A conversational introduction to algebraic number theory: Arithmetic beyond $\mathbb{Z}$

Paul Pollack

Department of Mathematics, Boyd Graduate Studies Research Center, University of Georgia, Athens, GA 30602

E-mail address: pollack@uga.edu

Contents

Preface

In a 1918 monograph, Edmund Landau refers to the theory of algebraic numbers as the prettiest part ("schönster Teil") of all of number theory.[1] This is an astonishing remark, coming as it does from a mathematician remembered primarily for his groundbreaking contributions to *analytic* number theory. This book is intended for those looking to quickly acquire a working knowledge of the subject for which Landau held so much admiration.

As far as prerequisites, it is assumed that the reader is familiar with linear algebra, commutative ring theory, Galois theory, and a little abelian group theory. (Most of the needed algebra can be found, for instance, in Chapters 1–12, + 14, of Hungerford's very readable *Abstract Algebra: An Introduction*, 3rd ed.) The theory of free abelian groups of finite rank is developed as needed. Acquaintance with elementary number theory up to and including the law of quadratic reciprocity is also expected. Many senior level math majors and beginning graduate students will meet these requirements, and I believe they will find the text quite approachable.

One special feature of this book is that the entire theory is developed first in the simple setting of quadratic fields; this includes full proofs of the three standard "core" theorems (the fundamental theorem of ideal theory, the finiteness of the class group, and the units theorem). All of this is done in the first third of the book. In Chapter 13, we wipe the slate clean and start over with number fields of arbitrary degree. At that point, the reader already knows (much of) what they should be trying to prove and is amply motivated to continue.

---

[1] see the Vorwort in: Landau, E. *Einführung in die Elementare und Analytische Theorie der Algebraischen Zahlen und der Ideale.* B. G. Teubner, Leipzig and Berlin, 1964.

Our leisurely pace makes it possible to consider a number of topics rarely treated in introductory texts. For instance, we discuss at length the **elasticity** of number rings, which is a precise way of measuring the failure of unique factorization. We devote a chapter to the **criterion of Frobenius–Rabinowitsch**, connecting prime values of special quadratic polynomials with unique factorization in imaginary quadratic number rings. In a series of exercises, we outline a proof that the equation $X^3 + DY^3 = 1$ (with D not a cube) always has at most one integer solution with $XY \neq 0$ (a weak version of the **Delone–Nagell theorem**). And in the final chapter, we describe some amazing connections — rooted in **Dirichlet's class number formula** — between the distribution of quadratic residues and nonresidues modulo an odd prime q and the arithmetic of the field $\mathbb{Q}(\sqrt{(-1)^{(q-1)/2}q})$.

This book grew out of my notes for a one-semester graduate course on algebraic number theory at the University of Georgia. (The final product ended up covering both a bit more and a bit less.) I have taken pains to preserve the conversational tone of the original lectures. As such, the book should be well-suited for self-study. But there is certainly more than enough here for a semester-long course at the senior undergraduate level. The book could also be used for an introductory graduate course, but advanced topics typically found in such a course (such as connections with commutative algebra, the theory of relative extensions of number fields, inertia and decomposition groups, and local theory) would have to be brought in from another source. I hope this is not seen as a serious impediment; anyone planning to continue on in number theory should learn to consult multiple references as a matter of course.

Acknowledgments. I would like to thank the many devoted teachers and mentors that have taken me under their wings over the years, especially Dan Phelon, Sharon Bellak, Jeff Miller, Noah Snyder, Dan Shapiro, Arnold Ross, Andrew Granville, Matt Baker, and Carl Pomerance. This book would not have been possible without them.

My own first exposure to algebraic number theory came in the form of online lecture notes by Robin J. Chapman, around 1999.[2] In

[2]These notes are still available; see `https://empslocal.ex.ac.uk/people/staff/rjchapma/courses/teach.html`.

the intervening years, I have continued to benefit from the generosity of mathematicians willing to freely share the fruits of their expository efforts. Particularly deserving of mention are Pete L. Clark[3] and Keith Conrad.[4] Pete is a colleague here at UGA, and it has been — and continues to be — a privilege to discuss mathematics with him in person.

I am very much indebted to Enrique Treviño for reading through the manuscript and pointing out a number of errors as well as places where the writing could be clearer.

Finally, I am grateful for the support of the National Science Foundation under award DMS-1402268.

Paul Pollack

[3] http://math.uga.edu/~pete/expositions2012.html
[4] http://www.math.uconn.edu/~kconrad/blurbs/

1

Getting our feet wet

Loosely speaking, algebraic number theory is the study of arithmetic in finite extensions of $\mathbb{Q}$. As motivation for undertaking this study, we begin with some examples illustrating how simpleminded questions about integers lead naturally to questions about arithmetic in larger number systems.

A warm-up

Problem 1.1. Find all integers x and y satisfying $y^2 = x^3 + x$.

Solution. Clearly, $x = 0$, $y = 0$ is a solution. We claim that there are no others. Suppose that there is a solution with $x \neq 0$. Rewrite the equation as

$$y^2 = x(x^2 + 1).$$

Since x and $x^2 + 1$ are relatively prime, every prime appearing in the factorization of x occurs to an even power, and similarly for $x^2 + 1$. Hence,

$$x = \pm\square \quad \text{and} \quad x^2 + 1 = \pm\square.$$

Since $x^2 + 1 > 0$, the $+$ sign holds in the second equation. Thus, x^2 and $x^2 + 1$ are positive integer squares with difference 1. But distinct positive integer squares differ by at least $4 - 1 = 3$. $\square$

An example of Fermat

> Can one find in whole numbers a square different from 25 that, when increased by 2, becomes a cube?

> This would seem at first to be difficult to discuss; and yet, I can prove by a rigorous demonstration that 25 is the only integer square that is less than a cube by two units. – P. de Fermat, marginal note in his copy of Diophantus's *Arithmetica*

Problem 1.2. Find all integers x and y satisfying $y^2 = x^3 - 2$.

In the quoted paragraph, Fermat is claiming that there are no solutions other than $x = 3, y = \pm 5$. The first surviving proof is Euler's. Euler's key insight is that one should work not over $\mathbb{Z}$ but over a larger ring[1], specifically the subring $\mathbb{Z}[\sqrt{-2}]$ of the complex numbers. (It is not important for this discussion which complex square root of -2 is denoted by the symbol $\sqrt{-2}$.) Note that over $\mathbb{Z}[\sqrt{-2}]$, Fermat's equation takes the form

$$x^3 = (y + \sqrt{-2})(y - \sqrt{-2}). \tag{1.1}$$

Definition 1.3. For $\alpha \in \mathbb{Z}[\sqrt{-2}]$, we define $N\alpha$ (the **norm** of α) by $N\alpha = \alpha\bar{\alpha}$, where $\bar{\cdot}$ denotes complex conjugation.

In other words, $N\alpha = |\alpha|^2$, where $|\alpha|$ is the usual complex absolute value.

Lemma 1.4. Let $\alpha, \beta \in \mathbb{Z}[\sqrt{-2}]$.

(a) $N(\alpha\beta) = N\alpha \cdot N\beta$,

(b) $N\alpha$ is a nonnegative integer, and $N\alpha = 0 \Leftrightarrow \alpha = 0$.

(c) $N\alpha = 1 \Longleftrightarrow \alpha$ is a unit in $\mathbb{Z}[\sqrt{-2}]$.

Proof. Part (a) is clear from the corresponding property of the complex absolute value. Writing $\alpha = a + b\sqrt{-2}$, with $a, b \in \mathbb{Z}$, we have $N(\alpha) = a^2 + 2b^2$; this makes (b) obvious. Turning to (c), if α is a unit, then $\alpha\beta = 1$ for some $\beta \in \mathbb{Z}[\sqrt{-2}]$; taking norms and applying the result of (a), we see $N\alpha \cdot N\beta = 1$. Keeping (b) in mind, we have $N\alpha = 1$ (and $N\beta = 1$). On the other hand, if $N\alpha = 1$, then α has an obvious inverse in $\mathbb{Z}[\sqrt{-2}]$, namely $\bar{\alpha}$. □

[1]Unless otherwise specified, the term **ring** in this book always refers to a commutative ring with 1.

The only solutions to $a^2 + 2b^2 = 1$ are $a = \pm 1, b = 0$. Hence, $U(\mathbb{Z}[\sqrt{-2}]) = \{\pm 1\}$.

Proof that $x = 3$, $y = \pm 5$. In any solution (x, y), the integer x is odd, since otherwise $y^2 \equiv 2 \pmod 4$. Thus, y is also odd. We claim that the right-hand factors in (1.1) have no nonunit common divisor. Indeed, if α is a common factor, Lemma 1.4(a) implies that

$$N\alpha \mid y^2 + 2.$$

Since y is odd, we see that $N\alpha$ is also odd. On the other hand, since α divides $(y + \sqrt{-2}) - (y - \sqrt{-2}) = 2\sqrt{2}$,

$$N\alpha \mid N(2\sqrt{-2}) = 8.$$

Thus, $N\alpha = 1$, and so α is a unit, as claimed.

The prime factorization argument from Problem #1 now shows that both right-hand factors in (1.1) are cubes, up to multiplication by a unit of $\mathbb{Z}[\sqrt{-2}]$. Now the only units are ± 1, and these can be absorbed into the cubes. Thus, there are $a, b \in \mathbb{Z}$ with

$$\begin{aligned} y + \sqrt{-2} &= (a + b\sqrt{-2})^3 \\ &= (a^3 - 6ab^2) + (3a^2b - 2b^3)\sqrt{-2}. \end{aligned}$$

Comparing imaginary parts, $b(3a^2 - 2b^2) = 1$, and so $b = \pm 1$. If $b = 1$, then $3a^2 - 2 = 1$, so that $a = \pm 1$. If $b = -1$, then $-3a^2 + 2 = 1$, which has no solution. So $b = 1, a = \pm 1$, and

$$y + \sqrt{-2} = (\pm 1 + \sqrt{-2})^3 = (\pm 5 + \sqrt{-2}).$$

Thus, $y = \pm 5$, and hence $x = 3$. □

A cautionary tale

Problem 1.5. Find all integers x and y satisfying $y^2 = x^3 - 26$.

"Solution". We imitate the above argument, working in $\mathbb{Z}[\sqrt{-26}]$ instead of $\mathbb{Z}[\sqrt{-2}]$. In this case, x and y satisfy

$$x^3 = (y + \sqrt{-26})(y - \sqrt{-26}).$$

Arguing as above, the right-hand factors share no nonunit divisors in $\mathbb{Z}[\sqrt{-26}]$. The only units in $\mathbb{Z}[\sqrt{-26}]$ are the cubes ± 1, and so there are integers a, b with

$$y + \sqrt{-26} = (a + b\sqrt{-26})^3.$$

Proceeding as above gives $a = \pm 3$, $b = 1$, and $y = \pm 207$. Plugging this back into the original equation, $x = 35$. So the integer solutions are $(35, \pm 207)$. □

Something is rotten in the state of Denmark: Our "proof" misses the two obvious solutions $(3, \pm 1)$!

What went wrong? In both this argument and the last, we appealed to a "prime factorization argument" to justify the following claim when $n = 3$:

nth power product principle. If α, β are nonzero elements whose product is an nth power, and α and β have no nonunit common divisor, then both α and β are nth powers, up to multiplication by a unit.

This principle has a transparent proof (for all n) in a unique factorization domain. And we will see later that $\mathbb{Z}[\sqrt{-2}]$ is a UFD. Thus, our solution to Fermat's equation is "correct", just incomplete (for now). We are not so lucky for $\mathbb{Z}[\sqrt{-26}]$. In this ring,

$$3 \cdot 3 \cdot 3 = (1 + \sqrt{-26})(1 - \sqrt{-26}),$$

and all of the elements involved in both the left and right-hand products are irreducible. (One can argue this using norms.) Hence, these two factorizations of 27 are irreconcilably distinct. Moreover, this equation shows directly that the power product principle fails in $\mathbb{Z}[\sqrt{-26}]$ for $n = 3$.

The moral here is that innocent-seeming questions about integers lead naturally to the study of factorization problems in certain overrings of $\mathbb{Z}$. We will spend a good deal of time investigating these problems, which quickly exhibit features rendering them interesting for their own sake.

A parting shot

Problem 1.6. Find all integers x and y satisfying $y^2 = x^3 + 1$.

The obvious solutions are $(-1, 0)$, $(0, \pm 1)$, and (the much more interesting) $(2, 3)$.

Are these all of them? Following our nose, we rewrite the equation in the form

$$(y - 1)(y + 1) = x^3.$$

If y is even, then $y - 1$ and $y + 1$ are nonzero and relatively prime; since their product is a cube (and since $\mathbb{Z}$ is a UFD!), both are cubes. But the only pair of integer cubes that differ by 2 are -1 and 1; hence, $y = 0$ and $x = -1$. Now suppose that y is odd. Then x is even, and

$$\frac{y-1}{2} \cdot \frac{y+1}{2} = 2 \cdot \left(\frac{x}{2}\right)^3.$$

The left-hand factors differ by 1 and so are coprime. Thinking about prime factorizations, one of $\frac{y-1}{2}$, $\frac{y+1}{2}$ is a cube while the other is twice a cube. (This holds even in the degenerate case where one of the left-hand factors vanishes.) Thus, we obtain a solution in integers X, Y to

$$X^3 - 2Y^3 = \pm 1.$$

Using the classification of units in the ring $\mathbb{Z}[\sqrt[3]{2}]$, we will show in Chapter 19 that the only integer solutions (X, Y) to this last equation are $(\pm 1, 0)$ and $(\pm 1, \pm 1)$ (with the same choice of sign in both coordinates). Working backwards through the analysis, one finds that all solutions to $y^2 = x^3 + 1$ belong to our initial list of "obvious" solutions.

The first proof of this result was given by Euler, by different methods. In fact, Euler showed that these "obvious solutions" comprise all of the *rational* points on the curve $y^2 = x^3 + 1$![2]

[2]For a lucid account of Euler's proof, see: Oesterlé, J. *On a Theorem of Euler.* Mathematics Newsletter, Ramanujan Mathematical Society **19**, no. 2 (2010), 5–6.

Exercises

(1) A *primitive Pythagorean triple* is a triple of positive integers (a, b, c) with $a^2 + b^2 = c^2$.
   (a) Show that if (a, b, c) is a primitive Pythagorean triple, then $a - bi$ and $a + bi$ have no common nonunit factors in $\mathbb{Z}[i]$.
   (b) Show that $U(\mathbb{Z}[i]) = \{\pm 1, \pm i\}$.
   (c) Show that, after possibly swapping a and b, there are coprime positive integers m and n of opposite parity with $m > n$ and

$$a = m^2 - n^2, \quad b = 2mn, \quad c = m^2 + n^2.$$

(2) (V. A. Lebesgue[3]) Let p be an odd prime. In this exercise, we outline a proof that there are no nonzero integer solutions to $y^2 = x^p - 1$.

Seeking a contradiction, suppose that (x, y) is an integer solution with $xy \neq 0$.
   (a) Show that x is odd and y is even.
   (b) By comparing imaginary parts in the equation $y + i = (a + bi)^p$, prove that $\sum_{k \geq 0} \binom{p}{2k} (-a^2)^k = \pm 1$. By looking modulo 4, show that the + sign holds. Conclude that $\sum_{k \geq 1} \binom{p}{2k} (-a^2)^k = 0$.
   (c) Let v be the exponent on 2 appearing in the prime factorization of $\binom{p}{2} a^2$. Show that

$$2^{v+1} \mid \binom{p}{2k} (-a^2)^k$$

   for every integer $k > 1$.
   (d) Using the result of (c), show that

$$2^{v+1} \nmid \sum_{k \geq 1} \binom{p}{2k} (-a^2)^k,$$

   contradicting the conclusion of (b).

(3) (Lunnon[4], Marshall and Perlis[5]) Let S be a finite subset of $\mathbb{R}^2$. Suppose that (1) every point of S has rational coordinates and (2) the squared distance between any two points of S is an integer.

---

[3] Lebesgue, V. A. *Sur l'impossibilité, en nombres entiers, de l'équation* $x^m = y^2 + 1$. Nouvelle Ann. de Math. **9** (1850), 178–181.

[4] Lunnon, W. F. *Lattice embedding of Heronian simplices* (2012), available at `http://arxiv.org/abs/1202.3198`.

[5] Marshall, S. H.; Perlis, A. R. *Heronian tetrahedra are lattice tetrahedra.* Amer. Math. Monthly **120** (2013), no. 2, 140–149.

The following argument, based on uniqueness of factorization in $\mathbb{Z}[i]$, shows that S can be carried to a subset of $\mathbb{Z}^2$ by a Euclidean motion — in fact, by a translation followed by a rotation. Supply the proofs of the underlined statements.

Proof sketch. It is enough to show that if S is a finite set of points satisfying (1) and (2) and containing the origin, then there is a rotation carrying S into $\mathbb{Z}^2$.

Making the usual identification of $\mathbb{R}^2$ with $\mathbb{C}$ identifies the points of S with elements of $\mathbb{Q}[i]$, say $0 = \gamma_0, \gamma_1, \ldots, \gamma_n$. Since $\mathbb{Q}[i]$ is the quotient field of the unique factorization domain $\mathbb{Z}[i]$, we can write each γ_i, for $i = 1, 2, \ldots, n$, in the form α_i/β_i where $\alpha_i, \beta_i \in \mathbb{Z}[i]$ and α_i is relatively prime to β_i. Here α_i and β_i are uniquely determined up to unit factors. If all $\gamma_i \in \mathbb{Z}[i]$, then $S \subseteq \mathbb{Z}^2$ already. Otherwise, some β_i is not a unit of $\mathbb{Z}[i]$, and so we may decompose $\beta_1 \cdots \beta_n$ as a nonempty product of irreducible elements of $\mathbb{Z}[i]$, say

$$\prod_{i=1}^{n} \beta_i = \pi_1 \cdots \pi_K.$$

We refer to the positive integer K as the *complexity* of S.

Write $\pi = \pi_1$. Reordering $\gamma_1, \ldots, \gamma_n$ if necessary, we can assume $\pi \mid \beta_1$. Since the squared distance from γ_0 to γ_1 is an integer,

$$N(\alpha_1)/N(\beta_1) = N(\gamma_1) = N(\gamma_1 - \gamma_0) \in \mathbb{Z},$$

and so

$$N(\pi) \mid N(\beta_1) \mid N(\alpha_1).$$

This implies that $\bar{\pi} \mid \alpha_1$. Moreover, for each $i \in \{2, 3, \ldots, n\}$, the relation $N(\gamma_i - \gamma_1) \in \mathbb{Z}$ implies that $\bar{\pi} \mid \alpha_i$ or $\pi \mid \beta_i$.

We multiply each element of S by $\frac{\pi}{\bar{\pi}}$ to obtain a new point set S'. Since $\frac{\pi}{\bar{\pi}}$ lies on the unit circle, multiplication by $\frac{\pi}{\bar{\pi}}$ corresponds to a rotation. Now start the argument over with S' replacing S. Either $S' \subseteq \mathbb{Z}^2$ or the complexity of S' is smaller than that of S. Thus, continuing the process, we reach a subset of $\mathbb{Z}^2$ within a finite number of iterations. □

2
Cast of characters

In this section, we define the fundamental objects of interest in algebraic number theory — number fields and their associated rings of algebraic integers — and establish their basic properties.

Number fields

Definition 2.1. A **number field** is a subfield K of the complex numbers satisfying $[K : \mathbb{Q}] < \infty$.

For example, $\mathbb{Q}$, $\mathbb{Q}(\sqrt{2}, \sqrt{3})$, $\mathbb{Q}(\sqrt[17]{2})$, and $\mathbb{Q}(\theta)$, where θ is a complex root of $x^5 + x + 1 = 0$, are all number fields. Their respective degrees over $\mathbb{Q}$ are $1, 4, 17$, and 5.

Definition 2.1 is slightly unconventional. Typically, any finite degree extension field of $\mathbb{Q}$ counts as a number field; e.g., the "abstract quotient" $\mathbb{Q}[x]/\langle x^3 - 2\rangle$ is included. Our restriction to subfields of $\mathbb{C}$ is a mild convenience that entails no loss of generality:

Proposition 2.2. Let K be any field of finite degree n over $\mathbb{Q}$. Then K embeds into the complex numbers; in fact, there are precisely n field embeddings of K into $\mathbb{C}$.

Proof. Since $\mathbb{Q}$ is a perfect field (i.e., all finite extensions are separable), the primitive element theorem may be applied to the extension $K/\mathbb{Q}$: There is some $\alpha \in K$ with $K = \mathbb{Q}(\alpha)$. Let $\min_\alpha(x) \in \mathbb{Q}[x]$ denote the minimal polynomial of α over $\mathbb{Q}$. Over $\mathbb{C}$,

$$\min_\alpha(x) = (x - \alpha_1)(x - \alpha_2) \cdots (x - \alpha_n)$$

for distinct complex numbers $\alpha_1, \ldots, \alpha_n$. Since

$$K = \mathbb{Q}(\alpha) = \mathbb{Q}[\alpha],$$

each element of K can be written in the form $g(\alpha)$, where $g(x) \in \mathbb{Q}[x]$ is uniquely determined modulo $\min_\alpha(x)$. It is now straightforward to check that the n maps

$$\sigma_i : K \to \mathbb{C}$$
$$g(\alpha) \mapsto g(\alpha_i)$$

(for $i = 1, 2, \ldots, n$) are well-defined and serve to embed K into $\mathbb{C}$. Finally, these are all of the embeddings of K into $\mathbb{C}$; each embedding σ is determined by where it sends α, and $\min_\alpha(\sigma(\alpha)) = \sigma(\min_\alpha(\alpha)) = \sigma(0) = 0$, so that $\sigma(\alpha) = \alpha_i$ for some $i = 1, 2, \ldots, n$. □

Embeddings, real and otherwise

Let K be a number field. A field embedding $\sigma : K \hookrightarrow \mathbb{C}$ is called **real** when $\sigma(K) \subseteq \mathbb{R}$ and **nonreal** otherwise. The nonreal embeddings naturally come in pairs, since postcomposing a nonreal embedding with complex conjugation gives a different nonreal embedding. It is usual to write r_1 for the number of real embeddings and r_2 for the number of pairs of nonreal embeddings, so that

$$r_1 + 2r_2 = [K : \mathbb{Q}].$$

Will the real integers please stand up?

Let K be a number field. Every field has a trivial factorization theory, in the sense that every element divides every other. To obtain interesting arithmetic, we we will work in a subring $\mathbb{Z}_K$ of K, the **ring of algebraic integers of** K, chosen to complete the analogy

$$\mathbb{Q} : \mathbb{Z} \quad :: \quad K : \mathbb{Z}_K.$$

In this chapter, we give Dedekind's definition of $\mathbb{Z}_K$. The congenial arithmetic properties of $\mathbb{Z}_K$ will be explored in subsequent chapters.

Before we can discuss algebraic integers, we should discuss algebraic numbers.

Definition 2.3. An **algebraic number** is a complex number that is algebraic over $\mathbb{Q}$ (i.e., the root of a nonconstant polynomial in $\mathbb{Q}[x]$). The set of all algebraic numbers is denoted by $\bar{\mathbb{Q}}$.

From the elementary theory of field extensions,

$$\bar{\mathbb{Q}} = \{\alpha \in \mathbb{C} : [\mathbb{Q}(\alpha) : \mathbb{Q}] < \infty\}.$$

This description of $\bar{\mathbb{Q}}$ makes it obvious that $\bar{\mathbb{Q}}$ is a subfield of $\mathbb{C}$ (since $[\mathbb{Q}(\alpha, \beta) : \mathbb{Q}] \leq [\mathbb{Q}(\alpha) : \mathbb{Q}][\mathbb{Q}(\beta) : \mathbb{Q}]$). It is also clear that every number field is a subfield of $\bar{\mathbb{Q}}$.

Definition 2.4. An **algebraic integer** is a complex number that is the root of a monic polynomial in $\mathbb{Z}[x]$. We let

$$\bar{\mathbb{Z}} = \{\text{complex algebraic integers}\}.$$

Let us check that $\bar{\mathbb{Z}}$ is in fact a subring of the complex numbers.

In the next lemma, the reader unacquainted with module theory should mentally replace the term "$\mathbb{Z}$-module" with its synonym "abelian group". The difference is purely psychological: "$\mathbb{Z}$-module" suggests we are thinking of our group as a "vector space over $\mathbb{Z}$".

Lemma 2.5 (Integrality criterion)**.** Let $\alpha \in \mathbb{C}$. Suppose that there is a finitely generated $\mathbb{Z}$-submodule $M \subseteq \mathbb{C}$ with $M \neq \{0\}$ and $\alpha M \subseteq M$. Then $\alpha \in \bar{\mathbb{Z}}$.

Proof. Suppose that $\beta_1, \ldots, \beta_n$ generate M as a $\mathbb{Z}$-module. Since $\alpha M \subseteq M$, each $\alpha\beta_i$ (for $i = 1, 2, \ldots, n$) is a $\mathbb{Z}$-linear combination of $\beta_1, \ldots, \beta_n$. Thus, there is an $n \times n$ integer matrix $C = (c_{ij})$ with

$$\alpha \begin{bmatrix} \beta_1 \\ \beta_2 \\ \vdots \\ \beta_n \end{bmatrix} = \begin{bmatrix} c_{1,1} & c_{1,2} & \cdots & c_{1,n} \\ c_{2,1} & c_{2,2} & \cdots & c_{2,n} \\ \vdots & \vdots & \ddots & \vdots \\ c_{n,1} & c_{n,2} & \cdots & c_{n,n} \end{bmatrix} \cdot \begin{bmatrix} \beta_1 \\ \beta_2 \\ \vdots \\ \beta_n \end{bmatrix}.$$

Since $M \neq \{0\}$, the β_i do not all vanish. Thus, α is an eigenvector of C, and hence a zero of the characteristic polynomial

$$p_C(x) = \det \begin{bmatrix} x - c_{1,1} & -c_{1,2} & \cdots & -c_{1,n} \\ -c_{2,1} & x - c_{2,2} & \cdots & -c_{2,n} \\ \vdots & \vdots & \ddots & \vdots \\ -c_{n,1} & -c_{n,2} & \cdots & x - c_{n,n} \end{bmatrix}.$$

Since C has integer entries, p_C is a monic polynomial with integer coefficients, and so $\alpha \in \bar{\mathbb{Z}}$. □

Proof that $\bar{\mathbb{Z}}$ is a ring. It suffices to show that $1 \in \bar{\mathbb{Z}}$ and that $\bar{\mathbb{Z}}$ is closed under subtraction and multiplication. The first of these is easy; in fact, it is obvious that $\mathbb{Z} \subseteq \bar{\mathbb{Z}}$, since n is a root of $x - n$. We move on to the closure conditions. Let $M = \mathbb{Z}[\alpha, \beta]$. M is a nonzero $\mathbb{Z}$-submodule of $\mathbb{C}$ with

$$(\alpha - \beta) \cdot M \subseteq M, \quad \text{and} \quad \alpha\beta \cdot M \subseteq M.$$

Thus, by Lemma 2.5, it is enough to prove that M is finitely generated. Let $f(x)$ and $g(x)$ be monic polynomials in $\mathbb{Z}[x]$ vanishing at α and β, respectively. Let $m = \deg f$ and $n = \deg g$. Let M' be the submodule of $\mathbb{Z}[\alpha, \beta]$ generated by the (finitely many!) elements

$$\alpha^i \beta^j, \quad \text{where} \quad 0 \leq i < m \text{ and } 0 \leq j < n.$$

We will show that $M = M'$. This is immediate once we know that each "monomial" $\alpha^I \beta^J$ (with $I, J \in \mathbb{Z}_{\geq 0}$) lies in M'. Since f and g are monic, long division of polynomials yields

$$x^I = f(x)q_1(x) + r_1(x), \quad x^J = g(x)q_2(x) + r_2(x)$$

for certain polynomials $q_i(x), r_i(x) \in \mathbb{Z}[x]$ with $\deg r_1 < m$ and $\deg r_2 < n$. Hence,

$$\alpha^I \beta^J = r_1(\alpha) r_2(\alpha);$$

the right-hand side is clearly in M'. □

Now that we have defined the ring of all algebraic integers, it is obvious how to define the ring of integers belonging to a particular number field.

Definition 2.6. Let K be a number field. The **ring of integers of** K (or **number ring associated to** K) is the ring

$$\mathbb{Z}_K := K \cap \bar{\mathbb{Z}}.$$

In other words, $\mathbb{Z}_K$ is the set of elements of K that are roots of monic polynomials with integer coefficients.

(So in a certain sense, $\bar{\mathbb{Z}}$ is the "one ring to rule them all".)

In general, given a number field K, determining $\mathbb{Z}_K$ is a nontrivial task (discussed in detail in Chapter 14). Luckily, we can at least easily check that $\mathbb{Z}_{\mathbb{Q}}$ is what it should be.

Proposition 2.7. $\mathbb{Z}_{\mathbb{Q}} = \mathbb{Z}$.

Proof. We have to show that if $\alpha \in \mathbb{Q}$ is the root of a monic polynomial with integer coefficients, then $\alpha \in \mathbb{Z}$. This follows immediately from the well-known **rational root theorem**: All rational roots of $a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0$ (where the $a_i \in \mathbb{Z}$, $a_n \neq 0$) have numerator dividing a_0 and denominator dividing a_n. In our case, $a_n = 1$, and so all rational roots are integers. □

We conclude by recording three results that will be needed later. The first allows us to determine whether α belongs to $\bar{\mathbb{Z}}$ from its minimal polynomial $\min_\alpha(x)$. (Here and elsewhere, the term "minimal polynomial" without further qualification refers to the minimal polynomial over the field $\mathbb{Q}$ of rational numbers.)

Proposition 2.8. If $\alpha \in \bar{\mathbb{Z}}$, then $\min_\alpha(x) \in \mathbb{Z}[x]$.

Of course, the converse of Proposition 2.8 holds trivially.

Proof. By hypothesis, there is a monic polynomial $f(x) \in \mathbb{Z}[x]$ for which $f(\alpha) = 0$. Thus, $\min_\alpha(x) \mid f(x)$. Hence, if we factor

$$\min_\alpha(x) = (x - \theta_1) \cdots (x - \theta_n),$$

then the θ_i are roots of f, and so are algebraic integers. Multiplying out the right-hand side, we see that the coefficients of $\min_\alpha(x)$ belong to $\bar{\mathbb{Z}}$, and hence also to $\mathbb{Q} \cap \bar{\mathbb{Z}} = \mathbb{Z}_{\mathbb{Q}} = \mathbb{Z}$. □

The next result can be thought of as asserting that $\mathbb{Z}_K$ is a "large" subring of K.

Proposition 2.9. $\mathbb{Z}_K$ has fraction field K. In fact, every element of K can be written in the form $\frac{1}{n}\alpha$, where $\alpha \in \mathbb{Z}_K$ and n is a positive integer.

Proof. It is enough to show that every $\beta \in K$ has a positive integer multiple belonging to $\bar{\mathbb{Z}}$. Clearing denominators from $\min_\beta(x)$, we obtain a nonconstant polynomial in $\mathbb{Z}[x]$ having β as a root, say $\sum_{j=0}^{d} a_j x^j$, where $a_d > 0$. Then

$$0 = a_d^{d-1} \cdot \sum_{j=0}^{d} a_j \beta^j = (a_d\beta)^d + \sum_{j=0}^{d-1} a_j a_d^{d-1-j} (a_d\beta)^j.$$

Hence, $a_d\beta$ is a root of

$$x^d + \sum_{j=0}^{d-1} a_j a_d^{d-1-j} x^j,$$

so that $a_d\beta \in \bar{\mathbb{Z}}$. □

Finally, we show that looking at roots of monic polynomials with algebraic integer coefficients does not give us anything new.

Theorem 2.10. If $\alpha \in \mathbb{C}$ is the root of a monic polynomial with coefficients in $\bar{\mathbb{Z}}[x]$, then $\alpha \in \bar{\mathbb{Z}}$.

Proof. Suppose that $f(\alpha) = 0$, where $f(x) = a_0 + a_1 x + \cdots + a_{n-1}x^{n-1} + x^n \in \bar{\mathbb{Z}}[x]$. Let $K = \mathbb{Q}(a_0, a_1, \ldots, a_{n-1})$, and let L be the Galois closure of K over $\mathbb{Q}$. For each $\sigma \in \mathrm{Gal}(L/\mathbb{Q})$ and each $g(x) \in L[x]$, let $(\sigma g)(x) \in L[x]$ denote the result of applying σ to each coefficient of g. Put $h(x) = \prod_{\sigma \in \mathrm{Gal}(L/\mathbb{Q})} \sigma f$, so that

$$h(x) = \prod_{\sigma \in \mathrm{Gal}(L/\mathbb{Q})} (\sigma(a_0) + \sigma(a_1)x + \cdots + \sigma(a_{n-1})x^{n-1} + x^n).$$

Clearly, h is a monic polynomial. Moreover, $f(x)$ is one of the factors in the right-hand product (corresponding to $\sigma = \mathrm{id}$.), and so $h(\alpha) =$

0. We now argue that $h(x) \in \mathbb{Z}[x]$, so that $\alpha \in \bar{\mathbb{Z}}$. For each $\tau \in \mathrm{Gal}(L/\mathbb{Q})$,

$$\tau h = \tau \left(\prod_{\sigma \in \mathrm{Gal}(L/\mathbb{Q})} \sigma f \right) = \left(\prod_{\sigma \in \mathrm{Gal}(L/\mathbb{Q})} (\tau\sigma) f \right) = h.$$

(As σ runs over the distinct elements of $\mathrm{Gal}(L/\mathbb{Q})$, so does $\tau\sigma$.) Thus, every coefficient of h is fixed by τ. Consequently, $h(x) \in \mathbb{Q}[x]$. On the other hand, each a_i is an algebraic integer, and thus all of the Galois conjugates $\sigma(a_i)$ are algebraic integers. Hence, $h(x) \in \bar{\mathbb{Z}}[x]$. Since $\mathbb{Q} \cap \bar{\mathbb{Z}} = \mathbb{Z}$, Theorem 2.10 follows. □

Exercises

(1) (Redheffer[1]) We say a nonempty set S of complex numbers is **closed under polynomial inversion** if, for every positive integer n and every $a_0, \ldots, a_n, w \in S$ with $a_n \neq 0$, there is a $z \in S$ with

$$a_n z^n + a_{n-1} z^{n-1} + \cdots + a_0 = w.$$

Show that if S is closed under polynomial inversion, then $S = \{0\}$ or S is an algebraically closed subfield of $\mathbb{C}$.

(2) The sum $1 + \sqrt{2} + \sqrt[3]{3} + \sqrt[4]{4} + \cdots + \sqrt[100]{100}$ lies strictly between 111 and 112. Knowing this, you can conclude immediately that the sum is irrational. Why?[2]

(3) Prove that every $\alpha \in \bar{\mathbb{Z}}$ admits a representation in the form $\alpha = \epsilon + \eta$, where $\epsilon, \eta \in U(\bar{\mathbb{Z}})$. *Hint:* Impose the additional constraint $\epsilon\eta = 1$.

(4) Let α be an algebraic integer. Show that the following are equivalent:
   (a) $\min_\alpha(0) = \pm 1$,
   (b) $\alpha \in U(\mathbb{Z}[\alpha])$,
   (c) $\alpha \in U(\bar{\mathbb{Z}})$.

---

[1] Redheffer, R. M. *Algebraic Numbers and a Point of View.* Amer. Math. Monthly **58** (1951), no. 6, 412–417.

[2] For a determination of the degree of $1 + \sqrt{2} + \sqrt[3]{3} + \cdots + \sqrt[n]{n}$ over $\mathbb{Q}$, see: Fried, E. *On linear combinations of roots.* (Hungarian) Magyar Tud. Akad. Mat. Fiz. Oszt. Közl. **3** (1954), 155–162.

Hint: To show that (c) ⇒ (a), express $\min_{1/\alpha}(x)$ in terms of $\min_{\alpha}(x)$.

(5) (Liouville[3]) Let α be a real algebraic number of degree $n \geq 2$. In this exercise, we prove the existence of a constant $A = A(\alpha) > 0$ for which the following holds: For every pair of integers p, q with $q > 0$,

$$\left| \frac{p}{q} - \alpha \right| \geq \frac{A}{q^n}. \tag{2.1}$$

Thus, an irrational algebraic number cannot get "too close" to a rational number.

Let $f(x)$ be the minimal polynomial of α, scaled by a positive integer factor to land in $\mathbb{Z}[x]$. Let $p, q \in \mathbb{Z}$ with $q > 0$.

(a) Show that $|f(p/q)| \geq 1/q^n$.

(b) Show that there is a ξ between $\frac{p}{q}$ and α with

$$f\left(\frac{p}{q}\right) = \left(\frac{p}{q} - \alpha\right) f'(\xi).$$

Hint: Mean value theorem.

(c) Let $B = \max_{\alpha-1 \leq \xi \leq \alpha+1} |f'(\xi)|$. Deduce from (a) and (b) that if $|\frac{p}{q} - \alpha| \leq 1$, then

$$B \cdot \left| \frac{p}{q} - \alpha \right| \geq \frac{1}{q^n}.$$

(d) Finish by proving (2.1) with $A = \min\{1/B, 1\}$.

Remark: For any irrational α, there are infinitely many solutions to $|p/q - \alpha| < 1/q^2$ (cf. Theorem 8.5). Thus, (2.1) is sharp when $n = 2$. But when $n \geq 3$, (2.1) can be strengthened substantially. In 1955, K.F. Roth showed that for each $\epsilon > 0$, the denominator q^n can be replaced with $q^{2+\epsilon}$, where the constant A now depends on both α and ϵ. For this result, which improved on a series of earlier estimates by Thue, Siegel, and Dyson, Roth was awarded the Fields Medal in 1958.

(6) (continuation) Let $L = \sum_{m=1}^{\infty} 10^{-m!}$. Show that L is not algebraic. A complex number that is not algebraic is called **transcendental**; L was one of the earliest known examples.

---

[3]Liouville, J. *Sur des classes très étendues de quantités dont la valeur n'est ni algébrique, ni même réductible à des irrationnelles algébriques.* J. Math. Pures Appl. **16** (1851), 133–142.

Hint: First, show that $L \notin \mathbb{Q}$. Then show that for each fixed $n \geq 2$, the partial sums of the defining series yield a sequence of p/q with $|p/q - L| \cdot q^n \to 0$. Thus, L is not algebraic of degree n.

(7) The following 1966 result of Alan Baker[4] subsumes several earlier theorems about transcendental numbers: *Let $\lambda_1, \ldots, \lambda_n$ be complex numbers with each $\exp(\lambda_i) \in \bar{\mathbb{Q}}$. If $\lambda_1, \ldots, \lambda_n$ are linearly independent over $\mathbb{Q}$, then the numbers $1, \lambda_1, \ldots, \lambda_n$ are linearly independent over $\bar{\mathbb{Q}}$.*

(a) Use Baker's theorem to show that $\log 2$, e, π, $\pi + \log 2$, e^π, and $2^{\sqrt{2}}$ are all transcendental.

(b) There are three real solutions to $x^2 = 2^x$, the obvious solutions $x = 2$ and $x = 4$, and the not-so-obvious solution $x = -0.76666\ldots$. Use Baker's theorem to prove that the last of these is transcendental.

(8) Let K be a number field admitting at least one real embedding, and let $\sigma_1, \ldots, \sigma_{r_1}$ be a list of the distinct real embeddings of K. For each nonzero $\alpha \in K$, define the **sign** of α as

$$(\operatorname{sgn} \sigma_1(\alpha), \ldots, \operatorname{sgn} \sigma_{r_1}(\alpha)) \in \{\pm 1\}^{r_1},$$

where sgn is the usual sign function on $\mathbb{R}$. Prove that all 2^{r_1} conceivable signs are taken on by some element of K.

Hint: It is enough to find elements having each of the r_1 signs $(1, \ldots, 1, -1, 1, \ldots, 1)$ (exactly one -1).

(9) Show that $\bar{\mathbb{Q}}$ admits a countable filtration by number fields. That is, there are number fields $K_1, K_2, K_3, \ldots$ with each $K_i \subseteq K_{i+1}$ and $\bigcup_{i=1}^{\infty} K_i = \bar{\mathbb{Q}}$.

(10) Let p be an odd prime. Show that

$$\sqrt[p]{\frac{1}{p}} + \sqrt[p]{\frac{2}{p}} + \cdots + \sqrt[p]{\frac{p-1}{p}} \in \bar{\mathbb{Z}}.$$

(11) (Trypanis[5]) Let p be a prime, and let a be a positive integer coprime to p. Show that for each nonnegative integer n,

$$a^{(p-1)/p^n} \equiv 1 \pmod{p^{1/p^n}},$$

[4] See Theorem 2.1 in: Baker, A. *Transcendental number theory.* 2nd edition. Cambridge Mathematical Library. Cambridge University Press, Cambridge, 1990.

[5] Trypanis, A. A. *An extension of Fermat's theorem.* Amer. Math. Monthly **57** (1950), 87–89.

where the congruence is being asserted in the ring $\bar{\mathbb{Z}}$.

3

Quadratic number fields: First steps

Over the course of the next several chapters, we will establish the core theorems of algebraic number theory when K is a **quadratic field**, meaning that $[K : \mathbb{Q}] = 2$. Most of the important features of the general theory are already visible in this special case, but the proofs are somewhat gentler on those meeting the subject for the first time.

The classification problem

In what follows, "$\sqrt{d}$" denotes $i\sqrt{|d|}$ when $d < 0$. (This choice is made only for definiteness of notation; it does not impact any results!)

Theorem 3.1. Every quadratic number field K has the form $\mathbb{Q}(\sqrt{d})$ for a unique squarefree integer d.

Proof of the existence half of Theorem 3.1. Let $\alpha \in \mathbb{C}$ be a primitive element for the extension $K/\mathbb{Q}$. Suitably scaling $\min_\alpha(x)$, we obtain a quadratic polynomial $Ax^2 + Bx + C$ having α as a root, with $A, B, C \in \mathbb{Z}$ and $A \neq 0$. Since $\alpha \notin \mathbb{Q}$, certainly $B^2 - 4AC \neq 0$. Let f be the largest positive integer for which $f^2 \mid B^2 - 4AC$. By the maximality of f,

$$B^2 - 4AC = df^2$$

for some squarefree integer d. So $\sqrt{B^2 - 4AC} = f\sqrt{d}$, and $K = \mathbb{Q}(\sqrt{B^2 - 4AC}) = \mathbb{Q}(\sqrt{d})$. □

The uniqueness of the squarefree integer d in Theorem 3.1 can be proved by an elementary but unenlightening computation. We choose a different path.

Definition 3.2. Let K be a number field for which $K/\mathbb{Q}$ is Galois. For $\alpha \in K$, we define its **norm** and **trace** by

$$\mathrm{N}(\alpha) = \prod_{\sigma \in \mathrm{Gal}(K/\mathbb{Q})} \sigma(\alpha), \quad \text{and} \quad \mathrm{Tr}(\alpha) = \sum_{\sigma \in \mathrm{Gal}(K/\mathbb{Q})} \sigma(\alpha).$$

By construction, $\mathrm{N}(\alpha)$ and $\mathrm{Tr}(\alpha)$ are invariant under the action of $\mathrm{Gal}(K/\mathbb{Q})$; hence, $\mathrm{N}(\alpha), \mathrm{Tr}(\alpha) \in \mathbb{Q}$. The norm map is multiplicative, meaning that

$$\mathrm{N}(\alpha\beta) = \mathrm{N}\alpha \cdot \mathrm{N}\beta \qquad \text{for all } \alpha, \beta \in K.$$

The trace, on the other hand, is $\mathbb{Q}$-linear;

$$\mathrm{Tr}(\alpha + \beta) = \mathrm{Tr}(\alpha) + \mathrm{Tr}(\beta), \quad \text{and} \quad \mathrm{Tr}(r\alpha) = r \cdot \mathrm{Tr}(\alpha)$$

for all $\alpha, \beta \in K$ and $r \in \mathbb{Q}$.

Now let d be any nonsquare integer and let $K = \mathbb{Q}(\sqrt{d})$. Then $K/\mathbb{Q}$ is a quadratic Galois extension, and the unique nontrivial automorphism interchanges $\sqrt{d}$ and $-\sqrt{d}$. The generic element of K has the form $a + b\sqrt{d}$ for rational numbers a and b. By a direct computation,

$$\mathrm{Tr}(a + b\sqrt{d}) = 2a \quad \text{and} \quad \mathrm{N}(a + b\sqrt{d}) = a^2 - db^2.$$

Proof of uniqueness in Theorem 3.1. Seeking a contradiction, suppose that the quadratic field K can be written as both $\mathbb{Q}(\sqrt{d_1})$ and $\mathbb{Q}(\sqrt{d_2})$, where d_1 and d_2 are distinct squarefree integers. Since K is quadratic, $d_1, d_2 \neq 1$. Moreover, d_1 and d_2 share the same sign; otherwise, exactly one of $\mathbb{Q}(\sqrt{d_1})$ and $\mathbb{Q}(\sqrt{d_2})$ would be contained in $\mathbb{R}$. So in order for d_1 and d_2 to be distinct, there must be a prime dividing d_1 that does not divide d_2. Then $d_1 d_2$ is divisible precisely by the first power of this prime, and so $d_1 d_2$ is a nonsquare. Since $\sqrt{d_1 d_2} = \pm\sqrt{d_1}\sqrt{d_2} \in K$, we know that $\mathbb{Q}(\sqrt{d_1 d_2}) \subseteq K$. It follows that

$$\mathbb{Q}(\sqrt{d_1}) = \mathbb{Q}(\sqrt{d_2}) = \mathbb{Q}(\sqrt{d_1 d_2}),$$

since the third field is contained in the first two and has the same degree over $\mathbb{Q}$.

To obtain a contradiction, choose rational numbers a, b with

$$0 + 1\sqrt{d_2} = a + b\sqrt{d_1}.$$

Taking the trace of both sides, $2 \cdot 0 = 2 \cdot a$. Thus, $a = 0$. Now multiply both sides of the last display by $\sqrt{d_1}$ to obtain

$$\pm\sqrt{d_1 d_2} = b d_1.$$

Taking the trace again, $0 = 2bd_1$. So $b = 0$, and $\sqrt{d_2} = 0 + 0\sqrt{d_1}$, an absurdity! □

Integers in quadratic fields

Our goal for the rest of the chapter is to determine the ring of integers in an arbitrary quadratic field.

Definition 3.3. Let K be a number field for which $K/\mathbb{Q}$ is Galois. For $\alpha \in K$, the **field polynomial** $\phi_\alpha(x)$ is defined by

$$\phi_\alpha(x) = \prod_{\sigma \in \mathrm{Gal}(K/\mathbb{Q})} (x - \sigma(\alpha)).$$

By Galois invariance, $\phi_\alpha(x) \in \mathbb{Q}[x]$.

Proposition 3.4. Let K be a number field for which $K/\mathbb{Q}$ is Galois. Then

$$\alpha \in \mathbb{Z}_K \iff \phi_\alpha(x) \in \mathbb{Z}[x].$$

Proof. Since α is a root of $\phi_\alpha(x)$, the backward direction ($\Leftarrow$) is clear. To handle the forward direction ($\Rightarrow$), let $\alpha \in \mathbb{Z}_K$. Each $\sigma(\alpha) \in \mathbb{Z}_K$, and so $\phi_\alpha(x) \in \mathbb{Z}_K[x] \subseteq \bar{\mathbb{Z}}[x]$. Since $\phi_\alpha(x) \in \mathbb{Q}[x]$, and $\bar{\mathbb{Z}} \cap \mathbb{Q} = \mathbb{Z}$, the proposition follows. □

We can see now that the trace and norm of α have interpretations as two particular coefficients of $\phi_\alpha(x)$: writing n for the degree of $K/\mathbb{Q}$,

$$\phi_\alpha(x) = x^n - \mathrm{Tr}(\alpha)x^{n-1} + \cdots + (-1)^n \mathrm{N}(\alpha).$$

When $n = 2$, the "…" is not needed. The next result is now immediate from Proposition 3.4.

Proposition 3.5. Let K be a quadratic field, and let $\alpha \in K$. Then $\alpha \in \mathbb{Z}_K \iff \mathrm{N}(\alpha), \mathrm{Tr}(\alpha) \in \mathbb{Z}$.

We now give the promised characterization of $\mathbb{Z}_K$.

Theorem 3.6. Let K be a quadratic field. Write $K = \mathbb{Q}(\sqrt{d})$, where d is squarefree. If $d \equiv 2, 3 \pmod 4$, then

$$\mathbb{Z}_K = \{a + b\sqrt{d} : a, b \in \mathbb{Z}\}.$$

If $d \equiv 1 \pmod 4$, then

$$\mathbb{Z}_K = \{\frac{a' + b'\sqrt{d}}{2} : a', b' \in \mathbb{Z} \text{ with } a' \equiv b' \pmod 2\}.$$

It is perhaps something of a shock that $\frac{1+\sqrt{d}}{2}$ is considered an "integer" when $d \equiv 1 \pmod 4$; c'est la math.

Proof. We look for the elements of K with integral norm and trace. Those singled out in the theorem statement have these properties (an easy check), and we argue that there are no others. Let $\alpha \in \mathbb{Z}_K$, and write $\alpha = a + b\sqrt{d}$ with $a, b \in \mathbb{Q}$. Since $\mathrm{N}\alpha \in \mathbb{Z}$,

$$(2a)^2 - d(2b)^2 = 4 \cdot \mathrm{N}\alpha \in 4\mathbb{Z}.$$

Since $2a = \mathrm{Tr}(\alpha) \in \mathbb{Z}$, we must have $d(2b)^2 \in \mathbb{Z}$. A prime dividing the denominator of $2b$ appears at least twice in the denominator of $(2b)^2$, and so at least once in the denominator of $d(2b)^2$ (since d is squarefree). Since $d(2b)^2 \in \mathbb{Z}$, there are no such primes. That is, $2b \in \mathbb{Z}$. So we may write $a = a'/2$ and $b = b'/2$, with $a, b \in \mathbb{Z}$. From the last display,

$$a'^2 \equiv db'^2 \pmod 4. \tag{3.1}$$

Take first the case when $d \equiv 2, 3 \pmod 4$. Since d is a nonsquare mod 4, we need $b'^2 \not\equiv 1 \pmod 4$. Thus, $2 \mid b'$. Inserting this back into (3.1) shows that $2 \mid a'$. Hence, $a = a'/2$ and $b = b'/2$ are both rational integers.[1] In the case when $d \equiv 1 \pmod 4$, (3.1) forces a' and b' to share the same parity. In both cases we land in the set described in the theorem statement. □

It is easy (Exercise 1) to see that Theorem 3.6 can be recast as follows. Recall that a $\mathbb{Z}$-module M is called **free of rank** n (with

[1] The adjective "rational" in front of "integer" indicates we mean an element of $\mathbb{Z}$, rather than a general algebraic integer.

$n \in \mathbb{Z}_{\geq 0}$) if it has an n-element **basis**. Here an n-element basis of M means a list $\omega_1, \ldots, \omega_n \in M$ with

$$M = \bigoplus_{i=1}^{n} \mathbb{Z}\omega_i.$$

In words, every element of M should have a unique expression as a $\mathbb{Z}$-linear combination of the ω_i. Initially, one might worry that a $\mathbb{Z}$-module could be free of two different ranks. One rules this out by observing that if M is free of rank n, then $M \cong \mathbb{Z}^n$ as abelian groups, and $M/2M \cong (\mathbb{Z}/2\mathbb{Z})^n$ as vector spaces over $\mathbb{Z}/2\mathbb{Z}$. Since the dimension of a vector space is well-defined, the rank of a free $\mathbb{Z}$-module is also well-defined.[2]

Theorem 3.7. Put

$$\tau = \begin{cases} \sqrt{d} & \text{if } d \equiv 2,3 \pmod 4, \\ \frac{1+\sqrt{d}}{2} & \text{if } d \equiv 1 \pmod 4. \end{cases}$$

Then $\mathbb{Z}_K$ is a free $\mathbb{Z}$-module of rank 2 with basis $1, \tau$.

We will see in Chapter 13 that for any number field K, the ring $\mathbb{Z}_K$ is a free $\mathbb{Z}$-module of rank $[K : \mathbb{Q}]$. This is called the theorem on the **existence of an integral basis**.

There is yet another interesting way of stating Theorem 3.6. Namely, with τ as defined above,

$$\mathbb{Z}_K = \mathbb{Z}[\tau]. \tag{3.2}$$

(Since $\tau \in \mathbb{Z}_K$, clearly $\mathbb{Z}[\tau] \subseteq \mathbb{Z}_K$, while the reverse inclusion follows from Theorem 3.7.) Thus, $\mathbb{Z}_K$ is **monogenic**, meaning generated as a ring by a single element. In Chapter 17, we will see that this is not always the case for the ring of integers of an arbitrary number field.

[2]That the dimension is well-defined for finite-dimensional vector spaces over $\mathbb{Z}/2\mathbb{Z}$ is particularly easy: An n-dimensional space has cardinality 2^n, and this determines n !

Exercises

(1) Deduce Theorem 3.7 from Theorem 3.6.

(2) Let $d_1, d_2, \ldots, d_k$ be nonzero integers. For each $\mathcal{I} \subseteq \{1, 2, \ldots, k\}$, let $D_{\mathcal{I}} = \prod_{i \in \mathcal{I}} d_i$. Suppose that $D_{\mathcal{I}}$ is never a square except in the trivial case when $\mathcal{I} = \emptyset$. Show that

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

is a number field of degree 2^k.

Hint: Consider a putative equation of the form $0 = \sum_{\mathcal{I}} c_{\mathcal{I}} \sqrt{D_{\mathcal{I}}}$. For each subset $\mathcal{I}' \subseteq \{1, 2, \ldots, k\}$, multiply the through by $\sqrt{D_{\mathcal{I}'}}$ and compute the trace from $\mathbb{Q}(\sqrt{d_1}, \ldots, \sqrt{d_k})$.

(3) (Bruce[3]) Define a sequence S_n recursively by setting $S_1 = 4$ and letting $S_n = S_{n-1}^2 - 2$ for $n = 2, 3, 4, \ldots$. This exercise outlines a proof of the following theorem of Lucas–Lehmer: If p is prime and $2^p - 1 \mid S_{p-1}$, then $2^p - 1$ is prime. It is this theorem which has been used to certify the primality of the largest known primes. (For odd p, the converse of the theorem also holds, but we do not discuss that here.)

For brevity, write $M_p = 2^p - 1$. Let $R = \mathbb{Z}[\sqrt{3}]$.

(a) Let $\omega = 2 + \sqrt{3}$ and $\tilde{\omega} = 2 - \sqrt{3}$. Show that $\omega\tilde{\omega} = 1$ and that

$$\omega^{2^{m-1}} + \tilde{\omega}^{2^{m-1}} = S_m$$

for all positive integers m.

(b) Assume for a contradiction that $M_p \mid S_{p-1}$ but that M_p is composite. Let q denote a prime divisor of M_p with $q \leq \sqrt{M_p}$. Show that

$$\omega^{2^{p-1}} \equiv -1 \bmod q.$$

Deduce that $\omega \bmod q$ has order exactly 2^p in the group $U(R/qR)$.

(c) Show that $\#R/qR = q^2$ and that $\#U(R/qR) \leq q^2 - 1$. Now obtain a contradiction to the conclusion of (b).

---

[3]Bruce, J.W. *A really trivial proof of the Lucas-Lehmer test*. Amer. Math. Monthly **100** (1993), no. 4, 370–371.

(4) (Davenport, Chowla[4]) Let n be a positive integer. Suppose that m can be written in the form

$$m = |x^2 - (n^2+1)y^2| \quad \text{for some } x, y \in \mathbb{Z}.$$

Show that if this representation of m is chosen with $|y|$ minimal, then $|yn - x| \geq |y|$. Deduce that if m is not a square, then $m \geq 2n$. *Hint for the first part:* If $m = |x^2 - (n^2+1)y^2|$, then also $m = |x'^2 - (n^2+1)y'^2|$, where

$$x' + y'\sqrt{n^2+1} = (x + y\sqrt{n^2+1})(n - \sqrt{n^2+1}).$$

[4] Chowla, S. *On the inequality* $|x^2 - y^2 - 2xyk| \geq 2k$ *(*x, y, k *odd).* Norske Vid. Selsk. Forh. (Trondheim) **34** (1961), 91.

4

Paradise lost — and found

Inferno

Our starting point in this chapter is the following "inconvenient truth": *The ring of integers of $K = \mathbb{Q}(\sqrt{-5})$ is not a unique factorization domain.* It is likely the reader is at least casually acquainted with this fact from their introductory algebra courses. Indeed, $\mathbb{Z}_K = \mathbb{Z}[\sqrt{-5}]$, and in that ring the number 6 (in)famously factors in two different ways as a product of irreducibles:

$$2 \cdot 3 = (1 + \sqrt{-5}) \cdot (1 - \sqrt{-5}). \tag{4.1}$$

There are details to verify to ensure that we are witnessing a genuine violation of unique factorization. Certainly we had better check

(a) All four of 2, 3, and $1 \pm \sqrt{-5}$ are irreducible.

But beyond that, we must also argue

(b) The two sides of (4.1) cannot be made to agree by introducing unit factors.

That some caution in this direction is warranted can be seen from an example such as

$$(5 + \sqrt{2}) \cdot 3 = (-123 + 87\sqrt{2}) \cdot (263 + 186\sqrt{2}),$$

in the ring $\mathbb{Z}[\sqrt{2}]$. All four factors here are irreducible. But unique factorization need not feel threatened, since

$$-123 + 87\sqrt{2} = 3 \cdot (-41 + 29\sqrt{2}),$$
$$263 + 186\sqrt{2} = (5 + \sqrt{2}) \cdot (41 + 29\sqrt{2}),$$

and $\pm 41 + 29\sqrt{2}$ are both units. In fact, it turns out that $\mathbb{Z}[\sqrt{2}]$ is a unique factorization domain.

Our main tool for checking (a) and (b) is the norm map on K. The unique nontrivial automorphism of K is complex conjugation. Hence, $N\alpha = |\alpha|^2$ (as in Chapter 1), and writing $\alpha = a + b\sqrt{-5}$,

$$N\alpha = a^2 + 5b^2.$$

Exactly as in the proof of Lemma 1.4, the units in $\mathbb{Z}_K$ are the elements of norm 1. Since the only integer solutions to $a^2 + 5b^2 = 1$ are $a = \pm 1$ and $b = 0$, we have $U(\mathbb{Z}_K) = \{\pm 1\}$.

Turning to the proof of (a), suppose for a contradiction that $2 = \alpha\beta$, with α and β nonunit elements of $\mathbb{Z}_K$. Taking norms,

$$4 = N(2) = N\alpha \cdot N\beta.$$

Since $N\alpha, N\beta > 1$ (because α and β are nonunits), $N\alpha = N\beta = 2$. Thus, writing $\alpha = a + b\sqrt{-5}$ with $a, b \in \mathbb{Z}$,

$$N\alpha = a^2 + 5b^2 = 2.$$

But this last equation clearly has no integer solutions! Thus, 2 is irreducible. In a similar way, one argues that the other three factors appearing in (4.1) are irreducible.

The proof of (b) is much simpler. Since $U(\mathbb{Z}_K) = \{\pm 1\}$, it is clear that neither of 2 or 3 is a unit multiple of either of $1 \pm \sqrt{-5}$.

Factorization theory: A taster

> You're a droid and I'm a 'noid. – Guinan to Data
> (Star Trek: The Next Generation)

To understand why unique factorization fails in $\mathbb{Z}[\sqrt{-5}]$ and what hope we have of restoring it, it is helpful to look at factorization from an abstract perspective.

Definition 4.1. A **monoid** is a nonempty set with an associative and commutative binary operation (here denoted $\cdot$ and written multiplicatively) and an identity element.

By an argument ubiquitous in algebra, the identity in a monoid is unique: If 1_a and 1_b are both identity elements, then $1_a = 1_a \cdot 1_b = 1_b$. Henceforth, we denote the identity element by 1.

Definition 4.2. A monoid M is **cancellative** if whenever $\alpha\beta = \alpha\gamma$, with α, β, and γ in M, we have $\beta = \gamma$.

Definitions 4.3. Let M be a cancellative monoid.

(a) For $\alpha, \beta \in M$, we say $\alpha \mid \beta$ (read "α **divides** β") if there is a $\gamma \in M$ with
$$\beta = \alpha\gamma.$$

(b) A **unit** in M is an element dividing 1.

(c) We say $\alpha, \beta \in M$ are **associates** if $\alpha = \beta\mu$ for some unit μ.

(d) A nonunit $\pi \in M$ is an **irreducible** (aka an **atom**) if whenever $\pi = \alpha\beta$, with $\alpha, \beta \in M$, either α is a unit or β is a unit.

(e) A nonunit $\pi \in M$ is **prime** if whenever $\pi \mid \alpha\beta$, with $\alpha, \beta \in M$, either $\pi \mid \alpha$ or $\pi \mid \beta$.

(f) Elements $\alpha, \beta \in M$ are said to possess a **greatest common divisor** $\delta \in M$ if $\delta \mid \alpha$ and $\delta \mid \beta$ and every $\gamma \in M$ for which $\gamma \mid \alpha$ and $\gamma \mid \beta$ satisfies $\gamma \mid \delta$.

(g) M is a **Unique Factorization Monoid** (also called a **factorial monoid**) if every nonunit element of M can be written uniquely — up to order and associates — as a product of irreducible elements.

Let R be any integral domain. Then $R \setminus \{0\}$, with multiplication inherited from R, is a cancellative monoid. For this monoid, the preceding definitions agree with the cognate ring-theoretic concepts. In particular, R is a UFD precisely when $R \setminus \{0\}$ is a UFM (unique factorization monoid). The monoidal point of view has the advantage of allowing us to discuss factorization in R without the excess baggage of addition on R.

We now give two criteria for a cancellative monoid M to possess unique factorization.

Definition 4.4. A cancellative monoid is **atomic** if every nonunit element can be written as a product of irreducibles.

Our first criterion for unique factorization is already implicit in Euclid's *Elements*.

Proposition 4.5. Let M be a cancellative monoid. Then M is a UFM $\iff$ M is atomic and every irreducible element of M is prime.

The proof of Proposition 4.5 is left to the reader. But it should have the air of the familiar; in the usual proofs that $\mathbb{Z}$ is a UFD, one first shows the existence of factorizations (atom-icity) and then proves uniqueness after establishing that irreducibles are prime (Euclid's lemma).

