p-1} + x^{p-2} + \cdots + 1$$

in $\mathbb{F}_p[x]$. By Exercise I.1.15, we see that

$$x^p - 1 \equiv (x - 1)^p \pmod p,$$

so

$$\Phi_p(x) = (x - 1)^{p-1}$$

in $\mathbb{F}_p[x]$. Thus

$$p\mathcal{O}_K = \bigl(p, \zeta_p - 1\bigr)^{p-1}.$$

Furthermore,

$$\mathcal{O}_K/\bigl(p, \zeta_p - 1\bigr) = \mathbb{Z}[\zeta_p]/(p, \zeta_p - 1) \cong \mathbb{Z}/p\mathbb{Z},$$

so $\bigl(p, \zeta_p - 1\bigr)$ is prime with inertial degree 1. Thus $p\mathcal{O}_K$ is totally ramified. Note that we actually already had a better form of this result; see Exercise 2.13.

3.3. Applications to quadratic fields. There are some very interesting applications of the arithmetic of cyclotomic fields to quadratic fields. Consider the field $\mathbb{Q}(\zeta_p)$ for some odd prime p. Recall that this is a Galois extension of $\mathbb{Q}$ with Galois group isomorphic to $(\mathbb{Z}/p\mathbb{Z})^*$, where the automorphism corresponding to $a \in (\mathbb{Z}/p\mathbb{Z})^*$ is σ_a characterized by

$$\sigma_a(\zeta_p) = \zeta_p^a.$$

Since $(\mathbb{Z}/p\mathbb{Z})^*$ is cyclic of order $p - 1$, it contains a unique subgroup of index 2, consisting of all of the squares in $(\mathbb{Z}/p\mathbb{Z})^*$. Denote by S the corresponding subgroup of $\mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})$. Let K be the fixed field of S; that is, K is the subfield of $\mathbb{Q}(\zeta_p)$ of elements fixed by all of S. Galois theory tells us that $[K : \mathbb{Q}] = 2$; thus K is a quadratic field. It remains to determine which quadratic field it is.

We can do this by considering ramification. Recall that p is totally ramified in $\mathbb{Q}(\zeta_p)$; that is, there is a unique prime $\mathfrak{P}$ of $\mathbb{Q}(\zeta_p)$ lying over p, and $(p) = \mathfrak{P}^{p-1}$.

Let $\mathfrak{p}$ be any prime of K lying over p. Then $\mathfrak{P}$ lies over $\mathfrak{p}$ (since $\mathfrak{P}$ is the only prime of K lying over p) and

$$e(\mathfrak{P}/p) = e(\mathfrak{P}/\mathfrak{p})e(\mathfrak{p}/p);$$

since $e(\mathfrak{P}/p) = p - 1$ and ramification indices are bounded by the degrees of the extensions, this implies that $e(\mathfrak{P}/\mathfrak{p}) = \frac{p-1}{2}$ and $e(\mathfrak{p}/p) = 2$. In particular, $\mathfrak{p}$ is the only prime of K lying over p, and it is totally ramified.

Let $\mathfrak{Q}$ be any other prime of $\mathbb{Q}(\zeta_p)$, let $\mathfrak{q}$ be the prime of K which it lies over, and let q be the prime of $\mathbb{Z}$ which it lies over. A similar argument, using the fact that $e(\mathfrak{Q}/q) = 1$, shows that $e(\mathfrak{q}/q) = 1$, so that q is not ramified in K. We conclude that p is the only prime of $\mathbb{Z}$ which ramifies in K.

Now, we have already determined the ramification in every quadratic field, and the only quadratic field in which only p ramifies is $\mathbb{Q}(\sqrt{\varepsilon p})$, where $\varepsilon = \pm 1$ is such that

$$\varepsilon p \equiv 1 \pmod 4.$$

(See Corollary 1.3.) We can take $\varepsilon = (-1)^{(p-1)/2}$. We have therefore established the following distinctly non-obvious fact.

PROPOSITION 3.5. *The field $\mathbb{Q}(\zeta_p)$ contains the quadratic field $\mathbb{Q}(\sqrt{\varepsilon p})$, where $\varepsilon = (-1)^{(p-1)/2}$. In particular, $\sqrt{\varepsilon p}$ can be written as a rational linear combination of p^{th} roots of unity.*

We are now in a position to prove the celebrated quadratic reciprocity law.

THEOREM 3.6 (Quadratic Reciprocity). *Let p and q be distinct, positive odd primes. Then*

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}.$$

PROOF. We showed above that $\sqrt{\varepsilon p} \in \mathbb{Q}(\zeta_p)$. Denote this element by τ. Consider the automorphism $\sigma_q \in \operatorname{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})$; it is defined by $\sigma_q(\zeta_p) = \zeta_p^q$. Since the conjugates of τ are simply $\pm\tau$, we must have

$$\sigma_q(\tau) = \pm\tau.$$

Furthermore, letting S be the subgroup of $\operatorname{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})$ defined above, $\sigma_q(\tau) = \tau$ if and only if $\sigma_q \in S$. (This is because $\mathbb{Q}(\tau)$ is the fixed field of S by definition.) Under the identification of $\operatorname{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})$ and $(\mathbb{Z}/p\mathbb{Z})^*$, S corresponds to the subgroup of squares; combining all of this, we see that $\sigma_q(\tau) = \tau$ if and only if q is a square in $(\mathbb{Z}/p\mathbb{Z})^*$; that is,

$$\sigma_q(\tau) = \left(\frac{q}{p}\right)\tau.$$

Now let $\mathfrak{q}$ be a prime of $\mathcal{O}_K$ lying over q. Write $\tau = a_0 + a_1\zeta_p + \cdots + a_{p-2}\zeta_p^{p-2}$ with $a_i \in \mathbb{Z}$. (Note that τ is visibly an algebraic integer.) Using that $\sigma_q(\zeta_p) = \zeta_p^q$ and $a^q = a$ for all $a \in \mathbb{F}_q$, we find that

$$\begin{aligned}
\sigma_q(\tau) &= a_0 + a_1\zeta_p^q + a_2\zeta_p^{2q} + \cdots + a_{p-2}\zeta_p^{(p-2)q} \\
&\equiv a_0^q + a_1^q\zeta_p^q + a_2^q\zeta_p^{2q} + \cdots + a_{p-2}^q\zeta_p^{(p-2)q} \pmod{\mathfrak{q}} \\
&\equiv (a_0 + a_1\zeta_p + a_2\zeta_p^2 + \cdots + a_{p-2}\zeta_p^{p-2})^q \pmod{\mathfrak{q}} \\
&\equiv \tau^q \pmod{\mathfrak{q}}.
\end{aligned}$$

Combining this with our other expression for $\sigma_q(\tau)$ yields

$$\left(\frac{q}{p}\right)\tau \equiv \tau^q \pmod{\mathfrak{q}}.$$

Since $\mathfrak{q}$ is prime and we clearly have $\tau \notin \mathfrak{q}$, we can cancel τ modulo $\mathfrak{q}$; we conclude that

$$\left(\frac{q}{p}\right) \equiv \tau^{q-1} \equiv (\varepsilon p)^{(q-1)/2} \pmod{\mathfrak{q}}.$$

By Exercise 3.9, this shows that

$$\left(\frac{q}{p}\right) \equiv \left(\frac{\varepsilon p}{q}\right) \pmod{\mathfrak{q}}.$$

By definition, this means that

$$\left(\frac{q}{p}\right) - \left(\frac{\varepsilon p}{q}\right) \in \mathfrak{q};$$

since $\left(\frac{q}{p}\right)$ and $\left(\frac{\varepsilon p}{q}\right)$ are integers, this difference is actually contained in $\mathfrak{q} \cap \mathbb{Z} = q\mathbb{Z}$. In fact, $\left(\frac{q}{p}\right)$ and $\left(\frac{\varepsilon p}{q}\right)$ are just ± 1, so the difference is certainly smaller than $\pm q$. It follows that we actually have an equality

$$\left(\frac{q}{p}\right) = \left(\frac{\varepsilon p}{q}\right).$$

The fact that

$$\left(\frac{\varepsilon}{q}\right) = \left(\frac{(-1)^{(p-1)/2}}{q}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$$

completes the proof. $\square$

4. Exercises

4.1. Relatively prime ideals. Recall that two ideals I, J of a ring R are said to be *relatively prime* if $I + J = R$. This is the same as there existing $i \in I$ and $j \in J$ such that $i + j = 1$.

EXERCISE 3.1. Show that if I and J are relatively prime, then I^m and J^n are relatively prime for every $m, n \geq 1$.

EXERCISE 3.2. Let R be a Dedekind domain and let I and J be ideals of R. Show that I and J are relatively prime if and only if they have no common prime ideal factors.

EXERCISE 3.3. Let K be a number field, let α be an algebraic integer in $\mathcal{O}_K$ and let p be a rational prime. Let $f(x), g(x) \in \mathbb{Z}[x]$ be two polynomials such that $\bar{f}(x), \bar{g}(x) \in \mathbb{F}_p[x]$ are relatively prime. Show that the ideals $\big(p, f(\alpha)\big)$ and $\big(p, g(\alpha)\big)$ of $\mathcal{O}_K$ are relatively prime.

EXERCISE 3.4. Let I and J be relatively prime ideals. Show that $I \cap J = IJ$. Generalize to pairwise relatively prime ideals $I_1, \ldots, I_n$.

EXERCISE 3.5 (Chinese remainder theorem). Let I and J be relatively prime ideals. Show that the natural map sending x to (x, x) induces an isomorphism

$$R/IJ \cong R/I \times R/J.$$

Generalize to pairwise relatively prime ideals $I_1, \ldots, I_n$.

EXERCISE 3.6 (Chinese remainder theorem, classical form). Reinterpret Exercise 3.5 to show that given pairwise relatively prime ideals $I_1, \ldots, I_n$ and elements $x_i \in R/I_i$, there exist $x \in R$ such that

$$x \equiv x_i \pmod{I_i}$$

for all i.

EXERCISE 3.7. Prove Lemma 2.12.

EXERCISE 3.8. Let L/K be an extension of number fields. Show that every prime $\mathfrak{P}$ of $\mathcal{O}_L$ lies over a unique prime of $\mathcal{O}_K$ (what does it have to be?) and show that every prime $\mathfrak{p}$ of $\mathcal{O}_K$ lies under at least one prime of $\mathcal{O}_L$. (Consider $\mathfrak{p}\mathcal{O}_L$ and use Exercise 3.7.)

4.2. The Legendre symbol. Let p be an odd prime. Recall that for any $a \in \mathbb{Z}$ we have defined the *Legendre symbol* $\left(\frac{a}{p}\right)$ by

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & a \text{ is a non-zero square modulo } p; \\ 0 & a \equiv 0 \pmod{p}; \\ -1 & a \text{ is not a square modulo } p. \end{cases}$$

EXERCISE 3.9. Show that

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod{p}.$$

EXERCISE 3.10. Show that $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$ for all $a, b \in \mathbb{Z}$.

EXERCISE 3.11. Let d be a positive integer and let p be a positive prime such that $p \equiv 1 \pmod{d}$. Show that $a \in (\mathbb{Z}/p\mathbb{Z})^*$ is a perfect d^{th} power modulo p if and only if

$$a^{(p-1)/d} \equiv 1 \pmod{p}.$$

EXERCISE 3.12. Use cyclotomic fields to show that

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}} = \begin{cases} 1 & p \equiv \pm 1 \pmod{8}; \\ -1 & p \equiv \pm 3 \pmod{8}. \end{cases}$$

(Hint: look at the field $\mathbb{Q}(\zeta_8)$.)

EXERCISE 3.13. Determine how 2 factors in quadratic fields.

4.3. Ramification and the discriminant.

EXERCISE 3.14. Let K be a number field of degree n and let α be a primitive element for K, with minimal polynomial $f(x)$. Show that

$$\Delta(1, \alpha, \alpha^2, \ldots, \alpha^{n-1}) = \pm \mathrm{N}_{K/\mathbb{Q}}(f'(\alpha)).$$

EXERCISE 3.15. Let $K = \mathbb{Q}(\zeta_p)$ be a cyclotomic field. Compute the discriminant Δ_K (up to sign).

EXERCISE 3.16. Let K be a number field such that $\mathcal{O}_K = \mathbb{Z}[\alpha]$ for some algebraic integer α. Show that a rational prime p ramifies in K if and only if p divides $\Delta(1, \alpha, \alpha^2, \ldots, \alpha^{n-1})$.

EXERCISE 3.17. Let K be a number field of degree n and let $\alpha_1, \ldots, \alpha_n$ and $\beta_1, \ldots, \beta_n$ be algebraic integers of $\mathcal{O}_K$. Suppose that

$$\mathbb{Z}\alpha_1 + \cdots + \mathbb{Z}\alpha_n \supseteq \mathbb{Z}\beta_1 + \cdots + \mathbb{Z}\beta_n$$

and that both are free of rank n. Show that

$$\frac{\Delta(\beta_1, \ldots, \beta_n)}{\Delta(\alpha_1, \ldots, \alpha_n)}$$

is a square in $\mathbb{Z}$.

EXERCISE 3.18. Let $K = \mathbb{Q}[x]/(x^3 + 2x + 1)$ and let α be the image of x in K. Show that $\Delta(1, \alpha, \alpha^2) = -59$, and use Exercise 3.17 to conclude that $\mathcal{O}_K = \mathbb{Z}[\alpha]$.

4.4. Some explicit factorizations.

EXERCISE 3.19. Let p be any prime of $\mathbb{Z}$ and let $\mathfrak{p}$ be a prime of $\mathbb{Q}(\zeta_7)$ lying over p. Determine the inertial degree of $\mathfrak{p}$ (in terms of p, of course).

EXERCISE 3.20. Determine the factorization of 3 and 5 in $\mathbb{Q}(\zeta_{15})$.

EXERCISE 3.21. Factor $2, 3, 5, 7, 11$ in $\mathcal{O}_K$, where $K = \mathbb{Q}(\sqrt[3]{2})$. Can you find a prime which splits completely in this field?

4.5. Primes which split completely.

EXERCISE 3.22. Let $f(x) \in \mathbb{Z}[x]$ be a non-constant polynomial. Show that there are infinitely many primes p for which $f(x)$ has a root modulo p.

EXERCISE 3.23. Let K be a number field such that $\mathcal{O}_K = \mathbb{Z}[\alpha]$ for some α. Prove that there are infinitely many primes $\mathfrak{p}$ of $\mathcal{O}_K$ such that $f(\mathfrak{p}/p) = 1$, where $(p) = \mathfrak{p} \cap \mathbb{Z}$.

EXERCISE 3.24. Use cyclotomic fields and Exercise 3.23 to show that there are infinitely many primes congruent to 1 modulo m, for any m.

CHAPTER 4

The Ideal Class Group

1. Definitions

1.1. Fractional ideals. In order to keep the algebra somewhat more pleasant, it will be useful to introduce the notion of fractional ideals. Specifically, the ideals of the ring of integers of a number field do not form a group, as there are no inverses. Fractional ideals, on the other hand, form a group; the relationship between fractional ideals and ideals is quite similar to the relationship between a number field and its ring of integers.

Let K be a number field with ring of integers $\mathcal{O}_K$. Let $\mathfrak{r}$ be a non-zero subset of K which is an $\mathcal{O}_K$-module; that is, $\mathfrak{r}$ is closed under addition and under multiplication by elements of $\mathcal{O}_K$. Such an $\mathfrak{r}$ is said to be a *fractional ideal* if there exist $\gamma_1, \dots, \gamma_m \in \mathfrak{r}$ such that

$$\mathfrak{r} = \{\alpha_1\gamma_1 + \cdots + \alpha_m\gamma_m \mid \alpha_i \in \mathcal{O}_K\};$$

that is, $\mathfrak{r}$ is generated over $\mathcal{O}_K$ by the γ_i. (The relevant thing here is that $\mathfrak{r}$ is finitely generated over $\mathcal{O}_K$. Not every $\mathcal{O}_K$-submodule of K has this property; see Exercise 4.1.)

There are two fundamental examples of fractional ideals. First of all, every non-zero ideal $\mathfrak{a}$ of $\mathcal{O}_K$ is also a fractional ideal: $\mathfrak{a}$ is an $\mathcal{O}_K$-module by definition and it has a finite generating set since $\mathcal{O}_K$ is noetherian. To avoid confusion, we shall refer to ideals of $\mathcal{O}_K$ as *integral ideals* from now on.

The second sort of example are fractional ideals of the form $\gamma\mathcal{O}_K$ for some $\gamma \in K^*$. (One checks easily that $\gamma\mathcal{O}_K$ is an $\mathcal{O}_K$-module, and it has the single generator γ.) Such a fractional ideal is called a *principal fractional ideal*. Note that the principal ideals of $\mathcal{O}_K$ are precisely the integral principal fractional ideals.

More generally, let $\mathfrak{a}$ be any ideal of $\mathcal{O}_K$ and let γ be any element of K^*. Then $\gamma\mathfrak{a}$ is a fractional ideal. ($\gamma\mathfrak{a}$ has a finite generating set since if $\alpha_1, \dots, \alpha_m$ generate $\mathfrak{a}$, then $\gamma\alpha_1, \dots, \gamma\alpha_m$ generate $\gamma\mathfrak{a}$.) The converse of this statement is also true.

LEMMA 1.1. *Let $\mathfrak{r}$ be an $\mathcal{O}_K$-submodule of K. Then $\mathfrak{r}$ is a fractional ideal if and only if there exists $\gamma \in K^*$ such that $\gamma\mathfrak{r}$ is an integral ideal. (In fact, one can actually take γ to be a rational integer.)*

PROOF. We saw above that if $\mathfrak{a}$ is an integral ideal and $\gamma \in K^*$, then $\gamma\mathfrak{a}$ is a fractional ideal. Conversely, if $\mathfrak{r}$ is a fractional ideal, then we can write

$$\mathfrak{r} = \{\alpha_1\gamma_1 + \ldots + \alpha_m\gamma_m \mid \alpha_i \in \mathcal{O}_K\}$$

for some $\gamma_1, \dots, \gamma_m \in \mathfrak{r}$. By Lemma II.2.10 there exist $a_1, \dots, a_m \in \mathbb{Z}$ such that $a_i\gamma_i \in \mathcal{O}_K$. One now easily checks that $a_1 \cdots a_m\mathfrak{r}$ is an integral ideal, which proves the lemma with $\gamma = a_1 \cdots a_m$. $\square$

We will denote by I_K the set of all fractional ideals of K. If $\mathfrak{r}, \mathfrak{s} \in I_K$, then we define the product $\mathfrak{r}\mathfrak{s}$ to be the $\mathcal{O}_K$-module generated by all products of pairs of elements of $\mathfrak{r}$ and $\mathfrak{s}$. Note that if $\mathfrak{r}$ is generated by $\gamma_1, \ldots, \gamma_m$ and $\mathfrak{s}$ is generated by $\delta_1, \ldots, \delta_k$, then $\mathfrak{r}\mathfrak{s}$ is generated by the products $\gamma_i\delta_j$. In particular, $\mathfrak{r}\mathfrak{s}$ is also a fractional ideal.

COROLLARY 1.2. *The set I_K is an abelian group under multiplication of fractional ideals.*

PROOF. We saw above that I_K is closed under multiplication. That this multiplication is commutative and associative is clear. The identity element is easily checked to be the unit ideal $\mathcal{O}_K$. It remains to find inverses. So let $\mathfrak{r}$ be a fractional ideal and choose $\gamma \in K^*$ such that $\gamma\mathfrak{r}$ is an integral ideal. By Proposition II.3.6 there is an integral ideal $\mathfrak{b}$ such that $\gamma\mathfrak{r}\mathfrak{b}$ is principal, say generated by $\alpha \in \mathcal{O}_K^*$. Take $\mathfrak{s} = \frac{\gamma}{\alpha}\mathfrak{b}$. Then $\mathfrak{s}$ is a fractional ideal, and we have

$$\mathfrak{r}\mathfrak{s} = \frac{\gamma\mathfrak{r}\mathfrak{b}}{\alpha} = \mathcal{O}_K.$$

Thus $\mathfrak{s}$ is an inverse for $\mathfrak{r}$ in I_K. □

Note that it is clear from the proof of Proposition II.3.6 that if $\mathfrak{r}$ is a fractional ideal, then its inverse is given by

$$\mathfrak{r}^{-1} = \{\gamma \in K \mid \gamma\mathfrak{r} \subseteq \mathcal{O}_K\}.$$

We can also characterize fractional ideals in terms of unique factorization of ideals.

PROPOSITION 1.3. *Every fractional ideal $\mathfrak{r}$ can be written as*

$$\mathfrak{r} = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_r^{e_r}$$

where the $\mathfrak{p}_i$ are distinct primes of $\mathcal{O}_K$ and the e_i are integers. (Note that we allow the e_i to be negative.) This expression is unique up to reordering of the factors. Thus I_K is the free abelian group on the set

$$\{\mathfrak{p} \mid \mathfrak{p} \text{ a prime of } \mathcal{O}_K\}.$$

Finally, $\mathfrak{r}$ is an integral ideal if and only if each e_i is non-negative.

PROOF. Let $\mathfrak{r}$ be a fractional ideal and choose a non-zero rational integer $a \in \mathbb{Z}$ such that that $a\mathfrak{r}$ is an integral ideal. Then we can write (uniquely up to reordering and adding factors with zero exponent)

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

$$a\mathfrak{r} = \mathfrak{p}_1^{e_1''} \cdots \mathfrak{p}_r^{e_r''};$$

here we allow some e_i' and e_i'' to be zero. Thus, since I_K is a group,

$$\mathfrak{r} = \mathfrak{p}_1^{e_1''-e_1'} \cdots \mathfrak{p}_r^{e_r''-e_r'}.$$

This shows that $\mathfrak{r}$ has such an expression; the fact that it is unique follows from the fact that the factorizations of $a\mathcal{O}_K$ and $a\mathfrak{r}$ were unique. The fact that $\mathfrak{r}$ is an integral ideal if and only if each e_i is positive is clear from unique factorization of ideals. □

Notice that this decomposition of fractional ideals in terms of prime ideals is completely analogous to the decomposition of rational numbers in terms of rational primes; see Section 1.1 of Chapter 2.

1.2. The ideal class group. Let K be a number field with ring of integers $\mathcal{O}_K$. We have seen that $\mathcal{O}_K$ may not be a unique factorization domain, although it will have unique factorization of ideals. We have also seen (see Exercise II.2.10) that $\mathcal{O}_K$ is a UFD if and only if it is a PID; that is, if and only if every ideal is principal. Furthermore, even when $\mathcal{O}_K$ is not a PID it is often useful to know when ideals are principal; see, for example, Proposition III.1.7.

These facts suggest that it would be useful to have some way to determine if an ideal is principal. Although in practice this is often quite difficult, we can proceed abstractly fairly well. Define P_K to be the subgroup of I_K of principal fractional ideals. Note that the integral ideals in P_K are precisely the principal ideals of $\mathcal{O}_K$. We define the *ideal class group* $\mathcal{C}_K$ of K to be the quotient

$$\mathcal{C}_K = I_K/P_K.$$

$\mathcal{C}_K$ naturally relates to the issues raised above. First of all, $\mathcal{C}_K$ is the trivial group if and only if $I_K = P_K$; that is, if and only if every fractional ideal of K is actually principal. Since the integral ideals in P_K are precisely the principal ideals, this is equivalent to $\mathcal{O}_K$ being a PID, which in turn is equivalent to $\mathcal{O}_K$ being a UFD. That is, $\mathcal{C}_K$ is trivial if and only if $\mathcal{O}_K$ is a UFD. Secondly, note that a fractional ideal $\mathfrak{r}$ is principal if and only if it maps to 0 in $\mathcal{C}_K$. Thus, if one could obtain a good description of $\mathcal{C}_K$, one would have a method to determine if an arbitrary ideal is principal.

We will call the elements of $\mathcal{C}_K$ *ideal classes*; thus an ideal class $\mathfrak{A}$ is simply a coset of P_K. By definition of $\mathcal{C}_K$, two fractional ideals $\mathfrak{a}$ and $\mathfrak{b}$ lie in the same ideal class if and only if there is some $\gamma \in K^*$ with

$$\gamma\mathfrak{a} = \mathfrak{b}.$$

We will write this relation as $\mathfrak{a} \sim \mathfrak{b}$. The following reinterpretation of Lemma 1.1 shows that fractional ideals are not really essential to the definition of the ideal class group.

LEMMA 1.4. *Let $\mathfrak{A}$ be an ideal class. Then there exists an integral ideal $\mathfrak{a}$ in the coset $\mathfrak{A}$.*

PROOF. Let $\mathfrak{r}$ be any fractional ideal in $\mathfrak{A}$. Then by Lemma 1.1 there exists $\gamma \in K^*$ such that $\gamma\mathfrak{r}$ is an integral ideal. Since $\gamma\mathcal{O}_K \in P_K$, we have $\gamma\mathfrak{r} \in \mathfrak{A}$, which proves the lemma. □

EXAMPLE 1.5. Take $K = \mathbb{Q}(\sqrt{-5})$ and consider the two ideals

$$\big(2, 1-\sqrt{-5}\big), \big(3, 1+\sqrt{-5}\big).$$

Note that

$$\big(2, 1-\sqrt{-5}\big) = \gamma\big(3, 1+\sqrt{-5}\big)$$

where

$$\gamma = -\frac{\sqrt{-5}}{3} + \frac{1}{3}.$$

Thus

$$\big(2, 1-\sqrt{-5}\big) \sim \big(3, 1+\sqrt{-5}\big).$$

As we saw in Section 4 of Chapter 2, the presence of non-principal ideals is closely related to the production of counterexamples to unique factorization. Thus the ideal class group is some sort of measure of how far $\mathcal{O}_K$ is from being a UFD.

The determination of the ideal class group of a number field is a central problem in algebraic number theory; it is also an extremely difficult problem in most cases. We will prove in the next section that it is finite, and often it is slightly easier to determine the *class number* $h_K = \#\mathcal{C}_K$. Later we will explain how to compute it in the case of quadratic imaginary fields and give an idea of the state of knowledge concerning ideal class groups of cyclotomic fields.

1.3. The unit group and the class number formula. We will never actually need the results of this section, but we state them for completeness. The second fundamental invariant of a number field K is the group of units $\mathcal{O}_K^*$. The importance of $\mathcal{O}_K^*$ stems from the fact that the units are precisely the ambiguity in moving from factorizations into principal ideals to factorizations of elements. This group is essentially as difficult to compute as the ideal class group, and they are closely related. We will try in this section to describe some of those relations.

To see the first relation, note that there is a natural surjection

$$K^* \twoheadrightarrow P_K$$

sending $\gamma \in K^*$ to the principal fractional ideal $\gamma\mathcal{O}_K$. The kernel of this map is just the set of $\gamma \in K^*$ for which $\gamma\mathcal{O}_K = \mathcal{O}_K$; these γ are easily seen to be precisely the units $\mathcal{O}_K^*$.

We also have a natural injection $P_K \hookrightarrow I_K$. The cokernel of this map is the ideal class group $\mathcal{C}_K$, by definition. In particular, if we consider the composite map

$$K^* \twoheadrightarrow P_K \hookrightarrow I_K,$$

we see that it has kernel $\mathcal{O}_K^*$ and cokernel $\mathcal{C}_K$. Thus we have exhibited a single map which connects these two fundamental invariants.

From here we omit all proofs. In order to state the second (much deeper) connection we need to know a bit more about the unit group. The fundamental theorem is due to Dirichlet. We first need to analyze the complex embeddings a bit. We will say that a complex embedding $\sigma : K \hookrightarrow \mathbb{C}$ is *real* if it has image in $\mathbb{R}$; otherwise it is *imaginary*. If σ is imaginary, then its complex conjugate $\bar{\sigma}$ is a different imaginary complex embedding of K. We let r be the number of real embeddings of K and s the number of complex conjugate pairs of imaginary embeddings of K. Thus $r + 2s = n$, where n is the degree of K over $\mathbb{Q}$.

Example 1.6. If $K = \mathbb{Q}(\sqrt{d})$ is quadratic with $d > 0$, then $r = 2$ and $s = 0$. Such a K is called a *real quadratic field*. If $K = \mathbb{Q}(\sqrt{d})$ with $d < 0$, then $r = 0$ and $s = 1$; K is called a *imaginary quadratic field*. If $K = \mathbb{Q}(\zeta_m)$ with $m > 2$, then every embedding is imaginary (since $\mathbb{R}$ contains no roots of unity of order > 2), so $r = 0$ and $s = \varphi(m)/2$. Note that in all of these cases we have one of r and s equal to 0; this is because the fields are Galois, and thus all embeddings have the same image. For a non-Galois example, take $K = \mathbb{Q}(\sqrt[3]{2})$: then $r = 1$ and $s = 1$.

Theorem 1.7 (Dirichlet Unit Theorem). *Let K be a number field with r real embeddings and s complex conjugate pairs of imaginary embeddings. Let W be the subgroup of $\mathcal{O}_K^*$ of roots of unity. Then*

$$\mathcal{O}_K^* \cong W \times \mathbb{Z}^{r+s-1}.$$

Note that this theorem implies that $\mathcal{O}_K^*$ is finite if and only if $r+s=1$; this occurs if and only if K is $\mathbb{Q}$ or an imaginary quadratic field. It is not a coincidence that these are the number fields of which we have the greatest understanding.

The proof of Theorem 1.7 rests upon the *logarithmic embedding* of K^*. This is a map

$$K^* \to \mathbb{R}^{r+s}$$

defined as follows: let $\sigma_1, \ldots, \sigma_r$ be the real embeddings of K and let $\sigma_{r+1}, \ldots, \sigma_{r+s}$ be a set of imaginary embeddings of K containing one of each complex conjugate pair. (Thus $\sigma_1, \ldots, \sigma_r, \sigma_{r+1}, \ldots, \sigma_{r+s}, \bar{\sigma}_{r+1}, \ldots, \bar{\sigma}_{r+s}$ are the n complex embeddings of K.) The logarithmic embedding is defined by sending $\alpha \in K^*$ to the $(r+s)$-tuple

$$\bigl(\log|\sigma_1(\alpha)|, \ldots, \log|\sigma_r(\alpha)|, 2\log|\sigma_{r+1}(\alpha)|, \ldots, 2\log|\sigma_{r+s}(\alpha)|\bigr).$$

One shows (using the fact that the norm of a unit is ± 1) that the image of $\mathcal{O}_K^*$ lies entirely within the hyperplane

$$x_1 + \cdots + x_{r+s} = 0.$$

Furthermore, by Exercise 2.16 one sees that the kernel of the logarithmic embedding is precisely the group of roots of unity W. The remainder of the proof of the theorem involves showing that the image of K^* is a lattice of maximal rank in the $r+s-1$ dimensional hyperplane $x_1 + \cdots + x_{r+s} = 0$.

We need the logarithmic embedding to define an important invariant of K. Let $\varepsilon_1, \ldots, \varepsilon_{r+s-1}$ be a basis for the free part of $\mathcal{O}_K^*$; thus every element of $\mathcal{O}_K^*$ can be written uniquely as

$$\zeta \varepsilon_1^{n_1} \cdots \varepsilon_{r+s-1}^{n_{r+s-1}}$$

with $\zeta \in W$ and each $n_i \in \mathbb{Z}$. We define the *regulator* R_K of K to be the determinant of the matrix

$$\bigl(\sigma_i(\varepsilon_j)\bigr)_{i,j=1}^{r+s-1}.$$

(It in fact doesn't matter which embedding σ_i one omits from the matrix, as each row can be written in terms of the other $r+s-1$ rows.) The *Dirichlet class number formula* states that, if $K/\mathbb{Q}$ is Galois with abelian Galois group (for example, a quadratic field or a cyclotomic field), then

$$h_K = \frac{w|\Delta_K|}{2^{r+s}\pi^s R_K} \lim_{s\to 1}(s-1)\zeta_K(1).$$

Here w is the number of roots of unity in K, Δ_K is the discriminant of $\mathcal{O}_K$, r and s are the number of real and pairs of complex conjugate imaginary embeddings respectively, and ζ_K is the *Dedekind zeta function*, defined for $\mathrm{Re}(s) > 1$ by

$$\zeta_K(s) = \sum_{\mathfrak{a} \text{ an ideal of } \mathcal{O}_K} \mathrm{N}_{K/\mathbb{Q}}(\mathfrak{a})^{-s},$$

which is a meromorphic function with an analytic continuation to the entire complex plane, with a simple pole at $s=1$.

All of these terms turn out to be reasonably easy to compute except for the regulator and the class number. One sees, therefore, that determination of the regulator is essentially the same as determination of the class number. Since to compute the regulator one virtually needs to know precisely what the units are, this means that computing the ideal class group and the unit group are almost the same problem.

2. Finiteness of the ideal class group

2.1. Norm bounds. The fact that the ideal class group is finite indicates that unique factorization never fails too spectacularly in rings of integers of number fields, and is perhaps the most important single fact in algebraic number theory. In this section we will give a surprisingly simple proof.

THEOREM 2.1. *Let K be a number field. There exists a number λ_K, depending only on K, such that every ideal non-zero $\mathfrak{a}$ of $\mathcal{O}_K$ contains a non-zero element α with*

$$|\operatorname{N}_{K/\mathbb{Q}}(\alpha)| \leq \lambda_K \operatorname{N}_{K/\mathbb{Q}}(\mathfrak{a}).$$

PROOF. Let $\alpha_1, \ldots, \alpha_n$ be an integral basis for $\mathcal{O}_K$ and let $\sigma_1, \ldots, \sigma_n$ be the complex embeddings of K. We will show that one can take

$$\lambda_K = \prod_{i=1}^{n} \left(\sum_{j=1}^{n} |\sigma_i(\alpha_j)| \right).$$

Let $\mathfrak{a}$ be a non-zero ideal of $\mathcal{O}_K$ and let m be the unique positive integer such that

$$m^n \leq \operatorname{N}_{K/\mathbb{Q}}(\mathfrak{a}) < (m+1)^n.$$

Consider the $(m+1)^n$ elements

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

Since $\mathcal{O}_K/\mathfrak{a}$ has order less than $(m+1)^n$, two of these elements must be congruent modulo $\mathfrak{a}$. Taking their difference we find an element

$$\alpha = \sum_{j=1}^{n} m_j' \alpha_j \in \mathfrak{a}$$

with $|m_j'| \leq m$. We compute

$$\begin{aligned}
|\operatorname{N}_{K/\mathbb{Q}}(\alpha)| &= \prod_{i=1}^{n} |\sigma_i(\alpha)| \\
&= \prod_{i=1}^{n} \left| \sigma_i \left(\sum_{j=1}^{n} m_j' \alpha_j \right) \right| \\
&= \prod_{i=1}^{n} \left| \sum_{j=1}^{n} m_j' \sigma_i(\alpha_j) \right| \\
&\leq \prod_{i=1}^{n} \sum_{j=1}^{n} |m_j'| |\sigma_i(\alpha_j)| \\
&\leq \prod_{i=1}^{n} \sum_{j=1}^{n} m |\sigma_i(\alpha_j)| \\
&= m^n \lambda_K \\
&\leq \lambda_K \operatorname{N}_{K/\mathbb{Q}}(\mathfrak{a})
\end{aligned}$$

as claimed. □

COROLLARY 2.2. *Let $\mathfrak{A}$ be an ideal class of $\mathcal{C}_K$. Then $\mathfrak{A}$ contains an integral ideal of norm $\leq \lambda_K$.*

PROOF. Let $\mathfrak{b}$ be any integral ideal in $\mathfrak{A}^{-1}$. By Theorem 2.1 we can find $\beta \in \mathfrak{b}$ with $|\operatorname{N}_{K/\mathbb{Q}}(\beta)| \leq \lambda_K \operatorname{N}_{K/\mathbb{Q}}(\mathfrak{b})$. The principal ideal $\beta\mathcal{O}_K$ is contained in $\mathfrak{b}$, so by Lemma II.3.8 there is an integral ideal $\mathfrak{a}$ such that $\mathfrak{a}\mathfrak{b} = \beta\mathcal{O}_K$. Since $\beta\mathcal{O}_K$ is principal we have $\mathfrak{a} \in \mathfrak{A}$, and we compute

$$\operatorname{N}_{K/\mathbb{Q}}(\mathfrak{a}) = \frac{|\operatorname{N}_{K/\mathbb{Q}}(\beta)|}{\operatorname{N}_{K/\mathbb{Q}}(\mathfrak{b})} \leq \lambda_K.$$

□

COROLLARY 2.3. *The ideal class group $\mathcal{C}_K$ is finite.*

PROOF. By Corollary 2.2 every ideal class contains an ideal of norm at most λ_K. By Exercise 4.2 there are only finitely many ideals of norm $\leq \lambda_K$, so this means that every ideal class contains one of a finite set of ideals. In particular, $\mathcal{C}_K$ must be finite. □

The bound given above is not terribly useful in actually computing the ideal class group, both because it is difficult to compute and because it gets large fairly fast. A much better bound can be obtained using Minkowski's theorem in the geometry of numbers; we state it here and will use it in the next section to compute ideal class groups of imaginary quadratic fields.

THEOREM 2.4 (Minkowski bound). *Let K be a number field of degree n. Then every ideal class of $\mathcal{O}_K$ contains an ideal $\mathfrak{a}$ satisfying*

$$\operatorname{N}_{K/\mathbb{Q}}(\mathfrak{a}) \leq \mu_K = \frac{n!}{n^n}\left(\frac{4}{\pi}\right)^s \sqrt{|\Delta_K|}.$$

Here s is the number of conjugate pairs of imaginary embeddings of K.

2.2. Computations of ideal class groups of cyclotomic fields. There are some immediate applications of the Minkowski bound. For example, take $K = \mathbb{Q}(\zeta_5)$. This field has discriminant $\Delta_K = 5^3$ and $s = 2$, so the Minkowski bound shows that every ideal class contains an ideal of norm at most

$$\mu_K = \frac{4!}{4^4}\left(\frac{4}{\pi}\right)^2 \sqrt{125} \approx 1.6992079064.$$

Thus every ideal class contains an ideal of norm 1. But the only ideal of norm 1 is $\mathcal{O}_K$, so every ideal class contains $\mathcal{O}_K$; thus there is only one ideal class, and $\mathcal{C}_K$ is trivial. It follows immediately that $\mathbb{Z}[\zeta_5]$ is a UFD.