It is convenient for what follows if our monoids have no nontrivial units. Luckily, it is easy to place ourselves in this situation. For a cancellative monoid M, let $\sim$ denote the equivalence relation of "associate"-ness, and let $M_{\text{red}} := M/\sim$ be the corresponding quotient. Then M_{red}, with multiplication induced from M, is itself a monoid (the **reduced monoid** associated to M). By construction, the only unit in M is the identity. Moreover, all of the interesting arithmetic of M is preserved in the passage to M_{red}: The irreducibles and primes of M_{red} are precisely the images of the irreducibles and primes of M, and

$$\begin{aligned} M \text{ is a UFM} &\iff M_{\text{red}} \text{ is a UFM} \\ &\iff \text{Every element of } M_{\text{red}} \text{ factors uniquely} \\ &\qquad \text{as a product of irreducibles, up to the} \\ &\qquad \text{order of the factors.} \end{aligned}$$

(There is no need to exclude the unit element of M_{red}; 1 factors uniquely as the empty product!)

The second criterion generalizes Euler's beautiful observation that any two factorizations of the same positive integer can be "explained" by a common refinement. For example, the equality

$$21 \cdot 10 = 14 \cdot 15$$

can be "explained" by the four factorizations

$$21 = 7 \cdot 3, \quad 10 = 2 \cdot 5, \quad 14 = 7 \cdot 2, \quad \text{and} \quad 15 = 3 \cdot 5.$$

Theorem 4.6 (Euler's four numbers theorem)**.** Let M be a cancellative, atomic monoid with 1 as its only unit. M is a UFM if and only if the following holds: Whenever $\alpha, \beta, \gamma, \delta \in M$ satisfy

$$\alpha\beta = \gamma\delta,$$

there are $\rho, \sigma, \tau, \upsilon \in M$ with

$$\alpha = \rho\sigma, \quad \beta = \tau\upsilon, \quad \gamma = \rho\tau, \quad \delta = \sigma\upsilon. \tag{4.2}$$

Proof. We start with "if". M is atomic, and so it suffices to prove that all of its irreducibles are prime. Suppose γ is irreducible and that $\gamma \mid \alpha\beta$. Write $\alpha\beta = \gamma\delta$ for some $\delta \in M$. Choose $\rho, \sigma, \tau, \upsilon$ as in (4.2). Since $\gamma = \rho\tau$ and γ is irreducible, either $\rho = 1$ and $\tau = \gamma$ or vice-versa. It is now immediate from (4.2) that $\gamma \mid \alpha$ or $\gamma \mid \beta$. Thus, γ is prime.

For the "only if" direction, we argue using greatest common divisors. It is easy to see that when M is a UFM with 1 as its only unit, any two elements of M have a unique gcd (namely, the product of the primes dividing both of them, taken with multiplicities). Given an equation of the form

$$\alpha\beta = \gamma\delta, \tag{4.3}$$

set $\rho = \gcd(\alpha, \gamma)$. Then there are $\sigma, \tau \in M$ with

$$\alpha = \rho\sigma, \quad \gamma = \rho\tau. \tag{4.4}$$

Inserting these expressions back into (4.3) and canceling ρ from both sides,

$$\sigma\beta = \tau\delta.$$

By the choice of ρ, the elements σ and τ have gcd 1. So by unique factorization, $\sigma \mid \delta$. Write

$$\delta = \sigma\upsilon. \tag{4.5}$$

Inserting this into the last display and canceling,

$$\beta = \tau\upsilon. \tag{4.6}$$

Assembling (4.4)—(4.6) finishes the proof of Theorem 4.6. □

The case of the missing numbers

Let us look again at our initial counterexample to unique factorization in $\mathbb{Z}[\sqrt{-5}]$, this time through the lens of Euler's four numbers theorem. Let $M = (\mathbb{Z}[\sqrt{-5}] \setminus \{0\})_{\text{red}}$. Using brackets $\langle\cdot\rangle$ to indicate when elements of $\mathbb{Z}[\sqrt{-5}] \setminus \{0\}$ are being viewed in M, our earlier example takes the form

$$\langle 1 + \sqrt{-5}\rangle \cdot \langle 1 - \sqrt{-5}\rangle = \langle 2\rangle \cdot \langle 3\rangle. \tag{4.7}$$

What exactly goes wrong here? From our more enlightened vantage point, we recognize (4.7) as a pair of factorizations of 6 failing to admit a common refinement. That is, there are no "four numbers" $\rho, \sigma, \tau, \upsilon$ giving us (4.3). Looked at from this angle, we catch a glimpse of a way forward. While it is not obvious how to "restore" unique factorization, it is clear what to do about not having the right four numbers: We should introduce more "numbers"!

Where should we look for these numbers? The monoid M was formed by taking $\mathbb{Z}[\sqrt{-5}]$, throwing away 0, and identifying elements up to associates. In any integral domain, associate elements are those generating the same principal ideal. Thus, there is a bijection between the elements of M and the nonzero principal ideals of $\mathbb{Z}[\sqrt{-5}]$, obtained by sending $\langle\alpha\rangle$ to the ideal generated by α. Throughout this text, we use brackets to enclose generating sets of ideals, so that the principal ideal generated by α is also denoted $\langle\alpha\rangle$. If we multiply principal ideals by the rule $\langle\alpha\rangle\langle\beta\rangle = \langle\alpha\beta\rangle$, then the nonzero principal ideals become a monoid isomorphic (in the obvious sense) to M.

There is now a natural and compelling choice for a set of "numbers" larger than M, namely the collection of **all** nonzero ideals of $\mathbb{Z}[\sqrt{-5}]$.

Definition 4.7. Let R be a ring. If I and J are ideals of R, their product IJ is the smallest ideal of R containing all products $\alpha\beta$, with $\alpha \in I, \beta \in J$. More explicitly,

$$IJ = \{\text{all finite sums } \textstyle\sum_i \alpha_i\beta_i : \alpha_i \in I, \beta_i \in J\}.$$

Definition 4.8. For any integral domain R, we let $\mathrm{Id}(R)$ denote the collection of nonzero ideals of R.

We leave to the reader the task of verifying the following basic properties of ideal multiplication.

Proposition 4.9. Let R be a ring.[1]

(a) Multiplication of ideals is commutative.

(b) Multiplication of ideals is associative.

(c) The identity element for ideal multiplication is $\langle 1\rangle$ (i.e., is R itself, viewed as an ideal).

(d) Ideal multiplication distributes over addition, in the sense that
$$I(J+K) = IJ + IK$$
for any three ideals I, J, and K.

(e) $IJ \subseteq I \cap J$ for all ideals I and J.

(f) If $I = \langle \alpha_1, \alpha_2, \ldots, \alpha_j\rangle$ and $J = \langle \beta_1, \beta_2, \ldots, \beta_k\rangle$, then $IJ = \langle \alpha_1\beta_1, \ldots, \alpha_1\beta_k, \ldots \alpha_j\beta_1, \ldots, \alpha_j\beta_k\rangle$.

(g) If I and J are nonzero ideals of R and R is a domain, then IJ is also a nonzero ideal.

Among other things, Proposition 4.9 guarantees that whenever R is an integral domain, ideal multiplication makes $\mathrm{Id}(R)$ into a monoid. The identity element is $\langle 1\rangle$ (by part (c)), which is also the only unit (by part (e)).

To appreciate what we have gained, we look again at (4.7), this time as an equation in $\mathrm{Id}(\mathbb{Z}[\sqrt{-5}])$. Happily, we are now in a position to offer an explanation for (4.7), in the sense of the four numbers theorem. Consider the four elements of $\mathrm{Id}(\mathbb{Z}[\sqrt{-5}])$ given by

$$I = \langle 1+\sqrt{-5},\ 2\rangle, \quad J = \langle 1+\sqrt{-5},\ 3\rangle, \tag{4.8}$$
$$I' = \langle 1-\sqrt{-5},\ 2\rangle, \quad J' = \langle 1-\sqrt{-5},\ 3\rangle.$$

We claim that

$$IJ = \langle 1+\sqrt{-5}\rangle, \quad I'J' = \langle 1-\sqrt{-5}\rangle, \tag{4.9}$$
$$JJ' = \langle 3\rangle, \quad II' = \langle 2\rangle,$$

thereby "explaining" (4.7).

[1] commutative with 1 (as always in this text).

Let us check the first of the assertions in (4.9). From Proposition 4.9(f),

$$\begin{aligned} IJ &= \langle (1+\sqrt{-5})^2,\ 3\cdot(1+\sqrt{-5}),\ 2\cdot(1+\sqrt{-5}),\ 6\rangle \\ &= \langle 1+\sqrt{-5}\rangle \cdot \langle 1+\sqrt{-5},\ 3,\ 2,\ 1-\sqrt{-5}\rangle. \end{aligned}$$

We observe for the last factor that

$$1 = 3 - 2 \in \langle 1+\sqrt{-5},\ 3,\ 2,\ 1-\sqrt{-5}\rangle;$$

hence, this factor is actually $\langle 1\rangle$. Thus, $IJ = \langle 1+\sqrt{-5}\rangle$, as desired. The remaining claims in (4.9) can be checked by entirely analogous calculations.

Paradiso

We opened this chapter with an example of a factorization in $\mathbb{Z}[\sqrt{-5}]$ that was problematic from the standpoint of the "elemental" world. We have just seen that these problems evaporate in our "idealized" universe. Amazingly, the maneuver of passing from elements to ideals can be shown to resolve *all* factorization problems not only in $\mathbb{Z}[\sqrt{-5}]$ but in the ring of integers of any number field. This is meant in the sense that $\mathrm{Id}(\mathbb{Z}_K)$ is a UFM for every number field K. This remarkable result of Dedekind[2] is one version of the justly-named **Fundamental Theorem of Ideal Theory**, which we will revisit in Chapters 6 and 15.

[2]Between 1871 and 1894, Dedekind published four somewhat different accounts of ideal theory, three in German as supplements to Dirichlet's *Vorlesungen über Zahlentheorie*, and a fourth account in French intended for a wider mathematical audience. These writings are collected in: Dedekind, R. *Über die Theorie der ganzen algebraischen Zahlen.* Vieweg+Teubner Verlag, Braunschweig, 1964.

Exercises

(1) Supply the proofs of Propositions 4.5 and 4.9.

(2) Let $R = \mathbb{Z}[\sqrt{-3}]$, and let $I = \langle 2, 1 + \sqrt{-3}\rangle$. Show that $I^2 = \langle 2\rangle I$ but that $I \neq \langle 2\rangle$. Hence, $\mathrm{Id}(R)$ is not cancellative. Why doesn't this contradict the fundamental theorem?

(3) Let K be a quadratic field.
   (a) Prove that the monoid $\mathbb{Z}_K \setminus \{0\}$ is atomic. *Hint:* Induct on the absolute value of the norm.
   (b) Prove that $\mathbb{Z}_K \setminus \{0\}$ has infinitely many pairwise nonassociate irreducible elements. *Hint:* For each rational prime p, pick an irreducible element $\pi_p \in \mathbb{Z}_K$ dividing p.

(4) Check that the equations

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

and

$$\sqrt{15} \cdot \sqrt{15} = 3 \cdot 5$$

exhibit genuine failures of unique factorization in $\mathbb{Z}[\sqrt{-6}]$ and $\mathbb{Z}[\sqrt{15}]$, respectively. Then show that the corresponding equations of ideals can be "explained" in the sense of the four numbers theorem, in analogy with how we dealt with (4.7).

(5) In Chapter 1, we observed that

$$3 \cdot 3 \cdot 3 = (1 + \sqrt{-26})(1 - \sqrt{-26})$$

and deduced that $\mathbb{Z}[\sqrt{-26}]$ is not a UFD. Show that if $P = \langle 3, 1 + \sqrt{-26}\rangle$ and $Q = \langle 3, 1 - \sqrt{-26}\rangle$, then $\langle 3\rangle = PQ$, $\langle 1 + \sqrt{-26}\rangle = P^3$, and $\langle 1 - \sqrt{-26}\rangle = Q^3$.

5

Euclidean quadratic fields

The following definition is probably familiar to the reader from a first course in ring theory.

Definition 5.1. A domain R is a **Euclidean Domain** if there is a function $n\colon R \setminus \{0\} \to \mathbb{Z}^+$ for which the following holds: Whenever $\alpha, \beta \in R$ with $\beta \neq 0$, there are $\xi, \rho \in R$ with

$$\alpha = \beta\xi + \rho \quad \text{and either} \quad \rho = 0 \quad \text{or} \quad n(\rho) < n(\beta).$$

We call $n(\cdot)$ a **Euclidean function on** R.

All Euclidean Domains are Principal Ideal Domains (PIDs), and all PIDs are Unique Factorization Domains (UFDs). So if one is interested in the arithmetic of quadratic fields, the following question is very natural.

Question 5.2. Call a quadratic field K **Euclidean** if $\mathbb{Z}_K$ is a Euclidean domain. What are all of the Euclidean quadratic fields?

The question becomes more approachable if we specify the Euclidean function in advance. Fortunately, there is an obvious candidate.

Question 5.3. Call a quadratic field K **norm-Euclidean** if $\mathbb{Z}_K$ is Euclidean with respect to the map $n(\alpha) = |\mathrm{N}(\alpha)|$. What are the norm-Euclidean quadratic fields?

Most of this chapter is devoted to a discussion of Question 5.3. The following criterion plays a key role in the investigation.

Proposition 5.4. Let K be a quadratic field. Then K is norm-Euclidean $\iff$ for all $\theta \in K$, there is a $\xi \in \mathbb{Z}_K$ with

$$|N(\theta - \xi)| < 1.$$

Proof. We start with the forward direction ($\Rightarrow$). Assume that K is norm-Euclidean. Given $\theta \in K$, we can write $\theta = \alpha/\beta$ with $\beta \in \mathbb{Z}_K$ and $\beta \neq 0$. (In fact, we showed in Proposition 2.9 that β can be taken as a positive integer.) By assumption, there are ξ and ρ in $\mathbb{Z}_K$ with

$$\alpha = \beta\xi + \rho \quad \text{and} \quad |N(\rho)| < |N(\beta)|.$$

(It is not necessary to single out the $\rho = 0$ case, since $N(0) = 0 < |N(\beta)|$.) Dividing the displayed equation by β, we find that

$$|N(\theta - \xi)| = |N(\rho/\beta)| = \left|\frac{N(\rho)}{N(\beta)}\right| < 1,$$

as desired. The proof of the backward direction ($\Leftarrow$) is similar: Given $\alpha, \beta \in \mathbb{Z}_K$ with $\beta \neq 0$, choose $\xi \in \mathbb{Z}_K$ with $|N(\frac{\alpha}{\beta} - \xi)| < 1$, and put $\rho = \alpha - \beta\xi$. Then $\alpha = \beta\xi + \rho$ and

$$|N(\rho)| = |N(\beta \cdot (\frac{\alpha}{\beta} - \xi))| = |N(\beta)| \cdot |N(\frac{\alpha}{\beta} - \xi)| < |N(\beta)|. \quad \square$$

Norm-Euclidean imaginary quadratic fields

A quadratic field K is called **real** if $K \subseteq \mathbb{R}$ and **imaginary** otherwise. In this section, we completely determine the norm-Euclidean imaginary quadratic fields. The following result is due Dedekind and appears in a supplement to Dirichlet's lectures on number theory.

Theorem 5.5. Let $K = \mathbb{Q}(\sqrt{d})$ where $d < 0$ is squarefree. Then $\mathbb{Z}_K$ is norm-Euclidean $\iff$ $d = -1, -2, -3, -7$, or -11.

It is helpful to say a few words about strategy before embarking on the formal proof. Thinking of $\mathbb{C}$ as the "complex plane" allows us to view K as a subset of $\mathbb{R}^2$. Under this identification, $\mathbb{Z}_K$ is sent to Λ, where Λ is the $\mathbb{Z}$-span of the vectors

$$\mathbf{v}_1 = \begin{bmatrix} 1 \\ 0 \end{bmatrix} \quad \text{and} \quad \mathbf{v}_2 = \begin{bmatrix} 0 \\ \sqrt{|d|} \end{bmatrix}$$

in the cases when $d \equiv 2, 3 \pmod 4$, and the $\mathbb{Z}$-span of

$$\mathbf{v}_1 = \begin{bmatrix} 1 \\ 0 \end{bmatrix} \quad \text{and} \quad \mathbf{v}_2 = \begin{bmatrix} \frac{1}{2} \\ \frac{1}{2}\sqrt{|d|} \end{bmatrix},$$

when $d \equiv 1 \pmod 4$. The field K is sent to the $\mathbb{Q}$-span of these two vectors, which we will denote by $\Lambda \otimes \mathbb{Q}$.

Since $d < 0$, the norm map on K coincides with the square of the complex absolute value. It now follows from Proposition 5.4 that $\mathbb{Z}_K$ is norm-Euclidean precisely when every element of $\Lambda \otimes \mathbb{Q}$ lies in an open unit disc centered around a point of Λ.

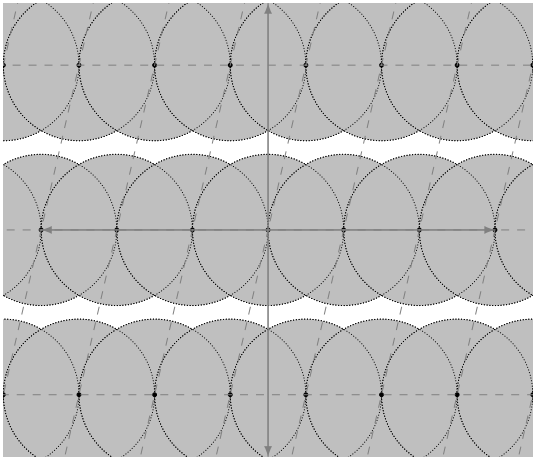


Figure 5.1. Illustration of the failure of $\mathbb{Z}[\frac{1+\sqrt{-19}}{2}]$ to be norm-Euclidean.

Geometrically, it quickly becomes apparent that this condition is satisfied for certain d and not others. For instance, glancing at Figure 5.1 shows that when $d = -19$, there are neighborhoods in $\mathbb{R}^2$ not covered by any disc. Since $\Lambda \otimes \mathbb{Q}$ is dense in $\mathbb{R}^2$, this implies that $\mathbb{Z}[\frac{1+\sqrt{-19}}{2}]$ is not norm-Euclidean. On the other, when $d = 2$ Figure 5.2 indicates that every point of $\mathbb{R}^2$ is contained in at least one disc. A fortiori, every point of $\Lambda \otimes \mathbb{Q}$ is covered, and so $\mathbb{Z}[\sqrt{-2}]$ is norm-Euclidean.

Proof of Theorem 5.5. In those cases where $\mathbb{Z}_K$ is claimed to be norm-Euclidean, we will show that every $\mathbf{v} \in \Lambda \otimes \mathbb{Q}$ is contained in the unit

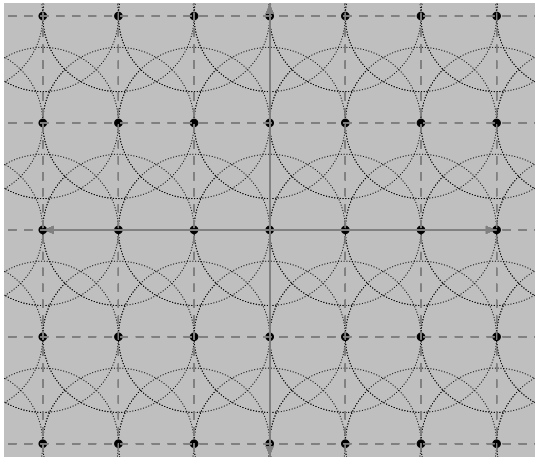


Figure 5.2. The ring $\mathbb{Z}[\sqrt{-2}]$ is norm-Euclidean.

disc about some $\mathbf{w} \in \Lambda$. In the remaining cases, we give an example of a $\mathbf{v} \in \Lambda \otimes \mathbb{Q}$ not contained in any such disc. We will write $\mathbf{v} = a\mathbf{v}_1 + b\mathbf{v}_2$ and $\mathbf{w} = A\mathbf{v}_1 + B\mathbf{v}_2$; here $a, b \in \mathbb{Q}$ and $A, B \in \mathbb{Z}$.

When $d \equiv 2, 3 \pmod 4$,

$$\|\mathbf{v} - \mathbf{w}\|^2 = (a - A)^2 + |d|(b - B)^2. \tag{5.1}$$

Given $\mathbf{v}$, let A and B be the nearest integers to a and b, respectively (breaking any ties arbitrarily). Then $|a - A| \leq \frac{1}{2}$, $|b - B| \leq \frac{1}{2}$, and

$$\|\mathbf{v} - \mathbf{w}\|^2 \leq \frac{|d| + 1}{4}.$$

The right-hand side is less than 1 when $d = -1$ or $d = -2$. Hence, $\mathbb{Z}[i]$ and $\mathbb{Z}[\sqrt{-2}]$ are norm-Euclidean. (The latter was remarked on above.)

Still supposing that $d \equiv 2, 3 \pmod 4$, assume now that $|d| > 2$. Then actually $|d| \geq 5$. Let $\mathbf{v}$ be the element of $\Lambda \otimes \mathbb{Q}$ given by $\mathbf{v} = \frac{1}{2}\mathbf{v}_1 + \frac{1}{2}\mathbf{v}_2$. It follows from (5.1) that for any $\mathbf{w} \in \Lambda$,

$$\|\mathbf{v} - \mathbf{w}\|^2 \geq \left(\frac{1}{2}\right)^2 + |d|\left(\frac{1}{2}\right)^2 = \frac{|d| + 1}{4} \geq \frac{3}{2}.$$

So $\mathbf{v}$ is not in any unit disc about any Λ, and $\mathbb{Z}_K$ is not norm-Euclidean.

Now suppose that $d \equiv 1 \pmod 4$. In this case,

$$\|\mathbf{v} - \mathbf{w}\|^2 = \left(a - A + \frac{b-B}{2}\right)^2 + |d|\left(\frac{b-B}{2}\right)^2. \tag{5.2}$$

Given $\mathbf{v}$, choose $B \in \mathbb{Z}$ with $|b - B| \le \frac{1}{2}$. Having chosen B, choose $A \in \mathbb{Z}$ with $|a - A + \frac{b-B}{2}| \le \frac{1}{2}$. Then

$$\|\mathbf{v} - \mathbf{w}\|^2 \le \frac{1}{4} + \frac{|d|}{16}.$$

If $d = -3, -7$, or -11, the right-hand side is smaller than 1. Thus, $\mathbb{Z}_K$ is norm-Euclidean in these cases.

Finally, suppose that $d \equiv 1 \pmod 4$ and $|d| > 11$. Then $|d| \ge 15$. As above, let $\mathbf{v}$ be the element of $\Lambda \otimes \mathbb{Q}$ given by $\mathbf{v} = \frac{1}{2}\mathbf{v}_1 + \frac{1}{2}\mathbf{v}_2$ (so that $a = b = \frac{1}{2}$). For any $A, B \in \mathbb{Z}$,

$$\left|a - A + \frac{b-B}{2}\right| = \left|\frac{3 - 4A - 2B}{4}\right| \ge \frac{1}{4},$$

while $|\frac{b-B}{2}| \ge \frac{1}{4}$. So from (5.2), for any $\mathbf{w} \in \Lambda$,

$$\|\mathbf{v} - \mathbf{w}\|^2 \ge \frac{1}{16} + 15 \cdot \frac{1}{16} = 1.$$

Hence, $\mathbb{Z}_K$ is not norm-Euclidean. □

Norm-Euclidean real quadratic fields

The norm-Euclidean real quadratic fields have also been completely determined.

Theorem 5.6. Let $K = \mathbb{Q}(\sqrt{d})$ where d is squarefree and $d > 1$. Then K is norm-Euclidean $\iff d = 2, 3, 5, 6, 7, 11, 13, 17, 19, 21, 29, 33, 37, 41, 57, 73$.

The proof of Theorem 5.6 is more difficult than that of Theorem 5.5 by several orders of magnitude. Here we content ourselves with a few remarks.

That the fields listed in Theorem 5.6 are all norm-Euclidean can be shown by geometric considerations similar to those seen above. We give one example, which is representative of the general case while

relatively simple to describe. Let $K = \mathbb{Q}(\sqrt{6})$. We embed K into $\mathbb{R}^2$ via the map

$$a + b\sqrt{6} \mapsto \begin{bmatrix} a \\ b \end{bmatrix}.$$

This identifies $\mathbb{Z}_K = \mathbb{Z}[\sqrt{6}]$ with the standard lattice $\mathbb{Z}^2 \subseteq \mathbb{R}^2$ and identifies K with $\mathbb{Q}^2$.

As before, we wish to interpret the condition of Proposition 5.4 in terms of coverings of the plane. If $\theta = a + b\sqrt{6}$ and $\xi = A + B\sqrt{6}$, then

$$|\mathrm{N}(\theta - \xi)| < 1 \iff |(a-A)^2 - 6(b-B)^2| < 1.$$

This motivates the following definition: For $\mathbf{v} \in \mathbb{Z}^2$, write $\mathbf{v} = \left[\begin{smallmatrix} A \\ B \end{smallmatrix}\right]$, and let

$$\mathcal{R}_{\mathbf{v}} := \left\{ \begin{bmatrix} a \\ b \end{bmatrix} \in \mathbb{R}^2 : |(a-A)^2 - 6(b-B)|^2 < 1 \right\}.$$

Each $\mathcal{R}_{\mathbf{v}}$ is a "four-armed" region bounded by hyperbolas; see Figure 5.3. Moreover,

$$\mathcal{R}_{\mathbf{v}} = \mathbf{v} + \mathcal{R}_{\left[\begin{smallmatrix} 0 \\ 0 \end{smallmatrix}\right]},$$

where + indicates translation. Thus, by Proposition 5.4,

$\mathbb{Z}[\sqrt{6}]$ is norm-Euclidean

$\iff$ the translates $\mathcal{R}_{\left[\begin{smallmatrix} 0 \\ 0 \end{smallmatrix}\right]} + \mathbf{v}$ cover $\mathbb{Q}^2$, for $\mathbf{v} \in \mathbb{Z}^2$

$\iff$ these translates cover the rational points of the square $[-1/2, 1/2] \times [-1/2, 1/2]$.

(We use here that the translations of $[-\frac{1}{2}, \frac{1}{2}] \times [-\frac{1}{2}, \frac{1}{2}]$ by elements of $\mathbb{Z}^2$ fill out the plane.)

Figure 5.4 shows the square $[-\frac{1}{2}, \frac{1}{2}] \times [-\frac{1}{2}, \frac{1}{2}]$ together with the three regions

$$\mathcal{R}_{\left[\begin{smallmatrix} 0 \\ 0 \end{smallmatrix}\right]}, \quad \mathcal{R}_{\left[\begin{smallmatrix} -1 \\ 0 \end{smallmatrix}\right]}, \quad \text{and} \quad \mathcal{R}_{\left[\begin{smallmatrix} 1 \\ 0 \end{smallmatrix}\right]}.$$

There are exactly four points of the square not contained in these three $\mathcal{R}_{\mathbf{v}}$. (Keep in mind that the square is closed while the $\mathcal{R}_{\mathbf{v}}$ are open.) These are the intersection points of the bounding hyperbolas, given explicitly by $\left[\begin{smallmatrix} \pm 1/2 \\ \pm\sqrt{5/24} \end{smallmatrix}\right]$. But these points are not in $\mathbb{Q}^2$! So our three regions **do** cover all of the rational points in $[-\frac{1}{2}, \frac{1}{2}] \times [-\frac{1}{2}, \frac{1}{2}]$, despite failing to cover all of the real points. This completes our proof by picture that $\mathbb{Z}[\sqrt{6}]$ is norm-Euclidean.

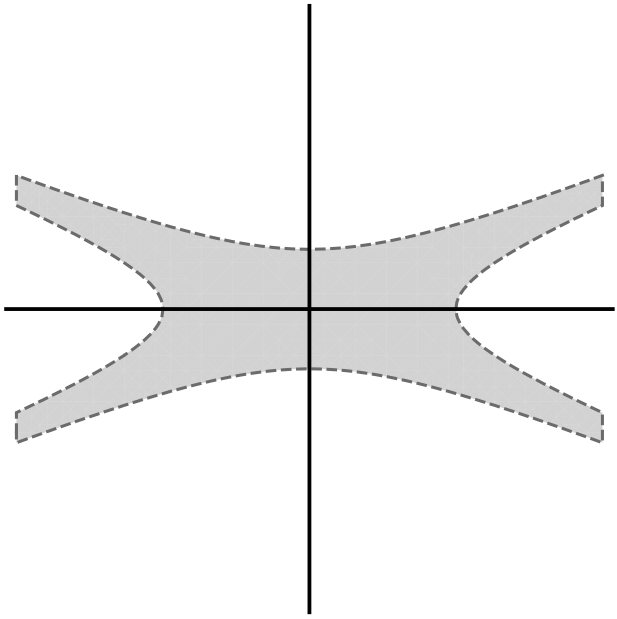


Figure 5.3. That portion of the "four-armed" region $\mathcal{R}_{\left[\begin{smallmatrix}0\\0\end{smallmatrix}\right]}$ lying in $[-2,2]\times[-2,2]$.

Proofs of the same geometric character can be given for all of the other fields appearing in Theorem 5.6. See, for instance, the American Mathematical Monthly article by Eggleton, Lacampagne, and Selfridge.[1]

The necessity half of Theorem 5.6 is much more involved and was not completely proved until 1952. Here one has to show that certain rational points are never covered, and due to the odd shape of the (unbounded!) regions involved, rather subtle arguments are required. Some partial results are given in the famous text of Hardy and Wright;[2] see also the article of Eggleton et al. cited above. Full references along with a detailed history of the proof can be found in a survey article of Lemmermeyer on Euclidean number fields.[3]

---

[1]Eggleton, R. B.; Lacampagne, C. B.; Selfridge, J. L. *Euclidean quadratic fields.* Amer. Math. Monthly **99** (1992), no. 9, 829–837.

[2]Hardy, G. H.; Wright, E. M. *An introduction to the theory of numbers.* Sixth edition. Oxford University Press, Oxford, 2008.

[3]Lemmermeyer, F. *The Euclidean algorithm in algebraic number fields.* Exposition. Math. **13** (1995), no. 5, 385–416.

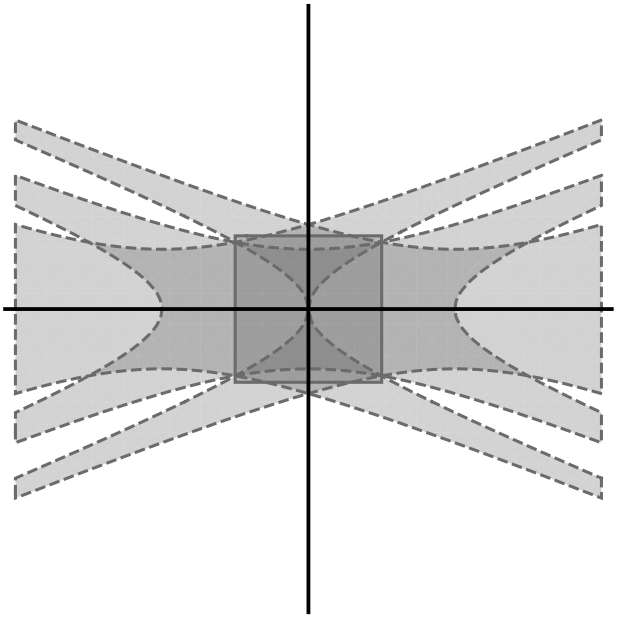


Figure 5.4. A "proof by picture" that $\mathbb{Z}[\sqrt{6}]$ is norm-Euclidean.

Goodbye, Norm

What about our original Question 5.2, where arbitrary Euclidean functions were allowed? Perhaps surprisingly, the answers in the imaginary and real cases diverge sharply.

When K is imaginary, the extra freedom makes no difference.

Theorem 5.7 (Motzkin[4])**.** If K is imaginary quadratic and K is Euclidean, then K is norm-Euclidean.

The proof of Theorem 5.7 relies on two lemmas, both of which are of independent interest.

Lemma 5.8. Let $K = \mathbb{Q}(\sqrt{d})$, where d is a negative squarefree integer. If $d = -1$, then

$$U(\mathbb{Z}_K) = \{\pm 1, \pm i\}.$$

[4]Motzkin, Th. *The Euclidean algorithm.* Bull. Amer. Math. Soc. **55** (1949), 1142–1146.

If $d = -3$, then setting $\omega = \frac{-1+\sqrt{-3}}{2}$,

$$U(\mathbb{Z}_K) = \{\pm 1, \pm\omega, \pm\omega^2\}.$$

In all other cases, $U(\mathbb{Z}_K) = \{\pm 1\}$.

Proof. By an argument familiar from Chapter 1, the units of $\mathbb{Z}_K$ are exactly the elements of norm 1.

If $d \equiv 2, 3 \pmod 4$, norm 1 elements correspond to integer solutions of $a^2 + |d|b^2 = 1$. When $d = -1$, the four solutions $a = \pm 1$, $b = 0$ and $a = 0$, $b = \pm 1$ yield the four units $\{\pm 1, \pm i\}$ of $\mathbb{Z}[i]$ listed above. For $d < -1$, the only solutions to $a^2 + |d|b^2 = 1$ are $a = \pm 1$, $b = 0$, so that $U(\mathbb{Z}_K) = \{\pm 1\}$.

When $d \equiv 1 \pmod 4$, the units of $\mathbb{Z}_K$ are the elements $\frac{a+b\sqrt{d}}{2}$, where a and b are integers of the same parity with $a^2 + |d|b^2 = 4$. This equation has six solutions when $d = -3$, namely $a = \pm 2$ and $a = \pm 1, b = \pm 1$. Straightforward computation reveals that these correspond to the six units $\pm 1, \pm\omega, \pm\omega^2$ in $\mathbb{Z}[\frac{1+\sqrt{-3}}{2}]$. When $|d| \geq 7$, every solution to $a^2 + |d|b^2 = 4$ has $b = 0$, and thus $a = \pm 2$. We deduce that $U(\mathbb{Z}_K) = \{\pm 1\}$ in these cases. □

We defer the proof of the following result to the next chapter.

Lemma 5.9. Let K be a quadratic field. For each nonzero $\beta \in \mathbb{Z}_K$,

$$\#\mathbb{Z}_K/\beta\mathbb{Z}_K = |\mathrm{N}\beta|.$$

Proof of Theorem 5.7. We give the proof as presented by Dubois and Steger.[5] Suppose for a contradiction that K is Euclidean but not in the list given in Theorem 5.5. Let $n(\cdot)$ be a Euclidean function on $\mathbb{Z}_K$, and let β be a nonzero, nonunit element of $\mathbb{Z}_K$ chosen with $n(\beta)$ as small as possible. Given any $\alpha \in \mathbb{Z}_K$, we can write

$$\alpha = \beta\xi + \rho, \quad \text{where} \quad \rho = 0 \quad \text{or} \quad n(\rho) < n(\beta).$$

Looking modulo β, we deduce that every coset of $\mathbb{Z}_K/\beta\mathbb{Z}_K$ is represented by 0 or a unit. Hence,

$$\#\mathbb{Z}_K/\beta\mathbb{Z}_K \leq 1 + \#U(\mathbb{Z}_K).$$

[5] Dubois, D. W.; Steger, A. *A note on division algorithms in imaginary quadratic number fields.* Canad. J. Math. **10** (1958), 285–286.

Since K is neither $\mathbb{Q}(\sqrt{-1})$ nor $\mathbb{Q}(\sqrt{-3})$, we have $\#U(\mathbb{Z}_K) = 2$. So by Lemma 5.9, $N\beta \leq 3$.

Suppose now that $d \equiv 2, 3 \pmod 4$. Then $\beta = a + b\sqrt{d}$ for some $a, b \in \mathbb{Z}$, and $a^2 + |d|b^2 \leq 3$. But $|d| \geq 5$ (since d is not in the list of Theorem 5.5), and so $b = 0$, which in turn forces $a = 0$ or $a = \pm 1$. Both cases contradict the choice of β. If instead $d \equiv 1 \pmod 4$, then $\beta = \frac{a+b\sqrt{d}}{2}$ for some integers a, b of the same parity, and $a^2 + |d|b^2 \leq 12$. Since $|d| \geq 15$, we must have $b = 0$, and thus $a = 0$ or $a = \pm 2$. Hence, $\beta = 0$ or $\beta = \pm 1$, which is again verboten. □

The situation for real quadratic fields K is stunningly different. For these, it is conjectured that

$$\mathbb{Z}_K \text{ a UFD} \Longrightarrow \mathbb{Z}_K \text{ is a Euclidean domain.}$$

In fact, this implication is believed to hold for every number field K that is *not* imaginary quadratic. (It certainly fails in the imaginary quadratic case; e.g., we will see in Chapter 11 that the ring of integers of $\mathbb{Q}(\sqrt{-19})$ is a UFD, whereas we know already that $\mathbb{Q}(\sqrt{-19})$ is not Euclidean.) A compelling piece of evidence for the strong form of the conjecture is that it becomes a theorem if one assumes a certain plausible-seeming generalization of the Riemann Hypothesis.[6]

What is known unconditionally? In 1994, Clark proved that $\mathbb{Q}(\sqrt{69})$ is Euclidean but not norm-Euclidean.[7] Ten years later, Harper gave several further examples of Euclidean quadratic fields that are not norm-Euclidean.[8] In 2007, Narkiewicz published the following striking result.[9]

Theorem 5.10. There are at most two real quadratic number fields K for which $\mathbb{Z}_K$ is a UFD but K is not Euclidean.

---

[6] Weinberger, P. J. *On Euclidean rings of algebraic integers.* Analytic number theory (Proc. Sympos. Pure Math., Vol. XXIV, St. Louis Univ., St. Louis, Mo., 1972), pp. 321–332. Amer. Math. Soc., Providence, R. I., 1973.

[7] Clark, D. A. *A quadratic field which is Euclidean but not norm-Euclidean.* Manuscripta Math. **83** (1994), no. 3–4, 327–330.

[8] Harper, M. $\mathbb{Z}[\sqrt{14}]$ *is Euclidean.* Canad. J. Math. **56** (2004), no. 1, 55–70.

[9] Narkiewicz, W. *Euclidean algorithm in small abelian fields.* Funct. Approx. Comment. Math. **37** (2007), part 2, 337–340.

Sadly, the method of proof (which goes back to Harper and Murty[10]) does not allow one to pin down the exceptions, in the unlikely event that they exist.

[10]Harper, M.; Murty, M. R. *Euclidean rings of algebraic integers.* Canad. J. Math. **56** (2004), no. 1, 71–76.

Exercises

(1) Let K be an imaginary quadratic field. Show that $U(\mathbb{Z}_K)$ coincides with the collection of complex roots of unity contained in K.

For the next two exercises (only!), we drop our requirement that rings are always commutative.

(2) Let $\mathbb{H}$ be the $\mathbb{Q}$-vector space with basis $\{1, i, j, k\}$. We define a multiplication on $\mathbb{H}$ by declaring that 1 is the identity, that $i^2 = j^2 = k^2 = -1$, and that

$$ij = -ji = k, \quad jk = -kj = i, \quad ki = -ik = j.$$

We extend the multiplication to all of $\mathbb{H}$ by bilinearity. It is straightforward (if tedious) to check that this makes $\mathbb{H}$ into a noncommutative ring, the so-called **rational quaternions**. If $\alpha = a+bi+cj+dk \in \mathbb{H}$, its **conjugate** $\bar{\alpha}$ is the element $a-bi-cj-dk$.[11] We define the **norm of** α by $\mathrm{N}\alpha = \alpha\bar{\alpha}$.

Let $\alpha, \beta \in \mathbb{H}$. Prove the following assertions.

(a) $\overline{\alpha+\beta} = \bar{\alpha} + \bar{\beta}$, $\overline{\alpha\beta} = \bar{\beta}\bar{\alpha}$, and $\bar{\bar{\alpha}} = \alpha$.
(b) $\mathrm{N}(\alpha\beta) = \mathrm{N}\alpha \cdot \mathrm{N}\beta$.
(c) If $\alpha = a + bi + cj + dk$, then $\mathrm{N}\alpha = a^2 + b^2 + c^2 + d^2$.
(d) If $\alpha \neq 0$, then α is invertible; in fact, $\alpha^{-1} = \frac{1}{\mathrm{N}\alpha} \cdot \bar{\alpha}$.

(3) (continued) An element $a+bi+cj+dk \in \mathbb{H}$ is called **integral** (in the sense of Hurwitz) if all of $a, b, c, d \in \mathbb{Z}$, or if all of $a, b, c, d \in \frac{1}{2} + \mathbb{Z}$. We denote the set of integral quaternions by $\mathbb{Z}_{\mathbb{H}}$.

(a) Show that $\mathbb{Z}_{\mathbb{H}}$ is a subring of $\mathbb{H}$ and is stable under conjugation (i.e., the conjugate of an element of $\mathbb{Z}_{\mathbb{H}}$ also lies in $\mathbb{Z}_{\mathbb{H}}$).
(b) Show that if $\alpha \in \mathbb{Z}_{\mathbb{H}}$, then $\mathrm{N}\alpha \in \mathbb{Z}$.
(c) Show that an element of $\mathbb{Z}_{\mathbb{H}}$ is a unit exactly when it has norm 1. Use this to determine $U(\mathbb{Z}_{\mathbb{H}})$. (You should find that $\#U(\mathbb{Z}_{\mathbb{H}}) = 24$.)
(d) Show that for every $\theta \in \mathbb{H}$, there is a $\xi \in \mathbb{Z}_{\mathbb{H}}$ with $\mathrm{N}(\theta - \xi) < 1$.
(e) Deduce from (d) that if $\alpha, \beta \in \mathbb{Z}_{\mathbb{H}}$, and $\beta \neq 0$, then there are $\xi, \rho \in \mathbb{Z}_{\mathbb{H}}$ with $\alpha = \beta\xi + \rho$ and $\mathrm{N}\rho < \mathrm{N}\beta$.
(f) Show that every right ideal of $\mathbb{Z}_{\mathbb{H}}$ is principal.

[11] Here and below, we write a instead of the more cumbersome $a \cdot 1$.

(4) (Dedekind[12], Hasse[13]; cf. Greene[14]) Let R be an integral domain. We say a function $n\colon R \to \mathbb{Z}_{\geq 0}$ is a **Dedekind–Hasse function** on R if:

- $n(\alpha) = 0 \iff \alpha = 0$, *and*
- for all nonzero $\alpha, \beta \in R$, either $\beta \mid \alpha$, or there are $\gamma, \delta \in R$ with $0 < n(\alpha\gamma - \beta\delta) < n(\beta)$.

A domain that admits a Dedekind–Hasse function is called **almost Euclidean**. (Before reading on, convince yourself that every Euclidean domain is "almost Euclidean", so that the terminology makes sense.)

(a) Show that an almost Euclidean domain is a PID.

(b) Prove that every PID is almost Euclidean. *Hint:* Suppose R is a PID. Set $n(0) = 0$, set $n(\alpha) = 1$ if α is a unit, and set $n(\alpha) = 2^r$ if $\alpha = \pi_1 \cdots \pi_r$ for irreducibles $\pi_1, \ldots, \pi_r$. Show that $n(\cdot)$ is a Dedekind–Hasse function on R.

(c) Suppose now that R is the ring of integers of a quadratic field. Show that if R is a PID, then the map $n(\alpha) = |\mathrm{N}\alpha|$ is a Dedekind–Hasse function on R.

---

[12] Dedekind, R. *Charakteristische Eigenschaft einklassiger Körper* Ω. Nachlaß, Werke, Bd. 2 (1931), 373–375.

[13] Hasse, H. *Über eindeutige Zerlegung in Primelemente oder in Primhauptideale in Integritätsbereichen*, J. reine angew. Math. **159** (1928), 3–12.

[14] Greene, J. *Principal ideal domains are almost Euclidean.* Amer. Math. Monthly **104** (1997), no. 2, 154–156.

6

Ideal theory for quadratic fields

Throughout this chapter, K denotes an arbitrary quadratic number field. Our principal aim is to prove the Fundamental Theorem of Ideal Theory for these fields. In fact, we will prove two versions of this important result.

Theorem 6.1 (Fundamental theorem of ideal theory, version 1)**.** The monoid $\mathrm{Id}(\mathbb{Z}_K)$ of nonzero ideals of $\mathbb{Z}_K$ is a UFM.

Recall that $\mathrm{Id}(\mathbb{Z}_K)$ has no nontrivial units. Thus, Theorem 6.1 tells us that every nonzero ideal of $\mathbb{Z}_K$ can be written uniquely as a product of prime (or, equivalently for a UFM, irreducible) elements of $\mathrm{Id}(\mathbb{Z}_K)$, with the only ambiguity being the order of the factors.

In the last sentence, "prime" is meant in the monoidal sense: a prime of $\mathrm{Id}(\mathbb{Z}_K)$ is a nonzero ideal that divides a factor whenever it divides a product. This would appear to be somewhat unfortunate terminology, since "prime ideal" already has a well-established meaning in ring theory: a **prime ideal of** R is a proper ideal such that

$$\text{for all } \alpha, \beta \in R, \quad \alpha\beta \in P \implies \alpha \in P \text{ or } \beta \in P.$$

Thankfully, we can — and will — show that the two definitions are in agreement; a nonzero ideal of $\mathbb{Z}_K$ is prime in the monoidal sense exactly when it is prime in the ring-theoretic sense. Hence, Theorem 6.1 may be restated as follows.

Theorem 6.2 (Fundamental theorem of ideal theory, version 2)**.** Every nonzero ideal of $\mathbb{Z}_K$ can be written as a product of nonzero prime ideals in exactly one way (up to the order of the factors).

Standard bases

In Chapter 3, we showed that the elements $1, \tau$ form a $\mathbb{Z}$-basis for $\mathbb{Z}_K$, where

$$\tau = \begin{cases} \sqrt{d} & \text{if } d \equiv 2,3 \pmod 4, \\ \frac{1+\sqrt{d}}{2} & \text{if } d \equiv 1 \pmod 4. \end{cases}$$

Our first order of business is to determine $\mathbb{Z}$-bases for the nonzero ideals of $\mathbb{Z}_K$.

Lemma 6.3. Let I be a nonzero ideal of $\mathbb{Z}_K$. Then I contains a nonzero rational integer as well as an element $a + b\tau$ with $b \neq 0$.

Proof. Choose any nonzero element α of I. Then $N\alpha$ is a nonzero rational integer. Since $N\alpha = \alpha\bar{\alpha}$ is a $\mathbb{Z}_K$-multiple of α, clearly $N\alpha \in I$. This proves the first half of the lemma. For the second, take any nonzero rational integer $m \in I$ and observe that $m\tau \in I$. □

Proposition 6.4. Let I be a nonzero ideal of $\mathbb{Z}_K$. Choose $n \in \mathbb{Z}^+$ as a generator of the ideal of rational integers contained in I, i.e., so that

$$n\mathbb{Z} = I \cap \mathbb{Z}.$$

Choose $B \in \mathbb{Z}^+$ to generate the ideal[1] of "τ-components" of elements of I; in other words,

$$B\mathbb{Z} = \{b \in \mathbb{Z} : a + b\tau \in I \text{ for some } a \in \mathbb{Z}\}.$$

Finally, choose $A \in \mathbb{Z}$ with $A + B\tau \in I$. Then $n, A + B\tau$ form a $\mathbb{Z}$-basis for I.

A $\mathbb{Z}$-basis for I obtained by the recipe of Proposition 6.4 is called a **standard basis**. It is unique up to the choice of A, which is only determined modulo n.

Proof. That n and B can be chosen to be positive follows from Lemma 6.3, which guarantees that the ideals of $\mathbb{Z}$ in question are nonzero. Now take an arbitrary element $a + b\tau \in I$. By the choice of B, we have that $b = Bs$ for some $s \in \mathbb{Z}$. Then

$$(a + b\tau) - s(A + B\tau) \in I \cap \mathbb{Z},$$

[1] If you don't already believe it, take a second to convince yourself that this really is an ideal of $\mathbb{Z}$.

so that by the definition of n,

$$a + b\tau = rn + s(A + B\tau)$$

for some $r \in \mathbb{Z}$. Hence $n, A + B\tau$ span I. Since n and B are nonzero, the $\mathbb{Z}$-independence of $n, A + B\tau$ is implied by the already known $\mathbb{Z}$-independence of $1, \tau$. □

Ideal norms

Definition 6.5. For each nonzero ideal I of $\mathbb{Z}_K$, the **norm of** I is defined by

$$\mathrm{N}(I) = \#\mathbb{Z}_K/I.$$

It is not a priori clear that the norm of an ideal is always finite. In fact, this (and a bit more) follows immediately from our work on standard bases.

Proposition 6.6. For every nonzero ideal I of $\mathbb{Z}_K$, the quotient $\mathbb{Z}_K/I$ is a finite ring. In fact, if I is a nonzero ideal of $\mathbb{Z}_K$ and $n, A + B\tau$ is a standard basis for I, then $\mathrm{N}(I) = nB$.

Proof. The elements $\{a + b\tau : 0 \le a < n, 0 \le b < B\}$ form a complete, irredundant set of coset representatives for $\mathbb{Z}_K/I$. We leave the easy check to the reader. □

It might seem strange to use the word "norm" in Definition 6.5, since the ideal norm does not bear any obvious relation to the elementwise norm defined in Chapter 3. The choice of terminology is justified by the next theorem. For each nonzero ideal I of $\mathbb{Z}_K$, we let $\tilde{I}$ denote the image of I under the nontrivial automorphism of K. Observe that $\tilde{I}$ is itself a nonzero ideal of $\mathbb{Z}_K$.

Theorem 6.7. Let I be a nonzero ideal of $\mathbb{Z}_K$. Then

$$I\tilde{I} = \langle \mathrm{N}(I) \rangle.$$

We need one preliminary observation before we can establish this fundamental result.

Lemma 6.8. Let I be a nonzero ideal with standard basis $n, A + B\tau$. Then $B \mid A$ and $B \mid n$.

Proof. Since $n\tau \in I$, our choice of B immediately implies that $B \mid n$. To see that $B \mid A$, we first write τ^2 in terms of the $\mathbb{Z}$-basis $1, \tau$. Since τ is a root of its field polynomial $x^2 - \mathrm{Tr}(\tau)x + \mathrm{N}\tau$, we have

$$\tau^2 = -\mathrm{N}(\tau) + \mathrm{Tr}(\tau) \cdot \tau.$$

Hence,

$$\begin{aligned}(A + B\tau)\tau &= A\tau + B(-\mathrm{N}\tau + \mathrm{Tr}(\tau) \cdot \tau) \\ &= -B \cdot \mathrm{N}\tau + (A + B \cdot \mathrm{Tr}(\tau))\tau.\end{aligned}$$

Since $(A + B \cdot \mathrm{Tr}(\tau))\tau \in I$, the definition of B shows that B divides $A + B \cdot \mathrm{Tr}(\tau)$. Thus, $B \mid A$. □

Proof of Theorem 6.7. Choose a standard basis $n, A + B\tau$ for I. Since $\mathbb{Z} \subseteq \mathbb{Z}_K$, any $\mathbb{Z}$-basis for I also generates I as an ideal; thus, $I = \langle n, A + B\tau \rangle$. By Lemma 6.8, $n' := n/B$ and $A' := A/B$ are integers, and so we can write

$$I = \langle B \rangle \cdot \langle n',\ A' + \tau \rangle.$$

Applying the nontrivial automorphism of $K/\mathbb{Q}$ to both sides (and continuing to denote this with a tilde),

$$\tilde{I} = \langle B \rangle \cdot \langle n',\ A' + \tilde{\tau} \rangle.$$

Hence,

$$I\tilde{I} = \langle B^2 \rangle \cdot \langle n'^2,\ n'(A' + \tilde{\tau}),\ n'(A' + \tau),\ \mathrm{N}(A' + \tau) \rangle. \tag{6.1}$$

Observe that

$$N(A' + \tau) = (A' + \tau) \cdot (A' + \tilde{\tau}) \in \langle n', A' + \tau \rangle,$$

so that

$$B \cdot N(A' + \tau) \in \langle B \rangle \cdot \langle n', A' + \tau \rangle = I.$$

Since n generates $I \cap \mathbb{Z}$, it follows that $n \mid B \cdot N(A' + \tau)$, and hence $n' \mid N(A' + \tau)$. Thus, all of the generators of the last ideal in (6.1) are divisible by n'; factoring this out,

$$I\tilde{I} = \langle B^2 n' \rangle \cdot \langle n',\ A' + \tilde{\tau},\ A' + \tau,\ \mathrm{N}(A' + \tau)/n' \rangle.$$

As we argue below, the second factor is $\langle 1 \rangle$. Thus,

$$I\tilde{I} = \langle B^2 n' \rangle = \langle (Bn')B \rangle = \langle nB \rangle.$$

The proof of the theorem is completed by recalling that $\mathrm{N}(I) = nB$, by Proposition 6.6.

To prove the remaining claim, notice that the ideal in question contains the ideal of $\mathbb{Z}$ generated by

$$n', \quad \frac{\mathrm{N}(A'+\tau)}{n'}, \quad \text{and} \quad (A'+\tau)+(A'+\tilde{\tau}) = \mathrm{Tr}(A'+\tau). \tag{6.2}$$

If we can show that this ideal of $\mathbb{Z}$ contains 1, we are home free. Since $\mathbb{Z}$ is a PID, our $\mathbb{Z}$-ideal contains 1 unless the three integers (6.2) share a common factor $g > 1$. In that case, $g^2 \mid n' \cdot \frac{\mathrm{N}(A'+\tau)}{n'} = \mathrm{N}(A'+\tau)$, and hence

$$\mathrm{N}\left(\frac{A'+\tau}{g}\right) \in \mathbb{Z}.$$

Moreover, since $g \mid \mathrm{Tr}(A'+\tau)$,

$$\mathrm{Tr}\left(\frac{A'+\tau}{g}\right) \in \mathbb{Z}.$$

Since the norm and trace of $\frac{A'+\tau}{g}$ are rational integers, $\frac{A'+\tau}{g} \in \mathbb{Z}_K$ (Proposition 3.5). This contradicts that $1, \tau$ is a $\mathbb{Z}$-basis for $\mathbb{Z}_K$. □

Theorem 6.7 is extremely useful; we illustrate this with two corollaries indicating that the ideal norm is better behaved than one might guess from its initial definition.

Corollary 6.9. For any pair of nonzero ideals I and J, $\mathrm{N}(IJ) = \mathrm{N}(I)\mathrm{N}(J)$.

Proof. The result almost proves itself. From Theorem 6.7,

$$\langle \mathrm{N}(IJ) \rangle = IJ \cdot \widetilde{IJ} = I\tilde{I} \cdot J\tilde{J} = \langle \mathrm{N}(I) \rangle \langle \mathrm{N}(J) \rangle = \langle \mathrm{N}(I)\mathrm{N}(J) \rangle.$$

As a consequence,

$$\frac{\mathrm{N}(IJ)}{\mathrm{N}(I)\mathrm{N}(J)} \in \mathbb{Z}_K \cap \mathbb{Q} \subseteq \tilde{\mathbb{Z}} \cap \mathbb{Q} = \mathbb{Z},$$

and similarly for the reciprocal $\frac{\mathrm{N}(I)\mathrm{N}(J)}{\mathrm{N}(IJ)}$. Thus,

$$\mathrm{N}(I)\mathrm{N}(J) = \pm \mathrm{N}(IJ).$$

Since ideal norms are positive, we take the + sign. □

We have already met the second corollary. It appeared as Lemma 5.9 in Chapter 5, where it was used to prove Motzkin's theorem on Euclidean imaginary quadratic fields.

Corollary 6.10. For every nonzero $\alpha \in \mathbb{Z}_K$,

$$N(\langle \alpha \rangle) = |N\alpha|.$$

Proof. By Theorem 6.7, $\langle N(\langle \alpha \rangle) \rangle = \langle \alpha \rangle \cdot \langle \tilde{\alpha} \rangle = \langle N\alpha \rangle$. Reasoning as in the last proof, the integers $N(\langle \alpha \rangle)$ and $N\alpha$ differ by at most a sign. Since ideal norms are positive, the result follows. □

Final preparations

It might seem that our lengthy discussion of norms was an unnecessary distraction from our primary mission, proving the fundamental theorem. In fact, the results of the last section will play an essential role in the proofs of Theorems 6.1 and 6.2. The following lemma, which is a weak consequence of Theorem 6.7, is especially pivotal.

Lemma 6.11 (Principal multiple lemma)**.** Let I be a nonzero ideal of $\mathbb{Z}_K$. There is a nonzero ideal J of $\mathbb{Z}_K$ for which IJ is principal.

Proof. By Theorem 6.7, we can take $J = \tilde{I}$. □

Let us use Lemma 6.11 to prove that $\mathrm{Id}(\mathbb{Z}_K)$ is cancellative. We begin with an easy special case.

Lemma 6.12. Let I be a nonzero principal ideal of $\mathbb{Z}_K$. If J and J' are nonzero ideals of $\mathbb{Z}_K$ for which $IJ = IJ'$, then $J = J'$.

It is convenient before giving the proof to introduce **dilations** of an ideal. For a nonzero ideal I of $\mathbb{Z}_K$ and a nonzero $\alpha \in K$, the **dilation of I by the factor α** is the subset of K defined by

$$\alpha I := \{\alpha\beta : \beta \in I\}.$$

The set αI is a $\mathbb{Z}_K$-submodule of K; in other words, it is closed under addition and absorbs multiplication from $\mathbb{Z}_K$. Thus, it is an ideal of $\mathbb{Z}_K$ whenever it is contained in $\mathbb{Z}_K$.

Proof of Lemma 6.12. Write $I = \langle \alpha \rangle$. The hypothesis $IJ = IJ'$ implies that $\alpha J = \alpha J'$. Now dilate both sides by α^{-1}. □

Theorem 6.13. The monoid $\mathrm{Id}(\mathbb{Z}_K)$ is cancellative. In other words, for any nonzero ideals I, J, J' with $IJ = IJ'$, we have $J = J'$.

Proof. Using Lemma 6.11, choose a nonzero ideal I' with $I'I$ principal. Multiply the given equation $IJ = IJ'$ through by I', then cancel $I'I$ using Lemma 6.12. □

The following linchpin result is summed up in the mantra

"To contain is to divide".

Learn it, live it, love it!

Theorem 6.14. Let I and J be nonzero ideals of $\mathbb{Z}_K$. Then I contains $J \iff I$ divides J.

Proof. The backward direction ($\Leftarrow$) follows from the definition of ideal multiplication and holds in any ring. So we only prove the forward direction ($\Rightarrow$).

Suppose $I \supseteq J$. We are seeking an ideal H with $J = IH$. As motivation, *assume* that $J = IH$. Multiply both sides by I', where I' is chosen so that $I'I$ is a nonzero principal ideal, say $\langle\alpha\rangle$. Then $I'J = I'IH = \alpha H$. Dilating by α^{-1},

$$H = \alpha^{-1}I'J.$$

For the actual proof, we simply define H by this last equation and show that H is an ideal of $\mathbb{Z}_K$ with $IH = J$. Since $J \subseteq I$,

$$I'J \subseteq I'I = \langle\alpha\rangle.$$

Hence, $H = \alpha^{-1}I'J$ is contained in $\mathbb{Z}_K$ and so is an ideal of $\mathbb{Z}_K$. Moreover,

$$IH = I(\alpha^{-1}I'J) = \alpha^{-1}II' \cdot J = \alpha^{-1}\langle\alpha\rangle \cdot J = \langle 1\rangle \cdot J = J,$$

as desired. □

The Fundamental Theorem, at last!

It is smooth sailing from here on out. Proposition 4.5 shows that Theorem 6.1 is implied by the next two results. Taking advantage of our previous work, both have short, simple proofs.

Lemma 6.15 (Id($\mathbb{Z}_K$) is atomic)**.** Every element of Id($\mathbb{Z}_K$) factors as a product of irreducible elements of Id($\mathbb{Z}_K$). Here the unit ideal is considered to be the empty product of irreducibles.

Lemma 6.16. Every irreducible element of $\mathrm{Id}(\mathbb{Z}_K)$ is prime (in the monoidal sense).

Proof of Lemma 6.15. If a counterexample exists, choose one with minimal ideal norm. This cannot be irreducible, so it factors as IJ, where $I, J \neq \langle 1 \rangle$. Since a nonunit ideal has norm larger than 1, we deduce from the multiplicativity of the norm that $\mathrm{N}(I)$ and $\mathrm{N}(J)$ are smaller than the norm of our minimal counterexample. Hence, I and J factor as products of irreducibles. But then IJ does as well, a contradiction. □

Proof of Lemma 6.16. Let P be an irreducible element of $\mathrm{Id}(\mathbb{Z}_K)$ that divides a product of nonzero ideals IJ. We assume that P does not divide I and argue that P divides J. Since "to contain is to divide", $P \not\supseteq I$, and so $P + I \supsetneq P$. By another application of "to contain is to divide", $P + I$ is a proper divisor of P. But P is irreducible, and so

$$P + I = \langle 1 \rangle.$$

Multiplying through by J,

$$PJ + IJ = J.$$

We are given that P divides IJ. Thus, the left-hand side is a multiple of P, and hence so is the right-hand side. □

This completes the proof of version 1 of the Fundamental Theorem (Theorem 6.1). To prove version 2 (Theorem 6.2), we argue that a nonzero ideal of $\mathbb{Z}_K$ is monoidally prime if and only if it is ring-theoretically prime. Since "to contain is to divide", the following lemma does the trick.

Lemma 6.17. Let R be a commutative ring, and let P be a proper ideal of R. Then P is prime in the ring-theoretic sense $\iff$ whenever $P \supseteq IJ$ for ideals I, J of R, either $P \supseteq I$ or $P \supseteq J$.

Proof. The backward implication ($\Leftarrow$) is immediate, letting I and J be arbitrary principal ideals. For the forward direction ($\Rightarrow$), assume that P is prime and $P \supseteq IJ$. Supposing that $P \not\supseteq I$, we argue that $P \supseteq J$. Fix $\alpha \in I \setminus P$. Let β be an arbitrary element of J. Since $\alpha\beta \in P$ and $\alpha \notin P$, we have $\beta \in P$. Hence, $J \subseteq P$, as desired. □

Exercises

In the following exercises, K is an arbitrary quadratic field.

(1) Verify the claim made in the proof of Proposition 6.6.

(2) Let I and I' be nonzero ideals of $\mathbb{Z}_K$, and factor $I = \prod_P P^{e_P}$ and $I' = \prod_P P^{e'_P}$, where P runs over the nonzero prime ideals of $\mathbb{Z}_K$, each $e_P, e'_P \in \mathbb{Z}_{\geq 0}$, and e_P and e'_P vanish for all but finitely many P. Show that

$$I + I' = \prod_P P^{\min\{e_P, e'_P\}}, \quad \text{and} \quad I \cap I' = \prod_P P^{\max\{e_P, e'_P\}}.$$

(3) A **fractional ideal** of $\mathbb{Z}_K$ is any dilation of a nonzero ideal of $\mathbb{Z}_K$ by a nonzero element of K.