For a slightly more involved example, take $K = \mathbb{Q}(\zeta_7)$. This time we compute that the Minkowski bound is $\mu_K \approx 4.12952833191$. Thus every ideal class contains an ideal of norm at most 4. Let $\mathfrak{a}$ be such an ideal, and assume that $\mathfrak{a} \neq \mathcal{O}_K$. Since the only possible prime factors of $\operatorname{N}_{K/\mathbb{Q}}(\mathfrak{a})$ are 2 and 3, every prime factor of $\mathfrak{a}$ must lie over 2 or 3.

Let us now determine these primes. Since 2 has order 3 in $(\mathbb{Z}/7\mathbb{Z})^*$, the primes lying over 2 will have inertial degree 3. In particular, they will have norm $2^3 = 8$; thus they can not appear as prime factors of $\mathfrak{a}$. Similarly, since 3 has order 6 in $(\mathbb{Z}/7\mathbb{Z})^*$, it actually remains prime in $\mathcal{O}_K$ and has norm $3^6 = 729$. It can not occur as a factor of $\mathfrak{a}$ either; thus $\mathfrak{a}$ must be $\mathcal{O}_K$. It follows that $\mathcal{C}_K$ is trivial and $\mathbb{Z}[\zeta_7]$ is a UFD.

Even the Minkowski bound becomes somewhat difficult to use past this point; this again illustrates how difficult it can be to compute ideal class groups.

We will conclude this section with a few comments on the study of ideal class groups of cyclotomic fields; this remains an important and active area of number theory. The determination of all cyclotomic fields of class number 1 was completed in 1971 by Masley, using work of Siegel, Montgomery and Uchida. Recall that if m is odd then $\mathbb{Q}(\zeta_m) = \mathbb{Q}(\zeta_{2m})$, so we can restrict our attention to those m which are not congruent to 2 modulo 4.

THEOREM 2.5 (Masley). *Let m be an integer which is not congruent to 2 modulo 4. Then $\mathbb{Q}(\zeta_m)$ has trivial ideal class group (and thus $\mathbb{Z}[\zeta_m]$ is a UFD) if and only if*

$$\begin{aligned} m =& 1, 3, 4, 5, 7, 8, 9, 11, 12, 13, 15, 16, 17, 19, 20, 21, 24, 25, 27, 28, \\ & 32, 33, 35, 36, 40, 44, 45, 48, 60, 84. \end{aligned}$$

PROOF. The proof is quite intricate; see [**20**, Chapter 11]. □

The first cyclotomic field with non-trivial ideal class group is $\mathbb{Q}(\zeta_{23})$, which has class number 3.

In the general case the first step is to break the ideal class group into smaller pieces. Let us write h_m for the class number of $\mathbb{Q}(\zeta_m)$ and h_m^+ for the class number of the real subfield $\mathbb{Q}(\zeta_m)^+$. One can show that h_m^+ divides h_m (the proof of this is an easy application of class field theory, but, being an application of class field theory, is not easy); set $h_m^- = h_m/h_m^+$. h_m^- turns out to be easy to compute in terms of certain Bernoulli numbers; its fine structure is now very well understood through the efforts of Herbrand, Ribet, Iwasawa, Mazur, Wiles, Thaine, Kolyvagin and Rubin, although we can not really state their results here.

Much less is known about h_m^+. We will return to it in the next chapter.

3. Ideal class groups of imaginary quadratic fields

3.1. Lattices. We turn now to the case of imaginary quadratic fields, where it is actually possible to give a reasonably straightforward algorithm for computing the ideal class group. For this section fix an imaginary quadratic field $K = \mathbb{Q}(\sqrt{d})$ with d a negative squarefree integer. We assume as usual that we have fixed an embedding of K into $\mathbb{C}$. Set

$$\alpha = \begin{cases} \sqrt{d} & d \equiv 2, 3 \pmod 4; \\ \frac{1+\sqrt{d}}{2} & d \equiv 1 \pmod 4; \end{cases}$$

which has minimal polynomial

$$f(x) = \begin{cases} x^2 - d & d \equiv 2, 3 \pmod 4; \\ x^2 - x + \frac{1-d}{4} & d \equiv 1 \pmod 4. \end{cases}$$

Consider an ideal $\mathfrak{a}$ of $\mathcal{O}_K$. Let a be any rational integer lying in $\mathfrak{a}$; then

$$a\mathcal{O}_K \subseteq \mathfrak{a} \subseteq \mathcal{O}_K,$$

so $\mathfrak{a}$ lies between two free $\mathbb{Z}$-modules of rank 2 and thus must itself be a free $\mathbb{Z}$-module of rank 2. Recall also that two ideals $\mathfrak{a}$ and $\mathfrak{b}$ of $\mathcal{O}_K$ lie in the same ideal class if and only if there is some $\gamma \in K^*$ such that $\gamma\mathfrak{a} = \mathfrak{b}$. Such submodules of $\mathbb{C}$ are called *complex lattices*; two lattices related by multiplication by a scalar are said to be *homothetic*. In this section we shall give the classification of complex lattices up to homothety; later we will use this to determine when two ideals lie in the same ideal class.

We omit all proofs; for the details, see [**17**, Chapter 7, Section 1]. Let $\Lambda \subseteq \mathbb{C}$ be a free $\mathbb{Z}$-module of rank 2 which contains an $\mathbb{R}$-basis for $\mathbb{C}$. (This last condition merely says that Λ does not lie entirely in a single line.) Thus we can write

$$\Lambda = \{a\lambda_1 + b\lambda_2 \mid a, b \in \mathbb{Z}\}$$

for some $\lambda_1, \lambda_2 \in \Lambda$; the condition that Λ is free of rank 2 amounts to the ratio

$$\frac{\lambda_1}{\lambda_2}$$

not lying in $\mathbb{Q}$, and the condition that Λ contains a $\mathbb{R}$-basis for $\mathbb{C}$ amounts to this ratio not lying in $\mathbb{R}$. We will call such a Λ a *complex lattice*. Two lattices Λ_1 and Λ_2 are said to be *homothetic* if there is some $\alpha \in \mathbb{C}^*$ such that $\alpha\Lambda_1 = \Lambda_2$. We wish to give a method to determine when two complex lattices are homothetic.

We begin by picking a basis: let λ_1, λ_2 be a $\mathbb{Z}$-basis for Λ as above. We assume throughout that all bases are ordered so that $\operatorname{Im}(\lambda_1/\lambda_2) > 0$. (As we said above, we can not have $\operatorname{Im}(\lambda_1/\lambda_2) = 0$, since then Λ would not contain an $\mathbb{R}$-basis for $\mathbb{C}$. Thus, if $\operatorname{Im}(\lambda_1/\lambda_2) < 0$, we can switch the order of the λ_i to get the imaginary part positive.) Let $\mathfrak{H} = \{z \in \mathbb{C} \mid \operatorname{Im} z > 0\}$ be the upper half-plane and define

$$\mathfrak{j}(\lambda_1, \lambda_2) = \frac{\lambda_1}{\lambda_2} \in \mathfrak{H}.$$

Note that for any $\alpha \in \mathbb{C}^*$,

$$\mathfrak{j}(\alpha\lambda_1, \alpha\lambda_2) = \mathfrak{j}(\lambda_1, \lambda_2),$$

which suggests that $\mathfrak{j}$ is a decent place to start in the classification of lattices up to homotopy.

Unfortunately, $\mathfrak{j}(\lambda_1, \lambda_2)$ depends not only on Λ but also on the choice of basis λ_1, λ_2. In order to use $\mathfrak{j}$ to classify lattices up to homothety we must remove this basis dependence.

We do this by determining the other possible bases for Λ and seeing how $\mathfrak{j}$ depends upon the choice. By standard linear algebra, the bases for Λ are of the form

$$\lambda_1' = a\lambda_1 + b\lambda_2, \lambda_2' = c\lambda_1 + d\lambda_2$$

where

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}_2(\mathbb{Z}),$$

the integer matrices of determinant ± 1. However, as above we want to restrict to only the bases λ_1', λ_2' of Λ ordered so that $\operatorname{Im}(\lambda_1'/\lambda_2') > 0$. One checks easily that the matrices which preserve this condition are precisely those in $\mathrm{SL}_2(\mathbb{Z})$; that is, those of determinant 1. We compute for these bases

$$\mathfrak{j}(a\lambda_1 + b\lambda_2, c\lambda_1 + d\lambda_2) = \frac{a\lambda_1 + b\lambda_2}{c\lambda_1 + d\lambda_2} = \frac{a\mathfrak{j}(\lambda_1, \lambda_2) + b}{c\mathfrak{j}(\lambda_1, \lambda_2) + d}.$$

FIGURE 1. The fundamental domain Y for the $SL_2(\mathbb{Z})$ action on $\mathfrak{H}$

These computations suggest the following approach. We define an action of $SL_2(\mathbb{Z})$ on $\mathfrak{H}$ by

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} z = \frac{az+b}{cz+d};$$

we leave it to the reader to check that this really is a group action. Let us denote by $\mathcal{Y}$ the quotient space of $\mathfrak{H}$ by this action. Recall that this means that $\mathcal{Y}$ consists of the orbits of the $\mathrm{SL}_2(\mathbb{Z})$ action on $\mathfrak{H}$: for any $z \in \mathfrak{H}$, its orbit is simply the set

$$\{\gamma z \mid \gamma \in \mathrm{SL}_2(\mathbb{Z})\}.$$

This action of $\mathrm{SL}_2(\mathbb{Z})$ is defined in such a way that if λ_1, λ_2 and λ_1', λ_2' are two correctly ordered bases of a lattice Λ, then $\mathfrak{j}(\lambda_1, \lambda_2)$ and $\mathfrak{j}(\lambda_1', \lambda_2')$ will lie in the same $\mathrm{SL}_2(\mathbb{Z})$ orbit of $\mathfrak{H}$; that is, they will be equal in $\mathcal{Y}$.

This tells us that if we compose our map

$$\mathfrak{j} : \text{ordered bases of lattices} \to \mathfrak{H}$$

with the quotient map $\mathfrak{H} \to \mathcal{Y}$, we obtain a map

$$\mathfrak{j} : \text{lattices} \to \mathcal{Y};$$

the basis dependence disappears in $\mathcal{Y}$ by our argument above. Furthermore, we saw above that $\mathfrak{j}$ is invariant under multiplying bases by constants; it follows that $\mathfrak{j}$ yields a well-defined map

$$\mathfrak{j} : \text{homothety classes of lattices} \to \mathcal{Y}.$$

By this we mean that if Λ and Λ' are homothetic, then $\mathfrak{j}(\Lambda) = \mathfrak{j}(\Lambda')$.

This map $\mathfrak{j}$ is easily seen to be surjective and it can also be shown to be injective. Thus $\mathfrak{j}$ establishes a set bijection between homothety classes of lattices and $\mathcal{Y}$. This means that if we have a good description of $\mathcal{Y}$ then we will have a good classification of lattices up to homothety. This description comes from the following result.

PROPOSITION 3.1. *Define*

$$Y = \left\{ z \in \mathbb{C}; \operatorname{Im} z > 0, \frac{-1}{2} < \operatorname{Re}(z) < \frac{1}{2}, |z| > 1 \right\} \cup \left\{ z \in \mathbb{C}; |z| = 1, 0 \le \operatorname{Re}(z) < \frac{1}{2} \right\} \cup \left\{ z \in \mathbb{C}; \operatorname{Re}(z) = \frac{1}{2}, \operatorname{Im}(z) \ge \frac{\sqrt{3}}{2} \right\}.$$

Then Y contains exactly one element of each $\mathrm{SL}_2(\mathbb{Z})$ orbit of $\mathfrak{H}$; that is, Y is in natural bijection with $\mathcal{Y}$.

PROOF. See [**17**, Chapter 7, Section 1.2] or [**18**, Proposition 1.5]. □

The last thing we need is a good way to determine which element of Y an element of $\mathfrak{H}$ corresponds to.

PROPOSITION 3.2. *Set*

$$S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}.$$

Then S and T generate $\mathrm{SL}_2(\mathbb{Z})$.

PROOF. See [**17**, Chapter 7, Section 1.2] or [**18**, Proposition 1.5]. □

Note that $S(z) = -\frac{1}{z}$ and $T(z) = z + 1$.

These results give us the following algorithm for determining the homothety class of a lattice Λ with basis λ_1, λ_2. First, compute $\mathfrak{j} = \mathfrak{j}(\Lambda) = \lambda_1/\lambda_2$. We want to modify $\mathfrak{j}$ by S and T to get it into Y. If $\operatorname{Im} \mathfrak{j} < 0$, replace $\mathfrak{j}$ by $1/\mathfrak{j}$; this corresponds to swapping the two basis elements. Now, if $\mathfrak{j}$ is in Y, then we are done. If $\mathfrak{j}$ is not in Y, then first add an integer m to $\mathfrak{j}$ so that

$$\frac{-1}{2} < \operatorname{Re}(\mathfrak{j} + m) \leq \frac{1}{2}.$$

If $\mathfrak{j} + m \in Y$, then we are done. If not, replace $\mathfrak{j} + m$ by $-\frac{1}{\mathfrak{j}+m}$ and start over. Proposition 3.2 (or more honestly its proof) guarantees that this will eventually yield an element of Y.

EXAMPLE 3.3. Let $\Lambda = 5\mathbb{Z} + (1+i)\mathbb{Z}$. We compute

$$\mathfrak{j}(\Lambda) = \frac{5}{1+i} = \frac{5}{2} - \frac{5}{2}i,$$

so we replace it by

$$\frac{1}{\mathfrak{j}(\Lambda)} = \frac{1}{5} + \frac{1}{5}i \in \mathfrak{H}$$

This does not yet lie in Y, as it has absolute value < 1. Since its real part is already between $-\frac{1}{2}$ and $\frac{1}{2}$, we replace it by its negative reciprocal, which is

$$-\frac{5}{2} + \frac{5}{2}i.$$

Adding 3 to this we obtain the element

$$\frac{1}{2} + \frac{5}{2}i$$

of Y.

Suppose that we used the basis $23+3i = 4(5)+3(1+i), 17+2i = 3(5)+2(1+i)$ of Λ instead. We compute

$$\mathfrak{j}(\Lambda) = \frac{23+3i}{17+2i} = \frac{397}{293} + \frac{5}{293}i.$$

Subtracting 1 yields $\frac{104}{293} + \frac{5}{293}i$, which has absolute value < 1. Its negative reciprocal is

$$\frac{-104}{37} + \frac{5}{37}i;$$

adding 3 yields

$$\frac{7}{37} + \frac{5}{37}i,$$

which still has absolute value < 1. Its negative reciprocal is

$$-\frac{7}{2} + \frac{5}{2}i;$$

adding 4 yields

$$\frac{1}{2} + \frac{5}{2}i \in Y,$$

as before.

3.2. Ideal generators and lattice generators. In order to take advantage of our lattice classification of the previous section we need a method to go from ideal generators to lattice generators. That is, given an ideal $\mathfrak{a} = (a_1, a_2)$ we want to find a $\mathbb{Z}$-basis for $\mathfrak{a}$. The general algorithm is little more than Gaussian elimination: we know that a_1, a_2 form a set of $\mathbb{Z}[\alpha]$-generators for $\mathfrak{a}$, so $a_1, a_1\alpha, a_2, a_2\alpha$ form a set of $\mathbb{Z}$-generators for $\mathfrak{a}$. Write all four out in terms of the basis $1, \alpha$ of $\mathcal{O}_K$. Now perform your favorite Gaussian elimination algorithm on these four vectors to obtain a two vector basis; one must remember that since we are working only with $\mathbb{Z}$-modules and not with vector spaces, the only scalars allowed are integers.

EXAMPLE 3.4. Take $K = \mathbb{Q}(\sqrt{-5})$ and $\mathfrak{a} = (10, \alpha + 5)$, where $\alpha = \sqrt{-5}$. Then $10, 10\alpha, 5 + \alpha, (5 + \alpha)\alpha = -5 + 5\alpha$ are $\mathbb{Z}$-generators for $\mathfrak{a}$; thus we wish to perform Gaussian elimination on the matrix

$$\begin{bmatrix} 10 & 0 & 5 & -5 \\ 0 & 10 & 1 & 5 \end{bmatrix}.$$

Adding -5 times the third column to the last column yields

$$\begin{bmatrix} 10 & 0 & 5 & 20 \\ 0 & 10 & 1 & 0 \end{bmatrix}.$$

Subtracting twice the first column from the last column now eliminates the last column. Subtracting 10 times the third column from the second column yields

$$\begin{bmatrix} 10 & -50 & 5 \\ 0 & 0 & 1 \end{bmatrix}.$$

Finally, adding 5 times the first column to the second column shows that the ideal generators $10, \alpha + 5$ are also a lattice basis for $\mathfrak{a}$.

In fact, it very often (but possibly not always; I haven't yet found a counterexample, but it seems that there could be one) happens that the "natural" ideal generators are also a lattice basis. For example, Exercise 4.3 shows that if $\mathfrak{p} = (p, \alpha + m)$ is a prime ideal of $\mathcal{O}_K$, then p and $\alpha + m$ are a lattice basis for $\mathfrak{p}$.

Note also that if $\mathfrak{a} = \big(a\big)$ is a principal ideal, then $\mathfrak{a}$ has lattice basis $a, a\alpha$.

3.3. Computing ideal class groups. We now have all of the tools we will need to compute ideal class groups of imaginary quadratic fields. Let $K = \mathbb{Q}(\sqrt{d})$ and define α and $f(x)$ as before. The first step is to determine generators for the ideal class group. To do this, compute the Minkowski bound: for imaginary quadratic fields, it works out as

$$\mu_K = \begin{cases} \frac{4}{\pi}\sqrt{-d} & d \equiv 2, 3 \pmod 4 \\ \frac{2}{\pi}\sqrt{-d} & d \equiv 1 \pmod 4). \end{cases}$$

Next, for every positive rational prime $p \leq \mu_K$, determine the factorization of p into primes of $\mathcal{O}_K$ as in Chapter 3, Section 1.1. If p is inert, then the ideal $p\mathcal{O}_K$ is principal, so it is irrelevant in computing the ideal class group. Thus we need only consider those p which split or ramify. Let P_0 be the set of primes of $\mathcal{O}_K$ lying over these p.

We claim that P_0 contains generators for the ideal class group $\mathcal{C}_K$. To see this, let $\mathfrak{A}$ be any ideal class. We know that there is some $\mathfrak{a} \in \mathfrak{A}$ with $\mathrm{N}_{K/\mathbb{Q}}(\mathfrak{a}) \leq \mu_K$. By unique factorization of ideals, $\mathfrak{a}$ factors into prime ideals, and each such prime must have norm $\leq \mu_K$. Thus $\mathfrak{a}$ can be written as a product of primes of norm

$\leq \mu_K$; this shows that the ideal class $\mathfrak{A}$ is generated by ideal classes of primes in P_0, and thus that P_0 generates $\mathcal{C}_K$.

The next step is to determine which of these generators are equal in the ideal class group. First one computes $\mathfrak{j}(\mathcal{O}_K) \in Y$ and $\mathfrak{j}(\mathfrak{p}) \in Y$ for each $\mathfrak{p} \in P_0$. If for any $\mathfrak{p}, \mathfrak{q} \in P_0$ one has $\mathfrak{j}(\mathfrak{p}) = \mathfrak{j}(\mathfrak{q})$, then we know that $\mathfrak{p}$ and $\mathfrak{q}$ are homothetic as complex lattices. That is, there is an $\alpha \in \mathbb{C}^*$ such that $\mathfrak{p} = \alpha\mathfrak{q}$. One shows easily that α must actually lie in K^* (see Exercise 4.4) so $\mathfrak{p} \sim \mathfrak{q}$. Thus $\mathfrak{p}$ and $\mathfrak{q}$ are equal in $\mathcal{C}_K$, and one must only include one of $\mathfrak{p}$ and $\mathfrak{q}$ as a generator of $\mathcal{C}_K$. Similarly, if $\mathfrak{j}(\mathfrak{p}) = \mathfrak{j}(\mathcal{O}_K)$, then $\mathfrak{p}$ is trivial in $\mathcal{C}_K$, and thus irrelevant to the computation. Let P_1 be a set containing one element of P_0 for each $\mathfrak{j}$-value obtained; P_1 still generates $\mathcal{C}_K$ and its elements are distinct in $\mathcal{C}_K$.

From here one needs to compute the full group $\mathcal{C}_K$ simultaneously with a multiplication table. Note first of all that we already know the inverses of every element of P_1, since for each $\mathfrak{p} \in P_1$ there is a $\mathfrak{p}' \in P_0$ such that $\mathfrak{p}\mathfrak{p}' = (p)$ is principal. If $\mathfrak{p}$ and $\mathfrak{q}$ are two primes of P_1 which are not inverses, we compute first ideal generators of $\mathfrak{p}\mathfrak{q}$, and from these we compute a lattice basis. We then determine $\mathfrak{j}(\mathfrak{p}\mathfrak{q}) \in Y$. If this equals $\mathfrak{j}(\mathfrak{a})$ for some ideal we have already computed, then we have $\mathfrak{p}\mathfrak{q} \sim \mathfrak{a}$ in $\mathcal{C}_K$. Otherwise we obtain a new element of $\mathcal{C}_K$ which we add to the multiplication table. From here one continues until every possible product has been determined; often one can use previously determined relations to determine others and thus simplify the computations. The end result is a multiplication table for the ideal class group $\mathcal{C}_K$, together with the $\mathfrak{j}$-invariants of each ideal class.

Note that as a special case of this algorithm we get a simple method to determine if an ideal is principal: simply compute a lattice basis, from that compute its $\mathfrak{j}$-invariant, and compare it to $\mathfrak{j}(\mathcal{O}_K)$; they will be equal if and only if the ideal is principal. More generally one can determine which element of the ideal class group a given ideal is equivalent to in the same manner.

3.4. Example : $\mathbb{Q}(\sqrt{-14})$. Take $K = \mathbb{Q}(\sqrt{-14})$. In this section we will compute $\mathcal{C}_K$. We compute $\mu_K \approx 4.764026148$, so the only primes we need consider are 2 and 3. $2\mathcal{O}_K$ factors as

$$2\mathcal{O}_K = \left(2, \sqrt{-14}\right)^2$$

and $3\mathcal{O}_K$ factors as

$$3\mathcal{O}_K = \left(3, \sqrt{-14}+1\right)\left(3, \sqrt{-14}+2\right).$$

Set $\mathfrak{a}_1 = \mathcal{O}_K$, $\mathfrak{a}_2 = \left(2, \sqrt{-14}\right)$, $\mathfrak{a}_3 = \left(3, \sqrt{-14}+1\right)$, $\mathfrak{a}_3' = \left(3, \sqrt{-14}+2\right)$.

We now compute $\mathfrak{j}$ of each of these ideals. We have

$$\mathfrak{j}(\mathfrak{a}_1) = \sqrt{14}i.$$

By Exercise 4.3 we know that 2 and $\sqrt{-14}$ are a lattice basis for $\mathfrak{a}_2$, so we find that

$$\mathfrak{j}(\mathfrak{a}_2) = \frac{\sqrt{14}}{2}i.$$

Similar computations for $\mathfrak{a}_3$ and $\mathfrak{a}_3'$ yield

$$\mathfrak{j}(\mathfrak{a}_3) = \frac{1}{3} + \frac{\sqrt{14}}{3}i;$$

$$\mathfrak{j}(\mathfrak{a}_3') = -\frac{1}{3} + \frac{\sqrt{14}}{3}i.$$

Thus all three generators are distinct in $\mathcal{C}_K$.

We now compute products. We already have the multiplication table

	$\mathfrak{a}_1$	$\mathfrak{a}_2$	$\mathfrak{a}_3$	$\mathfrak{a}_3'$
$\mathfrak{a}_1$	$\mathfrak{a}_1$	$\mathfrak{a}_2$	$\mathfrak{a}_3$	$\mathfrak{a}_3'$
$\mathfrak{a}_2$	$\mathfrak{a}_2$	$\mathfrak{a}_1$		
$\mathfrak{a}_3$	$\mathfrak{a}_3$			$\mathfrak{a}_1$
$\mathfrak{a}_3'$	$\mathfrak{a}_3'$		$\mathfrak{a}_1$	

We compute

$$\begin{aligned}\mathfrak{a}_2\mathfrak{a}_3 &= \big(2,\alpha\big)\big(3,\alpha+1\big)\\ &= \big(6, 2\alpha+2, 3\alpha, \alpha^2+\alpha\big)\\ &= \big(6, 2\alpha+2, 3\alpha, \alpha-14\big)\\ &= \big(6, \alpha+4\big).\end{aligned}$$

Call this ideal $\mathfrak{a}$. One easily checks that 6 and $\alpha+4$ are a lattice basis of $\mathfrak{a}$, so we compute

$$\mathfrak{j}(\mathfrak{a}) = -\frac{1}{3} + \frac{\sqrt{14}}{2}i.$$

Thus $\mathfrak{a}_2\mathfrak{a}_3 \sim \mathfrak{a}_3'$ in $\mathcal{C}_K$. This also allows us to compute

$$\begin{aligned}(\mathfrak{a}_3')^2 &\sim \mathfrak{a}_2\mathfrak{a}_3\mathfrak{a}_3' \sim \mathfrak{a}_2;\\ \mathfrak{a}_2\mathfrak{a}_3' &\sim \mathfrak{a}_2^2\mathfrak{a}_3 \sim \mathfrak{a}_3;\\ \mathfrak{a}_3^2 &\sim \mathfrak{a}_2\mathfrak{a}_3'\mathfrak{a}_3 \sim \mathfrak{a}_2.\end{aligned}$$

Thus we can fill in our multiplication table:

	$\mathfrak{a}_1$	$\mathfrak{a}_2$	$\mathfrak{a}_3$	$\mathfrak{a}_3'$
$\mathfrak{a}_1$	$\mathfrak{a}_1$	$\mathfrak{a}_2$	$\mathfrak{a}_3$	$\mathfrak{a}_3'$
$\mathfrak{a}_2$	$\mathfrak{a}_2$	$\mathfrak{a}_1$	$\mathfrak{a}_3'$	$\mathfrak{a}_3$
$\mathfrak{a}_3$	$\mathfrak{a}_3$	$\mathfrak{a}_3'$	$\mathfrak{a}_2$	$\mathfrak{a}_1$
$\mathfrak{a}_3'$	$\mathfrak{a}_3'$	$\mathfrak{a}_3$	$\mathfrak{a}_1$	$\mathfrak{a}_2$

Since every possible product of generators is now accounted for, we find that $\mathcal{C}_K \cong \mathbb{Z}/4\mathbb{Z}$ and $h_K = 4$.

3.5. Example : $\mathbb{Q}(\sqrt{-119})$. For a second example, take $K = \mathbb{Q}(\sqrt{-119})$, so that $\alpha = \frac{1+\sqrt{-119}}{2}$ and $f(x) = x^2 - x + 30$. (In particular, $\alpha^2 = \alpha - 30$.) The Minkowski bound is $\mu_K \approx 6.94470182322$, so we must check the rational primes 2, 3 and 5. We find that

$$\begin{aligned}(2) &= \big(2,\alpha\big)\big(2,\alpha+1\big);\\ (3) &= \big(3,\alpha\big)\big(3,\alpha+2\big);\\ (5) &= \big(5,\alpha\big)\big(5,\alpha+4\big).\end{aligned}$$

Set $\mathfrak{a}_1 = \mathcal{O}_K$, $\mathfrak{a}_2 = \big(2,\alpha\big)$, $\mathfrak{a}_2' = \big(2,\alpha+1\big)$, $\mathfrak{a}_3 = \big(3,\alpha\big)$, $\mathfrak{a}_3' = \big(3,\alpha+2\big)$, $\mathfrak{a}_5 = \big(5,\alpha\big)$, $\mathfrak{a}_5' = \big(5,\alpha+4\big)$. We compute (since by Exercise 4.3 we know that the ideal generators are a lattice basis)

$$\begin{aligned}
\mathsf{j}(\mathfrak{a}_1) &= \frac{1}{2} + \frac{\sqrt{119}}{2}i;\\
\mathsf{j}(\mathfrak{a}_2) &= \frac{1}{4} + \frac{\sqrt{119}}{4}i;\\
\mathsf{j}(\mathfrak{a}_2') &= -\frac{1}{4} + \frac{\sqrt{119}}{4}i;\\
\mathsf{j}(\mathfrak{a}_3) &= \frac{1}{6} + \frac{\sqrt{119}}{6}i;\\
\mathsf{j}(\mathfrak{a}_3') &= -\frac{1}{6} + \frac{\sqrt{119}}{6}i;\\
\mathsf{j}(\mathfrak{a}_5) &= \frac{1}{10} + \frac{\sqrt{119}}{10}i;\\
\mathsf{j}(\mathfrak{a}_5') &= -\frac{1}{10} + \frac{\sqrt{119}}{10}i.
\end{aligned}$$

Let us begin by determining the powers of $\mathfrak{a}_2$. We find that

$$\mathfrak{a}_2^2 = \big(4, 2\alpha, \alpha^2\big) = \big(4, 2\alpha, \alpha - 30\big) = \big(4, \alpha + 2\big).$$

Call this ideal $\mathfrak{a}_4$. One checks easily that it has lattice basis 4, $\alpha + 2$, so that we can compute

$$\mathsf{j}(\mathfrak{a}_4) = -\frac{3}{8} + \frac{\sqrt{119}}{8}i.$$

Next, we have

$$\begin{aligned}
\mathfrak{a}_2^3 = \mathfrak{a}_2\mathfrak{a}_4 &= \big(2, \alpha\big)\big(4, \alpha + 2\big) = \big(8, 4\alpha, 2\alpha + 4, \alpha^2 + 2\alpha\big)\\
&= \big(8, 4\alpha, 2\alpha + 4, 3\alpha - 30\big) = \big(8, \alpha + 6\big).
\end{aligned}$$

Call this ideal $\mathfrak{a}_8$. It has lattice basis $8, \alpha + 6$, so we compute

$$\mathsf{j}(\mathfrak{a}_8) = \frac{3}{8} + \frac{\sqrt{119}}{8}i.$$

Next, we have

$$\begin{aligned}
\mathfrak{a}_2^4 = \mathfrak{a}_2\mathfrak{a}_8 &= \big(2, \alpha\big)\big(8, \alpha + 6\big) = \big(16, 2\alpha + 12, 8\alpha, \alpha^2 + 6\alpha\big)\\
&= \big(16, 2\alpha + 12, 8\alpha, 7\alpha - 30\big) = \big(16, \alpha - 2\big).
\end{aligned}$$

This ideal has lattice basis 16, $\alpha - 2$, so we compute that it has j-invariant

$$-\frac{1}{4} + \frac{\sqrt{119}}{4}i.$$

Thus $\mathfrak{a}_2^4 \sim \mathfrak{a}_2'$. This also implies that $\mathfrak{a}_2^5 \sim \mathfrak{a}_1$, so we have found a subgroup of order 5 in $\mathcal{C}_K$.

We next compute the powers of $\mathfrak{a}_3$. We have

$$\mathfrak{a}_3^2 = \big(9, 3\alpha, \alpha - 30\big) = \big(9, \alpha + 6\big);$$

this has lattice basis $9, \alpha + 6$, and we compute that it has j-invariant

$$-\frac{3}{8} + \frac{\sqrt{119}}{8}i,$$

so $\mathfrak{a}_3^2 \sim \mathfrak{a}_4$. Thus we immediately know the even powers of $\mathfrak{a}_3$: $\mathfrak{a}_3^4 \sim \mathfrak{a}_4^2 \sim \mathfrak{a}_2'$ (compute this in the cyclic group generated by $\mathfrak{a}_2$), $\mathfrak{a}_3^6 \sim \mathfrak{a}_4^3 \sim \mathfrak{a}_2$, $\mathfrak{a}_3^8 \sim \mathfrak{a}_4^4 \sim \mathfrak{a}_8$, $\mathfrak{a}_3^{10} \sim \mathfrak{a}_4^5 \sim \mathfrak{a}_1$. To compute the odd powers of $\mathfrak{a}_3$ we simply need to multiply each of these by $\mathfrak{a}_3$.

We find that

$$\begin{aligned}\mathfrak{a}_3^3 \sim \mathfrak{a}_3\mathfrak{a}_4 &= (3,\alpha)(4,\alpha+2) = (12, 3\alpha+6, 4\alpha, \alpha^2+2\alpha)\\ &= (12, 3\alpha+6, 4\alpha, 3\alpha-30) = (12, \alpha+6).\end{aligned}$$

This has lattice basis $12, \alpha+6$, and $\mathfrak{j}$-invariant

$$\frac{1}{10} + \frac{\sqrt{119}}{10}i,$$

so $\mathfrak{a}_3^3 \sim \mathfrak{a}_5$. Since $\mathfrak{a}_3$ has order 10 and $\mathfrak{a}_5^{-1} = \mathfrak{a}_5'$, this also tells us that $\mathfrak{a}_3^7 \sim \mathfrak{a}_5'$. Since we also have $\mathfrak{a}_3^9 = \mathfrak{a}_3'$, every generator is a power of $\mathfrak{a}_3$; thus $\mathcal{C}_K$ is cyclic of order 10 with generator $\mathfrak{a}_3$.

The only remaining power to explicitly compute is $\mathfrak{a}_3^5$. We find that

$$\begin{aligned}\mathfrak{a}_3^5 \sim \mathfrak{a}_3\mathfrak{a}_2' &= (3,\alpha)(2,\alpha+1) = (6, 2\alpha, 3\alpha+3, \alpha^2+\alpha)\\ &= (6, 2\alpha, 3\alpha+3, 2\alpha-30) = (6, \alpha+3).\end{aligned}$$

Call this ideal $\mathfrak{a}_6$. It has lattice basis $6, \alpha+3$, and

$$\mathfrak{j}(\mathfrak{a}_6) = \frac{5}{12} + \frac{\sqrt{119}}{12}i.$$

This completes the calculation of $\mathcal{C}_K$.

3.6. Imaginary quadratic fields of class number 1. We have already seen a few imaginary quadratic fields with class number 1: $\mathbb{Q}(i)$, $\mathbb{Q}(\sqrt{-2})$, and $\mathbb{Q}(\sqrt{-3})$. It turns out that there are exactly 6 more imaginary quadratic fields of class number 1. They are $\mathbb{Q}(\sqrt{-7})$, $\mathbb{Q}(\sqrt{-11})$, $\mathbb{Q}(\sqrt{-19})$, $\mathbb{Q}(\sqrt{-43})$, $\mathbb{Q}(\sqrt{-67})$ and $\mathbb{Q}(\sqrt{-163})$. It is quite easy using our techniques to show that these all have class number 1. We will do the case of $K = \mathbb{Q}(\sqrt{-163})$, which is the most interesting.

In this case we find that $\mu_K \approx 8.12781715683$, so we must check the primes 2, 3, 5 and 7. Recall that an odd rational prime p is inert in $\mathcal{O}_K$ if and only if we have

$$\left(\frac{-163}{p}\right) = -1.$$

We compute

$$\begin{aligned}\left(\frac{-163}{3}\right) &= \left(\frac{2}{3}\right) = -1;\\ \left(\frac{-163}{5}\right) &= \left(\frac{2}{5}\right) = -1;\\ \left(\frac{-163}{7}\right) &= \left(\frac{5}{7}\right) = -1.\end{aligned}$$

Thus none of these primes split in $\mathcal{O}_K$. For $p = 2$, we need to determine the factorization of $x^2 - x + 41$ in $\mathbb{F}_2[x]$; it is irreducible, so 2 doesn't split either. Thus our set of generators of $\mathcal{C}_K$ is trivial, so $\mathcal{C}_K$ itself must be trivial.

Continuing the Legendre symbol calculations above, one finds that $\left(\frac{-163}{p}\right) = -1$ for all $p \leq 37$. This has an amusing consequence. Consider the polynomial

$f(x) = x^2 - x + 41$. It has been observed that this polynomial yields primes with remarkable frequency; in fact, it yields a prime for each of $x = 1, \dots, 40$. Using the Legendre symbol calculations we can give a quick proof of this.

Let x_0 be an integer and suppose that some prime p divides $f(x_0)$. Then

$$x_0^2 - x_0 + 41 \equiv 0 \pmod p.$$

Thus

$$(2x_0 - 1)^2 \equiv -163 \pmod p,$$

so $\left(\frac{-163}{p}\right) = 0$ or 1. But we have shown that this does not happen for any $p \leq 37$. Thus no $p \leq 37$ divides $f(x_0)$ for any x_0.

Next, note that $f(x)$ is positive and increasing for $x > 1/2$ and $f(40) = 1601 < 41^2$; thus $|f(x)| < 41^2$ for all $1 \leq x \leq 40$. It follows that if $f(x)$ is not prime for such x, then $f(x)$ is divisible by some prime ≤ 37. Since we showed above that this does not happen, every value $f(x)$ with $1 \leq x \leq 40$ must be prime. More generally, the fact that values $f(x)$ are not divisible by any small primes suggests that they should be prime unusually often.

It is much harder to show that the above are the only imaginary quadratic fields with class number 1; this was proved only in 1967 by Stark.

The case of real quadratic fields is quite different; in fact, it is conjectured that most real quadratic fields have class number 1.

4. Applications to quadratic forms

4.1. Example : $\mathbb{Q}(\sqrt{-5})$. Our explicit calculations of ideal class groups of imaginary quadratic fields can be used to yield some interesting refinements of our earlier results on quadratic forms. We begin with the case $K = \mathbb{Q}(\sqrt{-5})$ to illustrate the basic idea. Recall that we related this field to the quadratic form $x^2 + 5y^2$; we showed that an (unramified) positive rational prime p could be represented by this quadratic form if and only if it split into principal primes in $\mathcal{O}_K$. Unfortunately, we had no good characterization of which primes these were; that $\left(\frac{-5}{p}\right) = 1$ is a necessary condition, but it is not sufficient.

We will approach this problem from a different point of view in this section. Specifically, we will construct a second quadratic form which will represent any p with $\left(\frac{-5}{p}\right) = 1$ which $x^2 + 5y^2$ does not represent. In other words, we will show that there is a second quadratic form $q'(x, y)$ such that every positive rational prime p with $\left(\frac{-5}{p}\right) = 1$ can be represented by at least one of $x^2 + 5y^2$ and $q'(x, y)$. Furthermore, no primes with $\left(\frac{-5}{p}\right) = -1$ will be represented by either quadratic form.

We assume throughout this section that all primes are distinct from 2 and 5, the two primes which ramify in $K/\mathbb{Q}$.