(a) If I and J are fractional ideals of $\mathbb{Z}_K$, define the product IJ in the same way as for ordinary ideals, namely the $\mathbb{Z}$-span of $\{\alpha\beta : \alpha \in I, \beta \in J\}$. Show that IJ is again a fractional ideal.

(b) Show that for each fractional ideal I, there is a fractional ideal J with $IJ = \mathbb{Z}_K$.

(c) One deduces easily from (a) and (b) that the set of fractional ideals forms a group, say $\mathrm{Frac}(\mathbb{Z}_K)$. Show that every element of $\mathrm{Frac}(\mathbb{Z}_K)$ admits a unique representation in the form

$$\prod_P P^{e_P}, \tag{6.3}$$

where P runs over all nonzero prime ideals of $\mathbb{Z}_K$, the e_P are integers, and all but finitely many e_P vanish. (Thus, $\mathrm{Frac}(\mathbb{Z}_K)$ is a free abelian group with basis the nonzero prime ideals.)

(4) Let P be a fixed, nonzero prime ideal of $\mathbb{Z}_K$. We define a map $\mathrm{ord}_P : K \to \mathbb{Z} \cup \{\infty\}$ (the **P-adic valuation**) as follows. Set $\mathrm{ord}_P(0) = \infty$. For each $\alpha \in K^\times$, decompose the fractional ideal $\alpha\mathbb{Z}_K$ in the form (6.3), and let $\mathrm{ord}_P(\alpha)$ be the corresponding exponent on P. Show:

(a) $\mathrm{ord}_P(\alpha) \geq 0$ for every $P \iff \alpha \in \mathbb{Z}_K$,

(b) if $\alpha \in \mathbb{Z}_K$ and P is any nonzero prime ideal of $\mathbb{Z}_K$, then $\mathrm{ord}_P(\alpha) = 0 \iff \alpha \notin P$.

(c) if $\alpha \in K$ and P is any nonzero prime ideal of $\mathbb{Z}_K$, then

$$\mathrm{ord}_P(\alpha) \geq 0 \iff \alpha = \frac{\gamma}{\delta} \text{ for some } \gamma, \delta \in \mathbb{Z}_K \text{ with } \delta \notin P.$$

Hint for the forward direction in (c): We can assume $\alpha \neq 0$. Write $\alpha\mathbb{Z}_K = IJ^{-1}$ where I and J are coprime nonzero ideals of $\mathbb{Z}_K$ and P does not divide J. Show that δ can be chosen as any element of $J \setminus P$.

(5) (continuation) Let P be a nonzero prime ideal of $\mathbb{Z}_K$. Let $\alpha, \beta \in K$. Prove that:
   (a) $\mathrm{ord}_P(\alpha\beta) = \mathrm{ord}_P(\alpha) + \mathrm{ord}_P(\beta)$,
   (b) $\mathrm{ord}_P(\alpha + \beta) \geq \min\{\mathrm{ord}_P(\alpha), \mathrm{ord}_P(\beta)\}$,
   (c) as long as $\mathrm{ord}_P(\alpha) \neq \mathrm{ord}_P(\beta)$, we have $\mathrm{ord}_P(\alpha + \beta) = \min\{\mathrm{ord}_P(\alpha), \mathrm{ord}_P(\beta)\}$.

   Hint for (b) and (c): First, fix $\pi \in P$. Multiplying α and β by a (possibly large) power of π, reduce to the cases where $\mathrm{ord}_P(\alpha), \mathrm{ord}_P(\beta) \geq 0$. For these, represent α, β in the form described in Exercise 4(c).

7

Prime ideals in quadratic number rings

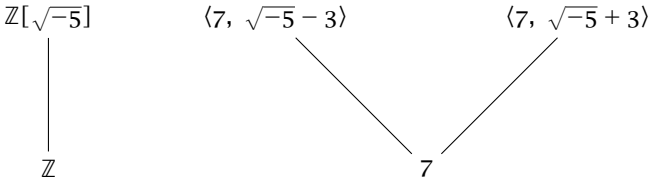
Let K be a number field. The fundamental theorem of ideal theory asserts that the nonzero prime ideals of $\mathbb{Z}_K$ are the building blocks of ideal arithmetic in the same way that the usual prime numbers are the building blocks of integer arithmetic. In this chapter, we give an explicit description of these building blocks in the case when K is a quadratic number field.

The origin story of a prime ideal

We begin by showing that each nonzero prime ideal of $\mathbb{Z}_K$ is a "descendant" of a unique rational prime p.

Definition 7.1. A nonzero ideal prime ideal P of $\mathbb{Z}_K$ is said to **lie above** the rational prime number p if $P \mid \langle p \rangle$. We also say that p **lies below** P.

Figure 7.1. A family tree; 7 along with the two prime ideals lying above it in $\mathbb{Z}[\sqrt{-5}]$. See Example 7.4.



Proposition 7.2. Every nonzero prime ideal P of $\mathbb{Z}_K$ lies above a unique rational prime p. Here p is that rational prime for which

$$P \cap \mathbb{Z} = p\mathbb{Z}.$$

Proof. Since P is a prime ideal of $\mathbb{Z}_K$, the intersection $P \cap \mathbb{Z}$ is a prime ideal of $\mathbb{Z}$. By Lemma 6.3, $P \cap \mathbb{Z} \neq \{0\}$. Hence, $P \cap \mathbb{Z} = p\mathbb{Z}$ for a uniquely determined rational prime p. Clearly, $p \in P$, and so $P \mid \langle p \rangle$ ("to contain is to divide"). It remains to show that P does not lie above another rational prime, say p'. If $P \mid \langle p' \rangle$, then

$$P \supseteq \langle p, p' \rangle \supseteq p\mathbb{Z} + p'\mathbb{Z} = \gcd(p, p')\mathbb{Z} = \mathbb{Z};$$

hence $1 \in P$, so that $P = \langle 1 \rangle$. This contradicts that P is prime. □

Proposition 7.2 reduces the problem of finding the prime ideals of $\mathbb{Z}_K$ to that of determining the prime ideal decomposition of $\langle p \rangle$, as p ranges over the rational primes.

Factorization of rational primes

Let p be a rational prime, and factor $\langle p \rangle$ as a product of not-necessarily distinct prime ideals of $\mathbb{Z}_K$,

$$\langle p \rangle = P_1 P_2 \cdots P_g.$$

Taking norms of both sides, $p^2 = \mathrm{N}(P_1) \cdots \mathrm{N}(P_g)$. Each right-hand factor $\mathrm{N}(P_i)$ is an integer larger than 1. So either $g = 1$, in which case $\langle p \rangle$ is a prime ideal of $\mathbb{Z}_K$ (of norm p^2), or $g = 2$, and

$$\langle p \rangle = P_1 P_2$$

where P_1 and P_2 are prime ideals of norm p. In the first case, we say p is **inert** in $\mathbb{Z}_K$ (or in K). In the second case, we say that p **splits** or **ramifies**, according to whether the prime ideals P_1 and P_2 are distinct or coincide, respectively. Which of these cases we find ourselves in can be read off from the next theorem.

Write $K = \mathbb{Q}(\sqrt{d})$ with d a squarefree. With τ as usual (i.e., as in the statement of Theorem 3.7), let $\min_\tau(x)$ denote the minimal

polynomial of τ over $\mathbb{Q}$, so that

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

Theorem 7.3. Let p be a rational prime. The prime ideal decomposition of $\langle p \rangle$ in $\mathbb{Z}_K$ mirrors the prime factorization of $\min_\tau(x) \bmod p$ in $(\mathbb{Z}/p\mathbb{Z})[x]$. More precisely, if $\min_\tau(x)$ is irreducible mod p, then $\langle p \rangle$ is inert. If instead

$$\min_\tau(x) \equiv (x-a)(x-b) \pmod p,$$

then

$$\langle p \rangle = P_1 P_2$$

where

$$P_1 = \langle p,\ \tau - a \rangle, \quad P_2 = \langle p,\ \tau - b \rangle$$

are prime ideals of norm p. The ideals P_1 and P_2 are distinct precisely when $x-a$ and $x-b$ are distinct mod p.

Example 7.4. Using Theorem 7.3, we determine the prime ideals above each of 2, 3, 5, 7, and 11 in $\mathbb{Z}_K$ when $K = \mathbb{Q}(\sqrt{-5})$. Note that $\min_\tau(x) = x^2 + 5$ in this example.

- 2: $x^2 + 5 \equiv (x+1)^2 \pmod 2$. Thus, $\langle 2 \rangle = \langle 2,\ \sqrt{-5}+1 \rangle^2$. Hence, 2 ramifies.
- 3: $x^2 + 5 \equiv x^2 - 1 \equiv (x-1)(x+1) \pmod 3$. Thus, $\langle 3 \rangle = \langle 3,\ \sqrt{-5}-1 \rangle \cdot \langle 3,\ \sqrt{-5}+1 \rangle$. The right-hand factors are distinct, and 3 splits.
- 5: $x^2 + 5 \equiv x^2 \pmod 5$. Thus, $\langle 5 \rangle = \langle 5,\ \sqrt{-5} \rangle^2 = \langle \sqrt{-5} \rangle^2$. So 5 ramifies.
- 7: $x^2 + 5 \equiv x^2 - 9 \equiv (x-3)(x+3) \pmod 7$. Thus, $\langle 7 \rangle = \langle 7,\ \sqrt{-5}-3 \rangle \cdot \langle 7,\ \sqrt{-5}+3 \rangle$. So 7 splits.
- 11: $x^2 + 5$ is irreducible mod 11, so 11 is inert.

The proof of Theorem 7.3 rests on two easy ring-theoretic preliminaries.

Lemma 7.5. The map

$$\begin{aligned} \mathbb{Z}[x] &\to \mathbb{Z}_K \\ f(x) &\mapsto f(\tau) \end{aligned}$$

induces a ring isomorphism $\mathbb{Z}[x]/\langle \min_\tau(x) \rangle \cong \mathbb{Z}_K$.

Proof. Since $\mathbb{Z}_K = \mathbb{Z}[\tau]$ (equation (3.2)), our map is a surjective homomorphism. From the theory of the minimal polynomial, the kernel consists of those $f(x) \in \mathbb{Z}[x]$ divisible, over $\mathbb{Q}$, by $\min_\tau(x)$. For the proof of the lemma, we would like the kernel to consist of those $f(x) \in \mathbb{Z}[x]$ divisible by $\min_\tau(x)$, *but over* $\mathbb{Z}$. Is there a difference? No! Since $\min_\tau(x)$ is monic, long division can be carried out without inverting any elements of $\mathbb{Z}$; hence, whenever the quotient of $f(x)$ by $\min_\tau(x)$ lies in $\mathbb{Q}[x]$, it in fact lies in $\mathbb{Z}[x]$. □

The next result says that if I and J are ideals of a ring R, modding out by $I + J$ is the same as first modding out by I, then modding out by the image of J in R/I. We leave the proof to the reader.

Lemma 7.6. Let R be a ring, and let I and J be ideals of R. Then

$$R/(I+J) \cong \frac{R/I}{(I+J)/I}.$$

Proof of Theorem 7.3. The isomorphism of Lemma 7.5 induces an isomorphism

$$\mathbb{Z}_K/\langle p \rangle \cong \frac{\mathbb{Z}[x]/\langle \min_\tau(x) \rangle}{\langle p \bmod \min_\tau(x) \rangle}.$$

To analyze the right-hand quotient, apply Lemma 7.6 with $R = \mathbb{Z}[x]$, $I = \langle \min_\tau(x) \rangle$, and $J = \langle p \rangle$;

$$\frac{\mathbb{Z}[x]/\langle \min_\tau(x) \rangle}{\langle p \bmod \min_\tau(x) \rangle} \cong \mathbb{Z}[x]/\langle p,\ \min_\tau(x) \rangle.$$

Now apply Lemma 7.6 once more, this time with $R = \mathbb{Z}[x]$, $I = \langle p \rangle$, and $J = \langle \min_\tau(x) \rangle$;

$$\mathbb{Z}[x]/\langle p,\ \min_\tau(x) \rangle \cong \frac{(\mathbb{Z}/p\mathbb{Z})[x]}{\langle \min_\tau(x) \bmod p \rangle}.$$

Since $(\mathbb{Z}/p\mathbb{Z})[x]$ is a PID, this last quotient is a field if $\min_\tau(x)$ is irreducible mod p. So in that case, $\langle p \rangle$ is a prime ideal. (Recall that an ideal is prime precisely when the corresponding quotient is an integral domain.)

Suppose now that $\min_\tau(x)$ factors mod p. Let P_1 and P_2 be the ideals defined in the statement of the theorem. Appealing again to Lemmas 7.5 and 7.6,

$$\begin{aligned}\mathbb{Z}_K/P_1 &\cong \frac{\mathbb{Z}[x]/\langle \min_\tau(x)\rangle}{\langle p \bmod \min_\tau(x),\ x-a \bmod \min_\tau(x)\rangle} \\ &\cong \frac{\mathbb{Z}[x]/p\mathbb{Z}[x]}{\langle x-a \bmod p,\ \min_\tau(x) \bmod p\rangle} \\ &\cong \frac{(\mathbb{Z}/p\mathbb{Z})[x]}{\langle x-a \bmod p\rangle} \cong \mathbb{Z}/p\mathbb{Z}.\end{aligned}$$

(In going from the second line to the third, we used that $x-a$ divides $\min_\tau(x)$, modulo p.) Since $\mathbb{Z}/p\mathbb{Z}$ is a field, P_1 is a prime ideal, of norm $\#\mathbb{Z}/p\mathbb{Z} = p$; completely similar reasoning shows that P_2 is also a prime ideal of norm p.

Let us see why $\langle p\rangle = P_1P_2$. Multiplying out the ideals in terms of the given generators,

$$P_1P_2 = \langle p^2,\ p(\tau-a),\ p(\tau-b),\ (\tau-a)(\tau-b)\rangle.$$

Since $\min_\tau(x) \equiv (x-a)(x-b) \pmod p$,

$$0 \equiv \min_\tau(\tau) \equiv (\tau-a)(\tau-b) \pmod p.$$

Hence, all four of the above generators of P_1P_2 are multiples of p. It follows that $\langle p\rangle \mid P_1P_2$. Since $\langle p\rangle$ and P_1P_2 have the same norm, the cofactor ideal has norm 1, so must be the unit ideal $\langle 1\rangle$. Therefore $\langle p\rangle = P_1P_2$.

It remains to prove that $P_1 = P_2$ exactly when $a \equiv b \pmod p$. It is obvious from the definitions that when $a \equiv b \pmod p$, we have $P_1 = P_2$. Suppose now that $P_1 = P_2$. Then P_2 contains both $\tau - a$ and $\tau - b$, and so contains $b - a$. Thus,

$$P_2 \supseteq p\mathbb{Z} + (b-a)\mathbb{Z} = \gcd(p, b-a)\mathbb{Z}.$$

Since P_2 is not the unit ideal, $\gcd(p, b-a) \neq 1$, and hence $p \mid b-a$. That is, $a \equiv b \pmod p$. □

In any field F of characteristic not equal to 2, the roots of a quadratic polynomial $ax^2 + bx + c$ are given by the usual quadratic formula:

$$\frac{-b \pm \sqrt{\Delta}}{2a}, \quad \text{where} \quad \Delta = b^2 - 4ac. \tag{7.1}$$

The catch here is that the roots are not guaranteed to live in F; it may be necessary to pass to a quadratic extension to obtain a square root of $b^2 - 4ac$. If one is interested only in roots that lie in F, then (7.1) shows that there are 0, 1, or 2 of these according to whether Δ is a nonsquare in F, Δ is zero, or Δ is a nonzero square in F. Combined with Theorem 7.3, this has the following consequence.

Corollary 7.7. Let K be a quadratic field. Write $K = \mathbb{Q}(\sqrt{d})$ with d squarefree. Let p be an odd prime. Then

$$\begin{aligned} p \text{ is inert in } \mathbb{Z}_K &\iff d \equiv \text{nonsquare} \pmod{p}, \\ p \text{ splits in } \mathbb{Z}_K &\iff d \equiv \text{nonzero square} \pmod{p}, \\ p \text{ ramifies in } \mathbb{Z}_K &\iff d \equiv 0 \pmod{p}. \end{aligned}$$

We leave the details of the proof to the reader. We also leave as an exercise the following straightforward consequence of Theorem 7.3 for the splitting behavior of $p = 2$.

Corollary 7.8. Let K be a quadratic field. Write $K = \mathbb{Q}(\sqrt{d})$ with d squarefree. If $d \equiv 5 \pmod 8$, then 2 is inert in $\mathbb{Z}_K$. If $d \equiv 1 \pmod 8$, then 2 splits. If $d \equiv 2, 3 \pmod 4$, then 2 ramifies.

Note that every squarefree d is included in one of the cases of Corollary 7.8.

Exercises

In Exercises 4–6, K denotes an arbitrary quadratic field.

(1) Supply a proof for Lemma 7.6.

(2) Prove Corollaries 7.7 and 7.8.

(3) Let K be a quadratic field for which $\mathbb{Z}_K$ is a PID. Let p be a rational prime. Show that p is not inert in $K \iff$ at least one of $\pm p$ can be written in the form $x^2 + \mathrm{Tr}(\tau)xy + \mathrm{N}(\tau)y^2$, with $x, y \in \mathbb{Z}$.

(4) Let P be a nonzero prime ideal of $\mathbb{Z}_K$.
   (a) Prove that $\mathbb{Z}_K/P$ is a field.
   (b) Show that if P lies above the rational prime p, then $\mathbb{Z}/p\mathbb{Z}$ injects into $\mathbb{Z}_K/P$ via the map sending $a \bmod p \mapsto a \bmod P$.

(5) Let $t = t(K)$ denote the number of rational primes that ramify in $\mathbb{Z}_K$. Show that $1 \le t < \infty$.

(6) Let $f(x)$ be an arbitrary nonconstant polynomial with rational integer coefficients. Show that the congruence $f(x) \equiv 0 \pmod{p}$ has a solution for infinitely many primes p. Taking $f(x) = \min_\tau(x)$, deduce that there are infinitely many primes p that split in $\mathbb{Z}_K$.

Hint for the first part: Mimic Euclid's proof of the infinitude of primes.

(7) (Kohnen[1]) Let $K = \mathbb{Q}(\sqrt{d})$, where $d \equiv 3 \pmod{4}$ is positive and squarefree. We outline a simple proof that there are infinitely many primes that remain inert in $\mathbb{Z}_K$. (The same result holds for any quadratic field, but the general case is trickier. For a much more precise statement, see Exercise 25.11.)

Let $X \ge 2$ be arbitrary, and define

$$P_X = \Big(\prod_{\substack{q \le X \\ q \nmid d}} q \Big)^2 + d.$$

Here the left-hand product extends over all rational primes $q \le X$ not dividing d.

(a) Show that there is at least one rational prime p dividing P_X with $p \equiv 3 \pmod{4}$.

(b) Prove that if p is as in (a), then

$$d^{(p-1)/2} \equiv -1 \pmod{p}.$$

Deduce that d is not a square mod p and therefore p is inert in $\mathbb{Z}_K$.

(c) Show that $p > X$.

Since X can be taken arbitrarily large, (b) and (c) imply that there are infinitely many inert primes in $\mathbb{Z}_K$.

[1] Kohnen, W. *An elementary proof in the theory of quadratic residues.* Bull. Korean Math. Soc. **45** (2008), no. 2, 273–275.

8

Units in quadratic number rings

In Chapter 5 (Lemma 5.8), we determined the group of units $U(\mathbb{Z}_K)$ for all imaginary quadratic fields K: Write $K = \mathbb{Q}(\sqrt{d})$ with d squarefree. Letting $\omega = e^{2\pi i/3}$,

$$U(\mathbb{Z}_K) = \begin{cases} \{\pm 1, \pm i\} & \text{when } d = -1, \\ \{\pm 1, \pm\omega, \pm\omega^2\} & \text{when } d = -3, \\ \{\pm 1\} & \text{otherwise.} \end{cases}$$

In particular, $\#U(\mathbb{Z}_K) \leq 6$, and almost always $\#U(\mathbb{Z}_K) = 2$. In this chapter, we prove a contrasting result for real quadratic fields.

Theorem 8.1. Let K be a real quadratic field. Then $\mathbb{Z}_K$ contains a unit $\epsilon_0 > 1$ with

$$U(\mathbb{Z}_K) = \{\pm\epsilon_0^j : j \in \mathbb{Z}\}.$$

There are two remarks to be made here. First, since $\epsilon_0 > 1$, the powers of ϵ_0 grow without bound. So in contrast with the imaginary quadratic case, $U(\mathbb{Z}_K)$ is an infinite group! In the opposite direction, as infinite abelian groups go, $U(\mathbb{Z}_K)$ is fairly tame. It is finitely generated, and one generator of infinite order suffices.

The element ϵ_0 whose existence is asserted in Theorem 8.1 is easily seen to be unique. (This is because of the condition that $\epsilon_0 > 1$.) It is usual to refer to ϵ_0 as the **fundamental unit** of $\mathbb{Z}_K$.

Later in this text (Chapters 18 and 20), we will determine the structure of $U(\mathbb{Z}_K)$ for all number fields K. Let r_1 denote the number of real embeddings of K and r_2 the number of pairs of nonreal complex

embeddings. Let μ_K denote the group of roots of unity belonging to K, i.e.,

$$\mu_K = \{\zeta \in K : \zeta^m = 1 \text{ for some positive integer } m\}.$$

A moment's thought shows that μ_K is a subgroup of $U(\mathbb{Z}_K)$. **Dirichlet's units theorem** asserts that there is an internal direct product decomposition

$$U(\mathbb{Z}_K) = \mu_K \times \prod_{i=1}^{r_1+r_2-1} \langle \epsilon_i \rangle,$$

for some $\epsilon_1, \ldots, \epsilon_{r_1+r_2-1} \in U(\mathbb{Z}_K)$ of infinite order. The reader should pause briefly to check that this is consistent with both Lemma 5.8 and Theorem 8.1 (cf. Exercise 5.1).

Déjà vu

The following lemma has been applied several times already when K is imaginary quadratic. Since we need it here for real quadratic K, we give the proof. The attentive reader will find it very familiar.

Table 8.1. Fundamental units in the ring of integers of $\mathbb{Q}(\sqrt{d})$ for squarefree $d \in [2, 43]$.

2	$1 + \sqrt{2}$	23	$24 + 5\sqrt{23}$
3	$2 + \sqrt{3}$	26	$5 + \sqrt{26}$
5	$\frac{1}{2}(1 + \sqrt{5})$	29	$\frac{1}{2}(5 + \sqrt{29})$
6	$5 + 2\sqrt{6}$	30	$11 + 2\sqrt{30}$
7	$8 + 3\sqrt{7}$	31	$1520 + 273\sqrt{31}$
10	$3 + \sqrt{10}$	33	$23 + 4\sqrt{33}$
11	$10 + 3\sqrt{11}$	34	$35 + 6\sqrt{34}$
13	$\frac{1}{2}(3 + \sqrt{13})$	35	$6 + \sqrt{35}$
14	$15 + 4\sqrt{14}$	37	$6 + \sqrt{37}$
15	$4 + \sqrt{15}$	38	$37 + 6\sqrt{38}$
17	$4 + \sqrt{17}$	39	$25 + 4\sqrt{39}$
19	$170 + 39\sqrt{19}$	41	$32 + 5\sqrt{41}$
21	$\frac{1}{2}(5 + \sqrt{21})$	42	$13 + 2\sqrt{42}$
22	$197 + 42\sqrt{22}$	43	$3482 + 531\sqrt{43}$

Lemma 8.2. Let K be a quadratic field. An element $\alpha \in \mathbb{Z}_K$ is a unit $\iff \mathrm{N}\alpha = \pm 1$.

Proof. If $\alpha \in U(\mathbb{Z}_K)$, then $\alpha \mid 1$ (in $\mathbb{Z}_K$). Since the norm is multiplicative, $\mathrm{N}\alpha \mid \mathrm{N}(1) = 1$ (in $\mathbb{Z}$). Hence, $\mathrm{N}\alpha = \pm 1$. On the other hand, if $\mathrm{N}\alpha = \pm 1$, then $\alpha^{-1} = \pm\tilde{\alpha} \in \mathbb{Z}_K$, and so $\alpha \in U(\mathbb{Z}_K)$. (As usual, a tilde denotes the action of the nontrivial automorphism of $K/\mathbb{Q}$.) □

Discrete thoughts

To prove Theorem 8.1, it is enough to show that the group of positive units of $\mathbb{Z}_K$ — say $U(\mathbb{Z}_K)^+$ — is infinite cyclic. We turn this multiplicative problem into an additive one via the logarithm. Viewing $\mathbb{R}^+$ as a group under multiplication and $\mathbb{R}$ as a group under addition, the map $\log\colon \mathbb{R}^+ \to \mathbb{R}$ is a group isomorphism, and so

$$U(\mathbb{Z}_K)^+ \cong \log U(\mathbb{Z}_K)^+.$$

Lemma 8.3. $\log U(\mathbb{Z}_K)^+$ is a **discrete** subgroup of $\mathbb{R}$. In other words, it intersects each interval $[-X, X]$ (for arbitrary real $X > 0$) in only finitely many points.

Proof. Since $\log(\epsilon^{-1}) = -\log(\epsilon)$, the set $\log U(\mathbb{Z}_K)^+$ is symmetric about 0. Thus, it is enough to show that this set has finite intersection with every interval of the form $[0, X]$. Assume that $\log \epsilon \in [0, X]$, and write $\epsilon = u + v\sqrt{d}$. Then

$$1 \le \epsilon = u + v\sqrt{d} \le \exp(X).$$

We argue below that that u and v are both nonnegative. Once this is proved, it follows immediately that

$$0 \le u \le \exp(X), \quad \text{and} \quad 0 \le v \le \exp(X).$$

Since u and v are integers or halves of odd integers, these inequalities restrict u and v to a finite set, and hence restrict $\epsilon = u + v\sqrt{d}$ to a finite set.

To prove the claim, notice that since $\epsilon \ge 1$, we have $0 < \epsilon^{-1} \le \epsilon$. Therefore,

$$\epsilon - \epsilon^{-1} \ge 0, \quad \text{and} \quad \epsilon + \epsilon^{-1} > 0.$$

Now either $\epsilon^{-1} = u - v\sqrt{d}$ (if $N(\epsilon) = 1$) or $\epsilon^{-1} = -u + v\sqrt{d}$ (if $N(\epsilon) = -1$). In either case, $\{\epsilon - \epsilon^{-1}, \epsilon + \epsilon^{-1}\} = \{2u, 2v\sqrt{d}\}$. Thus, $u, v \geq 0$, as desired. □

Fortune smiles upon us; there is a simple classification of the discrete subgroups of $\mathbb{R}$.

Lemma 8.4. Let Λ be a discrete subgroup of $\mathbb{R}$. If $\Lambda \neq \{0\}$, then Λ has a smallest positive element v, and

$$\Lambda = \mathbb{Z}v.$$

Proof. Since $\Lambda \neq \{0\}$, there is a nonzero $u \in \Lambda$. We can assume that $u > 0$; otherwise replace u with $-u$. By discreteness, the set $[0, u] \cap \Lambda$ is finite, and thus has a smallest positive element v (say). Clearly, v is also the smallest positive element of Λ.

If $\Lambda \neq \mathbb{Z}v$, then there is a $w \in \Lambda$ strictly between two integer multiples of v, say

$$nv < w < (n+1)v.$$

But then $w - nv$ is a positive element of Λ smaller than v, contradicting the choice of v. □

Lemmas 8.3 and 8.4 show that $\log U(\mathbb{Z}_K)^+$ is either trivial or infinite cyclic. We wish to rule out the former possibility, and so we are left with the task of showing that there is some positive unit in $\mathbb{Z}_K$ other than 1.

A nontrivial unit exists

We are seeking a positive $\epsilon \in \mathbb{Z}_K$, not equal to 1, with $N\epsilon = \pm 1$. To get a feel for where such an ϵ might be hiding, suppose $\epsilon = a + b\sqrt{d}$, with $a, b \in \mathbb{Z}$. (This is not the general case when $d \equiv 1 \pmod 4$, but let's ignore that for now.) The equation $N\epsilon = \pm 1$ becomes

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

Thus, $a^2 \approx db^2$, with the smallest possible nonzero error! This suggests that a/b should be an unusually good approximation to $\sqrt{d}$. Turning this around, we might hope that producing close rational approximations to $\sqrt{d}$ will point us in the direction of our desired ϵ.

In what follows, we use $\{x\}$ to denote the **fractional part** of the real number x, i.e., $x - \lfloor x \rfloor$. We write $\|x\|$ for the distance from x to the nearest integer.

Theorem 8.5 (Dirichlet's approximation theorem)**.** Let x be any real number. For all positive integers Q, there is a positive integer $q \le Q$ with

$$\|qx\| \le \frac{1}{Q+1}.$$

Proof. If we can find a $q \in [1, Q]$ with $\{qx\} \in [0, \frac{1}{Q+1})$ or $\{qx\} \in [1 - \frac{1}{Q+1}, 1)$, then $\|qx\| \le \frac{1}{Q+1}$, and we are done. Otherwise, all of the Q numbers $\{qx\}$, for $1 \le q \le Q$, fall into one of the $Q-1$ intervals $[\frac{1}{Q+1}, \frac{2}{Q+1})$, $[\frac{2}{Q+1}, \frac{3}{Q+1})$, $\ldots$, $[\frac{Q-1}{Q+1}, \frac{Q}{Q+1})$. By the pigeonhole principle, there are integers q_1 and q_2, with $1 \le q_1 < q_2 \le Q$, for which $\{q_1 x\}$ and $\{q_2 x\}$ belong to the same interval. In that case, we may take $q = q_2 - q_1$. □

Theorem 8.5 enables us to write down infinitely many elements of $\mathbb{Z}[\sqrt{d}]$ of bounded norm.

Corollary 8.6. There are infinitely many pairs of positive integers (p, q) with $|p^2 - dq^2| \le 2\sqrt{d}$.

Proof. Let Q be any positive integer. By Theorem 8.5, there are integers p and q with $1 \le q \le Q$ and

$$|p - q\sqrt{d}| \le \frac{1}{Q+1}. \tag{8.1}$$

The integer p is certainly positive, since $q\sqrt{d} > 1$ while $\frac{1}{Q+1} < 1$. For this pair of p and q,

$$\begin{aligned} |p^2 - dq^2| &= |p - q\sqrt{d}| \cdot |p + q\sqrt{d}| \\ &\le |p - q\sqrt{d}| \cdot (|p - q\sqrt{d}| + 2q\sqrt{d}) \\ &\le \frac{1}{Q+1} \cdot \left(\frac{1}{Q+1} + 2q\sqrt{d} \right). \end{aligned}$$

Since $q \le Q$, this is

$$\le \frac{1}{(Q+1)^2} + 2\sqrt{d} \left(1 - \frac{1}{Q+1} \right) \le 2\sqrt{d}.$$

It remains to show that infinitely many distinct pairs of p and q arise as Q ranges over the positive integers. But this follows from (8.1); since $\sqrt{d}$ is irrational, any single pair of p and q can satisfy (8.1) for only finitely many Q. □

How do we get from infinitely many elements of bounded norm to a nontrivial element of norm ± 1? The following lemma is key.

Lemma 8.7. For each real $X > 0$, there are only finitely many nonzero ideals of $\mathbb{Z}_K$ of norm bounded by X.

Proof. It is enough to show that for any given m, there are only finitely many ideals I of norm m. If $\mathrm{N}(I) = m$, then viewing $\mathbb{Z}_K/I$ as a group under addition, elementary group theory shows that

$$\overbrace{1 + 1 + 1 + \cdots + 1}^{m \text{ times}} \equiv 0 \pmod{I}.$$

Since "to contain is to divide", $I \mid \langle m \rangle$. But uniqueness of prime ideal factorization implies that every nonzero ideal of $\mathbb{Z}_K$ — and so $\langle m \rangle$ in particular — has at most finitely many ideal divisors. □

Our nontrivial unit is now within grasp. Consider the ideals of the form $\langle p + q\sqrt{d} \rangle$, where (p, q) ranges over the pairs of positive integers described in Corollary 8.6. For each of these,

$$\mathrm{N}(\langle p + q\sqrt{d} \rangle) = |\mathrm{N}(p + q\sqrt{d})| \leq 2\sqrt{d}.$$

There are infinitely many pairs (p, q) but only finitely many ideals of norm bounded by $2\sqrt{d}$. Hence, we can find distinct pairs (p, q) and (p', q') with

$$\langle p + q\sqrt{d} \rangle = \langle p' + q'\sqrt{d} \rangle.$$

Thus, $p + q\sqrt{d}$ and $p' + q'\sqrt{d}$ are associates, and

$$\frac{p' + q'\sqrt{d}}{p + q\sqrt{d}}$$

is a positive unit of $\mathbb{Z}_K$ not equal to 1. This completes the proof of Theorem 8.1.

Examples

For very small d, it is feasible to calculate the fundamental unit by hand. For instance, take $d = 2$. A careful reading of the proof of Lemma 8.3 shows that any unit $a + b\sqrt{2} > 1$ has both $a > 0$ and $b > 0$, and so is at least of size $1 + \sqrt{2}$. Since $1 + \sqrt{2}$ *is* a unit, it must be the fundamental unit. Playing with the same circle of ideas, one is led to the following naive algorithm, whose detailed justification is left as Exercise 1.

Naive algorithm for finding the fundamental unit. Test $v = 1, 2, 3, \ldots$ until one of $dv^2 \pm 4$ is a square. Choosing the $-$ sign whenever there is a choice, write $u^2 = dv^2 \pm 4$. Output

$$\epsilon_0 = \frac{1}{2}(u + v\sqrt{d}).$$

The naive approach can be quite impractical. For example, the fundamental unit in $\mathbb{Z}[\sqrt{94}]$ is

$$2143295 + 221064\sqrt{94},$$

which would not be discovered until step 442128 of our algorithm! Here (and in most other cases), the following approach via continued fractions is much more efficient.

Recall that every irrational number has a unique infinite expansion of the form

$$a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 + \cfrac{1}{a_4 + \ddots}}}, \tag{8.2}$$

where $a_1 \in \mathbb{Z}$ and $a_2, a_3, a_4, \ldots \in \mathbb{Z}^+$. The associated n**th convergent** is the rational number

$$\frac{p_n}{q_n} = a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 + \cfrac{1}{\ddots + \cfrac{1}{a_n}}}}.$$

Here the integers p_n and q_n are uniquely defined by insisting that the fraction $\frac{p_n}{q_n}$ is in lowest terms. We set

$$p_{-1} = 0,\ q_{-1} = 1 \quad \text{and} \quad p_0 = 1,\ q_0 = 0.$$

With these definitions, it can be shown that

$$p_{n+1} = a_n p_n + p_{n-1}, \quad q_{n+1} = a_n q_n + q_{n-1} \tag{8.3}$$

for all integers $n \geq 0$. The following elegant result appears to be due to Hasse, who published it in Chapter 16 of his *Vorlesungen über Zahlentheorie.*[1]

Theorem 8.8. Let τ be as in Theorem 3.5. Expand the real number $\frac{1}{\{\tau\}}$ in the form (8.2). Then the sequence $a_1, a_2, \ldots$ is purely periodic. If k is the (minimal) period length, then the fundamental unit is given by

$$\epsilon_0 = q_k \frac{1}{\{\tau\}} + q_{k-1}.$$

For example, let $d = 7$, so that $\{\tau\} = \sqrt{7} - 2$. Then

$$\begin{aligned}
\frac{1}{\sqrt{7}-2} &= \frac{\sqrt{7}+2}{3} = 1 + \frac{\sqrt{7}-1}{3}, \\
\frac{3}{\sqrt{7}-1} &= \frac{\sqrt{7}+1}{2} = 1 + \frac{\sqrt{7}-1}{2}, \\
\frac{2}{\sqrt{7}-1} &= \frac{\sqrt{7}+1}{3} = 1 + \frac{\sqrt{7}-2}{3}, \\
\frac{3}{\sqrt{7}-2} &= \sqrt{7}+2 = 4 + \sqrt{7} - 2.
\end{aligned}$$

At this point, we have enough data to conclude that the expansion (8.2) is purely periodic of length 4, with $a_1 = 1, a_2 = 1, a_3 = 1, a_4 = 4$. The recurrence for the q's in (8.3) yields $q_3 = 2$ and $q_4 = 9$. Hence, the fundamental unit of $\mathbb{Z}[\sqrt{7}]$ is

$$\begin{aligned}
\epsilon_0 &= 9 \cdot \frac{1}{\sqrt{7}-2} + 2 \\
&= 9 \cdot \frac{\sqrt{7}+2}{3} + 2 = 8 + 3\sqrt{7}.
\end{aligned}$$

[1] Hasse, H. *Vorlesungen über Zahlentheorie.* Second edition. Die Grundlehren der mathematischen Wissenschaften, **59**. Springer-Verlag, Berlin-New York, 1964.

Exercises

Below, ϵ_0 denotes the fundamental unit of $\mathbb{Z}_K$, where K is a real quadratic field.

(1) Justify the "naive algorithm" for computing ϵ_0.

(2) Let $d \in \mathbb{Z}$. Show that if $d > 1$ and $d^2 - 1$ is squarefree, then $d + \sqrt{d^2-1}$ is the fundamental unit of the ring of integers of $\mathbb{Q}(\sqrt{d^2-1})$. Show that if $d > 2$ and $d^2 + 1$ is squarefree, then $d + \sqrt{d^2+1}$ is the fundamental unit of the ring of integers of $\mathbb{Q}(\sqrt{d^2+1})$.

(3) Let $K = \mathbb{Q}(\sqrt{d})$, where $d > 1$ is squarefree. Show that $\epsilon_0 \in \mathbb{Z}[\sqrt{d}]$ except possibly when $d \equiv 5 \pmod 8$, in which case $\epsilon_0^3 \in \mathbb{Z}[\sqrt{d}]$.

(4) (solvability of **Pell's equation** $x^2 - dy^2 = 1$) Let d be a positive integer that is not a square (but not necessarily squarefree). Show that there is always an element $x + y\sqrt{d} \in \mathbb{Z}[\sqrt{d}]$ of norm 1.

Hint: Let $K = \mathbb{Q}(\sqrt{d})$. Show that there is an $f \in \mathbb{Z}^+$ with $\mathbb{Z} + f\mathbb{Z}_K \subseteq \mathbb{Z}[\sqrt{d}]$. Use this to argue that $x + y\sqrt{d}$ can be chosen as a suitable power of ϵ_0.

(5) Let K be a quadratic field, say $K = \mathbb{Q}(\sqrt{d})$ with d squarefree. When $d < 0$, there is a straightforward procedure for testing if $\mathbb{Z}_K$ contains an element of a given norm $n \in \mathbb{Z}^+$. Namely, exhaustively search $[0, \sqrt{n}] \times [0, \sqrt{n/|d|}]$ for a pair of $x, y \in \mathbb{Z}$ (or possibly also $x, y \in \frac{1}{2} + \mathbb{Z}$) with $x^2 + |d|y^2 = n$.

Now suppose instead that $d > 0$.

(a) We call an element $\beta \in \mathbb{Z}_K$ **primary** if $\beta > 0$ and $1 \le |\beta/\tilde{\beta}| < \epsilon_0^2$. Show that every nonzero element of $\mathbb{Z}_K$ has a unique primary associate.

(b) Suppose $N\epsilon_0 = 1$. Show that if n is a nonzero integer, then n is the norm of an element of $\mathbb{Z}_K \Leftrightarrow n$ is the norm of a primary element.

When $N\epsilon_0 = -1$, show that n is a norm $\Leftrightarrow \pm n$ is the norm of a primary element (for at least one choice of sign).

(c) Show that if β is primary and $N\beta = \pm n$, then $\beta = x + y\sqrt{d}$ where $x, y \ge 0$, and $\beta \le \epsilon_0\sqrt{|n|}$. Thus, $0 \le x \le \epsilon_0\sqrt{|n|}$ and $0 \le y \le \epsilon_0\sqrt{|n|/d}$.

(6) Let $K = \mathbb{Q}(\sqrt{82})$. Show that $\epsilon_0 = 9 + \sqrt{82}$. Then use the results of the last exercise (and a computer) to determine all $n \in \{1, \dots, 100\}$ for which $x^2 - 82y^2 = n$ has an integer solution.

(7) For each real $X > 0$, let $\mathcal{E}(X)$ denote the number of $\epsilon_0 \in [1, X]$ that appear as the fundamental unit of some real quadratic field K. Prove that $\lim_{X\to\infty} \frac{\mathcal{E}(X)}{2X} = 1$. *Hint:* Estimate the number of corresponding minimal polynomials $\min_{\epsilon_0}(x)$.

(8) (Belcher[2]) Let K be a real quadratic field. Write $K = \mathbb{Q}(\sqrt{d})$ with d squarefree. Show that every element of $\mathbb{Z}_K$ can be written as a finite sum of units if and only if either

- $d \equiv 2, 3 \pmod 4$ and $d + 1 = \square$ or $d - 1 = \square$,
- $d \equiv 1 \pmod 4$ and $d + 4 = \square$ or $d - 4 = \square$.

(9) (Ashrafi and Vámos[3]) Let K be a real quadratic field. Show that for every positive integer n, there is an $\alpha \in \mathbb{Z}_K$ not expressible as a sum of n units. *Hint:* Work modulo $\epsilon_0^m - 1$, where m is chosen sufficiently large in terms of n.

[2]Belcher, P. *Integers expressible as sums of distinct units.* Bull. London Math. Soc. **6** (1974), 66–68.

[3]Ashrafi, N.; Vámos, P. *On the unit sum number of some rings.* Q. J. Math. **56** (2005), no. 1, 1–12.

9

A touch of class

A blast from the past

The following problem is a close relative of those we encountered in Chapter 1.

Problem 9.1. Find all integers x and y satisfying $y^2 = x^3 - 5$.

Let us see where the approach of Chapter 1 leads us. Suppose we are in possession of an integer solution x, y. Rearranging and then factoring over $\mathbb{Z}[\sqrt{-5}]$,

$$x^3 = (y + \sqrt{-5})(y - \sqrt{-5}). \tag{9.1}$$

We now argue that the right-hand factors in (9.1) have no common nonunit divisor in $\mathbb{Z}[\sqrt{-5}]$. Any common divisor γ divides $(y+\sqrt{-5}) - (y - \sqrt{-5}) = 2\sqrt{-5}$. Thus,

$$\mathrm{N}\gamma \mid \mathrm{N}(2\sqrt{-5}) = 20.$$

Since $\gamma \mid y + \sqrt{-5}$, we also know that

$$\mathrm{N}\gamma \mid y^2 + 5.$$

Putting the last two displays together,

$$\mathrm{N}\gamma \mid \gcd(20, y^2 + 5) = \gcd(20, x^3).$$

Taking the original equation mod 4, we quickly realize that $2 \nmid x$. Looking at it mod 5, we find that if $5 \mid x$, then $5 \mid y$; but then $5^2 \mid y^2 - x^3 = -5$, which is absurd. So $5 \nmid x$. Thus, x is coprime to 20, and hence x^3 is as well. So $\mathrm{N}\gamma \mid 1$, and γ is a unit in $\mathbb{Z}[\sqrt{-5}]$.

In Chapter 1, we took the following as a working hypothesis in the solution of similar problems.

nth power product principle. If α and β are nonzero elements whose product is an nth power, and α and β have no nonunit common divisor, then α and β are both nth powers, up to multiplication by a unit.

Assume (!) for the moment that this hypothesis is valid for the ring $\mathbb{Z}[\sqrt{-5}]$ and the integer $n = 3$. Both units ± 1 of $\mathbb{Z}[\sqrt{-5}]$ are cubes, and so the power product principle implies that there are integers a, b with

$$\begin{aligned} y + \sqrt{-5} &= (a + b\sqrt{-5})^3 \\ &= (a^3 - 15ab^2) + (3a^2b - 5b^3)\sqrt{-5}. \end{aligned}$$

Since the coefficient of $\sqrt{-5}$ is a multiple of b, it must be that $b = \pm 1$ and that

$$3a^2 - 5 = \pm 1.$$

But there are no integers a satisfying this last equation. We conclude that $y^2 = x^3 - 5$ has no integer solutions.

Or do we?

A proof in peril

It turns out that our optimism was misplaced; the "3rd power product principle" does *not* hold in $\mathbb{Z}[\sqrt{-5}]$. Here is a counterexample:

$$\text{When } \alpha = 2 \text{ and } \beta = 7 + \sqrt{-5}, \quad \alpha\beta = (-1 - \sqrt{-5})^3.$$

Let's make sure we see why our ship is sunk. Certainly α is not a cube in $\mathbb{Z}[\sqrt{-5}]$, since that would force the cubic number field $\mathbb{Q}(\sqrt[3]{2})$ to be a subfield of the quadratic field $\mathbb{Q}(\sqrt{5})$. So the *conclusion* of the "3rd power product principle" fails. What about its *hypothesis*? How do we know that α and β have no common nonunit factor? To see this, let γ be a common divisor of α and β. Then

$$\begin{aligned} \langle \gamma \rangle \supseteq \langle \alpha, \beta \rangle &= \langle 2,\ 7 + \sqrt{-5} \rangle \\ &= \langle 2,\ 1 + \sqrt{-5} \rangle. \end{aligned}$$

Call the final ideal P. In Chapter 7, we saw that P is a prime ideal of norm 2. (In fact, we found there that $\langle 2 \rangle$ factors as P^2.) Since "to contain is to divide", either $\langle \gamma \rangle = \langle 1 \rangle$ or $\langle \gamma \rangle = P$. In the latter case, $N\gamma = 2$, but there are no norm 2 elements in $\mathbb{Z}[\sqrt{-5}]$. So $\langle \gamma \rangle = 1$, and γ is a unit.

Thus, our counterexample is genuine.

...Yet, there is a sense in which it is something of a cheat. While α and β have no common nonunit divisor in $\mathbb{Z}[\sqrt{-5}]$, the ideals $\langle \alpha \rangle$ and $\langle \beta \rangle$ have a nontrivial common *ideal* factor, namely P. This was not forbidden in the statement of the power product principle — after all, we didn't know about ideals when it was formulated — but maybe it should have been. Here is a proposed version 2.0.

modified nth power product principle. If α and β are nonzero elements whose product is an nth power, and $\langle \alpha \rangle$ and $\langle \beta \rangle$ have no common nonunit ideal factor, then both α and β are nth powers, up to multiplication by a unit.

For our purposes, the modified version is just as useful as the original. Indeed, the arguments we used to rule out nontrivial common divisors of $\gamma + \sqrt{-5}$ and $\gamma - \sqrt{-5}$ apply equally well to both elements and ideals. You should pause for a second, flip back, and convince yourself that this is true; keep in mind that "to divide is contain" and that the ideal norm is multiplicative.

Hence, if the modified 3rd power product principle holds in $\mathbb{Z}[\sqrt{-5}]$, then the argument of the last section is back on firm ground. Of course, this is a big *if*.

Spoiler alert: This story has a happy ending!

Here is the plan for the rest of the chapter. For each quadratic number field K, we will introduce a finite abelian group called the **class group of** $\mathbb{Z}_K$, denoted $\mathrm{Cl}(\mathbb{Z}_K)$. We will see that

$$\text{(9.2)} \qquad \begin{array}{c}\mathrm{Cl}(\mathbb{Z}_K) \text{ has order} \\ \text{prime to } n\end{array} \iff \begin{array}{c}\text{the modified } n\text{th power product} \\ \text{principle holds in } \mathbb{Z}_K.\end{array}$$

When $K = \mathbb{Q}(\sqrt{-5})$, we will compute that the class group has order 2. Thus, the modified 3rd power principle holds in $\mathbb{Z}[\sqrt{-5}]$, and we are out of danger.

The class group of a quadratic number ring

Let K be a quadratic field.

Definition 9.2. If I and J are nonzero ideals of $\mathbb{Z}_K$, we say that I and J are **dilation equivalent** if $I = \lambda J$ for some nonzero $\lambda \in K$. We write $I \approx J$.

For example, the ideals of $\mathbb{Z}_K$ that are dilation equivalent to $\langle 1 \rangle$ are exactly the principal ideals.

It is easy to check (and left to the reader) that $\approx$ is an equivalence relation on $\mathrm{Id}(\mathbb{Z}_K)$. The **class group of** $\mathbb{Z}_K$ is the corresponding quotient set,

$$\mathrm{Cl}(\mathbb{Z}_K) := \mathrm{Id}(\mathbb{Z}_K)/\approx,$$

with multiplication of equivalence classes defined by

$$[I][J] = [IJ].$$

Of course, one needs to check that this is well-defined, but this is easy: If $[I] = [I']$ and $[J] = [J']$, then there are nonzero $\alpha, \beta \in K$ with $I = \alpha I, J = \beta J'$; hence,

$$IJ = \alpha\beta I'J',$$

and so $[IJ] = [I'J']$.

Why is the class group a group? We have associativity — inherited from $\mathrm{Id}(\mathbb{Z}_K)$ — and a multiplicative identity, $[\langle 1 \rangle]$. What about inverses? For each $I \in \mathrm{Id}(\mathbb{Z}_K)$, there is a $J \in \mathrm{Id}(\mathbb{Z}_K)$ with IJ principal, say $IJ = \langle \alpha \rangle$. (This is the "Principal multiple lemma".) Then $[I][J] = [\langle \alpha \rangle] = [\langle 1 \rangle]$, and so $[J] = [I]^{-1}$ in $\mathrm{Cl}(\mathbb{Z}_K)$.

Now that we know the class group is a group, we ask: What kind? It is obviously abelian. The following result is much less trivial; its generalization to arbitrary number fields (which we will prove in Chapter 15) constitutes one of the central theorems of algebraic number theory.

Theorem 9.3. $\mathrm{Cl}(\mathbb{Z}_K)$ is a finite group.

We need two lemmas.

	1	2	3	5	6	7	10	11	13	14	15	17
$h_{\mathbb{Q}(\sqrt{d})}$	*	1	1	1	1	1	2	1	1	1	2	1
$h_{\mathbb{Q}(\sqrt{-d})}$	1	1	1	2	2	1	2	1	2	4	2	4

	19	21	22	23	26	29	30	31	33	34	35	37
$h_{\mathbb{Q}(\sqrt{d})}$	1	1	1	1	2	1	2	1	1	2	2	1
$h_{\mathbb{Q}(\sqrt{-d})}$	1	4	2	3	6	6	4	3	4	4	2	2

Table 9.1. Class numbers of the first several real and imaginary quadratic fields.

Lemma 9.4. There is a constant C, depending only on K, with the following property: Every $I \in \mathrm{Id}(\mathbb{Z}_K)$ contains a nonzero α with

$$|\mathrm{N}\alpha| \leq C \cdot \mathrm{N}(I).$$

In fact, we may take

$$C = 1 + \mathrm{Tr}(\tau) + |\mathrm{N}(\tau)|,$$

where τ is defined as in Theorem 3.7.

Proof. The collection of elements of the form $a + b\tau$, where $0 \leq a, b \leq \sqrt{\mathrm{N}(I)}$, has size

$$\lfloor \sqrt{\mathrm{N}(I)} + 1 \rfloor^2 > \mathrm{N}(I) = \#\mathbb{Z}_K/I.$$

By the pigeonhole principle, two distinct elements of this set occupy the same residue class modulo I. Their difference γ (say) is a nonzero element of I. Moreover, $\gamma = a' + b'\tau$, where $|a'|, |b'| \leq \sqrt{\mathrm{N}(I)}$. Hence,

$$\begin{aligned} |\mathrm{N}(\gamma)| &= |a'^2 + a'b'\mathrm{Tr}(\tau) + b'^2\mathrm{N}(\tau)| \\ &\leq |a'|^2 + |a'||b'| \cdot |\mathrm{Tr}(\tau)| + |b'|^2 \cdot |\mathrm{N}(\tau)| \\ &\leq (1 + |\mathrm{Tr}(\tau)| + |\mathrm{N}(\tau)|) \cdot \mathrm{N}(I). \end{aligned}$$

The coefficient of $\mathrm{N}(I)$ is the constant C appearing in the statement of the lemma. (The absolute value around $\mathrm{Tr}(\tau)$ is unnecessary, since $\mathrm{Tr}(\tau) = 0$ or 1.) □

Lemma 9.5. Let C be any admissible value of the constant in Lemma 9.4. Every element of $\mathrm{Cl}(\mathbb{Z}_K)$ is represented by a nonzero ideal of norm at most C.

Proof. Since $\mathrm{Cl}(\mathbb{Z}_K)$ is a group, $[I]^{-1}$ runs through all of $\mathrm{Cl}(\mathbb{Z}_K)$ whenever $[I]$ does. Hence, it is enough to show that $[I]^{-1}$ has a representative of norm at most C, for every $I \in \mathrm{Id}(\mathbb{Z}_K)$. Given I, choose a nonzero $\alpha \in I$ with $|\mathrm{N}(\alpha)| \leq C \cdot \mathrm{N}(I)$. Since "to contain is to divide", we can write $\langle\alpha\rangle = IJ$ for a nonzero ideal J. Then

$$\mathrm{N}(J) = \mathrm{N}(\langle\alpha\rangle) \cdot \mathrm{N}(I)^{-1} = |\mathrm{N}\alpha| \cdot \mathrm{N}(I)^{-1} \leq C.$$

Since $[I][J] = [IJ] = [\langle\alpha\rangle] = [\langle 1\rangle]$, we have $[J] = [I]^{-1}$. So J is our desired representative. □

Proof of Theorem 9.3. By Lemmas 9.4 and 9.5, every ideal class has a representative of norm at most C. By Lemma 8.7, the set of ideals of norm at most C is finite. □

It is usual to set $h_K := \#\mathrm{Cl}(\mathbb{Z}_K)$ and to refer to h_K as the **the class number** of K (or of $\mathbb{Z}_K$).

Revisiting the nth power product principle

We now explain why the double implication (9.2) holds, beginning with the (easier) forward direction ($\Rightarrow$). Let α, β be nonzero elements of $\mathbb{Z}_K$. Suppose that

$$\alpha\beta = \gamma^n$$

for some γ in $\mathbb{Z}_K$, and that $\langle\alpha\rangle$ and $\langle\beta\rangle$ have no nontrivial common ideal factor. Then in $\mathrm{Id}(\mathbb{Z}_K)$,

$$\langle\alpha\rangle \cdot \langle\beta\rangle = \langle\gamma\rangle^n.$$

Since the left-hand factors are coprime, the fundamental theorem implies that $\langle\alpha\rangle = I^n$ and $\langle\beta\rangle = J^n$ for some $I, J \in \mathrm{Id}(\mathbb{Z}_K)$. Since I^n and J^n are principal, $[I]$ and $[J]$ are n-torsion elements of $\mathrm{Cl}(\mathbb{Z}_K)$. But n is coprime to h_K, and so the n-torsion in $\mathrm{Cl}(\mathbb{Z}_K)$ is trivial. Thus, $[I] = [J] = [\langle 1\rangle]$, i.e., I and J are principal. Write $I = \langle\alpha'\rangle, J = \langle\beta'\rangle$. Then

$$\langle\alpha'^n\rangle = I^n = \langle\alpha\rangle, \quad \text{and} \quad \langle\beta'^n\rangle = J^n = \langle\beta\rangle.$$

Hence, α and β are associates of the nth powers α'^n and β'^n, in accordance with the power product principle.

The forward implication is the one useful in applications, and we take that as an excuse to be somewhat brisk in discussing the backward direction ($\Leftarrow$). We use a deep theorem of Landau from 1907, whose proof (not given here) involves analytic methods.[1] In this particular case, the appeal to Landau's result could be avoided. (See Exercise 7.) However, Landau's theorem will play an indispensable role in Chapter 10, and so it makes sense to introduce it now.

Theorem 9.6. Every ideal class is represented by infinitely many distinct prime ideals.

Assume n and h_K are not coprime, and pick a prime p that divides them both. By Cauchy's theorem, there is an order p element of $\mathrm{Cl}(\mathbb{Z}_K)$, say $[I]$. By Theorem 9.6, we can find a $J \in \mathrm{Id}(\mathbb{Z}_K)$ with $[J] = [I]^{-1}$ and with J coprime to I (in fact, J can even be chosen to be prime!). Since $[I]$ and $[J]$ have order p, and $p \mid n$, both I^n and J^n are trivial in the class group, and clearly IJ is also trivial there. Thus, I^n, J^n, and IJ are principal ideals, say

$$I^n = \langle\alpha\rangle, \quad J^n = \langle\beta\rangle, \quad \text{and} \quad IJ = \langle\gamma\rangle.$$

Since $I^n J^n = (IJ)^n$,

$$\alpha\beta = \epsilon\gamma^n \tag{9.3}$$

for some unit ϵ; replacing α with $\epsilon^{-1}\alpha$, we can assume that $\epsilon = 1$. Equation (9.3) is our sought-after counterexample to the modified nth power product principle: The ideals $\langle\alpha\rangle$ and $\langle\beta\rangle$ are coprime by construction. If α is an associate of an nth power α'^n, then $I^n = \langle\alpha'\rangle^n$, and hence $I = \langle\alpha'\rangle$; but then $[I]$ has order 1 instead of order p.

The class group of $\mathbb{Z}[\sqrt{-5}]$

By Lemmas 9.4 and 9.5, every ideal class of $\mathbb{Z}[\sqrt{-5}]$ is represented by an ideal of norm at most 6. All such ideals decompose as products

[1] Landau, E. *Über die Verteilung der Primideale in den Idealklassen eines algebraischen Zahlkörpers.* Math. Ann. **63** (1906), no. 2, 145–204.
Actually, Landau's result applies to all number fields, not only quadratic fields. The class group of a general number ring will be defined in Chapter 15.

of prime ideals lying above 2, 3, and 5, and those prime ideals were computed in Chapter 7;

$$\langle 2\rangle = P_1^2, \quad \text{with} \quad P_1 = \langle 2,\ \sqrt{-5}+1\rangle,$$
$$\langle 3\rangle = P_2P_3, \quad \text{with} \quad P_2 = \langle 3,\ \sqrt{-5}-1\rangle,\ P_3 = \langle 3,\ \sqrt{-5}+1\rangle,$$
$$\langle 5\rangle = P_4^2, \quad \text{with} \quad P_4 = \langle \sqrt{-5}\rangle.$$

Hence, $\mathrm{Cl}(\mathbb{Z}_K)$ is generated by $[P_1], [P_2], [P_3]$, and $[P_4]$. Since $[P_4]$ is trivial, it need not be considered. Since P_2P_3 is principal, $[P_2] = [P_3]^{-1}$, and so $[P_2]$ can also be scratched from our list of generators. In Chapter 4, we computed that $P_1P_3 = \langle 1+\sqrt{-5}\rangle$; thus, $[P_3] = [P_1]^{-1}$, and $[P_3]$ can be crossed off. We conclude that $\mathrm{Cl}(\mathbb{Z}_K)$ is cyclic, generated by $[P_1]$. Since $P_1^2 = \langle 2\rangle$, either $[P_1]$ is trivial or has order 2. In the former case, $\mathrm{Cl}(\mathbb{Z}_K)$ itself is trivial, so that $\mathbb{Z}[\sqrt{-5}]$ is a PID, and thus a UFD. But we have known for some time that this is false! Hence, $[P_1]$ has order 2, and $\mathrm{Cl}(\mathbb{Z}_K) \cong \mathbb{Z}/2\mathbb{Z}$.

A general theorem

The method used here to treat the equation $y^2 = x^3 - 5$ generalizes nicely. We leave the proof of the next theorem as a pleasant exercise for the motivated reader.[2]

Theorem 9.7. Let d be a negative squarefree integer with $d \equiv 2, 3 \pmod 4$. Let $K = \mathbb{Q}(\sqrt{d})$, and assume that $3 \nmid h_K$. Then the integer solutions (x, y) to

$$y^2 = x^3 + d$$

are precisely the pairs $(A^2 - d, A(A^2 + 3d))$, where A runs over all integers for which $3A^2 \pm 1 = -d$.

Example 9.8 ($d = -13$)**.** It can be proved that $\mathbb{Q}(\sqrt{-13})$ has class number 2, so that Theorem 9.7 can be applied. The only integers A with $3A^2 \pm 1 = 13$ are $A = \pm 2$. Plugging this into the theorem, the integer solutions to $y^2 = x^3 - 13$ are $(x, y) = (17, \pm 70)$.

One can deduce from a far-reaching 1929 theorem of Siegel that each equation $y^2 = x^3 + k$ (k fixed, $k \neq 0$) has only finitely many

[2] For a more general result, encompassing also those cases where $d \equiv 5 \pmod 8$, see §4.4 of: Lemmermeyer, F. *Quadratische Zahlkörper. Ein Schnupperkurs.* Südwestdeutscher Verlag für Hochschulschriften, Saarbrücken, 2011.

integer solutions (x, y). Several results concerning these solutions are discussed in Chapter 26 of Mordell's authoritative 1969 monograph on Diophantine equations.[3] For later developments, consult the recent paper of Bennett and Ghadermarzi[4] and the references therein.

Exercises

(1) Let g be an odd positive integer for which $3^g - 1$ is squarefree, and set $K = \mathbb{Q}(\sqrt{1 - 3^g})$.
  (a) Show that 3 splits in $\mathbb{Z}_K$.
  (b) Show that $\langle 1 + \sqrt{1 - 3^g} \rangle = P^g$ for a prime ideal P lying above 3. *Hint:* What is $N(\langle 1 + \sqrt{1 - 3^g} \rangle)$?
  (c) Show that P^ℓ is nonprincipal for all positive integers $\ell < g$. Conclude that $[P]$ has order exactly g in $\mathrm{Cl}(\mathbb{Z}_K)$.[5]

(2) (Hilbert's "Theorem 90" for quadratic fields) Let K be a quadratic field.
  (a) Let η be a norm 1 element of $\mathbb{Z}_K$. Show that there is an $\alpha \in \mathbb{Z}_K$ with $\eta = \alpha/\tilde{\alpha}$.[6] *Hint:* If $\eta \neq -1$, then $\alpha = 1 + \eta$ works.
  (b) Show that the conclusion of (a) holds for any norm 1 element $\eta \in K$ (not necessarily in $\mathbb{Z}_K$).

(3) (Taussky[7]) Show that the parametrization of primitive Pythagorean triples appearing in Exercise 1.1 can be recovered from Problem 2(b), taking $K = \mathbb{Q}(i)$.

(4) Let $K = \mathbb{Q}(\sqrt{d})$, where d is squarefree, $d < 0$, and d is not either of -1 or -3. Call a nonzero ideal I of $\mathbb{Z}_K$ **ambiguous** if $I = \tilde{I}$. Call I **primitive** if I is not divisible by $\langle p \rangle$ for any rational prime p.
  (a) Show that there are precisely two primitive, ambiguous principal ideals in $\mathbb{Z}_K$, namely the unit ideal and $\langle \sqrt{d} \rangle$.

---

[3] Mordell, L. J. *Diophantine equations.* Pure and Applied Mathematics, **30**. Academic Press, London–New York, 1969.

[4] Bennett, M. A.; Ghadermarzi, A. *Mordell's equation: a classical approach.* LMS J. Comput. Math. **18** (2015), no. 1, 633–646. These authors determine the integer solutions to $y^2 = x^3 + k$ for all k with $|k| < 10^7$.

[5] Ankeny and Chowla used a variation of this argument to show that there are infinitely many imaginary quadratic fields K with h_K divisible by any prescribed positive integer g. See: Ankeny, N. C.; Chowla, S. *On the divisibility of the class number of quadratic fields.* Pacific J. Math. **5** (1955), 321–324.

[6] As usual, the tilde denotes the nontrivial automorphism of $K/\mathbb{Q}$.

[7] Taussky, O. *Sums of squares.* Amer. Math. Monthly **77** (1970), 805–830.

(b) Let $p_1, \dots, p_t$ be the distinct rational primes that ramify in $\mathbb{Z}_K$. For each $i = 1, 2, \dots, t$, let P_i be the (unique) prime ideal of $\mathbb{Z}_K$ above p_i. Show that for any selection of $e_i \in \{0, 1\}$, the product $\prod_{i=1}^{t} P_i^{e_i}$ is a primitive, ambiguous ideal.

(c) Consider the map from $(\mathbb{Z}/2\mathbb{Z})^t \to \mathrm{Cl}(\mathbb{Z}_K)$ taking

$$(e_1 \bmod 2, \dots, e_k \bmod 2) \mapsto \prod_{i=1}^{t} [P_i]^{e_i}.$$

Show that this is a well-defined group homomorphism whose kernel has size 1 or 2.

(d) Conclude that $2^{t-1} \mid h_K$.

Remark: The same method carries over to real quadratic fields, though the details are more complicated. The final result is that 2^{t-1} divides h_K or $2h_K$, according to whether $\mathrm{N}\epsilon_0 = -1$ or 1, respectively. As above, t is the number of rational primes that ramify in $\mathbb{Z}_K$.[8]

(5) For each odd prime p, let $p^* = (-1)^{(p-1)/2} p$, and put $K = \mathbb{Q}(\sqrt{p^*})$. Here we outline a proof that h_K is always odd. (The same fact will emerge from a very different source in Chapter 26.)

(a) Suppose for a contradiction that $2 \mid \mathrm{Cl}(\mathbb{Z}_K)$, and choose I having order 2 in the class group. Explain why there is a nonzero $\eta \in K$ with $\tilde{I} = \eta I$.

(b) Deduce that there is a nonzero $\gamma \in \mathbb{Z}_K$ such that $J = \gamma I$ is ambiguous. *Hint:* Show $\mathrm{N}\eta = 1$; then apply Exercise 2(b).

(c) Show that every ambiguous ideal of $\mathbb{Z}_K$ is principal. (Applied to the ideal J in part (b), we get a contradiction with the choice of I !) *Hint:* One immediately reduces to the primitive case. Show that a primitive ambiguous ideal is composed entirely of prime ideals lying above ramified rational primes. Explicitly determine those prime ideals.

(6) This exercise and the next make use of P-adic valuations; look back at Exercise 6.4 for their definition.

---

[8] Rather more is true: For every quadratic field K, the "narrow" class group has 2-rank exactly $t - 1$. For the definition of the narrow class group, and a proof of this result (due essentially to Gauss), see §45 of: Hecke, E. *Lectures on the theory of algebraic numbers.* Translated from the 1923 German original. Graduate Texts in Mathematics **77**. Springer-Verlag, New York-Berlin, 1981.

Let $\mathcal{P}$ be a finite set of nonzero prime ideals of $\mathbb{Z}_K$. Suppose that for each $P \in \mathcal{P}$, we are given a nonnegative integer e_P. Here we outline a proof that there is always an $\alpha \in \mathbb{Z}_K$ with $\mathrm{ord}_P(\alpha) = e_P$ for all $P \in \mathcal{P}$.

(a) For each $P \in \mathcal{P}$, explain why it is possible to find an $\alpha_P \in P^{e_P} \setminus P^{e_P+1}$. Show that $\mathrm{ord}_P(\alpha_P) = e_P$.

(b) Explain why the ring-theoretic Chinese remainder theorem implies the existence of an $\alpha \in \mathbb{Z}_K$ with

$$\alpha \equiv \alpha_P \pmod{P^{e_P+1}}$$

for all $P \in \mathcal{P}$.[9] Then show that this α has the desired property.

(7) Let I and I' be any nonzero ideals of $\mathbb{Z}_K$. Using the last exercise, show that there is a nonzero ideal J coprime to I' with IJ principal. This result may be substituted for the deep Theorem 9.6 in our discussion of the nth power product principle. *Hint:* Construct an α where $I \mid \langle\alpha\rangle$ and $J = \langle\alpha\rangle I^{-1}$ is coprime to I'.

(8) Let $\mathrm{PrinFrac}(\mathbb{Z}_K)$ be the subgroup of $\mathrm{Frac}(\mathbb{Z}_K)$ consisting of **principal fractional ideals**, meaning fractional ideals[10] of the form $\alpha\mathbb{Z}_K$, with $\alpha \in K^\times$. Show that

$$\mathrm{Cl}(\mathbb{Z}_K) \cong \mathrm{Frac}(\mathbb{Z}_K)/\mathrm{PrinFrac}(\mathbb{Z}_K),$$

via the map sending $[I]$ to the coset of I. (The RHS is often taken as the definition of the class group.)

[9] Recall that the ring-theoretic CRT asserts: If $I_1, \ldots, I_n$ are pairwise comaximal ideals of a ring R, then $I_1 \cap \cdots \cap I_n = I_1 \cdots I_n$, and the map from $R/I_1 \cdots I_n$ to $\bigoplus_{k=1}^n R/I_k$ sending $x \bmod I$ to $(x \bmod I_1, \ldots, x \bmod I_n)$ is an isomorphism.

[10] See Exercise 6.3 for the definition of fractional ideals.

10

Measuring the failure of unique factorization

> The class group is a bitter group and a sweet group. It is bitter because when it is non-trivial it makes a mess. It is sweet because it makes things interesting.
> – Kazuya Kato

Let K be a quadratic number field.[1] Then K has class number 1 precisely when every nonzero ideal of $\mathbb{Z}_K$ is dilation equivalent to the unit ideal — in other words, principal. Hence,

$$h_K = 1 \iff \mathbb{Z}_K \text{ is a PID.}$$

We claim that one can take this a step further:

$$\mathbb{Z}_K \text{ is a PID} \iff \mathbb{Z}_K \text{ is a UFD.}$$

The forward implication is a familiar fact from algebra, valid for all integral domains, not only $\mathbb{Z}_K$. To prove the backward implication, we assume $\mathbb{Z}_K$ is a UFD and show that an arbitrary nonzero *prime* ideal P is principal. Since every nonzero ideal of $\mathbb{Z}_K$ factors as a product of prime ideals, this is enough. Let p be the rational prime lying below P, and factor p as a product of irreducibles in $\mathbb{Z}_K$, say

$$p = \pi_1 \pi_2 \cdots \pi_k.$$

[1] We restrict to quadratic fields in this chapter only because we have not defined the class group in general. After Chapter 15, it will be clear that the results of this chapter are valid for all number fields.

Since P divides $\langle p \rangle = \langle \pi_1 \rangle \cdots \langle \pi_k \rangle$ and P is prime, P divides $\langle \pi_i \rangle$ for some i. But $\langle \pi_i \rangle$ is itself a prime ideal, since "irreducible $\Rightarrow$ prime" in a UFD. By the fundamental theorem of ideal theory, whenever a nonzero prime ideal divides another, the two are equal. So $P = \langle \pi_i \rangle$, and thus P is principal.

The upshot:

$$h_K = 1 \iff \mathbb{Z}_K \text{ is a UFD.}$$

An arithmetic interpretation of class number 2

Thus, $h_K = 1$ has a simple arithmetic meaning. What about larger values of h_K? Is there a corresponding characterization, where uniqueness of factorization is replaced with some sort of quasi-uniqueness? An affirmative answer for the case $h_K = 2$ was given by Carlitz in a striking and influential 1960 paper.[2] In the following, the **length** of a factorization is the number of factors, counted with multiplicity. For instance, in $\mathbb{Z}[\sqrt{-5}]$, the two factorizations of 6 as $(1+\sqrt{-5}) \cdot (1-\sqrt{-5})$ and as $2 \cdot 3$ both have length 2.

Theorem 10.1 (Carlitz)**.**

$$h_K \leq 2 \iff \begin{array}{c}\text{Any two irreducible factorizations of} \\ \text{the same nonzero, nonunit element} \\ \text{have the same length.}\end{array}$$

(To single out $h_K = 2$ specifically, one could add "and $\mathbb{Z}_K$ is not a UFD" to the right-hand side.) Since $h_K = 2$ for $K = \mathbb{Q}(\sqrt{-5})$, we see it was no coincidence that both factorizations of 6 had the same length.

Let us prove the forward direction ($\Rightarrow$) of Theorem 10.1. If $h_K = 1$, the result is obvious, so assume that $h_K = 2$. To avoid the inconvenience of units, we rephrase what needs to be shown as a statement about ideals. Let $\mathrm{Prin}(\mathbb{Z}_K)$ denote the monoid of nonzero principal ideals of $\mathbb{Z}_K$, and recall that the irreducibles of $\mathrm{Prin}(\mathbb{Z}_K)$ are precisely the ideals generated by irreducible elements.[3] So our task is to show

[2] Carlitz, L. *A characterization of algebraic number fields with class number two.* Proc. Amer. Math. Soc. **11** (1960), 391–392.

For an overview of work inspired by Carlitz's paper, see: Chapman, S. T.; Coykendall, J. *Half-factorial domains, a survey.* Non-Noetherian commutative ring theory, 97–115, Math. Appl., **520**, Kluwer Acad. Publ., Dordrecht, 2000.

[3] When we speak about irreducible principal ideals, we mean irreducible with reference to $\mathrm{Prin}(\mathbb{Z}_K)$. They may factor into nonprincipal ideals, i.e., may not be irreducible in $\mathrm{Id}(\mathbb{Z}_K)$.

that if we factor a nonzero principal ideal into irreducibles, then the length of the factorization is entirely determined by the starting ideal. To this end, suppose

$$\langle \pi_1 \rangle \cdots \langle \pi_k \rangle = \langle \rho_1 \rangle \cdots \langle \rho_\ell \rangle, \tag{10.1}$$

where each π_i and ρ_j is irreducible. If any one of the π_i is prime, we deduce from the fact that $\pi_i \mid \rho_1 \cdots \rho_\ell$ that $\pi_i \mid \rho_j$ for some j. Since both π_i and ρ_j are irreducible, $\langle \pi_i \rangle = \langle \rho_j \rangle$, and this common factor can be canceled from (10.1). In this way, the lengths of the factorizations drop from k and ℓ to $k-1$ and $\ell - 1$. Naturally, the same idea applies if any one of the ρ_j is prime. We iterate, canceling any ideals generated by prime elements from both sides. At the end of the day, we see that for the sake of proving $k = \ell$, we can assume that in (10.1) no π_i or ρ_j is prime. Under this assumption, the following lemma allows us to quickly conclude.

Lemma 10.2. Assume $h_K = 2$. Let π be an irreducible element of $\mathbb{Z}_K$ that is not prime. Then $\langle \pi \rangle = P_1 P_2$ for nonzero prime ideals P_1, P_2 of $\mathbb{Z}_K$.

To finish off the forward direction of Theorem 10.1, factor both sides of (10.1) into prime ideals of $\mathbb{Z}_K$. By Lemma 10.2, the left-hand side will split into $2k$ prime ideal factors, while the right will involve 2ℓ. By the fundamental theorem of ideal theory, $k = \ell$.

Proof of Lemma 10.2. Write

$$\langle \pi \rangle = P_1 \cdots P_g,$$

where $P_1, \ldots, P_g$ are nonzero prime ideals. Since π is not prime, $g \geq 2$. To continue, we observe that none of the P_i are principal. Indeed, if (say) $P_i = \langle \omega \rangle$, then ω is a nonunit that divides the irreducible element π. Hence, $\langle \pi \rangle = \langle \omega \rangle$. But then π is prime, since it generates a prime ideal (namely, P_i). This contradiction shows that all of the P_i are nonprincipal, i.e., nontrivial in $\mathrm{Cl}(\mathbb{Z}_K)$. Since $\mathrm{Cl}(\mathbb{Z}_K) \cong \mathbb{Z}/2\mathbb{Z}$, the product $P_1 P_2$ *is* trivial in $\mathrm{Cl}(\mathbb{Z}_K)$. That is, $P_1 P_2 = \langle \sigma \rangle$ for some σ. Then σ is a nonunit divisor of π, and so $P_1 P_2 = \langle \sigma \rangle = \langle \pi \rangle$. Plugging this back into our original factorization of $\langle \pi \rangle$, we find that $\langle \pi \rangle = \langle \pi \rangle P_3 \cdots P_g$. Hence, the product $P_3 \cdots P_g$ is empty, meaning that $g = 2$. □

The proof for the backward direction ($\Leftarrow$) relies on Landau's theorem (from p. 85) and the following easy group-theoretic result.

Lemma 10.3. Let G be an abelian group with more than two elements. One can find three (not necessarily distinct) elements of G which multiply to the identity and where no proper nonempty subproduct multiplies to the identity.

Proof. If there is any $g \in G$ with order at least three, we can take the three elements to be g, g, g^{-2}. Otherwise, every non-identity element has order 2. Since $\#G \geq 3$, we can find $g, h \in G$ distinct from each other and distinct from the identity. Then our desired triple is g, h, gh. □

Before proceeding, the following remark is in order. If $P_1, P_2, \ldots, P_g$ are prime ideals whose product is principal, say $P_1 \cdots P_g = \langle \pi \rangle$, and no proper nonempty subproduct of the P_i is principal, then π is irreducible. The proof is simple: If ω is a nontrivial proper divisor of π, the prime ideal factorization of $\langle \omega \rangle$ gives us a forbidden subproduct.

We now return to the proof proper. It is enough to show that if $h_K > 2$, then some nonzero element of $\mathrm{Prin}(\mathbb{Z}_K)$ has irreducible factorizations of different lengths. We apply Lemma 10.3 to the group $\mathrm{Cl}(\mathbb{Z}_K)$. In conjunction with Landau's theorem, this allows us to choose prime ideals P_1, P_2, P_3 whose product is principal and where no proper nonempty subproduct is principal. By a further application of Landau's result, we can pick prime ideals Q_1, Q_2, Q_3 with each Q_i in the class inverse to P_i. Then the product of the Q_i is principal, and no proper nonempty subproduct is principal. There are $\pi, \rho, \omega_1, \omega_2, \omega_3 \in \mathbb{Z}_K$ with

$$P_1 P_2 P_3 = \langle \pi \rangle, \quad Q_1 Q_2 Q_3 = \langle \rho \rangle,$$

and

$$P_1 Q_1 = \langle \omega_1 \rangle, \quad P_2 Q_2 = \langle \omega_2 \rangle, \quad P_3 Q_3 = \langle \omega_3 \rangle.$$

By the observation of the last paragraph, all five of these elements are irreducible. Since $P_1 P_2 P_3 \cdot Q_1 Q_2 Q_3 = P_1 Q_1 \cdot P_2 Q_2 \cdot P_3 Q_3$, we have

$$\langle \pi \rangle \langle \rho \rangle = \langle \omega_1 \rangle \langle \omega_2 \rangle \langle \omega_3 \rangle.$$

So we have found an element of $\mathrm{Prin}(\mathbb{Z}_K)$ which factors as a product of two irreducibles and as a product of three irreducibles. This completes the proof of Theorem 10.1.

Elasticity

For each $I \in \mathrm{Prin}(\mathbb{Z}_K)$, define the **length spectrum** of I by

$$\mathcal{L}(I) = \left\{ n \in \mathbb{Z}_{\geq 0} : \begin{array}{c} I \text{ has a length } n \text{ factorization into} \\ \text{irreducible principal ideals} \end{array} \right\}.$$

When $h_K = 1$ or $h_K = 2$, the sets $\mathcal{L}(I)$ are always singletons. By contrast, when $h_K > 2$, we described in the last section how to construct a principal ideal J with both $2, 3 \in \mathcal{L}(J)$. For any such J, and any $r \in \mathbb{Z}^+$, the length spectrum of J^r contains $2r$ and $3r$. It follows that whenever $h_K > 2$,

$$\sup_{\substack{I \in \mathrm{Prin}(\mathbb{Z}_K) \\ m,n \in \mathcal{L}(I)}} (m - n) = \infty.$$

One obtains a more interesting theory if one looks at the ratios m/n rather than the differences $m - n$. The following definition is due to Valenza.[4]

Definition 10.4. The **elasticity** of $\mathbb{Z}_K$ is defined as

$$\sup_{\substack{I \in \mathrm{Prin}(\mathbb{Z}_K),\ I \neq \langle 1 \rangle \\ m,n \in \mathcal{L}(I)}} m/n.$$

We denote the elasticity of $\mathbb{Z}_K$ by ϱ_K.

By Theorem 10.1, $\varrho_K = 1 \iff h_K \leq 2$. In general, the elasticity of $\mathbb{Z}_K$ is intimately tied to the structure of the class group $\mathrm{Cl}(\mathbb{Z}_K)$. The following notion from combinatorial group theory will allow us to make this precise.

Definition 10.5. Let G be a finite abelian group, viewed multiplicatively. The **Davenport constant** of G, denoted $D(G)$, is the smallest

[4]Valenza, R. J. *Elasticity of factorization in number fields.* J. Number Theory **36** (1990), no. 2, 212–218. This paper has the curious distinction of appearing 10 years after its initial submission!

For a survey of related work in commutative algebra, see: Anderson, D. F. *Elasticity of factorizations in integral domains: a survey.* Factorization in integral domains (Iowa City, IA, 1996), 1–29, Lecture Notes in Pure and Appl. Math., **189**, Dekker, New York, 1997.

positive integer D with the property that any sequence of D elements of G has a nonempty subsequence whose product is the identity.[5]

Before stating the connection with ϱ_K, we pause to show that the Davenport constant is well-defined.

Proposition 10.6. Let G be a finite abelian group, say $\#G = n$. Every sequence of n elements of G contains a nonempty subsequence that multiplies to the identity. Hence,

$$D(G) \leq n.$$

Proof. Let $g_1, g_2, \ldots, g_n \in G$. If the n elements g_1, g_1g_2, $g_1g_2g_3$, $\ldots$, $g_1g_2\cdots g_n$ are all distinct, then one of these is equal to the identity, and we are done. Otherwise, $g_1g_2\cdots g_k = g_1g_2\cdots g_\ell$ for some integers k, ℓ with $1 \leq k < \ell \leq n$. In that case, $g_{k+1}, g_{k+2}, \ldots, g_\ell$ is the desired subsequence. □

The upper bound implicit in the next result is due to Valenza (op. cit.); equality was first shown by Steffan.[6]

Theorem 10.7. Assume $h_K \geq 2$. Then

$$\varrho_K = \frac{1}{2}D(\mathrm{Cl}(K)).$$

Proof. For ease of notation, set $g = D(\mathrm{Cl}(K))$. The proof of the lower bound follows the argument given for the backward direction of Carlitz's theorem. By Landau's theorem, there is a sequence $P_1, P_2, \ldots, P_{g-1}$ of nonzero prime ideals having no nonempty principal subproduct. Choose a prime ideal P_g in the class inverse to $[P_1\cdots P_{g-1}]$. Then $P_1\cdots P_g$ is principal, but no nonempty proper subproduct is principal. (If there were a nonempty, proper subproduct which was principal, it would have to involve P_g, but then the complementary subproduct would be a nonempty principal subproduct of $P_1, \ldots, P_{g-1}$.) Let $Q_1, \ldots, Q_g$ be prime ideals from the classes

[5]The constants are named for Harold Davenport, who proposed the problem of determining $D(G)$ at the Midwestern Conference on Group Theory and Number Theory, Ohio State University, April 1966.

[6]Steffan, J.-L. *Longueurs des décompositions en produits d'éléments irréductibles dans un anneau de Dedekind.* J. Algebra **102** (1986), no. 1, 229–236.

inverse to $[P_1], \ldots, [P_g]$, respectively. There are $\pi, \rho, \omega_1, \ldots, \omega_g \in \mathbb{Z}_K$ with

$$P_1 \cdots P_g = \langle \pi \rangle, \quad Q_1 \cdots Q_g = \langle \rho \rangle,$$

and

$$P_1 Q_1 = \langle \omega_1 \rangle, \quad \ldots, \quad P_g Q_g = \langle \omega_g \rangle.$$

For the same reason as in the proof of Theorem 10.1, π, ρ, and the ω_i are all irreducible. Since $(P_1 \cdots P_g) \cdot (Q_1 \cdots Q_g) = (P_1 Q_1) \cdot (P_2 Q_2) \cdots (P_g Q_g)$,

$$\langle \pi \rangle \langle \rho \rangle = \langle \omega_1 \rangle \cdots \langle \omega_g \rangle.$$

It follows immediately that $\varrho_K \geq \frac{g}{2}$.

Turning to the upper bound, let I be a nonzero principal ideal of $\mathbb{Z}_K$, not the unit ideal. Take any two factorizations of I as a product of irreducible principal ideals, say

$$\langle \pi_1 \rangle \cdots \langle \pi_m \rangle = \langle \rho_1 \rangle \cdots \langle \rho_n \rangle, \tag{10.2}$$

ordered so that $m \geq n$. We will show that $m \leq ng/2$. Thus, $\varrho_K \leq \frac{g}{2}$, which combined with the known lower bound finishes the proof.

Since we are assuming that $h_K > 1$, we have that $g \geq 2$. Indeed, it is clear from its definition that the Davenport constant of any nontrivial group is larger than 1.

As in the proof of Carlitz's theorem, we can cancel from (10.2) any ideals generated by prime elements. In this way, we obtain two factorizations of a new principal ideal I', where the lengths are now $m - d$ and $n - d$, for some nonnegative integer d. If we show that

$$(m - d) \leq (n - d)\frac{g}{2},$$

then

$$\begin{aligned} m &\leq n\frac{g}{2} + d(1 - \frac{g}{2}) \\ &\leq n\frac{g}{2}, \end{aligned}$$

as desired. So for the sake of proving that $m \leq ng/2$, we can (and will) assume that no π_i or ρ_j is prime.

Write down the (unique) factorization of I into prime ideals, say

$$I = P_1 \cdots P_\ell.$$

It suffices to show that

$$n \geq \ell/g$$

while

$$m \leq \ell/2.$$

The second inequality is easy: Since no π_i is prime, each factor $\langle \pi_i \rangle$ in (10.2) is made up of at least two prime ideals, but I has only ℓ prime factors in total. The same idea proves the lower bound on n, once we know that any irreducible element generates an ideal with at most g prime ideal factors. To see this, suppose for a contradiction that ρ is an irreducible with

$$\langle \rho \rangle = Q_1 \cdots Q_{g'},$$

where the Q_i are prime ideals and $g' > g$. By the definition of g, there is a nonempty subproduct of $Q_1, \ldots, Q_g$ that is principal, say equal to $\langle \beta \rangle$. But then β is a nonunit divisor of ρ whose cofactor is also a nonunit; this contradicts the irreducibility of ρ. □

In view of Theorem 10.7, one would like an easy way to compute Davenport constants. Say we are given that

$$G \cong \mathbb{Z}/d_1\mathbb{Z} \times \mathbb{Z}/d_2\mathbb{Z} \times \cdots \times \mathbb{Z}/d_r\mathbb{Z}, \tag{10.3}$$

where $d_1 \mid d_2 \mid \cdots \mid d_r$. (Recall that every finite abelian group has such a decomposition; the key words are "invariant factors".) One might hope for a simple description of $D(G)$ in terms of $d_1, \ldots, d_r$. Perhaps surprisingly, given the elementary definitions at play here, no such description is known. But there is at least an easy lower bound on $D(G)$ in terms of the d_i.

Proposition 10.8. Let G be a finite abelian group satisfying (10.3). Then

$$D(G) \geq (d_1 - 1) + \cdots + (d_r - 1) + 1.$$

Proof. The sequence of length $\sum_{i=1}^{r}(d_i - 1)$ obtained by concatenating $d_i - 1$ copies of

$$(0, 0, \ldots, \underbrace{1}_{i\text{th position}}, 0, \ldots, 0), \qquad \text{for } i = 1, 2, \ldots, r,$$

has no nonempty subsequence summing to the identity. Hence, $D(G) \geq 1 + \sum_{i=1}^{r}(d_i - 1)$. □

When the study of Davenport constants was still in its infancy, Olson conjectured that equality holds in Proposition 10.8, and he proved this if either (i) $r \leq 2$, or (ii) $\#G$ is a prime power. (The same results were also obtained around the same time by D. Kruyswijk.) But the general conjecture turns out to be false, and there are now several families of counterexamples in the literature. See the discussion in §3 of Gao and Geroldinger's survey article.[7]

It is a consequence of Proposition 10.8 that a large group necessarily has a large Davenport constant.

Corollary 10.9. $D(G) \to \infty$ as $\#G \to \infty$.

Proof. We will prove the more precise claim that

$$D(G) \geq \frac{\log(2\#G)}{\log 2}.$$

We use the inequality $2^m \geq m+1$, valid for all nonnegative integers m.[8] Write G in the form (10.3). By Proposition 10.8,

$$2^{D(G)} \geq 2^{1+\sum_{i=1}^r (d_i - 1)} = 2\prod_{i=1}^r 2^{d_i - 1} \geq 2\prod_{i=1}^r d_i = 2\#G.$$

Now take logarithms. □

The following result of Valenza (op. cit.) is immediate upon combining Corollary 10.9 and Theorem 10.7.

Theorem 10.10. $\varrho_K \to \infty$ as $h_K \to \infty$.

Thus, in a certain sense, the failure of unique factorization in $\mathbb{Z}_K$ becomes more and more pronounced as the class number heads off to infinity.

---

[7] Gao, W.; Geroldinger, A. *Zero-sum problems in finite abelian groups: a survey.* Expo. Math. **24** (2006), no. 4, 337–369.

[8] Notice that an m element set has at least $m+1$ subsets, namely the empty set along with each of the singleton subsets. But there are 2^m subsets in total.

Exercises

(1) (Śliwa[9]) Let K be a quadratic field. According to Theorem 10.1, $h_K \leq 2 \iff \#\mathcal{L}(I) = 1$ for every $I \in \mathrm{Prin}(\mathbb{Z}_K)$. We now show that when $h_K > 2$, the length spectrum of a nonzero principal ideal can possess any positive integer cardinality. We write ℓ for the maximum order of an element of $\mathrm{Cl}(\mathbb{Z}_K)$.

(a) Using Landau's theorem, let P_1 be a prime ideal with $[P_1]$ having order ℓ, and let P_2 be a prime ideal with $[P_2] = [P_1]^{-1}$. For each $m \in \mathbb{Z}^+$, show that $I = (P_1P_2)^{\ell(m-1)} \in \mathrm{Prin}(\mathbb{Z}_K)$ and that

$$\mathcal{L}(I) = \{2(m-1) + (\ell-2)j : j = 0, 1, \ldots, m-1\}.$$

In particular, if $\ell > 2$, then $\#\mathcal{L}(I) = m$.

(b) Now suppose that $\ell = 2$. Choose P_1 and P_2 nonprincipal prime ideals belonging to different ideal classes. (Recall we are assuming that $h_K > 2$, so this is possible by Landau's theorem.) Let P_3 be a prime ideal with $[P_3] = [P_1P_2]$. Given $m \in \mathbb{Z}^+$, let $I = (P_1P_2P_3)^{2(m-1)}$. Show that $I \in \mathrm{Prin}(\mathbb{Z}_K)$ and

$$\mathcal{L}(I) = \{3(m-1) - j : j = 0, 1, \ldots, m-1\}.$$

So again we have constructed an I with $\#\mathcal{L}(I) = m$.

Below, we assume that Definition 10.4 has been extended to arbitrary atomic monoids M in the obvious way; that is, the **elasticity of** M is the supremum of the ratio set

$$\{\frac{m}{n} : x_1 \cdots x_m = y_1 \cdots y_n, \text{ all } x_i, y_j \text{ irreducible}\}.$$

(2) For this problem, take as known the following theorem of Dirichlet: *For every pair of coprime integers a and m with $m > 0$, there are infinitely many prime numbers $p \equiv a \pmod{m}$.*[10]

Let m be a positive integer, and let

$$H_m = \{n \in \mathbb{Z}^+ : n \equiv 1 \pmod{m}\},$$

with multiplication inherited from $\mathbb{Z}^+$. These submonoids of $\mathbb{Z}^+$ are called **Hilbert monoids**.

[9] Śliwa, J. *Remarks on factorizations in algebraic number fields.* Colloq. Math. **46** (1982), no. 1, 123–130.

[10] See (e.g.) Chapter VI of: Serre, J.-P. *A course in arithmetic.* Graduate Texts in Mathematics **7**. Springer-Verlag, New York-Heidelberg, 1973.

(a) Show that H_m is atomic for every choice of m.
(b) Show that H_m possesses unique factorization if and only if $m = 1$ or $m = 2$.
(c) Show that when $m \in \{1, 2, 3, 4, 6\}$, any two irreducible factorizations of the same nonunit element of H_m have the same length.
(d) Show that when $m > 2$, the elasticity of H_m is

$$\frac{1}{2} \cdot D(U(\mathbb{Z}/m\mathbb{Z})).$$

Use this to establish the converse of (c).

A historical remark: H_5 is discussed in the official lecture notes ("Ausarbeitungen") of a course on elementary and algebraic number theory run by Hilbert at Göttingen in the Winter semester of 1897/1898. After some examples illustrating nonuniqueness of factorization in H_5, Hilbert remarks that order is restored once we introduce new elements corresponding to the greatest common divisors of existing elements. This is Hilbert's jumping off point for a discussion of Dedekind's ideal theory.

(3) (Banister, Chaika, Chapman, and Meyerson[11]) Let m be an integer larger than 1, and let M be the submonoid of $\mathbb{Z}^+$ given by

$$M = \{n \in \mathbb{Z}^+ : \gcd(n, m) > 1\} \cup \{1\}.$$

Show that M is not a UFM but that any two irreducible factorizations of the same nonunit element of M have the same length.

(4) Let m be a positive integer with at least two distinct prime factors, and let M be the submonoid of $\mathbb{Z}^+$ given by

$$M = \{n \in \mathbb{Z}^+ : n \equiv 0 \pmod{m}\} \cup \{1\}.$$

Show that every element of M can be written as a product of at most K irreducible elements of M, where K is a constant depending only on m. Deduce that M has infinite elasticity.[12]

---

[11] Banister, M.; Chaika, J.; Chapman, S. T.; Meyerson, W. *On a result of James and Niven concerning unique factorization in congruence semigroups*. Elem. Math. **62** (2007), no. 2, 68–72.

[12] For a more general result, see Theorem 2.4 in: Banister, M.; Chaika, J.; Chapman, S. T.; Meyerson, W. *On the arithmetic of arithmetical congruence monoids*. Colloq. Math. **108** (2007), no. 1, 105–118.

For further variations on the theme of Exercises 2–4, see: Baginski, P.; Chapman, S. T. *Arithmetic congruence monoids: a survey*. Combinatorial and additive number theory–CANT 2011 and 2012, 15–38, Springer Proc. Math. Stat. **101**, Springer, New York, 2014.

(5) Let m be an integer with $m > 1$. We define A_m as the monoid of monic polynomials in $(\mathbb{Z}/m\mathbb{Z})[x]$, with multiplication the familiar multiplication of polynomials. When $m = p$ is prime, the uniqueness of factorization in $\mathbb{F}_p[x]$ implies that A_m is a UFM.
   (a) Show that A_m is cancellative and atomic for every positive integer m.
   (b) The remainder of this exercise considers the case $m = pq$, where p, q are distinct primes. Given $\ell \in \mathbb{Z}^+$, let
   $$m_p(x), m_q(x) \in \mathbb{Z}[x]$$
   be monic polynomials of degree ℓ whose respective reductions mod p and mod q are irreducible. (Recall that over an arbitrary finite field, there are irreducible polynomials of any given degree, so we can always choose $m_p(x)$ and $m_q(x)$ like this.) Let $f(x) \in \mathbb{Z}[x]$ be a monic, degree ℓ solution to the simultaneous congruences
   $$f(x) \equiv m_p(x) \pmod{p}, \quad f(x) \equiv x^\ell \pmod{q},$$
   and let $g(x) \in \mathbb{Z}[x]$ be a monic, degree ℓ solution to the congruences
   $$g(x) \equiv x^\ell \pmod{p}, \quad g(x) \equiv m_q(x) \pmod{q}.$$
   Show that $f(x)$ mod pq and $g(x)$ mod pq are irreducible in A_{pq}.
   (c) Show that $f(x)g(x)$ mod pq has a factorization into irreducibles of A_{pq} of length $\ell + 1$.
   (d) By varying ℓ, deduce that A_{pq} has infinite elasticity.

(6) (continuation) Next we consider the case when $m = p^k$, where p is prime and $k \geq 2$.
   (a) Let ℓ be an arbitrary positive integer. Show that every factorization of $x^\ell + p^{k-1}$ into irreducibles of A_{p^k} has length less than k.
   (b) Prove that $(x^\ell + p^{k-1})^2$ has a factorization into irreducibles of length greater than ℓ.
   (c) Conclude that A_{p^k} has infinite elasticity. (This construction is a very special case of results of Frei and Frisch.[13])

[13] Frei, C.; Frisch, S. *Non-unique factorization of polynomials over residue class rings of the integers.* Comm. Algebra **39** (2011), no. 4, 1482–1490.

(7) (continuation) Finally, we treat the case of general integers $m > 1$. Show that if $d > 1$ is a divisor of m with $\gcd(d, m/d) = 1$, and A_d has infinite elasticity, then A_m also has infinite elasticity. Conclude that A_m has infinite elasticity unless m is prime.

(8) A **gcd monoid** is a cancellative monoid in which every pair of elements has a gcd, i.e., a common divisor divisible by every common divisor. We say the integral domain R is a **gcd domain** if $R \setminus \{0\}$ is a gcd monoid. For example, every UFD is a gcd domain.
   (a) Show that $\mathbb{Z}[\sqrt{-5}]$ is not a gcd domain by exhibiting two specific nonzero elements of $\mathbb{Z}[\sqrt{-5}]$ that do not have a gcd.
   (b) Now let K be any quadratic field. Show that if $\mathbb{Z}_K$ is a gcd domain, then in fact $\mathbb{Z}_K$ is a PID. This strengthens the implication UFD $\Rightarrow$ PID (for $\mathbb{Z}_K$) noted at the start of the chapter. You may assume Landau's theorem that every ideal class contains infinitely many prime ideals (although this can be avoided by appeal to Exercise 9.7).

11

Euler's prime-producing polynomial and the criterion of Frobenius–Rabinowitsch

The following mathematical magic trick is guaranteed to make you the life of the party. Claim that you have discovered a foolproof method for generating infinitely many prime numbers: Beginning with the prime "seed value" $q = 41$, successively add even numbers $2, 4, 6, \ldots$, to obtain

$$43, \quad 47, \quad 53, \quad 61, \quad 71, \quad 83, \quad 97, \quad 113, \quad 131, \ldots,$$

all of which are manifestly prime!

A moment's careful thought is enough to expose the deception here. The terms of our sequence are the values of the polynomial

$$x^2 - x + 41, \quad \text{for } x = 1, 2, 3, \ldots.$$

In this representation, it is obvious that the pattern eventually breaks down. Indeed, the 41st term of the sequence is 41^2, which could not be more clearly composite. What is startling — Euler calls it "especially remarkable"[1] — is that this is the very first occurrence of a composite value. The pattern holds for the first forty terms, and only breaks down when forced to by the algebra.

[1]Euler, L. *Extrait d'une lettre de M. Euler le Pere à M. Bernoulli, concernant le Mémoire imprimé parmi ceux de 1771.* Nouv. Mém. Acad. Berlin, Histoire (1772), 35–36.

The same "trick" could be attempted starting with any seed q. Let

$$f_q(x) = x^2 - x + q.$$

Then $f_q(q) = q^2$ is composite, and it is natural to ask when $x = q$ yields the first composite value. Surprisingly, the answer to this elementary-seeming question is most easily expressed using concepts from algebraic number theory.

The following striking result was independently discovered by F. G. Frobenius[2] and G. Rabinowitsch[3], around 1912. In what follows, τ_d denotes $\frac{1+\sqrt{d}}{2}$. Note that $f_q(x)$ coincides with $\min_\tau(x)$; we will find it convenient to use both notations.

Theorem 11.1. Let q be an integer with $q \geq 2$, and let $d = 1 - 4q$. Then

$$\begin{array}{c} f_q(x) \text{ is prime for all} \\ \text{integers } 0 < x < q \end{array} \iff \mathbb{Z}[\tau_d] \text{ is a UFD.}$$

Example 11.2 ($q = 5$)**.** Since 5, $5 + 2$, $5 + 2 + 4$, and $5 + 2 + 4 + 6$ are all prime, $\mathbb{Z}[\frac{1+\sqrt{-19}}{2}]$ is a UFD.

The next two sections are devoted to the proof of Theorem 11.1. The proof is cleanest when $1 - 4q$ is squarefree. The reason is that then $\mathbb{Z}[\tau_d]$ is the ring of integers of $\mathbb{Q}(\sqrt{d})$, and so all of the machinery we have developed in earlier chapters can be brought to bear. When d is not squarefree, $\mathbb{Z}[\tau_d]$ is a proper subring of the ring of integers; to work around this, slightly ad hoc arguments are required.

Assuming $\mathbb{Z}[\tau_d]$ is a UFD

We begin the proof of Theorem 11.1 with the backward direction ($\Leftarrow$). Assume first that d is squarefree.

Seeking a contradiction, suppose that $f_q(x)$ is composite for some positive integer $x < q$. Since

$$0 < f_q(x) < f_q(q) = q^2,$$

the integer $f_q(x)$ has a prime divisor

$$p < q. \tag{11.1}$$

[2]Frobenius, F. G. *Über quadratische Formen, die viele Primzahlen darstellen.* Sitzungsber. d. Kgl. Preuß. Akad. Wiss. Berlin (1912), 966–980.

[3]Rabinowitsch, G. *Eindeutigkeit der Zerlegung in Primfaktoren in quadratischen Zahlkörpern.* J. reine angew. Math **142** (1913), 153–164.

Thus, $\min_\tau$ has a root modulo p, namely the residue class x mod p. We proved in Chapter 7 (see Theorem 7.3) that there are then two prime ideals of $\mathbb{Z}[\tau_d]$ lying above p, both of norm p. And we proved in Chapter 10 that when $\mathbb{Z}[\tau_d]$ is a UFD, it is in fact a PID. Hence, there are integers a and b with

$$p = N(a + b\tau_d) = (a + b/2)^2 + (q - \frac{1}{4})b^2$$

But $b \neq 0$ (since p is not a square), and so $p \geq q - \frac{1}{4}$. Since p and q are integers, $p \geq q$. This contradicts (11.1).

What if $d = 1 - 4q$ is not squarefree? In that case, $\mathbb{Z}[\tau_d]$ is not a UFD! (So this case does not actually arise.) To see this, write $d = f^2 d'$, where $f \in \mathbb{Z}^+$ and d' is squarefree. Then f is an odd integer larger than 1, and $d' \equiv 1 \pmod 4$. Notice that

$$\tau_d = \frac{1 + f\sqrt{d'}}{2} = f\tau_{d'} - \frac{f-1}{2},$$

and so

$$\mathbb{Z}[\tau_d] = \mathbb{Z}[f\tau_{d'}].$$

For use in a moment, we observe that

$$\tau_{d'} \notin \mathbb{Z}[\tau_d]. \tag{11.2}$$

Indeed, if $\tau_{d'} = a + b\tau_d$ for integers a and b, then $fa + fb\tau_d = f\tau_{d'} = \frac{f-1}{2} + \tau_d$. Comparing imaginary parts yields $fb = 1$, contrary to the fact that $f > 1$.

In a UFD, every fraction can be put in reduced form. Assuming $\mathbb{Z}[\tau_d]$ is a UFD, reduce $\frac{f\tau_{d'}}{f}$. We obtain coprime $\alpha, \beta \in \mathbb{Z}[\tau_d]$ with $\tau_{d'} = \alpha/\beta$. Plugging α/β into the minimal polynomial of $\tau_{d'}$ and multiplying through by β^2,

$$\alpha^2 - \alpha\beta + \frac{1 - d'}{4}\beta^2 = 0.$$

Hence, β divides α^2 in $\mathbb{Z}[\tau_d]$. Since β and α are coprime and $\mathbb{Z}[\tau_d]$ is a UFD, β is a unit in $\mathbb{Z}[\tau_d]$, and $\tau_{d'} = \alpha\beta^{-1} \in \mathbb{Z}[\tau_d]$. This contradicts (11.2).

Assuming f_q generates many primes

We will prove a bit more than is claimed in the forward direction ($\Rightarrow$) of Theorem 11.1. Namely, we show that $\mathbb{Z}[\tau_d]$ is a UFD whenever $f_q(x)$ is prime for all integers x in the (shorter!) range

$$1 \le x \le \frac{1}{2}\sqrt{|d|/3} + \frac{1}{2}. \tag{11.3}$$

We can easily dispense of the case when d is not squarefree. As before, we actually show that this case does not occur. Suppose for a contradiction that $p^2 \mid d$, where p is prime. Since d is odd, p is also odd. Then with $x := \frac{p+1}{2}$,

$$f_q(x) = (p^2 + 4q - 1)/4 = (p^2 - d)/4,$$

which is a multiple of p^2. Hence, $p^2 - d \ge 4p^2$, so that

$$p \le \sqrt{|d|/3}.$$

Thus, $x = \frac{p+1}{2}$ belongs to the range (11.3), and so $f_q(x)$ is supposed to be prime. This is absurd: $p^2 \mid f_q(x)$!

For the rest of the proof, we assume that d is squarefree.

We claim that p is inert in $\mathbb{Z}[\tau_d]$ for all $p \le \sqrt{|d|/3}$. By Theorem 7.3, this amounts to proving that $\min_{\tau_d}$ is irreducible modulo each such p. Suppose instead that it factors. Then $\min_{\tau_d}$ has two roots that (by Vieta's formulas) sum to 1 mod p. Hence, one of the roots has the form x mod p, where $1 \le x \le \frac{p+1}{2} \le \frac{1}{2}\sqrt{|d|/3} + \frac{1}{2}$. Then $p \mid \min_\tau(x)$, but

$$\min_\tau(x) = x^2 - x + q \ge q > \sqrt{\frac{4q-1}{3}} = \sqrt{\frac{|d|}{3}} \ge p.$$

Thus, $\min_\tau(x)$ is composite, which contradicts that f_q is prime-producing in the range (11.3).

The next result delivers the coup de grâce.

Proposition 11.3. Let d be a negative squarefree integer with $d \equiv 1 \pmod 4$. The class group of $\mathbb{Z}[\tau_d]$ is generated by the classes of prime ideals lying above rational primes $p \le \sqrt{|d|/3}$.

We just showed that the prime ideals lying above the primes $p \le \sqrt{|d|/3}$ are the principal ideals generated by those primes. Principal

ideals are trivial in the class group, and so by Proposition 11.3, the class group itself is trivial. Thus, $\mathbb{Z}[\tau_d]$ is a PID and hence a UFD.

To complete the proof of Theorem 11.1, it remains (only) to prove Proposition 11.3.

Generating the class group with small primes

The following lemma plays the key role in the proof of Proposition 11.3.[4]

Lemma 11.4. Let d be a negative squarefree integer with $d \equiv 1 \pmod 4$, and let $K = \mathbb{Q}(\sqrt{d})$. For each $\theta \in K$, there is a positive integer $t \le \sqrt{|d|/3}$ and a $\xi \in \mathbb{Z}_K$ with

$$\mathrm{N}(t\theta - \xi) < 1. \tag{11.4}$$

Recall from Chapter 5 that K is Euclidean exactly when (11.4) can always be always satisfied with $t = 1$. So Lemma 11.4 is asserting that certain fields are "almost-Euclidean".

Proof. Write $\theta = a + b\tau$, with $a, b \in \mathbb{Q}$. A generic $\xi \in \mathbb{Z}_K$ can be written as $A + B\tau$, with $A, B \in \mathbb{Z}$. So our task is to find an integer $t \in [1, \sqrt{|d|/3}]$ along with integers A and B such that $\mathrm{N}((ta - A) + (tb - B)\tau) < 1$, i.e.,

$$\left(ta - A + \frac{tb - B}{2}\right)^2 + |d| \left(\frac{tb - B}{2}\right)^2 < 1. \tag{11.5}$$

Using Dirichlet's approximation theorem (Theorem 8.5), we can find a positive integer $t \le \sqrt{|d|/3}$ with

$$\|tb\| < \frac{1}{\sqrt{|d|/3}}.$$

(Here the approximation theorem has been applied with $Q = \lfloor \sqrt{|d|/3} \rfloor$.) We select B be as a nearest integer to tb. Then

$$|d| \left(\frac{tb - B}{2}\right)^2 < \frac{3}{4}.$$

Now (11.5) holds if A is taken as an integer nearest to $ta + \frac{tb-B}{2}$. □

[4] The lemma and its proof are taken from: Fendel, D. *Prime-producing polynomials and principal ideal domains.* Math. Mag. **58** (1985), no. 4, 204–210.

Proof of Proposition 11.3. Let I be any nonzero ideal of $\mathbb{Z}_K$; we will find a J with $[J] = [I]$ and J composed entirely of prime ideals lying above rational primes $p \le \sqrt{|d|/3}$.

Fix a nonzero $\beta \in I$ chosen so that the norm of β is minimal. We claim that for each $\alpha \in I$, there is a positive integer $t \le \sqrt{|d|/3}$ with $t\alpha \in \langle\beta\rangle$. To see this, use Lemma 11.4 to find a $t \in [1, \sqrt{|d|/3}]$ and a $\xi \in \mathbb{Z}_K$ with

$$\mathrm{N}\left(t\frac{\alpha}{\beta} - \xi\right) < 1.$$

Then $t\alpha - \beta\xi \in I$ while

$$\mathrm{N}(t\alpha - \beta\xi) < \mathrm{N}(\beta).$$

The minimality of β forces

$$t\alpha = \beta\xi \in \langle\beta\rangle,$$

as desired.

Thus, if we set $T = \prod_{t \le \sqrt{|d|/3}} t$, then $T\alpha \in \langle\beta\rangle$ for every $\alpha \in I$. That is, $TI \subseteq \langle\beta\rangle$. Hence, $J := \frac{T}{\beta} I \subseteq \mathbb{Z}_K$. This containment guarantees that J is an ideal of $\mathbb{Z}_K$, and J is obviously dilation equivalent to I. Moreover, since $\beta \in I$,

$$T = \frac{T}{\beta}\beta \in \frac{T}{\beta} I = J,$$

and hence J divides $\langle T\rangle$. It is now immediate from the definition of T that the prime ideals dividing J all lie above rational primes $p \le \sqrt{|d|/3}$. □

Addressing the elephant in the room

Theorem 11.1 tells us that two conditions are equivalent, one having to do with prime production and the other with unique factorization. When does either condition hold? We saw in the course of the proof that for this to happen, d must be squarefree, so that $\mathbb{Z}[\tau_d]$ is the ring of integers of $\mathbb{Q}(\sqrt{d})$. Thus, our question really amounts to the following.

Question 11.5. For which negative integers $d \equiv 1 \pmod 4$ does $\mathbb{Q}(\sqrt{d})$ have class number 1?

Actually, it is easy to show that for negative squarefree $d \equiv 2, 3 \pmod 4$, the class number is 1 only when $d = -1$ or $d = -2$ (see Exercise 1). So we might as well remove the restriction to $d \equiv 1 \pmod 4$ and ask for a list of all imaginary quadratic fields of class number 1.

Building on earlier work of Hecke, Deuring, and Mordell, Heilbronn showed in 1934 that this is a finite list. In fact, he proved that

$$h_{\mathbb{Q}(\sqrt{d})} \to \infty \quad \text{as} \quad d \to -\infty. \tag{11.6}$$

(Here d is restricted to squarefree values.) Unfortunately, the method of proof is *ineffective*. Given a B, there is no way (even in principle) to bound those negative d for which $h_{\mathbb{Q}(\sqrt{d})} \le B$. This applies even when $B = 1$!

It was almost twenty years later, in 1952, that Kurt Heegner made the first rigorous determination of the class number 1 imaginary quadratic fields. Heegner's work was not easy to read, and his arguments were widely thought to contain serious gaps. The first generally accepted solutions to the problem were given by Baker (in 1966) and Stark (in 1967). Shortly afterwards, Deuring and Stark re-examined Heegner's work and found that it was essentially correct. Sadly, Heegner passed away in 1965, and so never lived to see his vindication.

Theorem 11.6 (Heegner–Baker–Stark)**.** Let $d < 0$ be squarefree. Then $\mathbb{Q}(\sqrt{d})$ has class number 1 if and only if d is one of -1, -2, -3, -7, -11, -19, -43, -67, -163.

A proof of Theorem 11.6, following Heegner's original approach, is described in a beautiful monograph of David A. Cox.[5]

What is the upshot of all of this for Theorem 11.1? The largest value of $|d|$ in Theorem 11.6 is 163, and

$$-163 = 1 - 4 \cdot 41.$$

Thus, the example $x^2 - x + 41$, known already to Euler in 1772, cannot be beat!

We conclude with two remarks. First, these is a natural related problem in which Euler's example is almost certainly not optimal.

[5]Cox, D. A. *Primes of the form $x^2 + ny^2$. Fermat, class field theory, and complex multiplication.* Second edition. John Wiley & Sons, Inc., Hoboken, NJ, 2013.

Problem 11.7. Find the largest $B \in \mathbb{Z}^+$ for which there is some seed value $q \in \mathbb{Z}^+$ with

$$x^2 - x + q \text{ prime for all } x = 1, 2, 3, \ldots, B.$$

Actually, Problem 11.7 is probably ill-formed, in that there is no largest B. Andrew Granville noted[6] that this would follow from the **Hardy–Littlewood prime tuples conjecture**, which is a certain plausible generalization of the celebrated twin prime conjecture. (See Exercise 7.) But so far, no one has discovered a seed value q that works when $B = 41$ (thus supplanting Euler's example). Computations of Lukes, Patterson, and Williams[7] show that any such q exceeds 10^{18}. Euler, winner and still champion!

Second, the reader may be wondering about class number 1 *real* quadratic fields. Here the story is very different from the imaginary case. Corresponding to (11.6), one can show that

$$h_{\mathbb{Q}(\sqrt{d})} \cdot \log \epsilon_d \to \infty, \tag{11.7}$$

as $d \to \infty$ (through squarefree values), where ϵ_d is the fundamental unit.[8] But this leaves open the possibility that there are infinitely many real quadratic fields of class number 1 (necessarily having a large fundamental unit). In fact, a heuristic model of Cohen and Lenstra — borne out by computation — predicts that $\mathbb{Q}(\sqrt{p})$ has class number 1 for more than 75% of all primes p.[9]

---

[6] See Theorem 3.3 in: Louboutin, S.; Mollin, R. A.; Williams, H. C. *Class numbers of real quadratic fields, continued fractions, reduced ideals, prime-producing quadratic polynomials and quadratic residue covers.* Canad. J. Math. **44** (1992), no. 4, 824–842.

[7] Lukes, R. F.; Patterson, C. D.; Williams, H. C. *Numerical sieving devices: their history and some applications.* Nieuw Arch. Wisk. (4) **13** (1995), no. 1, 113–139.

[8] For proofs of (11.6) and (11.7), see Chapter 21 of: Davenport, H. *Multiplicative number theory.* 3rd edition. Graduate Texts in Mathematics **74**. Springer-Verlag, New York, 2000.

[9] See: Cohen, H.; Lenstra, H. W., Jr. *Heuristics on class groups of number fields.* Number theory, Noordwijkerhout 1983 (Noordwijkerhout, 1983), 33–62, Lecture Notes in Math. **1068**, Springer, Berlin, 1984.

The exact proportion of these primes p is supposed to be $\left(\frac{1}{2} \cdot \prod_{i=1}^{\infty}(1 - 2^{-i})^{-1}\right) \cdot \prod_{j=1}^{\infty} \zeta(j+1)$, where $\zeta(s) := \sum_{n=1}^{\infty} \frac{1}{n^s}$. This works out to ≈ 0.754458.

Exercises

(1) Prove that if d is squarefree, $d < -2$, and $d \equiv 2, 3 \pmod 4$, then the class number of $\mathbb{Q}(\sqrt{d})$ is even. *Hint:* 2 ramifies in $\mathbb{Q}(\sqrt{d})$. Show that the prime ideal above 2 has order 2 in $\mathrm{Cl}(\mathbb{Z}_K)$.

(2) Prove the easy half of the Heegner–Baker–Stark theorem: $\mathbb{Q}(\sqrt{d})$ has class number 1 for each of $d = -1, -2, -3, -7, -11, -19, -43, -67, -163$.

(3) Let K be a quadratic field, and write $K = \mathbb{Q}(\sqrt{d})$ with d squarefree. Put

$$\Delta = \begin{cases} 4d & \text{if } d \equiv 2, 3 \pmod 4, \\ d & \text{if } d \equiv 1 \pmod 4. \end{cases}$$

(This is called the **discriminant of** K. We will define discriminants of number fields in Chapter 13.)

(a) First, suppose that $d < 0$. When $d \equiv 1 \pmod 4$, Proposition 11.3 asserts that the class group of $\mathbb{Z}_K$ is generated by the classes $[P]$, where P runs over the prime ideals above rational primes $p \le \sqrt{|\Delta|/3}$. Prove that the same is true when $d \equiv 2, 3 \pmod 4$.

(b) Now suppose that $d > 0$. Prove that $\mathrm{Cl}(\mathbb{Z}_K)$ is generated by the classes $[P]$, where P runs over the prime ideals above rational primes $p \le \sqrt{\Delta/5}$.

(4) (Möller[10]) Let $q \in \mathbb{Z}$ with $q \ge 2$, and assume that $d = 1 - 4q$ is squarefree. Let $K = \mathbb{Q}(\sqrt{d})$, and let D_q denote the Davenport constant of $\mathrm{Cl}(\mathbb{Z}_K)$. Writing $\Omega(\cdot)$ for the number of prime factors, counted with multiplicity, set

$$\mathrm{Ono}_q = \max\{\Omega(x^2 - x + q) : 1 \le x \le q - 1\}.$$

(a) Choose $x \in \{1, 2, \ldots, q-1\}$ with $\Omega(x^2 - x + q) = \mathrm{Ono}_q$. Show that $\langle x - \tau \rangle$ is a product of Ono_q (not necessarily distinct) prime ideals.

(b) Show that $\langle x - \tau \rangle$ cannot be written as a nontrivial product of principal ideals.

(c) Deduce that $\mathrm{Ono}_q \le D_q$.

---

[10] Möller, H. *Verallgemeinerung eines Satzes von Rabinowitsch über imaginär-quadratische Zahlkörper.* J. reine angew. Math. **285** (1976), 100–113.

(5) (Sasaki[11]) Let $q \in \mathbb{Z}$ with $q \geq 2$, and assume $d = 1-4q$ is squarefree. Let $K = \mathbb{Q}(\sqrt{d})$. In this exercise, we outline a proof that

$$h_K = 2 \iff \mathrm{Ono}_q = 2.$$

(a) Show the forward ($\Rightarrow$) implication using Exercise 4 and the Frobenius–Rabinowitsch theorem. In the remaining parts, we focus on the backward ($\Leftarrow$) direction.
Assume $\mathrm{Ono}_q = 2$.

(b) Let p be a prime that splits in $\mathbb{Z}_K$. Show that $x^2 - x + q$ has a root modulo p^2.

(c) Let p be a prime that splits in $\mathbb{Z}_K$ with $p \leq \sqrt{|d|/3}$. Show that there is an integer x with $1 \leq x \leq q-1$ and $x^2 - x + q = p^2$. Deduce that if $\langle p \rangle = P_1 P_2$, with P_1 and P_2 prime ideals, then $[P_1]^2 = [P_2]^2 = [\langle 1 \rangle]$; moreover, $[P_1] = [P_2]$.

(d) Let p_1 and p_2 be distinct non-inert primes in $\mathbb{Z}_K$. Explain why $x^2 - x + q$ has a root modulo $p_1 p_2$.

(e) Show that if p_1 and p_2 are distinct non-inert primes in $\mathbb{Z}_K$ with $p_1, p_2 \leq \sqrt{|d|/3}$, then there is an integer x with $1 \leq x \leq q-1$ and $x^2 - x + q = p_1 p_2$. Deduce that if P_1 is any prime above p_1 and P_2 any prime above p_2, then $[P_1] = [P_2]$.

(f) Prove that $h_K = 2$.

Warning concerning Exercises 4 and 5: Do not fall into the trap of thinking that $h_K = \mathrm{Ono}_q$ generally. It is a simple exercise to show that $\mathrm{Ono}_q \leq 3 \log q$ for all q. (Try it!) On the other hand, the known quantitative versions of (11.6) imply that $h_K \geq q^{1/2-\epsilon}$, for any $\epsilon > 0$ and all $q > q_0(\epsilon)$. Thus, $\mathrm{Ono}_q = h_K$ for only finitely many q ![12]

(6) Deduce from the Heegner–Baker–Stark theorem and the law of quadratic reciprocity that if p is a prime, $p \equiv 3 \pmod 4$, and $p > 163$, then there is a prime $\ell \leq \sqrt{p/3}$ which is a quadratic residue modulo p.

---

[11] Sasaki, R. *On a lower bound for the class number of an imaginary quadratic field.* Proc. Japan Acad. Ser. A Math. Sci. **62** (1986), no. 1, 37–39. This article is also the origin of the term **Ono invariant** for the quantity we are denoting Ono_q.

[12] For a probably, but not yet provably, complete list, see: Louboutin, S. R. *On the Ono invariants of imaginary quadratic number fields.* J. Number Theory **129** (2009), no. 10, 2289–2294.

(7) (Granville) The **Hardy–Littlewood prime tuples conjecture** claims the following: *Let* $\{a_1, \ldots, a_k\}$ *be a finite set of integers with the property that for each prime* p*, the list of residue classes*

$$a_1 \bmod p, \quad a_2 \bmod p, \quad \ldots, \quad a_k \bmod p$$

omits at least one residue class mod p*. Then there are infinitely many* $n \in \mathbb{Z}^+$ *for which all of* $n + a_1$*,* $n + a_2$*, . . . ,* $n + a_k$ *are simultaneously prime.*[13] The still-unproved **twin prime conjecture** is the special case $\{0, 2\}$ of the tuples conjecture.

Assuming the tuples conjecture, prove that for every B, there is a $q \in \mathbb{Z}^+$ such that $x^2 - x + q$ is prime for all integers $1 \le x \le B$.

Hint: Apply the tuples conjecture to $\{x^2 - x : 1 \le x \le B\}$.

[13] See Theorem X (part I), p. 61, and the preceding discussion in: Hardy, G. H.; Littlewood, J. E. *Some problems of 'Partitio numerorum' III: On the expression of a number as a sum of primes.* Acta. Math. **44** (1923), 1–70. In fact, Hardy and Littlewood conjecture an asymptotic formula for the count of such $n \le x$, as $x \to \infty$.

12

Interlude: Lattice points

A (standard) **lattice point** in $\mathbb{R}^n$ is a point $(x_1, \ldots, x_n)$ with all of the x_i integers, i.e., an element of $\mathbb{Z}^n$. The following problem is the launching off point for the subfield of number theory known as the **geometry of numbers**.

Problem 12.1. Given a bounded region $\mathcal{R}$ in n-dimensional Euclidean space, estimate the number of lattice points contained inside, i.e.,

$$\sum_{\mathbf{v} \in \mathbb{Z}^n} 1_{\mathcal{R}}(\mathbf{v}).$$

One expects that for most reasonable choices of $\mathcal{R}$, the count of lattice points is well approximated by the volume of $\mathcal{R}$.[1] To see why, imagine that every lattice point in $\mathcal{R}$ is taken as the "lower-left" corner of an n-dimensional unit cube. If the region is large and the boundary is not too irregular, the sum of the volumes of the cubes — which is just the lattice point count — should not be too far off from the volume of $\mathcal{R}$.

To formulate a precise statement of this kind, we consider a family of expanding regions rather than a single region. Specifically, fix a bounded subset $\mathcal{R} \subseteq \mathbb{R}^n$ that is Jordan measurable (i.e., has a well-defined volume). For each $t > 0$, let $t\mathcal{R}$ denote the dilation of $\mathcal{R}$ by a factor of t, i.e.,

$$t\mathcal{R} = \{t\mathbf{x} : \mathbf{x} \in \mathcal{R}\}.$$

[1] Throughout this book, "volume" means **Jordan volume**, defined by $\mathrm{vol}(\mathcal{R}) := \int_{\mathbb{R}^n} 1_{\mathcal{R}}(\mathbf{x})\, d\mathbf{x}$, an n-dimensional *Riemann* integral.

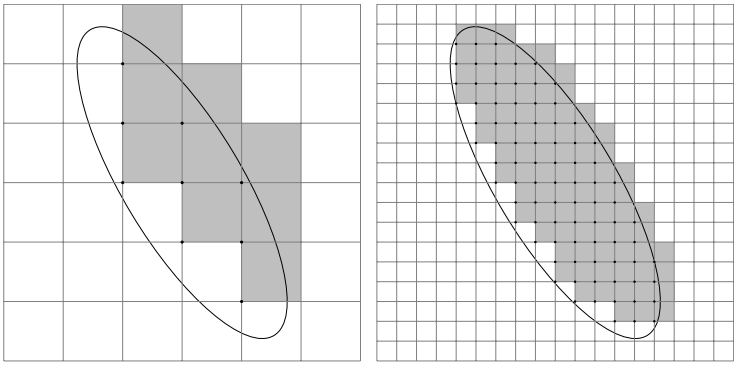


Figure 12.1. Approximations to the area of an ellipse in $\mathbb{R}^2$. The left-hand drawing illustrates the area approximation obtained by counting interior points from $\mathbb{Z} \times \mathbb{Z}$. The right-hand image shows the more accurate approximation using points of $\frac{1}{3}\mathbb{Z} \times \frac{1}{3}\mathbb{Z}$.