We first need to compute the ideal class group. One checks easily that $h_K = 2$, with $\mathfrak{a}_2 = \left(2, \sqrt{-5} + 1\right)$ a representative of the non-trivial element of $\mathcal{C}_K$. In particular, we have the j-invariants

$$\mathsf{j}(\mathcal{O}_K) = \sqrt{5}i;$$
$$\mathsf{j}(\mathfrak{a}_2) = \frac{1}{2} + \frac{1}{2}\sqrt{5}i.$$

Now, let p be a prime of $\mathbb{Z}$ which splits in $\mathcal{O}_K$; recall that we know that this occurs if and only if $\left(\frac{-5}{p}\right) = 1$. Let $\mathfrak{p} = \left(p, \sqrt{-5} + m\right)$ be one of the primes of $\mathcal{O}_K$ lying over p. Recall that to compute $\mathfrak{j}(\mathfrak{p})$ (using Exercise 4.3) we begin by computing

$$\frac{\sqrt{-5}+m}{p} = \frac{m}{p} + \frac{1}{p}\sqrt{5}i$$

and then applying appropriate elements of $\mathrm{SL}_2(\mathbb{Z})$ to get the value into the fundamental domain Y.

Suppose first that $\mathfrak{p}$ is actually principal. This means that $\mathfrak{p} \sim \mathcal{O}_K$, so $\mathfrak{j}(\mathfrak{p}) = \sqrt{5}i$ in the quotient space $\mathcal{Y}$. By definition of $\mathcal{Y}$ this means that there is some matrix

$$\begin{pmatrix} a & b \\ y & x \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$$

(the reason that we have chosen these strange variable names will become apparent later) such that

$$\begin{pmatrix} a & b \\ y & x \end{pmatrix}\left(\sqrt{5}i\right) = \frac{m}{p} + \frac{1}{p}\sqrt{5}i.$$

Expanding out the $\mathrm{SL}_2(\mathbb{Z})$ action, this tells us that

$$\begin{aligned} \frac{m}{p} + \frac{1}{p}\sqrt{5}i &= \frac{a(\sqrt{5}i)+b}{y(\sqrt{5}i)+x} \\ &= \frac{(a\sqrt{5}i+b)(-y\sqrt{5}i+x)}{(y\sqrt{5}i+x)(-y\sqrt{5}i+x)} \\ &= \frac{5ay+bx}{x^2+5y^2} + \frac{ax-by}{x^2+5y^2}\sqrt{5}i. \end{aligned}$$

Equating imaginary parts and using the fact that $ax - by = 1$ now tells us that

$$x^2 + 5y^2 = p.$$

That is, if $\mathfrak{p}$ is principal then we can find integer solutions to the quadratic form $x^2+5y^2 = p$. Of course, this isn't terribly surprising; it just duplicates one direction of Proposition III.1.7.

More interesting is the case where $\mathfrak{p}$ is not principal. This time we have $\mathfrak{p} \sim \mathfrak{a}_2$, so $\mathfrak{j}(\mathfrak{p}) = \frac{1}{2} + \frac{1}{2}\sqrt{5}i$ in $\mathcal{Y}$. Again, this tells us that there is a matrix

$$\begin{pmatrix} a & b \\ y & x \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$$

such that

$$\begin{pmatrix} a & b \\ y & x \end{pmatrix}\left(\frac{1}{2} + \frac{1}{2}\sqrt{5}i\right) = \frac{m}{p} + \frac{1}{p}\sqrt{5}i.$$

Expanding this out we find that

$$\begin{aligned}
\frac{m}{p}+\frac{1}{p}\sqrt{5}i &= \frac{a\left(\frac{1}{2}+\frac{1}{2}\sqrt{5}i\right)+b}{y\left(\frac{1}{2}+\frac{1}{2}\sqrt{5}i\right)+x} \\
&= \frac{\left(\frac{a}{2}+b\right)+\frac{a}{2}\sqrt{5}i}{\left(\frac{y}{2}+x\right)+\frac{y}{2}\sqrt{5}i} \\
&= \frac{\left[\left(\frac{a}{2}+b\right)+\frac{a}{2}\sqrt{5}i\right]\left[\left(\frac{y}{2}+x\right)-\frac{y}{2}\sqrt{5}i\right]}{\left[\left(\frac{y}{2}+x\right)+\frac{y}{2}\sqrt{5}i\right]\left[\left(\frac{y}{2}+x\right)-\frac{y}{2}\sqrt{5}i\right]} \\
&= \frac{\cdot}{\left(\frac{y}{2}+x\right)^2+\frac{5}{4}y^2}+\frac{\left(\frac{a}{2}+b\right)\frac{-y}{2}+\frac{a}{2}\left(\frac{y}{2}+x\right)}{\left(\frac{y}{2}+x\right)^2+\frac{5}{4}y^2}\sqrt{5}i
\end{aligned}$$

where the $\cdot$ is some real number which we don't need to evaluate. Equating imaginary parts gives

$$\begin{aligned}
\frac{1}{p} &= \frac{\left(\frac{a}{2}+b\right)\frac{-y}{2}+\frac{a}{2}\left(\frac{y}{2}+x\right)}{\left(\frac{y}{2}+x\right)^2+\frac{5}{4}y^2} \\
\left(\frac{y}{2}+x\right)^2+\frac{5}{4}y^2 &= p\left(\left(\frac{a}{2}+b\right)\frac{-y}{2}+\frac{a}{2}\left(\frac{y}{2}+x\right)\right) \\
\frac{1}{4}y^2+xy+x^2+\frac{5}{4}y^2 &= p\left(\frac{-ay}{4}+\frac{-by}{2}+\frac{ay}{4}+\frac{ax}{2}\right) \\
x^2+xy+\frac{3}{2}y^2 &= p\left(\frac{ax-by}{2}\right) \\
x^2+xy+\frac{3}{2}y^2 &= \frac{p}{2}.
\end{aligned}$$

Thus

$$2x^2+2xy+3y^2=p.$$

In particular, p can be represented by the quadratic form $2x^2+2xy+3y^2$.

Let us summarize our results to this point. We begin with any positive rational prime p such that $\left(\frac{-5}{p}\right)=1$; it necessarily splits as $\mathfrak{p}\mathfrak{p}'$ for some prime ideal $\mathfrak{p},\mathfrak{p}'$ of $\mathcal{O}_K$. These ideals must either both be in the ideal class of $\mathfrak{a}_1$ or in the ideal class of $\mathfrak{a}_2$; in the first case we have shown that we can write

$$p=x^2+5y^2$$

and in the second case we have shown that we can write

$$p=2x^2+2xy+3y^2.$$

Thus, if all we know is that $\left(\frac{-5}{p}\right)=1$ but not which ideal class $\mathfrak{p}$ actually belongs to, we can already say that p can be represented by at least one of these two quadratic forms.

Let us now show that these are the only p which are represented by these quadratic forms. That is, we want to show that if p is represented by one of these quadratic forms, then $\left(\frac{-5}{p}\right)=1$. (Remember that we are assuming $p\neq 2,5$.) We already know this for x^2+5y^2, so we just need to show it for $2x^2+2xy+3y^2$. The case $p=3$ is easy, so we assume $p\neq 3$. Suppose that we have

$$2x^2+2xy+3y^2=p.$$

We can not have x or y divisible by p, for the other would then have to be divisible by p as well (this is where we use $p \neq 3$), and then the entire left-hand side would be divisible by p^2. In particular, y must be invertible modulo p, so

$$\begin{aligned} 0 &\equiv 2x^2 + 2xy + 3y^2 \pmod{p} \\ &\equiv 2\left(\frac{x}{y}\right)^2 + 2\left(\frac{x}{y}\right) + 3. \end{aligned}$$

That is, the quadratic equation $2t^2 + 2t + 3$ has a root modulo p. On the other hand, the quadratic formula tells us that the roots of this equation are

$$\frac{-4 \pm \sqrt{4 - 24}}{4} = -1 \pm \sqrt{-5}.$$

Thus $2t^2 + 2t + 3$ has roots if and only if -5 is a square modulo p; that is, if and only if $\left(\frac{-5}{p}\right) = 1$. Combining these two facts shows that if p can be represented by $2x^2 + 2xy + 3y^2$, then $\left(\frac{-5}{p}\right) = 1$.

To make this result slightly better, let us determine which primes p have $\left(\frac{-5}{p}\right) = 1$. We have

$$\left(\frac{-5}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{5}{p}\right).$$

Since $5 \equiv 1 \pmod{4}$, quadratic reciprocity tells us that $\left(\frac{5}{p}\right) = \left(\frac{p}{5}\right)$; thus

$$\left(\frac{-5}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{p}{5}\right).$$

These Legendre symbols evaluate as

$$\left(\frac{-1}{p}\right) = \begin{cases} 1 & p \equiv 1 \pmod{4}; \\ -1 & p \equiv 3 \pmod{4}; \end{cases}$$

and

$$\left(\frac{p}{5}\right) = \begin{cases} 1 & p \equiv 1, 4 \pmod{5}; \\ -1 & p \equiv 2, 3 \pmod{5}. \end{cases}$$

Combining these two computations we find that

$$\left(\frac{-5}{p}\right) = \begin{cases} 1 & p \equiv 1, 3, 7, 9 \pmod{20}; \\ -1 & p \equiv 11, 13, 17, 19 \pmod{20}. \end{cases}$$

Put together, our above computations yield the following theorem.

THEOREM 4.1. *Let $p \neq 2, 5$ be a positive rational prime. Then p can be represented by at least one of the quadratic forms*

$$x^2 + 5y^2, 2x^2 + 2xy + 3y^2$$

if and only if

$$p \equiv 1, 3, 7, 9 \pmod{20}.$$

In fact, it turns out that the first form represents those p such that $p \equiv 1, 9 \pmod{20}$ and the second those such that $p \equiv 3, 7 \pmod{20}$, but the best proof of this requires class field theory.

4.2. The general case. The arguments of the previous section generalize easily. Let $K = \mathbb{Q}(\sqrt{d})$ be an imaginary quadratic field; we begin with the case $d \equiv 2, 3 \pmod 4$. Suppose that $\mathfrak{a}_1, \ldots, \mathfrak{a}_h$ are ideal representatives for its ideal class group. Let p be any positive rational prime such that $\left(\frac{d}{p}\right) = 1$ and let $\mathfrak{p} = \left(p, \sqrt{d} + m\right)$ be one of the primes of $\mathcal{O}_K$ lying over p.

By the definition of the ideal class group we have $\mathfrak{p} \sim \mathfrak{a}_i$ for a unique i. Note that it is clear from our definition of $\mathfrak{j}$ that $\mathfrak{j}(\mathfrak{a}_i) \in K$; thus we can write

$$\mathfrak{j}(\mathfrak{a}_i) = r + s\sqrt{d}$$

for some $r, s \in \mathbb{Q}$. Since $\mathfrak{p} \sim \mathfrak{a}_i$, the definition of $\mathfrak{j}$ tells us that there is some

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$$

such that

$$\begin{pmatrix} a & b \\ y & x \end{pmatrix} \left(r + s\sqrt{d}\right) = \frac{m}{p} + \frac{1}{p}\sqrt{d}.$$

Expanding out the $\mathrm{SL}_2(\mathbb{Z})$ action yields

$$\begin{aligned} \frac{m}{p} + \frac{1}{p}\sqrt{d} &= \frac{a(r + s\sqrt{d}) + b}{y(r + s\sqrt{d}) + x} \\ &= \frac{(ar + b) + as\sqrt{d}}{(yr + x) + ys\sqrt{d}} \\ &= \frac{\left((ar + b) + as\sqrt{d}\right)\left((yr + x) - ys\sqrt{d}\right)}{\left((yr + x) + ys\sqrt{d}\right)\left((yr + x) - ys\sqrt{d}\right)} \\ &= \frac{\cdot}{(yr + x)^2 - dy^2s^2} + \frac{(ar + b)(-ys) + as(yr + x)}{(yr + x)^2 - dy^2s^2}\sqrt{d} \end{aligned}$$

where $\cdot$ is some real number. Equating imaginary parts yields

$$\begin{aligned} p &= \frac{(yr + x)^2 - dy^2s^2}{(ar + b)(-ys) + as(yr + x)} \\ p\left((ar + b)(-ys) + as(yr + x)\right) &= (yr + x)^2 - dy^2s^2 \\ p(-arsy - bsy + arsy + asx) &= r^2y^2 + 2rxy + x^2 - ds^2y^2 \\ ps(ax - by) &= r^2y^2 + 2rxy + x^2 - ds^2y^2 \\ p &= \frac{1}{s}x^2 + \frac{2r}{s}xy + \frac{r^2 - ds^2}{s}y^2, \end{aligned}$$

using the fact that $ax - by = 1$. Note that the quadratic form depends only on r and s; that is, only on $\mathfrak{j}(\mathfrak{a}_i)$. We have therefore shown that if $\mathfrak{p} \sim \mathfrak{a}_i$, then p can be represented by the quadratic form

$$\frac{1}{s}x^2 + \frac{2r}{s}xy + \frac{r^2 - ds^2}{s}y^2.$$

Since every prime $\mathfrak{p}$ lying over a rational prime p with $\left(\frac{d}{p}\right) = 1$ is equivalent to some $\mathfrak{a}_j$, we obtain the following theorem. We will say that a prime p is *relatively prime* to a rational number q if p does not divide the numerator or denominator of q (in lowest terms).

THEOREM 4.2. *Let $d \equiv 2, 3 \pmod 4$ be a negative integer and let $\mathfrak{a}_1, \ldots, \mathfrak{a}_h$ be representatives for the ideal classes in $\mathbb{Q}(\sqrt{d})$. Write*

$$\mathfrak{j}(\mathfrak{a}_i) = r_i + s_i\sqrt{d}.$$

Then every positive rational prime p such that $\left(\frac{d}{p}\right) = 1$ can be represented by at least one of the h quadratic forms

$$\frac{1}{s_i}x^2 + \frac{2r_i}{s_i}xy + \frac{r_i^2 - ds_i^2}{s_i}y^2.$$

Furthermore, let p be a prime which is relatively prime to all of the coefficients of all of these quadratic forms and which is not ramified in $\mathbb{Q}(\sqrt{d})$. If for such a p we have $\left(\frac{d}{p}\right) = -1$, then p can not be represented by any of these quadratic forms.

PROOF. The only new information is the last statement. So let p be a positive rational prime which is relatively prime to all of the coefficients. Suppose that p can be represented as

$$\frac{1}{s}x^2 + \frac{2r}{s}xy + \frac{r^2 - ds^2}{s}y^2 = p$$

for some $x, y \in \mathbb{Z}$, with $(r, s) = (r_i, s_i)$ for some i. We must show that $\left(\frac{d}{p}\right) = 1$.

Note that under the hypothesis that p is relatively prime to the coefficients we must have both x and y relatively prime to p; if one were not, then the other would also be divisible by p and the entire left-hand side of the expression would be divisible by p^2. In particular, we must have that y is invertible modulo p. The representation above yields a solution to the congruence

$$\begin{aligned} 0 &\equiv \frac{1}{s}x^2 + \frac{2r}{s}xy + \frac{r^2 - ds^2}{s}y^2 \pmod p \\ 0 &\equiv \left(\frac{x}{y}\right)^2 + 2r\left(\frac{x}{y}\right) + r^2 - ds^2. \end{aligned}$$

(We can cancel the $\frac{1}{s}$ since by hypothesis p is relatively prime to all of the coefficients of all of the quadratic forms and the coefficient of x^2 is $\frac{1}{s}$.) By the quadratic formula, the roots of this are

$$\frac{-2r \pm \sqrt{4r^2 - 4(r^2 - ds^2)}}{2} = -r \pm \frac{\sqrt{4ds^2}}{2} = -r \pm s\sqrt{d}.$$

In particular, if p can be represented by the quadratic form, then

$$\frac{1}{s}\left(\frac{x}{y} + r\right)$$

will be a square root of d modulo p. Thus, $\left(\frac{d}{p}\right) = 1$. □

The analysis in the $d \equiv 1 \pmod 4$ case is entirely similar, except that we begin with the ideal

$$\mathfrak{p} = \left(p, m + \frac{1}{2} + \frac{1}{2}\sqrt{d}\right).$$

The only effect this has is removing an additional factor of 2.

THEOREM 4.3. *Let $d \equiv 1 \pmod 4$ be a negative integer and let $\mathfrak{a}_1, \dots, \mathfrak{a}_h$ be representatives for the ideal classes in $\mathbb{Q}(\sqrt{d})$. Write*

$$\mathfrak{j}(\mathfrak{a}_i) = r_i + s_i\sqrt{d}.$$

Then every positive rational prime p such that $\left(\frac{d}{p}\right) = 1$ can be represented by at least one of the h quadratic forms

$$\frac{1}{2s_i}x^2 + \frac{r_i}{s_i}xy + \frac{r_i^2 - ds_i^2}{2s_i}y^2.$$

Furthermore, let p be a prime which is relatively prime to all of the coefficients of all of these quadratic forms and which is not ramified in $\mathbb{Q}(\sqrt{d})$. If for such a p we have $\left(\frac{d}{p}\right) = -1$, then p can not be represented by any of these quadratic forms.

EXAMPLE 4.4. Take $d = -14$. We have already computed the ideal class group of $\mathbb{Q}(\sqrt{-14})$; the possible $\mathfrak{j}$-invariants are

$$\sqrt{-14}, \frac{1}{2}\sqrt{-14}, \frac{1}{3} + \frac{1}{3}\sqrt{-14}, -\frac{1}{3} + \frac{1}{3}\sqrt{-14}.$$

Plugging into our formula, we find that every p such that $\left(\frac{-14}{p}\right)$ can be represented by at least one of the quadratic forms

$$\begin{aligned} &x^2 + 14y^2 \\ &2x^2 + 7y^2 \\ &3x^2 + 2xy + 5y^2 \\ &3x^2 - 2xy + 5y^2. \end{aligned}$$

In fact, we can do slightly better. Note that if p factors as $\mathfrak{p}\mathfrak{p}'$ and $\mathfrak{j}(\mathfrak{p}) = \frac{1}{3} + \frac{1}{3}\sqrt{-14}$, then we must have $\mathfrak{j}(\mathfrak{p}') = -\frac{1}{3} + \frac{1}{3}\sqrt{-14}$, since $\mathfrak{p}$ and $\mathfrak{p}'$ are inverses in $\mathcal{C}_K$. This tells us that p can be represented by both

$$3x^2 + 2xy + 5y^2$$

and

$$3x^2 - 2xy + 5y^2,$$

so we only need one of those quadratic forms to represent all such p. (Note that this is obvious on replacing x by $-x$, as well.)

One can easily use quadratic reciprocity to characterize those p such that $\left(\frac{-14}{p}\right) = 1$; one finds that this occurs if and only if

$$p \equiv 1, 3, 5, 9, 13, 15, 19, 23, 25, 27, 39, 45 \pmod{56}.$$

We conclude that for $p \neq 2, 3, 5, 7$, p can be represented by at least one of

$$x^2 + 14y^2, x^2 + 7y^2, 3x^2 + 2xy + 5y^2$$

if and only if

$$p \equiv 1, 3, 5, 9, 13, 15, 19, 23, 25, 27, 39, 45 \pmod{56}.$$

5. Exercises

EXERCISE 4.1. Let K be a number field with ring of integers $\mathcal{O}_K$. Show that there are $\mathcal{O}_K$-submodules of K which are not finitely generated over $\mathcal{O}_K$.

EXERCISE 4.2. Let K be a number field and let N be a positive integer. Show that there are only finitely many ideals $\mathfrak{a}$ of $\mathcal{O}_K$ with $\mathrm{N}_{K/\mathbb{Q}}(\mathfrak{a}) < N$.

EXERCISE 4.3. Let $K = \mathbb{Q}(\sqrt{d})$ be an imaginary quadratic field and set

$$\alpha = \begin{cases} \sqrt{d} & d \equiv 2, 3 \pmod 4; \\ \frac{1+\sqrt{d}}{2} & d \equiv 1 \pmod 4). \end{cases}$$

Let p be a prime of $\mathbb{Z}$ which splits or ramifies in K and let $\mathfrak{p} = \bigl(p, \alpha + m\bigr)$ be one of the ideals lying over p. Show that p and $\alpha + m$ are a lattice basis for $\mathfrak{p}$.

EXERCISE 4.4. Let $\mathfrak{a}$ and $\mathfrak{b}$ be ideals of an imaginary quadratic field K and let $\gamma \in \mathbb{C}^*$ be such that $\gamma\mathfrak{a} = \mathfrak{b}$. Show that $\gamma \in K^*$.

EXERCISE 4.5. Compute the ideal class group of $\mathbb{Q}(\sqrt{-15})$ and write down a set of quadratic forms which represent every positive rational prime p such that $\left(\frac{-15}{p}\right) = 1$.

EXERCISE 4.6. Compute the ideal class group of $\mathbb{Q}(\sqrt{-26})$.

EXERCISE 4.7. Compute the ideal class group of $\mathbb{Q}(\sqrt{-41})$.

EXERCISE 4.8. Let $K = \mathbb{Q}(\sqrt{d})$ be an imaginary quadratic field. Suppose that $\mathcal{O}_K$ is a PID. Show that either $d = -1, -2, -7$ or $d \equiv 5 \pmod 8$. (Hint: Consider the factorization of 2.)

EXERCISE 4.9. Show that $\mathbb{Q}(\sqrt{10})$ has class number 2.

EXERCISE 4.10. Reduce the proof that $\mathbb{Q}(\zeta_{11})$ is a PID to the assertion that $\mathbb{Z}[\zeta_{11}]$ has an element of norm ± 23.

CHAPTER 5

Fermat's Last Theorem for Regular Primes

1. The theorem

Let p be an odd prime and let $K = \mathbb{Q}(\zeta_p)$. We will write ζ for ζ_p for this section. It was observed early in the 19$^{\text{th}}$ century that this field is intimately connected with Fermat's last theorem. Specifically, if one has an equality

$$x^p + y^p = z^p$$

with $x, y, z \in \mathbb{Z}$, one can use the factorization

$$x^p + y^p = (x+y)(x+\zeta y)(x+\zeta^2 y)\cdots(x+\zeta^{p-1}y)$$

to conclude that

$$(x+y)(x+\zeta y)(x+\zeta^2 y)\cdots(x+\zeta^{p-1}y) = z^p.$$

From here, one shows (with appropriate conditions on x, y, z) that the factors on the left side are pairwise relatively prime. If $\mathcal{O}_K$ is a UFD, it follows that each $x + \zeta^i y$ is a p^{th} power in $\mathcal{O}_K$, since their product is. From here one can easily obtain a contradiction, which shows that Fermat's equation has no non-trivial solution in this case.

This argument was first successfully carried out by Kummer in the mid 19$^{\text{th}}$ century. He realized that his proof applied to not only those p for which $\mathbb{Z}[\zeta_p]$ is a UFD, but also to a much larger class of primes. The key property turned out to be that p not divide the class number $h_{\mathbb{Q}(\zeta_p)}$. Kummer called such primes *regular*; if a prime is not regular, then it is said to be *irregular*.

We will prove Kummer's theorem with the additional simplifying hypothesis that p not divide xyz; this is classically referred to as Case I. Case I contains most of the interesting content of the general case and has the advantage of being far simpler technically.

THEOREM 1.1 (Kummer). *Let $p \geq 5$ be a regular prime. Then the equation*

$$x^p + y^p = z^p$$

has no solutions with $x, y, z \in \mathbb{Z}$ and p not dividing xyz.

PROOF. To begin, note that by Exercise 5.1 we can assume that x and y are not congruent modulo p.

Let $K = \mathbb{Q}(\zeta_p)$. Suppose that there is a solution $x^p + y^p = z^p$. As above we write

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

We first show that the *principal ideals* $\big(x+\zeta^i y\big)$ and $\big(x+\zeta^j y\big)$ have no common factors for $i \neq j$.

LEMMA 1.2. *Suppose $x^p + y^p = z^p$ and p does not divide xyz. Then the ideals $\bigl(x + \zeta^i y\bigr)$ are pairwise relatively prime for $i = 0, \dots, p-1$.*

PROOF. Let i and j be distinct integers between 0 and $p-1$ and suppose that there is some prime ideal $\mathfrak{q}$ of $\mathcal{O}_K$ which divides both $\bigl(x + \zeta^i y\bigr)$ and $\bigl(x + \zeta^j y\bigr)$. $\mathfrak{q}$ therefore also divides the principal ideals

$$\bigl((x + \zeta^i y) - (x + \zeta^j y)\bigr) = \bigl((\zeta^i - \zeta^j)y\bigr)$$

and

$$\bigl((x + \zeta^i y) - \zeta^{i-j}(x + \zeta^j y)\bigr) = \bigl((1 - \zeta^{i-j})x\bigr).$$

(See Exercise 5.2. Note that $\zeta^{i-j}(x+\zeta^j y)$ generates the same ideal as $x+\zeta^j y$ since ζ^{i-j} is a unit.) Recall that since $i \neq j$, $\zeta^i - \zeta^j = \zeta^i(1-\zeta^{j-i})$ and $1-\zeta^{i-j}$ are both associate to $1-\zeta$. We conclude that $\mathfrak{q}$ divides the ideals $\bigl(1-\zeta\bigr)\bigl(x\bigr)$ and $\bigl(1-\zeta\bigr)\bigl(y\bigr)$. However, since x and y are relatively prime in $\mathbb{Z}$ it follows that they can have no prime ideal factors in common in $\mathcal{O}_K$; therefore, the only possibility is $\mathfrak{q} = \bigl(1-\zeta\bigr)$.

Suppose, then, that $\bigl(1-\zeta\bigr)$ divides $\bigl(x + \zeta^i y\bigr)$ and $\bigl(x + \zeta^j y\bigr)$ as ideals. This implies immediately that $1-\zeta$ divides $x+\zeta^i y$ and $x+\zeta^j y$ as elements of $\mathcal{O}_K$. Thus

$$x + \zeta^i y \equiv 0 \pmod{1-\zeta}.$$

We also have $\zeta^i \equiv 1 \pmod{1-\zeta}$, so we conclude that

$$x + y \equiv 0 \pmod{1-\zeta}.$$

However, $x+y$ is a rational integer, so if it is divisible by $1-\zeta$, then it must be divisible by p. (See Lemma II.4.1.)

We have now that p divides $x+y$ in $\mathbb{Z}$. Since

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

it follows that p divides $x^p + y^p$, and therefore that p divides z. This contradicts our assumption that p does not divide xyz (or our assumption that x and y are relatively prime), so we conclude that $\bigl(x + \zeta^i\bigr)$ and $\bigl(x + \zeta^j y\bigr)$ are relatively prime ideals, as claimed. $\square$

Let

$$\bigl(z\bigr) = \mathfrak{q}_1^{n_1} \cdots \mathfrak{q}_r^{n_r}$$

be the ideal factorization of $\bigl(z\bigr)$ in $\mathcal{O}_K$. The equality of ideals

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

shows that

$$\bigl(x+y\bigr)\bigl(x+\zeta y\bigr)\cdots\bigl(x+\zeta^{p-1}y\bigr) = \mathfrak{q}_1^{pn_1}\cdots\mathfrak{q}_r^{pn_r}.$$

Since the ideals $\bigl(x + \zeta^i y\bigr)$ are pairwise relatively prime, each $\mathfrak{q}_i$ must occur in the factorization of exactly one of them. As each $\mathfrak{q}_i$ occurs with multiplicity divisible by p, it follows that every prime factor of each $\bigl(x + \zeta^i y\bigr)$ occurs with multiplicity divisible by p. Put differently, each $\bigl(x + \zeta^i y\bigr)$ is the p^{th} power of some ideal $\mathfrak{a}_i$ of $\mathcal{O}_K$:

$$\bigl(x + \zeta^i y\bigr) = \mathfrak{a}_i^p.$$

We now use the hypothesis that p is regular to conclude that the $\mathfrak{a}_i$ are all principal. Specifically, note that $\mathfrak{a}_i^p$ is trivial in $\mathcal{C}_K$, since it is just the principal ideal $\bigl(x + \zeta^i y\bigr)$. Since p does not divide the order of $\mathcal{C}_K$, this implies that $\mathfrak{a}_i$ itself must be trivial in $\mathcal{C}_K$ (since if $\mathcal{C}_K$ had an element of order p then it would have order divisible by p), and thus principal. Therefore we can write $\mathfrak{a}_i = \big(\alpha_i\big)$ for some $\alpha_i \in \mathcal{O}_K$, and we have the equality of principal ideals.

$$(x + \zeta^i y) = (\alpha_i)^p.$$

This implies that

$$x + \zeta^i y = u\alpha_i^p$$

for some $u \in \mathcal{O}_K^*$. The next step is to get a little more information on the unit u.

LEMMA 1.3. *Let u be a unit of $\mathcal{O}_K$. Then u can be written as $\zeta^a\varepsilon$ with ε a unit of the maximal real subfield of K.*

PROOF. By Exercise II.2.17 we know that $u/\bar{u} = \zeta^b$ for some b, where $\bar{u}$ is the complex conjugate of u. Now choose $a \in \mathbb{Z}$ such that $2a \equiv b \pmod{p}$ and set $\varepsilon = \zeta^{-a}u$. Then $u = \zeta^a\varepsilon$, and

$$\bar{\varepsilon} = \zeta^a\bar{u} = \zeta^a\zeta^{-b}u = \zeta^{-a}u = \varepsilon,$$

so ε is real and thus lies in the maximal real subfield of K. □

We now take $i = 1$; by our results to this point we can write

$$x + \zeta y = \zeta^a\varepsilon\alpha^p$$

for some integer a, some real unit ε and some $\alpha = \alpha_1 \in \mathcal{O}_K$. By Exercise 5.3 we have that $\alpha^p \equiv b \pmod{p}$ for some rational integer b, so we conclude that

$$x + \zeta y \equiv \zeta^a\varepsilon b \pmod{p}.$$

Since ε, b and p are all real, taking complex conjugates yields

$$\overline{x + \zeta y} \equiv \zeta^{-a}\varepsilon b \pmod{p}.$$

As $\overline{x + \zeta y} = x + \zeta^{-1}y$, we find that

$$x + \zeta^{-1}y \equiv \zeta^{-a}\varepsilon b \pmod{p}.$$

Combining these equations we conclude that

$$\zeta^{-a}(x + \zeta y) \equiv \zeta^a(x + \zeta^{-1}y) \pmod{p}$$

which simplifies to

$$x + \zeta y - \zeta^{2a-1}y - \zeta^{2a}x \equiv 0 \pmod{p}.$$

We can use this congruence to obtain our desired contradiction. Suppose first that none of the p^{th} roots of unity 1, ζ, ζ^{2a-1} and ζ^{2a} are equal. Since $p \geq 5$ this implies that these elements are part of an integral basis of $\mathcal{O}_K$. Now the fact that

$$x + \zeta y - \zeta^{2a-1}y - \zeta^{2a}x$$

is divisible by p in $\mathcal{O}_K$ implies that x and y must be divisible by p in $\mathbb{Z}$; this contradicts our assumption that p does not divide xyz, which finishes this case.

This leaves the cases where some of 1, ζ, ζ^{2a-1}, ζ^{2a} are equal. The possibilities are:

(1) $1 = \zeta^{2a-1}$. Then $\zeta = \zeta^{2a}$, so we find that

$$(x-y)+(y-x)\zeta \equiv 0 \pmod{p}.$$

This p divides $(x-y)(1-\zeta)$. As we assumed that x and y were not congruent modulo p, $x-y$ is relatively prime to p; since also p does not divide $1-\zeta$ (they aren't relatively prime, but it doesn't matter) this implies that p can not divide $(x-y)(1-\zeta)$; this is the desired contradiction.

(2) $1 = \zeta^{2a}$. Then $\zeta^{2a-1} = \zeta^{-1}$, so the congruence reduces to

$$\zeta y - \zeta^{-1} y \equiv 0 \pmod{p}.$$

This implies that p divides $y(\zeta - \zeta^{-1}) = -y\zeta^{-1}(1-\zeta^2)$; the fact that p does not divide y now yields a contradiction as in the previous case.

(3) $\zeta = \zeta^{2a-1}$. Then $\zeta^{2a} = \zeta^2$ and the congruence reduces to

$$(1-\zeta^2)x \equiv 0 \pmod{p}.$$

This time p divides $x(1-\zeta^2)$; the fact that p does not divide x now yields the contradiction.

This completes the proof. □

We used the fact that p does not divide xyz in an essential way, but Kummer was able to extend the theorem to the case $p|xyz$; see [**20**, Chapter 9] for a proof.

2. Regular primes

We have not yet given any methods for determining whether or not a prime is regular. In this section we will state some results of Kummer's which give easily computable criteria for regularity.

Define the *Bernoulli numbers* $B_n \in \mathbb{R}$ by the formula

$$\frac{t}{e^t-1} = \sum_{n=0}^{\infty} B_n \frac{t^n}{n!}.$$

Exercise 5.4 shows that $B_n = 0$ if n is odd and > 1. One also has the formula

$$\sum_{k=0}^{n-1} \binom{n}{k} B_k = 0$$

of Exercise 5.5, which makes them easy to compute explicitly and also shows that they are actually in $\mathbb{Q}$. We include a short table; for a more extensive table, see [**20**, pp. 407–409].

Kummer's main results on regular primes are the following theorems. Let h_p be the class number of $\mathbb{Q}(\zeta_p)$ and let h_p^+ be the class number of the maximal real subfield $\mathbb{Q}(\zeta_p + \zeta_p^{-1})$. Recall that h_p^+ divides h_p, and we set $h_p^- = h_p/h_p^+$. In the theorems below, whenever we speak of an integer dividing the numerator of a rational number, we assume that the rational number is written in lowest terms.

THEOREM 2.1 (Kummer). *Let p be an odd prime. Then p divides h_p^- if and only if p divides the numerator of some Bernoulli number B_j with $j = 2, 4, \ldots, p-3$.*

PROOF. See [**8**] for Kummer's original proof or [**20**, Theorem 5.16] for a proof using p-adic L-functions. This theorem has been strengthened by Herbrand, Ribet and Kolyvagin; they have shown that which Bernoulli number p divides gives information on how the Galois group acts on the ideal class group. □

n	Numerator	Denominator
0	1	1
1	-1	2
2	1	6
4	-1	30
6	1	42
8	-1	30
10	5	66
12	-691	2,730
14	7	6
16	$-3,617$	510
18	43,867	798
20	$-174,611$	330
22	854,513	138
24	$-236,364,091$	2,730
26	8,553,103	6
28	$-23,749,461,029$	870
30	8,615,841,276,005	14,322
32	$-7,709,321,041,217$	510
34	2,577,687,858,367	6

THEOREM 2.2 (Kummer). *If p divides h_p^+, then p divides h_p^-.*

PROOF. See [**8**] for Kummer's original proof or [**20**, Theorem 5.34] for a proof using the p-adic class number formula. Although there are infinitely many primes for which p divides h_p^-, there are no known p for which p divides h_p^+. It has been conjectured by Vandiver that this never occurs, although this conjecture is not universally believed. □

COROLLARY 2.3 (Kummer). *p divides h_p if and only if p divides the numerator of some Bernoulli number B_j with $j = 2, 4, \ldots, p-3$.*

Using these results we find that 37 is the first irregular prime; it divides the numerator of B_{32}. The next few irregular primes are 59, 67, 101, 103, 131, 149 and 157. For a longer list see [**20**, pp. 410–411].

We can give a heuristic argument for the percentage of primes which are irregular. Define the *index of irregularity* $i(p)$ to be the number of Bernoulli numbers B_j with $j = 2, 4, \ldots, p-3$ for which p divides the numerator of B_j; thus $i(p) = 0$ if and only if p is regular. Assuming that the Bernoulli numbers are randomly distributed modulo p (meaning that p divides B_j with probability $1/p$), the probability that $i(p) = k$ for some k is

$$\binom{(p-3)/2}{k}\left(1-\frac{1}{p}\right)^{\frac{p-3}{2}-k}\left(\frac{1}{p}\right)^{k}.$$

As p grows this approaches the *Poisson distribution*

$$\frac{\left(\frac{1}{2}\right)^{k} e^{-1/2}}{k!}.$$

Taking $k = 0$ we find that the proportion of regular primes should be $e^{-1/2}$, which is approximately 60.65%. This result agrees very closely with numerical evidence.

Strangely, even though no one has been able to prove that there are infinitely many regular primes, Kummer did succeed in proving that there are infinitely many irregular primes. His proof is based on the following theorems.

THEOREM 2.4 (von Staudt-Clausen). *Let n be even and positive. Then*

$$B_n + \sum_{(p-1)|n} \frac{1}{p}$$

is an integer.

PROOF. See [**20**, Theorem 5.10]. □

THEOREM 2.5 (Kummer). *Let p be a prime and let m and n be even positive integers, not divisible by $p - 1$, with*

$$m \equiv n \pmod{p-1}.$$

Then neither $\frac{B_m}{m}$ nor $\frac{B_n}{n}$ has any factors of p in the denominator, and

$$\frac{B_m}{m} \equiv \frac{B_n}{n} \pmod{p}.$$

PROOF. See [**20**, Corollary 5.14]. □

COROLLARY 2.6 (Kummer). *There are infinitely many irregular primes.*

PROOF. We will suppose that there are only finitely many irregular primes $p_1, p_2, \ldots, p_r$ and obtain a contradiction. Set

$$m = (p_1 - 1)(p_2 - 1) \cdots (p_r - 1).$$

By Exercise 5.9, $|B_{2n}/n|$ goes to infinity as n goes to infinity, so there must be some multiple M of m such that

$$|B_M/M| > 1.$$

Thus there exists some prime p dividing the numerator of $|B_M/M|$. Since $p_i - 1$ divides M for all i, Theorem 2.4 shows that each p_i is in the denominator of B_M; this means that there is no way that p_i could be in the numerator of B_M/M, and thus that $p \neq p_i$ for any i. Similarly, if $p - 1$ were to divide M, then Theorem 2.4 would imply that p was in the denominator of B_M, which can not occur since p is in the numerator of B_M/M. Thus $p - 1$ does not divide M.

We can now apply Theorem 2.5. Specifically, choose M' with $2 \leq M' \leq p - 3$ which is congruent to M modulo $p-1$. Since $p-1$ does not divide M we can apply Theorem 2.5 to conclude that

$$\frac{B_{M'}}{M'} \equiv \frac{B_M}{M} \equiv 0 \pmod{p},$$

since p divides the numerator of B_M/M by assumption. Thus p divides the numerator of $B_{M'}$, so by Corollary 2.3 it is irregular. This contradicts our assumption that there were finitely many irregular primes, and thus proves the corollary. □

3. Exercises

EXERCISE 5.1. Let $p \geq 5$ be a prime and let x, y, z be rational integers, relatively prime to p, such that

$$x^p + y^p = z^p.$$

Show that through reordering and negation, if necessary, one can obtain integers x', y', z', relatively prime to p, such that

$$(x')^p + (y')^p = (z')^p$$

and x' and y' are not congruent modulo p.

EXERCISE 5.2. Let K be a number field. Let α and β be elements of $\mathcal{O}_K$ and let $\mathfrak{a}$ be an ideal of $\mathcal{O}_K$. Show that if $\mathfrak{a}$ divides the principal ideals (α) and (β), then $\mathfrak{a}$ divides the principal ideal $(\alpha + \beta)$.

EXERCISE 5.3. Let $K = \mathbb{Q}(\zeta_p)$. Show that for any $\alpha \in \mathcal{O}_K$, α^p is congruent to a rational integer modulo p.

3.1. Problems on Bernoulli numbers.

Recall that the Bernoulli numbers are defined by

$$\frac{t}{e^t - 1} = \sum_{n=0}^{\infty} B_n \frac{t^n}{n!}.$$

EXERCISE 5.4. Show that $B_n = 0$ for n odd and > 1. (Hint: Write $\frac{t}{e^t-1}$ as an even function plus a linear function.)

EXERCISE 5.5. Use the known power series for $\frac{e^t-1}{t}$ to prove that

$$\sum_{k=0}^{n-1} \binom{n}{k} B_k = 0$$

for $n > 1$. Conclude that the B_n are all rational.

EXERCISE 5.6. Prove that

$$t \cot t = \sum_{n=0}^{\infty} (-1)^n \frac{2^{2n} B_{2n}}{(2n)!} t^{2n}.$$

(Hint: Rewrite the even function of Exercise 5.4 in a way in which you can use the expressions for $\sin t$ and $\cos t$ in terms of complex exponentials.)

Another useful expression is

$$\frac{\sin t}{t} = \prod_{k=1}^{\infty} \left(1 - \frac{t^2}{(k\pi)^2}\right);$$

this ought to proved in any complex analysis book and/or class.

EXERCISE 5.7. Use the product above to show that

$$\cot t = \frac{1}{t} + 2t \sum_{k=1}^{\infty} \frac{1}{t^2 - k^2\pi^2}.$$

Recall that the *Riemann zeta function* is defined (for $\mathrm{Re}(s) > 1$) by

$$\zeta(s) = \sum_{n=1}^{\infty} n^{-s}.$$

EXERCISE 5.8. Use the previous exercises to write down two different expressions for $\pi t \cot \pi t$. Further expand the one from Exercise 5.7 into a power series and conclude that

$$\zeta(2n) = (-1)^{n-1}\frac{2^{2n}B_{2n}}{2(2n)!}\pi^{2n}.$$

EXERCISE 5.9. Show that

$$\lim_{n\to\infty}\left|\frac{2^{2n-1}\pi^{2n}}{(2n)!}B_{2n}\right| = 1.$$

Conclude that

$$\lim_{n\to\infty}\left|\frac{B_{2n}}{2n}\right| = \infty.$$

APPENDIX A

Field Theory

1. Field extensions and minimal polynomials

Recall that a field L is said to be an *extension* of a field K if $L \supseteq K$; it is said to be a *finite extension* if L is a finite-dimensional K-vector space, and we write $[L : K]$ for this dimension; thinking of K as an additive subgroup of L, this agrees with the usual notation for indexes of subgroups in group theory. In particular, this interpretation immediately implies the following lemma.

Lemma 1.1. *Let M/L and L/K be finite extensions. Then M/K is a finite extension and*

$$[M : K] = [M : L][L : K].$$

Proof. This is a standard fact in group theory; for a more explicit proof, one easily shows that if $\alpha_1, \dots, \alpha_m$ is a basis for L over K and $\beta_1, \dots, \beta_n$ is a basis for M over L (so that $[L : K] = m$ and $[M : L] = n$), then the set of products $\alpha_i \beta_j$ is a basis for M over K. $\square$

Lemma 1.1 is particularly useful in the following two contexts: first, both $[M : L]$ and $[L : K]$ divide $[M : K]$. Second, if we have a diagram of fields

$$\begin{tikzcd}
& M \arrow[dl, dash] \arrow[dr, dash] & \\
L_1 \arrow[dr, dash] & & L_2 \arrow[dl, dash] \\
& K &
\end{tikzcd}$$

(meaning that M contains L_1 and L_2 which in turn both contain K) then knowledge of any three degrees yields the fourth.

Note also that if $[L : K] = 1$, then $L = K$. More generally, Lemma 1.1 implies that if $M \supseteq L \supseteq K$ and $[M : K] = [L : K]$, then $M = L$.

Let L and L' be two extensions of K. We say that a map

$$\varphi : L \to L'$$

is *K-linear* if it restricts to the identity map on K. Note that such a map is also K-linear as a map of vector spaces, but a map $L \to L'$ as K-vector spaces need not be K-linear in this sense, since it need not send 1 to 1.

Example 1.2. Let us fix now some examples which we will use for the remainder of this appendix. For the moment, let $\sqrt{2}$, $\sqrt{3}$ and $\sqrt{6}$ denote the positive real square roots of 2, 3 and 6 respectively. Define

$$\begin{aligned}
L_1 &= \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\} \subseteq \mathbb{R};\\
L_2 &= \{a + b\sqrt{3} \mid a, b \in \mathbb{Q}\} \subseteq \mathbb{R};\\
L_3 &= \{a + b\sqrt{6} \mid a, b \in \mathbb{Q}\} \subseteq \mathbb{R};\\
M &= \{a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6} \mid a, b, c, d \in \mathbb{Q}\} \subseteq \mathbb{R};
\end{aligned}$$

that these are fields is a standard fact which can be checked directly; we will also give proofs later. All four fields are extensions of $\mathbb{Q}$, and M is an extension of L_1, L_2 and L_3. One checks easily (using the fact that $\sqrt{2}$, $\sqrt{3}$ and $\sqrt{6}$ are irrational) that $\{1, \sqrt{2}\}$, $\{1, \sqrt{3}\}$ and $\{1, \sqrt{6}\}$ are $\mathbb{Q}$-bases for L_1, L_2 and L_3 respectively; thus $[L_1 : \mathbb{Q}] = [L_2 : \mathbb{Q}] = [L_3 : \mathbb{Q}] = 2$.

It is clear that $[M : \mathbb{Q}] \leq 4$, since $\{1, \sqrt{2}, \sqrt{3}, \sqrt{6}\}$ spans M over $\mathbb{Q}$ by definition. To show that $[M : \mathbb{Q}]$ actually equals 4 we use Lemma 1.1. Specifically, M contains L_1, and M does not equal L_1 since $\sqrt{3} \notin L_1$. (We leave it to the reader to check this.) Thus $[M : L_1] \geq 2$, so

$$[M : \mathbb{Q}] = [M : L_1][L_1 : \mathbb{Q}] \geq 4.$$

Thus $[M : \mathbb{Q}] = 4$, as claimed, and $\{1, \sqrt{2}, \sqrt{3}, \sqrt{6}\}$ is a $\mathbb{Q}$-basis. Note that both $\{1, \sqrt{3}\}$ and $\{1, \sqrt{6}\}$ are bases for M over L_1, which is entirely consistent with the proof of Lemma 1.1. (Of course, there are similar statements for L_2 and L_3.)

$$\begin{tikzcd}
 & M \arrow[dl, dash, "2"'] \arrow[d, dash, "2"] \arrow[dr, dash, "2"] & \\
L_1 \arrow[dr, dash, "2"'] & L_2 \arrow[d, dash, "2"] & L_3 \arrow[dl, dash, "2"] \\
 & \mathbb{Q} &
\end{tikzcd}$$

Let L/K be a (not necessarily finite) extension of fields and let α be an element of L. If there is some polynomial $f(x) \in K[x]$ such that $f(\alpha) = 0$, then α is said to be *algebraic over* K; otherwise α is said to be *transcendental over* K. Suppose now that α is algebraic over K. Let d be the smallest positive integer such that α satisfies a polynomial of degree d in $K[x]$; d is said to be the *degree of* α *over* K. One shows easily that there is a unique monic polynomial of degree d in $K[x]$ which α satisfies, and this polynomial is called the *minimal polynomial of* α *over* K.

Note that every $\alpha \in K$ is algebraic over K, with minimal polynomial $x - \alpha \in K[x]$.

Example 1.3. Let $L = \mathbb{C}$ and $K = \mathbb{Q}$. The elements $\pm\sqrt{2} \in \mathbb{C}$ are algebraic over $\mathbb{Q}$, with minimal polynomial $x^2 - 2$. On the other hand, π is transcendental over $\mathbb{Q}$, although this is a non-trivial fact. Note that the minimal polynomial of $\sqrt{2}$ in the field L_1 of Example 1.2 is $x - \sqrt{2}$; in general the minimal polynomial of an element is very dependent on the base field.

Lemma 1.4. *Let L/K be a field extension and let $\alpha \in L$ be algebraic over K with minimal polynomial $f(x) \in K[x]$. Then $f(x)$ is irreducible in $K[x]$. Furthermore, if $g(x) \in K[x]$ is such that $g(\alpha) = 0$, then $f(x)$ divides $g(x)$ in $K[x]$.*

PROOF. We first show that $f(x)$ is irreducible over K. So suppose that $f(x)$ factors as $g(x)h(x)$ with $g(x), h(x) \in K[x]$ both of degree less than $\deg f$. Then

$$\begin{aligned} f(x) &= g(x)h(x) \\ f(\alpha) &= g(\alpha)h(\alpha) \\ 0 &= g(\alpha)h(\alpha). \end{aligned}$$

Thus either $g(\alpha) = 0$ or $h(\alpha) = 0$. But then we have found a polynomial in $K[x]$ of smaller degree than $f(x)$ which α satisfies. This contradicts the definition of $f(x)$, and thus shows that $f(x)$ is irreducible.

Now, suppose that $g(x) \in K[x]$ is such that $g(\alpha) = 0$. By the division algorithm, we can write

$$g(x) = q(x)f(x) + r(x)$$

with $q(x), r(x) \in K[x]$ and $\deg r(x) < \deg f(x)$. Substituting α for x, we find that

$$r(\alpha) = 0.$$

But, since $\deg r(x) < \deg f(x)$ and $f(x)$ is minimal, this implies that $r(x)$ is the zero polynomial. Thus $f(x)$ divides $g(x)$, as claimed. $\square$

Let us also state a fact which will be extremely useful to us: let L_1 and L_2 be two extensions of K, and suppose that there is a K-linear map

$$\varphi : L_1 \to L_2.$$

Let α be an element of L_1 which is algebraic over K, and let $f(x) \in K[x]$ be its minimal polynomial. Then $\varphi(\alpha)$ is algebraic over K, with minimal polynomial $f(x)$. To see this, note that

$$f(\varphi(\alpha)) = \varphi(f(\alpha)) = \varphi(0) = 0$$

since φ is the identity on the coefficients of f (which are in K); thus $\varphi(\alpha)$ satisfies f. By Lemma 1.4 $f(x)$ is irreducible in $K[x]$, and Lemma 1.4 now also shows that $f(x)$ must be the only monic irreducible polynomial which $\varphi(\alpha)$ satisfies; thus it is the minimal polynomial of $\varphi(\alpha)$.

EXAMPLE 1.5. Let L_1 and M be as in Example 1.2. Then there is a natural injection

$$L_1 \hookrightarrow M$$

and the minimal polynomial $x^2 - 2$ of $\sqrt{2}$ over $\mathbb{Q}$ does not depend on which extension of $\mathbb{Q}$ we compute it in.

The next result gives a fundamental property of finite extensions.

LEMMA 1.6. *Let L/K be a finite extension. Then every $\alpha \in L$ is algebraic over K.*

PROOF. Let α be an element of L. Consider the powers of α

$$1, \alpha, \alpha^2, \alpha^3, \ldots \in L.$$

Since L is a finite dimensional vector space over K, there must be some n such that

$$1, \alpha, \alpha^2, \alpha^3, \ldots, \alpha^n$$

are linearly dependent over K. (Specifically, one can take n to be the degree $[L : K]$.) That is, there exist $a_i \in K$ such that

$$a_0 \cdot 1 + a_1\alpha + a_2\alpha^2 + \cdots + a_n\alpha^n = 0.$$

Put in other terms, α satisfies the polynomial

$$a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n \in K[x],$$

so α is algebraic over K. $\square$

Example 1.7. Continue with the notation of Example 1.2. Consider the real number

$$\sqrt{2} + \sqrt{3} \in M.$$

Lemma 1.6 implies that this is algebraic over $\mathbb{Q}$, since M is finite over $\mathbb{Q}$, although it is not immediately obvious what polynomials it satisfies.

The converse of Lemma 1.6 is false; there do exist infinite field extensions L/K in which every element of L is algebraic over K.

2. Primitive elements

Given any extension L/K and any $\alpha \in L$, we define $K(\alpha)$ to be the smallest subfield of L containing K and α. (This is somewhat misleading notation, as $K(\alpha)$ is defined only as a subfield of L, but L does not appear in the notation. Hopefully it will always be clear from context what is meant.) Since $K(\alpha)$ is to be closed under addition, subtraction, multiplication and division, one easily sees that it simply consists of all expressions

$$\frac{a_0 + a_1\alpha + a_2\alpha^2 + \cdots + a_m\alpha^m}{b_0 + b_1\alpha + b_2\alpha^2 + \cdots + b_n\alpha^n},$$

with $a_i, b_i \in K$ and the denominator non-zero. Of course, some of these expressions may equal others.

We have the following abstract description of $K(\alpha)$. (Recall that the field $K(x)$ of rational functions in an indeterminate x is defined to be the field of all expressions

$$\frac{a_0 + a_1 x + a_2 x^2 + \cdots + a_m x^m}{b_0 + b_1 x + b_2 x^2 + \cdots + b_n x^n}$$

with $a_i, b_i \in K$.)

Lemma 2.1. *Let L/K be a field extension and let α be an element of L. If α is transcendental over K, then $K(\alpha)$ is isomorphic to the field $K(x)$ of rational functions in x. If α is algebraic over K with minimal polynomial $f(x) \in K[x]$ of degree d, then $K(\alpha)$ is an extension of K of degree d, and it is isomorphic to $K[x]/(f(x))$. In particular, when α is algebraic $K(\alpha)$ can be expressed simply as the set of all polynomials in α, rather than as rational functions.*

Proof. Suppose first that α is transcendental over K. Then we can define a homomorphism

$$K(x) \to K(\alpha)$$

by sending x to α; this is well-defined since α satisfies no non-zero polynomials, and thus it can be substituted into any rational function without causing the denominator to vanish. (This is definitely not true for algebraic α.) This map is injective since every map of fields is injective, and it must be surjective since its image is a subfield of L containing K and α and $K(\alpha)$ is the smallest such field. Thus it is an isomorphism.

Suppose now that α is algebraic over K with minimal polynomial $f(x) \in K[x]$. We define a ring homomorphism

$$\psi : K[x]/(f(x)) \to K(\alpha)$$

to be the identity on K and to send x to α; this is well-defined since $f(\alpha) = 0$. It is injective since $f(x)$ is the polynomial of minimal degree satisfied by α. Furthermore, since $K[x]$ is a principal ideal domain the ideal generated by $f(x)$ is maximal, so $K[x]/(f(x))$ is a field. The image of ψ is therefore a subfield of $K(\alpha)$ containing K and α; since $K(\alpha)$ is the smallest subfield of L containing α, it follows that the image of ψ is all of $K(\alpha)$, and thus that ψ is an isomorphism. Now, $1, x, \ldots, x^{d-1}$ is clearly a basis for $K[x]/(f(x))$ over K, and thus $1, \alpha, \ldots, \alpha^{d-1}$ is a basis for $K(\alpha)$. The remainder of the lemma is now clear. $\square$

A particular consequence of the lemma is that if L/K is a finite extension and α is an element of L, then the degree of α over K divides $[L : K]$.

Example 2.2. Let L_1, L_2, L_3 be as in Example 1.2. Then we have

$$L_1 \cong \mathbb{Q}[x]/(x^2 - 2),\ L_2 \cong \mathbb{Q}[x]/(x^2 - 3),\ L_3 \cong \mathbb{Q}[x]/(x^2 - 6).$$

There are many other possible expressions for these fields as quotients of $\mathbb{Q}[x]$. For example, considering L_1 as generated by $\sqrt{2} + 1$ rather than $\sqrt{2}$, we find that

$$L_1 \cong \mathbb{Q}[x]/(x^2 - 2x - 1).$$

We can write M in many obvious ways; for example, any of

$$L_1[x]/(x^2 - 3),\ L_1[x]/(x^2 - 6),\ L_2[x]/(x^2 - 2)$$

work. It is less clear how M can be written as a quotient of $\mathbb{Q}[x]$. To do this, we must find a primitive element for M over $\mathbb{Q}$.

If L/K is a field extension and if there exists an $\alpha \in L$ with $K(\alpha) = L$, then α is said to be a *primitive element* for L/K. In fact, in the situation which we will primarily be studying, every finite extension has a primitive element. Recall that a field extension L/K is said to be *separable* if every irreducible polynomial $f(x) \in K[x]$ has no multiple roots in L. In particular, by Exercise 1.12 every field of characteristic 0 is separable.

Proposition 2.3 (The Primitive Element Theorem). *Let L/K be a finite extension and suppose that K is separable. Then there exists a primitive element for L/K; that is, there is an $\alpha \in L$ such that $L = K(\alpha)$.*

Proof. See [**2**, Chapter 14, Theorem 4.1]. $\square$

The primitive element theorem should not be considered to be surprising. Essentially, if L/K is a finite extension, then *most* elements of L are primitive elements; the proof of the theorem consists in just writing down enough elements so that at least one is primitive.

Example 2.4. One can show that $\sqrt{2}+\sqrt{3}$ has minimal polynomial $x^4 - 10x^2 + 1$. (See Exercise 1.10.) Thus $\sqrt{2} + \sqrt{3}$ has degree 4, which means that it must be a primitive element for the field M of Example 1.2 over $\mathbb{Q}$. This also shows that

$$M \cong \mathbb{Q}[x]/(x^4 - 10x^2 + 1).$$

In particular, this implies that $\sqrt{2}$, $\sqrt{3}$ and $\sqrt{6}$ can be written in terms of powers of $\sqrt{2}+\sqrt{3}$. With a little effort one can compute

$$\begin{aligned}\sqrt{2} &= \frac{(\sqrt{2}+\sqrt{3})^3 - 9(\sqrt{2}+\sqrt{3})}{2}\\ \sqrt{3} &= \frac{11(\sqrt{2}+\sqrt{3}) - (\sqrt{2}+\sqrt{3})^3}{2}\\ \sqrt{6} &= \frac{(\sqrt{2}+\sqrt{3})^2 - 5}{2}.\end{aligned}$$

3. Algebraic extensions

Let M/K be a field extension. Suppose that we are given two subfields L_1 and L_2 of M, both containing K. We define the *compositum* L_1L_2 of L_1 and L_2 to be the smallest subfield of M containing both L_1 and L_2. (It is easy to see that such a field exists. We will give a more concrete description of L_1L_2 in certain cases in a moment.) We define the *intersection* $L_1 \cap L_2$ to be the largest subfield of M contained in both L_1 and L_2; it is easily seen to be nothing more than the usual set theoretic intersection of L_1 and L_2, and it contains K. We have the following field diagram:

$$\begin{tikzcd}[arrows=-]
 & M \arrow[d] & \\
 & L_1L_2 \arrow[dl] \arrow[dr] & \\
L_1 \arrow[dr] & & L_2 \arrow[dl] \\
 & L_1 \cap L_2 \arrow[d] & \\
 & K &
\end{tikzcd}$$

LEMMA 3.1. *Let K, L_1, L_2, M be as above and suppose that $[L_1 : L_1 \cap L_2]$ is finite. Then L_1L_2 consists of finite sums of products of elements of L_1 and L_2; that is,*

$$L_1L_2 = \left\{\sum \alpha_i\beta_i \mid \alpha_i \in L_1, \beta_i \in L_2\right\}.$$

PROOF. Let R be the set of all sums of products of elements of L_1 and L_2; R is clearly a ring, and it is the smallest ring containing L_1 and L_2. To show that $R = L_1L_2$ we must show that R is actually a field.

Set $L_1 \cap L_2 = L$. We will give the proof in the case where L_1 has a primitive element over L; by Proposition 2.3 this covers the case where everything has characteristic 0, and we leave the general case to the reader.

So, write $L_1 = L(\alpha)$ for some α. Reading through all of the relevant definitions, we find that

$$L_1L_2 = L_2(\alpha).$$

But α is certainly algebraic over L_2 (since it is algebraic over $L \subseteq L_2$), so we know that $L_2(\alpha)$ consists of polynomials in α with coefficients in L_2. Certainly this is contained in R; taking into account the minimality properties of everything involved, one can now conclude that $R = L_2(\alpha)$, and thus is a field. $\square$

EXAMPLE 3.2. If both L_1 and L_2 are infinite over $L_1 \cap L_2$, then L_1L_2 is more complicated. For example, take $K = \mathbb{Q}$, $L_1 = \mathbb{Q}(x)$, $L_2 = \mathbb{Q}(y)$ and $M = \mathbb{Q}(x, y)$, where x and y are indeterminates. Then $L_1L_2 = M$, but one can not write $1/(x+y)$ as a sum of products of elements of L_1 and L_2.

LEMMA 3.3. *Let K, L_1, L_2, M be as above and suppose that $[L_1L_2 : L_1 \cap L_2] < \infty]$. Then*

$$[L_1L_2 : L_1] \leq [L_2 : L_1 \cap L_2]$$

and

$$[L_1L_2 : L_2] \leq [L_1 : L_1 \cap L_2].$$

PROOF. Let $\alpha_1, \ldots, \alpha_n$ be a basis for L_2 over $L_1 \cap L_2$. We claim that the α_i span L_1L_2 over L_1, which will prove the lemma (the second inequality being virtually the same). So let $\sum \beta_j\gamma_j$ be an arbitrary element of L_1L_2, $\beta_j \in L_1$, $\gamma_j \in L_2$. By hypothesis we can write

$$\gamma_j = \sum c_{ij}\alpha_i$$

with $c_{ij} \in L_1 \cap L_2$. Now we have

$$\sum \beta_j\gamma_j = \sum c_{ij}\beta_j\alpha_i$$

and $c_{ij}\beta_j \in L_1$; this shows that the α_i span L_1L_2 over L_1, as claimed. $\square$

We will show in Chapter 1 that we have equality in the above lemma in the case where at least one of L_1 and L_2 is Galois over $L_1 \cap L_2$.

In the case that $L_1 = K(\alpha_1)$ and $L_2 = K(\alpha_2)$ are both primitive, we will write $K(\alpha_1, \alpha_2)$ for the compositum L_1L_2. More generally, we define the field $K(\alpha_1, \ldots, \alpha_m)$ to be the compositum of the fields $K(\alpha_1), \ldots, K(\alpha_m)$.

EXAMPLE 3.4. Continue with the fields of Example 1.2. We have

$$L_iL_j = \begin{cases} M & i \neq j; \\ L_i & i = j; \end{cases}$$

and

$$L_i \cap L_j = \begin{cases} \mathbb{Q} & i \neq j; \\ L_i & i = j. \end{cases}$$

Now let L/K be any extension of fields. A fundamental (but not immediately obvious fact) is that the subset of L of elements which are algebraic over K is closed under sums, products and inverses; that is, it is a field. With the above results we can give a comparatively simple proof of this fact.

PROPOSITION 3.5. *Let L/K be a field extension and let L' be the subset of L of elements which are algebraic over K. Then L' is a field.*

PROOF. Let $\alpha, \beta \in L$ be algebraic over K. We wish to show that $\alpha+\beta$, $\alpha\beta$ and α^{-1} are all algebraic over K as well. Note that all of these elements are contained in $K(\alpha, \beta)$.

Now, by Lemma 2.1 $K(\alpha)$ and $K(\beta)$ are finite extensions of K. From this, Lemma 1.1 and Lemma 3.3, we find that

$$\begin{aligned}[K(\alpha,\beta):K] &= [K(\alpha,\beta):K(\alpha)][K(\alpha):K] \\ &\leq [K(\beta):K(\alpha)\cap K(\beta)][K(\alpha):K] \\ &\leq [K(\beta):K][K(\alpha):K] \\ &\leq \infty.\end{aligned}$$

Thus $K(\alpha,\beta)$ is a finite extension of K, so by Lemma 1.6 every element of $K(\alpha,\beta)$ is algebraic over K. As we observed above, this is what we needed to prove. □

4. Characteristic polynomials

We recall briefly the definition of the characteristic polynomial of a linear transformation. Let K be a field and let V be a finite dimensional K-vector space, say of dimension n. Let $T : V \to V$ be a K-linear transformation of V. Choosing any basis for V over K, let A be the $n \times n$ matrix with entries in K representing T with respect to this basis. We define the *characteristic polynomial* of T to be

$$\det(xI - A) \in K[x]$$

where I is the $n \times n$ identity matrix. It is a standard fact that this is independent of the choice of basis of V over K.

Let L/K be a finite extension of degree n and choose $\alpha \in L$. Multiplication by α defines a map of K-vector spaces

$$m_\alpha : L \to L;$$

thus m_α is a linear transformation from the n-dimensional K-vector space L to itself. We define the *characteristic polynomial of α for L/K* to be the characteristic polynomial of the linear transformation m_α.

Lemma 4.1. *Let α be an element of L with characteristic polynomial $f(x)$ over K. Then $f(\alpha) = 0$.*

Proof. Write $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0$. By the Cayley-Hamilton theorem, $f(m_\alpha)$ is the zero linear transformation. On the other hand,

$$\begin{aligned}f(m_\alpha) &= m_\alpha^n + a_{n-1}m_\alpha^{n-1} + \cdots + a_0 I \\ &= m_{\alpha^n} + a_{n-1}m_{\alpha^{n-1}} + \cdots + a_0 m_1 \\ &= m_{\alpha^n} + m_{a_{n-1}\alpha^{n-1}} + \cdots + m_{a_0} \\ &= m_{\alpha^n + a_{n-1}\alpha^{n-1} + \cdots + a_0} \\ &= m_{f(\alpha)}\end{aligned}$$

where we have used some easy properties of linear transformations. Thus $m_{f(\alpha)}$ is the zero linear transformation; in particular, $f(\alpha)\cdot 1 = 0$, so $f(\alpha) = 0$. □

Lemma 4.2. *Let L/K be a finite extension and let $\alpha \in L$ be a primitive element. Then the characteristic polynomial for α in L/K is equal to the minimal polynomial of α over K.*

Proof. Since α is primitive its minimal polynomial will have degree $[L : K]$; the characteristic polynomial also has this degree, and since it is a monic polynomial satisfied by α, it must equal the minimal polynomial. □

More generally, it is true that the characteristic polynomial is a power of the minimal polynomial. This will follow from the next proposition.

PROPOSITION 4.3. *Let M/L and L/K be finite extensions. Fix $\gamma \in L$ and let $f(x), g(x) \in K[x]$ be the characteristic polynomials for γ in L/K and in M/K respectively. Then*

$$g(x) = f(x)^{[M:L]}.$$

PROOF. Let $\alpha_1, \dots, \alpha_m$ be a basis for L over K and let $\beta_1, \dots, \beta_n$ be a basis for M over L, so that $\alpha_1\beta_1, \alpha_2\beta_1, \dots, \alpha_m\beta_1, \alpha_1\beta_2, \dots, \alpha_m\beta_2, \dots, \alpha_m\beta_n$ is basis for M over K. Let $A = (a_{ij})$ be the matrix for γ acting on L with respect to this basis, so that

$$\gamma\alpha_j = a_{1j}\alpha_1 + a_{2j}\alpha_2 + \cdots + a_{mj}\alpha_m,$$

with $a_{ij} \in K$. Then

$$\gamma\alpha_j\beta_i = a_{1j}\alpha_1\beta_i + a_{2j}\alpha_2\beta_i + \cdots + a_{mj}\alpha_m\beta_i.$$

This is an expression for $\gamma\alpha_j\beta_i$ in terms of our basis for M/K, with coefficients in K, so we can use it to form the matrix for α acting on M. This matrix has the form

$$\begin{bmatrix} A & 0 & 0 & & 0 \\ 0 & A & 0 & \cdots & 0 \\ 0 & 0 & A & & 0 \\ & \vdots & & & \vdots \\ 0 & 0 & 0 & \cdots & A \end{bmatrix}$$

where the first A acts on the $\alpha_j\beta_1$, the second on the $\alpha_j\beta_2$, and so on. From this matrix it is easy to see that the characteristic polynomial for α in M/K is just the characteristic polynomial of A taken to the power of the number of copies of A in the above matrix. This number is just $n = [M : L]$, which proves the proposition. □

COROLLARY 4.4. *Let L/K be a finite extension. Fix $\alpha \in L$ with minimal polynomial $f(x)$ and characteristic polynomial $g(x)$. Then*

$$g(x) = f(x)^{[L:K(\alpha)]}.$$

PROOF. This is simply the special case of Proposition 4.3 for the tower of extensions $L/K(\alpha)/K$, using Lemma 4.2 to identify the characteristic polynomial of α in $K(\alpha)/K$ with $f(x)$. □

Let the characteristic polynomial of α be given by

$$x^n + a_{n-1}x^{n-1} + \cdots + a_0 \in K[x].$$

We define the *trace relative to L/K* of α by

$$\operatorname{Tr}_{L/K} \alpha = -a_{n-1} = \operatorname{Tr}(m_\alpha) \in K$$

(where $\operatorname{Tr}(m_\alpha)$ is the trace of the linear transformation m_α) and the *norm relative to L/K* of α by

$$\mathrm{N}_{L/K} \alpha = (-1)^n a_0 = \det(m_\alpha) \in K.$$

(The other coefficients of the characteristic polynomial are also invariants of α (relative to the extension L/K), but they tend to be much less useful in practice.)

Lemma 4.5. *Let L/K be a finite extension of degree n. For any $\alpha, \beta \in L$,*

$$\mathrm{Tr}_{L/K}(\alpha + \beta) = \mathrm{Tr}_{L/K}(\alpha) + \mathrm{Tr}_{L/K}(\beta)$$

and

$$\mathrm{N}_{L/K}(\alpha\beta) = \mathrm{N}_{L/K}(\alpha)\,\mathrm{N}_{L/K}(\beta).$$

If $c \in K$, then

$$\mathrm{Tr}_{L/K}(c\alpha) = c\,\mathrm{Tr}_{L/K}(\alpha)$$

and

$$\mathrm{N}_{L/K}(c\alpha) = c^n\,\mathrm{N}_{L/K}(\alpha).$$

Proof. All of these properties are clear from the description of $\mathrm{Tr}_{L/K}$ and $\mathrm{N}_{L/K}$ as traces and determinants of matrices. □

Note that the norm and trace of $\alpha \in L$ depend on considering α as an element of L. The next lemma shows how norms and traces depend on the fields being considered.

Lemma 4.6. *Let M/L and L/K be finite extensions. Then for any $\alpha \in M$,*

$$\mathrm{Tr}_{M/K}(\alpha) = \mathrm{Tr}_{L/K}\big(\mathrm{Tr}_{M/L}(\alpha)\big)$$

and

$$\mathrm{N}_{M/K}(\alpha) = \mathrm{N}_{L/K}\big(\mathrm{N}_{M/L}(\alpha)\big).$$

Proof. The general proof requires some ugly linear algebra. For an easier proof in the case of number fields see [**14**, Chapter 2, Theorem 5]; this proof makes use of some of the machinery developed in Chapter 1. □

Example 4.7. With the notation of Example 1.2, consider the element $\sqrt{2} \in M$. This has minimal polynomial $x^2 - 2$ over $\mathbb{Q}$. On the other hand, choosing the $\mathbb{Q}$-basis $1, \sqrt{2}, \sqrt{3}, \sqrt{6}$ for M, $m_{\sqrt{2}}$ is given by the matrix

$$\begin{bmatrix} 0 & 2 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 2 \\ 0 & 0 & 1 & 0 \end{bmatrix},$$

which has characteristic polynomial $x^4 - 4x^2 + 4$. Note that this is the square of $x^2 - 2$, as claimed above. Note also that $\mathrm{Tr}_{L_1/\mathbb{Q}}(\sqrt{2}) = \mathrm{Tr}_{M/\mathbb{Q}}(\sqrt{2}) = 0$, $\mathrm{N}_{L_1/\mathbb{Q}}(\sqrt{2}) = 2$ and $\mathrm{N}_{M/\mathbb{Q}}(\sqrt{2}) = 4$, which is consistent with Lemma 4.6.

APPENDIX B

Mobius Inversion

1. Theory over rings

Let $\mathbb{N}$ denote the natural numbers.

DEFINITION 1.1. Let R be a commutative ring. An *R-arithmetical function* is a function

$$\psi : \mathbb{N} \to R.$$

We will denote by $\mathrm{Ar}(R)$ the set of R-arithmetical functions.

Note that if $f : R \to S$ is a map of rings, then for any $\psi \in \mathrm{Ar}(R)$, $f \circ \psi$ is an S-arithmetical function. Thus f induces a map $\mathrm{Ar}(R) \to \mathrm{Ar}(S)$. (If one wants to be fancy, this means that Ar is a covariant functor from rings to sets.) In particular, the canonical map $\mathbb{Z} \to R$ (sending 1 to 1) induces a map $\mathrm{Ar}(\mathbb{Z}) \to \mathrm{Ar}(R)$. (All that this really means is that you interpret the values $f(n)$ in R rather then in $\mathbb{Z}$.)

EXAMPLE 1.2. There are many arithmetical functions of importance in number theory. Among the simpler examples are

$$\tau(n) = \sum_{d|n} 1 \quad \text{(the number of divisors of } n\text{)}$$

$$\sigma(n) = \sum_{d|n} d \quad \text{(the sum of the divisors of } n\text{)}$$

(here $\sum_{d|n}$ means that the sum is done over the positive divisors of n) and the Euler totient function $\varphi(n)$, defined to be the number of positive integers less than or equal to n and relatively prime to n. These are all $\mathbb{Z}$-arithmetical functions, and thus by the above discussion can be considered in $\mathrm{Ar}(R)$ for any R. We also define two less interesting $\mathbb{Z}$-arithmetical functions which will nevertheless be useful later on:

$$I(n) = \begin{cases} 1, & \text{if } n = 1; \\ 0, & \text{otherwise.} \end{cases}$$

$$u(n) = 1 \quad \text{for all } n.$$

A somewhat more complicated example is the Mobius function.

DEFINITION 1.3. Define the Mobius function $\mu \in \mathrm{Ar}(\mathbb{Z})$ by

$$\mu(n) = \begin{cases} 1, & \text{if } n = 1; \\ (-1)^k, & \text{if } n = p_1 \cdots p_k \text{ where the } p_i \text{ are distinct primes;} \\ 0, & \text{if } p^2 | n \text{ for any prime } p. \end{cases}$$

For example, $\mu(2) = -1$, $\mu(4) = 0$, and $\mu(6) = 1$.

We now prove a fundamental property of μ.

LEMMA 1.4.
$$\sum_{d|n} \mu(d) = I(n).$$

PROOF. Note that if $n = p_1^{m_1} \cdots p_k^{m_k}$ then
$$\sum_{d|n} \mu(d) = \sum_{d|p_1 \cdots p_k} \mu(d)$$
since the additional terms are all 0. It is thus enough to prove the formula for the case where n is squarefree.

The formula is clear for $n = 1$. By the definition of $I(n)$ it remains to prove that
$$\sum_{d|p_1 \cdots p_k} \mu(d) = 0.$$
For each $i \leq k$ and each divisor d of n consisting of exactly i prime factors, we will have $\mu(d) = (-1)^i$. There are exactly $\binom{k}{i}$ such d, (we must choose i primes from a set of k) so
$$\sum_{d|n} \mu(d) = \sum_{i=0}^{k} (-1)^i \binom{k}{i}.$$
But by the binomial theorem the second sum is just $(1-1)^k = 0$. This completes the proof. $\square$

We have already seen divisor sums $\sum_{d|n}$ come up several times. This helps to motivate the following definition.

DEFINITION 1.5. If f and g are two R-arithmetical functions, we define their *Dirichlet product* $f * g \in \mathrm{Ar}(R)$ to be the arithmetical function given by
$$(f * g)(n) = \sum_{d|n} f(d) g\left(\frac{n}{d}\right).$$

Lemma 1.4 then says precisely that $\mu * u = I$.

This product operation turns out to have many interesting properties. We will confine ourselves to proving what we need for the Mobius inversion formula; for more information see [**1**, Chapter 2].

PROPOSITION 1.6. *The Dirichlet product on* $\mathrm{Ar}(R)$ *is associative and commutative and has* $I \in \mathrm{Ar}(R)$ *as an identity element. That is, if* f, g, h *are* R*-arithmetical functions, then* $f * (g * h) = (f * g) * h$, $f * g = g * f$ *and* $f * I = I * f = f$.

PROOF. We calculate
$$\begin{aligned} f * I(n) &= \sum_{d|n} f(d) I\left(\frac{n}{d}\right) \\ &= f(n) I(1) \\ &= f(n). \end{aligned}$$
The case of $I * f$ is virtually identical.

Now, for associativity,

$$\begin{aligned} f*(g*h)(n) &= \sum_{d|n} f(d)(g*h)\left(\frac{n}{d}\right) \\ &= \sum_{de=n} f(d)(g*h)(e) \\ &= \sum_{de=n} f(d)\sum_{a|e} g(a)h\left(\frac{e}{a}\right) \\ &= \sum_{de=n} f(d)\sum_{ab=e} g(a)h(b) \\ &= \sum_{dab=n} f(d)g(a)h(b). \end{aligned}$$

Similarly, we find that

$$(f*g)*h(n) = \sum_{dab=n} f(d)g(a)h(b).$$

Thus $f*(g*h) = (f*g)*h$.

The commutativity is clear. □

Now, often in number theory one has a formula of the form

$$f(n) = \sum_{d|n} g(d)$$

and wishes to determine g in terms of f. Using Dirichlet multiplication this is quite easy.

THEOREM 1.7 (The Mobius inversion formula). *Suppose that f and g are R-arithmetical functions such that*

$$f(n) = \sum_{d|n} g(d).$$

Then

$$g(n) = \sum_{d|n} f(d)\mu\left(\frac{n}{d}\right).$$

PROOF. We have $f = g*u$. Thus

$$\begin{aligned} f*\mu &= (g*u)*\mu \\ &= g*(u*\mu) \\ &= g*(\mu*u) \\ &= g*I \\ &= g \end{aligned}$$

which is exactly the desired formula. □

2. Theory over groups

DEFINITION 2.1. Let G be an abelian group written additively. We define a *G-arithmetical function* to be a map

$$\psi : \mathbb{N} \to G.$$

We denote by $\mathrm{Ar}(G)$ the set of G-arithmetical functions.