Then, as $t \to \infty$, the count of lattice points inside $t\mathbb{R}$ agrees with $\mathrm{vol}(t\mathcal{R})$, up to lower order terms:

Theorem 12.2 (Fundamental point counting principle)**.** As $t \to \infty$,

$$\frac{1}{t^n} \sum_{\mathbf{v} \in \mathbb{Z}^n} 1_{t\mathcal{R}}(\mathbf{v}) \to \mathrm{vol}(\mathcal{R}).$$

There is surprisingly little to prove here once one unwinds the relevant definitions. Observe that

$$\frac{1}{t^n} \sum_{\mathbf{v} \in \mathbb{Z}^n} 1_{t\mathcal{R}}(\mathbf{v}) = \frac{1}{t^n} \sum_{\mathbf{w} \in (\frac{1}{t}\mathbb{Z})^n} 1_{\mathcal{R}}(\mathbf{w}).$$

The right-hand side is a Riemann sum for

$$\int_{\mathbb{R}^n} 1_{\mathcal{R}}(\mathbf{x})\, d\mathbf{x},$$

where the plane has been partitioned into cubes of side length t^{-1}. (Cf. Figure 12.1.) Since the mesh of this partition tends to 0 as $t \to \infty$, Theorem 12.2 follows from the definition of the multidimensional Riemann integral.

Minkowski's convex body theorem, take one

It is easy to see that there are n-dimensional regions with arbitrarily large volume that fail to intersect $\mathbb{Z}^n$ (consider, for instance, a large ball with holes cut out). Thus, any theorem guaranteeing the existence of lattice points in $\mathcal{R}$ must assume more that a lower bound on $\mathrm{vol}(\mathcal{R})$. The following elegant result in this direction was proved by Hermann Minkowski ca. 1891.[2]

Theorem 12.3. Let $\mathcal{R} \subseteq \mathbb{R}^n$ be a bounded region that is

(a) **convex**: the line segment connecting any two points in $\mathcal{R}$ is contained in $\mathcal{R}$, *and*

(b) **centrally symmetric**: whenever $\mathbf{x} \in \mathcal{R}$, also $-\mathbf{x} \in \mathcal{R}$.

If $\mathrm{vol}(\mathcal{R}) > 2^n$, then $\mathcal{R}$ contains a nonzero lattice point.

We make two remarks. First, it is clear that a nonempty, convex, centrally symmetric set always contains $\mathbf{o}$. So the word "nonzero" in the conclusion of Theorem 12.3 is needed for the theorem to be nontrivial. Second, the lower bound assumed on the volume cannot be improved upon; the n-dimensional open "cube" $(-1,1)^n$ is centrally symmetric, convex, and has volume exactly 2^n, but contains no nonzero lattice points.

The following crisp proof of Theorem 12.3 is due to Mordell.[3]

Proof. For all sufficiently large positive integers m, the fundamental point counting principle shows that

$$\frac{1}{m^n} \sum_{\mathbf{v} \in \mathbb{Z}^n} 1_{m\mathcal{R}}(\mathbf{v}) > 2^n, \quad \text{so that} \quad \sum_{\mathbf{v} \in \mathbb{Z}^n} 1_{m\mathcal{R}}(\mathbf{v}) > (2m)^n.$$

(We use here the assumption that $\mathrm{vol}(\mathcal{R}) > 2^n$.) Since the quotient $\mathbb{Z}^n / 2m\mathbb{Z}^n$ has size $(2m)^n$, there are distinct lattice points $\mathbf{v}_1, \mathbf{v}_2 \in m\mathcal{R}$ with $\mathbf{v}_1 \equiv \mathbf{v}_2 \pmod{2m}$. Thus,

$$\frac{\mathbf{v}_1 - \mathbf{v}_2}{2m} \in \mathbb{Z}^n \setminus \{\mathbf{o}\}.$$

[2] This statement first appears (for $n = 3$) in the written summary of an 1891 lecture by Minkowski in the city of Halle, Germany. See: *Über Geometrie der Zahlen.* Werke, Bd. 1 (1911), 264–265.

[3] Mordell, L. J. *On some arithmetical results in the geometry of numbers.* Compos. Math. **1** (1935), 248–253.

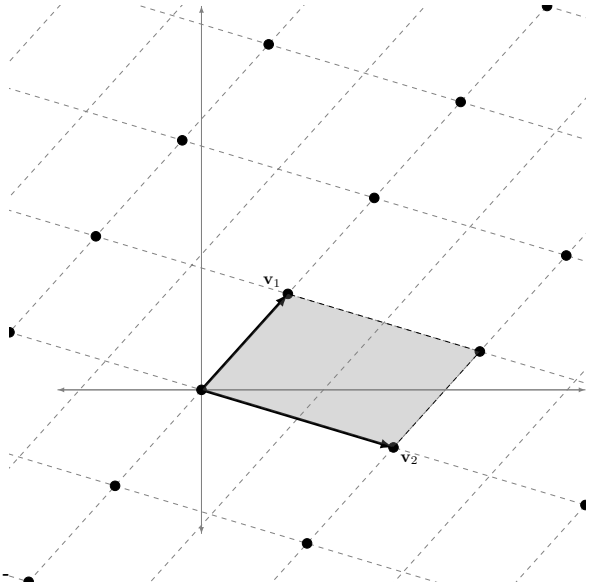


Figure 12.2. A lattice in $\mathbb{R}^2$ generated by vectors $\mathbf{v}_1$, $\mathbf{v}_2$, along with the corresponding fundamental parallelepiped (shaded).

It suffices to argue that the left-hand side also belongs to $\mathcal{R}$. We know that $\frac{1}{m}\mathbf{v}_1, \frac{1}{m}\mathbf{v}_2 \in \mathcal{R}$. By central symmetry, $-\frac{1}{m}\mathbf{v}_2 \in \mathcal{R}$. By convexity, the midpoint of $\frac{1}{m}\mathbf{v}_1$ and $-\frac{1}{m}\mathbf{v}_2$ lies in $\mathcal{R}$; but this is just $\frac{\mathbf{v}_1-\mathbf{v}_2}{2m}$. □

Minkowski's theorem, take two

In applications, one often needs to show that a region contains points from a specified "lattice" other than $\mathbb{Z}^n$.

Definition 12.4. Let $n \in \mathbb{Z}^+$. By a **lattice** Λ in $\mathbb{R}^n$, we mean any subgroup of $\mathbb{R}^n$ obtained by taking the $\mathbb{Z}$-span of a collection of $\mathbb{R}$-linearly independent vectors (which are said to form a **basis** for Λ).

In general, a given lattice Λ has many different bases. For example, the standard lattice $\mathbb{Z}^2$ is (obviously) generated by $\left[\begin{smallmatrix}1\\0\end{smallmatrix}\right], \left[\begin{smallmatrix}0\\1\end{smallmatrix}\right]$, and (less obviously) generated by $\left[\begin{smallmatrix}3\\2\end{smallmatrix}\right], \left[\begin{smallmatrix}7\\5\end{smallmatrix}\right]$. However, the number of elements in each basis is the same. To see why, notice that if $\mathbf{v}_1, \ldots, \mathbf{v}_k$ is a basis for Λ, then the $\mathbb{R}$-span of Λ — call this $\Lambda \otimes \mathbb{R}$ — is the $\mathbb{R}$-span of the

$\mathbf{v}_i$. Thus, the number of vectors in any basis for Λ coincides with the $\mathbb{R}$-dimension of the real vector space $\Lambda \otimes \mathbb{R}$. We call this nonnegative integer the **rank** of Λ.

Suppose that Λ is a rank n lattice in $\mathbb{R}^n$ with basis $\mathbf{v}_1, \ldots, \mathbf{v}_n$. (A lattice whose rank matches the dimension of the ambient space is called a **full lattice**.) The **fundamental parallelepiped** corresponding to the $\mathbf{v}_i$ is the region in $\mathbb{R}^n$ defined by

$$\mathcal{P}(\mathbf{v}_1, \ldots, \mathbf{v}_n) := \{c_1\mathbf{v}_1 + \cdots + c_n\mathbf{v}_n : 0 \leq c_i < 1 \text{ for each } i\}.$$

It is a basic fact from multivariable calculus that

$$\text{vol}(\mathcal{P}(\mathbf{v}_1, \ldots, \mathbf{v}_n)) = |\det[\mathbf{v}_1, \ldots, \mathbf{v}_n]|, \tag{12.1}$$

where $[\mathbf{v}_1, \ldots, \mathbf{v}_n]$ is the matrix whose columns are the $\mathbf{v}_i$. Suppose now that $\mathbf{w}_1, \ldots, \mathbf{w}_n$ is another basis for Λ. Since the $\mathbf{v}_j$ generate Λ, each $\mathbf{w}_i$ can be written as a $\mathbb{Z}$-linear combination of the $\mathbf{v}_j$; doing so, we obtain an $n \times n$ integer matrix M with

$$[\mathbf{w}_1, \ldots, \mathbf{w}_n] = [\mathbf{v}_1, \ldots, \mathbf{v}_n] \cdot M. \tag{12.2}$$

But we could equally well have started in the other direction; we would then have found an $n \times n$ integer matrix N with

$$[\mathbf{v}_1, \ldots, \mathbf{v}_n] = [\mathbf{w}_1, \ldots, \mathbf{w}_n] \cdot N.$$

Plug this back into (12.2). We find that right-multiplication by NM preserves $[\mathbf{w}_1, \ldots, \mathbf{w}_n]$. The matrix $[\mathbf{w}_1, \ldots, \mathbf{w}_n]$ is invertible (since the $\mathbf{w}_i$ are linearly independent), and so NM must be the $n \times n$ identity matrix. Hence,

$$\det(N)\det(M) = \det(NM) = 1.$$

Since N and M have integer entries, $\det(N) = \det(M) = \pm 1$. We now deduce from (12.1) and (12.2) that

$$\text{vol}(\mathcal{P}(\mathbf{w}_1, \ldots, \mathbf{w}_n)) = \text{vol}(\mathcal{P}(\mathbf{v}_1, \ldots, \mathbf{v}_n)).$$

Hence, the volume of the fundamental parallelepiped is independent of the choice of basis for Λ; we call this invariant the **covolume of** Λ and denote it $\text{covol}(\Lambda)$.

We are now ready to state version 2.0 of Minkowski's fundamental theorem.

Theorem 12.5. Let Λ be a full rank lattice in $\mathbb{R}^n$. Let $\mathcal{R}$ be a bounded, convex, centrally symmetric region in $\mathbb{R}^n$ with

$$\mathrm{vol}(\mathcal{R}) > 2^n \,\mathrm{covol}(\Lambda).$$

Then $\mathcal{R}$ contains a nonzero vector from Λ.

Theorem 12.5 can be deduced from Theorem 12.3 by the following maneuver. Let $\mathbf{v}_1, \ldots, \mathbf{v}_n$ be vectors generating Λ. Let $T\colon \mathbb{R}^n \to \mathbb{R}^n$ be the linear transformation sending the ith standard basis vector $\mathbf{e}_i$ (say) to $\mathbf{v}_i$. Since the $\mathbf{v}_i$ are linearly independent, T is a linear isomorphism, and clearly

$$T(\mathbb{Z}^n) = \Lambda.$$

Moreover — this is essentially the same basic fact from multivariable calculus alluded to above — a region $\mathcal{R}_0 \subseteq \mathbb{R}^n$ has a well-defined n-dimensional volume if and only if the same is true for $T(\mathcal{R}_0)$, in which case $\mathrm{vol}(T(\mathcal{R}_0)) = \mathrm{vol}(\mathcal{R}_0) \cdot \mathrm{covol}(\Lambda)$.

With these facts in hand, we leave it to the reader to check that, under the assumptions of Theorem 12.5, the region $T^{-1}(\mathcal{R})$ satisfies the hypotheses of Theorem 12.3. Thus, there is a nonzero $\mathbf{v} \in T^{-1}(\mathcal{R}) \cap \mathbb{Z}^n$, and $T(\mathbf{v})$ is a nonzero element of $\mathcal{R} \cap \Lambda$.

Sums of four squares

To illustrate the power of Minkowski's theorem, we give a conceptually simple proof of one of the most remarkable results of elementary number theory.

Theorem 12.6 (Lagrange[4])**.** Every positive integer can be written as a sum of four squares.

The argument we present is a simplification due to Davenport[5] of an 1853 proof of Hermite (who, of course, did not have Minkowski's theorem at his disposal).

The proof depends on the following elementary lemma.

[4]Lagrange, J.L. *Demonstration d'un théorème d'arithmétique.* Nouv. Mém. Acad. Berlin **1** (1770), 123–133.

[5]Davenport, H. *The geometry of numbers.* Math. Gaz. **31** (1947), 206–210.

Lemma 12.7. For each squarefree positive integer m, there are integers A and B with

$$A^2 + B^2 + 1 \equiv 0 \pmod{m}.$$

Proof. By the Chinese remainder theorem, it is enough to treat the case when m is prime, say $m = p$. If $p = 2$, we can take $A = 1$ and $B = 0$, and so we suppose that p is an odd prime. The assertion of the lemma is equivalent to the claim that the sets $S := \{A^2 \bmod p : A \in \mathbb{Z}\}$ and $\mathcal{T} := \{-1 - B^2 \bmod p : B \in \mathbb{Z}\}$ are not disjoint subsets of $\mathbb{Z}/p\mathbb{Z}$. Since $\mathbb{Z}/p\mathbb{Z}$ is a field,

$$x^2 \equiv y^2 \pmod{p} \iff x \equiv \pm y \pmod{p}.$$

As a consequence, there are precisely $\frac{p+1}{2}$ distinct squares modulo p, namely the reductions mod p of $0^2, 1^2, \ldots, (\frac{p-1}{2})^2$. Thus, both S and $\mathcal{T}$ have size $\frac{p+1}{2}$. Since $\frac{p+1}{2} > \frac{1}{2}\#\mathbb{Z}_p$, the sets S and $\mathcal{T}$ are not disjoint. □

Given a squarefree positive integer m, we fix integers A and B satisfying the conclusion of Lemma 12.7. Put $\gamma = A + Bi \in \mathbb{Z}[i]$, so that $N\gamma \equiv -1 \pmod{m}$.

We consider all pairs of $\alpha, \beta \in \mathbb{Z}[i]$ satisfying the congruence

$$\alpha \equiv \beta\gamma \pmod{m}. \tag{12.3}$$

Note that for each such pair,

$$\bar{\alpha} \equiv \bar{\beta}\bar{\gamma} \pmod{m}.$$

(Here $\bar{\cdot}$ denotes complex conjugation.) Multiplying the last two displays,

$$N(\alpha) \equiv N(\beta)N(\gamma) \equiv -N(\beta) \pmod{m},$$

and so

$$N(\alpha) + N(\beta) \equiv 0 \pmod{m}.$$

Hence, writing $\alpha = a + bi$ and $\beta = c + di$,

$$a^2 + b^2 + c^2 + d^2 \equiv 0 \pmod{m}. \tag{12.4}$$

We now argue that the vectors $\begin{bmatrix} a \\ b \\ c \\ d \end{bmatrix} \in \mathbb{Z}^4$ that arise in this way (i.e., from a pair of α, β satisfying (12.3)) make up a lattice in $\mathbb{R}^4$. We

can rewrite (12.3) in the form

$$a + bi = (c + di)(A + Bi) + m(C + Di) \quad \text{for some } C, D \in \mathbb{Z}.$$

Expanding the right-hand side and comparing real and imaginary parts,

$$\begin{aligned} a &= Ac - Bd + Cm, \\ b &= Ad + Bc + Dm. \end{aligned}$$

Equivalently,

$$\begin{aligned} \begin{bmatrix} a \\ b \\ c \\ d \end{bmatrix} &= \begin{bmatrix} Ac - Bd + Cm \\ Ad + Bc + Dm \\ c \\ d \end{bmatrix} \\ &= c \begin{bmatrix} A \\ B \\ 1 \\ 0 \end{bmatrix} + d \begin{bmatrix} -B \\ A \\ 0 \\ 1 \end{bmatrix} + C \begin{bmatrix} m \\ 0 \\ 0 \\ 0 \end{bmatrix} + D \begin{bmatrix} 0 \\ m \\ 0 \\ 0 \end{bmatrix}. \end{aligned} \tag{12.5}$$

We conclude that the tuples $\begin{bmatrix} a \\ b \\ c \\ d \end{bmatrix}$ corresponding to the pairs α, β are precisely those belonging to Λ, where Λ is defined as the $\mathbb{Z}$-span of the four vectors on the right-hand side of (12.5).

An easy calculation shows that

$$\det \begin{bmatrix} A & -B & m & 0 \\ B & A & 0 & m \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{bmatrix} = m^2.$$

Since the determinant is nonzero, the columns are linearly independent, which allows us to conclude that Λ is a full rank lattice in $\mathbb{R}^4$. Moreover, as a byproduct of this calculation,

$$\operatorname{covol}(\Lambda) = m^2.$$

Let $\mathcal{R}$ denote the 4-dimensional open ball centered at the origin and having radius $\sqrt{2m}$, i.e.,

$$\mathcal{R} = \{\mathbf{x} \in \mathbb{R}^4 : \|\mathbf{x}\|^2 < 2m\}. \tag{12.6}$$

It is obvious that $\mathcal{R}$ is centrally symmetric. The convexity of $\mathcal{R}$ is a straightforward consequence of the triangle inequality for the Euclidean norm. Moreover,[6]

$$\begin{aligned}\operatorname{vol}(\mathcal{R}) = \frac{1}{2}\pi^2(\sqrt{2m})^4 &= 2\pi^2 m^2 \\ &> 2^4 m^2.\end{aligned}$$

(Note that $2\pi^2 \approx 19.74$.) By Minkowski's theorem, $\mathcal{R}$ contains a nonzero element of Λ, say $\begin{bmatrix} a \\ b \\ c \\ d \end{bmatrix}$. From (12.4) and (12.6), $a^2+b^2+c^2+d^2$ is a nonzero multiple of m smaller than $2m$. Hence,

$$a^2 + b^2 + c^2 + d^2 = m.$$

The arguments so far show that every *squarefree* positive integer m is a sum of four squares. The general case is no harder: Any $m \in \mathbb{Z}^+$ can be written in the form $f^2 m'$, where m' is squarefree. A representation of m' as a sum of four squares immediately yields a corresponding representation of m, upon absorbing the factor of f^2 into each of the summands.

Exercises

(1) Fix an integer d. Show that if p is a prime that can be written in the form $x^2 + dy^2$, with $x, y \in \mathbb{Z}$, then $-d$ is a square modulo p.

(2) (Fermat's two squares theorem) Let p be a prime, $p \equiv 1 \pmod 4$.
   (a) From elementary number theory, -1 is a square mod p. Use this fact to construct a lattice $\Lambda \subseteq \mathbb{Z}^2$ having $\operatorname{covol}(\Lambda) = p$ and with the property that $x^2 + y^2 \equiv 0 \pmod p$ whenever $(x, y) \in \Lambda$.
   (b) Using Theorem 12.5, show that Λ contains a nonzero point (a, b) with $x^2 + y^2 < 2p$. Conclude that p is a sum of two squares.

(3) (a) Let p be a prime with $p \equiv 1, 3 \pmod 8$, so that -2 is a square mod p. Show that $p = x^2 + 2y^2$ for some $x, y \in \mathbb{Z}$.

[6] Recall that the volume of a ball of radius r in $\mathbb{R}^n$ is $\frac{\pi^{n/2}}{\frac{n}{2}!} r^n$ when n is even and is $2\frac{(2\pi)^{(n-1)/2}}{1\cdot 3\cdot 5\cdots n} r^n$ when n is odd.

(b) Let $p \equiv 1 \pmod 3$, so that -3 is a square mod p. Show that $p = x^2 + 3y^2$ for some $x, y \in \mathbb{Z}$. *Hint:* Show that $x^2 + 3y^2$ represents a positive multiple of p smaller than $3p$. Then argue that $2p$ is not represented.

(4) Let p be a prime $\neq 2, 5$. It is known that -5 is a square mod p precisely when $p \equiv 1, 3, 7,$ or $9 \pmod{20}$.

(a) Show that if $p \equiv 3$ or $7 \pmod{20}$, then p is *not* expressible in the form $x^2 + 5y^2$. *Hint:* Look mod 4.

(b) Show that if $p \equiv 1$ or $9 \pmod{20}$, then p is so expressible.[7]

(5) (van der Corput[8]) Let k be a positive integer.

(a) Let $\mathcal{R}$ be a bounded region in $\mathbb{R}^n$ with $\mathrm{vol}(\mathcal{R}) > k$. Show that $\mathcal{R}$ contains $k+1$ distinct points that are mutually congruent modulo $\mathbb{Z}^n$. *Hint:* The number of $\mathbb{Z}^n$-points in $m\mathcal{R}$ exceeds $m^n k$, for all large enough positive integers m.

(b) Let $\mathcal{R}$ be a bounded, convex, centrally symmetric region in $\mathbb{R}^n$ with $\mathrm{vol}(\mathcal{R}) > 2^n k$. Show that one can find k distinct nonzero points

$$\mathbf{v}_1, \ldots, \mathbf{v}_k \in \mathcal{R} \cap \mathbb{Z}^n,$$

no one of which can be obtained from another by a reflection about the origin.

(c) Part (b) generalizes Theorem 12.3. Formulate and prove the corresponding generalization of Theorem 12.5.

(6) (Four squares theorem, encore) This exercise outlines a proof of Lagrange's four squares theorem based on quaternion arithmetic, as introduced in Exercises 5.2 and 5.3.[9]

(a) Let p be a prime number. Choose $A, B \in \mathbb{Z}$ with $A^2 + B^2 + 1 \equiv 0 \pmod p$, and let I be the right ideal of $\mathbb{Z}_{\mathbb{H}}$ generated by $1 + Ai + Bj$ and p. Show that I is not the unit ideal of $\mathbb{Z}_{\mathbb{H}}$.

Hint: Show that the norm of every element of I is a multiple of p.

---

[7] For much more on the theme of Exercises 1–3, see: Clark, P.L.; Hicks, J.; Parshall, H.; Thompson, K. *GoNI: Primes represented by binary quadratic forms.* INTEGERS **13** (2013), A37, 18pp.

[8] van der Corput, J. *Verallgemeinerung einer Mordellschen Beweismethode in der Geometrie der Zahlen, Zweite Mitteilung.* Acta Arith. **2** (1936), 145–146.

[9] Hurwitz was the first to prove the four squares theorem this way: Hurwitz, A. *Vorlesungen über die Zahlentheorie der Quaternionen.* Julius Springer, Berlin, 1919. Actually Hurwitz goes further; he (re)derives Jacobi's formula for the number of ways of writing n as a sum of four squares.

(b) By Exercise 5.3, I is principal; let $\pi \in \mathbb{Z}_{\mathbb{H}}$ be a generator. Write $p = \pi\eta$, where $\eta \in \mathbb{Z}_{\mathbb{H}}$. By (a), π is not a unit. Show that η is also not a unit. Deduce that $N\pi = p$.

(c) Show that p is a sum of four integer squares. *Hint:* If the $1, i, j, k$-coefficients of π are rational integers, this is immediate. Otherwise, multiply π by a norm 1 element of the form $\frac{1}{2}(\pm 1 \pm i \pm j \pm k)$ chosen to make the product have rational integer coefficients.

(d) Parts (a)–(c) show that every prime is a sum of four squares. Complete the proof of Lagrange's theorem by exploiting the multiplicativity of the norm map.

13

Back to basics: Starting over with arbitrary number fields

> For last year's words belong to last year's language.
> And next year's words await another voice.
> – T. S. Eliot

Up to now, our efforts have focused almost exclusively on quadratic fields. It is time for a new beginning.

Norm and trace

In Chapter 3, we defined the norm and trace maps for *Galois* number fields. We now explain how to proceed in the general case.

Let K be an arbitrary number field of degree n. Recall from Chapter 2 that there are n distinct embeddings $\sigma : K \hookrightarrow \mathbb{C}$. For each $\alpha \in K$, we define the **field polynomial** $\phi_\alpha(x)$ by

$$\phi_\alpha(x) = \prod_{\sigma : K \hookrightarrow \mathbb{C}} (x - \sigma(\alpha)).$$

A priori, the coefficients of $\phi_\alpha(x)$ are complex numbers. It is natural to hope that these coefficients are in fact rational numbers, as was the case in Chapter 3. This is an immediate consequence of our next result.

Proposition 13.1. Suppose that $[\mathbb{Q}(\alpha) : \mathbb{Q}] = r$. (Thus, r is a divisor of n.) Then

$$\phi_\alpha(x) = \min_\alpha(x)^{n/r}.$$

For the proof, we need a simple field-theoretic lemma.

Lemma 13.2. Let K be a number field with $[K:\mathbb{Q}] = n$, and let F be a subfield of K with $[F:\mathbb{Q}] = r$. Each of the r embeddings $\tau: F \hookrightarrow \mathbb{C}$ extends in n/r ways to an embedding $\sigma: K \hookrightarrow \mathbb{C}$.

Proof. Using the primitive element theorem, write $K = F(\theta)$ for some $\theta \in K$. Let $m(x)$ denote the minimal polynomial of θ over F, so that

$$\deg m = [K:F] = n/r.$$

Let $\tau m(x)$ be the polynomial obtained by applying τ to each coefficient of $m(x)$. If σ is an embedding of K into $\mathbb{C}$ extending τ, then applying σ to both sides of the equation $m(\theta) = 0$ shows that $\sigma(\theta)$ is one of the roots of $\tau m(x)$. Thus, there are at most $\deg(\tau m) = n/r$ possibilities for $\sigma(\theta)$. Since σ is determined by where it sends θ, it follows that τ has *at most* n/r extensions. But there are n embeddings of K into $\mathbb{C}$ in total, each of which extends one of the r embeddings of F into $\mathbb{C}$. This is only possible if each $\tau: F \hookrightarrow \mathbb{C}$ has *exactly* n/r extensions $\sigma: K \hookrightarrow \mathbb{C}$. □

Proof of Proposition 13.1. Let $F = \mathbb{Q}(\alpha)$. Recall from the proof of Proposition 2.2 that

$$\min_\alpha(x) = \prod_\tau (x - \tau(\alpha)),$$

where τ runs over the embeddings of F into $\mathbb{C}$. Letting σ run over the embeddings of K into $\mathbb{C}$, Lemma 13.2 shows that

$$\begin{aligned}\phi_\alpha(x) &= \prod_\sigma (x - \sigma(\alpha)) \\ &= \left(\prod_\tau (x - \tau(\alpha))\right)^{n/r} = \min_\alpha(x)^{n/r}.\end{aligned}$$

□

The next result generalizes Proposition 3.4 to the not-necessarily-Galois situation.

Proposition 13.3. Let K be any number field. For each $\alpha \in K$,

$$\alpha \in \mathbb{Z}_K \iff \phi_\alpha(x) \in \mathbb{Z}[x].$$

Proof. Since $\phi_\alpha(x)$ is a monic polynomial that vanishes at α, the backward direction ($\Leftarrow$) is immediate. To prove the forward direction ($\Rightarrow$), recall that when $\alpha \in \mathbb{Z}_K$, its minimal polynomial $\min_\alpha(x) \in \mathbb{Z}[x]$ (Proposition 2.8). Now invoke Proposition 13.1. □

Suppose that the field polynomial of α takes the form

$$\phi_\alpha(x) = x^{n-1} + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0.$$

We define the **norm** and **trace** of α as the numbers $-a_{n-1}$ and $(-1)^n a_0$. Equivalently,

$$\mathrm{N}(\alpha) = \prod_{\sigma\colon K \hookrightarrow \mathbb{C}} \sigma(\alpha), \quad \mathrm{Tr}(\alpha) = \sum_{\sigma\colon K \hookrightarrow \mathbb{C}} \sigma(\alpha).$$

From Propositions 13.1 and 13.3,

$$\mathrm{N}(\alpha), \mathrm{Tr}(\alpha) \in \mathbb{Q} \quad \text{for all } \alpha \in K,$$

and

$$\mathrm{N}(\alpha), \mathrm{Tr}(\alpha) \in \mathbb{Z} \quad \text{for all } \alpha \in \mathbb{Z}_K.$$

As in Chapter 3, the norm is multiplicative in the sense that

$$\mathrm{N}(\alpha\beta) = \mathrm{N}\alpha \cdot \mathrm{N}\beta \quad \text{for all } \alpha, \beta \in K,$$

while the trace is $\mathbb{Q}$-linear, meaning that

$$\mathrm{Tr}(a\alpha + b\beta) = a\mathrm{Tr}(\alpha) + b\mathrm{Tr}(\beta) \quad \text{for } a, b \in \mathbb{Q},\ \alpha, \beta \in K.$$

Discriminants of n-tuples

We continue to assume that $[K : \mathbb{Q}] = n$. We let $\sigma_1, \ldots, \sigma_n$ be a list of the embeddings of K into $\mathbb{C}$ (ordered arbitrarily).

Definition 13.4. The **discriminant** $\Delta(\omega_1, \ldots, \omega_n)$ of an n-tuple of elements $\omega_1, \ldots, \omega_n \in K$ is defined as

$$\det(D_{\omega_1,\ldots,\omega_n})^2.$$

Here $D_{\omega_1,\ldots,\omega_n}$ is the $n \times n$ complex matrix with ith row, jth column entry $\sigma_i(\omega_j)$; i.e.,

$$D_{\omega_1,\ldots\omega_n} = \begin{bmatrix} \sigma_1(\omega_1) & \sigma_1(\omega_2) & \ldots & \sigma_1(\omega_n) \\ \sigma_2(\omega_1) & \ddots & \vdots & \vdots \\ \vdots & \vdots & \ddots & \vdots \\ \sigma_n(\omega_1) & \ldots & \ldots & \sigma_n(\omega_n) \end{bmatrix}.$$

(You have probably encountered the term "discriminant" in the context of polynomials; our discriminants are closely related, as we will see in the next chapter.)

The squaring in Definition 13.4 is crucial. If we reorder the σ_i or the ω_j, then we permute the rows or columns of $D_{\omega_1,\ldots,\omega_n}$; the squaring ensures that this has no effect on the final value of $\Delta(\omega_1,\ldots,\omega_n)$.

There is another way of viewing the discriminant that is often useful. For brevity, put $D = D_{\omega_1,\ldots,\omega_n}$. Then

$$\Delta(\omega_1,\ldots,\omega_n) = \det(D)^2 = \det(D^T D).$$

The ith row, jth column entry of $D^T D$ is

$$\sum_{k=1}^{n} \sigma_k(\omega_i)\sigma_k(\omega_j) = \sum_{k=1}^{n} \sigma_k(\omega_i\omega_j) = \mathrm{Tr}(\omega_i\omega_j),$$

and so

$$\Delta(\omega_1,\ldots,\omega_n) = \det(D^{\mathrm{Tr}}_{\omega_1,\ldots,\omega_n}), \tag{13.1}$$

where we let

$$D^{\mathrm{Tr}}_{\omega_1,\ldots,\omega_n} := \begin{bmatrix} \mathrm{Tr}(\omega_1\omega_1) & \mathrm{Tr}(\omega_1\omega_2) & \ldots & \mathrm{Tr}(\omega_1\omega_n) \\ \mathrm{Tr}(\omega_2\omega_1) & \ddots & \vdots & \vdots \\ \vdots & \vdots & \ddots & \vdots \\ \mathrm{Tr}(\omega_n\omega_1) & \ldots & \ldots & \mathrm{Tr}(\omega_n\omega_n) \end{bmatrix}.$$

This representation has the advantage of making it obvious that $\Delta(\omega_1,\ldots,\omega_n)$ always belongs to $\mathbb{Q}$, and that $\Delta(\omega_1,\ldots,\omega_n) \in \mathbb{Z}$ whenever the ω_i all belong to $\mathbb{Z}_K$.

We can now explain why the "discriminant" deserves its name; it tells apart (i.e., discriminates between) bases and nonbases of K.

Proposition 13.5. Let $\omega_1, \ldots, \omega_n$ be elements of K. Then

$$\Delta(\omega_1, \ldots, \omega_n) \neq 0 \iff \omega_1, \ldots, \omega_n \text{ is a } \mathbb{Q}\text{-basis for } K.$$

Proof. We prove the forward direction ($\Rightarrow$) by showing the contrapositive. If the ω_i are not a $\mathbb{Q}$-basis for K, then they are $\mathbb{Q}$-linearly dependent. Given any dependence relation, we can immediately read off a corresponding dependence relation among the columns of $D_{\omega_1,\ldots,\omega_n}$. Hence, $\det(D_{\omega_1,\ldots,\omega_n}) = 0$.

For the backward direction ($\Leftarrow$), we proceed by contradiction. Suppose that $\omega_1, \ldots, \omega_n$ form a basis but that $\Delta = 0$. The vanishing of Δ implies a linear dependence among the columns of $D^{\mathrm{Tr}}_{\omega_1,\ldots,\omega_n}$. Thus, there are $c_1, \ldots, c_n \in \mathbb{Q}$, not all zero, with

$$\sum_{j=1}^{n} c_j \mathrm{Tr}(\omega_i \omega_j) = 0 \quad \text{for all } i = 1, 2, \ldots, n. \tag{13.2}$$

Set

$$\beta = \sum_{j=1}^{n} c_j \omega_j.$$

Then $\beta \neq 0$, since the ω_j are a $\mathbb{Q}$-basis for K and the c_j do not all vanish. Taking advantage of the $\mathbb{Q}$-linearity of the trace, (13.2) can be put in the form

$$\mathrm{Tr}(\omega_i \beta) = 0 \quad \text{for all } i = 1, 2, \ldots, n.$$

But every $\alpha \in K$ is a $\mathbb{Q}$-linear combination of the ω_i. It follows that $\mathrm{Tr}(\alpha\beta) = 0$ for all $\alpha \in K$. But this is absurd: When $\alpha = 1/\beta$, we have $\mathrm{Tr}(\alpha\beta) = \mathrm{Tr}(1) = n \neq 0$. □

Integral bases

With the proof of the next result, we discharge a debt that has been hanging over our heads since Chapter 3.

Theorem 13.6 (Existence of integral bases)**.** Let K be a number field of degree n. Then $\mathbb{Z}_K$ is a free $\mathbb{Z}$-module of rank n.

We call a $\mathbb{Z}$-basis for $\mathbb{Z}_K$ an **integral basis for** K.

We preface the proof of Theorem 13.6 with a simple but important observation. Suppose that $\omega_1, \ldots, \omega_n$ and $\theta_1, \ldots, \theta_n$ are n-tuples of elements of K related by an equation of the form

$$[\omega_1, \ldots, \omega_n] = [\theta_1, \ldots, \theta_n]M,$$

where M is an $n \times n$ matrix with rational entries. Then

$$D_{\omega_1,\ldots,\omega_n} = D_{\theta_1,\ldots,\theta_n} \cdot M,$$

so that taking determinants and squaring,

$$\Delta(\omega_1, \ldots, \omega_n) = \Delta(\theta_1, \ldots, \theta_n) \cdot \det(M)^2.$$

Proof of Theorem 13.6. It is certainly possible to find an n-tuple ω_1, $\omega_2, \ldots, \omega_n \in \mathbb{Z}_K$ with

$$\Delta(\omega_1, \ldots, \omega_n) \neq 0. \tag{13.3}$$

For example, one can start with any $\mathbb{Q}$-basis for K and then scale the basis elements by suitable positive integers so that they land in $\mathbb{Z}_K$ (cf. Proposition 2.9).

Now look among all tuples $\omega_1, \ldots, \omega_n \in \mathbb{Z}_K$ satisfying (13.3). For each of these, $\Delta(\omega_1, \ldots, \omega_n)$ is a nonzero *integer*. Hence, the quantity $|\Delta(\omega_1, \ldots, \omega_n)|$ achieves a minimum value. Let $\omega_1, \ldots, \omega_n$ be a minimizing tuple; we shall prove that the ω_i form a $\mathbb{Z}$-basis for $\mathbb{Z}_K$.

Since $\Delta(\omega_1, \ldots, \omega_n) \neq 0$, the ω_i are a $\mathbb{Q}$-basis for K (by Proposition 13.5). So the only way they can fail to be a $\mathbb{Z}$-basis for $\mathbb{Z}_K$ is if there is an $\alpha \in \mathbb{Z}_K$ not in their $\mathbb{Z}$-span. Given such an α, write

$$\alpha = c_1\omega_1 + \cdots + c_n\omega_n$$

for some rational numbers c_i. By assumption, some $c_i \notin \mathbb{Z}$, and (reordering the ω_i if necessary) there is no loss of generality in assuming that $c_1 \notin \mathbb{Z}$. Set

$$\begin{aligned}\beta &:= \alpha - \sum_{i=1}^{n} \lfloor c_i \rfloor \omega_i \\ &= \{c_1\}\omega_1 + \{c_2\}\omega_2 + \cdots + \{c_n\}\omega_n.\end{aligned}$$

Since α and the ω_i belong to $\mathbb{Z}_K$, so does β. Moreover,

$$[\beta, \omega_2, \ldots, \omega_n] = [\omega_1, \ldots, \omega_n]M,$$

where

$$M = \begin{bmatrix} \{c_1\} & 0 & 0 & \dots & 0 \\ \{c_2\} & 1 & 0 & \dots & 0 \\ \{c_3\} & 0 & 1 & \dots & 0 \\ \vdots & 0 & 0 & \ddots & 0 \\ \{c_n\} & 0 & 0 & \dots & 1 \end{bmatrix}.$$

Thus,

$$\begin{aligned} \Delta(\beta, \omega_2, \dots, \omega_n) &= \Delta(\omega_1, \dots, \omega_n) \cdot \det(M)^2 \\ &= \Delta(\omega_1, \dots, \omega_n) \cdot \{c_1\}^2. \end{aligned}$$

Since $0 < \{c_1\} < 1$,

$$0 < |\Delta(\beta, \omega_2, \dots, \omega_n)| < |\Delta(\omega_1, \dots, \omega_n)|.$$

This contradicts the choice of the ω_i. □

The field discriminant

Suppose that $\omega_1, \dots, \omega_n$ and $\theta_1, \dots, \theta_n$ are both integral bases of K. Then the ω_i can be expressed as $\mathbb{Z}$-linear combinations of the θ_j and vice versa; in this way, we obtain $n \times n$ integer matrices M and N with

$$[\omega_1, \dots, \omega_n] = [\theta_1, \dots, \theta_n]M$$

and

$$[\theta_1, \dots, \theta_n] = [\omega_1, \dots, \omega_n]N.$$

Substituting the second equation back into the first shows that

$$[\omega_1, \dots, \omega_n] = [\omega_1, \dots, \omega_n]NM.$$

Since the ω_i are a $\mathbb{Z}$-basis for $\mathbb{Z}_K$, this forces NM to be the $n \times n$ identity matrix. So $\det(N) = \det(M) = \pm 1$. Now comparing discriminants,

$$\begin{aligned} \Delta(\omega_1, \dots, \omega_n) &= \Delta(\theta_1, \dots, \theta_n) \cdot \det(M)^2 \\ &= \Delta(\theta_1, \dots, \theta_n). \end{aligned}$$

Thus, Δ assumes the same value at every integral basis of K. This common integer is called the **discriminant of** $\mathbb{Z}_K$ (or of K), and is denoted Δ_K.

Example 13.7 (Discriminant of a quadratic field)**.** Let $K = \mathbb{Q}(\sqrt{d})$ with d squarefree, $d \neq 1$. Then $1, \tau$ is a $\mathbb{Z}$-basis for $\mathbb{Z}_K$, where $\tau = \sqrt{d}$ if $d \equiv 2, 3 \pmod 4$ and $\tau = \frac{1}{2}(1 + \sqrt{d})$ if $d \equiv 1 \pmod 4$. Using a tilde for the nontrivial element of $\mathrm{Gal}(K/\mathbb{Q})$, we have that $\Delta_K = \det \left[\begin{smallmatrix} 1 & \tau \\ 1 & \tilde{\tau} \end{smallmatrix}\right]^2$, from which we obtain

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

Here are two reasons to care about the discriminant. First, there is a result of Hermite (proved in Chapter 21) that there are only finitely many number fields K with $|\Delta_K|$ lying below any given bound. Thus, the discriminant provides a sensible way of ordering number fields. Second, the discriminant encodes useful arithmetic information. An important manifestation of this phenomenon is the theorem of Dedekind (proved in Chapter 22) that a rational prime ramifies in $\mathbb{Z}_K$ precisely when it divides Δ_K.[1] (The reader should check that in the quadratic case, this theorem agrees with the criterion for ramification proved in Chapter 7.)

Ideal norms

As in Chapter 6, the **norm** of a nonzero ideal I of $\mathbb{Z}_K$ is defined by

$$\mathrm{N}(I) = \#\mathbb{Z}_K/I.$$

In the quadratic case, the standard basis representation of an ideal gave us enough leverage that we were able to quickly prove the important properties of the ideal norm "with our bare hands". In the general case, we will have to tease out these properties more gradually.

Naturally, our first goal is to show that $\mathrm{N}(I)$ is finite for all nonzero ideals I.

Lemma 13.8. For each nonzero $\alpha \in \mathbb{Z}_K$,

$$\alpha \mid \mathrm{N}\alpha \qquad \text{(in the ring } \mathbb{Z}_K\text{)}.$$

[1] In general, we say that a rational prime p **ramifies in** $\mathbb{Z}_K$ when there is a prime ideal appearing to an exponent larger than 1 in the factorization of $\langle p \rangle$.

Proof. This might appear obvious, since $\mathrm{N}\alpha = \alpha \cdot \beta$, where

$$\beta := \prod_{\substack{\sigma : K \hookrightarrow \mathbb{C} \\ \sigma \neq \mathrm{id}.}} \sigma(\alpha).$$

And indeed, it *is* obvious, once we know that $\beta \in \mathbb{Z}_K$. (There is something to show here, since there is no reason for the individual terms $\sigma(\alpha)$ to even lie in K.) To prove this containment, we make two observations. First, $\beta \in \bar{\mathbb{Z}}$, since each $\sigma(\alpha) \in \bar{\mathbb{Z}}$, being a root of the monic polynomial $\min_\alpha(x) \in \mathbb{Z}[x]$. Second, $\beta \in K$, since $\beta = \frac{\mathrm{N}(\alpha)}{\alpha}$. Thus, $\beta \in K \cap \bar{\mathbb{Z}} = \mathbb{Z}_K$, as desired. □

Proposition 13.9. Let I be a nonzero ideal of $\mathbb{Z}_K$. Then

$$\#\mathbb{Z}_K/I < \infty.$$

Proof. Let α be a nonzero element of I, and let $m = \mathrm{N}\alpha$. Then m is a nonzero integer. By Lemma 13.8, $\alpha \mid m$, and so $I \supseteq \langle m \rangle$. Thus, we obtain a well-defined surjection from $\mathbb{Z}_K/\langle m \rangle$ onto $\mathbb{Z}_K/I$ via the map $\theta \bmod m \mapsto \theta \bmod I$. So it is sufficient to prove that $\mathbb{Z}_K/\langle m \rangle$ is finite. But the finiteness of $\mathbb{Z}_K/\langle m \rangle$ is clear from the existence of integral bases. Indeed, as abelian groups, $\mathbb{Z}_K \cong \mathbb{Z}^n$ (with $n = [K : \mathbb{Q}]$), and so

$$\mathbb{Z}_K/\langle m \rangle \cong \mathbb{Z}^n/m\mathbb{Z}^n \cong (\mathbb{Z}/m\mathbb{Z})^n.$$ □

Next, we show that the ideal norm and elementwise norm agree in the sense of Corollary 6.10. This requires two preliminary results. The first is a theorem usually encountered in courses on module theory. For the convenience of the reader, a self-contained proof is given in the appendix to this chapter.

Theorem 13.10 (Index=determinant)**.** Let M be a free $\mathbb{Z}$-module of rank n, and let H be a $\mathbb{Z}$-submodule of M that is also free of rank n. Let $\omega_1, \ldots, \omega_n$ be a $\mathbb{Z}$-basis for M, and let $\theta_1, \ldots, \theta_n$ be a $\mathbb{Z}$-basis for H. Let A be the $n \times n$ integer matrix with

$$[\theta_1, \ldots, \theta_n] = [\omega_1, \ldots, \omega_n]A. \tag{13.4}$$

Then

$$\#M/H = |\det(A)|.$$

The second result we need reinterprets Theorem 13.10 in terms of discriminants, in the case when $M = \mathbb{Z}_K$.

Corollary 13.11. Let K be a degree n number field. Let H be a $\mathbb{Z}$-submodule of $\mathbb{Z}_K$ that is free of rank n. If $\theta_1, \ldots, \theta_n$ is a $\mathbb{Z}$-basis for H, then

$$(\#\mathbb{Z}_K/H)^2 = \Delta(\theta_1, \ldots, \theta_n)/\Delta_K.$$

Proof. Let $\omega_1, \ldots, \omega_n$ be a $\mathbb{Z}$-basis for $\mathbb{Z}_K$. Write

$$[\theta_1, \ldots, \theta_n] = [\omega_1, \ldots, \omega_n]A,$$

where A is an $n \times n$ integer matrix. Then

$$\begin{aligned}\Delta(\theta_1, \ldots, \theta_n) &= \Delta(\omega_1, \ldots, \omega_n) \cdot \det(A)^2 \\ &= \Delta_K \cdot (\#\mathbb{Z}_K/H)^2.\end{aligned}$$

Rearranging yields the corollary. □

Proposition 13.12 (generalizing Corollary 6.10)**.** If α is a nonzero element of $\mathbb{Z}_K$, then

$$\mathrm{N}(\langle\alpha\rangle) = |\mathrm{N}\alpha|.$$

Proof. Let $\omega_1, \ldots, \omega_n$ be an integral basis for K. Then $\langle\alpha\rangle$ is a free $\mathbb{Z}$-submodule of $\mathbb{Z}_K$ with $\mathbb{Z}$-basis $\alpha\omega_1, \ldots, \alpha\omega_n$. By Corollary 13.11,

$$\mathrm{N}(\langle\alpha\rangle)^2 = \#(\mathbb{Z}_K/\langle\alpha\rangle)^2 = \Delta(\alpha\omega_1, \ldots, \alpha\omega_n)/\Delta_K.$$

The rows of the matrix $D_{\alpha\omega_1,\ldots,\alpha\omega_n}$ differ from the corresponding rows of $D_{\omega_1,\ldots,\omega_n}$ by factors of $\sigma_1(\alpha), \ldots, \sigma_n(\alpha)$. Hence,

$$\begin{aligned}\Delta(\alpha\omega_1, \ldots, \alpha\omega_n) &= \left(\prod_{i=1}^{n} \sigma_i(\alpha)\right)^2 \Delta(\omega_1, \ldots, \omega_n) \\ &= \mathrm{N}(\alpha)^2 \cdot \Delta_K.\end{aligned}$$

Plugging this into the previous display shows that $\mathrm{N}(\langle\alpha\rangle)^2 = \mathrm{N}(\alpha)^2$. Now take square roots, keeping in mind that $\mathrm{N}(\langle\alpha\rangle) > 0$. □

We will see later that the ideal norm is multiplicative (in analogy with Corollary 6.9) and that $N(I)$ can be interpreted as the product of the conjugate ideals of I (in analogy with Theorem 6.7). Both of these results will be easier to prove once the fundamental theorem of ideal theory is in place.[2]

[2] In fact, the multiplicativity of the ideal norm is in some sense equivalent to the fundamental theorem. See: Butts, H.S.; Wade, L.I. *Two criteria for Dedekind domains.* Amer. Math. Monthly **73** (1966), 14–21.

Appendix: a point-counting proof that index=determinant

We now show how to deduce Theorem 13.10 from the following slight extension of the fundamental point counting principle (Theorem 12.2).

Proposition 13.13. Let $\mathcal{R}$ be a bounded region in $\mathbb{R}^n$ possessing a Jordan volume. Let $\Lambda \subseteq \mathbb{R}^n$ be a full rank lattice. As $t \to \infty$,

$$\frac{1}{t^n} \sum_{\mathbf{v} \in \Lambda} 1_{t\mathcal{R}}(\mathbf{v}) \to \frac{\mathrm{vol}(\mathcal{R})}{\mathrm{covol}(\Lambda)}.$$

Proposition 13.13 can be deduced from Theorem 12.2 in the same way that the general form of Minkowski's theorem (Theorem 12.5) was deduced from the version for the standard lattice (Theorem 12.3).

Proof of Theorem 13.10. It is sufficient to prove the result when $M = \mathbb{Z}^n$ and $\omega_1, \ldots, \omega_n$ are the standard basis vectors for $\mathbb{R}^n$. In this case, (13.4) tells us that $\theta_1, \ldots, \theta_n$ are the column vectors of A; we will denote these by the more suggestive symbols $\mathbf{v}_1, \ldots, \mathbf{v}_n$. By assumption, the $\mathbf{v}_i$ are linearly independent over $\mathbb{Z}$, and so also over $\mathbb{Q}$. So linear algebra over $\mathbb{Q}$ guarantees that $\det(A) \neq 0$. Now thinking of A as a matrix over $\mathbb{R}$, we deduce from the nonvanishing of $\det(A)$ that the $\mathbf{v}_i$ are $\mathbb{R}$-linearly independent. So H is in fact a full rank lattice in $\mathbb{R}^n$. The statement of Theorem 13.10 is precisely the assertion that

$$\#\mathbb{Z}^n/H = \mathrm{covol}(H). \tag{13.5}$$

Let $\mathcal{B}(r)$ denote the open ball of radius r in $\mathbb{R}^n$, centered at the origin. Let $N(r)$ denote the number of standard lattice points contained in $\mathcal{B}(r)$. We will prove (13.5) by estimating $N(r)$ in two different ways, as $r \to \infty$.

Let $\mathcal{B}$ be the open unit ball centered at the origin. (Thus, $\mathcal{B}(r) = r\mathcal{B}$.) A direct application of the fundamental point counting principle shows that

$$\frac{1}{r^n} N(r) \to \mathrm{vol}(\mathcal{B}), \quad \text{as } r \to \infty.$$

Alternatively, we may proceed as follows. Fix a complete set of representatives $\mathcal{R}$ for $\mathbb{Z}^n/H$. For each $\mathbf{w} \in \mathcal{R}$, let

$$N(r; \mathbf{w} \bmod H) = \sum_{\substack{\mathbf{v} \in \mathcal{B}(r) \cap \mathbb{Z}^n \\ \mathbf{v} \equiv \mathbf{w} \pmod{H}}} 1.$$

Then

$$N(r) = \sum_{\mathbf{w} \in \mathcal{R}} N(r; \mathbf{w} \bmod H). \tag{13.6}$$

We now fix an element $\mathbf{w} \in \mathcal{R}$ and study the corresponding summand in (13.6). We can interpret $N(r; \mathbf{w} \bmod H)$ as the count of points of H lying in the translated ball $\mathcal{B}(r) - \mathbf{w}$. We would like to apply Proposition 13.13 to estimate this count, but some care is needed since $\mathcal{B}(r) - \mathbf{w}$ is not the dilate of a fixed region. To work around this, notice that for all large enough values of r,

$$\mathcal{B}(r - \sqrt{r}) \subseteq \mathcal{B}(r) - \mathbf{w} \subseteq \mathcal{B}(r + \sqrt{r}),$$

so that

$$\sum_{\mathbf{v} \in \mathcal{B}(r-\sqrt{r}) \cap H} 1 \leq N(r; \mathbf{w} \bmod H) \leq \sum_{\mathbf{v} \in \mathcal{B}(r+\sqrt{r}) \cap H} 1.$$

If we divide the leftmost term by r^n and let $r \to \infty$, we obtain a limit of $\operatorname{vol}(\mathcal{B})/\operatorname{covol}(H)$, by Proposition 13.13. (We use here that the ratio between $r - \sqrt{r}$ and r tends to 1, as $r \to \infty$.) The same holds if we divide the rightmost term by r^n and let $r \to \infty$. So by the squeeze theorem,

$$\frac{1}{r^n} N(r; \mathbf{w} \bmod H) \to \frac{\operatorname{vol}(\mathcal{B})}{\operatorname{covol}(H)}.$$

We are ready to finish up. Dividing (13.6) through by r^n shows that

$$\frac{1}{r^n} N(r) = \sum_{\mathbf{w} \in \mathcal{R}} \frac{N(r; \mathbf{w} \bmod H)}{r^n}.$$

We send $r \to \infty$ and compare limits. As noted already, the left-hand side tends to $\operatorname{vol}(\mathcal{B})$. On the other hand, the right-hand summands are nonnegative, and each fixed summand tends to $\operatorname{vol}(\mathcal{B})/\operatorname{covol}(H)$. Since the limit of the sum has to come out to $\operatorname{vol}(\mathcal{B})$, we must have $\#\mathcal{R} = \operatorname{covol}(H)$. But $\#\mathcal{R} = \#\mathbb{Z}_K/H$, and so the theorem is proved. □

Exercises

(1) (Stickelberger[3]) Show that $\Delta_K \equiv 0$ or $1 \pmod 4$ for every number field K. *Hint:* (following Schur[4]) Write $\det(D_{\omega_1,\ldots,\omega_n}) = P - N$, where

$$P = \sum_{\substack{\pi \in S_n \\ \pi \text{ even}}} \prod_{i=1}^{n} \sigma_i(\omega_{\pi(i)}), \quad N = \sum_{\substack{\pi \in S_n \\ \pi \text{ odd}}} \prod_{i=1}^{n} \sigma_i(\omega_{\pi(i)}).$$

Then P and N are algebraic integers (why?). Show that $P+N$ and PN are fixed by every element of $\mathrm{Gal}(L/\mathbb{Q})$, where L denotes the Galois closure of $K/\mathbb{Q}$. Deduce that $P+N, PN$ are rational integers. Conclude using that $\Delta_K = (P-N)^2 = (P+N)^2 - 4PN$.

(2) (Brill[5]) Let K be a number field. Show that the sign of Δ_K is given by $(-1)^{r_2}$, where r_2 is the number of pairs of nonreal complex embeddings of K. *Hint:* By performing a sequence of elementary row operations on the matrix $D_{\omega_1,\ldots,\omega_n}$, replace each pair of rows $\left[\begin{smallmatrix} \sigma(\omega_1) & \ldots & \sigma(\omega_n) \\ \overline{\sigma}(\omega_1) & \ldots & \overline{\sigma}(\omega_n) \end{smallmatrix}\right]$ with $\left[\begin{smallmatrix} \Re\sigma(\omega_1) & \ldots & \Re\sigma(\omega_n) \\ \Im\sigma(\omega_1) & \ldots & \Im\sigma(\omega_n) \end{smallmatrix}\right]$. How does this affect the squared determinant?

(3) Let L/K be an extension of number fields. For $\alpha \in L$, define the **relative field polynomial** $\phi_{L/K,\alpha}(x)$ by

$$\phi_{L/K,\alpha}(x) = \prod_{\sigma} (x - \sigma(\alpha)),$$

where σ runs over the embeddings of L into $\mathbb{C}$ that fix K. Show that $\phi_{L/K,\alpha}(x) \in K[x]$ for all $\alpha \in L$, and that $\phi_{L/K,\alpha}(x) \in \mathbb{Z}_K[x]$ if and only if $\alpha \in \mathbb{Z}_L$.

(4) (Norm expression for the polynomial discriminant) Let $f(x)$ be a monic, degree n polynomial with rational coefficients, irreducible over $\mathbb{Q}$. Write

$$f(x) = (x - \theta_1) \cdots (x - \theta_n),$$

---

[3]Stickelberger, L. *Über eine neue Eigenschaft der Diskriminanten algebraischer Zahlkörper.* Proceedings of the First International Congress of Mathematicians, Zürich (1897), 182–193.

[4]Schur, I. *Elementarer Beweis eines Satzes von L. Stickelberger.* Math. Z. **29** (1929), 464–465.

[5]Brill, A. *Ueber die Discriminante.* Math. Ann. **12** (1877), 87–89.

where the $\theta_i \in \bar{\mathbb{Q}}$. Show that $f'(\theta_i) = \prod_{j \neq i}(\theta_j - \theta_i)$ for each $i = 1, 2, \ldots, n$. Use this to prove that[6]

$$\Delta(f(x)) = (-1)^{\binom{n}{2}} \cdot \mathrm{N} f'(\theta_1),$$

where $\Delta(f(x))$ is the discriminant of $f(x)$, and the norm is taken with respect to $\mathbb{Q}(\theta_1)$.

(5) Suppose that a and b are rational numbers for which $x^n + ax + b$ is irreducible over $\mathbb{Q}$. Using the result of the last exercise, show that

$$\begin{aligned}\Delta(x^n + ax + b) \\ = (-1)^{\binom{n}{2}}((1-n)^{n-1}a^n + n^n b^{n-1}).\end{aligned}$$

(6) Suppose that $\xi_1, \ldots, \xi_n$ are complex roots of unity whose average is an algebraic integer. Show that either $\xi_1 + \cdots + \xi_n = 0$ or $\xi_1 = \xi_2 = \cdots = \xi_n$. *Hint:* Let μ denote the average and let $K = \mathbb{Q}(\mu)$. Argue that $|\sigma(\mu)| \leq 1$ for all embeddings $\sigma : K \hookrightarrow \mathbb{C}$. What can you conclude knowing that $\mathrm{N}\mu \in \mathbb{Z}$?

[6] Here is a reminder of the definition of the **polynomial discriminant**. Let $f(x)$ be a nonconstant polynomial over a field F. Write $f(x) = a_n(x - \theta_1) \cdots (x - \theta_n)$, where $a_n \in F$ and the θ_i live in some extension of F (we are assuming here that $\deg f = n$). Then $\Delta(f(x))$ is defined as $a_n^{2n-2} \prod_{i<j}(\theta_j - \theta_i)^2$. It can be shown that this quantity belongs to F and depends only on $f(x)$ and not on the choice of extension field. See §14.6 of: Dummit, D. S.; Foote, R. M. *Abstract algebra.* Third edition. John Wiley & Sons, Inc., Hoboken, NJ, 2004.

14

Integral bases: From theory to practice, and back

According to Theorem 13.6, integral bases always exist. OK, how do we get our hands on one?

Depending on how one interprets this question, there are at least two possible responses. The first — and maybe most to the point — would be to describe a fast, general purpose algorithm for the problem, of the kind deserving to be implemented in a computer algebra system. The second response would be to explain how to navigate existing software that has such an algorithm already built in.

Hopefully the reader will not be too disappointed to find that neither answer appears in this chapter.[1]

What *do* we do? In the first half of the chapter, we describe in detail a naive algorithm for producing an integral basis. This suits our present goal very well, which is to show that in many natural examples (involving number fields defined by low degree polynomials with small coefficients), computing an integral basis is not a fearsome task; all it takes is some elbow grease and a computer (but no cleverness or specialized software!).

In the second half of the chapter, we discuss an idea involving Eisenstein polynomials that can sometimes be used to circumvent the

[1]For the first style of answer, see: Cohen, H. *A course in computational algebraic number theory*. Graduate Texts in Mathematics **138**. Springer-Verlag, Berlin, 1993.

For the second, see the free online textbook of William Stein: `http://wstein.org/books/ant/`

need for detailed computation. We also advertise (without proofs) known results for pure cubic and biquadratic fields.

Integral bases by successive approximation

Let K be a number field for which we wish to determine an integral basis. We suppose we are given as a "seed" a tuple $\theta_1, \ldots, \theta_n$ of elements of $\mathbb{Z}_K$ forming a $\mathbb{Q}$-basis for K. Such a tuple is usually easy to come by. For instance, if K is a degree n number field given to us in the form $K = \mathbb{Q}(\alpha)$, where $\alpha \in \bar{\mathbb{Z}}$, then the θ_i can be taken as

$$1, \quad \alpha, \quad \alpha^2, \quad \ldots, \quad \alpha^{n-1}.$$

Our algorithm will either prove $\theta_1, \ldots, \theta_n$ is already an integral basis or will gradually transform $\theta_1, \ldots, \theta_n$ into such a basis.

To get started, let H be the $\mathbb{Z}$-submodule of $\mathbb{Z}_K$ generated by the θ_i. That is,

$$H = \bigoplus_{i=1}^{n} \mathbb{Z}\theta_i.$$

(The sum is direct since the θ_i are a $\mathbb{Q}$-basis for K.) By Corollary 13.11,

$$\Delta(\theta_1, \ldots, \theta_n) = \Delta_K \cdot [\mathbb{Z}_K : H]^2. \tag{14.1}$$

We know $\theta_1, \ldots, \theta_n$ and so we can compute $\Delta(\theta_1, \ldots, \theta_n)$. But we cannot assume that we know the value of Δ_K. (We are trying to find an integral basis, and the simplest way to get one's hands on Δ_K is to already have an integral basis!) Nevertheless, we may deduce that

$$[\mathbb{Z}_K : H] \mid I, \tag{14.2}$$

where I is the largest positive integer for which

$$I^2 \mid \Delta(\theta_1, \ldots, \theta_n),$$

i.e.,[2]

$$I = \prod_{p^e \| \Delta(\theta_1, \ldots, \theta_n)} p^{\lfloor e/2 \rfloor}.$$

If $I = 1$, there is no need to continue; $H = \mathbb{Z}_K$, and so the θ_i are already an integral basis. We record this observation formally.

[2]The notation $p^e \| m$ means that p^e divides m but that $p^{e+1} \nmid m$.

Proposition 14.1. Let $\theta_1, \ldots, \theta_n \in \mathbb{Z}_K$. If $\Delta(\theta_1, \ldots, \theta_n)$ is squarefree, then $\theta_1, \ldots, \theta_n$ is an integral basis.[3]

Here is a summary of the algorithm to be used when $I > 1$. The following two preconditions are assumed.

- $\theta_1, \ldots, \theta_n \in \mathbb{Z}_K$ form a $\mathbb{Q}$-basis for K.
- With $H := \bigoplus_{i=1}^n \mathbb{Z}\theta_i$, the divisibility relation (14.2) holds, where $I \in \mathbb{Z}^+$ is larger than 1.

The algorithm proceeds by letting p be any prime divisor of I. It is then shown that (14.2) can be improved upon in one of two ways. Either:

(a) The algorithm finds an order p element of $\mathbb{Z}_K/H$. Out of this, it constructs a new candidate for an integral basis, say $\theta'_1, \ldots, \theta'_n \in \mathbb{Z}_K$. These elements form a $\mathbb{Q}$-basis for K and, if we let $H' := \bigoplus_{j=1}^n \mathbb{Z}\theta'_j$, then $[\mathbb{Z}_K : H'] \mid I'$, where $I' = I/p$. *Or*:

(b) The algorithm proves that $p \nmid [\mathbb{Z}_K : H]$. Hence, $[\mathbb{Z}_K : H] \mid I'$, where I' is the largest divisor of I coprime to p. In this case, we set $\theta'_j = \theta_j$ for each $j = 1, 2, \ldots, n$.

In either case, $I' \leq I/p < I$. If $I' = 1$, then $\theta'_1, \ldots, \theta'_n$ is our desired integral basis. Otherwise, we can start the algorithm over, with the θ_j replaced by the θ'_j and I replaced by I'. Since I decreases at each pass, the algorithm is guaranteed to terminate in finitely many steps.

It remains to describe how to obtain either (a) or (b).

If p divides $[\mathbb{Z}_K : H]$, then the quotient $\mathbb{Z}_K/H$ has an element of order p. Concretely, this means that there are integers $c_1, \ldots, c_n$, not all divisible by p, with

$$\theta := \frac{c_1\theta_1 + \cdots + c_n\theta_n}{p} \in \mathbb{Z}_K. \tag{14.3}$$

In fact, it is possible to arrange (Exercise 1) that

$$c_i = 1 \quad \text{for some } i.$$

[3]Warning: The condition of Proposition 14.1 is sufficient for the θ_i to form an integral basis but not necessary! Indeed, we have already seen that when $K = \mathbb{Q}(\sqrt{d})$, the integral bases have discriminant $2^2 \cdot d$ when $d \equiv 2, 3 \pmod 4$.

Adjusting θ by a suitable element of H, we can also assume that

$$0 \le c_1, \dots, c_n < p.$$

There are only finitely many θ of the form (14.3) satisfying these constraints. For each of these, we compute the field polynomial $\phi_\theta(x)$ and check whether it belongs to $\mathbb{Z}[x]$. If no $\phi_\theta(x)$ belong to $\mathbb{Z}[x]$, we have ruled out elements of order p in $\mathbb{Z}_K/H$, and we are in case (b).

If our search turns up a θ with $\phi_\theta(x) \in \mathbb{Z}[x]$, then we are in case (a). We choose an index i with $c_i = 1$. We set $\theta'_j = \theta_j$ for all indices $j \in \{1, 2, \dots, n\}$ except for $j = i$, and we set $\theta'_i = \theta$.

Observe that since $c_i = 1$,

$$\begin{aligned} \theta_i &= p\theta - \sum_{\substack{1 \le j \le n \\ j \ne i}} c_j \theta_j \\ &= p\theta'_i - \sum_{\substack{1 \le j \le n \\ j \ne i}} c_j \theta'_j. \end{aligned}$$

Remembering that $\theta_j = \theta'_j$ when $j \ne i$, we see from this last display that the $\mathbb{Z}$-span H of $\theta_1, \dots, \theta_n$ is contained in the $\mathbb{Z}$-span H' (say) of $\theta'_1, \dots, \theta'_n$. The same argument shows that the $\mathbb{Q}$-span of $\theta_1, \dots, \theta_n$ is contained in the $\mathbb{Q}$-span of $\theta'_1, \dots, \theta'_n$. Since $\theta_1, \dots, \theta_n$ form a $\mathbb{Q}$-basis for K, so do $\theta'_1, \dots, \theta'_n$.

The quotient group H'/H has an element of order p, namely $\theta'_i \bmod H$. Thus, $p \mid [H' : H]$ and

$$[\mathbb{Z}_K : H'] = \frac{[\mathbb{Z}_K : H]}{[H' : H]} \mid \frac{[\mathbb{Z}_K : H]}{p} \mid \frac{I}{p},$$

as desired for case (a).

Example 14.2. Let $K = \mathbb{Q}(\alpha)$, where α is a root of the irreducible quintic $f(x) = x^5 - 3x^2 + 1$. (We leave to the reader the task of checking that this is indeed irreducible.) We will show that $\mathbb{Z}_K = \mathbb{Z}[\alpha]$.

We apply our method with the seed tuple taken as 1, α, α^2, α^3, α^4. Let $\sigma_1, \ldots, \sigma_5$ denote the five embeddings of K into $\mathbb{C}$. Then

$$\Delta(1, \alpha, \alpha^2, \alpha^3, \alpha^4) = \det \begin{bmatrix} 1 & \sigma_1(\alpha) & \sigma_1(\alpha)^2 & \sigma_1(\alpha)^3 & \sigma_1(\alpha)^4 \\ 1 & \sigma_2(\alpha) & \sigma_2(\alpha)^2 & \sigma_2(\alpha)^3 & \sigma_2(\alpha)^4 \\ 1 & \sigma_3(\alpha) & \sigma_3(\alpha)^2 & \sigma_3(\alpha)^3 & \sigma_3(\alpha)^4 \\ 1 & \sigma_4(\alpha) & \sigma_4(\alpha)^2 & \sigma_4(\alpha)^3 & \sigma_4(\alpha)^4 \\ 1 & \sigma_5(\alpha) & \sigma_5(\alpha)^2 & \sigma_5(\alpha)^3 & \sigma_5(\alpha)^4 \end{bmatrix}^2.$$

Using the well-known formula for the determinant of a Vandermonde matrix,[4] we find that

$$\begin{aligned} \Delta(1, \alpha, \alpha^2, \alpha^3, \alpha^4) &= \prod_{1 \le i < j \le 5} (\sigma_j(\alpha) - \sigma_i(\alpha))^2 \\ &= \Delta(x^5 - 3x^2 + 1), \end{aligned}$$

where the final appearance of Δ is the polynomial discriminant (*not* the tuple discriminant).

We now pause to recall some 19th century algebra that deserves to be more widely known. Suppose we are given a degree n polynomial

$$g(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0$$

(over an arbitrary ground field). Write

$$g'(x) = b_{n-1} x^{n-1} + \cdots + b_0.$$

(Of course, b_i is simply $(i+1)a_{i+1}$, but we prefer the abbreviated notation for typographical reasons.) We associate to g the following $(2n-1) \times (2n-1)$ **Sylvester matrix**, denoted $\mathrm{Syl}_{g(x)}$:

$$\begin{bmatrix} a_n & a_{n-1} & \ldots & a_0 & & & & \\ & a_n & a_{n-1} & \ldots & a_0 & & & \\ & & a_n & a_{n-1} & \ldots & a_0 & & \\ & & & \ddots & & & & \\ & & & & a_n & a_{n-1} & \ldots & a_0 \\ b_{n-1} & b_{n-2} & \ldots & b_0 & & & & \\ & b_{n-1} & b_{n-2} & \ldots & b_0 & & & \\ & & b_{n-1} & b_{n-2} & \ldots & b_0 & & \\ & & & \ddots & & & & \\ & & & & b_{n-1} & b_{n-2} & \ldots & b_0 \end{bmatrix}.$$

[4] namely, $\det([x_i^{j-1}]_{1 \le i,j \le n}) = \prod_{1 \le i < j \le n} (x_j - x_i)$

(Here the first $n-1$ rows are formed from the coefficients of g, while the last n rows are formed from the coefficients of g'. The blank entries in the matrix are to be filled in with zeroes.) Then[5]

$$\Delta(g(x)) = \frac{(-1)^{\binom{n}{2}}}{a_n} \det(\mathrm{Syl}_{g(x)}).$$

Returning to our example, it is now routine to compute (or to ask a machine to compute) that

$$\Delta(x^5 - 3x^2 + 1) = -23119, \quad \text{which factors as} \quad -1 \cdot 61 \cdot 379.$$

Since $\Delta(1, \alpha, \alpha^2, \alpha^3, \alpha^4)$ is squarefree, Proposition 14.1 tells us that $1, \alpha, \alpha^2, \alpha^3, \alpha^4$ is a $\mathbb{Z}$-basis for $\mathbb{Z}_K$.

Example 14.3. Let $K = \mathbb{Q}(\alpha)$, where α is a root of the irreducible cubic $f(x) = x^3 + x^2 - 2x + 8$. We apply our successive approximation method with our seed tuple taken as $1, \alpha, \alpha^2$. Proceeding as in the last example, we eventually find that

$$\Delta(1, \alpha, \alpha^2) = \Delta(f(x)) = -2012 = -4 \cdot 503.$$

We are not as lucky as last time; $\Delta(1, \alpha, \alpha^2)$ is not squarefree, and so the algorithm must be run with $I = 2$. Hence, we consider all elements of the form

$$\theta = \frac{1}{2}(c_1 + c_2\alpha + c_3\alpha^2),$$

where each $c_i \in \{0, 1\}$ and not all $c_i = 0$. (Note that the condition that some $c_i = 1$ is then automatic.) For each θ, we test whether the field polynomial

$$\phi_\theta(x) = (x - \theta)(x - \theta')(x - \theta'') \in \mathbb{Z}[x].$$

Here $'$ and $''$ are used for the non-identity embeddings into $\mathbb{C}$. The actual computations of the $\phi_\theta(x)$ can be carried out either symbolically (using the theory of symmetric functions), or numerically, computing θ, θ', and θ'' in terms of floating point approximations to the roots of $f(x)$. (In this latter approach, it is helpful to first notice that

$$8 \cdot \phi_\theta(x) = \phi_{2\theta}(2x) \in \mathbb{Z}[x],$$

[5]See, for instance, Chapter 12 of: Gelfand, I. M.; Kapranov, M. M.; Zelevinsky, A. V. *Discriminants, resultants, and multidimensional determinants.* Mathematics: Theory & Applications. Birkhäuser Boston, Inc., Boston, MA, 1994.

so that even a crude approximation to the coefficients of $\phi_\theta(x)$ is sufficient to pin down their exact values.) Either way, our search turns up that for $\theta = \frac{1}{2}(\alpha + \alpha^2)$,

$$\phi_\theta(x) = x^3 - 2x^2 + 3x - 10 \in \mathbb{Z}[x].$$

We therefore replace $1, \alpha, \alpha^2$ with $1, \alpha, \frac{1}{2}(\alpha + \alpha^2)$. We are guaranteed (by our earlier discussion) that these new elements generate a subgroup of index dividing $2/2 = 1$. Hence, they form an integral basis for K.

Example 14.4. Let $K = \mathbb{Q}(\sqrt{2}, \sqrt{3})$. Then K is a degree 4 Galois extension of $\mathbb{Q}$, where the four embeddings of K into $\mathbb{C}$ are described by independently choosing whether or not to swap the signs of $\sqrt{2}$ and $\sqrt{3}$. To compute an integral basis for K, start with the seed $1, \sqrt{2}, \sqrt{3}, \sqrt{6}$. Then

$$\begin{aligned}\Delta(1, \sqrt{2}, \sqrt{3}, \sqrt{6}) &= \det \begin{bmatrix} 1 & \sqrt{2} & \sqrt{3} & \sqrt{6} \\ 1 & -\sqrt{2} & \sqrt{3} & -\sqrt{6} \\ 1 & \sqrt{2} & -\sqrt{3} & -\sqrt{6} \\ 1 & -\sqrt{2} & -\sqrt{3} & \sqrt{6} \end{bmatrix}^2 \\ &= 9216 = 2^{10} \cdot 3^2.\end{aligned}$$

Thus, we run the algorithm with $I = 2^5 \cdot 3$. For the first pass, we can choose either the prime $p = 2$ or $p = 3$. We pick $p = 3$, and so we consider all elements of the form

$$\theta = \frac{1}{3}(c_0 + c_1\sqrt{2} + c_2\sqrt{3} + c_3\sqrt{6}),$$

with each $0 \le c_i < 3$, and some $c_i = 1$. Explicitly computing all the $\phi_\theta(x)$, we find that none have integer coefficients. Hence, we restart the algorithm, keeping the seed value the same, but now taking $I = 2^5$ and $p = 2$. We look among the elements

$$\theta = \frac{1}{2}(c_0 + c_1\sqrt{2} + c_2\sqrt{3} + c_3\sqrt{6}),$$

where each $c_i \in \{0, 1\}$, and not all $c_i = 0$. We find that when $\theta = \frac{1}{2}(\sqrt{2} + \sqrt{6})$,

$$\phi_\theta(x) = x^4 - 4x + 1.$$

Thus, we replace our tuple with $1, \frac{1}{2}(\sqrt{2} + \sqrt{6}), \sqrt{3}, \sqrt{6}$. We run the algorithm again on these elements, this time with $I = 2^4$ and $p = 2$.

None of the field polynomials that show up have integer coefficients. We conclude that $1, \frac{1}{2}(\sqrt{2}+\sqrt{6}), \sqrt{3}, \sqrt{6}$ is an integral basis for K.

An integral basis for $\mathbb{Q}(\zeta_p)$

The method outlined in the last section is useful in individual cases. To treat infinite families of number fields, cunning is required to circumvent the need for infinitely many separate computations. The following proposition is often helpful.

Proposition 14.5. Let α be an algebraic integer whose minimal polynomial satisfies Eisenstein's criterion with respect to the prime p; that is,

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

where $p \mid a_i$ for all $0 \le i < n$, and $p^2 \nmid a_0$. Then with $K = \mathbb{Q}(\alpha)$,

$$p \nmid [\mathbb{Z}_K : \mathbb{Z}[\alpha]].$$

Before giving the proof, we isolate the key insight. Plugging α into $\min_\alpha(x)$ and rearranging shows that in $\mathbb{Z}_K$,

$$\begin{aligned} \alpha^n &= -a_{n-1}\alpha^{n-1} - a_{n-2}\alpha^{n-2} - \cdots - a_0 \\ &\equiv 0 \pmod{p}, \end{aligned} \tag{14.4}$$

since each of $a_0, \ldots, a_{n-1}$ is divisible by p.

Proof of Proposition 14.5. We will show that the (additive) quotient group $\mathbb{Z}_K/\mathbb{Z}[\alpha]$ has no order p elements. Equivalently, whenever

$$p \mid b_0 + \cdots + b_{n-1}\alpha^{n-1} \quad (\text{in } \mathbb{Z}_K), \tag{14.5}$$

each coefficient b_i is a multiple of p (in $\mathbb{Z}$). Supposing we have a counterexample, choose the smallest index i for which $p \nmid b_i$. Then taking (14.5) modulo p,

$$b_i\alpha^i + b_{i+1}\alpha^{i+1} + \cdots + b_{n-1}\alpha^{n-1} \equiv 0 \pmod{p}.$$

Multiplying through by α^{n-1-i} and recalling (14.4), we find that

$$b_i\alpha^{n-1} \equiv 0 \pmod{p}.$$

That is,

$$\frac{b_i\alpha^{n-1}}{p} \in \mathbb{Z}_K.$$

We derive a contradiction by observing that $\mathrm{N}\frac{b_i\alpha^{n-1}}{p} \notin \mathbb{Z}$. Indeed,

$$\mathrm{N}\left(\frac{b_i\alpha^{n-1}}{p}\right) = \frac{b_i^n}{p^n}\mathrm{N}(\alpha)^{n-1} = \pm\frac{b_i^n a_0^{n-1}}{p^n};$$

since $p \nmid b_i$ and $p \parallel a_0$, the final numerator is divisible by p^{n-1} but not by p^n. □

Here is one application (others are given in the exercises). For p a prime number, let $\zeta_p = e^{2\pi i/p}$, and set $K = \mathbb{Q}(\zeta_p)$. The field K is called the pth **cyclotomic field**. (In general, the m**th cyclotomic field** is $\mathbb{Q}(e^{2\pi i/m})$.) Since $\zeta_p^p = 1$ and $\zeta_p \neq 1$, we have that ζ_p is a root of

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

The right-hand polynomial, which we will denote by $\Phi_p(x)$, is well-known to be irreducible. The simplest proof of this goes by substituting $x \mapsto x + 1$;

$$\begin{aligned}\Phi_p(x+1) &= \frac{(x+1)^p - 1}{x} \\ &= x^{p-1} + \binom{p}{p-1}x^{p-2} + \cdots + \binom{p}{2}x + p,\end{aligned}$$

which satisfies Eisenstein's criterion with respect to p. Consequently,

$$[K : \mathbb{Q}] = p - 1.$$

Using Proposition 14.5, we now prove that the most natural guess for the ring of integers of K is correct.

Theorem 14.6. $\mathbb{Z}_K = \mathbb{Z}[\zeta_p]$.

Proof. We can assume that p is odd. Indeed, if $p = 2$, then $K = \mathbb{Q}$, and the assertion of the theorem is clear. Let $H = \mathbb{Z}[\zeta_p]$, i.e., the $\mathbb{Z}$-submodule of $\mathbb{Z}_K$ generated by

$$1, \quad \zeta_p, \quad \zeta_p^2, \quad \ldots, \quad \zeta_p^{p-2}.$$

The $p-1$ embeddings of K into $\mathbb{C}$ send ζ_p to ζ_p^j, for $j \in \{1, 2, \ldots, p-1\}$. So by a familiar Vandermonde determinant argument,

$$\Delta(1, \zeta_p, \ldots, \zeta_p^{p-2}) = \prod_{1 \le i < j \le p-1} (\zeta_p^j - \zeta_p^i)^2.$$

It is not hard to evaluate the right-hand product. We start by noticing that $(\zeta_p^j - \zeta_p^i)^2 = -(\zeta_p^j - \zeta_p^i)(\zeta_p^i - \zeta_p^j)$; hence,

$$\prod_{1\le i<j\le p-1} (\zeta_p^j - \zeta_p^i)^2 = (-1)^{\binom{p-1}{2}} \prod_{\substack{1\le i,j\le p-1\\ i\ne j}} (\zeta_p^j - \zeta_p^i).$$

The right-hand side here

$$= (-1)^{\binom{p-1}{2}} \prod_{1\le j\le p-1} \zeta_p^j \prod_{\substack{1\le i\le p-1\\ i\ne j}} (1 - \zeta_p^{i-j})$$

$$= (-1)^{\binom{p-1}{2}} \prod_{1\le j\le p-1} \frac{\zeta_p^j}{1-\zeta_p^{p-j}} \prod_{\substack{1\le i\le p\\ i\ne j}} (1 - \zeta_p^{i-j});$$

moreover, for each j, the final product on i takes the same value, namely

$$\prod_{1\le k\le p-1} (1 - \zeta_p^k) = \Phi_p(1) = p.$$

Putting this back in above,

$$\Delta(1, \zeta_p, \dots, \zeta_p^{p-2}) = (-1)^{\binom{p-1}{2}} p^{p-1} \prod_{1\le j\le p-1} \frac{\zeta_p^j}{1-\zeta_p^{p-j}}.$$

Now

$$\prod_{1\le j\le p-1} \frac{\zeta_p^j}{1-\zeta_p^{p-j}} = (\zeta_p^p)^{(p-1)/2} \prod_{1\le k\le p-1} \frac{1}{1-\zeta_p^k} = \frac{1}{p},$$

while $\binom{p-1}{2}$ and $\frac{p-1}{2}$ have the same parity. Thus,

$$\Delta(1, \zeta_p, \dots, \zeta_p^{p-2}) = (-1)^{(p-1)/2} p^{p-2}.$$

Recall that $[\mathbb{Z}_K : H]^2 \mid \Delta(1, \zeta_p, \dots, \zeta_p^{p-2})$ (see (14.1)). Thus,

$$[\mathbb{Z}_K : H] \text{ is a power of } p.$$

Now for the punchline: The minimal polynomial of $\zeta_p - 1$ is $\Phi_p(x+1)$, which is Eisenstein with respect to p. So by Proposition 14.5, $p \nmid [\mathbb{Z}_K : \mathbb{Z}[\zeta_p - 1]]$. But $\mathbb{Z}[\zeta_p - 1] = \mathbb{Z}[\zeta_p] = H$! So $p \nmid [\mathbb{Z}_K : H]$. Since $[\mathbb{Z}_K : H]$ is a power of p, it must be the zeroth power of p. That is, $\mathbb{Z}_K = \mathbb{Z}[\zeta_p]$, as desired. Note that as a byproduct of this proof, we have $\Delta_K = (-1)^{(p-1)/2} p^{p-2}$. □

It can be shown that the ring of integers of $\mathbb{Q}(e^{2\pi i/m})$ is always $\mathbb{Z}[e^{2\pi i/m}]$. The proof given above generalizes easily to the case when $m = p^r$ is a prime power (Exercise 5). See (e.g.) Marcus's text[6] (pp. 33–36) for a description of how to reduce the general case to the prime power case.

Presented with limited interruption, for your viewing pleasure

We end the chapter by exhibiting integral bases for two special classes of number fields. The results are not needed elsewhere and are included only "for flavor". Proofs are sketched in Marcus's book (ibid.; see Exercises 41–42 on pp. 49–52).

First up are the **pure cubic fields**, those number fields of the form $\mathbb{Q}(\sqrt[3]{d})$ for a noncube integer d. It is clearly enough to consider d that are positive and cubefree. Such a d has a unique representation in the form $d = ab^2$, where a and b are coprime and squarefree. If $3 \mid d$, we can also assume that $3 \mid a$, since $\mathbb{Q}(\sqrt[3]{ab^2}) = \mathbb{Q}(\sqrt[3]{a^2b})$.

Theorem 14.7. Assume d, a, and b are as above. If $d \not\equiv \pm 1 \pmod 9$, then an integral basis for $\mathbb{Q}(\sqrt[3]{d})$ is

$$1, \quad \sqrt[3]{d}, \quad \frac{1}{b}(\sqrt[3]{d})^2.$$

If $d \equiv \pm 1 \pmod 9$, then an integral basis for $\mathbb{Q}(\sqrt[3]{d})$ is

$$\sqrt[3]{d}, \quad \frac{1}{b}(\sqrt[3]{d})^2, \quad \frac{1 \pm \sqrt[3]{d} + (\sqrt[3]{d})^2}{3},$$

where the $\pm$ matches the sign in the congruence for d mod 9.

The second family we consider is the class of **biquadratic number fields** K. These are the quartic Galois extensions of $\mathbb{Q}$ with $\mathrm{Gal}(K/\mathbb{Q}) \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$. Since $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$ has three index two subgroups, K has three quadratic subfields, any two of which generate K. Writing these as $\mathbb{Q}(\sqrt{m})$, $\mathbb{Q}(\sqrt{n})$, and $\mathbb{Q}(\sqrt{k})$, where m, n, and k are squarefree, it is easy to see that

$$k = \frac{mn}{\gcd(m,n)^2};$$

[6] Marcus, D. A. *Number fields.* Universitext. Springer-Verlag, New York-Heidelberg, 1977.

of course, the same relation holds for any permutation of m, n, and k. Using this, it is straightforward to show that after relabeling m, n, and k, we may assume that

$$(m, n) \equiv (1,1), (1,2), (2,3), \text{ or } (3,3) \pmod 4.$$

Theorem 14.8. Let m, n, and k be as above. Set

$$m_1 = m/\gcd(m,n), \quad \text{and} \quad n_1 = n/\gcd(m,n).$$

(a) If $(m, n) \equiv (1,1)$ and $(m_1, n_1) \equiv (1,1) \bmod 4$, then an integral basis for K is

$$1, \quad \frac{1+\sqrt{m}}{2}, \quad \frac{1+\sqrt{n}}{2}, \quad \frac{1+\sqrt{m}+\sqrt{n}+\sqrt{k}}{4}.$$

(b) If $(m, n) \equiv (1,1)$ and $(m_1, n_1) \equiv (3,3) \bmod 4$, an integral basis for K is

$$1, \quad \frac{1+\sqrt{m}}{2}, \quad \frac{1+\sqrt{n}}{2}, \quad \frac{1-\sqrt{m}+\sqrt{n}+\sqrt{k}}{4}.$$

(c) If $(m, n) \equiv (1,2) \bmod 4$, an integral basis for K is

$$1, \quad \frac{1+\sqrt{m}}{2}, \quad \sqrt{n}, \quad \frac{\sqrt{n}+\sqrt{k}}{2}.$$

(d) If $(m, n) \equiv (2,3) \bmod 4$, an integral basis for K is

$$1, \quad \sqrt{m}, \quad \sqrt{n}, \quad \frac{\sqrt{m}+\sqrt{k}}{2}.$$

(e) If $(m, n) \equiv (3,3) \bmod 4$, an integral basis for K is

$$1, \quad \sqrt{m}, \quad \frac{\sqrt{m}+\sqrt{n}}{2}, \quad \frac{1+\sqrt{k}}{2}.$$

Explicit integral bases are known for several other families of number fields; the reader should be warned that their descriptions are sometimes quite complicated. For instance, Berwick[7] gave a complete answer for all pure binomial fields $\mathbb{Q}(\sqrt[n]{a})$, but stating his result requires consideration of 23 separate cases.

[7]Berwick, W. E. H. *Integral bases.* Cambridge Tracts in Mathematics and Mathematical Physics, **22**. Stechert-Hafner, Inc., New York, 1964. Originally published in 1927 by Cambridge University Press.

Exercises

(1) Prove the claim from p. 145: When $p \mid [\mathbb{Z}_K : H]$, it is always possible to choose integers $c_1, \ldots, c_n$ in (14.3) with some $c_i = 1$.

(2) Let $K = \mathbb{Q}(\alpha)$, where α is a root of the irreducible cubic polynomial $f(x) = x^3 + x^2 + 2$. Show that $\mathbb{Z}_K = \mathbb{Z}[\alpha]$. *Hint:* Show that either $\mathbb{Z}_K = \mathbb{Z}[\alpha]$ or $\Delta_K = -29$. Rule out the latter using Stickelberger's criterion (Exercise 13.1).

(3) Let $L = \mathbb{Q}(\sqrt{2}, \sqrt{3})$. Give another proof that 1, $\sqrt{2}$, $\sqrt{3}$, and $\frac{1}{2}(\sqrt{2} + \sqrt{6})$ form a $\mathbb{Z}$-basis for $\mathbb{Z}_L$, using Exercise 13.3 instead of the successive approximation algorithm.

(4) Let p be an odd prime. Show that $\zeta_p + \zeta_p^{-1}$ is algebraic of degree $\frac{p-1}{2}$. With $K = \mathbb{Q}(\zeta_p + \zeta_p^{-1})$, show that $\mathbb{Z}_K = \mathbb{Z}[\zeta_p + \zeta_p^{-1}]$. *Hint for the second part:* Assuming otherwise, obtain a contradiction with Theorem 14.6.

(5) Let $\zeta_m = e^{2\pi i/m}$. Show that when m is a prime power, the ring of integers of $\mathbb{Q}(\zeta_m)$ is $\mathbb{Z}[\zeta_m]$. *Hint:* Start by showing that when $m = p^k$, the minimal polynomial of ζ_m is $\Phi_p(x^{p^{k-1}})$.

(6) Suppose that d is a squarefree integer with $d \not\equiv \pm 1 \pmod 9$.
   (a) Show that $x^3 - d$ is irreducible over $\mathbb{Q}$.
   (b) Let $K = \mathbb{Q}(\sqrt[3]{d})$. Show that every prime dividing $[\mathbb{Z}_K : \mathbb{Z}[\sqrt[3]{d}]]$ also divides $3d$. *Hint:* Start by computing $\Delta(1, \sqrt[3]{d}, (\sqrt[3]{d})^2)$, perhaps using Exercise 13.5.
   (c) Show that if $p \mid d$, then $p \nmid [\mathbb{Z}_K : \mathbb{Z}[\sqrt[3]{d}]]$. *Hint:* Proposition 14.5.
   (d) Show that $3 \nmid [\mathbb{Z}_K : \mathbb{Z}[\sqrt[3]{d}]]$. *Hint:* $\mathbb{Z}[\sqrt[3]{d}] = \mathbb{Z}[\sqrt[3]{d} \pm 1]$.
   (e) Conclude that $\mathbb{Z}_K = \mathbb{Z}[\sqrt[3]{d}]$ (a special case of Theorem 14.7).

(7) Let p be a prime number. By Fermat's little theorem, $2^p \equiv 2 \pmod p$. Suppose that $2^p \not\equiv 2 \pmod{p^2}$.[8]
   (a) Let $K = \mathbb{Q}(\sqrt[p]{2})$. Show that every prime dividing $[\mathbb{Z}_K : \mathbb{Z}[\sqrt[p]{2}]]$ divides $2p$.
   (b) Show that $2 \nmid [\mathbb{Z}_K : \mathbb{Z}[\sqrt[p]{2}]]$.

[8] Empirically, this noncongruence condition holds the overwhelming majority of the time. Indeed, the only primes $p < 5 \cdot 10^{11}$ satisfying $2^p \equiv 2 \pmod{p^2}$ are $p = 1093$ and $p = 3511$. Nevertheless, it is not even known that there are infinitely many primes p with $2^p \not\equiv 2 \pmod{p^2}$. (But that much would follow from the abc conjecture; see: Silverman, J.H. *Wieferich's criterion and the abc-conjecture.* J. Number Theory **30** (1988), no. 2, 226–237.)

(c) Show that $p \nmid [\mathbb{Z}_K : \mathbb{Z}[\sqrt[p]{2}]]$. *Hint:* $\mathbb{Z}[\sqrt[p]{2}] = \mathbb{Z}[\sqrt[p]{2} - 2]$.

(d) Conclude that $\mathbb{Z}_K = \mathbb{Z}[\sqrt[p]{2}]$.

In Exercise 17.17 you are asked to prove the converse: If $\mathbb{Z}_K = \mathbb{Z}[\sqrt[p]{2}]$, then $p^2 \nmid 2^p - 2$.[9]

(8) (Cyclotomic polynomials) For each $m \in \mathbb{Z}^+$, set

$$\Phi_m(x) = \prod_{\substack{0 \le k < m \\ \gcd(k,m)=1}} (x - e^{2\pi i k/m}).$$

Note that when $m = p$ is prime, this agrees with our earlier definition of $\Phi_p(x)$.

(a) Show that $\prod_{d|m} \Phi_d(x) = x^m - 1$ for every positive integer m. *Hint:* The roots of $\Phi_d(x)$ are the elements of exact order d in $\mathbb{C}^\times$.

(b) By definition, $\Phi_m(x) \in \mathbb{C}[x]$. Using (a) and mathematical induction, prove that $\Phi_m(x) \in \mathbb{Z}[x]$ for all $m \in \mathbb{Z}^+$.

(c) In the remaining parts, we show that $\Phi_m(x)$ is always irreducible over $\mathbb{Q}$.[10]
Let $f(x)$ be the minimal polynomial of $e^{2\pi i/m}$ over $\mathbb{Q}$. Let ζ be any root of $f(x)$. Show that if p is any prime, then $p \mid f(\zeta^p)$, where the divisibility is claimed in $\bar{\mathbb{Z}}$.

(d) Keeping the same notation, show that if $f(\zeta^p) \neq 0$, then $f(\zeta^p) \mid \Delta(x^m - 1) \mid m^m$ (again, in $\bar{\mathbb{Z}}$).

(e) Deduce from (c) and (d) that if ζ is a root of $f(x)$ and p is a prime not dividing m (where the "not dividing" this time is taking place in $\mathbb{Z}$), then $f(\zeta^p) = 0$. Iterating, show that if ζ is a root of f, then $f(\zeta^k) = 0$ for every positive integer k coprime to m.

(f) Deduce that every root of $\Phi_m(x)$ is a root of $f(x)$. This is enough to conclude that $\Phi_m(x)$ is irreducible — why?

[9] It follows that $\mathbb{Z}[\sqrt[p]{2}]$ is the ring of integers of $\mathbb{Q}(\sqrt[p]{2})$ for all primes $p < 1093$ but not for $p = 1093$!

[10] This proof is taken from: Schur, I. *Zur Irreduzibilität der Kreisteilungsgleichung.* Math. Z. **29** (1929), 463.

15

Ideal theory in general number rings

We are now in a position to establish the two central results of ideal theory — unique factorization and the finiteness of the class number — for rings of integers of arbitrary number fields. We follow a path suggested by Hurwitz,[1] where the finiteness of the class number is proved first and then used as a stepping stone in the proof of the fundamental theorem.

A finite monoid

Let K be an arbitrary number field. As in Chapter 9, let $\mathrm{Cl}(\mathbb{Z}_K) = \mathrm{Id}(\mathbb{Z}_K)/\approx$, where $\approx$ is the relation of dilation equivalence. Define multiplication on $\mathrm{Cl}(\mathbb{Z}_K)$ by setting $[I][J] = [I][J]$. That this is a well-defined operation making $\mathrm{Cl}(\mathbb{Z}_K)$ into a monoid can be checked exactly as in Chapter 9. Note that nothing special about $\mathbb{Z}_K$ is being used yet; at this stage, the entire construction could be carried out for any integral domain.

While it is entirely routine to prove that $\mathrm{Cl}(\mathbb{Z}_K)$ is a monoid, it is not at all obvious that $\mathrm{Cl}(\mathbb{Z}_K)$ should be a finite group. In fact, both pieces of that description — "finite" and "group" — encapsulate nontrivial claims. In this section, we prove that $\mathrm{Cl}(\mathbb{Z}_K)$ is finite; in the

[1] Hurwitz, A. *Zur Theorie der algebraischen Zahlen.* Gött. Nachr. (1895), no. 3, 324–331.
Our exposition is modeled on Chapter 12 of: Ireland, K.; Rosen, M. *A classical introduction to modern number theory.* Second edition. Graduate Texts in Mathematics, **84**. Springer-Verlag, New York, 1990.

next section, we describe how to "promote" $\mathrm{Cl}(\mathbb{Z}_K)$ from a monoid to a group.

The next proposition should be compared with Lemma 11.4, which gave a more precise result for certain imaginary quadratic fields.

Proposition 15.1 (Every number field is "almost-Euclidean")**.** For every number field K, there is a constant $T = T(K) \in \mathbb{Z}^+$ with the following property. For every $\theta \in K$, there is a positive integer $t \leq T$ and a $\xi \in \mathbb{Z}_K$ with

$$|\mathrm{N}(t\theta - \xi)| < 1.$$

The proof of Lemma 11.4 used Dirichlet's approximation theorem (Theorem 8.5). Our proof of Proposition 15.1 rests on the following variant of that result.

Lemma 15.2 (Dirichlet's simultaneous approximation theorem)**.** Let $n \in \mathbb{Z}^+$. Let $x_1, \ldots, x_n$ be arbitrary real numbers. For all $Q \in \mathbb{Z}^+$, there is a positive integer $q \leq Q^n$ with

$$\|qx_i\| \leq \frac{1}{Q} \qquad \text{for all } i = 1, 2, \ldots, n. \tag{15.1}$$

Taking $n = 1$ in Lemma 15.2, we *almost* recover Theorem 8.5; the new bound is a tiny bit weaker, $1/Q$ vs. $1/(Q+1)$. But see Exercise 7.

Proof. Consider the $Q^n + 1$ points in the n-dimensional unit cube $[0,1)^n$ given by

$$(\{qx_1\}, \ldots, \{qx_n\}),$$

for $q = 0, 1, 2, \ldots, Q^n$. Subdividing $[0,1)^n$ into Q^n subcubes of edge length $1/Q$ in the obvious way, two of these points — say those corresponding to q_1 and q_2 with $q_1 < q_2$ — must lie in the same subcube. We may take $q = q_2 - q_1$. □

Proof of Proposition 15.1. Let $n = [K : \mathbb{Q}]$. Fix an integral basis $\omega_1, \ldots, \omega_n$ for K. Letting σ run over the embeddings of K into $\mathbb{C}$, set

$$Q = 1 + \left\lfloor \sum_{i=1}^{n} \sum_{\sigma} |\sigma(\omega_i)| \right\rfloor.$$

We will prove that Proposition 15.1 holds with

$$T = Q^n.$$

Since the ω_i form a $\mathbb{Q}$-basis for K, each $\theta \in K$ can be written in the form $\theta = x_1\omega_1 + \cdots + x_n\omega_n$, with $x_1, \ldots, x_n \in \mathbb{Q}$. Use Lemma 15.2 to select an integer $t \in [1, T]$ with $\|tx_i\| \le 1/Q$ for all $i = 1, 2, \ldots, n$. Let A_i be the nearest integer to each tx_i, and let $\xi = A_1\omega_1 + \cdots + A_n\omega_n$. Then $\xi \in \mathbb{Z}_K$, and $t\theta - \xi = c_1\omega_1 + \cdots + c_n\omega_n$, where $c_1, \ldots, c_n$ are rational numbers satisfying $\max_i |c_i| \le 1/Q$. Hence,

$$\begin{aligned} |\mathrm{N}(t\theta - \xi)| &= \prod_\sigma |c_1\sigma(\omega_1) + \cdots + c_n\sigma(\omega_n)| \\ &\le \prod_\sigma \left(\max_i |c_i| \cdot \sum_i |\sigma(\omega_i)| \right) \le \prod_\sigma \left(\frac{\sum_i |\sigma(\omega_i)|}{Q} \right). \end{aligned}$$

By the choice of Q, each term in the final product is < 1, and so $|\mathrm{N}(t\theta - \xi)| < 1$. □

In Chapter 11, Lemma 11.4 was used to prove that (for certain imaginary quadratic fields) small prime ideals generate the class group. A very slight modification of this argument, using Proposition 15.1 in place of Lemma 11.4, shows that $\mathrm{Cl}(\mathbb{Z}_K)$ is finite.

Theorem 15.3. $\#\mathrm{Cl}(\mathbb{Z}_K) < \infty$.

As before, we set $h_K := \#\mathrm{Cl}(\mathbb{Z}_K)$, and we call h_K the **class number of** K (or of $\mathbb{Z}_K$).

Proof. Let $T = T(K)$ be as in the statement of Proposition 15.1. We will show that for each nonzero ideal I, there is an ideal J in the same class as I that contains $T!$. The ideals of $\mathbb{Z}_K$ containing $T!$ are in bijection with the ideals of the finite ring $\mathbb{Z}_K/T!\mathbb{Z}_K$; hence, there are only finitely many of them. So Theorem 15.3 follows.

Let β be an element of I chosen with $|\mathrm{N}\beta|$ as small as possible. We first argue that for each $\alpha \in I$, there is a positive integer $t \le T$ with $t\alpha \in \langle\beta\rangle$. Applying Proposition 15.1 with $\theta = \alpha/\beta$, we obtain a positive integer $t \le T$ and a $\xi \in \mathbb{Z}_K$ with $|\mathrm{N}(t\alpha/\beta - \xi)| < 1$. Then $t\alpha - \beta\xi \in I$ (since both $\alpha, \beta \in I$) and $|\mathrm{N}(t\alpha - \beta\xi)| < |\mathrm{N}\beta|$. The minimality of β forces $t\alpha = \beta\xi$. Hence, $t\alpha \in \langle\beta\rangle$.

Since $T!$ is a multiple of each $t \in [1, T]$, the result of the last paragraph gives that $T!\alpha \in \langle\beta\rangle$ for every $\alpha \in I$. That is, $T!I \subseteq \langle\beta\rangle$.

Hence, if we put $J := \frac{T!}{\beta} I$, then J is an ideal of $\mathbb{Z}_K$. Clearly, J is dilation equivalent to I, and so $[I] = [J]$. Moreover, since $\beta \in I$,

$$T! = \frac{T!}{\beta}\beta \in \frac{T!}{\beta} I = J.$$

That is, J contains $T!$. □

"Class" mobility: From monoid to group

To prove that $\mathrm{Cl}(\mathbb{Z}_K)$ is a group, we must show that every ideal class is invertible; equivalently, every nonzero ideal has a principal multiple. We give a proof depending on Theorem 15.3 and some special cases of the cancellation law in $\mathrm{Id}(\mathbb{Z}_K)$.

Lemma 15.4. Let I and J be nonzero ideals of $\mathbb{Z}_K$. If $IJ = J$, then $I = \langle 1 \rangle$.

Proof. If $IJ = J$, then every element of J is a linear combination of elements of J with coefficients from I. To exploit this, choose a finite list of elements of J that generate J as an ideal, say

$$J = \langle \beta_1, \ldots, \beta_m \rangle.$$

We will address the question of how we know J is finitely generated at the end of the proof. Then each β_j, for $j = 1, 2, \ldots, m$, can be written in the form

$$\beta_j = \sum_{i=1}^{m} A_{i,j} \beta_i,$$

where all the $A_{i,j} \in I$. In matrix form,

$$[\beta_1, \ldots, \beta_m] = [\beta_1, \ldots, \beta_m] \begin{bmatrix} A_{1,1} & A_{1,2} & \cdots & A_{1,m} \\ A_{2,1} & A_{2,2} & \cdots & A_{2,m} \\ \vdots & \vdots & \ddots & \vdots \\ A_{m,1} & A_{m,2} & \cdots & A_{m,m} \end{bmatrix}.$$

Since J is not the zero ideal, at least one β_j is nonzero. So denoting the right-hand matrix by A, we see that $\mathrm{Id} - A$ has a nonzero left-kernel. Hence, $\det(\mathrm{Id} - A) = 0$. But computing modulo I (keeping in mind that each $A_{i,j} \in I$), $\det(\mathrm{Id} - A) \equiv \det(\mathrm{Id}) \equiv 1 \pmod{I}$. Thus, $0 \equiv 1 \pmod{I}$, so that $1 \in I$ and $I = \langle 1 \rangle$.

Returning to earlier in the proof: How do we know that J is a finitely generated ideal? We will prove a somewhat stronger statement, namely that each nonzero ideal J of $\mathbb{Z}_K$ is finitely generated as a $\mathbb{Z}$-module. Let α be a nonzero element of J. Then $\langle\alpha\rangle \subseteq J \subseteq \mathbb{Z}_K$. By Proposition 13.9, $\mathbb{Z}_K/\langle\alpha\rangle$ is finite, and so $J/\langle\alpha\rangle$ is a finite abelian group. If $\gamma_1, \ldots, \gamma_\ell$ are a full set of coset representatives for $J/\langle\alpha\rangle$, and $\omega_1, \ldots, \omega_n$ is a $\mathbb{Z}$-basis for $\mathbb{Z}_K$, then J is the $\mathbb{Z}$-span of $\gamma_1, \ldots, \gamma_\ell, \alpha\omega_1, \ldots, \alpha\omega_n$. □

Lemma 15.5. Let I and J be nonzero ideals of $\mathbb{Z}_K$, and let β be a nonzero element of $\mathbb{Z}_K$. If

$$IJ = \beta J,$$

then $I = \langle\beta\rangle$.

Proof. It is tempting to argue as follows: Dilating both sides of the given equation by $1/\beta$ shows that

$$\left(\frac{1}{\beta}I\right)J = J.$$

So by Lemma 15.4, $\frac{1}{\beta}I = \langle 1\rangle$. Thus, $I = \langle\beta\rangle$.

Unfortunately, we cannot make this argument unless and until we know that $\frac{1}{\beta}I$ is an ideal of $\mathbb{Z}_K$. That will be true if (and only if) I is contained in $\langle\beta\rangle$. Is it?

Yes! Let α be any element of I. Then

$$\frac{\alpha}{\beta}J \in \frac{1}{\beta}IJ = \frac{1}{\beta}\cdot\beta J = J.$$

Thus, multiplication by α/β maps J into itself. J is a finitely generated $\mathbb{Z}$-submodule of $\mathbb{C}$ (by the argument at the end of the last proof). By assumption, $J \neq \{0\}$. Invoking Lemma 2.5, $\alpha/\beta \in \bar{\mathbb{Z}}$. Thus, $\beta \mid \alpha$ in $\mathbb{Z}_K$. Since this holds for every $\alpha \in I$, we have that $I \subseteq \langle\beta\rangle$. □

Now for the main event.

Lemma 15.6 (Principal multiple lemma)**.** For each nonzero ideal I of $\mathbb{Z}_K$, there is a nonzero ideal J of $\mathbb{Z}_K$ with IJ principal.

Proof. Consider the infinite sequence $[I]$, $[I]^2$, $[I]^3$, ... of powers of $[I]$ in $\mathrm{Cl}(\mathbb{Z}_K)$. Since $\mathrm{Cl}(\mathbb{Z}_K)$ is finite, two terms coincide, say $[I]^k = [I]^\ell$ with positive integers $k < \ell$. Thus, $I^k = \lambda I^\ell$ for some nonzero $\lambda \in K$.

Using Proposition 2.9, we can write $\lambda = \alpha/m$, where $\alpha \in \mathbb{Z}_K$ and $m \in \mathbb{Z}^+$. Then

$$mI^k = \alpha I^\ell = \alpha I^{\ell-k} \cdot I^k.$$

By Lemma 15.5,

$$\alpha I^{\ell-k} = \langle m \rangle.$$

Hence, $\alpha \mid m$. Write $m = \alpha\beta$, where $\beta \in \mathbb{Z}_K$. Then dilating both sides of the last displayed equation by $1/\alpha$,

$$I^{\ell-k} = \langle \beta \rangle.$$

Hence, we can take $J = I^{\ell-k-1}$. □

The fundamental theorem revisited

With the principal multiple lemma established, the rest of the theory quickly falls into place. For example, our piecemeal results on cancellation (Lemmas 15.4 and 15.5) are immediately made obsolete by the next theorem, whose proof is identical with that of Theorem 6.13.

Theorem 15.7. The monoid $\mathrm{Id}(\mathbb{Z}_K)$ is cancellative. In other words, for any nonzero ideals I, J, J' with $IJ = IJ'$, we have $J = J'$.

Now we set our sights on the fundamental theorem.

Theorem 15.8 (Fundamental theorem of ideal theory, general case)**.** Let K be an arbitrary number field. Every nonzero ideal of $\mathbb{Z}_K$ factors uniquely as a product of nonzero prime ideals.

The proof of Theorem 15.8 follows the exact same lines as the special case treated in Chapter 6. We summarize the main steps.

First up is a reaffirmation of our slogan "to contain is to divide".

Theorem 15.9 (generalizing Theorem 6.14)**.** Let I and J be nonzero ideals of $\mathbb{Z}_K$. Then I contains $J \iff I$ divides J.

The proof is the same, word-for-word, as for Theorem 6.14.

Next, one shows that $\mathrm{Id}(\mathbb{Z}_K)$ satisfies the criterion for unique factorization set down in Proposition 4.5. This is done in two stages.

Lemma 15.10 (Id($\mathbb{Z}_K$) is atomic; generalizing Lemma 6.15)**.** Every element of Id($\mathbb{Z}_K$) factors as a product of irreducible elements of Id($\mathbb{Z}_K$). Here the unit ideal is considered to be the empty product of irreducibles.

Lemma 15.11 (generalizing Lemma 6.16)**.** Every irreducible element of Id($\mathbb{Z}_K$) is prime (in the monoidal sense).

The proofs are identical to the Chapter 6 versions, except for one small wrinkle. To prove Lemma 15.10 by the induction argument used for Lemma 6.15, we need a small auxiliary result.

Lemma 15.12. Let I and J be nonzero, nonunit ideals of $\mathbb{Z}_K$. Then

$$\mathrm{N}(I), \mathrm{N}(J) < \mathrm{N}(IJ).$$

We needed this also in Chapter 6, but there we could appeal to the (already-known) multiplicativity of the ideal norm. That result will be proved in the next section, *as a consequence of the fundamental theorem*. So we give a different proof of Lemma 15.12 here.

Proof of Lemma 15.12. Observe that

$$\mathrm{N}(IJ) = [\mathbb{Z}_K : IJ] = [\mathbb{Z}_K : I] \cdot [I : IJ] = \mathrm{N}(I) \cdot [I : IJ].$$

Hence, $\mathrm{N}(IJ) \geq \mathrm{N}(I)$, with equality only if $I = IJ$. But $I = IJ$ implies that $J = \langle 1 \rangle$, contrary to hypothesis. So $\mathrm{N}(IJ) > \mathrm{N}(I)$, and similarly $\mathrm{N}(IJ) > \mathrm{N}(J)$. □

The remaining steps in the proofs of Lemmas 15.10 and 15.11 go through exactly as before.

The arguments thus far show that nonzero ideals factor uniquely into prime ideals, where "prime" is meant in the monoidal sense. To finish up, one needs that the "monoidally prime" elements of Id($\mathbb{Z}_K$) coincide with the nonzero prime ideals of $\mathbb{Z}_K$, in the ring-theoretic sense. Since "to divide is to contain," this is immediate from Lemma 6.17. This completes the proof of Theorem 15.8.

Ideal norms redux

When we discussed ideal norms in Chapter 13, we left open the generalizations of Corollary 6.9 (that the ideal norm is multiplicative)

and Theorem 6.7 (that $I\tilde{I} = \langle \mathrm{N}(I) \rangle$). In this section, we fill these much-unneeded gaps. We start with multiplicativity.

Theorem 15.13. Let I and J be nonzero ideals of $\mathbb{Z}_K$. Then $\mathrm{N}(IJ) = \mathrm{N}(I)\mathrm{N}(J)$.

Since $\mathrm{Id}(\mathbb{Z}_K)$ is a unique factorization monoid with no nontrivial units, every pair of nonzero ideals has a unique greatest common divisor. This gcd can be described as the product of the prime ideals appearing in both ideal factorizations, raised to the appropriate multiplicities. But there is another, simpler description. Since "to divide is to contain", the gcd of two ideals is the smallest ideal of $\mathbb{Z}_K$ containing them both. So it is also true that

$$\gcd(I, J) = I + J.$$

We will use this observation below.

Proof. It is enough to show that $\mathrm{N}(IP) = \mathrm{N}(I)\mathrm{N}(P)$ whenever I is a nonzero ideal of $\mathbb{Z}_K$ and P is a nonzero prime ideal. Now

$$\frac{\mathrm{N}(IP)}{\mathrm{N}(I)} = \frac{[\mathbb{Z}_K : IP]}{[\mathbb{Z}_K : I]} = [I : IP].$$

So we would like to prove that I/IP and $\mathbb{Z}_K/P$ have the same size. In fact, we will show that

$$\mathbb{Z}_K/P \cong I/IP$$

as abelian groups. To this end, we start by observing that $I \supsetneq IP$. (The nontrivial part is the strict containment; this follows from the cancellation law or unique factorization.) Choose $\beta \in I \setminus IP$. Since $\beta P \subseteq IP$, the map $\psi : \mathbb{Z}_K/P \to I/IP$ defined by

$$\alpha \bmod P \to \alpha\beta \pmod{IP}$$

is a well-defined homomorphism of abelian groups. Clearly, ψ has image $(\langle \beta \rangle + IP)/IP$. Our choice of β implies (keeping in mind the remarks preceding this proof) that $\langle \beta \rangle + IP = \gcd(\langle \beta \rangle, IP) = I$, and so ψ is surjective. If $\alpha \bmod P$ lies in the kernel of ψ, then $\alpha\beta \in IP$, and hence

$$IP \mid \langle \alpha \rangle \langle \beta \rangle.$$

Since $\beta \in I$, we may write $\langle \beta \rangle = IJ$ for some J; then

$$P \mid \langle \alpha \rangle J.$$

If $P \mid J$, then $IP \mid \langle\beta\rangle$, and so $\beta \in IP$, contrary to hypothesis. So $P \mid \langle\alpha\rangle$. But then $\alpha \in P$ and so $\alpha \bmod P$ is the zero element of $\mathbb{Z}_K/P$. Thus, $\ker\psi$ is trivial and ψ is an isomorphism. □

We now look at generalizing the formula $I\tilde{I} = \langle \mathrm{N}(I)\rangle$, which expresses the ideal generated by the norm of I as the product of the conjugate ideals of I. An obvious obstacle presents itself when seeking to extend this to a non-Galois number field K; the "conjugate ideals" $\sigma(I)$ are ideals of $\mathbb{Z}_{\sigma(K)}$, rather than ideals of $\mathbb{Z}_K$. So in order to multiply the conjugate ideals together, we should first pass to an extension of K containing all of the conjugate fields $\sigma(K)$.

Theorem 15.14. Let L be any number field containing the Galois closure of $K/\mathbb{Q}$. Let I be a nonzero ideal of $\mathbb{Z}_K$. Then, as σ runs through the embeddings of K into $\mathbb{C}$,

$$\prod_\sigma \sigma(I)\mathbb{Z}_L = \mathrm{N}(I)\mathbb{Z}_L.$$

Warning: Do not confuse $\mathrm{N}(I)\mathbb{Z}_L$ with $\mathrm{N}(I\mathbb{Z}_L)$! When we write $\mathrm{N}(I)$ above, we mean the norm of the original $\mathbb{Z}_K$-ideal I, not the norm of its extension to $\mathbb{Z}_L$.

Proof. Let m be the order of $[I]$ in $\mathrm{Cl}(\mathbb{Z}_K)$. Then I^m is principal, say $I^m = \alpha\mathbb{Z}_K$, and

$$\left(\prod_\sigma \sigma(I)\mathbb{Z}_L\right)^m = \prod_\sigma \sigma(I^m)\mathbb{Z}_L = \prod_\sigma \sigma(\alpha)\mathbb{Z}_L = \mathrm{N}_{K/\mathbb{Q}}(\alpha)\mathbb{Z}_L.$$

Here the subscript in the notation "$\mathrm{N}_{K/\mathbb{Q}}(\alpha)$" means that the norm of α is computed with α viewed as an element of K, not as an element of L. By Proposition 13.12 and Theorem 15.13, $|\mathrm{N}_{K/\mathbb{Q}}(\alpha)| = \mathrm{N}(\alpha\mathbb{Z}_K) = \mathrm{N}(I^m) = \mathrm{N}(I)^m$, and so

$$\left(\prod_\sigma \sigma(I)\mathbb{Z}_L\right)^m = \mathrm{N}(I)^m\mathbb{Z}_L = (\mathrm{N}(I)\mathbb{Z}_L)^m.$$

Now take the mth root of both sides, which is justified by unique factorization in $\mathrm{Id}(\mathbb{Z}_L)$. □

Exercises

In Exercises 1–6, K is an arbitrary number field.

(1) Let I be a nonzero ideal of $\mathbb{Z}_K$. Show that the quotient $\mathbb{Z}_K/I$ has no nonzero nilpotent elements $\iff$ I is squarefree (by which we mean a product of distinct prime ideals).

(2) Let I be a nonzero ideal of $\mathbb{Z}_K$, and let α be any nonzero element of I. Prove that there is a $\beta \in \mathbb{Z}_K$ with $I = \langle \alpha, \beta \rangle$. In particular, every ideal of $\mathbb{Z}_K$ can be generated by at most two elements.

Hint: By Exercise 6.2, $\langle \alpha, \beta \rangle = \prod_P P^{\min\{\mathrm{ord}_P(\alpha), \mathrm{ord}_P(\beta)\}}$. Use Exercise 9.6 to select β so that the exponents on the prime ideals match those appearing in the factorization of I.[2]

(3) Let P be a nonzero prime ideal of $\mathbb{Z}_K$, and let $\pi \in P \setminus P^2$. Let $R \subseteq \mathbb{Z}_K$ be a complete set of coset representatives for $\mathbb{Z}_K/P$. Show that for each positive integer m, the elements

$$\rho_0 + \rho_1 \pi + \cdots + \rho_{m-1} \pi^{m-1}, \quad \text{with each } \rho_i \in R,$$

form a complete set of coset representatives for $\mathbb{Z}_K/P^m$.

(4) (a) For each nonzero ideal I of $\mathbb{Z}_K$, put $\Phi(I) = \#U(\mathbb{Z}_K/I)$; this is the $\mathbb{Z}_K$-analogue of Euler's totient function. Prove the corresponding version of Euler's theorem: Whenever $\alpha \in \mathbb{Z}_K$ is invertible modulo I, we have $\alpha^{\Phi(I)} \equiv 1 \pmod{I}$.

(b) Show that if I and J are coprime nonzero ideals of $\mathbb{Z}_K$, then $\Phi(IJ) = \Phi(I)\Phi(J)$. *Hint:* Chinese remainder theorem.

(c) Show that if P is a nonzero prime ideal of $\mathbb{Z}_K$, and m is any positive integer, then $\Phi(P^m) = \mathrm{N}(P)^m(1 - 1/\mathrm{N}(P))$.

Hint: To show the case $m = 1$, observe that $\mathbb{Z}_K/P$ is a finite integral domain (why?), and recall from basic algebra that all such objects are fields. (We give a different proof that $\mathbb{Z}_K/P$ is a field in Chapter 17.) To deal with the cases where $m > 1$, use the representation of the residue classes modulo P^m described in Exercise 3.

(d) Conclude that for any nonzero ideal I, we have $\Phi(I) = \mathrm{N}(I) \cdot \prod_{P|I}(1 - 1/\mathrm{N}(P))$.

---

[2] At this point, the reader will have no trouble checking that the results of the referenced exercises, though originally stated for quadratic fields, are valid for all number fields K.

(5) Let P be a nonzero prime ideal of $\mathbb{Z}_K$.
   (a) It is a standard result from elementary number theory that $U(\mathbb{Z}/p\mathbb{Z})$ is cyclic for every rational prime p. Take whichever proof of this you learned and generalize it to show that $U(\mathbb{Z}_K/P)$ is cyclic.
   (b) Show that $U(\mathbb{Z}_K/P^2)$ is cyclic $\iff$ $\mathrm{N}(P)$ is a rational prime number. *Hint for the forward direction*: Since $\mathbb{Z}_K/P$ is a finite field (see the previous hint), $\#\mathbb{Z}_K/P = p^f$ for some prime p and some $f \in \mathbb{Z}^+$. Show that the exponent of $U(\mathbb{Z}_K/P^2)$ always divides $p(p^f - 1)$.

(6) Let I be a nonzero ideal of $\mathbb{Z}_K$. Show that $\mathrm{N}(I) = \gcd_{\alpha \in I}\{\mathrm{N}\alpha\}$. (If you get stuck, try coming back to this problem after Chapter 17.)

(7) Strengthen the simultaneous approximation theorem as stated in Lemma 15.2 by showing that the denominator Q in (15.1) can be replaced with $(Q^n + 1)^{1/n}$. (Now taking $n = 1$ exactly recovers Theorem 8.5.) *Hint:* Apply Minkowski's theorem to show that for each $D < (Q^n + 1)^{1/n}$, there is a nonzero $\mathbb{Z}^{n+1}$-point in the $(n+1)$-dimensional region

$$\{(X, Y_1, \ldots, Y_n) : |X| < Q^n + 1, |x_i \cdot X - Y_i| \leq \frac{1}{D} \; \forall i\}.$$

Then take a sequence of D increasing towards $(Q^n + 1)^{1/n}$.

16

Finiteness of the class group and the arithmetic of $\bar{\mathbb{Z}}$

In this chapter, we discuss four interconnected consequences of the finiteness of the class group.

How to generate a nonprincipal ideal with a single element

> This was sometime a paradox, but now the time gives it proof. – Hamlet

The two defining properties of an ideal can be motivated by musing on basic facts about divisibility. Let R be any ring, and let α be any element of R. Then the sum of any two multiples of α is a multiple of α, and any multiple of a multiple of α is again a multiple of α. Of course, the set of all multiples of α is precisely the principal ideal αR.

Less trivially, some nonprincipal ideals of R can also be described as the set of multiples of a single element. To explain this paradoxical sounding statement, suppose that R is a subring of a larger ring S. Take any $\beta \in S$. Then the collection of all multiples of β *that lie in* R, i.e., $\beta S \cap R$, is an ideal of R which need not be principal.

Specializing to $R = \mathbb{Z}_K$ and $S = \bar{\mathbb{Z}}$, we see that $\beta\bar{\mathbb{Z}} \cap \mathbb{Z}_K$ is an ideal of $\mathbb{Z}_K$, for every $\beta \in \bar{\mathbb{Z}}$. It is a rather remarkable fact that the converse also holds.

Theorem 16.1 (Dedekind; "actuality" of ideals)**.** Let K be a number field. For every ideal I of $\mathbb{Z}_K$, there is a $\beta \in \bar{\mathbb{Z}}$ for which $I = \beta\bar{\mathbb{Z}} \cap \mathbb{Z}_K$.

For the proof, we need some results about extensions of ideals. Suppose that R is a subring of S and that I is an ideal of R. Then the **extension of** I **to** S, denoted IS, is the smallest ideal of S containing I. Equivalently,

$$IS = \{\text{finite sums } \sum a_i b_i : a_i \in I, b_i \in S\}.$$

The following two properties follow quickly from the definition; we omit the straightforward proofs.

(a) If $a_1, \ldots, a_k \in R$ and $I = \langle a_1, \ldots, a_k \rangle$ as an R-ideal, then $IS = \langle a_1, \ldots, a_k \rangle$ as an S-ideal.

(b) For any two ideals I and J of R, we have $(IJ)S = (IS)(JS)$.

Lemma 16.2. Let K be a number field, and let I be a nonzero ideal of $\mathbb{Z}_K$. There is an extension of number fields L/K in which $I\mathbb{Z}_L$ is principal.

Proof. Let m be the order of $[I]$ in $\mathrm{Cl}(\mathbb{Z}_K)$. Then I^m is principal, say $I^m = \langle \alpha \rangle$. Let $L = K(\beta)$, where β is a complex mth root of α. Then β is an algebraic integer (see Theorem 2.10), and we have the following equation of $\mathbb{Z}_L$-ideals:

$$(I\mathbb{Z}_L)^m = I^m\mathbb{Z}_L = \alpha\mathbb{Z}_L = \beta^m\mathbb{Z}_L = (\beta\mathbb{Z}_L)^m.$$

By unique factorization, $I\mathbb{Z}_L = \beta\mathbb{Z}_L$. □

Lemma 16.3 ("Up-down" lemma)**.** Let K be a number field, and let I be a nonzero ideal of $\mathbb{Z}_K$. Let R be a subring of $\bar{\mathbb{Z}}$ containing $\mathbb{Z}_K$. Then

$$IR \cap \mathbb{Z}_K = I.$$

Proof. It is clear that $I \subseteq IR \cap \mathbb{Z}_K$, and so we concentrate on the reverse containment. Suppose first that I is principal, say $I = \alpha\mathbb{Z}_K$. Then $IR = \alpha R$. If $\beta \in IR \cap \mathbb{Z}_K$, then $\beta/\alpha \in R \cap K = \mathbb{Z}_K$. Thus, $\beta \in \alpha\mathbb{Z}_K = I$.

In the general case, pick an $m \in \mathbb{Z}^+$ with I^m principal. From the special case just treated,

$$I^m R \cap \mathbb{Z}_K = I^m. \tag{16.1}$$

Now let γ be any element of $IR \cap \mathbb{Z}_K$; we argue that $\gamma \in I$. We have that $\gamma^m \in (IR)^m = I^m R$ and $\gamma^m \in \mathbb{Z}_K$. By (16.1), $\gamma^m \in I^m$. That is, $I^m \mid \langle\gamma\rangle^m$, as ideals of $\mathbb{Z}_K$. Comparing exponents in the prime ideal factorizations shows that $I \mid \langle\gamma\rangle$, and hence $\gamma \in I$. □

Proof of Theorem 16.1. If $I = \{0\}$, we may take $\beta = 0$. So we will assume that $I \neq \{0\}$. Using Lemma 16.2, pass to an extension L/K in which $I\mathbb{Z}_L$ is principal, say $I\mathbb{Z}_L = \beta\mathbb{Z}_L$. Then

$$I\bar{\mathbb{Z}} = (I\mathbb{Z}_L)\bar{\mathbb{Z}} = (\beta\mathbb{Z}_L)\bar{\mathbb{Z}} = \beta\bar{\mathbb{Z}}.$$

Now intersect with $\mathbb{Z}_K$ and use the "up-down" lemma (with $R = \bar{\mathbb{Z}}$):

$$I = (I\bar{\mathbb{Z}}) \cap \mathbb{Z}_K = \beta\bar{\mathbb{Z}} \cap \mathbb{Z}_K.$$ □

Example 16.4. Consider the ideal $\langle 2, 1 + \sqrt{-5}\rangle$ of $\mathbb{Z}[\sqrt{-5}]$. We know from earlier (see the examples of Chapter 7) that $I^2 = 2\mathbb{Z}[\sqrt{-5}]$. Now the proof of Theorem 16.1 shows that I is the set of elements of $\mathbb{Z}[\sqrt{-5}]$ that are algebraic integer multiples of $\sqrt{2}$.