Of course, if R is a ring then the two definitions of $\mathrm{Ar}(R)$ are the same, where in the second we regard R as its additive group. Ar is again a covariant functor, this time from abelian groups to sets.

We would like to get a Mobius inversion formula for G-arithmetical functions. This is complicated by the fact that we can not define a Dirichlet product on $\mathrm{Ar}(G)$, as there is no "multiplication". Nevertheless, we can still define it in the cases we will need.

DEFINITION 2.2. Let $f \in \mathrm{Ar}(G)$ and let $g \in \mathrm{Ar}(\mathbb{Z})$. We define $f * g \in \mathrm{Ar}(G)$ by

$$(f * g)(n) = \sum_{d|n} f(d) g\left(\frac{n}{d}\right)$$

where $f(d)g(n/d)$ means $f(d)$ added to itself $g(n/d) \in \mathbb{Z}$ times.

PROPOSITION 2.3. *For any $f \in \mathrm{Ar}(G)$, $f * I = f$. If $g, h \in \mathrm{Ar}(\mathbb{Z})$, then $f * (g * h) = (f * g) * h$.*

PROOF. The proof is exactly the same as the proof in the classical case; one must merely note that all of the expressions make sense, which they do. $\square$

The above proposition means that the monoid $\mathrm{Ar}(\mathbb{Z})$ acts on $\mathrm{Ar}(G)$ on the right.

We can now prove a Mobius inversion formula.

THEOREM 2.4 (Generalized Mobius inversion). *Let f, g be G-arithmetical functions such that*

$$f(n) = \sum_{d|n} g(d).$$

Then

$$g(n) = \sum_{d|n} f(d) \mu\left(\frac{n}{d}\right).$$

PROOF. We have $f = g * u$, and the proof proceeds as before. $\square$

EXAMPLE 2.5. Let $G = \mathbb{C}(x)^*$. (Note that we will now be writing everything multiplicatively despite our above notation.) Consider the G-arithmetical functions f and g given by

$$f(n) = \Phi_n(x)$$
$$g(n) = x^n - 1,$$

where $\Phi_n(x)$ is the n^{th} cyclotomic polynomial. (See Chapter 1, Section 4.) Then

$$g(n) = \prod_{d|n} f(d),$$

so by Mobius inversion

$$f(n) = \prod_{d|n} g(d)^{\mu(n/d)}.$$

APPENDIX C

Factorization

1. Definitions

Let R be a commutative integral domain. (While one can consider factorizations in any ring, the case of an integral domain is somewhat simpler; since it is the only case we will need, we will make this simplifying hypothesis. We will also assume without further comment that all rings under discussion are commutative.) We recall some standard definitions. Given $a, b \in R$, we say that a *divides* b, written $a|b$, if there exists $c \in R$ such that $b = ac$. An element $u \in A$ is said to be a *unit* in R if u divides 1; equivalently, u is a unit if there exists $v \in R$ with $uv = 1$. One easily shows that v is unique, and we will write it as u^{-1}. We denote by R^* the subset of R of units; R^* is an abelian group with multiplication in R as the group law. Two elements $a, b \in R$ are said to be *associates* if there is some unit $u \in R^*$ with $a = bu$; this is clearly an equivalence relation.

Note that fields are always integral domains, and that if R is an integral domain, then so is $R[x]$.

Primes in $\mathbb{Z}$ have two essential properties, one involving factorizations and one involving divisibilities. In more general situations it is important to separate these two notions. An element $\pi \in R$ is said to be *irreducible* if it is not a unit and if it can not be written as a product $\pi = ab$ with neither a nor b a unit. π is said to be *prime* if it is not a unit and if it has the property that whenever π divides a product ab, then either π divides a or π divides b.

EXAMPLE 1.1. Take $R = \mathbb{Z}[\sqrt{-5}]$. One can easily show that 2 is irreducible in R. However, 2 divides $(1 + \sqrt{-5})(1 - \sqrt{-5}) = 6$. Since 2 clearly does not divide either factor, it follows that 2 is not prime in R.

While irreducible and prime are not equivalent, in our situation there is an implication in one direction.

LEMMA 1.2. *Let R be an integral domain and let π be a prime in R. Then π is irreducible in R.*

PROOF. Suppose that π factors as $\pi = ab$. Then π divides ab, so since π is prime π must divide one factor; we suppose without loss of generality that it is a. Thus we can write $a = \pi c$ for some $c \in R$. Now

$$\pi = ab = \pi cb;$$

since R is an integral domain this implies that $cb = 1$, and thus that b is a unit. Therefore any factorization of π involves a unit, so π is irreducible. $\square$

2. Review of ideals

Let R be a commutative ring. Recall that an *ideal* I of R is a subset of R which is closed under addition and which has the property that $ri \in I$ for all $r \in R$ and $i \in I$. Given an ideal I, the quotient ring R/I is defined to be the quotient group R/I as an additive group; one shows that the multiplicative closure of the ideal implies that R/I inherits a multiplication from R and thus is a ring.

An ideal I is said to be *prime* if R/I is an integral domain; this is equivalent to the property that whenever $ab \in I$, then either $a \in I$ or $b \in I$. I is said to be *maximal* if R/I is a field; this is equivalent to the property that if J is an ideal of R containing I, then $J = R$ or $J = I$. Since every field is an integral domain, every maximal ideal is necessarily prime.

Given a subset $S \subseteq R$, the *ideal* (S) *generated by* S is defined to be the set of all finite linear combinations of elements of S with coefficients in R; that is,

$$(S) = \{a_1 s_1 + \cdots + a_r s_r \mid a_i \in R, s_i \in S\}.$$

If $S = \{a\}$ consists of a single element, then the ideal (a) is called a *principal ideal.* Properties of principal ideals are closely connected to properties of the corresponding elements. For example, the principal ideal (a) is all of R if and only if a is a unit, and the principal ideal (a) is prime if and only if a is a prime element. Also, an element a divides an element b if and only if $(a) \supseteq (b)$. We leave the proofs of all of these facts to the reader.

Given two ideals I, J of R, we define the *product ideal* IJ to be the ideal of R generated by all products of elements ij with $i \in I$ and $j \in J$. That is,

$$IJ = \{a_1 i_1 j_1 + \cdots + a_r i_r j_r \mid a_k \in R, i_k \in I, j_k \in J\}.$$

Note that if I has generators $i_1, \ldots, i_r$ and J has generators $j_1, \ldots, j_s$, then the products $i_\alpha j_\beta$ generate IJ. In particular, if $I = (i)$ and $J = (j)$ are both principal, then $IJ = (ij)$ is also principal.

We define the *intersection* $I \cap J$ to be the set-theoretic intersection of I and J; it is an ideal of R, and it is some sort of least common multiple of I and J. We define the *sum* $I + J$ to be the ideal of R consisting of all sums of elements of I and J:

$$I + J = \{i + j \mid i \in I, j \in J\}.$$

Note that $I + J$ is the smallest ideal of R containing both I and J; it is to be thought of as a greatest common divisor of I and J.

3. Unique factorization

We continue to let R denote an integral domain. We say that an element $a \in R$ has an *irreducible factorization* if a can be written as a finite product

$$a = \pi_1 \cdots \pi_r$$

where each π_i is irreducible in R.

Example 3.1. While there are example of rings where not every element has an irreducible factorization, they are somewhat contrived. Here is one: let R be a polynomial ring over some field K in infinitely many variables x_i, $i \geq 0$. Let I be the ideal of R generated by the polynomials $x_i - x_{i+1}^2$ for all i. Set $S = R/I$ and consider the image $\bar{x}_0$ of x_0 in S. We have

$$\bar{x}_0 = \bar{x}_1^2 = \bar{x}_2^4 = \bar{x}_3^8 = \cdots$$

and so on, and none of the $\bar{x}_i$ are units. With a little more effort one can show that this is the only way to factor $\bar{x}_0$; since none of the $\bar{x}_i$ are ever irreducible, it follows that $\bar{x}_0$ has no irreducible factorization.

There is one standard condition that insures the existence of irreducible factorizations. Recall that a ring R is said to be *noetherian* if every increasing sequence of ideals is eventually constant; that is, if given a chain of ideals

$$I_1 \subseteq I_2 \subseteq I_3 \subseteq I_4 \subseteq \cdots,$$

there must be some n such that

$$I_m = I_{m'}$$

for all $m, m' \geq n$. There are many equivalent formulations of this condition; see Exercise 2.7.

EXAMPLE 3.2. $\mathbb{Z}$ is noetherian and any field K is noetherian. If R is noetherian, then $R[x]$ is noetherian (the Hilbert basis theorem; see [**2**, Chapter 12, Theorem 5.18, p. 469]), and any quotient of R is also noetherian. From these examples one can show that almost any ring that ever comes up is noetherian. Of course, the rings R and S of Example 3.1 are not noetherian.

The relevance of the noetherian hypothesis to us comes from the following fact.

PROPOSITION 3.3. *Let R be a noetherian integral domain. Then every non-zero element of R has an irreducible factorization.*

PROOF. Let $\mathcal{S}$ denote the set of ideals I of R such that one can write $I = (a)$ for some $a \in R$ such that $a \neq 0$ and a does not have an irreducible factorization. We will show that $\mathcal{S}$ is empty, which is the statement of the proposition. Suppose that $\mathcal{S}$ is non-empty. Then by Exercise 2.7 $\mathcal{S}$ has at least one maximal element; choose one, say $I = (a)$ where a does not have an irreducible factorization. a can not be irreducible itself, since it has no irreducible factorization, so we can write $a = bc$ for some $b, c \in R$ with neither b nor c a unit. This clearly implies that the ideal (a) is contained in the ideals (b) and (c). Furthermore, (a) can not equal (b) or (c) since if it did equal one, say (b), then c would be a unit. Thus (a) is strictly contained in both (b) and (c); since (a) is a maximal element of $\mathcal{S}$, it follows that $(b), (c) \notin \mathcal{S}$. Thus b and c have irreducible factorizations; combining them yields an irreducible factorization of a. This is a contradiction, so $\mathcal{S}$ must have been empty, as desired. $\square$

The above proof is really nothing more than a fairly slick way to say "start factoring a and eventually you end up with irreducibles."

Now, let R be an integral domain in which every element has an irreducible factorization; by Proposition 3.3 it would suffice for R to be noetherian. We will say that R is a *unique factorization domain* (or a *UFD*) if every element of R can be written uniquely as a product of irreducibles. By "uniquely" here we mean the following: let a be in R, and suppose that a has two expressions

$$a = \pi_1 \cdots \pi_r = \pi'_1 \cdots \pi'_s$$

as products of irreducibles of R. We will consider these two factorizations to be equivalent if $r = s$ and if there is a permutation $\sigma : [1, r] \to [1, r]$ such that π_i and $\pi'_{\sigma(i)}$ are associates for all i. (By $[1, r]$ we mean the set of integers $\{1, 2, \ldots, r\}$.) We say that a can be written uniquely as a product of irreducibles if any two factorizations of a are equivalent in the above sense. Note in particular that one can use units of R to develop many different factorizations of a, but none of these are to be considered to be inequivalent.

This definition is in fact fundamentally related to the notions of irreducible and prime elements. Before we prove this we give a useful lemma.

Lemma 3.4. *Let R be a unique factorization domain and let a and π be elements of R with π irreducible. Suppose that π divides a. Then some associate of π appears in every irreducible factorization of a.*

Proof. Let $b = a/\pi$. Then we can form an irreducible factorization of a by taking π and an irreducible factorization of b; since π appears in this factorization, by unique factorization some associate of π must appear in every irreducible factorization of a. This proves the lemma. □

Proposition 3.5. *Let R be an integral domain in which every element has an irreducible factorization. Then R is a unique factorization domain if and only if every irreducible element in R is prime.*

Proof. Suppose first that R is a unique factorization domain. Let $\pi \in R$ be irreducible. We must show that π is prime. So suppose that π divides a product ab in R. Then by Lemma 3.4 some associate of π appears in every irreducible factorization of ab. It follows that some associate of π must appear in the irreducible factorization of either a or b, since otherwise we would be able to form an irreducible factorization of ab without any associate of π. But if π appears in an element's irreducible factorization, then it divides that element. This shows that π divides either a or b, as desired.

Now suppose that every irreducible in R is prime. Let a be an element of R and let

$$a = \pi_1 \cdots \pi_r = \pi_1' \cdots \pi_s'$$

be two irreducible factorizations of a. We must show that $r = s$ and define a map $\sigma : [1, r] \to [1, s]$ as above. Now, π_1 is prime and divides $\pi_1' \cdots \pi_s'$; it follows that π_1 must divide at least one of the π_i'; let $\sigma(1)$ be any one of these values of i. Since $\pi_{\sigma(1)}'$ is irreducible, π_1 and $\pi_{\sigma(1)}'$ must be associates. Let $u \in R^*$ be the unit such that $u\pi_1 = \pi_{\sigma(1)}'$. Then canceling π_1 from each side we find that

$$\pi_2 \cdots \pi_r = u\pi_1' \cdots \pi_{\sigma(1)-1}' \pi_{\sigma(1)+1}' \cdots \pi_s'.$$

Continuing in this way we can cancel off each π_i, so $r \leq s$. But the same argument applied to the π_i' shows that $s \leq r$, so $r = s$. Now the above argument does indeed construct the desired permutation σ of $[1, r]$; the units are irrelevant because we are only trying to prove that things are associates. □

4. Principal ideal domains and Euclidean domains

There are several ways to obtain UFDs. The first shows that polynomial rings over UFDs are still UFDs.

Proposition 4.1. *Let R be a UFD. Then $R[x]$ is a UFD.*

Proof. The proof is exactly the same as the proof given in Problem Set, Exercises 1-4, with $\mathbb{Z}$ replaced by R and $\mathbb{Q}$ replaced by the fraction field of R. □

EXAMPLE 4.2. Since any field K is a UFD trivially, the rings $K[x]$ are all UFDs. More generally, $K[x_1, \ldots, x_n]$ is a UFD for any n. Similarly, $\mathbb{Z}[x_1, \ldots, x_n]$ is a UFD for any n since $\mathbb{Z}$ is.

In preparation for the next results, let us recall a standard method for proving that a ring R is a UFD. Suppose that R has the property that for every two irreducibles π, π' of R which are not associates, the ideal (π, π') is all of R; equivalently, there exist $a, b \in R$ such that

$$a\pi + b\pi' = 1.$$

(We will call this the *Diophantine property.*) We claim that R is then a UFD.

PROPOSITION 4.3. *Let R be an integral domain in which every element has an irreducible factorization, and suppose that R has the Diophantine property. Then R is a UFD.*

PROOF. Let π be an irreducible of R. By Proposition 3.5 it will suffice to show that π is prime. In fact, it will suffice to prove the following: suppose that π divides $\pi' a$, where π' is an irreducible which is not an associate of π. Then π divides a. We leave the reduction of the general case to this case to the reader.

So suppose that π divides $\pi' a$ and π and π' are not associates. Write $\pi' a = \pi b$. By the Diophantine property there exist $c, d \in R$ such that $c\pi + d\pi' = 1$. Now,

$$\begin{aligned} d\pi' a &= d\pi b \\ (1 - c\pi)a &= d\pi b \\ a &= d\pi b + c\pi a \\ a &= \pi(db + ca). \end{aligned}$$

Thus π divides a, as desired. $\square$

EXAMPLE 4.4. The converse of Proposition 4.3 is false. For example, take $R = \mathbb{Z}[x]$, which is a UFD. One sees easily that R does not have the Diophantine property using the two irreducibles 2 and x.

The next step is to find ways to prove that rings have the Diophantine property. The standard way to do this is to show that R is a principal ideal domain. Recall that R is a *principal ideal domain* (or a *PID*) if every ideal of R is principal; that is, if for every ideal I of R, there is some $a \in I$ such that $I = (a)$.

PROPOSITION 4.5. *Let R be a noetherian principal ideal domain. Then R is a UFD.*

PROOF. Let π and π' be two irreducibles of R which are not associates. Since R is a UFD the ideal $I = (\pi, \pi')$ is principal, say generated by a. Since $\pi \in I$ we must have that a divides π. Similarly, a divides π'. But the only elements of R dividing both π and π' are units, since otherwise π and π' would be associates. Thus a is a unit, so $I = R$, and the Diophantine property is now immediate by Proposition 4.3. $\square$

Lastly, then, we need a way to show that rings are PIDs. Algebraic number theory will give one method; we give here another one.

Let R be a noetherian integral domain. Let

$$\mathrm{N} : R - \{0\} \to \mathbb{N}$$

be some function from the non-zero elements of R to the natural numbers. We also set $\mathrm{N}(0) = -1$. Suppose that for any $a, b \in R$ with $b \neq 0$ there exist $q, r \in R$ such that

$$a = bq + r$$

and

$$\mathrm{N}(r) < \mathrm{N}(a).$$

Then R is said to be a *Euclidean domain*. (This is not exactly the standard definition, but it will suffice for our purposes.)

EXAMPLE 4.6. $\mathbb{Z}$ is a Euclidean domain with $\mathrm{N}(a) = |a|$ for $a \neq 0$ and $\mathrm{N}(0) = -1$. A polynomial ring over a field is a Euclidean domain with N the degree function, where we take the zero polynomial to have degree -1.

PROPOSITION 4.7. *Let R be a Euclidean domain. Then R is a PID, and thus a UFD.*

PROOF. Let $a, b \in R$ and let $I = (a, b)$. We will show that I is principal. This will suffice to show that R is a PID, since every ideal of R has a finite generating set, and repeated application of the above fact will show that every ideal is principal.

We prove that I is principal by induction on $\mathrm{N}(a)$. If $\mathrm{N}(a) = -1$, then $a = 0$, so $I = (b)$, which is principal. Suppose then that we know that (a', b') is principal for all a' with $\mathrm{N}(a') < n$ and all b'. Let a be an element with $\mathrm{N}(a) \leq n$, let b be any element, and let $I = (a, b)$. Since R is Euclidean we can find $q, r \in R$ with $a = bq + r$ and $\mathrm{N}(r) < \mathrm{N}(a)$. Note that $a - bq, b$ generate the same ideal as a, b, so

$$I = (a, b) = (a - bq, b) = (r, b).$$

But now by the induction hypothesis I is principal, since $\mathrm{N}(r) < n$. This completes the induction. $\square$

It is not true that every PID is Euclidean, although counterexamples are fairly hard to give.

5. Finitely generated modules

We give in this section a quick review of finitely generated modules over rings. Let R be a commutative ring; an *R-module* M is an abelian group with an action of R; that is, for every $r \in R$ and $m \in M$ we have defined an element $rm \in M$ such that $1m = m$, $(rs)m = r(sm)$ and $(r + s)m = rm + sm$ for all $r, s \in R$ and $m \in M$. In the case that R is a field, an R-module is nothing more than an R-vector space.

Let M be an R-module and let S be some subset of M. The *R-module generated by S* is the set of linear combinations of elements of S with coefficients in R. If the R-module generated by S is all of M, then S is said to *generate* M. If there is some finite set $S \subseteq M$ such that S generates M, then M is said to be *finitely-generated over R*. That is, M is said to be finitely generated over R if there are elements $m_1, \ldots, m_n \in M$ such that

$$M = \{r_1 m_1 + \cdots + r_n m_n \mid r_i \in R\}.$$

Let n be a positive integer and let R^n denote the R-module of n-tuples of elements of R, with all operations done componentwise. R^n is called a *free R-module of rank n*; more generally, any module isomorphic to R^n is said to be free of rank n.

Now let R be a principal ideal domain and let M be a finitely-generated R-module. Let M' be the sub-module of $m \in M$ of elements for which there exists $r \in R$, $r \neq 0$, such that $rm = 0$; M' is called the *torsion sub-module* of M. It is a basic fact that

$$M \cong M' \oplus R^n$$

for some (unique) integer n. (The integer n is called the *rank* of M.) In particular, if M is torsion-free (meaning that $M' = 0$) and finitely-generated, then it is free. See [**13**, Chapter 3, Theorem 7, p. 147] for details.

Continue to let R be a principal ideal domain and let M and N be two finitely-generated R-modules such that $M \subseteq N$. One shows easily that the rank of M is less then or equal to the rank of N. In particular, if $M \subseteq N \subseteq P$ and M and P both have rank n, then N also has rank n. If P is also torsion-free, then N is as well, so it must be free of rank n.

APPENDIX D

Solutions to Exercises

1. Chapter 1

SOLUTION 1.1. Write

$$f(x) = \frac{a_n}{b_n}x^n + \cdots + \frac{a_0}{b_0}$$

where each fraction a_i/b_i is in lowest terms. Let a be the greatest common divisor of the a_i and let b be the least common multiple of the b_i. We claim that $c = \frac{b}{a}$ is the unique rational number such that $cf(x)$ is primitive. In fact, this is quite easy to see, as multiplying by b has the effect of clearing all denominators, and dividing by a has the effect of removing any common factors from the numerators.

SOLUTION 1.2. Let $f(x)$ and $g(x)$ be primitive polynomials and suppose that there is some prime p which divides every coefficient of $f(x)g(x)$. Then

$$f(x)g(x) \equiv 0 \pmod{p};$$

since $\mathbb{F}_p[x]$ is an integral domain this implies that either

$$f(x) \equiv 0 \pmod{p}$$

or

$$g(x) \equiv 0 \pmod{p}.$$

This contradicts the assumption that $f(x)$ and $g(x)$ were primitive, so $f(x)g(x)$ must have been primitive as well.

SOLUTION 1.3. It is clear that if $f(x)$ factors in $\mathbb{Z}[x]$, then it factors in $\mathbb{Q}[x]$, so we will prove the converse. Suppose that we can write $f(x) = g(x)h(x)$ with $g(x), h(x) \in \mathbb{Q}[x]$. We must show that we can write $f(x) = g'(x)h'(x)$ with $g'(x), h'(x) \in \mathbb{Z}[x]$. Let $a, b, c \in \mathbb{Q}^*$ be the rational numbers such that $af(x)$, $bg(x)$, $ch(x)$ are all primitive. Since $f(x) \in \mathbb{Z}[x]$, we must have $1/a \in \mathbb{Z}$.

We claim that $af(x) = bg(x)ch(x)$. To see this, note that $af(x)$ is primitive by definition and $bg(x)ch(x)$ is primitive by Exercise 1.2. Furthermore, these polynomials are rational multiples of each other since $f(x) = g(x)h(x)$. But any given polynomial has only one rational multiple which is primitive, so these polynomials must be equal, as claimed.

We now have

$$f(x) = \frac{1}{a}(bg(x))(ch(x));$$

$\frac{1}{a} \in \mathbb{Z}$ and $bg(x), ch(x) \in \mathbb{Z}[x]$, so this yields a a factorization of $f(x)$ in $\mathbb{Z}[x]$.

SOLUTION 1.4. This is a special case of Exercise 1.3, using the fact that we have $b, c \in \mathbb{Z}$ (since $g(x), h(x)$ are monic) and $a = 1$ (since $f(x)$ is monic and integral, and thus primitive).

SOLUTION 1.5. By the division algorithm in $\mathbb{Q}[x]$, we can find polynomials $q(x), r(x) \in \mathbb{Q}[x]$ with

$$f(x) = q(x)(x - \alpha) + r(x)$$

and $\deg r(x) < \deg(x - \alpha) = 1$. Thus $r(x)$ is a constant polynomial. Plugging in α and using the fact that $f(\alpha) = 0$, we conclude that $r(x)$ is the zero polynomial. Thus $f(x) = q(x)(x - \alpha)$, so $x - \alpha$ divides $f(x)$ in $\mathbb{Q}[x]$.

Now let $f(x)$ have degree 2 or 3. If $f(x)$ has a rational root, then what we just proved shows that $f(x)$ is not irreducible. Conversely, if $f(x)$ is not irreducible, then it has some factor $g(x)$. If $g(x)$ is linear, say $g(x) = x - \alpha$, then $f(x)$ has the rational root α. If $g(x)$ is not linear, then $f(x)$ must be cubic and $g(x)$ must be quadratic; now $f(x)/g(x)$ is a linear polynomial dividing $f(x)$, which in turn yields a rational root of $f(x)$.

SOLUTION 1.6. We prove the contrapositive. So suppose that $f(x) = g(x)h(x)$ in $\mathbb{Q}[x]$. Since $f(x)$ is primitive, Exercise 1.3 shows that we can assume $g(x), h(x) \in \mathbb{Z}[x]$. Reducing modulo p, we find that $\bar{f}(x)$ factors as $\bar{g}(x)\bar{h}(x)$, so $f(x)$ is not irreducible in $\mathbb{F}_p[x]$.

SOLUTION 1.7. Suppose that $f(x)$ factors as $g(x)h(x)$ in $\mathbb{Q}[x]$; as usual, we can assume that $g(x), h(x) \in \mathbb{Z}[x]$. Modulo p we have

$$f(x) \equiv a_n x^n \pmod{p},$$

and a_n is non-zero modulo p. It follows from unique factorization in $\mathbb{F}_p[x]$ that $\bar{g}(x), \bar{h}(x) \in \mathbb{F}_p[x]$ are monomials, say

$$\bar{g}(x) = bx^d, \bar{h}(x) = cx^{n-d}$$

with $bc \equiv a_n \pmod{p}$. Also, we can not have $d = 0$ or $d = n$ since then either $g(x)$ or $h(x)$ would have degree n, which would contradict the fact that $f(x)$ factors.

In particular, we find that the constant terms of $g(x)$ and $h(x)$ are divisible by p. The constant term of $f(x)$ is the product of these two constant terms, so it is divisible by p^2. This contradicts our hypotheses on $f(x)$, so $f(x)$ must have been irreducible.

SOLUTION 1.8. This is an immediate application of Exercise 1.7.

SOLUTION 1.9. Substituting $y + 1 = x$, we have

$$\begin{aligned} \frac{x^p - 1}{x - 1} &= \frac{(y+1)^p - 1}{y} \\ &= \frac{1}{y}\left(y^p + \binom{p}{p-1}y^{p-1} + \cdots + \binom{p}{1}y + 1 - 1\right) \\ &= y^{p-1} + \binom{p}{p-1}y^{p-2} + \cdots + \binom{p}{1}. \end{aligned}$$

It is well known (and easy to prove) that p divides $\binom{p}{i}$ for all $i \neq 0, p$. Since $\binom{p}{1} = p$, we now see that the above polynomial is an Eisenstein polynomial, so Exercise 1.7 shows that it is irreducible in $\mathbb{Q}[x]$. (Note that any factorization involving y can be converted into a factorization involving x, so "irreducible with respect to y" and "irreducible with respect to x" are the same thing.)

SOLUTION 1.10. Note that if $f(x) = x^4 - 10x^2 + 1$ factors, then it has either a linear factor or a quadratic factor. We show first that it has no linear factor. So suppose that it does; by Exercise 1.5 it then has a rational root $\frac{a}{b}$ with a, b relatively prime. Thus

$$\begin{aligned}\left(\frac{a}{b}\right)^4 - 10\left(\frac{a}{b}\right)^2 + 1 &= 0\\ a^4 - 10a^2b^2 + b^4 &= 0.\end{aligned}$$

Now, if any prime p divides b, then this implies that it also divides a. Since we assumed a and b were relatively prime, we must have $b = 1$. The same argument shows that we must have $a = 1$, and now we check immediately that $\frac{a}{b} = 1$ is not a root of $f(x)$. Thus $f(x)$ has no linear (and therefore no cubic) factors.

It remains to check that $f(x)$ has no quadratic factors. So suppose that $f(x) = g(x)h(x)$ with $g(x), h(x)$ quadratic; by Exercise 1.3 and Exercise 1.4 we can assume that $g(x), h(x)$ are monic with integer coefficients. Thus

$$\begin{aligned}x^4 - 10x^2 + 1 &= (x^2 + ax + b)(x^2 + cx + d)\\ &= x^4 + (a + c)x^3 + (ac + b + d)x^2 + (ad + bc)x + bd.\end{aligned}$$

We conclude that $a = -c$, $ac + b + d = -10$ and $b = d = \pm 1$. If $b = d = 1$, then

$$-10 = ac + b + d = -a^2 + 2,$$

so $a^2 = 12$, which doesn't work. If $b = d = -1$, then

$$-10 = ac + b + d = -a^2 - 2,$$

so $a^2 = 8$, which also doesn't work. Thus $f(x)$ has no quadratic factors, and thus is irreducible.

Solution 1.11. Linearity is immediate. To check the product rule, we first check it for products of monomials:

$$\begin{aligned}\big((x^m)(x^n)\big)' &= \big(x^{m+n}\big)'\\ &= (m + n)x^{m+n-1}\\ &= (mx^{m-1})(x^n) + (x^m)(nx^{n-1})\\ &= (x^m)'(x^n) + (x^m)(x^n)'.\end{aligned}$$

Next, we use linearity to show that if $f(x)$ and $g(x)$ both satisfy the product rule with $h(x)$, then $f(x) + g(x)$ also satisfies the product rule with $h(x)$:

$$\begin{aligned}\big((f(x) + g(x))h(x)\big)' &= (f(x)h(x))' + (g(x)h(x))'\\ &= f'(x)h(x) + f(x)h'(x) + g'(x)h(x) + g(x)h'(x)\\ &= (f'(x) + g'(x))h(x) + (f(x) + g(x))h'(x)\\ &= (f(x) + g(x))'h(x) + (f(x) + g(x))h'(x).\end{aligned}$$

These two calculations and an easy induction prove the product rule in general.

For the chain rule, a similar linearity calculation reduces us to checking that for any polynomial $f(x)$,

$$\big(f(x)^n\big)' = nf(x)^{n-1}f'(x).$$

We prove this formula by induction on n, the case $n = 1$ being obvious. So, suppose that we know that the above formula holds. Then, using the product rule, we compute that

$$\begin{aligned}\big(f(x)^{n+1}\big) &= \big(f(x)^n f(x)\big)\\ &= \big(f(x)^n\big)' f(x) + f(x)^n f'(x)\\ &= nf(x)^{n-1}f'(x)f(x) + f(x)^n f'(x)\\ &= (n+1)f(x)^n f'(x)\end{aligned}$$

which completes the induction.

Now, suppose that $g(x)^2$ divides $f(x)$. Write $f(x) = g(x)^2h(x)$ for some $h(x) \in K[x]$. Then by the product rule and the chain rule

$$\begin{aligned}f'(x) &= \big(g(x)^2\big)' h(x) + g(x)^2h'(x)\\ &= 2g(x)g'(x)h(x) + g(x)^2h'(x)\\ &= g(x)\big(2g'(x)h(x) + g(x)h'(x)\big)\end{aligned}$$

which shows that $g(x)$ divides $f'(x)$.

Solution 1.12. First, note that $f(x)$ and $f'(x)$ are relatively prime in $K[x]$, since $f(x)$ is irreducible in $K[x]$ and $f'(x)$ is non-zero of smaller degree than $\deg f(x)$. (This requires the assumption that K is of characteristic 0, since otherwise it is possible for $f'(x)$ to be zero.) This implies that there exist $r(x), s(x) \in K[x]$ such that

$$f(x)r(x) + f'(x)s(x) = 1.$$

This equality continues to hold in $L[x]$, so $f(x)$ and $f'(x)$ must be relatively prime in $L[x]$ as well.

Now, suppose that $f(x) = g(x)^2h(x)$ in $L[x]$. Then by Exercise 1.11 $g(x)$ divides $f'(x)$. In particular, $f(x)$ and $f'(x)$ are not relatively prime. This is a contradiction, so $f(x)$ can not have any repeated factors in $L[x]$.

Solution 1.13. We apply Lemma I.5.9 with $L_1 = K(\alpha)$ and $L_2 = L$; our hypothesis is that $L_1 \cap L_2 = K$. Note that $L_1L_2 = L(\alpha)$, so the lemma tells us that $[L(\alpha) : L] = [K(\alpha) : K]$. In particular, the minimal polynomial of α over L has the same degree as the minimal polynomial of α over K; since $f(x)$ is a polynomial of this degree which α satisfies, it must be the minimal polynomial.

Solution 1.14. Let n be the degree $[L : K]$ and let $\gamma_1, \ldots, \gamma_n$ be a basis for L over K. Let m_α and m_β be the matrices for the linear transformations on L defined by multiplication by α and β respectively. Then

$$\begin{aligned}m_\alpha + m_\beta &= m_{\alpha+\beta};\\ m_\alpha m_\beta &= m_{\alpha\beta};\\ m_\alpha^{-1} &= m_{\alpha^{-1}}.\end{aligned}$$

Thus, if we can determine the matrices for α and β we can also determine the matrices for $\alpha+\beta$, $\alpha\beta$ and α^{-1}. The Cayley-Hamilton theorem tells us that these matrices satisfy their characteristic polynomials (which again we can compute), and one concludes that $\alpha+\beta$, $\alpha\beta$ and α^{-1} satisfy the characteristic polynomials of $m_\alpha + m_\beta$, $m_\alpha m_\beta$ and m_α^{-1} respectively.

For a silly example where this does not yield a minimal polynomial, take $K = \mathbb{Q}$, $L = \mathbb{Q}(\sqrt{2})$, $\alpha = \beta = 1$. One computes that the characteristic polynomial of $m_\alpha + m_\beta$ is $(x-2)^2$, which is the square of the minimal polynomial of $\alpha + \beta$.

Now take $L = \mathbb{Q}(\sqrt{2}, \sqrt{3})$. We take as our basis $1, \sqrt{2}, \sqrt{3}, \sqrt{6}$. The matrix of $\sqrt{2}+\sqrt{3}$ is now

$$\begin{pmatrix} 0 & 2 & 3 & 0 \\ 1 & 0 & 0 & 3 \\ 1 & 0 & 0 & 2 \\ 0 & 1 & 1 & 0 \end{pmatrix}$$

This has characteristic polynomial

$$x^4 - 10x^2 + 1.$$

Furthermore, by Exercise 1.10 we know that this polynomial is irreducible over $\mathbb{Q}$, so it must be the minimal polynomial of $\sqrt{2}+\sqrt{3}$.

Solution 1.15. Note that in $\mathbb{F}_p[x]$

$$\begin{aligned}(x+y)^p &= x^p + \binom{p}{p-1}x^{p-1}y + \binom{p}{p-2}x^{p-2}y^2 + \cdots + \binom{p}{1}xy^{p-1} + y^p \\ &= x^p + y^p\end{aligned}$$

since p divides $\binom{p}{i}$ for $i \neq 0, p$. Using this, if $f(x) = a_n x^n + \cdots + a_0$, we find that

$$\begin{aligned}f(x)^p =& \big(a_n x^n + \cdots + a_0\big)^p \\ =& (a_n x^n)^p + \big(a_{n-1}x^{n-1} + \cdots + a_0\big)^p \\ =& (a_n x^n)^p + (a_{n-1}x^{n-1})^p + \big(a_{n-2}x^{n-2} + \cdots + a_0\big)^p \\ & \vdots \\ =& (a_n x^n)^p + (a_{n-1}x^{n-1})^p + \cdots + (a_0)^p.\end{aligned}$$

The fact that $a_n^p = a_n$ for $a_n \in \mathbb{F}_p$ shows that this is just

$$a_n x^{np} + a_{n-1}x^{(n-1)p} + \cdots + a_0 = f(x^p).$$

Solution 1.16. We begin with some trace computations. Let Tr be the trace from $\mathbb{Q}(\sqrt[4]{2})$ to $\mathbb{Q}$. $\sqrt[4]{2}$ has minimal polynomial $x^4 - 2$ by Exercise 1.8, so we have $\mathrm{Tr}(\sqrt[4]{2}) = 0$ by definition of the trace. $\sqrt{2}$ has characteristic polynomial $(x^2-2)^2$ by Corollary A.4.4, so we again find that $\mathrm{Tr}(\sqrt{2}) = 0$. Next, $\sqrt[4]{8}$ has minimal polynomial $x^4 - 8$ (we can not apply Exercise 1.8 here, but we can see that this polynomial is irreducible since $\sqrt[4]{8}$ and $\sqrt[4]{2} = 2/\sqrt[4]{8}$ generate the same extension of $\mathbb{Q}$ and thus have the same degree), so also $\mathrm{Tr}(\sqrt[4]{8}) = 0$.

Assuming that $\sqrt{3} \in \mathbb{Q}(\sqrt[4]{2})$, it will have characteristic polynomial $(x^2-3)^2$ and thus by Corollary A.4.4 also $\mathrm{Tr}(\sqrt{3}) = 0$. Writing

$$\sqrt{3} = a + b\sqrt[4]{2} + c\sqrt{2} + d\sqrt[4]{8}$$

and using the linearity of the trace and our trace computations, we find that $4a = 0$, so $a = 0$. Thus

$$\frac{\sqrt{3}}{\sqrt[4]{2}} = b + c\sqrt[4]{2} + d\sqrt{2}.$$

$\sqrt{3}/\sqrt[4]{2}$ has minimal polynomial $x^4 - \frac{9}{2}$ (it is easy to check that this is irreducible), so it has trace 0. As before we conclude that $4b = 0$, so $b = 0$. Dividing again we find that

$$\sqrt{\frac{3}{2}} = c + d\sqrt[4]{2}.$$

$\sqrt{\frac{3}{2}}$ has minimal polynomial $x^2 - \frac{3}{2}$, and characteristic polynomial $(x^2 - \frac{3}{2})^2$; thus it has trace 0. Once again we conclude that $c = 0$, so we find that

$$\frac{\sqrt{3}}{\sqrt[4]{8}}$$

is rational, which is absurd. Thus $\sqrt{3} \notin \mathbb{Q}(\sqrt[4]{2})$.

SOLUTION 1.17. We will prove by induction on n that $\mathbb{Q}(\sqrt{d_1}, \ldots, \sqrt{d_n})$ has $\mathbb{Q}$-basis

$$\left\{ \sqrt{d_1}^{\varepsilon_1} \cdots \sqrt{d_n}^{\varepsilon_n} \mid \varepsilon_i = 0, 1 \right\}.$$

This will prove the result since this basis has 2^n elements.

The case $n = 1$ is clear. For the general case, we assume that

$$K = \mathbb{Q}(\sqrt{d_1}, \ldots, \sqrt{d_{n-1}})$$

has degree 2^{n-1} with the asserted basis and we wish to show that

$$L = K(\sqrt{d_n})$$

has degree 2^n with the asserted basis. To do this it will suffice to show that $[L : K] = 2$; the fact that the basis is as claimed will follow immediately from the methods of the proof of Lemma A.1.1, using the basis $1, \sqrt{d_n}$ for L/K. To prove that $[L : K] = 2$, it will suffice to show that

$$\sqrt{d_n} \notin K.$$

So suppose that $\sqrt{d_n} \in K$. Then we can write

$$\sqrt{d_n} = \sum a_{\varepsilon_1 \cdots \varepsilon_{n-1}} \sqrt{d_1}^{\varepsilon_1} \cdots \sqrt{d_{n-1}}^{\varepsilon_{n-1}}$$

with $a_{\varepsilon_1 \cdots \varepsilon_{n-1}} \in \mathbb{Q}$ and $\varepsilon_i = 0, 1$. Let $\sqrt{m}$ be one of the basis elements other than 1. Then m is not a perfect square (since the d_i are relatively prime), so $\sqrt{m}$ will have characteristic polynomial $(x^2 - m)^{2^{n-2}}$ in K. In particular, it has trace 0. Since $\sqrt{d_n}$ also has trace 0, taking traces of the above equality shows that

$$a_{0,\ldots,0} = 0;$$

that is, the coefficient of 1 is 0.

One can now divide through by $\sqrt{d_1}$ and repeat the above argument. Once again every element but one will have trace 0 (we use the fact that the d_i are relatively prime to insure that we only get the one such basis element), and we conclude that

$$a_{1,0,\ldots,0} = 0.$$

Similarly, dividing through by $\sqrt{d_1 d_2}$ will show that

$$a_{1,1,0,\ldots,0} = 0;$$

Continuing in this way one finds that every coefficient is 0, which is a contradiction. Thus $\sqrt{d_n} \notin K$, which proves the result.

This result allows us to prove the following: let $d_1, \ldots, d_n$ be any rational numbers which are not squares. Then the only rational number of the form

$$a_1 \sqrt{d_1} + \cdots + a_n \sqrt{d_n}$$

with $a_i \in \mathbb{Q}$ is 0.

To prove this, let $p_1, \ldots, p_m$ be the prime factors of the numerators and denominators of the d_i. We have just shown that the numbers

$$\left\{ \sqrt{p_1^{\varepsilon_1} \cdots p_m^{\varepsilon_m}} \mid \varepsilon_i = 0, 1 \right\}$$

are linearly independent over $\mathbb{Q}$. Each $\sqrt{d_i}$ is a rational multiple of one of these basis elements, and since none of the d_i are squares, none of them are rational multiples of 1. The result now follows from the fact that these numbers (including 1) are all linearly independent over $\mathbb{Q}$.

Solution 1.18. Since $5 \cdot 72^\circ = 360^\circ$, we wish to find a formula for $\cos(5x)$ in terms of $\cos(x)$. To do this, we use the fact that

$$e^{ix} = \cos(x) + i \sin(x).$$

We find that

$$\begin{aligned}
\cos(5x) + i\sin(5x) &= e^{i5x} \\
&= \left(e^{ix}\right)^5 \\
&= (\cos(x) + i\sin(x))^5 \\
&= \cos^5(x) + 5i\cos^4(x)\sin(x) - 10\cos^3(x)\sin^2(x) + \\
&\quad - 10i\cos^2(x)\sin^3(x) + 5\cos(x)\sin^4(x) + i\sin^5(x).
\end{aligned}$$

Equating real parts we find that

$$\begin{aligned}
\cos(5x) &= \cos^5(x) - 10\cos^3(x)\sin^2(x) + 5\cos(x)\sin^4(x) \\
&= \cos^5(x) - 10\cos^3(x)(1 - \cos^2(x)) + 5\cos(x)(1 - \cos^2(x))^2 \\
&= 16\cos^5(x) - 20\cos^3(x) + 5\cos(x).
\end{aligned}$$

Plugging in $x = 72^\circ$, we find that $\cos(72^\circ)$ satisfies

$$f(x) = 16x^5 - 20x^3 + 5x - 1.$$

Next, $(\sqrt{5} - 1)/4$ has conjugate $(-\sqrt{5} - 1)/4$ and thus minimal polynomial

$$g(x) = \left(x - \frac{\sqrt{5} - 1}{4}\right)\left(x - \frac{-\sqrt{5} - 1}{4}\right) = x^2 + \frac{1}{2}x - \frac{1}{4}.$$

We find that $g(x)$ does indeed divide $f(x)$, with quotient

$$16x^3 - 8x^2 - 12x + 4.$$

In fact, $g(x)$ divides this as well, with quotient

$$16x - 16.$$

Thus $\cos(72^\circ)$ satisfies

$$f(x) = 16\left(x^2 + \frac{1}{2}x - \frac{1}{4}\right)^2 (x - 1).$$

Since certainly $\cos(72^\circ)$ does not equal 1, this implies that $\cos(72^\circ)$ is a root of $g(x)$. Any sort of approximation now determine which root it is and completes the proof.

SOLUTION 1.19. The trace is easy to compute. Recall that $\mathbb{Q}(\zeta_5)$ has $\mathbb{Q}$-basis $1, \zeta_5, \zeta_5^2, \zeta_5^3$, and each of the primitive 5^{th} roots of unity has minimal polynomial

$$x^4 + x^3 + x^2 + x + 1$$

and thus trace -1. Linearity of the trace now shows that

$$\operatorname{Tr}_{\mathbb{Q}(\zeta_5)/\mathbb{Q}}(a + b\zeta_5 + c\zeta_5^2 + d\zeta_5^3) = 4a - b - c - d.$$

One can attempt to compute the norm directly, but it gets quite ugly. It is more efficient to use Exercise 1.18. Recall that

$$\zeta_5 = \cos(72^\circ) + i\sin(72^\circ).$$

We know from Exercise 1.18 that

$$\cos(72^\circ) = \frac{\sqrt{5} - 1}{4},$$

so

$$\zeta_5 + \zeta_5^4 = \zeta_5 + \overline{\zeta_5} = 2\cos(72^\circ) = \frac{\sqrt{5} - 1}{2}.$$

Thus $\sqrt{5} \in \mathbb{Q}(\zeta_5)$. This means that we can consider $\mathbb{Q}(\zeta_5)$ as a sequence of two quadratic extensions; we can now use Lemma A.4.6 to cut down on our work.

We will first compute

$$\mathrm{N}_{\mathbb{Q}(\zeta_5)/\mathbb{Q}(\sqrt{5})}(a + b\zeta_5 + c\zeta_5^2 + d\zeta_5^3)$$

using Corollary I.5.4. We first need to know the conjugates of ζ_5 over $\mathbb{Q}(\sqrt{5})$. There are many ways to see that the conjugates of ζ_5 are ζ_5 and ζ_5^4; for example, one can use the fact that $\zeta_5 + \zeta_5^4$ is in $\mathbb{Q}(\sqrt{5})$ and thus fixed by $\operatorname{Gal}(\mathbb{Q}(\zeta_5)/\mathbb{Q}(\sqrt{5}))$. Similarly, ζ_5^2 and ζ_5^3 are conjugates. We now have

$$\mathrm{N}_{\mathbb{Q}(\zeta_5)/\mathbb{Q}(\sqrt{5})}(a + b\zeta_5 + c\zeta_5^2 + d\zeta_5^3) = (a + b\zeta_5 + c\zeta_5^2 + d\zeta_5^3)(a + b\zeta_5^4 + c\zeta_5^3 + d\zeta_5^2).$$

Multiplying this out (which is quite easy) we get

$$(a^2 + b^2 + c^2 + d^2) + (ab + bc + cd)(\zeta_5 + \zeta_5^4) + (ac + ad + bd)(\zeta_5^2 + \zeta_5^3).$$

Since $\zeta_5^4 = -1 - \zeta_5 - \zeta_5^2 - \zeta_5^3$ this equals

$$(a^2 + b^2 + c^2 + d^2 - ab - bc - cd) + (ac + ad + bd - ab - bc - cd)(\zeta_5^2 + \zeta_5^3).$$

We now need to compute the norm from $\mathbb{Q}(\sqrt{5})$ to $\mathbb{Q}$ of this expression. We have

$$\zeta_5^2 + \zeta_5^3 = 2\cos(144^\circ);$$

using the double angle formula we find that this is

$$\frac{-1 - \sqrt{5}}{2}.$$

Our expression therefore equals (after some simplification)

$$\left(a^2 + b^2 + c^2 + d^2 - \frac{1}{2}(ab + ac + ad + bc + bd + cd)\right) -$$
$$\frac{1}{2}(ac + ad + bd - ab - bc - cd)\sqrt{5}.$$

Using the formula for norms from $\mathbb{Q}(\sqrt{5})$, we finally find that

$$\mathrm{N}_{\mathbb{Q}(\zeta_5)/\mathbb{Q}}(a + b\zeta_5 + c\zeta_5^2 + d\zeta_5^3) =$$

$$\left(a^2+b^2+c^2+d^2-\frac{1}{2}(ab+ac+ad+bc+bd+cd)\right)^2 -$$
$$\frac{5}{4}\left(ac+ad+bd-ab-bc-cd\right)^2.$$

SOLUTION 1.20. The fact that $\varphi(mn)=\varphi(m)\varphi(n)$ is immediate from the fact that

$$\mathbb{Z}/mn\mathbb{Z} \cong \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}.$$

This isomorphism is given by sending a to the ordered pair (a,a): it is easily seen to be a homomorphism; it is injective since its kernel consists of those integers divisible by both m and n, and thus by mn since m and n are relatively prime; and it then must be surjective since each ring has the same size. This isomorphism of rings implies immediately that

$$(\mathbb{Z}/mn\mathbb{Z})^* \cong (\mathbb{Z}/m\mathbb{Z})^* \times (\mathbb{Z}/n\mathbb{Z})^*;$$

since the left-hand side has size $\varphi(mn)$ and the right-hand side has size $\varphi(m)\varphi(n)$, this proves the formula.

We compute $\varphi(p^k)$ directly. Specifically, an integer is relatively prime to p^k if and only if it is not divisible by p. The integers in

$$1, 2, \cdots, p^k$$

which are divisible by p are precisely

$$p, 2p, \cdots, p^k.$$

There are p^{k-1} of these integers, and subtracting this from the p^k total yields the formula.

2. Chapter 2

SOLUTION 2.1. We wish to solve the Diophantine equation

$$x^2 + 21^2 = z^2.$$

Factoring this equation, we are interested in

$$(z+x)(z-x) = 21^2.$$

As in Example 1.1 solving this equation amounts to determining all complimentary pairs (d, e) of factors of 21^2 such that $d \equiv e \pmod 2$. These pairs (up to negation and reordering) are

$$(d, e) = (441, 1), (147, 3), (63, 7), (49, 9), (21, 21).$$

These give rise to the solutions

$$(x, z) = (220, 221), (72, 75), (28, 35), (20, 29), (0, 21).$$

Of course, the last solution doesn't really count.

SOLUTION 2.2. The case $p = 2$ is obvious, so we can assume that p is odd. Choose a generator g of the cyclic group $(\mathbb{Z}/p\mathbb{Z})^*$. The polynomial $x^2 - 1$ has at most 2 roots in $\mathbb{Z}/p\mathbb{Z}$, so -1 and 1 are the only elements of $(\mathbb{Z}/p\mathbb{Z})^*$ of square 1. Since p is odd this implies that

$$g^{(p-1)/2} = -1,$$

since both elements have square 1. Since $(\mathbb{Z}/p\mathbb{Z})^*$ is cyclic of even order, $g^{(p-1)/2}$ will be a square if and only if $(p-1)/2$ is even; that is, if and only if

$$p \equiv 1 \pmod 4.$$

For an explicit square root when $p \equiv 1 \pmod 4$, we will show that

$$s = 1 \cdot 2 \cdot 3 \cdots \frac{p-3}{2} \cdot \frac{p-1}{2} \in \mathbb{Z}/p\mathbb{Z}$$

has square -1. To see this, recall first that

$$(p-1)! \equiv -1 \pmod p;$$

this is proven by pairing up inverses and observing that only ± 1 are left. If we set

$$s' = \frac{p+1}{2} \cdot \frac{p+3}{2} \cdots (p-2) \cdot (p-1) \in \mathbb{Z}/p\mathbb{Z},$$

this tells us that $ss' = -1$ in $\mathbb{Z}/p\mathbb{Z}$. However, there are $(p-1)/2$ terms in the product for s'; $(p-1)/2$ is even, so we can put in $(p-1)/2$ minus signs and we find that

$$\begin{aligned}
s' &\equiv -\frac{p+1}{2} \cdot -\frac{p+3}{2} \cdots -(p-2) \cdot -(p-1) \pmod p \\
&\equiv \frac{p-1}{2} \cdot \frac{p-3}{2} \cdots 2 \cdot 1 \\
&\equiv s.
\end{aligned}$$

Thus $s^2 = -1$ in $\mathbb{Z}/p\mathbb{Z}$.

SOLUTION 2.3. Recall that we have a prime π of $\mathbb{Z}[i]$ which divides some positive prime $p \in \mathbb{Z}$ such that $p \equiv 1 \pmod 4$. We know that p is not prime in $\mathbb{Z}[i]$, so p and π are not associates. Setting $\pi' = p/\pi$, we have

$$p^2 = N(p) = N(\pi)N(\pi');$$

the fact π and π' are not units implies that they both have norm p; in particular, π' is prime as well. Furthermore, the fact that $\pi\pi'$ is real implies that π' is a real multiple of $\bar{\pi}$; since $\bar{\pi}$ and π' have the same norm, this implies that $\pi' = \bar{\pi}$.

It remains to show that π and $\bar{\pi}$ are not associate and that every prime π'' of norm p is associate to one of them. The second fact is easy; such a π'' divides $p = \pi\bar{\pi}$ in $\mathbb{Z}[i]$, so the fact that $\mathbb{Z}[i]$ is a UFD implies that it divides (and thus is associate to) one of π and $\bar{\pi}$. To see that π and $\bar{\pi}$ are not associate one simply has to check that if $x + yi \in \mathbb{Z}[i]$ and $x \neq y$ and $x, y \neq 0$ (as is easily seen to be the case here, since p is not even), then none of $\pm(x + yi)$ and $\pm i(x + yi)$ are equal to $\overline{x + yi} = x - yi$. This is easy.

SOLUTION 2.4. Note that for $\alpha = a + b\sqrt{-2} \in \mathbb{Z}[\sqrt{-2}]$ we have

$$N(\alpha) = a^2 + 2b^2 = \alpha\bar{\alpha}$$

where $\bar{\alpha}$ denotes the complex conjugate of α. Given this, the proof of Lemma 1.2 carries over exactly to this situation; the only difference is the bound on the remainder. More precisely, we can again write

$$\alpha = \beta q + r$$

where $r = r_1 + r_2\sqrt{-2}$ and $|r_i| \leq \frac{1}{2}\,\mathrm{N}(\beta)$. Thus

$$\begin{aligned}
\bar{\beta} r &= r_1 + r_2\sqrt{-2} \\
N(\bar{\beta})N(r) &= N(r_1 + r_2\sqrt{-2}) \\
N(r) &= \frac{N(r_1 + r_2\sqrt{-2})}{N(\beta)} \\
&= \frac{r_1^2 + 2r_2^2}{N(\beta)} \\
&\leq \frac{N(\beta)^2 + 2N(\beta)^2}{N(\beta)} \\
&= \frac{3}{4}N(\beta).
\end{aligned}$$

In particular, $N(r) < N(\beta)$, which is enough to show that $\mathbb{Z}[\sqrt{-2}]$ is Euclidean and thus is a UFD.

The analysis of primes in $\mathbb{Z}[\sqrt{-2}]$ is very similar to that in $\mathbb{Z}[i]$. The analogues of Lemma 1.3 and Lemma 1.4 continue to hold, so we are again reduced to factoring primes of $\mathbb{Z}$ in $\mathbb{Z}[\sqrt{-2}]$. 2 once again behaves strangely; it factors as

$$2 = -(\sqrt{-2})^2,$$

and $\sqrt{-2}$ is prime since it has norm 2.

For the other primes, suppose first that p factors in $\mathbb{Z}[\sqrt{-2}]$. Then as in $\mathbb{Z}[i]$ we conclude that there is an element $\alpha = a + b\sqrt{-2} \in \mathbb{Z}[\sqrt{-2}]$ with

$$a^2 + 2b^2 = N(\alpha) = p.$$

Clearly we can not have a or b divisible by p, so we find that

$$\begin{aligned} a^2 + 2b^2 &\equiv 0 \pmod{p} \\ a^2 &\equiv -2b^2 \\ \left(\frac{a}{b}\right)^2 &\equiv -2. \end{aligned}$$

Thus if p factors, then -2 is a square modulo p.

Conversely, if -2 is a square modulo p, then we can find $a \in \mathbb{Z}$ with

$$a^2 \equiv -2 \pmod{p};$$

Thus p divides $a^2 + 2 = (a + \sqrt{-2})(a - \sqrt{-2})$ in $\mathbb{Z}[\sqrt{-2}]$. If p were prime, then p would divide one of $a \pm \sqrt{-2}$, which can not happen since p does not divide the coefficient of $\sqrt{-2}$. We conclude that p factors in $\mathbb{Z}[\sqrt{-2}]$ if and only if -2 is a square modulo p. Using quadratic reciprocity one can show that this occurs if and only $p \equiv 1, 7 \pmod{8}$.

As with $\mathbb{Z}[i]$ and $x^2 + y^2$, the study of the quadratic form $x^2 + 2y^2$ is closely connected with primes in $\mathbb{Z}[\sqrt{-2}]$. Specifically, one proves exactly as with Proposition 1.7 that a positive prime p can be written in the form $x^2 + 2y^2$ if and only if p factors in $\mathbb{Z}[\sqrt{-2}]$. Our above results show that this occurs if and only $p = 2$ or $p \equiv 1, 7 \pmod{8}$.

Solution 2.5. The proof that $\mathbb{Z}[\zeta_3]$ is Euclidean is virtually identical to that for $\mathbb{Z}[i]$ and $\mathbb{Z}[\sqrt{-2}]$. The only difference is the the norm form is slightly more complicated, as

$$\begin{aligned} \mathrm{N}_{\mathbb{Q}(\zeta_3)/\mathbb{Q}}(a + b\zeta_3) &= (a + b\zeta_3)(a + b\zeta_3^2) \\ &= a^2 + b^2 + ab(\zeta_3 + \zeta_3^2) \\ &= a^2 - ab + b^2. \end{aligned}$$

This only affects the proof in the computation of the bound on the remainder; one finds that

$$N(r) \leq \frac{3}{4}\mathrm{N}(\beta),$$

which is good enough to show that $\mathbb{Z}[\zeta_3]$ is Euclidean.

In this case $p = 3$ is the exceptional prime; we can factor 3 as

$$3 = -\zeta_3^2(1 - \zeta_3)^2;$$

here $-\zeta_3^2$ is a unit and $1 - \zeta_3$ is prime.

So, let $p \neq 3$ be a prime of $\mathbb{Z}$ and suppose that p factors in $\mathbb{Z}[\zeta_3]$. As usual, this implies that there are $x, y \in \mathbb{Z}$, relatively prime to p, such that

$$\begin{aligned} x^2 - xy + y^2 &\equiv 0 \pmod{p} \\ \left(\frac{x}{y}\right)^2 - \frac{x}{y} + 1 &\equiv 0 \pmod{p}. \end{aligned}$$

Set $\alpha \equiv -x/y \in \mathbb{F}_p$. Then

$$\alpha^2 + \alpha + 1 \equiv 0 \pmod{p};$$

multiplying by $\alpha - 1$, we find that

$$\alpha^3 \equiv 1 \pmod{p}.$$

Clearly $\alpha \neq 1$, since $p \neq 3$, so we conclude that p factors only if there is a non-trivial third root of unity modulo p. In fact, the above argument is reversible, so $p \neq 3$ factors if and only if $\mathbb{F}_p^*$ has a non-trivial third root of unity. Since $\mathbb{F}_p^*$ is cyclic of order $p-1$, this will happen if and only if 3 divides $p-1$; that is, if and only

$$p \equiv 1 \pmod 3.$$

The naturally related quadratic form in this case is just $x^2 - xy + y^2$. The usual arguments show that p factors if and only if p can be written as $x^2 - xy + y^2$; thus p can be written in this form if and only if $p = 3$ or $p \equiv 1 \pmod 3$.

Solution 2.6. Let R be a finite integral domain and let a be any non-zero element of R. We need to show that a has an inverse in R. Consider the map from $R \to R$ given by multiplication by a. The kernel is

$$\{r \in R | ar = 0\} = \{0\};$$

thus this map is injective. Since R is finite, injective maps are also surjective; in particular, 1 is in the image and we conclude that there is $b \in R$ such that $ab = 1$. Thus a has an inverse in R.

Solution 2.7. We first show that (1) implies (2). So suppose that we have an increasing chain

$$I_1 \subseteq I_2 \subseteq I_3 \subseteq \cdots$$

of ideals of R. Let I be the union of the I_n. One shows from the definitions that I is an ideal of R. For example, if $i, j \in I$, then $i \in I_m$, $j \in I_n$ for some m, n, so $i + j \in I_{\max\{m,n\}} \subseteq I$. Now, by our assumption (1) I has a finite generating set $a_1, \ldots, a_k$. Since I is the union of the I_n, each a_j must lie in some I_{n_j}. Taking n to be the maximum of the n_j, we find that $a_1, \ldots, a_k \in I_n$; thus $I_n = I$, as it contains all of the generators of I. We conclude that the chain of ideals becomes constant at the n^{th} ideal.

Next we show that (2) implies (3). So let $\mathcal{S}$ be a non-empty set of ideals of R and suppose that $\mathcal{S}$ has no maximal elements. Let I_1 be any element of $\mathcal{S}$. Since $\mathcal{S}$ has no maximal elements, we can choose $I_2 \in \mathcal{S}$ such that

$$I_1 \subsetneq I_2.$$

I_2 is not maximal either, so we can choose $I_3 \in \mathcal{S}$ such that

$$I_1 \subsetneq I_2 \subsetneq I_3.$$

Continuing in this way we can construct an infinite sequence of ideals of R which is not constant, which contradicts (2).

Finally we show that (3) implies (1). Let I be an ideal of R and take $\mathcal{S}$ to be the set of ideals J of R such that $J \subseteq I$ and J is finitely generated. $\mathcal{S}$ is certainly non-empty (for example, it contains the zero ideal), so by (3) $\mathcal{S}$ has a maximal element, say J_0. Suppose that $J_0 \neq I$. Then we can choose $i \in I - J_0$; set $J_1 = J_0 + iR$. J_1 is generated by the generators of J_0 together with i, so it is finitely generated; since it is also in I, we conclude that $J_1 \in \mathcal{S}$. But J_1 is strictly larger than J_0, which contradicts the maximality of J_0. It follows that $J_0 = I$, so $I \in \mathcal{S}$ and thus is finitely generated by the definition of $\mathcal{S}$.

Solution 2.8. Let $\varphi : R \to R/I$ be the quotient map and let J be any ideal of R/I. We will show that J is finitely generated, which will prove that R is noetherian by Exercise 2.7. Let J' be the ideal $\varphi^{-1}(J)$; one checks that it is an ideal directly from the definition. Since R is noetherian, J' has a finite generating set $a_1, \ldots, a_m$. We claim that $\varphi(a_1), \ldots, \varphi(a_m)$ generate J.

Note first that since $a_i \in J'$, $\varphi(a_i) \in J$. Thus the ideal generated by the $\varphi(a_i)$ lies in J. It remains to show that it is all of J. To see this, let j be any element of J, and let $j' \in R$ be such that $\varphi(j') = j$. Then $j' \in J'$, so we can write

$$j' = r_1 a_1 + \cdots + r_m a_m$$

for some $r_i \in R$. Now,

$$j = \varphi(j') = \varphi(r_1)\varphi(a_1) + \cdots + \varphi(r_m)\varphi(a_m),$$

so j is a linear combination of the $\varphi(a_i)$, as claimed.

SOLUTION 2.9. Suppose that $\mathfrak{p}$ does not contain any of the I_i. Then for each i we can find $\pi_i \in I_i$ such that $\pi_i \notin \mathfrak{p}$. Thus the product $\pi_1 \cdots \pi_n$ is not in $\mathfrak{p}$ either, since $\mathfrak{p}$ is prime. This contradicts the fact that $\mathfrak{p}$ contains $I_1 \cdots I_n$, so $\mathfrak{p}$ must have contained one of the I_i.

SOLUTION 2.10. We know that PID implies UFD, so we must show the converse. So let R be a Dedekind domain and suppose that R is a UFD. Let $\mathfrak{a}$ be any non-zero ideal of R; we must show that it is principal. Let α be any non-zero element of $\mathfrak{a}$. Let

$$\alpha = \pi_1 \cdots \pi_n$$

be a factorization of α into irreducibles; since we are assuming that R is a UFD, each of the π_i is actually a prime element. This implies that each ideal $\big(\pi_i\big)$ is prime, so the ideal equation

$$\big(\alpha\big) = \big(\pi_1\big) \cdots \big(\pi_n\big)$$

gives a factorization of $\big(\alpha\big)$ into prime ideals. Now, $\big(\alpha\big) \subseteq \mathfrak{a}$, so $\mathfrak{a}$ divides $\big(\alpha\big)$. In particular, this implies (using unique factorization of ideals) that all of the prime ideal factors of $\mathfrak{a}$ are among the $\big(\pi_i\big)$. In particular, all of the prime ideal factors of $\mathfrak{a}$ are principal, so $\mathfrak{a}$ is a product of principal ideals and thus principal. This completes the proof.

SOLUTION 2.11. Let L be any one of the fields $\mathbb{Q}(\sqrt{2})$, $\mathbb{Q}(\sqrt{3})$, $\mathbb{Q}(\sqrt{6})$. We show first that $\alpha \in K$ is an algebraic integer if and only if $\mathrm{Tr}_{K/L}(\alpha)$ and $\mathrm{N}_{K/L}(\alpha)$ are algebraic integers. One implication is clear: if α is an algebraic integer, then all of the conjugates of α are also algebraic integers, so any trace or norm of α is an algebraic integer. For the other implication, note that α satisfies its K/L characteristic polynomial

$$x^2 - \mathrm{Tr}_{K/L}(\alpha)x + \mathrm{N}_{K/L}(\alpha).$$

If $\mathrm{Tr}_{K/L}(\alpha)$ and $\mathrm{N}_{K/L}(\alpha)$ are both algebraic integers, then they both lie in $\mathcal{O}_L$ and thus in $\mathcal{O}_K$; since $\mathcal{O}_K$ is integrally closed in K, this implies that $\alpha \in \mathcal{O}_K$. This completes the proof of the claim.

Now, let

$$\alpha = a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6},$$

$a, b, c, d \in \mathbb{Q}$, be any element of K. By the above argument, if $\alpha \in \mathcal{O}_K$, then

$$\begin{aligned}
\mathrm{Tr}_{K/\mathbb{Q}(\sqrt{2})}(\alpha) &= (a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6}) + (a + b\sqrt{2} - c\sqrt{3} - d\sqrt{6}) \\
&= 2a + 2b\sqrt{2} \in \mathcal{O}_{\mathbb{Q}(\sqrt{2})} \\
\mathrm{Tr}_{K/\mathbb{Q}(\sqrt{3})}(\alpha) &= 2a + 2c\sqrt{3} \in \mathcal{O}_{\mathbb{Q}(\sqrt{3})} \\
\mathrm{Tr}_{K/\mathbb{Q}(\sqrt{6})}(\alpha) &= 2a + 2d\sqrt{6} \in \mathcal{O}_{\mathbb{Q}(\sqrt{6})}.
\end{aligned}$$

Using our knowledge of these rings of integers, we see that the trace conditions amount to

$$2a, 2b, 2c, 2d \in \mathbb{Z}.$$

This leaves us with the norm conditions. Here we have

$$\begin{aligned}
\mathrm{N}_{K/\mathbb{Q}(\sqrt{2})}(\alpha) &= (a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6})(a + b\sqrt{2} - c\sqrt{3} - d\sqrt{6}) \\
&= (a + b\sqrt{2})^2 - (c\sqrt{3} + d\sqrt{6})^2 \\
&= (a^2 + 2b^2 - 3c^2 - 6d^2) + (2ab - 6cd)\sqrt{2} \in \mathcal{O}_{\mathbb{Q}(\sqrt{2})} \\
\mathrm{N}_{K/\mathbb{Q}(\sqrt{3})}(\alpha) &= (a^2 - 2b^2 + 3c^2 - 6d^2) + (2ac - 4bd)\sqrt{3} \in \mathcal{O}_{\mathbb{Q}(\sqrt{3})} \\
\mathrm{N}_{K/\mathbb{Q}(\sqrt{6})}(\alpha) &= (a^2 - 2b^2 - 3c^2 + 6d^2) + (2ad - 2bc)\sqrt{6} \in \mathcal{O}_{\mathbb{Q}(\sqrt{6})}.
\end{aligned}$$

Combining the rational parts of the first and third norm conditions, we find that

$$2a^2 - 6c^2 \in \mathbb{Z}.$$

In particular, this implies (using the fact that 4 does not divide 2 or 6) that either both $a, c \in \mathbb{Z}$ or both $a, c \notin \mathbb{Z}$. Note also that by the second norm condition we have $2ac - 4bd \in \mathbb{Z}$; since $4bd$ is necessarily in $\mathbb{Z}$, this implies that $2ac \in \mathbb{Z}$. Combining all of this we see that we must have $a, c \in \mathbb{Z}$, since otherwise $2ac \notin \mathbb{Z}$.

Since $a, c \in \mathbb{Z}$, the first norm condition now tells us that

$$2b^2 - 6d^2 \in \mathbb{Z};$$

as before this implies that either $b, d \in \mathbb{Z}$ or $b, d \notin \mathbb{Z}$. Combining all of this, we have found that either

$$a, b, c, d \in \mathbb{Z}$$

or

$$a, c \in \mathbb{Z}; \qquad 2b, 2d \in \mathbb{Z} - 2\mathbb{Z}.$$

One checks easily that all such α are indeed algebraic integers (just by checking the norm conditions), and it is now easy to see that

$$1, \sqrt{2}, \sqrt{3}, \frac{\sqrt{2} + \sqrt{6}}{2}$$

is an integral basis.

Solution 2.12. Set $\zeta = \zeta_p$. We first consider the case $i = 1$. By the usual formula for a geometric series,

$$\frac{1 - \zeta^j}{1 - \zeta} = 1 + \zeta + \zeta^2 + \cdots + \zeta^{j-1} \in \mathbb{Z}[\zeta].$$

On the other hand, there exists some k such that

$$(\zeta^j)^k = \zeta;$$

specifically, one can take for k an inverse of j modulo p. Thus

$$\frac{1-\zeta}{1-\zeta^j} = \frac{1-(\zeta^j)^k}{1-\zeta^j} = 1 + (\zeta^j) + (\zeta^j)^2 + \cdots + (\zeta^j)^{k-1} \in \mathbb{Z}[\zeta].$$

Since both $(1-\zeta)/(1-\zeta^j)$ and its inverse lie in $\mathbb{Z}[\zeta]$, it is a unit; thus $1-\zeta$ and $1-\zeta^j$ are associates.

For the general case, one can modify the argument above; alternatively, one can note that, if k is an inverse for i modulo p, then

$$\sigma_k(1-\zeta^i) = 1-\zeta$$

and

$$\sigma_k(1-\zeta^j) = 1-\zeta^{jk}$$

are associates by the above special case. Since σ_k is an automorphism, this implies that $1-\zeta^i$ and $1-\zeta^j$ are associates as well.

Solution 2.13. Recall that

$$\mathbb{Z}[\zeta_p] \cong \mathbb{Z}[x]/(\Phi_p(x)).$$

Thus

$$\mathbb{Z}[\zeta_p]/\big(1-\zeta_p\big) \cong \mathbb{Z}[x]/(\Phi_p(x), 1-x) \cong (\mathbb{Z}[x]/(1-x))/I$$

where I is the ideal of $\mathbb{Z}[x]/(1-x)$ generated by $\Phi_p(x)$. The map sending x to 1 yields an isomorphism $\mathbb{Z}[x]/(1-x) \cong \mathbb{Z}$, and under this isomorphism the image of I is the ideal generated by $\Phi_p(1) = p$. Thus

$$\mathbb{Z}[\zeta_p]/\big(1-\zeta_p\big) \cong \mathbb{Z}/p\mathbb{Z};$$

this is an integral domain, so the ideal $\big(1-\zeta_p\big)$ is prime by definition.

To factor $\big(p\big)$, we begin with the expression

$$p = \Phi_p(1) = (1-\zeta_p)\cdots(1-\zeta_p^{p-1}).$$

By Exercise 2.12, we know that all of the factors on the right-hand side are associates. Thus, as ideals,

$$\big(p\big) = \big(1-\zeta_p\big)\cdots\big(1-\zeta_p^{p-1}\big) = \big(1-\zeta_p\big)^{p-1}.$$

Since $\big(1-\zeta_p\big)$ is prime, this must be the prime factorization of p.

Solution 2.14. Set $\zeta = \zeta_{p^n}$. The proofs are quite similar to the $n = 1$ case. Specifically, the argument that $1-\zeta$ and $1-\zeta^j$ are associate is exactly the same, using the fact that p does not divide j to find the inverse k. (This is why, for example, $1-\zeta_p$ and $1-\zeta_{p^2}$ are not associate.) The general case can again be deduced from this case using appropriate automorphisms.

The proof that

$$\mathbb{Z}[\zeta]/(1-\zeta) \cong \mathbb{Z}/p\mathbb{Z}$$

is exactly the same as in the $n = 1$ case; it does require the additional piece of information that $\Phi_{p^n}(1) = p$, which is proven in the solution to Exercise 2.15. The factorization of p proceeds as before.

Solution 2.15. We first prove that

$$\Phi_m(1) = \begin{cases} p & m = p^n \text{ is a prime power;} \\ \pm 1 & \text{otherwise.} \end{cases}$$

We prove the prime power case by induction on n. The case $n = 1$ is clear. Suppose, then, that we know that $\Phi_{p^k}(1) = p$ for $k < n$. Consider the expression

$$x^{p^n} - 1 = \prod_{k=0}^{n} \Phi_{p^k}(x).$$

Dividing both sides by $x - 1 = \Phi_1(x)$, we have

$$x^{p^n-1} + x^{p^n-2} + \cdots + 1 = \prod_{k=1}^{n} \Phi_{p^k}(x).$$

Plugging in 1, we find that

$$p^n = \prod_{k=1}^{n} \Phi_{p^k}(1);$$

the induction hypothesis implies that the right-hand side is $p^{n-1}\Phi_{p^n}(1)$, so $\Phi_{p^n}(1) = p$, as claimed.

For the case of m with more than 1 prime factor, we again consider the product

$$x^{m-1} + x^{m-2} + \cdots + 1 = \prod_{d|m, d\neq 1} \Phi_d(x).$$

Plugging in 1, we have

$$m = \prod_{d|m, d\neq 1} \Phi_d(1).$$

Write $m = p_1^{n_1} \cdots p_j^{n_j}$. Note that the terms for which d is a power of p_i contribute

$$\prod_{k=1}^{n_i} \Phi_{p_i^{n_i}}(1) = p_i^{n_i}$$

by the prime power case. Canceling all of these, we find that

$$1 = \prod_{d|m, d \text{ has multiple prime factors}} \Phi_d(1).$$

Since each $\Phi_d(1)$ is an integer, this implies that they are all ± 1; in particular, $\Phi_m(1) = \pm 1$, as claimed.

Given this, the exercise is easy. Specifically, if m is a prime power then the fact that $1 - \zeta_m$ generates a prime ideal (see Exercise 2.14) shows that it can not possibly be a unit. If m is composite, then we use the expression

$$\Phi_m(x) = \prod_{\substack{1 \leq k < m \\ (k,m)=1}} (x - \zeta_m^k).$$

Plugging in 1, we find that

$$\pm 1 = \prod_{\substack{1 \leq k < m \\ (k,m)=1}} (1 - \zeta_m^k).$$

This expresses $1 - \zeta_m$ as part of a product of elements of $\mathbb{Z}[\zeta_m]$ which multiply to 1, so it must be a unit.

SOLUTION 2.16. Define $\mathcal{S}$ to be the set of all $\alpha \in \mathcal{O}_K$ such that $\sigma_i(\alpha)$ has absolute value 1 for each i. Observe first that $\mathcal{S}$ is actually a group under multiplication; this is because, if $\alpha, \beta \in \mathcal{S}$, then

$$|\sigma_i(\alpha\beta)| = |\sigma_i(\alpha)| \cdot |\sigma_i(\beta)| = 1,$$

so $\alpha\beta \in \mathcal{S}$. That $\mathcal{S}$ is closed under inverses is proven in the same way. We will show that $\mathcal{S}$ is finite; this will imply that everything in $\mathcal{S}$ has finite order under multiplication, and thus is a root of unity.

Let $f(x) \in \mathbb{Z}[x]$ be the characteristic polynomial of any $\beta \in \mathcal{S}$. ($f(x)$ has integer coefficients since β is an algebraic integer.) We have

$$f(x) = \big(x - \sigma_1(\beta)\big) \cdots \big(x - \sigma_n(\beta)\big).$$

Consider the coefficient a_{n-1} of x^{n-1} in $f(x)$. It is an integer, since $f(x) \in \mathbb{Z}[x]$. It also has the expression

$$a_{n-1} = -\big(\sigma_1(\beta) + \cdots + \sigma_n(\beta)\big).$$

Since each $\sigma_i(\beta)$ has absolute value 1, this implies that

$$|a_{n-1}| \leq n.$$

In the same way, one shows that for any k,

$$|a_k| \leq \binom{n}{k}.$$

Thus there are only finitely many possibilities for each a_k, since each is an integer in a bounded range.

In particular, this means that there are only finitely many possible choices for $f(x)$, since there are only finitely many choices for each coefficient of $f(x)$. (Note also that the degree of $f(x)$ is fixed at n.) Each such $f(x)$ has at most n roots, so all together there can only be a finite number of roots of polynomials which could possibly be characteristic polynomials of elements of $\mathcal{S}$. In particular, $\mathcal{S}$ itself must be finite, as claimed.

SOLUTION 2.17. Set $\zeta = \zeta_p$ and let $\sigma_1, \ldots, \sigma_{p-1}$ be the complex embeddings of $\mathbb{Q}(\zeta)$, ordered in the usual way. It is easy to check that for any $\alpha \in \mathbb{Q}(\zeta)$,

$$\sigma_i(\bar{\alpha}) = \overline{\sigma_i(\alpha)}.$$

(One way to check this is to observe that $\sigma_{-1}(\alpha) = \bar{\alpha}$ and to use the commutativity of the Galois group.) In particular, every conjugate of $\alpha/\bar{\alpha}$ will have absolute value 1, since a complex number and its complex conjugate have the same absolute value.