Zou Bisou Bézout

Our work in the last section has an interesting implication for the arithmetic of $\bar{\mathbb{Z}}$. To get the discussion started, we observe that $\bar{\mathbb{Z}}$ has many (infinitely many!) nonunits. Indeed, the only integers invertible in $\bar{\mathbb{Z}}$ are ± 1. Yet the nonunits of $\bar{\mathbb{Z}}$ do not factor into irreducibles, for *there are no irreducibles for them to factor into.* Indeed, no $\alpha \in \bar{\mathbb{Z}}$ is irreducible, since we can always write

$$\alpha = \sqrt{\alpha} \cdot \sqrt{\alpha},$$

and the right-hand factors are nonunits whenever α is.[1]

This pathological behavior is of course incompatible with $\bar{\mathbb{Z}}$ being a principal ideal domain. Nevertheless, there is a sense in which $\bar{\mathbb{Z}}$ is very close to a PID.

Theorem 16.5. Finitely generated ideals of $\bar{\mathbb{Z}}$ are principal.

An integral domain where every finitely generated ideal is principal is called a **Bézout domain**.

[1] Some authors use the playful term **antimatter domain** for an integral domain with no irreducibles. Here "antimatter" = "no atoms".

Proof. Clearly it suffices to consider nonzero ideals I of $\bar{\mathbb{Z}}$. Suppose I is generated by the finitely many elements $\alpha_1, \ldots, \alpha_k$. Let $K = \mathbb{Q}(\alpha_1, \ldots, \alpha_k)$. Since each α_i is algebraic over $\mathbb{Q}$ and there are only finitely many of them, K is a *finite* extension of $\mathbb{Q}$, i.e., a number field. Let I be the ideal of $\mathbb{Z}_K$ generated by the α_i. Using Lemma 16.2, pass to an extension L of K in which $I\mathbb{Z}_L$ is principal, say $I\mathbb{Z}_L = \beta\mathbb{Z}_L$. Then as ideals of $\mathbb{Z}_L$,

$$\langle \alpha_1, \ldots, \alpha_k \rangle = \langle \beta \rangle.$$

Extending both sides to $\bar{\mathbb{Z}}$ shows that $I\bar{\mathbb{Z}} = \beta\bar{\mathbb{Z}}$. □

Kronecker's generalization of Gauss's lemma

Theorem 16.5 can be used to establish a lovely theorem of Kronecker. To set the stage, we recall the statement of Gauss's classical **content lemma**. For any $f(x) \in \mathbb{Z}[x]$, the **content of** $f(x)$, denoted $c(f)$ here, is defined as the greatest common divisor of the coefficients of f. Gauss's content lemma asserts that for any pair of polynomials $f(x), g(x) \in \mathbb{Z}[x]$,

$$c(fg) = c(f)c(g).$$

For a general integral domain R, and an arbitrary $f(x) \in R[x]$, we define the **content ideal of** $f(x)$, denoted $C(f)$, as the ideal of R generated by the coefficients of f. We call an integral domain R **Gaussian** if $C(fg) = C(f)C(g)$ for all nonzero[2] $f(x), g(x) \in R[x]$. Gauss's content lemma says that $\mathbb{Z}$ is a Gaussian domain.

Theorem 16.6 (Kronecker)**.** $\bar{\mathbb{Z}}$ is Gaussian, as is $\mathbb{Z}_K$ for every number field K.

Proof that $\bar{\mathbb{Z}}$ is Gaussian. We give a proof valid in any Bézout domain R. Let $f(x), g(x)$ be nonzero polynomials in $R[x]$. Since R is a Bézout domain, $C(f)$ and $C(g)$ are principal; say $C(f) = \langle \alpha \rangle$ and $C(g) = \langle \beta \rangle$. Put $F = \alpha^{-1}f$ and $G = \beta^{-1}g$. Then $F(x), G(x) \in R[x]$, both $C(F) = \langle 1 \rangle$ and $C(G) = \langle 1 \rangle$, and $fg = \alpha\beta FG$. From the last equality,

$$C(fg) = \alpha\beta \cdot C(FG) = C(f)C(g) \cdot C(FG).$$

[2]Of course, $C(fg) = C(f)C(g)$ holds automatically if f or g is zero; our restricted definition allows us to avoid repeatedly mentioning these trivial cases.

So the desired result will follow if we show that $C(FG)$ is the unit ideal. We proceed by contradiction. Recall that a nonunit ideal (in any ring) is always contained in a maximal ideal. (This is a routine application of Zorn's lemma.) So if $C(FG)$ is not the unit ideal, then there is a maximal ideal M of R with $C(FG) \subseteq M$; hence, (the image of) FG vanishes in $(R/M)[x]$. But R/M is a field. Thus, either every coefficient of F lies in M or every coefficient of G lies in M. But then $C(F) \subseteq M$ or $C(G) \subseteq M$, contradicting that $C(F) = C(G) = \langle 1 \rangle$. □

Proof that $\mathbb{Z}_K$ is Gaussian. Let $f(x)$ and $g(x)$ be nonzero polynomials with $\mathbb{Z}_K$-coefficients. If $C(f)$ and $C(g)$ are their contents over $\mathbb{Z}_K$, then the contents of f and g viewed as polynomials with $\bar{\mathbb{Z}}$-coefficients are $C(f)\bar{\mathbb{Z}}$ and $C(g)\bar{\mathbb{Z}}$. Similarly, if $C(fg)$ is the $\mathbb{Z}_K$-content of fg, then the $\bar{\mathbb{Z}}$-content of fg is $C(fg)\bar{\mathbb{Z}}$. Since $\bar{\mathbb{Z}}$ is Gaussian, it follows that

$$(C(f)\bar{\mathbb{Z}}) \cdot (C(g)\bar{\mathbb{Z}}) = C(fg)\bar{\mathbb{Z}}.$$

But $(C(f)\bar{\mathbb{Z}}) \cdot (C(g)\bar{\mathbb{Z}}) = (C(f)C(g))\bar{\mathbb{Z}}$, and so

$$C(f)C(g)\bar{\mathbb{Z}} = C(fg)\bar{\mathbb{Z}}.$$

Intersecting with $\mathbb{Z}_K$ and applying the "up-down" lemma gives us that $C(f)C(g) = C(fg)$. □

The reader interested in the study of Gaussian domains will find a list of 22 equivalent conditions, compiled from Gilmer's *Multiplicative ideal theory*,[3] in a paper of Bazzoni and Glaz.[4]

Simultaneous principalization

Lemma 16.2 can be souped-up in the following way, where all ideals of $\mathbb{Z}_K$ are considered at once.

Theorem 16.7. Let K be a number field. There is a finite extension of number fields L/K having the property that $I\mathbb{Z}_L$ is principal for *every* ideal I of $\mathbb{Z}_K$.

---

[3] Gilmer, R. *Multiplicative ideal theory.* Corrected reprint of the 1972 edition. Queen's Papers in Pure and Applied Mathematics, **90**. Queen's University, Kingston, ON, 1992.

[4] Bazzoni, S.; Glaz, S. *Prüfer rings.* Multiplicative ideal theory in commutative algebra, 55–72, Springer, New York, 2006.

Proof. Let $h = h_K$ and let $I_1, \ldots, I_h$ be a full set of representatives of $\mathrm{Cl}(\mathbb{Z}_K)$. By Lagrange's theorem, each I_j^h is a principal ideal of $\mathbb{Z}_K$, say $I_j^h = \alpha_j \mathbb{Z}_K$ for $j = 1, 2, \ldots, h$. Let $\beta_1, \ldots, \beta_h$ be complex hth roots of $\alpha_1, \ldots, \alpha_h$, and let $L = K(\beta_1, \ldots, \beta_h)$. Then (reasoning as in the proof of Lemma 16.2) $I_j \mathbb{Z}_L = \beta_j \mathbb{Z}_L$, for each $i = 1, 2, \ldots, h$.

Now let I be any nonzero ideal of $\mathbb{Z}_L$. Then $[I] = [I_j]$ for some $j = 1, 2, \ldots, h$. Hence, $I = \lambda I_j$ for some $\lambda \in K$. Write $\lambda = \delta/m$, where $\delta \in \mathbb{Z}_K$ and $m \in \mathbb{Z}^+$. Then $mI = \delta I_j$, and

$$mI\mathbb{Z}_L = \delta I_j \mathbb{Z}_L = (\delta \beta_j)\mathbb{Z}_L.$$

So $m \mid \delta\beta_j$ in $\mathbb{Z}_L$, and $I\mathbb{Z}_L = \frac{\delta\beta_j}{m}\mathbb{Z}_L$. □

Example 16.8. As the class number of $\mathbb{Q}(\sqrt{-5})$ is 2, the nonprincipal ideal $\langle 2, 1 + \sqrt{-5}\rangle$ represents the only nontrivial ideal class. Since $\langle 2, 1 + \sqrt{-5}\rangle^2 = \langle 2\rangle$, the proof of Theorem 16.7 shows that all ideals of $\mathbb{Z}[\sqrt{-5}]$ become principal in $\mathbb{Q}(\sqrt{-5}, \sqrt{2})$.

A remarkable consequence of Theorem 16.7 is that unique factorization on the elemental level can always be restored by passing to a finite extension, in the following somewhat restricted sense: For any number field K, there is a finite extension L/K such that the map $I \mapsto I\mathbb{Z}_L$ embeds the unique factorization monoid $\mathrm{Id}(\mathbb{Z}_K)$ as a submonoid of $\mathrm{Prin}(\mathbb{Z}_L)$.

The above construction is not altogether satisfactory. While it arranges for the ideals of $\mathbb{Z}_K$ to become principal in $\mathbb{Z}_L$, a typical ideal of $\mathbb{Z}_L$ does not arise by extension from $\mathbb{Z}_K$. If we dare to dream, we might hope that starting from any number field K, we can always find *some* finite extension L/K where *all* ideals of $\mathbb{Z}_L$ are principal, not merely those coming from $\mathbb{Z}_K$. For instance, it can be shown that when $K = \mathbb{Q}(\sqrt{-5})$, this holds with $L = K(i)$.[5]

A beautiful dream, but we do not live in such a world.

Theorem 16.9 (Golod and Shafarevich[6])**.** For every n, there are infinitely many number fields K of degree n which do not admit any finite

[5]It does *not* hold with $L = K(\sqrt{2})$; the class number of $\mathbb{Q}(\sqrt{-5}, \sqrt{2})$ can be shown to be 2.

[6]Golod, E. S.; Shafarevich, I. R. *On the class field tower.* (Russian) Izv. Akad. Nauk SSSR Ser. Mat. **28** (1964), 261–272.

extension of class number 1. For example,

$$\mathbb{Q}(\sqrt{-3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 17 \cdot 19})$$

is one such field (for $n = 2$).

Much remains mysterious. At present, there is no known algorithm to decide, given an arbitrary number field K, whether K is a subfield of some class number 1 number field.

Exercises

(1) Let $L = \mathbb{Q}(\sqrt{-5}, \sqrt{2})$. Let I, J, I', J' be the ideals of $\mathbb{Z}[\sqrt{-5}]$ listed in (4.8). Give an explicit generator in $\mathbb{Z}_L$ for each of the four ideals $I\mathbb{Z}_L$, $J\mathbb{Z}_L$, $I'\mathbb{Z}_L$, and $J'\mathbb{Z}_L$.

(2) Since every finitely generated ideal of $\bar{\mathbb{Z}}$ is principal but $\bar{\mathbb{Z}}$ is not a PID, there must be an ideal of $\bar{\mathbb{Z}}$ that is not finitely generated. Exhibit a specific example.

(3) (The ideal norm as the content of a polynomial) Let K be an arbitrary number field, and let $\alpha_0, \ldots, \alpha_{m-1} \in \mathbb{Z}_K$, not all zero. Show that

$$\prod_{\sigma : K \hookrightarrow \mathbb{C}} (\sigma(\alpha_0) + \sigma(\alpha_1)x + \cdots + \sigma(\alpha_m)x^m) \in \mathbb{Z}[x],$$

and that the content of this product is the norm of the ideal $\langle \alpha_0, \ldots, \alpha_m \rangle \subseteq \mathbb{Z}_K$.

(4) (Dedekind's "Prague theorem") Let $F, G \in \bar{\mathbb{Z}}[x]$. Let $\gamma \in \bar{\mathbb{Z}}$, and suppose that γ divides every coefficient of FG. Show that γ divides the product of any coefficient of F with any coefficient of G.

(5) According to the fundamental theorem of algebra, every nonconstant polynomial over $\mathbb{C}$ factors as a product of linear polynomials over $\mathbb{C}$. Show that the same statement holds with $\mathbb{C}$ replaced everywhere by $\bar{\mathbb{Z}}$.

(6) (continuation) Show that if we start with a primitive polynomial over $\bar{\mathbb{Z}}$ — meaning one whose coefficients generate the unit ideal — then its decomposition into linear factors is unique, up to ordering and multiplication by units of $\bar{\mathbb{Z}}$.[7]

(7) Show that $\bar{\mathbb{Z}}$ has no nontrivial finite quotients: If I is a proper ideal of $\bar{\mathbb{Z}}$, then $\bar{\mathbb{Z}}/I$ is infinite.

(8) Prove that if K is a number field, then every nonzero prime ideal of $\mathbb{Z}_K$ is maximal. Then prove the same assertion with $\mathbb{Z}_K$ replaced by $\bar{\mathbb{Z}}$.

[7] Exercises 5 and 6 are based on: Magidin, A.; McKinnon, D. *Gauss's lemma for number fields.* Amer. Math. Monthly **112** (2005), no. 5, 385–416.

(9) (Stiemke[8]) Let $K_1, K_2, K_3, \ldots$ be a sequence of number fields with each $K_i \subseteq K_{i+1}$ and $\bigcup_{i=1}^{\infty} K_i = \bar{\mathbb{Q}}$. (The existence of such a sequence was shown in Exercise 2.9.)

(a) Let P be a nonzero prime ideal of $\bar{\mathbb{Z}}$, and define $P_1, P_2, P_3, \ldots$ by setting $P_i = P \cap \mathbb{Z}_{K_i}$. Prove that each P_i is a nonzero prime ideal of $\mathbb{Z}_{K_i}$ and that $P_i \subseteq P_{i+1}$ for all i.

(b) Now suppose we are given $P_1, P_2, P_3, \ldots$ with each P_i a nonzero prime ideal of $\mathbb{Z}_{K_i}$ and each $P_i \subseteq P_{i+1}$. Show that there is a unique prime ideal P of $\bar{\mathbb{Z}}$ with $P \cap \mathbb{Z}_{K_i} = P_i$ for all i. *Hint:* Try $P = \bigcup_{i=1}^{\infty} P_i$.

(c) (hard; probably you will want to return to this later) Using (b), prove that $\bar{\mathbb{Z}}$ has uncountably many distinct prime ideals.

[8] Stiemke, E. *Über unendliche algebraische Zahlkörper.* Math. Z. **25** (1926), 9–39.

17

Prime decomposition in general number rings

As easy as e-f-g

Let K be any number field. Extending our earlier definition for quadratic fields, we say that the nonzero prime ideal P of $\mathbb{Z}_K$ **lies above** the rational prime p (or that p **lies below** P) when $P \mid \langle p \rangle$. Just as in Chapter 7, every nonzero prime ideal P of $\mathbb{Z}_K$ lies above a unique rational prime p, determined by the relation

$$P \cap \mathbb{Z} = p\mathbb{Z}.$$

The proof is the same, word for word, as that of Proposition 7.2.

So if we wish to understand the prime ideals of $\mathbb{Z}_K$, we are compelled to investigate how rational primes decompose in K (more precisely, how the principal ideals $\langle p \rangle$ factor as products of prime ideals of $\mathbb{Z}_K$). Our next result describes a fundamental relationship (eq. (17.2)) between the prime ideals P that show up in the factorization of a given prime number p.

Theorem 17.1 (e-f-g theorem)**.** Let K be a degree n number field. Let p be a rational prime, and write

$$\langle p \rangle = P_1^{e_1} \cdots P_g^{e_g}, \tag{17.1}$$

where the P_i are distinct prime ideals of $\mathbb{Z}_K$ and the e_i are positive integers. Then for each $1 \le i \le g$,

$$N(P_i) = p^{f_i}$$

for some positive integer f_i, and

$$\sum_{i=1}^{g} e_i f_i = n. \tag{17.2}$$

In the situation of Theorem 17.1, f_i is called the **residual degree** (or simply the **degree**) of P_i over p, and e_i is called the **ramification index**. In place of f_i and e_i we will often write $f(P_i/p)$ and $e(P_i/p)$, respectively.

Proof. The homomorphism from $\mathbb{Z}$ to $\mathbb{Z}_K/P_i$ sending a to a mod P_i has kernel $P_i \cap \mathbb{Z} = p\mathbb{Z}$; hence, it induces an identification of $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ with a subring of $\mathbb{Z}_K/P_i$. This identification provides us a way to view $\mathbb{Z}_K/P_i$ as an $\mathbb{F}_p$-vector space. Clearly,

$$\mathrm{N}(P_i) = \#\mathbb{Z}_K/P_i = p^{f_i},$$

where

$$f_i = \dim_{\mathbb{F}_p} \mathbb{Z}_K/P_i.$$

Taking norms of both sides of (17.1) now shows that

$$p^n = \prod_{i=1}^{g} \mathrm{N}(P_i)^{e_i} = \prod_{i=1}^{g} p^{e_i f_i} = p^{\sum_{i=1}^{g} e_i f_i}.$$

Comparing exponents yields (17.2). □

The term "residual degree" for $f(P_i/p)$ is explained by the easy (but important) observation that the quotient $\mathbb{Z}_K/P_i$ is a field, the so-called **residue field of** P_i. To see that $\mathbb{Z}_K/P_i$ is a field, notice that P_i is a maximal ideal, since any nonunit ideal properly containing P_i would also properly divide P_i — an absurdity. Thus, what we are calling the residual degree is precisely the degree of the residue field viewed as an extension field of $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$.

If $p\mathbb{Z}_K$ is a prime ideal of $\mathbb{Z}_K$ (so that $g = 1, e_1 = 1$, and $f_1 = n$), we say that p is **inert**. If $g = n$ (which forces $e_i = f_i = 1$ for each $i = 1, 2, \ldots, n$), we say that p **splits completely**. If any exponent $e_i > 1$ (i.e., if $p\mathbb{Z}_K$ is divisible by the square of a prime ideal), we say that p **ramifies**.

The decomposition theorem of Dedekind–Kummer

The following important result of Dedekind[1] (extending earlier results of Kummer) allows one to explicitly write down the factorization of $p\mathbb{Z}_K$, in *almost* every case. It is a vast generalization of Theorem 7.3, which corresponds to $K = \mathbb{Q}(\sqrt{d})$ and $\alpha = \tau$.

Theorem 17.2 (Dedekind–Kummer)**.** Let K be a number field, and let α be an algebraic integer with $K = \mathbb{Q}(\alpha)$. Let p be a rational prime, and suppose that

$$p \nmid [\mathbb{Z}_K : \mathbb{Z}[\alpha]]. \tag{17.3}$$

Then the prime ideal factorization of $\langle p \rangle$ mirrors the factorization into irreducibles of $\min_\alpha(x)$ modulo p. More precisely, say

$$\min_\alpha(x) \equiv p_1(x)^{e_1} \cdots p_g(x)^{e_g} \pmod{p}, \tag{17.4}$$

where each $p_i(x) \in \mathbb{Z}[x]$ is monic, and where the mod p reductions of the $p_i(x)$ are the distinct monic irreducibles dividing $\min_\alpha(x)$ in $\mathbb{F}_p[x]$. For each $i = 1, 2, \ldots, g$, let

$$P_i = \langle p, p_i(\alpha) \rangle.$$

Then the P_i are distinct prime ideals of $\mathbb{Z}_K$, and

$$\langle p \rangle = P_1^{e_1} \cdots P_g^{e_g}.$$

Finally, $f_i = \deg p_i$ for all $1 \le i \le g$.

The catch here is the condition (17.3). If $\mathbb{Z}_K$ is monogenic, meaning that $\mathbb{Z}_K = \mathbb{Z}[\alpha]$ for some α, then (17.3) is satisfied for all primes p. That was the situation in Chapter 7. But, as already alluded to in Chapter 3, not all number rings are monogenic. So (17.3) in general requires throwing out a possibly nonempty (but finite!) set of primes. Which primes are bad depends, of course, on the choice of α used in the representation $K = \mathbb{Q}(\alpha)$. However, it is an unfortunate fact of life (demonstrated in the next section) that there can be primes where (17.3) fails for all choices of α; for these primes, Theorem 17.2 has nothing to say.

[1] Dedekind, R. *Über den Zusammenhang zwischen der Theorie der ideale und der Theorie der höheren Congruenzen.* Abh. d. Kgl. Ges. d. Wiss. zu Göttingen **23** (1878), 3–38.

The following sufficient condition for (17.3) is simpler to check than (17.3) itself, and so is often useful.

Proposition 17.3. Suppose that the number field K is written in the form $\mathbb{Q}(\alpha)$, where α is an algebraic integer. If $p^2 \nmid \Delta(\min_\alpha(x))$, then $p \nmid [\mathbb{Z}_K : \mathbb{Z}[\alpha]]$.

Proof of Proposition 17.3. Let $n = [K : \mathbb{Q}]$. According to equation (14.1),

$$\Delta(1, \alpha, \ldots, \alpha^{n-1}) = \Delta_K \cdot [\mathbb{Z}_K : \mathbb{Z}[\alpha]]^2.$$

But

$$\Delta(1, \alpha, \ldots, \alpha^{n-1}) = \Delta(\min_\alpha(x))$$

(Vandermonde). So if $p^2 \nmid \Delta(\min_\alpha(x))$, then $p \nmid [\mathbb{Z}_K : \mathbb{Z}[\alpha]]$. □

We will prove Theorem 17.2 at the end of this section. First, an illustration.

Example 17.4. Let $K = \mathbb{Q}(\alpha)$, where α is a root of the irreducible cubic $f(x) = x^3 + x^2 - 2x + 8$. By a direct computation,

$$\Delta(f(x)) = -4 \cdot 503.$$

So by Proposition 17.3, condition (17.3) is satisfied for all p except possibly $p = 2$. In fact, in Example 14.3, we showed that $1, \alpha, \frac{1}{2}(\alpha^2 + \alpha)$ is a $\mathbb{Z}$-basis for $\mathbb{Z}_K$. Hence, $[\mathbb{Z}_K : \mathbb{Z}[\alpha]] = 2$, and $p = 2$ is a genuine exception to (17.3).

Let us see what Theorem 17.2 says in a few examples. Modulo 3, the polynomial $f(x)$ is irreducible, and so 3 is inert in $\mathbb{Z}_K$. Modulo $p = 5$,

$$f(x) \equiv (x + 1)(x^2 - 2),$$

and so $\langle 5 \rangle = P_1 P_2$ where $f(P_1/p) = 1$ and $f(P_2/p) = 2$. Modulo $p = 59$,

$$f(x) \equiv (x + 11)(x + 20)(x + 29),$$

and so 59 splits completely. Finally, modulo 503,

$$f(x) \equiv (x + 299)(x + 354)^2; \tag{17.5}$$

thus, $\langle 503 \rangle = P_1 P_2^2$, where $f(P_1/p) = f(P_2/p) = 1$. Since P_2 appears to a power larger than the first, 503 ramifies.

It should not come as a shock that 503 ramifies. For any monic polynomial $f(x) \in \mathbb{Z}[x]$ and any rational prime p, the $\mathbb{F}_p$-discriminant of $f(x)$ is the mod p reduction of the $\mathbb{Q}$-discriminant. That is,

$$\Delta(f(x) \bmod p) = \Delta(f(x)) \bmod p. \tag{17.6}$$

This is clear from the Sylvester matrix method for calculating discriminants, but a direct proof is also possible (Exercise 11). Returning to our example,

$$\Delta(f(x)) \bmod p = -4 \cdot 503 \bmod p.$$

Hence, f has a multiple root in $\bar{\mathbb{F}}_{503}$, and so a repeated factor must appear in (17.5). Reasoning in the other direction, $\Delta(f(x) \bmod p)$ is nonvanishing for all $p \neq 2$ or 503, and so 503 is the only odd prime ramified in K. (Remember that we only know the conclusion of Theorem 17.2 for $p \neq 2$, and so we must remain agnostic for the time being about whether 2 ramifies.)

We now give the promised proof of Theorem 17.2. It is convenient to isolate exactly what the condition (17.3) is buying us.

Lemma 17.5. Let K be a number field written in the form $K = \mathbb{Q}(\alpha)$, where α is an algebraic integer. If (17.3) holds, then the ring inclusion $\iota\colon \mathbb{Z}[\alpha] \hookrightarrow \mathbb{Z}_K$ induces an isomorphism

$$\mathbb{Z}[\alpha]/p\mathbb{Z}[\alpha] \cong \mathbb{Z}_K/p\mathbb{Z}_K.$$

Proof. We start by showing that

$$p\mathbb{Z}_K \cap \mathbb{Z}[\alpha] = p\mathbb{Z}[\alpha]. \tag{17.7}$$

Clearly, $p\mathbb{Z}[\alpha] \subseteq p\mathbb{Z}_K \cap \mathbb{Z}[\alpha]$. To see the reverse inclusion, let $\beta \in p\mathbb{Z}_K \cap \mathbb{Z}[\alpha]$. Then $\beta/p \in \mathbb{Z}_K$, and the image of β/p in the quotient $\mathbb{Z}_K/\mathbb{Z}[\alpha]$ has order dividing p. Since p does not divide $[\mathbb{Z}_K : \mathbb{Z}[\alpha]]$, it must be that $\beta/p \in \mathbb{Z}[\alpha]$, i.e., $\beta \in p\mathbb{Z}[\alpha]$.

Now for the proof proper. Since $\iota(p\mathbb{Z}[\alpha]) \subseteq p\mathbb{Z}_K$, the map ι descends to a well-defined homomorphism

$$\bar{\iota}\colon \mathbb{Z}[\alpha]/p\mathbb{Z}[\alpha] \to \mathbb{Z}_K/p\mathbb{Z}_K.$$

Injectivity follows immediately from (17.7). Since both $\mathbb{Z}[\alpha]$ and $\mathbb{Z}_K$ are free abelian groups of rank n,

$$\#\mathbb{Z}[\alpha]/p\mathbb{Z}[\alpha] = p^n = \#\mathbb{Z}_K/p\mathbb{Z}_K \quad (\text{with } n = [K : \mathbb{Q}]).$$

Thus, $\bar{\imath}$ is an isomorphism. □

Proof of Theorem 17.2. For notational convenience, we will write $m(x)$ instead of $\min_\alpha(x)$. We first prove that each P_i is a prime ideal with $f(P_i/p) = \deg p_i$. Observe that

$$\mathbb{Z}_K/P_i = \mathbb{Z}_K/\langle p, p_i(\alpha)\rangle \cong \frac{\mathbb{Z}_K/p\mathbb{Z}_K}{\langle p_i(\alpha) \bmod p\rangle}.$$

(This is the first of many applications of Lemma 7.6 sprinkled throughout this proof.) By Lemma 17.5,

$$\begin{aligned}\frac{\mathbb{Z}_K/p\mathbb{Z}_K}{\langle p_i(\alpha) \bmod p\rangle} &\cong \frac{\mathbb{Z}[\alpha]/p\mathbb{Z}[\alpha]}{\langle p_i(\alpha) \bmod p\rangle}\\ &\cong \mathbb{Z}[\alpha]/\langle p, p_i(\alpha)\rangle.\end{aligned}$$

The proof of Lemma 7.5 shows that

$$\mathbb{Z}[\alpha] \cong \mathbb{Z}[x]/\langle m(x)\rangle.$$

Hence,

$$\begin{aligned}\mathbb{Z}[\alpha]/\langle p, p_i(\alpha)\rangle &\cong \frac{\mathbb{Z}[x]/\langle m(x)\rangle}{\langle p \bmod m(x), p_i(x) \bmod m(x)\rangle}\\ &\cong \frac{\mathbb{Z}[x]/p\mathbb{Z}[x]}{\langle p_i(x) \bmod p, m(x) \bmod p\rangle}\\ &\cong \frac{(\mathbb{Z}/p\mathbb{Z})[x]}{\langle p_i(x) \bmod p\rangle} \cong \mathbb{F}_{p^{\deg p_i}}.\end{aligned}$$

(In going from the second line to the third, we used that $p_i(x)$ divides $m(x)$, modulo p.) Since $\mathbb{Z}_K/P_i$ is a field, P_i is a prime ideal, and since $\#\mathbb{Z}_K/P_i = p^{\deg p_i}$, we indeed have $f(P_i/p) = \deg p_i$.

Next, we show that the prime ideals we just constructed are all distinct. Suppose that $1 \le i, j \le n$ and $i \ne j$. Since the mod p reductions of $p_i(x)$ and $p_j(x)$ are distinct monic irreducibles, there are $X(x), Y(x) \in \mathbb{Z}[x]$ with $p_i(x)X(x) + p_j(x)Y(x) \equiv 1 \pmod p$. Hence, for some $Q(x) \in \mathbb{Z}[x]$,

$$p_i(x)X(x) + p_j(x)Y(x) = pQ(x) + 1.$$

Substituting α for x and rearranging,

$$p_i(\alpha)X(\alpha) + p_j(\alpha)Y(\alpha) - pQ(\alpha) = 1.$$

But $P_i + P_j$ contains $p, p_i(\alpha)$, and $p_j(\alpha)$. Thus, $1 \in P_i + P_j$, and so $P_i + P_j = \langle 1\rangle$. Clearly, this implies that $P_i \ne P_j$.

It remains only to show that $\prod_{i=1}^{g} P_i^{e_i} = \langle p \rangle$. Notice that

$$P_i^{e_i} = \langle p, p_i(\alpha) \rangle^{e_i} \subseteq \langle p, p_i(\alpha)^{e_i} \rangle.$$

(The final containment may need some explanation; by the usual method for multiplying ideals in terms of generators, $\langle p, p_i(\alpha) \rangle^{e_i}$ is generated by 2^{e_i} elements, one of which is $p_i(\alpha)^{e_i}$, and all the rest of which are divisible by p.) Continuing,

$$\prod_{i=1}^{g} P_i^{e_i} \subseteq \prod_{i=1}^{g} \langle p, p_i(\alpha)^{e_i} \rangle \subseteq \langle p, \prod_{i=1}^{g} p_i(\alpha)^{e_i} \rangle.$$

From (17.4), $\prod_{i=1}^{g} p_i(\alpha)^{e_i} \equiv m(\alpha) \equiv 0 \pmod{p}$. Thus,

$$\prod_{i=1}^{g} P_i^{e_i} \subseteq \langle p \rangle.$$

Hence, $\langle p \rangle$ is a divisor of $\prod_{i=1}^{g} P_i^{e_i}$. To see that it is not a proper divisor, compare norms;

$$\mathrm{N}\Big(\prod_{i=1}^{g} P_i^{e_i} \Big) = p^{\sum_{i=1}^{g} e_i \deg p_i} = p^{\deg m(x)} = p^n,$$

which coincides with $\mathrm{N}(\langle p \rangle)$. Hence, $\langle p \rangle = \prod_{i=1}^{g} P_i^{e_i}$. □

Example 17.4, revisited

We continue our study of $K = \mathbb{Q}(\alpha)$, where α is a root of $f(x) = x^3 + x^2 - 2x + 8$. Recall that Theorem 17.2 was powerless to yield the factorization of $2\mathbb{Z}_K$. Since the hook fails, we bring out the crook. By ad hoc methods, we show the following.

Proposition 17.6. $2\mathbb{Z}_K = P_1 P_2 P_3$, where the P_i are distinct prime ideals of norm 2. In other words, 2 splits completely.

We see from Proposition 17.6 that the factorization of $2\mathbb{Z}_K$ does *not* mirror the factorization of f mod 2 ! So the "escape clause" (17.3) cannot be removed from Theorem 17.2.

Proof. For each integer t, let $I_t = \langle t - \alpha \rangle$. Writing $'$ and $''$ for the nontrivial complex embeddings of K,

$$\mathrm{N}(I_t) = |\mathrm{N}(t - \alpha)| = |(t - \alpha)(t - \alpha')(t - \alpha'')| = |f(t)|.$$

In particular,

$$\mathrm{N}(I_{-1}) = 10, \quad \mathrm{N}(I_{-2}) = 8, \quad \mathrm{N}(I_1) = 8, \quad \mathrm{N}(I_0) = 8.$$

As a consequence, all four of I_{-1}, I_{-2}, I_1, and I_0 have prime ideal factors lying above 2.

Notice that I_{-1} and I_{-2} are coprime, since any common divisor contains $(-1-\alpha)-(-2-\alpha) = 1$. By a similar argument, I_1 and I_0 are coprime. From either statement, we deduce that there are at least two distinct prime ideals lying over 2.

Suppose for a contradiction that there are *exactly* two, say P_1 and P_2. Then either

(a) $\langle 2\rangle = P_1P_2$ with $\mathrm{N}(P_1) = 2$ and $\mathrm{N}(P_2) = 4$, *or*

(b) $\langle 2\rangle = P_1P_2P_3$, where each $\mathrm{N}(P_i) = 2$ and $P_3 \in \{P_1, P_2\}$.

In case (a), the only ideals of norm 8 are P_1^3 and P_1P_2; both are divisible by P_1. Hence, P_1 is a common divisor of I_1 and I_0, which is impossible. So we must be in case (b). Since I_1 and I_0 are coprime, we find that after possibly interchanging P_1 and P_2,

$$I_1 = P_1^3, \quad I_0 = P_2^3.$$

Now we argue that I_{-2} and I_1 are coprime. Any common divisor contains $(1-\alpha)-(-2-\alpha) = 3$, so its norm divides $\mathrm{N}(\langle 3\rangle) = 27$. But its norm also divides $\mathrm{N}(I_{-2}) = 8$. Hence, the norm is 1 and the divisor is the unit ideal.

Since $\mathrm{N}(I_{-2}) = 2^3$, the only remaining possibility is that

$$I_{-2} = P_2^3 = I_0.$$

Hence,

$$2 = (-\alpha) - (-2-\alpha) \in P_2^3,$$

and so $P_2^3 \mid \langle 2\rangle$. This contradicts (b).

Thus, there are at least three distinct prime ideals above 2. By equation (17.2), there are exactly three, each of which has degree 1 and appears to the first power in the factorization of $\langle 2\rangle$. □

The above argument could have been shortened substantially if we knew in advance that the prime ideal divisors of $2\mathbb{Z}_K$ were distinct, i.e., that 2 is unramified. This may be deduced from a theorem of

Dedekind to be proved in Chapter 22, that the primes ramifying in a given number field K are exactly those dividing the discriminant of K. In our example, $\Delta_K = -503$ (a straightforward calculation using the known integral basis).

Proposition 17.6 has the following noteworthy consequence.

Proposition 17.7 (Dedekind's example of a non-monogenic number field)**.** Let $K = \mathbb{Q}(\alpha)$, where α is a root of $f(x) = x^3 + x^2 - 2x + 8$. There is no θ with $\mathbb{Z}_K = \mathbb{Z}[\theta]$. In fact, $[\mathbb{Z}_K : \mathbb{Z}[\theta]]$ is even for every $\theta \in \mathbb{Z}_K$ with $K = \mathbb{Q}(\theta)$.

Proof. Suppose for the sake of contradiction that there is a $\theta \in \mathbb{Z}_K$ with $K = \mathbb{Q}(\theta)$ and with $2 \nmid [\mathbb{Z}_K : \mathbb{Z}[\theta]]$. Then by Theorem 7.3, the prime ideal factorization of $2\mathbb{Z}_K$ mirrors the factorization of $\min_\theta(x)$ mod 2. Since 2 splits into three distinct prime ideal factors of degree 1, the polynomial $\min_\theta(x)$ decomposes as a product of three distinct linear polynomials modulo 2. But there are only 2 linear polynomials in $\mathbb{F}_2[x]$, namely x and $x + 1$! □

We conclude the chapter by highlighting some modern research connected with the study of monogenic number fields.

- If K is a degree n number field, then $\mathbb{Z}_K$ can always be generated (as a ring) by fewer than $\frac{\log(2n)}{\log 2}$ elements. This is a theorem of Pleasants, who also showed that when 2 splits completely, the minimal number of generators is the largest integer less than $\frac{\log(2n)}{\log 2}$.[2]
- M.-N. Gras[3] proved that if n is an integer coprime to 2 and 3, then there are only finitely many monogenic, degree n number fields which are Galois with abelian Galois group.
- In the opposite direction, it follows from work of Kedlaya[4] that for every $n \geq 2$, there are infinitely many monogenic number fields of degree n with Galois group S_n.

[2]Pleasants, P. A. B. *The number of generators of the integers of a number field.* Mathematika **21** (1974), 160–167.

[3]Gras, M.-N. *Non monogénéité de l'anneau des entiers de certaines extensions abéliennes de* $\mathbb{Q}$. Number theory (Besançon), 1983–1984, Exp. No. 5, 25 pp., Publ. Math. Fac. Sci. Besançon, Univ. Franche-Comté, Besançon, 1984.

[4]Kedlaya, K. S. *A construction of polynomials with squarefree discriminants.* Proc. Amer. Math. Soc. **140** (2012), no. 9, 3025–3033.

- Bhargava, Shankar, and Wang[5] recently proved the following striking probabilistic result, earlier conjectured by H. Lenstra[6] : Fix $n \geq 2$. Choose a degree n monic irreducible polynomial $f(x) \in \mathbb{Z}[x]$ at random, and let θ be a complex root of $f(x)$. Then the probability that $\mathbb{Z}[\theta]$ is the full ring of integers of $\mathbb{Q}(\theta)$ is $\frac{6}{\pi^2}$.[7]
- By contrast, it is conjectured that for each fixed $n \geq 3$, a randomly chosen degree n number field is monogenic with probability 0.[8] Bhargava has proved this for $n = 3, 4$, and 5.[9]

  At first blush, this prediction might appear to contradict the theorem of Bhargava–Shankar–Wang just mentioned. But sampling random number fields is a different ball game from sampling random polynomials, and there is no (obvious) reason why both statements cannot be true.

Exercises

Recommended problems

(1) Let $K = \mathbb{Q}(\sqrt[3]{2})$. Let p be a prime, $p \neq 2, 3$.
   (a) When $p \equiv 2 \pmod 3$, show that $p\mathbb{Z}_K = P_1P_2$, where $f(P_1/p) = 1$ and $f(P_2/p) = 2$.
   (b) When $p \equiv 1 \pmod 3$, show that p is either split completely or inert, according to whether 2 is or is not a cube mod p, respectively.
   (c) Determine the factorizations of $2\mathbb{Z}_K$ and $3\mathbb{Z}_K$. You may take as known that $\mathbb{Z}_K = \mathbb{Z}[\sqrt[3]{2}]$.

(2) Let $K = \mathbb{Q}(\sqrt{7}, \sqrt{10})$.

---

[5] Bhargava, M.; Shankar, A.; Wang, X. *Squarefree values of polynomial discriminants I.* `arXiv:1611.09806 [math.NT]`

[6] See: Ash, A.; Brakenhoff, J.; Zarrabi, T. *Equality of polynomial and field discriminants.* Experiment. Math. **16** (2007), no. 3, 367–374.

[7] Here "at random" means that we sample uniformly from monic irreducibles of bounded height, and let the height bound tend to infinity.

[8] In this case, "at random" means that we sample uniformly from number fields of bounded discriminant, and let the discriminant bound tend to infinity.

[9] See the references on p. 235. For a more precise version of the conjecture, see §6 of the paper of Bhargava, Shankar, and Wang (ibid.).

(a) Show that every $\alpha \in \mathbb{Z}_K$ is congruent, modulo 3, to an element of the form $a + b\sqrt{7} + c\sqrt{10} + d\sqrt{70}$, where $a, b, c, d \in \mathbb{Z}$.

Hint: One approach is to compute an integral basis for K. But that is overkill. For "just enough kill", work out what can be deduced from knowing that $\mathrm{Tr}(\alpha\beta) \in \mathbb{Z}$ for $\beta = 1, \sqrt{7}, \sqrt{10}, \sqrt{70}$.

(b) Show that each $\alpha \in \mathbb{Z}_K$ satisfies $\alpha^3 \equiv \alpha \pmod 3$.

(c) Use (b) to show that 3 is unramified in K. *Hint:* Show that $\mathbb{Z}_K/3\mathbb{Z}_K$ has no nonzero nilpotent elements. Then apply Exercise 15.1.

(d) Use (b) to prove that every prime ideal above 3 has residual degree 1. *Hint:* If P is a prime ideal above 3, then $\mathbb{Z}_K/P$ is a field in which every element is its own cube.

(e) Deduce that 3 splits completely in $\mathbb{Z}_K$.

(f) Conclude that K is not monogenic.

(3) Let $K = \mathbb{Q}(\zeta_8)$, where $\zeta_8 = e^{2\pi i/8}$. Show that no rational prime remains inert in $\mathbb{Z}_K$. *Hint:* x^4+1 factors as a difference of squares modulo every odd prime p.

(4) Prove that in any given number field, only finitely many rational primes ramify.

(5) Prove Dedekind's discriminant theorem, that p ramifies in $K \iff p \mid \Delta_K$, in the special case when K is a monogenic number field.

(6) Let K be a number field with $K/\mathbb{Q}$ Galois. Let p be a rational prime, and suppose that $p\mathbb{Z}_K$ is divisible by some degree 1 prime ideal P. Show that

$$p\mathbb{Z}_K = \prod_{\sigma \in \mathrm{Gal}(K/\mathbb{Q})} \sigma(P),$$

and deduce that every prime ideal above p has degree 1. *Hint:* Apply Theorem 6.7.

(7) (Prime decomposition in Galois number fields) Let K be a degree n number field with $K/\mathbb{Q}$ Galois. Generalize the result of Exercise 6 by proving that if p is any rational prime and $P_1, \ldots, P_g$ are the distinct prime ideals of $\mathbb{Z}_K$ above p, then $f(P_1/p) = \cdots = f(P_g/p)$. Show also that $e(P_1/p) = \cdots = e(P_g/p)$. With f and e denoting these common values, show that $efg = n$.

(8) Let L/K be an extension of number fields. Let p be a rational prime.
   (a) Let P be any prime ideal of $\mathbb{Z}_K$ lying above p. Show that $P\mathbb{Z}_L$ is not the unit ideal of $\mathbb{Z}_L$. *Hint:* Use the "up-down" lemma (Lemma 16.3).
   (b) Part (a), along with the fundamental theorem of ideal theory applied to $\mathbb{Z}_L$, implies that there is a prime ideal Q of $\mathbb{Z}_L$ dividing $P\mathbb{Z}_L$. Show that Q lies above p and that $e(Q/p)$ is a multiple of $e(P/p)$. *Hint:* Write down the factorization of $p\mathbb{Z}_K$ and then extend to $\mathbb{Z}_L$.
   (c) With P, Q having the meanings from (a) and (b), show that $\mathbb{Z}_K/P$ embeds into $\mathbb{Z}_L/Q$ via the map $\theta \bmod P \mapsto \theta \bmod Q$. Deduce that $f(Q/p)$ is a multiple of $f(P/p)$.
   (d) Conclude that if p is unramified in L, then p is unramified in K, and that if p splits completely in L, then p splits completely in K.

(9) Suppose $K = \mathbb{Q}(\alpha)$, where α is the root of a monic, degree n polynomial in $\mathbb{Z}[x]$ that satisfies Eisenstein's criterion with respect to the prime p. Show that $p\mathbb{Z}_K = P^n$ for some prime ideal P of $\mathbb{Z}_K$.
   Hint: Combine Proposition 14.5 and the theorem of Dedekind–Kummer.

(10) Let $K = \mathbb{Q}(\zeta_p)$, where p is an odd prime.
   (a) Show that $p\mathbb{Z}_K = P^{p-1}$ for some prime ideal P, and that p is the only prime that ramifies in K.
   (b) Let q be a prime distinct from p, and let ℓ be the order of q modulo p. Show that
   $$\alpha^{q^\ell} \equiv \alpha \pmod{q}$$
   for every $\alpha \in \mathbb{Z}_K$. (It will help to remember that $\mathbb{Z}_K = \mathbb{Z}[\zeta_p]$, by Theorem 14.6.)
   (c) Let Q be a prime ideal above q. Use (b) to show $f(Q/q) \mid \ell$.
   (d) With Q as in (c), show that $j = \ell$ is the smallest positive integer with $\zeta_p^{q^j} \equiv \zeta_p \pmod{Q}$. Deduce that $f(Q/q) = \ell$.
   (e) Conclude that $q\mathbb{Z}_K$ factors as a product of $\frac{p-1}{\ell}$ distinct prime ideals, each of norm q^ℓ.

Extra! extra!

(11) (Discriminants under reduction mod p) Let $f(x) \in \mathbb{Z}[x]$ be a nonconstant, monic polynomial. Let K be a number field containing all of the roots of $f(x)$, and let P be a prime ideal of $\mathbb{Z}_K$ lying above p. Deduce (17.6) by writing out the definition of $\Delta(f(x))$ and reducing mod P.

(12) (a) Use Theorem 14.7 to show that $1, \sqrt[3]{175}, \sqrt[3]{245}$ form an integral basis for $K = \mathbb{Q}(\sqrt[3]{175})$.
(b) Using (a), prove that $\Delta_K = -3^3 \cdot 5^2 \cdot 7^2$.
(c) Let $a, b, c \in \mathbb{Z}$ with $b, c \neq 0$, and let $\alpha = a + b\sqrt[3]{175} + c\sqrt[3]{245}$. Show that

$$\Delta(1, \alpha, \alpha^2) = -3^3 \cdot 5^2 \cdot 7^2 \cdot (5b^3 - 7c^3)^2.$$

(d) Deduce from (b, c) that $[\mathbb{Z}_K : \mathbb{Z}[\alpha]] = |5b^3 - 7c^3|$.
(e) Prove that K is not monogenic.

(13) Let K be any number field. Show that $p\mathbb{Z}_K$ is divisible by a degree 1 prime ideal for infinitely many rational primes p. *Hint:* Say K is obtained by adjoining to $\mathbb{Q}$ the root of a monic, irreducible polynomial $f(x) \in \mathbb{Z}[x]$. By Dedekind–Kummer, it suffices to prove that there are infinitely many primes p for which $f(x)$ has a root mod p. Now look back at Exercise 7.6.

(14) (continuation) Let $g(x)$ be a nonconstant, monic polynomial with integer coefficients. By applying Exercise 13 to the splitting field of $g(x)$ over $\mathbb{Q}$, prove that $g(x)$ splits over $\mathbb{Z}/p\mathbb{Z}$ for infinitely many primes p.

(15) (continuation) Strengthen the result of Exercise 13 by proving that in any number field, infinitely many rational primes split completely.

(16) (converse of Exercise 9) Let K be a degree n number field. Let p be a rational prime, and suppose that $p\mathbb{Z}_K = P^n$ for some prime ideal P of $\mathbb{Z}_K$. (In this situation, we say that p is **totally ramified**.) Fix an element

$$\alpha \in P \setminus P^2.$$

In this exercise, you will show that $K = \mathbb{Q}(\alpha)$ and that the minimal polynomial of α is Eisenstein with respect to p.
(a) Let L be the Galois closure of $K/\mathbb{Q}$, and let Q be any prime ideal of $\mathbb{Z}_L$ lying above p. Show that $\alpha \in Q$. *Hint:* Show that

$Q \cap \mathbb{Z}_K$ is a prime ideal of $\mathbb{Z}_K$ containing p, and deduce that $Q \cap \mathbb{Z}_K = P$.

(b) In (a), you showed that α is contained in every prime ideal of $\mathbb{Z}_L$ lying above p. Deduce that the same holds for $\sigma(\alpha)$, for each $\sigma \in \mathrm{Gal}(L/\mathbb{Q})$.

(c) Using (b), prove that the field polynomial $\phi_\alpha(x)$, computed with respect to K (not L), has multiples of p for all of its non-leading coefficients.

(d) Show that p^2 does not divide $\phi_\alpha(0)$. With (c), this proves that $\phi_\alpha(x)$ is p-Eisenstein.

(e) Conclude that $\min_\alpha(x) = \phi_\alpha(x)$ and that $K = \mathbb{Q}(\alpha)$.

(17) (converse to Exercise 14.7) Let p be a prime number. With $K = \mathbb{Q}(\sqrt[p]{2})$, suppose that $\mathbb{Z}_K = \mathbb{Z}[\sqrt[p]{2}]$.

(a) Show that $\langle p \rangle = P^p$ where $P = \langle p, \sqrt[p]{2} - 2 \rangle$.

(b) Use (a) to prove that $\sqrt[p]{2} - 2 \notin P^2$. Deduce that p^2 does not divide $\mathrm{N}(\sqrt[p]{2} - 2)$.

(c) Conclude that $2^p \not\equiv 2 \pmod{p^2}$.

(18) Let p be an odd prime. Prove that if a is an integer that is not a pth power, then p ramifies in $\mathbb{Q}(\sqrt[p]{a})$.

(19) Let K be a degree n number field. Let α be an algebraic integer that is also a primitive element for $K/\mathbb{Q}$ (that is, $K = \mathbb{Q}(\alpha)$). Let p be a rational prime. Suppose that

$$\min_\alpha(x) \equiv p_1(x)^{e_1} \cdots p_g(x)^{e_g} \pmod{p},$$

where $p_1(x), \ldots, p_g(x)$ are monic polynomials in $\mathbb{Z}[x]$ whose mod p reductions are the distinct monic irreducible factors of $\min_\alpha(x)$ mod p. Put

$$Q(x) = \frac{p_1(x)^{e_1} \cdots p_g(x)^{e_g} - \min_\alpha(x)}{p}.$$

Clearly, $Q(x) \in \mathbb{Z}[x]$. In this exercise and the next, we prove **Dedekind's criterion**:[10]

$$p \mid [\mathbb{Z}_K : \mathbb{Z}[\alpha]] \iff \begin{array}{c} p_j(x) \text{ divides } Q(x), \text{ mod } p, \\ \text{for some } j \text{ with } e_j \geq 2. \end{array}$$

[10] Dedekind, op. cit.

We first treat the backward direction ($\Leftarrow$). Thus, we suppose $j \in \{1, 2, \ldots, g\}$ is such that $p_j(x)$ divides $Q(x)$, modulo p, and that $e_j \geq 2$.

(a) Show that there are $a(x), b(x) \in \mathbb{Z}[x]$ with

$$p_1(x)^{e_1} \cdots p_g(x)^{e_g} = \min_\alpha(x) + p \cdot a(x) p_j(x) + p^2 \cdot b(x). \tag{17.8}$$

(b) Set

$$\beta = \frac{p_j(\alpha)^{e_j - 1} \prod_{\substack{1 \leq i \leq g \\ i \neq j}} p_i(\alpha)^{e_i}}{p}.$$

Show that β is the root of a monic, quadratic polynomial with coefficients from $\mathbb{Z}[\alpha]$. Conclude that $\beta \in \mathbb{Z}_K$. *Hint for the first part:* Plug α into (17.8), then multiply both sides by

$$\frac{1}{p^2} p_j(\alpha)^{e_j - 2} \prod_{\substack{1 \leq i \leq g \\ i \neq j}} p_i(\alpha)^{e_i}.$$

(c) Show that β represents an order p element of the quotient group $\mathbb{Z}_K / \mathbb{Z}[\alpha]$. Hence, p divides $[\mathbb{Z}_K : \mathbb{Z}[\alpha]]$.

(20) (continuation) Now we consider the forward direction ($\Rightarrow$). Suppose that $p \mid [\mathbb{Z}_K : \mathbb{Z}[\alpha]]$.

(a) Show that there is an $A_0(x) \in \mathbb{Z}[x] \setminus p\mathbb{Z}[x]$ with $\deg A_0(x) < n$ and $A_0(\alpha) \in p\mathbb{Z}_K$.

(b) Write the mod p gcd of $A_0(x)$ and $\min_\alpha(x)$ in the form $\prod_{i=1}^g p_i(x)^{t_i} \bmod p$, where the t_i are nonnegative integers with $0 \leq t_i \leq e_i$ for each i. (We keep notation as in (17.8).) Define $A(x), B(x) \in \mathbb{Z}[x]$ by

$$A(x) = \prod_{i=1}^g p_i(x)^{t_i}, \quad B(x) = \prod_{i=1}^g p_i(x)^{e_i - t_i}.$$

Show that $A(\alpha) \in p\mathbb{Z}_K$.

(c) Deduce that the field polynomial $\phi_{A(\alpha)}$ of $A(\alpha)$ has the form

$$x^n + p a_{n-1} x^{n-1} + p^2 a_{n-2} x^{n-2} + \cdots + p^n a_0$$

for rational integers $a_0, \ldots, a_{n-1}$.

(d) Use (c) to show that $\min_\alpha(x)$ divides $A(x)^n$, mod p. Conclude that $A(x)$ is divisible, mod p, by each $p_i(x)$ (for $1 \leq i \leq g$).

(e) Show that $A(\alpha)B(\alpha) = pQ(\alpha)$.

(f) Prove that

$$Q(\alpha)^n + a_{n-1}B(\alpha)Q(\alpha)^{n-1} + a_{n-2}B(\alpha)^2Q(\alpha)^{n-2} + \cdots + a_0B(\alpha)^n = 0.$$

Hint: $B(\alpha)^n\phi_{A(\alpha)}(A(\alpha)) = 0$.

(g) Prove that $B(x)$ divides $Q(x)^n$, mod p.

(h) Show that $t_j < e_j$ for some $j \in \{1, 2, \ldots, g\}$.

(i) For any j as in (h), prove that $p_j(x)$ divides $Q(x)$, mod p, and that $e_j \geq 2$.

(21) (Uchida's reformulation of Dedekind's criterion[11]) Let K be a number field of degree n, and let α be an algebraic integer that is also a primitive element for $K/\mathbb{Q}$. Let p be a rational prime. Show that p divides $[\mathbb{Z}_K : \mathbb{Z}[\alpha]] \iff \min_\alpha(x) \in M^2$ for some maximal ideal M of $\mathbb{Z}[x]$ containing p.

[11] Uchida, K. *When is $\mathbb{Z}[\alpha]$ the ring of the integers?* Osaka J. Math. **14** (1977), no. 1, 155–157.

18

Dirichlet's units theorem, I

> It is said that, after many years of futile efforts around this difficult problem [the structure of the unit group], Dirichlet grasped the solution in Rome in the Sistine Chapel while listening to the Easter music. To what extent this fact speaks to the conjectured affinity between mathematics and music, I dare not discuss. – H. Minkowski[1]

Throughout this chapter, K denotes a degree n number field with r_1 real embeddings, labeled $\sigma_1, \dots, \sigma_{r_1}$, and r_2 pairs of nonreal embeddings, $\sigma_{r_1+1}, \overline{\sigma_{r_1+1}}, \dots, \sigma_{r_1+r_2}, \overline{\sigma_{r_1+r_2}}$. Thus, $r_1 + 2r_2 = n$. We let μ_K denote the set of roots of unity contained in K, i.e.,

$$\mu_K = \{\zeta \in K : \zeta^n = 1 \text{ for some } n \in \mathbb{Z}^+\}.$$

Clearly, μ_K is a subgroup of $K^\times$; in fact, since roots of unity are algebraic integers, μ_K is a subgroup of $U(\mathbb{Z}_K)$.

The structure of $U(\mathbb{Z}_K)$ as an abelian group was first determined in general by Dirichlet, who published the following theorem in 1846.[2]

Theorem 18.1 (Dirichlet's units theorem)**.** For every number field K, there are elements $\epsilon_1, \dots, \epsilon_{r_1+r_2-1} \in U(\mathbb{Z}_K)$ of infinite order for which

$$U(\mathbb{Z}_K) = \mu_K \times \prod_{i=1}^{r_1+r_2-1} \langle \epsilon_i \rangle. \tag{18.1}$$

[1] Minkowski, H. *Peter Gustav Lejeune Dirichlet und seine Bedeutung für die heutige Mathematik.* Jahresber. Dtsch. Math.-Ver. **14** (1905), 149–163.

[2] Dirichlet, P. G. L. *Zur Theorie der complexen Einheiten.* Ber. Verhandl. Kgl. Preuß. Akad. Wiss. (1846), 103–107.

Moreover, $\#\mu_K < \infty$.

As a simple illustration of Theorem 18.1, we determine all K for which $U(\mathbb{Z}_K)$ is finite. From (18.1), $\#U(\mathbb{Z}_K) < \infty$ precisely when $r_1 + r_2 = 1$, so that either $r_1 = 1$ and $r_2 = 0$ or $r_1 = 0$ and $r_2 = 1$. In the first case, K has degree $n = 1 + 2 \cdot 0_2 = 1$, and so $K = \mathbb{Q}$. In the second case, K has degree $n = 0 + 2 \cdot 1 = 2$ and admits no real embeddings, so that K is an imaginary quadratic field.

In this chapter, we take the first steps towards the proof of Theorem 18.1. Our main result is the existence of the decomposition (18.1), but with an unspecified nonnegative integer $g \le r_1 + r_2 - 1$ in place of the precise value $r_1 + r_2 - 1$. We will return in Chapter 20 to the problem of proving that $g = r_1 + r_2 - 1$.

The plan of attack

When K is real quadratic, Theorem 18.1 was shown in Chapter 8. The proof in the general case follows the same broad strokes. Define a homomorphism $\operatorname{Log}\colon K^\times \to \mathbb{R}^{r_1+r_2}$ by[3]

$$\operatorname{Log}\alpha = (\log|\sigma_1(\alpha)|, \dots, \log|\sigma_{r_1}(\alpha)|, \\ 2\log|\sigma_{r_1+1}(\alpha)|, \dots, 2\log|\sigma_{r_1+r_2}(\alpha)|).$$

(It might seem at first that the embeddings $\overline{\sigma_{r_1+1}}, \dots, \overline{\sigma_{r_1+r_2}}$ are not involved in the definition of the Log map; however, since $|\sigma(\alpha)| = |\overline{\sigma}(\alpha)|$, they are there in spirit.) There are then four main steps:

(1) Prove that $\ker(\operatorname{Log}|_{U(\mathbb{Z}_K)}) = \mu_K$, and that $\#\mu_K < \infty$.

(2) Show that $\operatorname{Log} U(\mathbb{Z}_K)$ is a **discrete** subgroup of $\mathbb{R}^{r_1+r_2}$, in a sense to be defined shortly. (This step is analogous to what we proved in Lemma 8.3.)

(3) Characterize the discrete subgroups of $\mathbb{R}^{r_1+r_2}$. These turn out to be precisely the lattices in $\mathbb{R}^{r_1+r_2}$, as defined in Chapter 12. (This step generalizes Lemma 8.4.)

(4) By combining (1)–(3), prove the units theorem (Theorem 18.1) with $r_1 + r_2 - 1$ replaced by the rank of the lattice $\operatorname{Log} U(\mathbb{Z}_K)$.

[3] The reason for the strange-seeming factors of 2 will emerge at the end of the chapter. *Hint:* What is the sum of the components of $\operatorname{Log}\alpha$?

(5) Show that $\operatorname{rk} \operatorname{Log} U(\mathbb{Z}_K) = r_1 + r_2 - 1$.

Steps 1–4 are carried out over the course of the next few sections. Step 5 is by far the most difficult. In this chapter, we content ourselves with proving only that $\operatorname{rk} \operatorname{Log} U(\mathbb{Z}_K) \leq r_1 + r_2 - 1$; one can think of this compromise as a sort of "Step $4\frac{1}{2}$".

Step 1: Analysis of the kernel

Lemma 18.2. Let M be a positive real number. Let $\alpha \in \mathbb{Z}_K$. If $|\sigma(\alpha)| \leq M$ for all embeddings σ of K into $\mathbb{C}$, then α is a root of a polynomial from the (finite!) set

$$\mathcal{P}_{n,M} := \{x^n + a_{n-1}x^{n-1} + \cdots + a_0 : \text{each } a_i \in \mathbb{Z}, \text{ and } |a_i| \leq \binom{n}{i} M^{n-i}\}.$$

Proof. Certainly α is a root of its field polynomial

$$\phi_\alpha(x) = \prod_\sigma (x - \sigma(\alpha)).$$

We will show that $\phi_\alpha(x) \in \mathcal{P}_{n,M}$. Write

$$\phi_\alpha(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0.$$

Up to sign, a_i is the sum of all $\binom{n}{i}$ products of the $\sigma(\alpha)$ taken $n - i$ at a time. Since each $|\sigma(\alpha)| \leq M$, each $|a_i| \leq \binom{n}{i} M^{n-i}$. That all the a_i are rational integers is a consequence of the fact that $\alpha \in \mathbb{Z}_K$ (Proposition 13.3). □

Proposition 18.3. $\ker(\operatorname{Log}|_{U(\mathbb{Z}_K)})$ is finite.

Proof. Suppose that $\alpha \in U(\mathbb{Z}_K)$ and $\operatorname{Log} \alpha = \mathbf{0}$. Then $\alpha \in \mathbb{Z}_K$ and $|\sigma(\alpha)| = 1$ for every embedding $\sigma : K \hookrightarrow \mathbb{C}$. By Lemma 18.2, α is a root of one of the finitely many polynomials belonging to $\mathcal{P}_{n,1}$. □

Proposition 18.4. $\ker(\operatorname{Log}|_{U(\mathbb{Z}_K)}) = \mu_K$.

Proof. That μ_K is contained in the kernel is easy: Complex embeddings map roots of unity to roots of unity, and every complex root of unity lies on the unit circle. So if $\zeta \in \mu(K)$, then $\log|\sigma(\zeta)| = 0$ for all σ, and so $\operatorname{Log} \zeta = \mathbf{0}$. To prove the reverse containment, take any ζ

in the kernel. Since the kernel is finite (Proposition 18.3), ζ has finite multiplicative order. Hence, ζ is a root of unity. □

Step 2: Discreteness of $\operatorname{Log} U(\mathbb{Z}_K)$

Definition 18.5. Let $d \in \mathbb{Z}^+$, and let Λ be a subgroup of $\mathbb{R}^d$. We say that Λ is **discrete** if for every $R > 0$,

$$\#\left(\mathcal{B}(R) \cap \Lambda\right) < \infty,$$

where $\mathcal{B}(R)$ is the closed ball of radius R about $\mathbf{0}$.