In the case of $u/\bar{u}$, where u is a unit, $u/\bar{u}$ is also an algebraic integer, since $\bar{u}$ is a unit. We can now apply Exercise 2.16 to conclude that $u/\bar{u}$ is a root of unity. By Corollary I.3.7, this implies that

$$\frac{u}{\bar{u}} = \pm\zeta^k$$

for some k. We must show that the sign is actually $+$.

So suppose that $u/\bar{u} = -\zeta^k$ for some k. Write

$$u = a_0 + a_1\zeta + \cdots + a_{p-2}\zeta^{p-2}.$$

Then

$$u \equiv a_0 + a_1 + \cdots + a_{p-2} \pmod{1-\zeta}.$$

Similarly, since $1-\zeta$ and $1-\bar{\zeta} = 1-\zeta^{p-1}$ are associates,

$$\bar{u} \equiv a_0 + a_1 + \cdots + a_{p-2} \pmod{1-\zeta}.$$

Thus,

$$\bar{u} \equiv u \equiv -\zeta^k \bar{u} \equiv -\bar{u} \pmod{1-\zeta}.$$

Therefore $2\bar{u} \in \big(1-\zeta\big)$; since $\big(1-\zeta\big)$ is prime and 2 is not in this ideal, this implies that $\bar{u} \in \big(1-\zeta\big)$. But this is absurd, since $\bar{u}$ is a unit and this is a non-unit ideal. This yields the desired contradiction.

SOLUTION 2.18. By the definition of the Galois correspondence, $\mathbb{Q}(\zeta_m)^+$ is given by

$$\mathbb{Q}(\zeta_m)^+ = \{\alpha \in \mathbb{Q}(\zeta_m) \mid \sigma_{-1}(\alpha) = \alpha\}.$$

Here σ_{-1} is the automorphism of $\mathbb{Q}(\zeta_m)$ sending ζ_m to ζ_m^{-1}. Since

$$\sigma_{-1}(\zeta_m + \zeta_m^{-1}) = \zeta_m^{-1} + \zeta_m,$$

it is clear that $\mathbb{Q}(\zeta_m + \zeta_m^{-1}) \subseteq \mathbb{Q}(\zeta_m)^+$. To show that the two fields are equal it will suffice to show that

$$[\mathbb{Q}(\zeta_m) : \mathbb{Q}(\zeta_m + \zeta_m^{-1})] \leq 2;$$

since we already know that

$$[\mathbb{Q}(\zeta_m) : \mathbb{Q}(\zeta_m + \zeta_m^{-1})] \geq [\mathbb{Q}(\zeta_m) : \mathbb{Q}(\zeta_m)^+] = 2,$$

this will complete the proof. But to show the first inequality is easy; ζ_m satisfies the polynomial

$$x^2 - (\zeta_m + \zeta_m^{-1})x + 1 \in \mathbb{Q}(\zeta_m + \zeta_m^{-1})[x],$$

so ζ_m has degree at most 2 over $\mathbb{Q}(\zeta_m + \zeta_m^{-1})$.

Since every complex embedding of $\mathbb{Q}(\zeta_m)^+$ is the restriction of some complex embedding of $\mathbb{Q}(\zeta_m)$, to show that every complex embedding of $\mathbb{Q}(\zeta_m)^+$ has image in $\mathbb{R}$ we just need to show that

$$\sigma_i\left(\mathbb{Q}(\zeta_m)^+\right) \subseteq \mathbb{R}$$

for every complex embedding σ_i of $\mathbb{Q}(\zeta_m)$. Since $\mathbb{Q}(\zeta_m)^+$ is generated over $\mathbb{Q}$ by $\zeta_m + \zeta_m^{-1}$, it will suffice to show that

$$\sigma_i(\zeta_m + \zeta_m^{-1}) \in \mathbb{R}$$

for every i. For this, we simply compute

$$\sigma_i(\zeta_m + \zeta_m^{-1}) = \zeta_m^i + \zeta_m^{-i} = 2\cos\left(\frac{2\pi}{m}\right) \in \mathbb{R}.$$

SOLUTION 2.19. Since $\zeta_m + \zeta_m^{-1}$ is an algebraic integer, it is clear that $\mathbb{Z}[\zeta_m + \zeta_m^{-1}] \subseteq \mathcal{O}_{\mathbb{Q}(\zeta_m)^+}$; we need to show the other inclusion. Let α be an algebraic integer of $\mathbb{Q}(\zeta_m)^+$ and write

$$\alpha = a_0 + a_1(\zeta_m + \zeta_m^{-1}) + \cdots + a_k(\zeta_m + \zeta_m^{-1})^k$$

where $k \leq \varphi(m)/2 = [\mathbb{Q}(\zeta_m)^+ : \mathbb{Q}]$, $a_i \in \mathbb{Q}$ and $a_k \neq 0$. We are to show that each a_i is an integer; so suppose that this is not the case. If a_k is an integer, then we can replace α by $\alpha - a_k(\zeta_m + \zeta_m)^k$ and still have an algebraic integer; continuing in this way and reducing k if necessary, we can assume that a_k is not an integer. Now consider $\zeta_m^k\alpha$. Writing this in terms of $1, \zeta_m, \ldots, \zeta_m^{2k}$, we see that the coefficients of 1 and ζ_m^{2k} will both be a_k. Now, $\zeta_m^k\alpha$ is an algebraic integer of $\mathbb{Q}(\zeta_m)$, so it lies in $\mathbb{Z}[\zeta_m]$. Since $1, \zeta_m, \ldots, \zeta_m^{2k}$ is a subset of an integral basis for $\mathbb{Z}[\zeta_m]$, this implies that the coefficients of $1, \zeta_m, \dots, \zeta_m^{2k}$ in $\zeta_m^k \alpha$ must all be integers. In particular, a_k must be an integer, which is a contradiction. This completes the proof.

SOLUTION 2.20. Suppose first that the α_i are linearly independent over $\mathbb{Q}$. This yields a linear dependence among the columns of the matrix $\big(\sigma_i(\alpha_j)\big)$, and thus shows that $\Delta(\alpha_1, \dots, \alpha_n) = 0$.

Conversely, suppose that $\Delta(\alpha_1, \dots, \alpha_n) = 0$. We must show that $\alpha_1, \dots, \alpha_n$ is not a basis for K, so assume the opposite. Now, note that $\Delta = 0$ implies that the rows of the matrix $\big(\mathrm{Tr}(\alpha_i\alpha_j)\big)$ are linearly dependent; since the entries of this matrix are all in $\mathbb{Q}$, there must be such a linear dependence with coefficients in $\mathbb{Q}$. Fix one such; letting R_i be the i^{th} row, this means we choose rational numbers $a_1, \dots, a_n$, not all zero, such that

$$a_1R_1 + \cdots + a_nR_n = 0.$$

Set $\alpha = a_1\alpha_1 + \cdots + a_n\alpha_n$; $\alpha \neq 0$ since we assumed that the α_i are a basis. We compute that

$$\mathrm{Tr}(\alpha\alpha_j) = \mathrm{Tr}(a_1\alpha_1\alpha_j) + \cdots + \mathrm{Tr}(a_n\alpha_n\alpha_j) = 0$$

since this is just the j^{th} entry in the vector $a_1R_1 + \cdots + a_nR_n$. Observe also that $\alpha\alpha_1, \dots, \alpha\alpha_n$ is a basis for $K/\mathbb{Q}$ since the α_i are (think of α as a linear transformation on K). This implies that $\mathrm{Tr}(\beta) = 0$ for every $\beta \in K$, since every such β can be written in terms of the $\alpha\alpha_i$ with rational coefficients. But this is clearly absurd; for example, $\mathrm{Tr}(1) = n \neq 0$. This yields the desired contradiction.

SOLUTION 2.21. By standard linear algebra (over free $\mathbb{Z}$-modules), the fact that $\alpha_1, \dots, \alpha_n$ and $\alpha'_1, \dots, \alpha'_n$ are both bases for the same $\mathbb{Z}$-module implies that there is some $n \times n$ matrix A with integer coefficients and determinant ± 1 such that

$$\begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{pmatrix} = A \begin{pmatrix} \alpha'_1 \\ \vdots \\ \alpha'_n \end{pmatrix}$$

Applying each σ_i to this matrix equation (this doesn't do anything to A, since A has integer entries) and combining them all into one big matrix equation, we find that

$$\big(\sigma_i(\alpha_j)\big) = A \cdot \big(\sigma_i(\alpha'_j)\big).$$

The discriminants are just the squares of the determinants of the matrices, so the fact that $\det A = \pm 1$ shows that it will have no effect on the discriminants.

SOLUTION 2.22. First assume $d \equiv 2, 3 \pmod 4$, so that $\mathcal{O}_K$ has integral basis $1, \sqrt{d}$. Then

$$\Delta_K = \Delta(1, \sqrt{d}) = \det \begin{pmatrix} 1 & \sqrt{d} \\ 1 & -\sqrt{d} \end{pmatrix}^2 = (-\sqrt{d} - \sqrt{d})^2 = 4d.$$

Now, suppose that $d \equiv 1 \pmod 4$, so that $\mathcal{O}_K$ has integral basis $1, \frac{1+\sqrt{d}}{2}$. We compute

$$\Delta_K = \det \begin{pmatrix} 1 & \frac{1+\sqrt{d}}{2} \\ 1 & \frac{1-\sqrt{d}}{2} \end{pmatrix}^2 = \left(\frac{1-\sqrt{d}}{2} - \frac{1+\sqrt{d}}{2}\right)^2 = (-\sqrt{d})^2 = d.$$

3. Chapter 3

SOLUTION 3.1. Let $i \in I$ and $j \in J$ be such that $i + j = 1$. Then

$$\begin{aligned} 1 &= (i+j)^{m+n} \\ &= i^{m+n} + \binom{m+n}{m+n-1} i^{m+n-1} j + \cdots + \binom{m+n}{1} i j^{m+n-1} + j^{m+n} \end{aligned}$$

Every term in this sum is a multiple of either i^m or j^n and therefore lies in I^m or J^n. Thus $1 \in I^m + J^n$, so I^m and J^n are relatively prime.

SOLUTION 3.2. Suppose first that I and J have a common prime factor, say $\mathfrak{p}$. Then we can write $I = \mathfrak{p}I'$, $J = \mathfrak{p}J'$ for ideals I' and J'. Now,

$$I + J = \mathfrak{p}(I' + J') \subseteq \mathfrak{p}.$$

Therefore $I + J \neq R$, so I and J are not relatively prime.

For the other direction, suppose that $I + J \neq R$. Since R is noetherian, this implies that $I + J$ is contained in some maximal ideal $\mathfrak{p}$ of R. Since $I \subseteq I + J$, this in turn implies that $I \subseteq \mathfrak{p}$. Similarly, $J \subseteq \mathfrak{p}$. $\mathfrak{p}$ is therefore a common prime divisor of I and J, which completes the proof.

SOLUTION 3.3. Since $\bar{f}(x)$ and $\bar{g}(x)$ are relatively prime in $\mathbb{F}_p[x]$ and $\mathbb{F}_p[x]$ is a PID, we can find $\bar{a}(x), \bar{b}(x) \in \mathbb{F}_p[x]$ such that

$$\bar{a}(x)\bar{f}(x) + \bar{b}(x)\bar{g}(x) = 1.$$

Lifting this back to $\mathbb{Z}[x]$, this says that

$$a(x)f(x) + b(x)g(x) = 1 + pc(x)$$

for some $c(x) \in \mathbb{Z}[x]$, where $a(x), b(x) \in \mathbb{Z}[x]$ are any lifts of $\bar{a}(x), \bar{b}(x)$. Plugging in α, we find that

$$a(\alpha)f(\alpha) + b(\alpha)g(\alpha) = 1 + pc(\alpha).$$

Now, consider the ideal

$$\big(p, f(\alpha)\big) + \big(p, g(\alpha)\big).$$

$a(\alpha)f(\alpha)$ is contained in the first, $b(\alpha)g(\alpha)$ is contained in the second, and $pc(\alpha)$ is contained in either of them; this and the expression above implies that 1 is contained in this ideal sum. Thus $\big(p, f(\alpha)\big)$ and $\big(p, g(\alpha)\big)$ are relatively prime.

SOLUTION 3.4. It follows from the definition of an ideal that $IJ \subseteq I$ and $IJ \subseteq J$; thus $IJ \subseteq I \cap J$. We must prove the other inclusion. Let $i \in I$ and $j \in J$ be such that $i + j = 1$ and let x be any element of $I \cap J$. Since $x \in I$, $xj \in IJ$; since $x \in J$, $xi \in IJ$. Therefore,

$$x = x(i + j) = xi + xj \in IJ$$

which completes the proof.

Before we prove the general case, we show that if I_1, I_2, J are ideals such that $I_1 + J = R$ and $I_2 + J = R$, then $I_1 I_2 + J = R$. To prove this, let $i_1 \in I_1$, $i_2 \in I_2$, $j_1, j_2 \in J$ be such that $i_1 + j_1 = 1$ and $i_2 + j_2 = 1$. Then

$$1 = (i_1 + j_1)(i_2 + j_2) = i_1 i_2 + j_1 i_2 + i_1 j_2 + j_1 j_2.$$

The last three summand all lie in J and the first lies in $I_1 I_2$, so this shows that the ideals are indeed relatively prime.

For the general case we are to show that for any n pairwise relatively prime ideals $I_1, I_2, \dots, I_n$, we have

$$I_1 \cap I_2 \cap \cdots \cap I_n = I_1 I_2 \cdots I_n.$$

We prove this by induction on n, the case $n = 2$ having been done above. So suppose that we know the result for any collection of $n-1$ pairwise relatively prime ideals. Our result above shows that $I_1 I_2$ is relatively prime to $I_3, \dots, I_n$, so by the induction hypothesis we know that

$$I_1 I_2 \cap I_3 \cdots \cap I_n = (I_1 I_2) I_3 \cdots I_n.$$

By the $n = 2$ case we also know that $I_1 I_2 = I_1 \cap I_2$, which gives the desired equality and completes the induction.

Solution 3.5. Consider the map

$$R \to R/I \times R/J$$

sending $x \in R$ to $(x, x) \in R/I \times R/J$. The kernel of this map consists precisely of those x mapping to 0 in each factor; this is just $I \cap J$. By Exercise 3.4 $I \cap J = IJ$, so we obtain an injective map

$$R/IJ \to R/I \times R/J.$$

It remains to show that this map is surjective. For this, first pick $i \in I$ and $j \in J$ such that $i + j = 1$. Now let $(\bar{x}, \bar{y})$ be any element of $R/I \times R/J$ and choose any lifts x, y of $\bar{x}, \bar{y}$ to R; that is $x \equiv \bar{x} \pmod{I}$ and $y \equiv \bar{y} \pmod{J}$. Let $z = jx + iy$. We claim that z maps to $(\bar{x}, \bar{y})$. To see this, note that modulo I,

$$z = jx + iy \equiv jx = (1 - i)x = x - ix \equiv x \pmod{I}.$$

Similarly,

$$z \equiv y \pmod{J}.$$

These congruences mean precisely that z maps to $(\bar{x}, \bar{y})$, as claimed.

The case of n ideals follows from this case by an easy induction.

Solution 3.6. This is precisely the surjectivity statement of Exercise 3.5.

Solution 3.7. We prove that each statement is equivalent to the next. The equivalence of (1) and (2) is Lemma II.3.8. The equivalence of (2) and (3) is just the definition of the ideal $\mathfrak{p}\mathcal{O}_L$ generated by $\mathfrak{p}$. That (4) implies (3) is clear; for the other direction, suppose that $\mathfrak{P} \supseteq \mathfrak{p}$. $\mathfrak{P} \cap \mathcal{O}_K$ is an ideal of $\mathcal{O}_K$, and we are assuming that it contains $\mathfrak{p}$. Since $\mathfrak{p}$ is maximal this implies that either $\mathfrak{P} \cap \mathcal{O}_K = \mathcal{O}_K$ or $\mathfrak{P} \cap \mathcal{O}_K = \mathfrak{p}$. However, we can not have $\mathfrak{P} \cap \mathcal{O}_K = \mathcal{O}_K$ since then $\mathfrak{P}$ would contain 1 and would be the unit ideal. This shows that (3) implies (4). Lastly, the equivalence of (4) and (5) follows from Lemma 2.15.

Solution 3.8. Let $\mathfrak{P}$ be a prime ideal of $\mathcal{O}_L$. Then $\mathfrak{P} \cap \mathcal{O}_K$ is a non-zero prime ideal of $\mathcal{O}_K$ (that it is prime follows from the definitions; that it is non-zero follows, for example, from the fact that $\mathfrak{P}$ contains non-zero rational integers), and by Lemma 2.12 it must be the unique prime of $\mathcal{O}_K$ which $\mathfrak{P}$ lies over.

For the converse, consider the ideal $\mathfrak{p}\mathcal{O}_L$. If we knew that $\mathfrak{p}\mathcal{O}_L \neq \mathcal{O}_L$, then it must be contained in some maximal ideal $\mathfrak{P}$ of $\mathcal{O}_L$. Lemma 2.12 then implies that $\mathfrak{P}$ lies over $\mathfrak{p}$.

It remains to show that $\mathfrak{p}\mathcal{O}_L \neq \mathcal{O}_L$. We use Lemma II.3.5, which tells us that we can choose $\gamma \in K - \mathcal{O}_K$ such that $\gamma\mathfrak{p} \subseteq \mathcal{O}_K$. It follows that $\gamma\mathfrak{p}\mathcal{O}_L \subseteq \mathcal{O}_L$.

However, if $\mathfrak{p}\mathcal{O}_L = \mathcal{O}_L$, then $1 \in \mathfrak{p}\mathcal{O}_L$, so $\gamma \in \gamma\mathfrak{p}\mathcal{O}_L$. Since $\gamma \notin \mathcal{O}_L$ (since it is not in $\mathcal{O}_K$ and $\mathcal{O}_L \cap K = \mathcal{O}_K$), this is a contradiction. Thus $\mathfrak{p}\mathcal{O}_L \neq \mathcal{O}_L$, as claimed.

SOLUTION 3.9. The result is clear for $a \equiv 0 \pmod{p}$, so we assume $a \in (\mathbb{Z}/p\mathbb{Z})^*$. Note that the squaring map

$$(\mathbb{Z}/p\mathbb{Z})^* \to (\mathbb{Z}/p\mathbb{Z})^*$$

has kernel $\{\pm 1\}$, as these are the two roots of $x^2 - 1$. It follows that the image has order $\frac{p-1}{2}$; that is, there are exactly $\frac{p-1}{2}$ squares in $(\mathbb{Z}/p\mathbb{Z})^*$.

Now, recall that every $a \in (\mathbb{Z}/p\mathbb{Z})^*$ is a root of

$$x^{p-1} - 1 = (x^{(p-1)/2} - 1)(x^{(p-1)/2} + 1),$$

so every $a \in (\mathbb{Z}/p\mathbb{Z})^*$ is a root of exactly one of $x^{(p-1)/2} - 1$ and $x^{(p-1)/2} + 1$. Note also that if $a = b^2$ is a square, then

$$a^{(p-1)/2} = b^{p-1} = 1,$$

so a is a root of $x^{(p-1)/2} - 1$. Since we have already seen that there are exactly $\frac{p-1}{2}$ squares, this shows that the squares are precisely the roots of $x^{(p-1)/2} - 1$. In general, then, we have that a is a root of

$$x^{(p-1)/2} - \left(\frac{a}{p}\right),$$

which is the statement of the exercise.

SOLUTION 3.10. By Exercise 3.9,

$$\begin{aligned}\left(\frac{ab}{p}\right) &\equiv (ab)^{(p-1)/2} \pmod{p} \\ &\equiv a^{(p-1)/2} b^{(p-1)/2} \\ &\equiv \left(\frac{a}{p}\right)\left(\frac{b}{p}\right).\end{aligned}$$

Since both sides of the congruence lie in $\{0, \pm 1\}$ and $p \neq 2$, this implies that they are actually equal.

SOLUTION 3.11. Recall that $(\mathbb{Z}/p\mathbb{Z})^*$ is cyclic of order $p - 1$. Fix a generator g. Since d divides $p - 1$, one sees that $a \in (\mathbb{Z}/p\mathbb{Z})^*$ is a d^{th} power if and only if $a = g^k$ with k divisible by d.

Now, let $a = g^l$ be an arbitrary element of $(\mathbb{Z}/p\mathbb{Z})^*$. We have

$$a^{(p-1)/d} = g^{l(p-1)/d}.$$

Since g has order $p - 1$, this will be 1 precisely when d divides l. This is the same condition as we gave for an element to be a d^{th} power, so this tells us that a is a d^{th} power if and only if

$$a^{(p-1)/d} \equiv 1 \pmod{p}.$$

SOLUTION 3.12. We work in the field $\mathbb{Q}(\zeta_8)$. Note that

$$\zeta_8 + \zeta_8^{-1} = 2\cos\left(\frac{2\pi}{8}\right) = \sqrt{2}.$$

Thus $\mathbb{Q}(\sqrt{2})$ is a subfield of $\mathbb{Q}(\zeta_8)$; since

$$\sigma_7(\zeta_8 + \zeta_8^{-1}) = \zeta_8^{-1} + \zeta_8$$

we see that it is the fixed field of the subgroup $\{1, \sigma_7\}$ of $\mathrm{Gal}(\mathbb{Q}(\zeta_8)/\mathbb{Q})$.

Let $\mathfrak{p}$ be a prime of $\mathbb{Z}[\zeta_8]$ lying over p. We compute

$$\begin{aligned}\sigma_p(\sqrt{2}) &= \sigma_p(\zeta_8+\zeta_8^{-1})\\ &= \zeta_8^p+\zeta_8^{-p}\\ &\equiv (\zeta_8+\zeta_8^{-1})^p \pmod{\mathfrak{p}}\\ &\equiv (\sqrt{2})^p \pmod{\mathfrak{p}}.\end{aligned}$$

(We are using here that $p \in \mathfrak{p}$.) Now, the subfield $\mathbb{F}_p$ of $\mathbb{Z}[\zeta_8]/\mathfrak{p}$ is characterized as the roots of $x^p - x$. (It is well known that every element of $\mathbb{F}_p$ is a root of this polynomial, and since it has at most p roots they must be the only roots.) Thus

$$(\sqrt{2})^p \equiv \sqrt{2} \pmod{\mathfrak{p}}$$

if and only if $\sqrt{2} \in \mathbb{F}_p$; that is, if and only if $\left(\frac{2}{p}\right) = 1$. Combining all of this and using the fact that $2 \notin \mathfrak{p}$, we find that

$$\sigma_p(\sqrt{2}) = \left(\frac{2}{p}\right)\sqrt{2}.$$

Since $\mathbb{Q}(\sqrt{2})$ is the fixed field of $\{1, \sigma_7\}$, we know that

$$\sigma_p(\sqrt{2}) = \begin{cases}\sqrt{2} & p \equiv 1,7 \pmod 8;\\ -\sqrt{2} & p \equiv 3,5 \pmod 8).\end{cases}$$

Combining these expressions yields the desired formula.

Solution 3.13. Let $K = \mathbb{Q}(\sqrt{d})$ be a quadratic field with d a squarefree integer. Suppose first that $d \equiv 1 \pmod 4$. In this case the factorization of 2 depends on the factorization of the polynomial $x^2 - x + \frac{1-d}{4}$ modulo 2. If

$$\frac{1-d}{4} \equiv 0 \pmod 2$$

(or equivalently, $d \equiv 1 \pmod 8$), then this polynomial factors modulo 2 as $x(x-1)$ and we find that

$$\bigl(2\bigr) = \bigl(2, \frac{1+\sqrt{-d}}{2}\bigr)\bigl(2, \frac{1+\sqrt{-d}}{2} - 1\bigr).$$

If

$$\frac{1-d}{4} \equiv 1 \pmod 2$$

(equivalently $d \equiv 5 \pmod 8$), then the polynomial is irreducible, so $\bigl(2\bigr)$ remains prime.

Next take $d \equiv 2 \pmod 4$. In this case the relevant polynomial is $x^2 - d$, and modulo 2 it is just x^2. Thus 2 ramifies as

$$\bigl(2\bigr) = \bigl(2, \sqrt{-d}\bigr)^2.$$

When $d \equiv 3 \pmod 4$, the polynomial $x^2 - d$ factors as $(x+1)^2$ modulo 2, so we get

$$\bigl(2\bigr) = \bigl(2, \sqrt{-d}+1\bigr)^2.$$

SOLUTION 3.14. Recall that $\Delta(1, \alpha, \ldots, \alpha^{n-1})$ is the square of the determinant of the matrix

$$\begin{pmatrix} \sigma_1(1) & \sigma_1(\alpha) & \sigma_1(\alpha^2) & \cdots & \sigma_1(\alpha^{n-1}) \\ \sigma_2(1) & \sigma_2(\alpha) & \sigma_2(\alpha^2) & \cdots & \sigma_2(\alpha^{n-1}) \\ \vdots & \vdots & \vdots & & \vdots \\ \sigma_n(1) & \sigma_n(\alpha) & \sigma_n(\alpha^2) & \cdots & \sigma_n(\alpha^{n-1}) \end{pmatrix} =$$

$$\begin{pmatrix} \sigma_1(1) & \sigma_1(\alpha) & \sigma_1(\alpha)^2 & \cdots & \sigma_1(\alpha)^{n-1} \\ \sigma_2(1) & \sigma_2(\alpha) & \sigma_2(\alpha)^2 & \cdots & \sigma_2(\alpha)^{n-1} \\ \vdots & \vdots & \vdots & & \vdots \\ \sigma_n(1) & \sigma_n(\alpha) & \sigma_n(\alpha)^2 & \cdots & \sigma_n(\alpha)^{n-1} \end{pmatrix}$$

where the σ_i are the complex embeddings of K. This is just a Vandermonde matrix for $\sigma_1(\alpha), \sigma_2(\alpha), \ldots, \sigma_n(\alpha)$, and by standard results on Vandermonde matrices (which are easily proven by induction) it has determinant

$$\pm \prod_{i<j} \big(\sigma_i(\alpha) - \sigma_j(\alpha)\big).$$

The square of this determinant, then, is

$$\pm \prod_{i \neq j} \big(\sigma_i(\alpha) - \sigma_j(\alpha)\big).$$

We wish to show that this equals $\pm \mathrm{N}_{K/\mathbb{Q}}(f'(\alpha))$. Using the fact that $f'(x)$ has rational coefficients, we have

$$\begin{aligned} \mathrm{N}_{K/\mathbb{Q}}(f'(\alpha)) &= \prod_i \sigma_i(f'(\alpha)) \\ &= \prod_i f'(\sigma_i(\alpha)). \end{aligned}$$

Writing

$$f(x) = \prod_j \big(x - \sigma_j(\alpha)\big),$$

we find that

$$f'(x) = \sum_k \prod_{j \neq k} \big(x - \sigma_j(\alpha)\big).$$

When we plug in $\sigma_i(\alpha)$, every summand but one vanishes, and we have

$$f'(\sigma_i(\alpha)) = \prod_{j \neq i} \big(\sigma_i(\alpha) - \sigma_j(\alpha)\big).$$

Multiplying over all i now gives

$$\mathrm{N}_{K/\mathbb{Q}}(f'(\alpha)) = \pm \prod_i \prod_{j \neq i} \big(\sigma_i(\alpha) - \sigma_j(\alpha)\big),$$

which equals our expression for the discriminant, up to sign.

SOLUTION 3.15. We apply Exercise 3.14 with $K = \mathbb{Q}(\zeta_p)$, $\alpha = \zeta_p$ and $f(x) = x^{p-1} + x^{p-2} + \cdots + x + 1$. Since $\mathcal{O}_K = \mathbb{Z}[\zeta_p]$ it has integral basis $1, \zeta_p, \zeta_p^2, \ldots, \zeta_p^{p-2}$ and we find that

$$\Delta_K = \Delta(1, \zeta_p, \ldots, \zeta_p^{p-2}) = \pm \mathrm{N}_{K/\mathbb{Q}}(f'(\zeta_p)).$$

We compute $f'(\zeta_p)$ by using the fact that

$$x^p - 1 = (x-1)f(x).$$

Taking the derivative, we find that

$$px^{p-1} = f(x) + (x-1)f'(x).$$

Plugging in ζ_p yields

$$p\zeta_p^{p-1} = f(\zeta_p) + (\zeta_p - 1)f'(\zeta_p) = (\zeta_p - 1)f'(\zeta_p).$$

It now follows from Exercise 2.13 that $f'(\zeta_p)$ is a unit multiple of $(\zeta_p - 1)^{p-2}$. Since $\zeta_p - 1$ has norm p (we have computed this before in many different forms) and units have norm ± 1, we find that

$$\Delta_K = \pm \mathrm{N}_{K/\mathbb{Q}}\big((\zeta_p - 1)^{p-2}\big) = \pm p^{p-2}.$$

Solution 3.16. By Exercise 3.14 we know that

$$\Delta_K = \mathrm{N}_{K/\mathbb{Q}}(f'(\alpha))$$

where $f(x) \in \mathbb{Z}[x]$ is the minimal polynomial of α It follows that p divides Δ_K if and only if there is some prime $\mathfrak{p}$ of K, lying over p, such that $f'(\alpha) \in \mathfrak{p}$. (The only way to get a factor of p in $\mathrm{N}_{K/\mathbb{Q}}(f'(\alpha))$ is to have a prime lying over p in the ideal factorization of $f'(\alpha)$.)

So suppose first that p divides Δ_K, and let $\mathfrak{p}$ be the prime over p occurring in the factorization of $f'(\alpha)$. Let $\mathfrak{p} = \big(p, g(\alpha)\big)$ where $g(x) \in \mathbb{Z}[x]$ is such that $\bar{g}(x)$ is an irreducible factor of $f(x)$ modulo p. Since $f'(\alpha) \in \mathfrak{p}$, we can write

$$f'(\alpha) = pa(\alpha) + g(\alpha)b(\alpha)$$

for some $a(x), b(x) \in \mathbb{Z}[x]$. Since $\mathbb{Z}[\alpha] = \mathbb{Z}[x]/(f(x))$, this equation means precisely that

$$f'(x) = pa(x) + g(x)b(x) + f(x)c(x)$$

in $\mathbb{Z}[x]$ for some polynomial $c(x) \in \mathbb{Z}[x]$. Since $\bar{g}(x)$ is a factor of $\bar{f}(x)$ in $\mathbb{F}_p[x]$, this implies that $\bar{g}(x)$ is also a factor of $\bar{f}'(x)$ in $\mathbb{F}_p[x]$.

Write $\bar{f}(x) = \bar{g}(x)\bar{h}(x)$. Then

$$\bar{f}'(x) = \bar{g}'(x)\bar{h}(x) + \bar{g}(x)\bar{h}'(x),$$

so $\bar{g}(x)$ must divide $\bar{g}'(x)\bar{h}(x)$. Since $\bar{g}(x)$ is irreducible in $\mathbb{F}_p[x]$, this means that either $\bar{g}(x)$ divides $\bar{h}(x)$ or $\bar{g}(x)$ divides $\bar{g}'(x)$. In the first case, we see that $\bar{f}(x)$ has a repeated factor, so p ramifies in K, as claimed. In the second case, we must have $\bar{g}'(x) = 0$, since it has smaller degree than $\bar{g}(x)$. This means that we can write $\bar{g}(x)$ as a polynomial in x^p (powers of x^p are the only terms which vanish under differentiation):

$$\bar{g}(x) = a_n x^{np} + \cdots + a_1 x^p + a_0 = (a_n x^n + \cdots + a_1 x + a_0)^p.$$

But this is ridiculous, since $\bar{g}(x)$ is irreducible. This shows that the second case can not occur, and this completes the proof that p ramifies.

For the other direction, under the assumption that p ramifies, we know that $\bar{f}(x)$ has a repeated factor. It follows that there is some irreducible factor $\bar{g}(x)$ of $\bar{f}(x)$ dividing $\bar{f}'(x)$. Writing

$$f'(x) = pa(x) + g(x)b(x)$$

in $\mathbb{Z}[x]$, we see that

$$f'(\alpha) \in \big(p, g(\alpha)\big);$$

this is a prime lying over p, and therefore p divides $\mathrm{N}_{K/\mathbb{Q}}(f'(\alpha))$, as claimed.

SOLUTION 3.17. Let A be the $n \times n$ integer matrix such that

$$A \begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{pmatrix} = \begin{pmatrix} \beta_1 \\ \vdots \\ \beta_n \end{pmatrix}.$$

(A has integer entries since by assumption the b_j can be written as $\mathbb{Z}$-linear combinations of the a_j.) Applying the complex embeddings σ_i and rewriting the n matrix equations as one big matrix equation, we find that

$$A\big(\sigma_i(\alpha_j)\big) = \big(\sigma_i(\beta_j)\big).$$

Therefore

$$(\det A)^2 \Delta(\alpha_1, \ldots, \alpha_n) = \Delta(\beta_1, \ldots, \beta_n),$$

which proves the claim.

SOLUTION 3.18. By Lemma 2.18 we have

$$\Delta(1, \alpha, \alpha^2) = \det \begin{pmatrix} \mathrm{Tr}(1) & \mathrm{Tr}(\alpha) & \mathrm{Tr}(\alpha^2) \\ \mathrm{Tr}(\alpha) & \mathrm{Tr}(\alpha^2) & \mathrm{Tr}(\alpha^3) \\ \mathrm{Tr}(\alpha^2) & \mathrm{Tr}(\alpha^3) & \mathrm{Tr}(\alpha^4) \end{pmatrix}$$

where Tr denotes $\mathrm{Tr}_{K/\mathbb{Q}}$. It remains to compute these traces. Since α has minimal polynomial $x^3 + 2x + 1$, we have

$$\mathrm{Tr}(\alpha) = 0.$$

To compute $\mathrm{Tr}(\alpha^2)$ we must find the minimal polynomial of α^2. Note that α^2 has degree 3 since α does, so we only need to find the characteristic polynomial. In fact, since all we care about are traces we just need to compute the trace of the matrix for α^2. This matrix (with respect to the basis $1, \alpha, \alpha^2$) is

$$\begin{pmatrix} 0 & -1 & 0 \\ 0 & -2 & -1 \\ 1 & 0 & -2 \end{pmatrix}$$

which has trace -4.

For $\alpha^3 = -2\alpha - 1$, we have

$$\mathrm{Tr}(\alpha^3) = \mathrm{Tr}(-2\alpha - 1) = -2\,\mathrm{Tr}(\alpha) - \mathrm{Tr}(1) = -3.$$

For $\alpha^4 = -2\alpha^2 - \alpha$, we have

$$\mathrm{Tr}(\alpha^4) = \mathrm{Tr}(-2\alpha^2 - \alpha) = -2\,\mathrm{Tr}(\alpha^2) - \mathrm{Tr}(\alpha) = 8.$$

We have now computed the trace matrix; it is

$$\begin{pmatrix} 3 & 0 & -4 \\ 0 & -4 & -3 \\ -4 & -3 & 8 \end{pmatrix}$$

This has determinant -59, which completes the calculation.

Now, α is an algebraic integer, so we clearly have

$$\mathbb{Z}[\alpha] \subseteq \mathcal{O}_K.$$

Suppose that this was not an equality and let $\beta_1, \beta_2, \beta_3$ be an integral basis for $\mathcal{O}_K$. By Exercise 3.17, $\Delta_K = \Delta(\beta_1, \beta_2, \beta_3)$ must be the quotient of $\Delta(1, \alpha, \alpha^2) = -59$

by a square. Since Δ_K is an integer and -59 is squarefree, this is impossible. Thus $\mathbb{Z}[\alpha] = \mathcal{O}_K$, as claimed.

SOLUTION 3.19. We know that the inertial degree of $\mathfrak{p}$ equals the order of p modulo 7; therefore,

$$f(\mathfrak{p}/p) = \begin{cases} 1 & p \equiv 1 \pmod 7; \\ 2 & p \equiv 6 \pmod 7; \\ 3 & p \equiv 2, 4 \pmod 7; \\ 6 & p \equiv 3, 5 \pmod 7. \end{cases}$$

There is also the case of $p = 7$, which is totally ramified; thus the prime lying over 7 has inertial degree 1.

SOLUTION 3.20. First take $p = 3$. We have

$$\Phi_{15}(x) = \frac{(x^{15} - 1)(x - 1)}{(x^5 - 1)(x^3 - 1)} = x^8 - x^7 + x^5 - x^4 + x^3 - x + 1$$

and we wish to determine its factorization modulo 3. The easiest way to do this is to determine the factorization of each $x^n - 1$ for $n = 3, 5, 15$. First,

$$x^3 - 1 = (x - 1)^3.$$

We have

$$x^5 - 1 = (x - 1)(x^4 + x^3 + x^2 + x + 1).$$

In fact, the second factor is just $\Phi_5(x)$, and our factorization results on cyclotomic fields apply in this case to tell us that it is irreducible modulo 3. The last polynomial is

$$x^{15} - 1 = (x^5 - 1)^3 = (x - 1)^3(x^4 + x^3 + x^2 + x + 1)^3.$$

Combining these factorizations, we find that

$$\Phi_{15}(x) = (x^4 + x^3 + x^2 + x + 1)^2.$$

$\big(3\big)$ therefore factors as

$$\big(3\big) = \big(3, \zeta_{15}^4 + \zeta_{15}^3 + \zeta_{15}^2 + \zeta_{15} + 1\big)^2;$$

in particular, it has inertial degree 4 and ramification index 2.

For $p = 5$ we use the same method. This time, we have

$$x^3 - 1 = (x - 1)(x^2 + x + 1)$$

and the second factor is irreducible. We also have

$$x^5 - 1 = (x - 1)^5$$

and

$$x^{15} - 1 = (x^3 - 1)^5 = (x - 1)^5(x^2 + x + 1)^5.$$

Thus

$$\Phi_{15}(x) = (x^2 + x + 1)^4,$$

so

$$\big(5\big) = \big(5, \zeta_{15}^2 + \zeta_{15} + 1\big)^4.$$

We also see that $\big(5\big)$ has inertial degree 2 and ramification index 4.

SOLUTION 3.21. By Proposition 2.26 we know that $\mathcal{O}_K = \mathbb{Z}[\sqrt[3]{2}]$. We can therefore factor primes by factoring $x^3 - 2$ modulo p. We find that

$$\begin{aligned}
x^3 - 2 &\equiv x^3 \pmod 2\\
x^3 - 2 &\equiv (x+1)^3 \pmod 3\\
x^3 - 2 &\equiv (x+2)(x^2+3x+4) \pmod 5\\
x^3 - 2 &\equiv (x+4)(x^2+7x+5) \pmod{11}
\end{aligned}$$

while it is irreducible modulo 7. This yields the ideal factorizations

$$\begin{aligned}
(2) &= \left(2, \sqrt[3]{2}\right)^3\\
(3) &= \left(3, \sqrt[3]{2}+1\right)^3\\
(5) &= \left(5, \sqrt[3]{2}+2\right)\left(5, \sqrt[3]{4}+3\sqrt[3]{2}+4\right)\\
(11) &= \left(11, \sqrt[3]{2}+4\right)\left(11, \sqrt[3]{4}+7\sqrt[3]{2}+5\right)
\end{aligned}$$

while the ideal (7) is still prime.

To find a prime which splits completely we should first limit our search as much as possible. Note that p will split completely if and only if 2 has three distinct cube roots modulo p. This will occur if and only if 1 has three distinct cube roots and 2 has a cube root modulo p. The first condition is easy; this occurs precisely when $p \equiv 1 \pmod 3$. The second condition is somewhat harder to give a simple condition for. The best easy one is to observe that by Exercise 3.11 if $p \equiv 1 \pmod 3$, then 2 is a cube modulo p if and only if

$$2^{(p-1)/3} \equiv 1 \pmod p.$$

This at least gives a solid criterion with which to check values of p.

Using these conditions one finds that 31 is the first prime which works. Specifically,

$$x^3 - 2 \equiv (x-11)(x-24)(x-27) \pmod{31},$$

so

$$(31) = \left(31, \sqrt[3]{2}-11\right)\left(31, \sqrt[3]{2}-24\right)\left(31, \sqrt[3]{2}-27\right).$$

SOLUTION 3.22. We must show that as x runs through all integers, the values $f(x)$ have infinitely many distinct prime factors. If $f(0) = 0$, then this value alone has infinitely many prime factors, so the assertion is clear.

Suppose next that $f(x)$ has constant term 1; that is, $f(0) = 1$. Consider the values $f(n!)$. Since $f(0) = 1$, one sees immediately that $f(n!)$ is not divisible by any of $2, 3, \dots, n$. In particular, $f(n!)$ will only have prime factors larger than n. Taking n to be large now shows that $f(x)$ can have arbitrarily large prime factors, and therefore that these values must have infinitely many different prime factors.

For the general case, set $a = f(0)$ and consider instead the polynomial

$$g(x) = \frac{f(ax)}{a} \in \mathbb{Z}[x].$$

($g(x)$ is in $\mathbb{Z}[x]$ since every coefficient of $f(ax)$ is divisible by a.) $g(x)$ satisfies $f(0) = 1$, so the argument above shows that there are infinitely many primes dividing values of $g(x)$. Since $g(x)$ divides $f(ax)$, this proves the claim.

SOLUTION 3.23. Let $f(x) \in \mathbb{Z}[x]$ be the minimal polynomial for α. We know that there exists $\mathfrak{p}$ lying over p with $f(\mathfrak{p}/p) = 1$ if and only if $f(x)$ has a linear factor modulo p; that is, if and only if $f(x)$ has a root modulo p. By Exercise 3.22 $f(x)$ has roots modulo infinitely many different primes, which now proves this exercise as well.

SOLUTION 3.24. Let $\mathfrak{p}$ be a prime of $\mathbb{Q}(\zeta_m)$, lying over p relatively prime to m, such that $f(\mathfrak{p}/p) = 1$; by Exercise 3.23 there are infinitely many such $\mathfrak{p}$ and p. On the other hand, by our characterization of splitting in cyclotomic fields, we know that $f(\mathfrak{p}/p)$ equals the order of p modulo m. We see, therefore, that there are infinitely many primes p of order 1 modulo m. That is, there are infinitely many p such that

$$p \equiv 1 \pmod{m}.$$

4. Chapter 4

SOLUTION 4.1. There are many ways to do this. The simplest is to take any $\gamma \in K - \mathcal{O}_K$ and let $\mathfrak{r}$ be the $\mathcal{O}_K$-module generated by the powers of γ. Note that $\mathfrak{r}$ has the property that $\gamma\mathfrak{r} \subseteq \mathfrak{r}$. If $\mathfrak{r}$ is finitely generated over $\mathcal{O}_K$, then Proposition II.2.9 tells us that $\gamma \in \mathcal{O}_K$, which is a contradiction. Thus $\mathfrak{r}$ is not a finitely generated $\mathcal{O}_K$-module.

SOLUTION 4.2. Let $\mathfrak{a}$ be an ideal of $\mathcal{O}_K$ and suppose that $\mathrm{N}_{K/\mathbb{Q}}(\mathfrak{a}) < N$. Let

$$\mathfrak{a} = \mathfrak{p}_1^{n_1} \cdots \mathfrak{p}_r^{n_r}$$

be the prime factorization of $\mathfrak{a}$ and let p_i be the rational prime lying under $\mathfrak{p}_i$, with inertial degree f_i. Then

$$\mathrm{N}_{K/\mathbb{Q}}(\mathfrak{a}) = p_1^{f_1 n_1} \cdots p_r^{f_r n_r}.$$

In particular, for each p_i we have

$$p_i < N$$

and

$$n_i < \log_{p_i}(N).$$

This tells us that there are only a finite number of choices for the p_i and for each p_i there are only a finite number of choices for the n_i. Furthermore, there are at most $[K : \mathbb{Q}]$ prime ideals of $\mathcal{O}_K$ lying over each p_i, and thus only a finite number of choices for the $\mathfrak{p}_i$. Since there are only finitely many choices for the $\mathfrak{p}_i$ and the n_i, it follows that there are only finitely many possibilities for $\mathfrak{a}$.

SOLUTION 4.3. The ideal $\big(p, \alpha + m\big)$ has $\mathbb{Z}[\alpha]$-generators $p, \alpha + m$, and thus $\mathbb{Z}$-generators $p, p\alpha, \alpha + m, \alpha^2 + m\alpha$. We must show how to express $p\alpha$ and $\alpha^2 + m\alpha$ as $\mathbb{Z}$-linear combinations of p and $\alpha + m$.

First suppose that $d \equiv 2, 3 \pmod 4$. Then $-m$ is a root of $x^2 - d$ modulo p, so p divides $m^2 - d$. We also have $\alpha^2 + m\alpha = d + m\alpha$, so we can write

$$p\alpha = -m \cdot (p) + p \cdot (\alpha + m)$$
$$d + m\alpha = \frac{d - m^2}{p} \cdot (p) + m \cdot (\alpha + m).$$

Now suppose that $d \equiv 1 \pmod 4$. $-m$ is a root of $x^2 - x + \frac{1-d}{4}$, so p divides

$$m^2 + m + \frac{1-d}{4}.$$

We have $\alpha^2 = \alpha - \frac{1-d}{4}$, so $\alpha^2 + m\alpha = (m+1)\alpha - \frac{1-d}{4}$ and we can write

$$p\alpha = -m \cdot (p) + p \cdot (\alpha + m)$$
$$-\frac{1-d}{4} + (m+1)\alpha = \frac{-m^2 - m - \frac{1-d}{4}}{p} \cdot (p) + (m+1) \cdot (\alpha + m).$$

SOLUTION 4.4. Let α be any element of $\mathfrak{a}$. Then $\gamma\alpha$ is some element of $\mathfrak{b}$, say β. Thus $\gamma = \beta/\alpha$ lies in K^*, since both β and α do.

SOLUTION 4.5. We have $K = \mathbb{Q}(\sqrt{-15})$, $\alpha = \frac{1+\sqrt{-15}}{2}$, $f(x) = x^2 - x + 4$. In particular, $\alpha^2 = \alpha - 4$. The Minkowski bound is $\mu_K \approx 2.46561777625$, so we must consider only the factorization of $\big(2\big)$:

$$\big(2\big) = \big(2, \alpha\big)\big(2, \alpha + 1\big).$$

Let $\mathfrak{a}_1 = \mathcal{O}_K$, $\mathfrak{a}_2 = \bigl(2, \alpha\bigr)$, $\mathfrak{a}_2' = \bigl(2, \alpha + 1\bigr)$. We compute (using Exercise 4.3) that

$$\begin{aligned} \mathsf{j}(\mathfrak{a}_1) &= \frac{1}{2} + \frac{\sqrt{15}}{2} i; \\ \mathsf{j}(\mathfrak{a}_2) &= \frac{1}{4} + \frac{\sqrt{15}}{4} i; \\ \mathsf{j}(\mathfrak{a}_2') &= \frac{1}{4} + \frac{\sqrt{15}}{4} i. \end{aligned}$$

(Note that in the computation of $\mathsf{j}(\mathfrak{a}_2')$ we first get $-\frac{1}{4} + \frac{\sqrt{-15}}{4}$, which lies on the unit circle but on the wrong side of it. Replacing it with its negative reciprocal yields the results above.) We conclude that $\mathfrak{a}_2 \sim \mathfrak{a}_2'$, and thus that $\mathcal{C}_K$ is cyclic of order 2.

Our formula for the appropriate quadratic forms yields the two forms

$$x^2 + xy + 4y^2$$

and

$$2x^2 + xy + 2y^2.$$

We also find that

$$\left(\frac{-15}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{3}{p}\right)\left(\frac{5}{p}\right) = \left(\frac{p}{3}\right)\left(\frac{p}{5}\right),$$

using quadratic reciprocity. (The $\left(\frac{-1}{p}\right)$ cancels with the sign coming from QR applied to $\left(\frac{3}{p}\right)$.) This easily shows that $\left(\frac{-15}{p}\right) = 1$ if and only if

$$p \equiv 1, 2, 4, 8 \pmod{15}.$$

We conclude that a positive rational prime $p \neq 2, 3, 5$ can be written as at least one of

$$x^2 + xy + 4y^2, 2x^2 + xy + 2y^2$$

if and only if

$$p \equiv 1, 2, 4, 8 \pmod{15}.$$

SOLUTION 4.6. We have $K = \mathbb{Q}(\sqrt{-26})$, $\alpha = \sqrt{-26}$, $f(x) = x^2 + 26$ and $\mu_K \approx 6.49227328409$. The relevant factorizations are

$$\begin{aligned} (2) &= \bigl(2, \alpha\bigr)^2 \\ (3) &= \bigl(3, \alpha + 1\bigr)\bigl(3, \alpha + 2\bigr); \\ (5) &= \bigl(5, \alpha + 2\bigr)\bigl(5, \alpha + 3\bigr). \end{aligned}$$

Set $\mathfrak{a}_1 = \mathcal{O}_K$, $\mathfrak{a}_2 = \bigl(2, \alpha\bigr)$, $\mathfrak{a}_3 = \bigl(3, \alpha + 1\bigr)$, $\alpha_3' = \bigl(3, \alpha + 2\bigr)$, $\alpha_5 = \bigl(5, \alpha + 2\bigr)$, $\alpha_5' = \bigl(5, \alpha + 3\bigr)$. We compute

$$\begin{aligned} \mathsf{j}(\mathfrak{a}_1) &= \sqrt{26} i; \\ \mathsf{j}(\mathfrak{a}_2) &= \frac{\sqrt{26}}{2} i; \\ \mathsf{j}(\mathfrak{a}_3) &= \frac{1}{3} + \frac{\sqrt{26}}{3} i; \end{aligned}$$

$$\mathfrak{j}(\mathfrak{a}_3') = -\frac{1}{3} + \frac{\sqrt{26}}{3}i;$$
$$\mathfrak{j}(\mathfrak{a}_5) = \frac{2}{5} + \frac{\sqrt{26}}{5}i;$$
$$\mathfrak{j}(\mathfrak{a}_5') = -\frac{2}{5} + \frac{\sqrt{26}}{5}i.$$

Let us first compute the powers of $\mathfrak{a}_3$. We find that

$$\mathfrak{a}_3^2 = \big(9, 3\alpha+3, \alpha^2+2\alpha+1\big) = \big(9, 3\alpha+3, 2\alpha-25\big) = \big(9, \alpha+1\big).$$

This has $\mathfrak{j} = -\frac{1}{3} + \frac{\sqrt{26}}{3}i$, so $\mathfrak{a}_3^2 \sim \mathfrak{a}_3'$. We conclude that $\mathfrak{a}_3$ has order 3.

Next we compute the powers of $\mathfrak{a}_5$. We find that

$$\mathfrak{a}_5^2 = \big(25, 5\alpha+10, \alpha^2+4\alpha+4\big) = \big(25, 5\alpha+10, 4\alpha-22\big) = \big(25, \alpha+7\big).$$

This has $\mathfrak{j} = -\frac{1}{3} + \frac{\sqrt{26}}{3}i$, so $\mathfrak{a}_5^2 \sim \mathfrak{a}_3'$. In particular, we know that $\mathfrak{a}_5$ has order 6, and we know that $\mathfrak{a}_5^4 \sim \mathfrak{a}_3$ and $\mathfrak{a}_5^5 \sim \mathfrak{a}_5'$. It remains to compute $\mathfrak{a}_5^3$. We find that

$$\begin{aligned}\mathfrak{a}_5^3 \sim \mathfrak{a}_5\mathfrak{a}_3' &= \big(5, \alpha+2\big)\big(3, \alpha+2\big) = \big(15, 5\alpha+10, 3\alpha+6, \alpha^2+4\alpha+4\big)\\ &= \big(15, 5\alpha+10, 3\alpha+6, 4\alpha-22\big) = \big(15, \alpha+2\big).\end{aligned}$$

This has $\mathfrak{j} = \frac{\sqrt{26}}{2}i$, so we conclude that $\mathfrak{a}_5^3 \sim \mathfrak{a}_2$. Thus $\mathcal{C}_K$ is cyclic of order 6 with generator $\mathfrak{a}_5$.

Solution 4.7. We have $K = \mathbb{Q}(\sqrt{-41})$, $\alpha = \sqrt{-41}$, $f(x) = x^2 + 41$ and $\mu_K \approx 8.15271098894$. The relevant factorizations are

$$(2) = \big(2, \alpha+1\big)^2$$
$$(3) = \big(3, \alpha+1\big)\big(3, \alpha+2\big);$$
$$(5) = \big(5, \alpha+2\big)\big(5, \alpha+3\big);$$
$$(7) = \big(7, \alpha+1\big)\big(7, \alpha+6\big).$$

Set $\mathfrak{a}_1 = \mathcal{O}_K$, $\mathfrak{a}_2 = \big(2, \alpha+1\big)$, $\mathfrak{a}_3 = \big(3, \alpha+1\big)$, $\alpha_3' = \big(3, \alpha+2\big)$, $\alpha_5 = \big(5, \alpha+2\big)$, $\alpha_5' = \big(5, \alpha+3\big)$, $\alpha_7 = \big(7, \alpha+1\big)$, $\alpha_7' = \big(7, \alpha+6\big)$. We compute

$$\mathfrak{j}(\mathfrak{a}_1) = \sqrt{41}i;$$
$$\mathfrak{j}(\mathfrak{a}_2) = \frac{1}{2} + \frac{\sqrt{41}}{2}i;$$
$$\mathfrak{j}(\mathfrak{a}_3) = \frac{1}{3} + \frac{\sqrt{41}}{3}i;$$
$$\mathfrak{j}(\mathfrak{a}_3') = -\frac{1}{3} + \frac{\sqrt{41}}{3}i;$$
$$\mathfrak{j}(\mathfrak{a}_5) = \frac{2}{5} + \frac{\sqrt{41}}{5}i;$$
$$\mathfrak{j}(\mathfrak{a}_5') = -\frac{2}{5} + \frac{\sqrt{41}}{5}i;$$
$$\mathfrak{j}(\mathfrak{a}_7) = -\frac{1}{6} + \frac{\sqrt{41}}{6}i;$$
$$\mathfrak{j}(\mathfrak{a}_7') = \frac{1}{6} + \frac{\sqrt{41}}{6}i.$$

We begin by computing the powers of $\mathfrak{a}_3$. We have

$$\mathfrak{a}_3^2 = \big(9, 3\alpha+3, \alpha^2+2\alpha+1\big) = \big(9, 3\alpha+3, 2\alpha-40\big) = \big(9, \alpha+7\big).$$

This has $\mathfrak{j} = \frac{2}{5} + \frac{\sqrt{41}}{5}i$, so we find that $\mathfrak{a}_3^2 \sim \mathfrak{a}_5$. Next we have

$$\begin{aligned}\mathfrak{a}_3^3 &\sim \mathfrak{a}_5\mathfrak{a}_3 = \big(5, \alpha+2\big)\big(3, \alpha+1\big) = \big(15, 5\alpha+5, 3\alpha+6, \alpha^2+3\alpha+2\big)\\ &= \big(15, 5\alpha+5, 3\alpha+6, 3\alpha-39\big) = \big(15, \alpha+7\big).\end{aligned}$$

This has $\mathfrak{j} = -\frac{1}{6} + \frac{\sqrt{41}}{6}i$, so $\mathfrak{a}_3^3 \sim \mathfrak{a}_7$. Next we compute

$$\begin{aligned}\mathfrak{a}_3^4 &\sim \mathfrak{a}_7\mathfrak{a}_3 = \big(7, \alpha+1\big)\big(3, \alpha+1\big) = \big(21, 7\alpha+7, 3\alpha+3, \alpha^2+2\alpha+1\big)\\ &= \big(21, 7\alpha+7, 3\alpha+3, 2\alpha-40\big) = \big(21, \alpha+1\big).\end{aligned}$$

This has $\mathfrak{j} = \frac{1}{2} + \frac{\sqrt{41}}{2}i$, so $\mathfrak{a}_3^4 \sim \mathfrak{a}_2$. This tells us that $\mathfrak{a}_3$ has order 8, and we find that $\mathfrak{a}_3^5 \sim \mathfrak{a}_7'$, $\mathfrak{a}_3^6 \sim \mathfrak{a}_5'$ and $\mathfrak{a}_3^7 \sim \mathfrak{a}_3'$. In particular, $\mathcal{C}_K$ is cyclic of order 8.

SOLUTION 4.8. We begin with the case that $d \equiv 2, 3 \pmod 4$. In this case $\big(2\big)$ factors as either

$$\big(2\big) = \big(2, \alpha\big)^2$$

or

$$\big(2\big) = \big(2, \alpha+1\big)^2.$$

In particular, if K is a PID, then the prime lying over 2 is principal. This ideal has norm 2, so any generator would also have to have norm 2. But in $\mathbb{Z}[\sqrt{d}]$, we have

$$\mathrm{N}_{K/\mathbb{Q}}(x + y\sqrt{d}) = x^2 - dy^2.$$

The Diophantine equation $x^2 - dy^2 = 2$ only has solutions (with $d < 0$) if $d = -1$ or $d = -2$, which shows that if $\mathcal{O}_K$ is a PID and $d \equiv 2, 3 \pmod 4$, then $d = -1$ or -2.

We turn now to the $d \equiv 1 \pmod 4$ case. We must show that if $\mathcal{O}_K$ is a PID and $d \equiv 1 \pmod 8$, then $d = -7$. When $d \equiv 1 \pmod 8$, 2 factors as

$$\big(2\big) = \big(2, \alpha\big)\big(2, \alpha+1\big),$$

where as usual $\alpha = \frac{1+\sqrt{d}}{2}$. We will show that $\big(2, \alpha\big)$ is not principal unless $d = -7$. We could again use a norm argument, but instead we use our $\mathfrak{j}$-invariant methods. Specifically, $\mathcal{O}_K$ has $\mathfrak{j}$-invariant

$$\frac{1}{2} + \frac{\sqrt{-d}}{2}i$$

and $\big(2, \alpha\big)$ has $\mathfrak{j}$-invariant

$$\frac{1}{4} + \frac{\sqrt{-d}}{4}i.$$

If both of these lie in the fundamental domain Y then it follows that $\big(2, \alpha\big)$ is not principal and thus that $\mathcal{O}_K$ is not a PID. The value for $\mathcal{O}_K$ is certainly in Y since $-d \geq 7$. The value for $\big(2, \alpha\big)$ will be in Y so long as it has absolute value at least 1. This occurs when

$$\begin{aligned}\left|\frac{1}{4} + \frac{\sqrt{-d}}{4}i\right| &\geq 1\\ \frac{1}{16} + \frac{-d}{16} &\geq 1\\ -d &\geq 15.\end{aligned}$$

Since $d \equiv 1 \pmod 8$, this leaves only the case $d = -7$, which was the desired exception.

SOLUTION 4.9. We have $K = \mathbb{Q}(\sqrt{10})$, $\alpha = \sqrt{10}$, $f(x) = x^2 - 10$ and $\mu_K \approx 4.02633696836$. The relevant factorizations are

$$\begin{aligned}(2) &= \bigl(2, \alpha\bigr)^2;\\ (3) &= \bigl(3, \alpha + 1\bigr)\bigl(3, \alpha + 2\bigr).\end{aligned}$$

Let us first show that these ideals are not principal. Note that if any of them were principal, then they would have to be generated by elements of $\mathcal{O}_K$ of norm 2 or 3. In particular, there would exists solutions of the Diophantine equations $x^2 - 10y^2 = 2$ or $x^2 - 10y^2 = 3$. However, considering these equations modulo 5 shows that there are no solutions (since 2 and 3 are not squares in $\mathbb{Z}/5\mathbb{Z}$), so no such elements exist and these ideals are not principal.

It remains to show, then, that these ideals are all equivalent. We begin with $\bigl(2, \alpha\bigr)$ and $\bigl(3, \alpha + 1\bigr)$. Note that assuming that they are equivalent, the fractional ideal

$$\bigl(2, \alpha\bigr)\bigl(3, \alpha + 1\bigr)^{-1}$$

is principal. Since

$$\bigl(3, \alpha + 1\bigr)^{-1} \sim \bigl(3, \alpha + 2\bigr),$$

this should mean that the ideal

$$\bigl(2, \alpha\bigr)\bigl(3, \alpha + 2\bigr)$$

is principal. We compute

$$\bigl(2, \alpha\bigr)\bigl(3, \alpha + 2\bigr) = \bigl(6, 2\alpha + 4, 3\alpha, \alpha^2 + 2\alpha\bigr) = \bigl(6, 2\alpha + 4, 3\alpha, 2\alpha + 10\bigr) = \bigl(6, \alpha + 2\bigr).$$

We find that $\mathrm{N}_{K/\mathbb{Q}}(\alpha + 2) = -6$, so $\alpha + 2$ divides 6 and this ideal is indeed a principal ideal:

$$\bigl(2, \alpha\bigr)\bigl(3, \alpha + 2\bigr) = \bigl(\alpha + 2\bigr).$$

Going backwards we find that

$$\bigl(2, \alpha\bigr) = \frac{\alpha + 2}{3}\bigl(3, \alpha + 1\bigr),$$

so these ideals are equivalent. Since $\bigl(2, \alpha\bigr)$ is its own inverse this also implies that $\bigl(2, \alpha\bigr)$ and $\bigl(3, \alpha+2\bigr)$ are equivalent, and thus also that $\bigl(3, \alpha+1\bigr)$ and $\bigl(3, \alpha+2\bigr)$ are equivalent Thus $h_K = 2$.

SOLUTION 4.10. Let $K = \mathbb{Q}(\zeta_{11})$. We have $\Delta_K = 11^9$, $n = 10$ and $s = 5$, so we compute

$$\mu_K \approx 58.9631543984.$$

We must therefore show that every prime of $\mathcal{O}_K$ of norm at most 59 is principal.

Let $\mathfrak{p}$ be a prime of $\mathcal{O}_K$ of norm < 59. Let p be a prime of $\mathbb{Z}$ lying under $\mathfrak{p}$ and let f be the inertial degree $f(\mathfrak{p}/p)$. Since $\mathrm{N}_{K/\mathbb{Q}}(\mathfrak{p}) = p^f$, we must have $p^f < 59$. In particular, we must either have $p \leq 7$ or $f = 1$.

For $p = 2, 3, 5, 7$, we compute $f = 10, 5, 5, 10$ respectively. It follows that theses cases can not occur.

Recall that we will have $f = 1$ if and only if $p = 11$ or $p \equiv 1 \pmod{11}$. For $p = 11$, we have the prime

$$\bigl(\zeta_{11} - 1\bigr)$$

which we know to be principal. This leaves the case of $p = 23$. 23 splits completely in $\mathcal{O}_K$, so there are 10 ideals $\mathfrak{p}_1, \ldots, \mathfrak{p}_{10}$ of $\mathcal{O}_K$ lying over 23. Note that if any one of them is principal then they all must be principal; for example, one can use Lemma III.2.14. We have therefore reduced ourselves to the question of whether or not the primes lying over 23 are principal. Note that any element of $\mathcal{O}_K$ of norm ± 23 would generate such an ideal, and conversely any generator of such an ideal must have norm ± 23. Thus $\mathcal{O}_K$ will be a UFD if and only if it has an element of norm ± 23.

5. Chapter 5

SOLUTION 5.1. If x and y are not congruent modulo p, then there is nothing to do, so suppose that $x \equiv y \pmod{p}$. Then

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

Set $x' = x$, $y' = -z$, $z' = -y$. Since p is odd we have

$$(x')^p + (y')^p = x^p - z^p = -y^p = (z')^p.$$

Also,

$$y' = -z \equiv -2x \pmod{p}.$$

This means that if $x' \equiv y' \pmod{p}$, then $x \equiv -2x \pmod{p}$, so p divides $3x$. Since $p \geq 5$ and p does not divide x this is impossible; thus x' and y' are not congruent modulo p, as desired.

SOLUTION 5.2. Since $\mathfrak{a}$ divides (α) and (β), we have $\alpha, \beta \in \mathfrak{a}$. Since $\mathfrak{a}$ is an ideal, this implies that $\alpha + \beta \in \mathfrak{a}$, and thus that $\mathfrak{a} \supseteq (\alpha + \beta)$. Since $\mathcal{O}_K$ is a Dedekind domain, this in turn implies that $\mathfrak{a}$ divides $(\alpha + \beta)$, as claimed.

SOLUTION 5.3. Write

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

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

$$\begin{aligned}
\alpha^p &\equiv \big(a_0 + a_1\zeta + \cdots + a_{p-2}\zeta^{p-2}\big)^p \pmod{p} \\
&\equiv a_0^p + a_1^p\zeta^p + \cdots + a_{p-2}^p\zeta^{(p-2)p} \\
&\equiv a_0 + a_1 + \cdots + a_{p-2} \pmod{p},
\end{aligned}$$

which is an integer, as claimed.

SOLUTION 5.4. Recall that if $f : \mathbb{R} \to \mathbb{R}$ is any function, then we can write

$$f(t) = \frac{f(t) + f(-t)}{2} + \frac{f(t) - f(-t)}{2}$$

where the first summand is even and the second summand is odd. We simply apply this formula to $f(t) = \frac{t}{e^t - 1}$. We find

$$\begin{aligned}
f(t) + f(-t) &= \frac{t}{e^t - 1} + \frac{-t}{e^{-t} - 1} \\
&= \frac{t(e^{-t} - 1) - t(e^t - 1)}{(e^t - 1)(e^{-t} - 1)} \\
&= \frac{t(e^t - e^{-t})}{e^t - 2 + e^{-t}} \\
&= \frac{t(e^t - e^{-t})}{(e^{t/2} - e^{-t/2})^2}
\end{aligned}$$

and

$$\begin{aligned}
f(t) - f(-t) &= \frac{t}{e^t - 1} - \frac{-t}{e^{-t} - 1} \\
&= \frac{t(e^{-t} - 1) + t(e^t - 1)}{(e^t - 1)(e^{-t} - 1)} \\
&= \frac{t(e^t - 2 + e^{-t})}{-e^t + 2 - e^{-t}} \\
&= -t.
\end{aligned}$$

Thus we can write

$$\frac{t}{e^t - 1} = \frac{t(e^t - e^{-t})}{2(e^{t/2} - e^{-t/2})^2} + \frac{-t}{2}$$

where the first function is even and the second is odd. Since the first function is even its power series will only involve even powers of t; we conclude that the only odd term in the power series for $\frac{t}{e^t-1}$ is $-\frac{t}{2}$, and thus that $B_n = 0$ for n odd and > 1.

Solution 5.5. We have

$$\begin{aligned}
e^t &= \sum_{n=0}^{\infty} \frac{t^n}{n!} \\
e^t - 1 &= \sum_{n=1}^{\infty} \frac{t^n}{n!} \\
\frac{e^{t-1} - 1}{t} &= \sum_{n=0}^{\infty} \frac{t^n}{(n+1)!}.
\end{aligned}$$

Thus

$$\begin{aligned}
\left(\frac{e^t - 1}{t}\right)\left(\frac{t}{e^t - 1}\right) &= 1 \\
\left(\sum_{i=0}^{\infty} \frac{t^i}{(i+1)!}\right)\left(\sum_{j=0}^{\infty} B_j \frac{t^j}{j!}\right) &= 1 \\
\sum_{i=0}^{\infty}\sum_{j=0}^{\infty} B_j \frac{t^{i+j}}{(i+1)!j!} &= 1.
\end{aligned}$$

Grouping together the terms of degree n, we find that

$$\sum_{n=0}^{\infty}\left(\sum_{k=0}^{n} B_k \frac{1}{(n-k+1)!k!}\right) t^n = 1.$$

Equating coefficients of t^{n-1} for $n > 1$ gives

$$\sum_{k=0}^{n-1} B_k \frac{1}{(n-k)!k!} = 0.$$

Multiplying by $n!$ now yields the formula

$$\sum_{k=0}^{n-1} B_k \binom{n}{k} = 0,$$

as desired.

The fact that each B_k is rational follows from this formula by an easy induction, using the fact that $B_0 = 1$ and $B_1 = -\frac{1}{2}$ are both rational for the base case.

SOLUTION 5.6. Recall that

$$\begin{aligned}\cos(x) &= \frac{e^{ix} + e^{-ix}}{2} \\ \sin(x) &= \frac{e^{ix} - e^{-ix}}{2i}.\end{aligned}$$

Now, by the solution to Exercise 5.4 we have

$$\sum_{n=0}^{\infty} B_{2n} \frac{t^{2n}}{(2n)!} = \frac{t(e^t - e^{-t})}{2(e^{t/2} - e^{-t/2})^2}.$$

Replacing the exponentials by sines gives

$$\sum_{n=0}^{\infty} B_{2n} \frac{t^{2n}}{(2n)!} = \frac{2it \sin(-it)}{-8 \sin^2(-it/2)}.$$

The double angle formula now yields

$$\begin{aligned}\sum_{n=0}^{\infty} B_{2n} \frac{t^{2n}}{(2n)!} &= \frac{2it2 \cos(-it/2) \sin(-it/2)}{-8 \sin^2(-it/2)} \\ &= \frac{-it \cos(-it/2)}{2 \sin(-it/2)} \\ &= \frac{-it}{2} \cot(-it/2).\end{aligned}$$

Now, setting $s = -it/2$, we find that

$$\begin{aligned}\sum_{n=0}^{\infty} B_{2n} \frac{(2is)^{2n}}{(2n)!} &= s \cot(s) \\ \sum_{n=0}^{\infty} (-1)^n \frac{2^{2n} B_{2n}}{(2n)!} s^{2n} &= s \cot(s)\end{aligned}$$

as claimed.

SOLUTION 5.7. Taking logarithms of the formula

$$\sin t = t \prod_{k=1}^{\infty} \left(1 - \frac{t^2}{(k\pi)^2}\right)$$

yields

$$\log \sin t = \log t + \sum_{k=1}^{\infty} \log \left(1 - \frac{t^2}{(k\pi)^2}\right).$$

Differentiating now yields

$$\begin{aligned}\frac{\cos t}{\sin t} &= \frac{1}{t} + \sum_{k=1}^{\infty} \frac{\frac{-2t}{(k\pi)^2}}{1 - \frac{t^2}{(k\pi)^2}} \\ \cot t &= \frac{1}{t} - 2t \sum_{k=1}^{\infty} \frac{1}{(k\pi)^2 - t^2} \\ &= \frac{1}{t} + 2t \sum_{k=1}^{\infty} \frac{1}{t^2 - k^2\pi^2}.\end{aligned}$$

SOLUTION 5.8. Using the formula of Exercise 5.6 we have

$$\pi t \cot(\pi t) = \sum_{n=0}^{\infty} (-1)^n \frac{2^{2n} B_{2n}}{(2n)!} (\pi t)^{2n} = \sum_{n=0}^{\infty} (-1)^n \frac{2^{2n} \pi^{2n} B_{2n}}{(2n)!} t^{2n}.$$

On the other hand, the formula of Exercise 5.7 yields

$$\begin{aligned}t \cot t &= 1 + 2t^2 \sum_{k=1}^{\infty} \frac{1}{t^2 - k^2\pi^2} \\ \pi t \cot(\pi t) &= 1 + 2\pi^2 t^2 \sum_{k=1}^{\infty} \frac{1}{\pi^2 t^2 - k^2 \pi^2} \\ &= 1 + 2t^2 \sum_{k=1}^{\infty} \frac{1}{t^2 - k^2} \\ &= 1 - 2 \sum_{k=1}^{\infty} \frac{t^2}{k^2} \frac{1}{1 - (t/k)^2}.\end{aligned}$$

Expanding the term inside the sum as a geometric series yields

$$\begin{aligned}\pi t \cot(\pi t) &= 1 - 2 \sum_{k=1}^{\infty} \frac{t^2}{k^2} \sum_{n=0}^{\infty} \left(\frac{t}{k}\right)^{2n} \\ &= 1 - 2 \sum_{k=1}^{\infty} \sum_{n=1}^{\infty} \left(\frac{t}{k}\right)^{2n} \\ &= 1 - 2 \sum_{n=1}^{\infty} \sum_{k=1}^{\infty} \frac{1}{k^{2n}} t^{2n} \\ &= 1 - 2 \sum_{n=1}^{\infty} \zeta(2n) t^{2n}.\end{aligned}$$

Equating coefficients of t^{2n} in our two power series for $\pi t \cot(\pi t)$ yields

$$\begin{aligned}-2\zeta(2n) &= (-1)^n \frac{2^{2n} B_{2n} \pi^{2n}}{(2n)!} \\ \zeta(2n) &= (-1)^{n-1} \frac{2^{2n} B_{2n}}{2(2n)!} \pi^{2n}\end{aligned}$$

SOLUTION 5.9. We show that $\lim_{s\to\infty} \zeta(s) = 1$, which together with Exercise 5.8 will prove the first limit. For this, we group the sum in the zeta function as

$$\zeta(s) = 1 + \left(\frac{1}{2^s} + \frac{1}{3^s}\right) + \left(\frac{1}{4^s} + \cdots + \frac{1}{7^s}\right) + \left(\frac{1}{8^s} + \cdots + \frac{1}{15^s}\right) + \cdots$$

where each block has twice as many terms as the previous block. We find that

$$\begin{aligned} \frac{1}{2^s} + \frac{1}{3^s} &\leq \frac{2}{2^s} \\ \frac{1}{4^s} + \cdots + \frac{1}{7^s} &\leq \frac{4}{4^s} \\ \frac{1}{8^s} + \cdots + \frac{1}{15^s} &\leq \frac{8}{8^s} \end{aligned}$$

and so on. Thus

$$\zeta(s) \leq 1 + \frac{1}{2^{s-1}} + \frac{1}{4^{s-1}} + \frac{1}{8^{s-1}} + \cdots .$$

This is a geometric series with ratio 2^{1-s}, so this yields

$$\zeta(s) \leq \frac{1}{1 - 2^{1-s}}.$$

As $s \to \infty$ the right hand side clearly approaches 1. Since $1 \leq \zeta(s)$ for all $s > 1$, this shows that

$$\lim_{s\to\infty} \zeta(s) = 1.$$

For the second limit, it will suffice to show that

$$\lim_{n\to\infty} \frac{2^{2n-1}\pi^{2n}}{(2n-1)!} = 0,$$

as this and the first limit imply that we must have

$$\lim_{n\to\infty} \left|\frac{B_{2n}}{2n}\right| = \infty.$$

That the remaining limit approaches 0 can be seen in many ways; for example, writing the n^{th} term as

$$\pi \frac{2\pi}{1}\frac{2\pi}{2}\frac{2\pi}{3}\cdots\frac{2\pi}{2n-2}\frac{2\pi}{2n-1}$$

makes it quite clear that the limit is 0.

Bibliography

1. Thomas Apostol, *An introduction to analytic number theory*, Springer-Verlag, New York, 1976.
2. Michael Artin, *Algebra*, Prentice Hall, Englewood Cliffs, NJ, 1991.
3. Ian Cassels, *Global fields*, Algebraic number fields, Academic Press, 1967, pp. 42–84.
4. Ian Cassels and A. Frohlich (eds.), *Algebraic number fields*, Academic Press, London, 1967.
5. Henri Cohen, *A course in computational algebraic number theory*, Springer-Verlag, New York, 1993.
6. Keith Conrad, *Math 250a, solution set 4*, Harvard University, Fall, 1996.
7. David Cox, *Primes of the form* $x^2 + ny^2$, John Wiley and sons, New York, 1989.
8. Harold Edwards, *Fermat's last theorem*, Springer-Verlag, New York, 1977.
9. Jody Esmonde and Ram Murty, *Problems in algebraic number theory*, Springer-Verlag, New York, 1999.
10. Kenneth Ireland and Michael Rosen, *A classical introduction to modern number theory*, Springer-Verlag, New York, 1984.
11. Serge Lang, *Algebraic number theory*, Springer-Verlag, New York, 1986.
12. ______, *Cyclotomic fields I and II*, Springer-Verlag, New York, 1990.
13. ______, *Algebra*, Addison-Wesley, Reading, Massachusetts, 1993.
14. Daniel Marcus, *Number fields*, Springer-Verlag, New York, 1977.
15. Pierre Samuel, *Algebraic theory of numbers*, Kershaw Publishing Company, London, 1970.
16. Jean-Pierre Serre, *Local fields*, Springer-Verlag, New York, 1967.
17. ______, *A course in arithmetic*, Springer-Verlag, New York, 1973.
18. Joseph Silverman, *Advanced topics in the arithmetic of elliptic curves*, Springer-Verlag, New York, 1994.
19. Ian Stewart and David Tall, *Algebraic number theory*, Chapman and Hall, London, 1987.
20. Lawrence Washington, *Introduction to cyclotomic fields*, Springer-Verlag, New York, 1997.