Proposition 18.6. The subgroup $\operatorname{Log} U(\mathbb{Z}_K)$ of $\mathbb{R}^{r_1+r_2}$ is discrete.

Proof. If $\alpha \in U(\mathbb{Z}_K)$ and $\operatorname{Log}\alpha \in \mathcal{B}(R)$, then $|\sigma(\alpha)| \le e^R$ for all embeddings $\sigma\colon K \hookrightarrow \mathbb{C}$. By Lemma 18.2, α is a root of one of the finitely many polynomials in $\mathcal{P}_{n,e^R}$. □

Step 3: Characterization of discrete subgroups

Theorem 18.7. Let Λ be a discrete subgroup of $\mathbb{R}^d$. Then Λ is a lattice of rank g, where $0 \le g \le d$.

Since the proof is on the long side, it may be helpful to summarize the main steps. It suffices (as explained below) to treat the case when the $\mathbb{R}$-span of Λ is all of $\mathbb{R}^d$. We look at all full rank lattices in $\mathbb{R}^d$ that are contained within Λ and pick one with minimal covolume; the discreteness hypothesis is needed here to show that a minimum exists. We then prove that Λ coincides with this minimizing sublattice.

Proof of Theorem 18.7. Among all collections of linearly independent vectors contained in Λ, choose one — say $\mathbf{v}_1, \dots, \mathbf{v}_g$ — with g as large as possible. To start off, we will assume that $g = d$. At the end of the proof, we describe how to reduce the general case to this one.

Let $\Lambda' = \bigoplus_{i=1}^{d} \mathbb{Z}\mathbf{v}_i$. Clearly, $\Lambda' \subseteq \Lambda$. We now argue that there is some positive integer f with

$$\Lambda \subseteq \frac{1}{f}\Lambda'. \tag{18.2}$$

To prove this, it is enough to show that the quotient group Λ/Λ' is finite, for then we may take $f = \#\Lambda/\Lambda'$. Let $\mathbf{v}$ be an arbitrary element

of Λ. Since $\mathbf{v}_1, \dots, \mathbf{v}_d$ are linearly independent over $\mathbb{R}$, they form a basis for $\mathbb{R}^d$, and so $\mathbf{v} = \sum_{i=1}^d c_i \mathbf{v}_i$, for some $c_i \in \mathbb{R}$. Subtracting off $\sum_{i=1}^d \lfloor c_i \rfloor \mathbf{v}_i \in \Lambda'$ yields an element of Λ that is congruent to $\mathbf{v}$ modulo Λ' and that belongs to

$$\mathcal{F}(\mathbf{v}_1, \dots, \mathbf{v}_d) := \{t_1\mathbf{v}_1 + \cdots + t_d\mathbf{v}_d : \text{each } 0 \le t_i < 1\}.$$

But $\mathcal{F}(\mathbf{v}_1, \dots, \mathbf{v}_d)$ is bounded and Λ is discrete. Consequently,

$$\#\Lambda/\Lambda' \le \#\mathcal{F}(\mathbf{v}_1, \dots, \mathbf{v}_d) \cap \Lambda < \infty,$$

as desired.

To continue, we mimic the argument of Theorem 13.6 (proving the existence of integral bases). For each d-tuple of vectors $\mathbf{w}_1, \dots, \mathbf{w}_d \in \mathbb{R}^d$, put[4]

$$D(\mathbf{w}_1, \dots, \mathbf{w}_d) = |\det[\mathbf{w}_1, \dots, \mathbf{w}_d]|.$$

When $\mathbf{w}_1, \dots, \mathbf{w}_d$ are $\mathbb{R}$-linearly independent, this is > 0 (and is the covolume of the lattice generated by the $\mathbf{w}_i$). We can certainly find $\mathbf{w}_1, \dots, \mathbf{w}_d \in \Lambda$ with

$$D(\mathbf{w}_1, \dots, \mathbf{w}_d) > 0;$$

for example, this holds when each $\mathbf{w}_i = \mathbf{v}_i$. We choose $\mathbf{w}_1, \dots, \mathbf{w}_d \in \Lambda$ with $D(\mathbf{w}_1, \dots, \mathbf{w}_d)$ nonzero and minimal; the following argument shows that this is possible. For each tuple $\mathbf{w}_1, \dots, \mathbf{w}_d \in \Lambda$, (18.2) implies that there is a $d \times d$ integer matrix A with $[\mathbf{w}_1, \dots, \mathbf{w}_d] = [\frac{1}{f}\mathbf{v}_1, \dots, \frac{1}{f}\mathbf{v}_d]A$. Then

$$D(\mathbf{w}_1, \dots, \mathbf{w}_d) = D\big(\frac{1}{f}\mathbf{v}_1, \dots, \frac{1}{f}\mathbf{v}_d\big) \cdot |\det(A)|.$$

But $\det(A) \in \mathbb{Z}$. So $D(\mathbf{w}_1, \dots, \mathbf{w}_d)$ is an integer multiple of the (fixed) quantity $D\big(\frac{1}{f}\mathbf{v}_1, \dots, \frac{1}{f}\mathbf{v}_d\big)$. Hence, the existence of a minimizing tuple $\mathbf{w}_1, \dots, \mathbf{w}_d$ follows from the familiar well-ordering principle.

The $\mathbf{w}_i$ in our minimizing tuple are linearly independent, since $D(\mathbf{w}_1, \dots, \mathbf{w}_d) \neq 0$. So to prove that Λ is a lattice (of rank d), it suffices to show that Λ is the $\mathbb{Z}$-span of the $\mathbf{w}_i$. Since the $\mathbf{w}_i$ are a basis for $\mathbb{R}^d$, each $\mathbf{w} \in \Lambda$ can be written in the form $\mathbf{w} = c_1\mathbf{w}_1 + \cdots + c_d\mathbf{w}_d$, where the c_i are real numbers. We will show that each $c_i \in \mathbb{Z}$. Suppose

[4]When we write $[\mathbf{w}_1, \dots, \mathbf{w}_d]$, we mean the matrix whose column vectors are the $\mathbf{w}_i$.

otherwise. For notational simplicity, assume $c_1 \notin \mathbb{Z}$ (the other cases are similar). Put $\mathbf{w}' = \mathbf{w} - \sum_{i=1}^{d} \lfloor c_i \rfloor \mathbf{w}_i$. Then $\mathbf{w}' \in \Lambda$,

$$[\mathbf{w}', \mathbf{w}_2, \ldots, \mathbf{w}_d] = [\mathbf{w}_1, \ldots, \mathbf{w}_d] \cdot \begin{bmatrix} \{c_1\} & 0 & 0 & \ldots & 0 \\ \{c_2\} & 1 & 0 & \ldots & 0 \\ \{c_3\} & 0 & 1 & \ldots & 0 \\ \vdots & 0 & 0 & \ddots & 0 \\ \{c_n\} & 0 & 0 & \ldots & 1 \end{bmatrix},$$

and thus

$$D(\mathbf{w}', \mathbf{w}_2, \ldots, \mathbf{w}_d) = \{c_1\} \cdot D(\mathbf{w}_1, \mathbf{w}_2, \ldots, \mathbf{w}_d).$$

Hence,

$$0 < D(\mathbf{w}', \mathbf{w}_2, \ldots, \mathbf{w}_d) < D(\mathbf{w}_1, \mathbf{w}_2, \ldots, \mathbf{w}_d),$$

contradicting the choice of the $\mathbf{w}_i$.

It remains only to justify our opening assumption that $g = d$. If $g < d$, we transport the entire problem to a lower dimensional setting. The maximality of g implies that $\Lambda \subseteq V$, where V is the $\mathbb{R}$-span of $\mathbf{v}_1, \ldots, \mathbf{v}_g$. Let $T\colon V \to \mathbb{R}^g$ be a linear isomorphism. It is straightforward to show that T preserves discrete subgroups (Exercise 1). Now restart the argument with Λ replaced by $T\Lambda$ and d replaced by g. □

As a byproduct of Theorem 18.7, we obtain a quick proof of the following purely algebraic result.

Corollary 18.8. Let M be a free $\mathbb{Z}$-module of rank d. Then every submodule H of M is free of rank g, where $0 \le g \le d$.

Proof. We can assume that $M = \mathbb{Z}^d$. Since $\mathbb{Z}^d$ is a discrete subgroup of $\mathbb{R}^d$, our subgroup H of $\mathbb{Z}^d$ is as well. Hence, H is a lattice of rank g, where $0 \le g \le d$. But a lattice of rank g is also a free $\mathbb{Z}$-module of rank g. □

Step 4: Some assembly required

Theorem 18.9 ("Weak" units theorem)**.** Let g be the rank of the lattice $\operatorname{Log} U(\mathbb{Z}_K)$. There are $\epsilon_1, \ldots, \epsilon_g \in U(\mathbb{Z}_K)$ of infinite order with

$$U(\mathbb{Z}_K) = \mu_K \times \prod_{i=1}^{g} \langle \epsilon_i \rangle.$$

(We leave the finiteness of μ_K, established in Step 1, out of the statement this time.)

Proof. From Steps 2 and 3, we know that $\operatorname{Log} U(\mathbb{Z}_K)$ is a lattice. Choose $\epsilon_1, \ldots, \epsilon_g \in U(\mathbb{Z}_K)$ with $\operatorname{Log}\epsilon_1, \ldots, \operatorname{Log}\epsilon_g$ forming a $\mathbb{Z}$-basis for $\operatorname{Log} U(\mathbb{Z}_K)$. Then for any $\epsilon \in U(\mathbb{Z}_K)$, we can find integers $n_1, \ldots, n_g$ with

$$\operatorname{Log}\epsilon = n_1 \operatorname{Log}\epsilon_1 + \cdots + n_g \operatorname{Log}\epsilon_g.$$

Thus,

$$\operatorname{Log}\left(\epsilon \prod_{i=1}^{g} \epsilon_i^{-n_i}\right) = 0.$$

Hence, by our determination of $\ker(\operatorname{Log}|_{U(\mathbb{Z}_K)})$ (Proposition 18.4),

$$\epsilon = \zeta \cdot \prod_{i=1}^{g} \epsilon_i^{n_i} \tag{18.3}$$

for some $\zeta \in \mu_K$. So every $\epsilon \in U(\mathbb{Z}_K)$ has a representation as a product of an element of μ_K with integer powers of ϵ_i, for $i = 1, 2, \ldots, g$. The theorem follows if it is shown that this representation is unique; this is routine, using the $\mathbb{Z}$-independence of the $\operatorname{Log}\epsilon_i$, and is left to the reader as Exercise 2. □

Step $4\frac{1}{2}$: An upper bound on the rank

Proposition 18.10. $\operatorname{rk}\operatorname{Log} U(\mathbb{Z}_K) \leq r_1 + r_2 - 1$.

The argument relies on the following very familiar lemma. (Why prove it again? If you look back, you will see that the lemma's previous avatars only concerned quadratic fields. Nevertheless, there are no surprises in the proof.)

Lemma 18.11 (déjà vu all over again)**.** Let $\alpha \in \mathbb{Z}_K$. Then $\alpha \in U(\mathbb{Z}_K) \iff \mathrm{N}\alpha = \pm 1$.

Proof. According to Lemma 13.8, $\alpha \mid \mathrm{N}\alpha$ in $\mathbb{Z}_K$. So if $\mathrm{N}\alpha = \pm 1$, then $\alpha \in U(\mathbb{Z}_K)$. Conversely, if $\alpha \in U(\mathbb{Z}_K)$, then $\alpha \mid 1$ in $\mathbb{Z}_K$. Since the norm is multiplicative, $\mathrm{N}\alpha \mid \mathrm{N}(1) = 1$, in $\mathbb{Z}$, and so $\mathrm{N}\alpha = \pm 1$. □

Proof of Proposition 18.10. Recall that the rank of a lattice Λ is the dimension of the real vector space $\Lambda \otimes \mathbb{R}$. Thus, it suffices to show that $\operatorname{Log} U(\mathbb{Z}_K)$ is contained in an $r_1 + r_2 - 1$ dimensional subspace of $\mathbb{R}^{r_1+r_2}$. Let $\mathbf{w} = (1, 1, \ldots, 1) \in \mathbb{R}^{r_1+r_2}$. For any $\alpha \in U(\mathbb{Z}_K)$,

$$\begin{aligned}\mathbf{w} \cdot \operatorname{Log} \alpha &= \sum_{i=1}^{r_1} \operatorname{Log} |\sigma_i(\alpha)| + \sum_{i=1}^{r_1+r_2} 2 \operatorname{Log} |\sigma_i(\alpha)| \\ &= \sum_{\sigma\colon K \hookrightarrow \mathbb{C}} \operatorname{Log} |\sigma(\alpha)| = \operatorname{Log} |\mathrm{N}\alpha| = \operatorname{Log} 1 = 0.\end{aligned}$$

Thus, $\operatorname{Log} U(\mathbb{Z}_K)$ is contained in the orthogonal complement of $\mathbf{w}$, which indeed has real dimension $r_1 + r_2 - 1$. □

Exercises

(1) Let V be a g-dimensional real subspace of $\mathbb{R}^d$, and let $T\colon V \to \mathbb{R}^g$ be a linear isomorphism. Show that if Λ is a discrete subgroup of $\mathbb{R}^d$ contained in V, then $T\Lambda$ is a discrete subgroup of $\mathbb{R}^g$. *Hint:* Check that T^{-1} takes bounded sets in $\mathbb{R}^g$ to bounded sets in $\mathbb{R}^d$.

(2) Verify that the decomposition of ϵ in (18.3) is unique. In other words, given ϵ, both the element ζ of μ_K and the integer tuple $(n_1, \ldots, n_g)$ are uniquely determined.

(3) Show that if K admits a real embedding, then $\mu_K = \{\pm 1\}$. Deduce that $\mu_K = \{\pm 1\}$ whenever K has odd degree.

(4) Show that μ_K is cyclic for every number field K. *Hint:* The set of $\theta \in \mathbb{R}$ with $e^{i\theta} \in \mu_K$ is a discrete subgroup.

(5) (Kronecker[5]) Show that if α is an algebraic integer all of whose conjugates are contained in the real interval $[-2, 2]$, then $\alpha =$

[5]Kronecker, L. *Zwei Sätze über Gleichungen mit ganzzahligen Coefficienten.* J. reine angew. Math. **53** (1857), 173–175.

$2\cos(2\pi r)$ for some rational number r. *Hint:* Write $\alpha = \beta + 1/\beta$, and show that all the conjugates of β have absolute value 1.

Remark: It is a theorem of Schur and Pólya[6] that if I is any real interval of length < 4, then there are only finitely many algebraic integers α all of whose conjugates belong to I. On the other hand, Robinson[7] proved that there are infinitely many such α whenever I has length > 4. The problem is open when the length of I is exactly 4, except for intervals whose endpoints are rational integers (when we can easily reduce to the case $[-2, 2]$ treated above!).

(6) Let K be a degree n number field.
   (a) Show that if μ_K contains an element of order m, then $\phi(m) \mid n$. *Hint:* Look at Exercise 14.8.
   (b) Use (a) to give another proof that $\#\mu_K < \infty$.

(7) Let K be a degree 4 number field.
   (a) Show that every element of μ_K has order 1, 2, 3, 4, 5, 6, 8, 10, or 12.
   (b) Show that if μ_K contains an element of order $m = 5$, 8, 10, or 12, then $K = \mathbb{Q}(e^{2\pi i/m})$.
   (c) Show that for each of $m = 1, 2, 3, 4, 6$, there are infinitely many nonisomorphic degree 4 number fields K for which μ_K contains an element of order m.

(8) Let $K = \mathbb{Q}(\sqrt{-1}, \sqrt{-5})$.
   (a) Show that $\mu_K = \{\pm 1, \pm i\}$.
   (b) Prove that $\operatorname{rk} \operatorname{Log} U(\mathbb{Z}_K) = 1$.
   (c) By Theorem 18.9, we can write $U(\mathbb{Z}_K) = \mu_K \times \langle \epsilon \rangle$ for some unit ϵ. Show that there are integers m and n, as well as a $\zeta \in \mu_K$, with
$$\epsilon\bar{\epsilon} = \left(\frac{1+\sqrt{5}}{2}\right)^m \quad \text{and} \quad \frac{1+\sqrt{5}}{2} = \zeta\epsilon^n.$$
   (d) Show that $2 = mn$.
   (e) Show that if $m = \pm 1$, then $N\epsilon = -1$.
   (f) Prove that in fact every nonzero element of K has positive norm. Conclude that $U(\mathbb{Z}_K) = \mu_K \times \langle \frac{1+\sqrt{5}}{2} \rangle$.

---

[6] Schur, I. *Über die Verteilung der Wurzeln bei gewissen algebraischen Gleichungen mit ganzzahligen Koeffizienten.* Math. Z. **1** (1918), 377–402.

[7] Robinson, R. M. *Intervals containing infinitely many sets of conjugate algebraic integers*, in: Studies in Mathematical Analysis, 305–315, Stanford, 1962.

(9) (Nakahata[8], Daileda[9]) Given a number field K, we let $U_{\mathbb{R}}(\mathbb{Z}_K)$ and $U_{S^1}(\mathbb{Z}_K)$ denote the subgroups of $U(\mathbb{Z}_K)$ consisting of the real units and those of absolute value 1, respectively. Clearly, $\mu_K \subseteq U_{S^1}(\mathbb{Z}_K)$.

For the remainder of the exercise, assume K is closed under complex conjugation.

(a) Show that $\operatorname{Log} U_{\mathbb{R}}(\mathbb{Z}_K) \cap \operatorname{Log} U_{S^1}(\mathbb{Z}_K) = \{\mathbf{0}\}$.

(b) Prove that $\epsilon^2 \in U_{\mathbb{R}}(\mathbb{Z}_K)U_{S^1}(\mathbb{Z}_K)$ for every unit ϵ of $\mathbb{Z}_K$. *Hint:* $\epsilon^2 = \epsilon\bar{\epsilon} \cdot \frac{\epsilon}{\bar{\epsilon}}$.

(c) Using (b), show that the internal direct sum $\operatorname{Log} U_{\mathbb{R}}(\mathbb{Z}_K) \oplus \operatorname{Log} U_{S^1}(\mathbb{Z}_K)$ has finite index in $\operatorname{Log} U(\mathbb{Z}_K)$.

(d) Deduce that $U_{S^1}(\mathbb{Z}_K)$ properly contains $\mu_K \iff U(\mathbb{Z}_F)$ has infinite index in $U(\mathbb{Z}_K)$, where $F = K \cap \mathbb{R}$.

(10) Suppose that K is a number field with $K/\mathbb{Q}$ Galois and with complex conjugation belonging to the center of $\operatorname{Gal}(K/\mathbb{Q})$. Show that every unit in $\mathbb{Z}_K$ of absolute value 1 is a root of unity. Thus, from Exercise 9, $[U(\mathbb{Z}_K) : U(\mathbb{Z}_F)] < \infty$, where $F = K \cap \mathbb{R}$.

[8] Nakahata, N. *On units of Galois extensions over* $\mathbb{Q}$. Proc. Fac. Sci. Tokai Univ. **15** (1980), 23–27.

[9] Daileda, R. C. *Algebraic integers on the unit circle.* J. Number Theory **118** (2006), 189–191.

19

A case study: Units in $\mathbb{Z}[\sqrt[3]{2}]$ and the Diophantine equation $X^3 - 2Y^3 = \pm 1$

We now pause the development of the general theory in order to determine the group of units of the ring of integers of $\mathbb{Q}(\sqrt[3]{2})$.[1] Feeding the answer into an argument of Nagell,[2] we then deduce a complete list of integer solutions to $X^3 - 2Y^3 = \pm 1$.

What should we be trying to prove?

What does the units theorem tell us when $K = \mathbb{Q}(\sqrt[3]{2})$? Since $x^3 - 2$ has one real root and two complex roots, there are $r_1 = 1$ real embeddings of K and $r_2 = 1$ pairs of complex conjugate embeddings. So $r_1 + r_2 - 1 = 1$. Because $K \subseteq \mathbb{R}$, the only roots of unity in K are ± 1. From the weak units theorem (Theorem 18.9) and the upper bound on the rank (Proposition 18.10), either

$$U(\mathbb{Z}_K) = \{\pm 1\}, \tag{19.1}$$

or

$$U(\mathbb{Z}_K) = \{\pm 1\} \times \langle \epsilon_0 \rangle \tag{19.2}$$

for some unit ϵ_0 of infinite order.

[1] Expressions of the form $\sqrt[3]{D}$ in this chapter always refer to the real cube root of D.

[2] Nagell, T. *Solution complète de quelques équations cubiques à deux indeterminées.* J. Math. Pures Appl. **4** (1925), 209–270. Our presentation is inspired by Appendix A of: Lemmermeyer, F. *Quadratische Zahlkörper. Ein Schnupperkurs.* Südwestdeutscher Verlag für Hochschulschriften, Saarbrücken, 2011.

The full units theorem would predict (19.2), which tells us that we should be trying to rule out (19.1). This is easy to do; we simply have to write down a unit other than ± 1 ! Since

$$1 = (\sqrt[3]{2})^3 - 1 = (\sqrt[3]{2} - 1)(1 + \sqrt[3]{2} + \sqrt[3]{4}),$$

either of $\sqrt[3]{2} - 1$ or $1 + \sqrt[3]{2} + \sqrt[3]{4}$ does the trick.

Now that we know (19.2) is the truth, we can ask for the value of ϵ_0. To make the answer to this question well-defined, we impose the additional requirement that $\epsilon_0 > 1$; we call this ϵ_0 the **fundamental unit** of $\mathbb{Z}_K$.

Right under our nose

We have only written down one unit in $\mathbb{Z}_K$ that is larger than 1. As luck would have it, this turns out to be the fundamental unit.

Proposition 19.1. $\epsilon_0 = 1 + \sqrt[3]{2} + \sqrt[3]{4}$.

Not surprisingly, to prove Proposition 19.1 it is helpful to first determine the ring of integers of K.

Proposition 19.2. $\mathbb{Z}_K = \mathbb{Z}[\sqrt[3]{2}]$.

Proof. From (14.1), if p divides the index $[\mathbb{Z}_K : \mathbb{Z}[\sqrt[3]{2}]]$, then $p^2 \mid \Delta(1, \sqrt[3]{2}, \sqrt[3]{4})$. This divisibility condition forces $p = 2$ or 3. In fact, this is already forced by the weaker condition that $p \mid \Delta(x^3 - 2)$, as shown by the following simple argument:[3] If $p \mid \Delta(x^3 - 2)$, then $x^3 - 2$ has a multiple root over $\bar{\mathbb{F}}_p$, and so $x^3 - 2$ and $(x^3 - 2)' = 3x^2$ have a common root. If $p \neq 3$, then $x = 0$ is the only root of $3x^2$, and this is a root of $x^3 - 2$ only when $p = 2$.

Thus, it suffices to show that 2 and 3 do not divide $[\mathbb{Z}_K : \mathbb{Z}[\sqrt[3]{2}]]$. Since $x^3 - 2$ is Eisenstein with respect to 2, Proposition 14.5 implies that $2 \nmid [\mathbb{Z}_K : \mathbb{Z}[\sqrt[3]{2}]]$. Also,

$$\min_{\sqrt[3]{2}+1}(x) = (x-1)^3 - 2 = x^3 - 3x^2 + 3x - 3,$$

[3] The reader who prefers to "compute first and ask questions later" will have no trouble using the Sylvester matrix method to determine that $\Delta(x^3 - 2) = -2^2 \cdot 3^3$. Alternatively, Exercise 13.5 could be applied.

which is Eisenstein with respect to 3. So by Proposition 14.5 again,

$$3 \nmid [\mathbb{Z}_K : \mathbb{Z}[\sqrt[3]{2}+1]] = [\mathbb{Z}_K : \mathbb{Z}[\sqrt[3]{2}]].$$

(This argument is a special case of the one sketched in Exercise 14.6.) □

We now turn to Proposition 19.1. As preparation for its proof, we write down expressions for the trace and norm of arbitrary elements of K. Denote the nonreal embeddings of K by $'$ and $''$. Then $\sqrt[3]{2}' = \omega\sqrt[3]{2}$ and $\sqrt[3]{2}'' = \omega^2\sqrt[3]{2}$, where ω is a primitive third root of unity. Thus,

$$\begin{aligned}&\mathrm{Tr}(A + B\sqrt[3]{2} + C\sqrt[3]{4})\\ &\quad = 3A + B(1+\omega+\omega^2)\sqrt[3]{2} + C(1+\omega^2+\omega^4)\sqrt[3]{4} = 3A.\end{aligned}$$

(The last step uses that $\omega^3 = 1$ and $\omega^2 + \omega + 1 = 0$.) A less pleasant but equally straightforward calculation (see Exercise 1) shows that

$$\mathrm{N}(A + B\sqrt[3]{2} + C\sqrt[3]{4}) = A^3 + 2B^3 + 4C^3 - 6ABC.$$

Proof of Proposition 19.1. Clearly, the fundamental unit ϵ_0 is the smallest unit larger than 1. Set $\xi = 1 + \sqrt[3]{2} + \sqrt[3]{4}$, and suppose for a contradiction that there is an $\epsilon \in U(\mathbb{Z}_K)$ with

$$1 < \epsilon < \xi.$$

Since $1 = |\mathrm{N}\epsilon| = \epsilon|\epsilon'|^2$, we have

$$|\epsilon'| = |\epsilon''| = \frac{1}{\sqrt{\epsilon}}.$$

Now write

$$\epsilon = a + b\sqrt[3]{2} + c\sqrt[3]{4}$$

where (by Proposition 19.2) $a, b, c \in \mathbb{Z}$.

Recalling our formula for the trace, $3a = \mathrm{Tr}(\epsilon) = \epsilon + \epsilon' + \epsilon''$, and so by the triangle inequality,

$$3|a| \le \epsilon + |\epsilon'| + |\epsilon''| = \epsilon + \frac{2}{\sqrt{\epsilon}}.$$

A quick calculation with derivatives reveals that the function $x \mapsto x + 2x^{-1/2}$ is increasing for $x > 1$. Since $1 < \epsilon < \xi$, it follows that

$$\epsilon + \frac{2}{\sqrt{\epsilon}} < \xi + \frac{2}{\sqrt{\xi}} < 4.87.$$

Since $a \in \mathbb{Z}$, we conclude that $|a| \le 1$.

Similar methods can be used to bound b and c. We have $6b = \mathrm{Tr}(\sqrt[3]{4} \cdot \epsilon) = \sqrt[3]{4} \cdot \epsilon + \sqrt[3]{4}' \cdot \epsilon' + \sqrt[3]{4}'' \epsilon''$. Both nontrivial conjugates of $\sqrt[3]{4}$ have absolute value $\sqrt[3]{4}$, and so

$$6|b| \le \sqrt[3]{4}\,(\epsilon + |\epsilon'| + |\epsilon''|) \le \sqrt[3]{4}\left(\xi + \frac{2}{\sqrt{\xi}}\right) < 7.73.$$

Thus, $|b| \le 1$. Finally, $6c = \mathrm{Tr}(\sqrt[3]{2} \cdot \epsilon)$. Arguing as above,

$$6|c| \le \sqrt[3]{2}\left(\xi + \frac{2}{\sqrt{\xi}}\right) < 6.14.$$

Thus, $|c| \le 1$.

So $\epsilon = a + b\sqrt[3]{2} + c\sqrt[3]{4}$, where each of $a, b, c \in \{-1, 0, 1\}$. Explicitly checking all 3^3 possibilities, we find no case where $\mathrm{N}\epsilon = \pm 1$ and $1 < \epsilon < \xi$. □

Nagell's proof

The main result of this section was already announced in Chapter 1, where it was explained how it could be applied to determine all integer solutions to $y^2 = x^3 + 1$.

Theorem 19.3. The only integer solutions (X, Y) to $X^3 - 2Y^3 = \pm 1$ are $(1, 0), (-1, 0), (1, 1)$, and $(-1, -1)$.

It will be convenient for most of the proof to work with $\eta := \epsilon^{-1} = \sqrt[3]{2} - 1$ rather than ϵ. Note that η shares with ϵ the property that $U(\mathbb{Z}_K) = \{\pm 1\} \times \langle \eta \rangle$.

To get the proof of Theorem 19.3 going, observe that $\mathrm{N}(X - Y\sqrt[3]{2}) = X^3 - 2Y^3$. So if (X, Y) is an integer solution to $X^3 - 2Y^3 = 1$, then $X - Y\sqrt[3]{2}$ is a unit in $\mathbb{Z}_K$. Thus,

$$X - Y\sqrt[3]{2} = \pm(\sqrt[3]{2} - 1)^j \tag{19.3}$$

for some integer j. This equation suggests a change in perspective; rather than look for X and Y directly, we look for values of j where the $\sqrt[3]{4}$ coefficient in the expansion of $(\sqrt[3]{2} - 1)^j$ vanishes.

If $j < 0$, then

$$(\sqrt[3]{2} - 1)^j = (1 + \sqrt[3]{2} + \sqrt[3]{4})^{|j|},$$

and it is obvious that when expanded out the coefficient of $\sqrt[3]{4}$ on the RHS will be positive. Thus, $j \geq 0$.

If $j = 0$, then (19.3) shows that $(X, Y) = (1, 0)$ or $(-1, 0)$; these are two of the given solutions in Theorem 19.3. If $j = 1$, then $(X, Y) = (1, 1)$ or $(-1, -1)$, which are the other two listed solutions.

The remainder of the argument consists in proving that the $\sqrt[3]{4}$ coefficient in $(\sqrt[3]{2} - 1)^j$ is nonvanishing for each integer $j \geq 2$.

Expanding by the binomial theorem,

$$(\sqrt[3]{2} - 1)^j = \sum_{k=0}^{j} \binom{j}{k} \sqrt[3]{2}^k (-1)^{j-k}.$$

The $\sqrt[3]{4}$ coefficient arises from the terms $k = 3\ell + 2$ (with $\ell \geq 0$) and is given by

$$\sum_{\ell \geq 0} \binom{j}{3\ell + 2} 2^\ell (-1)^{j-(3\ell+2)} = (-1)^j \sum_{\ell \geq 0} \binom{j}{3\ell + 2} (-2)^\ell.$$

So for the $\sqrt[3]{4}$ coefficient in $(\sqrt[3]{2} - 1)^j$ to vanish, we need that

$$\begin{aligned} 0 &= \sum_{\ell \geq 0} (-2)^\ell \binom{j}{3\ell + 2} \\ &= \sum_{\ell \geq 0} (-2)^\ell \frac{j(j-1)}{(3\ell + 2)(3\ell + 1)} \binom{j-2}{3\ell} \\ &= j(j-1) \sum_{\ell \geq 0} (-2)^\ell \frac{1}{(3\ell + 2)(3\ell + 1)} \binom{j-2}{3\ell}. \end{aligned}$$

Since $j \geq 2$, the factor $j(j-1)$ is nonzero; hence,

$$\sum_{\ell \geq 0} (-2)^\ell \frac{1}{(3\ell + 2)(3\ell + 1)} \binom{j-2}{3\ell} = 0.$$

The denominators appearing here are coprime to 3, and so it is sensible to reduce this last equation modulo 3. We find that

$$\sum_{\ell \geq 0} \binom{j-2}{3\ell} \equiv 0 \mod 3.$$

But this contradicts our next result.

Proposition 19.4. Let J be any nonnegative integer. Then

$$\binom{J}{0} + \binom{J}{3} + \binom{J}{6} + \cdots \not\equiv 0 \pmod 3.$$

Proof. Let

$$S_0 = \binom{J}{0} + \binom{J}{3} + \binom{J}{6} + \ldots,$$
$$S_1 = \binom{J}{1} + \binom{J}{4} + \binom{J}{7} + \ldots,$$
$$S_2 = \binom{J}{2} + \binom{J}{5} + \binom{J}{8} + \ldots.$$

Observe that

$$\begin{aligned}\binom{J}{3k+1} &= \frac{J!}{(3k+1)!(J-(3k+1))!} \\ &= \binom{J}{3k} \cdot \frac{J-3k}{3k+1} \equiv J\binom{J}{3k} \pmod 3,\end{aligned}$$

and

$$\begin{aligned}\binom{J}{3k+2} &= \binom{J}{3k} \cdot \frac{(J-3k)(J-(3k+1))}{(3k+2)(3k+1)} \\ &\equiv \binom{J}{3k} \cdot \frac{J(J-1)}{2} \pmod 3.\end{aligned}$$

It follows that $S_1 \equiv JS_0$ and $S_2 \equiv \frac{J(J-1)}{2} S_0$, modulo 3. Thus,

$$2^J = S_0 + S_1 + S_2 \equiv \left(1 + J + \frac{J(J-1)}{2}\right) S_0 \pmod 3.$$

Since $3 \nmid 2^J$, it must be that $3 \nmid S_0$. □

Nagell's actual result (op. cit.) is quite a bit more general than Theorem 19.3. Let $K = \mathbb{Q}(\sqrt[3]{D})$, where D is a positive, noncube integer. By Dirichlet's units theorem in its full form, we have (just as above) $U(\mathbb{Z}_K) = \{\pm 1\} \times \langle \eta_D \rangle$ for some unit η_D of infinite order, uniquely determined by the condition $0 < \eta_D < 1$. Nagell's theorem, which refines an earlier result of Delone, is as follows:

Theorem 19.5. Let D be a positive integer that is not a cube. Then the equation $X^3 + DY^3 = 1$ has at most one integer solution (X, Y)

with $XY \neq 0$. If there is any such solution (X, Y), then $X + Y\sqrt[3]{D} = \eta_D$ except for finitely many values of D, where $X + Y\sqrt[3]{D} = \eta_D^2$.[4]

For an exposition, see volume 2 of LeVeque's *Topics in Number Theory*.[5]

Exercises

The exercises in this chapter guide you through the proof of a "poor man's version" of Theorem 19.5.[6]

Theorem 19.6. Let D be a noncube integer with $D \geq 9$. Then the equation $X^3 + DY^3 = 1$ has at most one integer solution (X, Y) with $XY \neq 0$.

In contrast with Theorem 19.5, Theorem 19.6 does not give us a means of deciding whether or not there is a nonzero solution (X, Y). But if we happen to know one already, then we are assured that it is unique. For instance, $X^3 + 9Y^3 = 1$ has the unique nonzero integer solution $(-2, 1)$.

Let $K = \mathbb{Q}(\sqrt[3]{D})$, where D is a noncube positive integer. (We will restrict to $D \geq 9$ only when it becomes necessary.) We will work throughout not in $\mathbb{Z}_K$ but in the (often smaller) subring $\mathbb{Z}[\sqrt[3]{D}]$.

(1) (Explicit description of the norm) We begin by computing the norm (with respect to K) of elements expressed in the basis $1, \sqrt[3]{D}, \sqrt[3]{D^2}$. Here and below, we write $'$ and $''$ for the (complex conjugate) nonreal embeddings of K.

(a) Let $\alpha = a + b\sqrt[3]{D} + c\sqrt[3]{D^2}$, where $a, b, c \in \mathbb{Q}$. Show, by a direct calculation, that $\alpha'\alpha''$ equals

$$a^2 - bcD + (c^2D - ab)\sqrt[3]{D} + (b^2 - ac)\sqrt[3]{D^2}.$$

[4] If we restrict to cubefree D, then this second case arises only for $D = 19, 20$, and 28: Nagell, T. *Einige Gleichungen von der Form $ay^2 + by + c = dx^3$*. Vid. Akad. Skrifter Oslo **7** (1930), 1–15.

[5] LeVeque, W. J. *Topics in number theory*. Vols. 1 and 2. Addison-Wesley Publishing Co., Inc., Reading, Mass., 1956.

[6] The argument we sketch is due to Nagell and appears as "Note II" at the end of the paper cited on p. 205.

(b) Use your answer to (a) to prove that

$$\mathrm{N}\alpha = a^3 + Db^3 + D^2c^3 - 3abcD.$$

(2) (The weak units theorem for $\mathbb{Z}[\sqrt[3]{D}]$)
   (a) Let $\epsilon \in \mathbb{Z}[\sqrt[3]{D}]$. Show that $\epsilon \in U(\mathbb{Z}[\sqrt[3]{D}]) \iff \mathrm{N}\epsilon = \pm 1$. Deduce that $U(\mathbb{Z}[\sqrt[3]{D}]) = U(\mathbb{Z}_K) \cap \mathbb{Z}[\sqrt[3]{D}]$.
   (b) Assume that $\mathbb{Z}[\sqrt[3]{D}]$ contains a unit other than ± 1. Using what was proved in Chapter 18 about units in $\mathbb{Z}_K$, prove that there is a unique $\eta \in U(\mathbb{Z}[\sqrt[3]{D}])$ lying between 0 and 1 with

$$U(\mathbb{Z}[\sqrt[3]{D}]) = \{\pm 1\} \times \langle \eta \rangle.$$

   We will refer to η as the **reduced fundamental unit** of $\mathbb{Z}[\sqrt[3]{D}]$.
   Hint: What can a subgroup of $U(\mathbb{Z}_K)$ look like?

(3) We call $\epsilon \in U(\mathbb{Z}[\sqrt[3]{D}])$ a **binomial unit** when $\epsilon = x + y\sqrt[3]{D}$ for some $x, y \in \mathbb{Z}$. Show that the conclusion of Theorem 19.6 is equivalent to the claim that $\mathbb{Z}[\sqrt[3]{D}]$ has at most one positive, binomial unit $\neq 1$.

   A positive, binomial unit $\neq 1$ will be referred to as an **exceptional unit**.

(4) Suppose that $\epsilon = x + y\sqrt[3]{D}$ is an exceptional unit.
   (a) Show that $xy < 0$.
   (b) Prove that $0 < \epsilon < 1$. Deduce that $\epsilon = \eta^j$ for some *positive* integer j, where η is the reduced fundamental unit. *Hint:* Use Exercise 1(a) to write ϵ^{-1} down explicitly, and show that your result is > 1.
   (c) Show that $|x| \leq 1 + |y|\sqrt[3]{D}$.
   (d) Prove that $|\epsilon'| \leq \sqrt{3}(1 + |y|\sqrt[3]{D})$. *Hint:* $|\epsilon'|^2 = |x^2 - xy\sqrt[3]{D} + y^2\sqrt[3]{D^2}|$, by Exercise 1(a). Now apply (c).

(5) Henceforth, assume that $D > 2$. Prove that if ϵ is an exceptional unit, and $j > 1$, then ϵ^j is not exceptional. Proceed as follows.
   (a) Let $\epsilon = x + y\sqrt[3]{D}$ be an exceptional unit. Show that $|x| > 1$ and $\gcd(x, yD) = 1$.
   (b) Assume for the sake of contradiction that ϵ^j is exceptional, where $j \geq 2$. Show that

$$0 = \sum_{\ell} \binom{j}{3\ell + 2} y^{3\ell+2} D^{\ell} x^{j-(3\ell+2)}.$$

(c) Let p be a prime divisor of x. Show that the $\ell = \lfloor (j-2)/3 \rfloor$ term in the right-hand sum is divisible by a strictly smaller power of p than all other terms. Conclude that the equality asserted in (b) is impossible.

(6) We now complete the proof of Theorem 19.6. Suppose for a contradiction that $\mathbb{Z}[\sqrt[3]{D}]$ has two exceptional units. Then by Exercise 4(b), $\xi := \eta^a$ and $\epsilon := \eta^b$ are exceptional for distinct positive integers a and b. We can (and will) assume that b is the smallest positive integer for which η^b is exceptional. In particular, $b < a$.

(a) Write $a = bq + r$, where $q, r \in \mathbb{Z}$ and $0 \le r < b$. Explain why $r \neq 0$.

(b) Put $\lambda = \eta^r$, and write

$$\lambda = l + m\sqrt[3]{D} + n\sqrt[3]{D^2},$$

where l, m, and n are integers. Show that $n \neq 0$.

(c) Write $\epsilon = x + y\sqrt[3]{D}$ and $\xi = X + Y\sqrt[3]{D}$. The relation $a = bq + r$ implies that

$$X + Y\sqrt[3]{D} = (x + y\sqrt[3]{D})^q (l + m\sqrt[3]{D} + n\sqrt[3]{D^2}).$$

Taking this modulo y, prove that y divides $x^q n$. Deduce that $y \mid n$ and hence that $|n| \ge |y|$.

(d) Show that $3nD = \mathrm{Tr}(\lambda\sqrt[3]{D})$ and establish the bound

$$|\mathrm{Tr}(\lambda\sqrt[3]{D})| \le \sqrt[3]{D}(1 + 2|\lambda'|).$$

Then prove that $|\lambda'| \le |\epsilon'|$ and conclude that

$$3|y|D \le (1 + 2|\epsilon'|)\sqrt[3]{D}.$$

(e) Show that the last inequality contradicts Exercise 4(d) for $D \ge 9$.

Remark: By a more elaborate argument, it can be shown that the reduced fundamental unit η is the only possible exceptional unit. In fact, this was the original theorem of Delone.[7]

[7] Delone, B. *Vollständige Lösung der unbestimmten Gleichung $X^3q + Y^3 = 1$ in ganzen Zahlen.* Math Z. **28** (1928), 1–9. Delone had this result already in 1915 and originally published it in the (somewhat obscure) Journal of the Kharkov Mathematical Society.

20

Dirichlet's units theorem, II

Let K be a degree n number field with r_1 real embeddings, labeled $\sigma_1, \dots, \sigma_{r_1}$, and r_2 pairs of (complex conjugate) nonreal embeddings, $\sigma_{r_1+1}, \overline{\sigma_{r_1+1}}, \dots, \sigma_{r_1+r_2}, \overline{\sigma_{r_1+r_2}}$. Write μ_K for the collection of roots of unity contained in K. Let $\mathrm{Log}\colon K^\times \to \mathbb{R}^{r_1+r_2}$ be defined by

$$\mathrm{Log}\,\alpha = (\log|\sigma_1(\alpha)|, \dots, \log|\sigma_{r_1}(\alpha)|, \\ 2\log|\sigma_{r_1+1}(\alpha)|, \dots, 2\log|\sigma_{r_1+r_2}(\alpha)|).$$

In Chapter 18, we proved a weak version of Dirichlet's units theorem by analyzing the kernel and image of Log. Specifically, we showed there that for some integer $g \le r_1 + r_2 - 1$,

$$U(\mathbb{Z}_K) = \mu_K \times \prod_{i=1}^{g} \langle \epsilon_i \rangle, \tag{20.1}$$

where $\epsilon_1, \dots, \epsilon_g$ are units of infinite order. In this chapter, we improve the inequality on g to an equality, thereby completing the proof of Dirichlet's units theorem.

Theorem 20.1. $g = r_1 + r_2 - 1$.

Geometric preliminaries

Our proof of Theorem 20.1 will depend on locating elements $\alpha \in \mathbb{Z}_K$ whose conjugates are restricted in magnitude in convenient ways. We will deduce the existence of these α from the results of Chapter 12 guaranteeing lattice points in convex, centrally symmetric regions

of sufficiently large volume. But first, we need a way of identifying subsets of K with regions of Euclidean space.

Definition 20.2. The **Minkowski embedding of** K is the map $\iota\colon K \mapsto \mathbb{R}^{r_1} \oplus \mathbb{C}^{r_2}$ where

$$\alpha \mapsto (\sigma_1(\alpha), \dots, \sigma_{r_1}(\alpha), \sigma_{r_1+1}(\alpha), \dots, \sigma_{r_1+r_2}(\alpha)).$$

We will usually identify each factor of $\mathbb{C}$ in the codomain of ι with $\mathbb{R}^2$, via

$$a + bi \longleftrightarrow (a, b);$$

this allows us to view ι as an injective, $\mathbb{Q}$-linear map from K into $\mathbb{R}^{r_1+2r_2} = \mathbb{R}^n$.

The relevant lattice for our purposes is the image of $\mathbb{Z}_K$ under the Minkowski embedding.

Proposition 20.3. $\iota(\mathbb{Z}_K)$ is a lattice in $\mathbb{R}^n$ of full rank.

Proof. It is clear that $\iota(\mathbb{Z}_K)$ is a subgroup of $\mathbb{R}^n$. Let us check that it is discrete. Take any $R > 0$. Suppose that $\alpha \in \mathbb{Z}_K$ and that $\iota(\alpha)$ lies in the closed ball of radius R about the origin. Then

$$|\sigma(\alpha)| \le R \quad \text{for all embeddings } \sigma\colon K \hookrightarrow \mathbb{C}.$$

By Lemma 18.2, there are only finitely many possibilities for α, and so also only finitely many possibilities for $\iota(\alpha)$. So by Theorem 18.7, $\iota(\mathbb{Z}_K)$ is a lattice. To determine its rank, recall that the rank of a lattice always coincides with its rank as a $\mathbb{Z}$-module. Since $\mathbb{Z}_K$ is free of rank n and ι is an injective group homomorphism, $\iota(\mathbb{Z}_K)$ is also free of rank n. □

From Proposition 20.3, the covolume of $\iota(\mathbb{Z}_K)$ is a well-defined, positive quantity. We leave the reader in suspense about its precise value for the moment. (The answer will be revealed in Chapter 21.)

Further reductions

By our work in Chapter 18, the integer g in (20.1) is the rank of the lattice $\operatorname{Log} U(\mathbb{Z}_K) \subseteq \mathbb{R}^{r_1+r_2}$. By definition,

$$\operatorname{rk} \operatorname{Log} U(\mathbb{Z}_K) = \dim_{\mathbb{R}} V, \quad \text{where} \quad V = \operatorname{Log} U(\mathbb{Z}_K) \otimes \mathbb{R}.^1$$

[1] Recall that "$\operatorname{Log} U(\mathbb{Z}_K) \otimes \mathbb{R}$" refers to the real subspace of $\mathbb{R}^{r_1+r_2}$ generated by $\operatorname{Log} U(\mathbb{Z}_K)$.

Basic linear algebra tells us that $\dim_{\mathbb{R}} V + \dim_{\mathbb{R}} V^{\perp} = r_1 + r_2$. Hence,

$$g = r_1 + r_2 - \dim_{\mathbb{R}} V^{\perp},$$

and Theorem 20.1 amounts to the claim that $\dim_{\mathbb{R}} V^{\perp} = 1$.

In Chapter 18, we found that the vector $(1, 1, \dots, 1) \in \mathbb{R}^{r_1+r_2}$ belongs to $V^{\perp}$. So what needs to be proved is that every member of $V^{\perp}$ is a scalar multiple of this vector.

If $V^{\perp}$ contains a "rogue" vector that is not a scalar multiple of $(1, 1, \dots, 1)$, then subtracting a suitable $\mathbb{R}$-multiple of $(1, 1, \dots, 1)$, we obtain an element of $V^{\perp}$ of the form

$$(c_1, c_2, \dots, c_{r_1+r_2-1}, 0),$$

where the c_i are real numbers not all of which vanish. We will prove that this is impossible.

To this end, fix — and keep fixed for the remainder of this chapter — arbitrary real numbers $c_1, c_2, \dots, c_{r_1+r_2-1}$, not all zero. Define a homomorphism $F\colon K^{\times} \mapsto \mathbb{R}$ by

$$F(\alpha) = (c_1, \dots, c_{r_1+r_2-1}, 0) \cdot \operatorname{Log} \alpha.$$

We will show:

Proposition 20.4. *$F(U(\mathbb{Z}_K)) \neq \{0\}$.*

Consequently, $(c_1, \dots, c_{r_1+r_2-1}, 0) \notin V^{\perp}$, and Theorem 20.1 follows.

Proposition 20.4 will be deduced from the following key lemma, whose proof is given in the next section. For the remainder of the chapter, we adopt the convention that $C_1, C_2, C_3, \dots$ denote positive constants that *depend only on the fixed parameters K and $c_1, \dots, c_{r_1+r_2-1}$*.

Lemma 20.5. There is a sequence of $\alpha \in \mathbb{Z}_K$ along which

$$|F(\alpha)| \to \infty,$$

and where each

$$|\mathrm{N}\alpha| < C_1.$$

Deduction of Proposition 20.4 from Lemma 20.5. Take a sequence of the kind described in Lemma 20.5. Each of its terms generates a principal ideal of norm smaller than C_1. But there are only finitely many ideals of $\mathbb{Z}_K$ whose norm falls below any given bound, and

so in particular, below C_1. (For quadratic fields, this is Lemma 8.7; the argument there works just as well for general number fields.) By the Pigeonhole principle, we can pass to a subsequence along which $|F(\alpha)| \to \infty$ but where $\langle\alpha\rangle$ is constant. Choose α_1, α_2 from this subsequence with $F(\alpha_1) \neq F(\alpha_2)$. Since $\langle\alpha_1\rangle = \langle\alpha_2\rangle$, the quotient α_1/α_2 lies in $U(\mathbb{Z}_K)$, while $F(\alpha_1/\alpha_2) = F(\alpha_1) - F(\alpha_2) \neq 0$. □

Proof of Lemma 20.5

For each tuple of positive real numbers $\lambda_1, \dots, \lambda_{r_1+r_2}$, let

$$\mathcal{R}_{\lambda_1,\dots,\lambda_{r_1+r_2}} = \{(x_1, \dots, x_{r_1+r_2}) \in \mathbb{R}^{r_1} \oplus \mathbb{C}^{r_2} : |x_i| \leq \lambda_i \ \forall i\}.$$

We think of $\mathcal{R}_{\lambda_1,\dots,\lambda_{r_1+r_2}}$ as a subset of $\mathbb{R}^{r_1+2r_2} = \mathbb{R}^n$ (via the identification of $\mathbb{R}^{r_1+2r_2}$ with $\mathbb{R}^n$ discussed earlier). It is easy to see that $\mathcal{R}_{\lambda_1,\dots,\lambda_{r_1+r_2}}$ is both

- centrally symmetric (since $|x| = |-x|$), *and*
- convex (use the triangle inequality).

To compute $\mathrm{vol}(\mathcal{R}_{\lambda_1,\dots,\lambda_{r_1+r_2}})$, notice that $\mathcal{R}_{\lambda_1,\dots,\lambda_{r_1+r_2}}$ is the Cartesian product of r_1 (1-dimensional) intervals of "radii" $\lambda_1, \dots, \lambda_{r_1}$ together with r_2 (2-dimensional) discs of radii $\lambda_{r_1+1}, \dots, \lambda_{r_1+r_2}$. Thus,

$$\begin{aligned} \mathrm{vol}(\mathcal{R}_{\lambda_1,\dots,\lambda_{r_1+r_2}}) &= \prod_{i=1}^{r_1}(2\lambda_i) \prod_{i=r_1+1}^{r_1+r_2}(\pi\lambda_i^2) \\ &= 2^{r_1}\pi^{r_2}\lambda_1 \dots \lambda_n, \end{aligned} \tag{20.2}$$

where we have set

$$\lambda_{r_1+r_2+i} := \lambda_{r_1+i} \quad \text{for } i = 1, 2, \dots, r_2.$$

From now on, we will only work with tuples $\lambda_1, \dots, \lambda_{r_1+r_2}$ whose entries are related by the condition

$$\mathrm{vol}(R_{\lambda_1,\dots,\lambda_{r_1+r_2}}) = 2 \cdot (2^n \,\mathrm{covol}(\iota(\mathbb{Z}_K))). \tag{20.3}$$

Observe that if we are given any real numbers

$$\lambda_1, \dots, \lambda_{r_1+r_2-1} > 0,$$

then there is a unique $\lambda_{r_1+r_2} > 0$ for which (20.3) holds.

By Minkowski's convex body theorem (Theorem 12.5), for any tuple $\lambda_1, \dots, \lambda_{r_1+r_2}$ as above, there is a nonzero $\alpha \in \mathbb{Z}_K$ with $\iota(\alpha) \in R_{\lambda_1,\dots,\lambda_{r_1+r_2}}$. For this α,

$$|\mathrm{N}\alpha| = \prod_{i=1}^{r_1} |\sigma_i(\alpha)| \prod_{i=r_1+1}^{r_1+r_2} |\sigma_i(\alpha)|^2 \le \prod_{i=1}^{r_1} \lambda_i \prod_{i=r_1+1}^{r_1+r_2} \lambda_i^2 = \prod_{i=1}^{n} \lambda_i.$$

From (20.2) and (20.3),

$$\begin{aligned}\prod_{i=1}^{n} \lambda_i &= 2^{-r_1}\pi^{-r_2} \cdot \mathrm{vol}(R_{\lambda_1,\dots,\lambda_{r_1+r_2}}) \\ &= 2^{-r_1}\pi^{-r_2} \cdot 2^{n+1}\,\mathrm{covol}(\iota(\mathbb{Z}_K)).\end{aligned}$$

This quantity depends only on K, and we denote it by C_1. Thus,

$$|\mathrm{N}\alpha| \le C_1. \tag{20.4}$$

So we have a method that allows us, starting from any "seed tuple" $\lambda_1, \dots, \lambda_{r_1+r_2}$ (subject to (20.3)), to write down an element α of bounded norm. The next stage of the proof is to show that by a careful selection of the λ_i, we can force $|F(\alpha)|$ to be large.

Observe that for each $i = 1, 2, \dots, n$,

$$\begin{aligned}1 \le |\mathrm{N}\alpha| = \prod_{i=1}^{n} |\sigma_i(\alpha)| &= |\sigma_i(\alpha)| \prod_{\substack{1\le j\le n \\ j\ne i}} |\sigma_j(\alpha)| \\ &\le \frac{|\sigma_i(\alpha)|}{\lambda_i} \prod_{j=1}^{n} \lambda_j.\end{aligned}$$

Hence,

$$1 \le \frac{\lambda_i}{|\sigma_i(\alpha)|} \le \prod_{j=1}^{n} \lambda_j = C_1.$$

Taking logs,

$$0 \le \log \lambda_i - \log|\sigma_i(\alpha)| \le C_2. \tag{20.5}$$

Recall that by definition,

$$F(\alpha) = (c_1, \dots, c_{r_1+r_2-1}, 0) \cdot \mathrm{Log}\,\alpha, \tag{20.6}$$

where

$$\operatorname{Log}\alpha = (\log|\sigma_1(\alpha)|,\dots,\log|\sigma_{r_1}(\alpha)|, \\ 2\log|\sigma_{r_1+1}(\alpha)|,\dots,2\log|\sigma_{r_1+r_2}(\alpha)|).$$

Put

$$\mathbf{L} = (\log\lambda_1,\log\lambda_2,\dots,\log\lambda_{r_1},2\log\lambda_{r_1+1},\dots,2\log\lambda_{r_1+r_2}).$$

From (20.5),

$$|\mathbf{L}-\operatorname{Log}\alpha| \le C_3,$$

and now (20.6) implies (Cauchy–Schwarz) that

$$|F(\alpha)-(c_1,\dots,c_{r_1+r_2-1},0)\cdot\mathbf{L}| \le C_4.$$

So $|F(\alpha)|$ will be large whenever $|(c_1,\dots,c_{r_1+r_2-1},0)\cdot\mathbf{L}|$ is large. To arrange for this, fix an index $i \in \{1,2,\dots,r_1+r_2-1\}$ with $c_i \neq 0$. (Remember that the c_i do not all vanish.) Choose tuples $\lambda_1,\dots,\lambda_{r_1+r_2}$ where λ_i is large, where $\lambda_j = 1$ for those $j = 1,2,\dots,r_1+r_2-1$ with $j \neq i$, and where $\lambda_{r_1+r_2}$ is determined by (20.3). Since "large" in the last sentence can be arbitrarily large, in this way we can construct a sequence of α where $|F(\alpha)| \to \infty$. Keeping in mind (20.4), we have proved the lemma.

Exercises

(1) Characterize those number fields K where $\mathbb{Z}_K$ has nonzero elements of arbitrarily small absolute value.

(2) Let K be a cubic number field contained in $\mathbb{R}$. Suppose that the two non-identity complex embeddings of K are nonreal. Then by Dirichlet's units theorem,

$$U(\mathbb{Z}_K) = \{\pm1\}\times\langle\epsilon_0\rangle$$

for some unit ϵ_0 of infinite order. If we insist that $\epsilon_0 > 1$, then ϵ_0 is unique; we call it the **fundamental unit** of $\mathbb{Z}_K$. The next few exercises give some examples of the determination of ϵ_0.

Our main tool will be **Artin's inequality**: If ϵ is any unit of $\mathbb{Z}_K$ exceeding 1, then

$$|\Delta_K| < 4\epsilon^3 + 28. \tag{20.7}$$

This exercise outlines a proof.[2]

(a) Denote the images of ϵ under the (complex conjugate) nonreal embeddings by $re^{i\theta}$ and $re^{-i\theta}$, where $r > 0$. Prove that $|\epsilon| = r^{-2}$.

(b) Show that

$$\Delta(1, \epsilon, \epsilon^2) = -4\sin^2(\theta)(r^3 + r^{-3} - 2\cos(\theta))^2.$$

(c) Prove that the absolute value of the right-hand side is smaller than

$$4(r^3 + r^{-3})^2 + 16.$$

Hint: Let $x = r^3 + r^{-3}$ and $c = \cos(\theta)$. Then we are being asked to show that

$$4(1 - c^2)(x - 2c)^2 < 4x^2 + 16.$$

In fact, this inequality holds for all $x > 2$ and all $c \in [-1, 1]$. (Note that $r^3 + r^{-3} > 2$.) To prove this, argue that the LHS achieves its maximum at that $c \in [-1, 0]$ with $4c - 2/c = x$. Plug this expression for x into the difference

$$4(1 - c^2)(x - 2c)^2 - 4x^2$$

and simplify.

(d) Deduce (20.7).

(3) (continuation) Show that if ϵ is a unit of $\mathbb{Z}_K$ with $\epsilon > 1$ and $4\epsilon^{3/2} + 28 \leq |\Delta_K|$, then ϵ is the fundamental unit of $\mathbb{Z}_K$.

(4) (a) Use the last exercise to show that $1 + \sqrt[3]{2} + \sqrt[3]{4}$ is the fundamental unit of the ring of integers of $\mathbb{Q}(\sqrt[3]{2})$.

(b) Show that $(\sqrt[3]{9} - 2)^{-1}$ and $(2 - \sqrt[3]{7})^{-1}$ are the fundamental units of the rings of integers of $\mathbb{Q}(\sqrt[3]{3})$ and $\mathbb{Q}(\sqrt[3]{7})$, respectively.

(5) When $K = \mathbb{Q}(\sqrt[3]{5})$, the fundamental unit is $\epsilon = 41 + 24\sqrt[3]{5} + 14\sqrt[3]{25}$. Check that this unit does *not* satisfy the criterion of Exercise 3. Nevertheless, explain how you could verify (in a finite number of steps) that this is indeed the fundamental unit. If you are feeling ambitious, carry out this procedure.

---

[2] In fact, Artin had a slightly stronger result, with 24 instead of 28 on the right-hand side of (20.7). See Chapter 13 in: Artin, E. *Theory of algebraic numbers.* Notes by Gerhard Würges from lectures held at the Mathematisches Institut, Göttingen, Germany, in the Winter Semester, 1956/7. Translated by George Striker. George Striker, Schildweg 12, Göttingen, 1959.

(6) (Ishida[3]) Let $f(x) = x^3 + \ell x - 1$, where $\ell \geq 2$ is an integer for which $4\ell^3 + 27$ is squarefree.
   (a) Show that f is irreducible over $\mathbb{Q}$.
   (b) Show that f has a unique real root θ (say).
   (c) Let $K = \mathbb{Q}(\theta)$. Prove that $\mathbb{Z}_K = \mathbb{Z}[\theta]$ and that $|\Delta_K| = 4\ell^3 + 27$.
   (d) Prove that $1/\theta$ is the fundamental unit of $\mathbb{Z}_K$.

(7) Let K be a degree n number field, and let $\mathcal{O}$ be a subring of K that is free of rank n as a $\mathbb{Z}$-module. Such a ring is called an **order** in K. (To give an example familiar from the last chapter, the ring $\mathbb{Z}[\sqrt[3]{D}]$ is an order in the pure cubic field $\mathbb{Q}(\sqrt[3]{D})$, for any noncube integer D.)
   (a) Show that $\mathcal{O} \subseteq \mathbb{Z}_K$. *Hint:* Apply Lemma 2.5.
   (b) Explain why $[\mathbb{Z}_K : \mathcal{O}] < \infty$.
   (c) Show that $U(\mathcal{O}) = U(\mathbb{Z}_K) \cap \mathcal{O}$. *Hint:* Apply Exercise 2.4.
   (d) Show that for each $\epsilon \in U(\mathbb{Z}_K)$, there is some positive power of ϵ belonging to $U(\mathcal{O})$. *Hint:* Find a power of ϵ congruent to 1 mod f, where $f = [\mathbb{Z}_K : \mathcal{O}]$.
   (e) (Dirichlet's units theorem for orders) Let $\mu_{\mathcal{O}}$ be the group of roots of unity contained in $\mathcal{O}$. Prove that there are elements $\eta_1, \ldots, \eta_{r_1+r_2-1} \in U(\mathcal{O})$ of infinite order with

$$U(\mathcal{O}) = \mu_{\mathcal{O}} \times \prod_{i=1}^{r_1+r_2-1} \langle \eta_i \rangle.$$

(8) Let p be an odd prime and put $\zeta_p = e^{2\pi i/p}$. Let $K = \mathbb{Q}(\zeta_p)$.
   (a) Show that $\mu_K = \{\pm\zeta_p^k : 0 \leq k < p\}$. *Hint:* By Exercise 18.4, μ_K is cyclic. If μ_K is generated by an element of order m, show that $p \mid m$ and that $\phi(m) \mid p - 1$. Which m satisfy these conditions?
   (b) Show that the ratio $\frac{1-\zeta_p^k}{1-\zeta_p} \in U(\mathbb{Z}_K)$ for all integers k coprime to p. Are any of these ratios roots of unity?

(9) Let $K = \mathbb{Q}(\zeta_p)$, where p is an odd prime, and let $\epsilon \in U(\mathbb{Z}_K)$.
   (a) Show that $\epsilon = \pm\zeta_p^k \cdot \bar{\epsilon}$ for some $k \in \mathbb{Z}$ and some choice of sign. Here the bar denotes complex conjugation. *Hint:* Look back at Exercise 18.10.

---

[3]Ishida, M. *Fundamental units of certain algebraic number fields.* Abh. Math. Sem. Univ. Hamburg **39** (1973), 245–250.

(b) Show that $\epsilon \equiv \bar{\epsilon} \pmod{1-\zeta_p}$. Use this to argue that the $+$ sign holds in (a). *Hint:* Start by writing $\epsilon = \sum_j a_j \zeta_p^j$, with all $a_j \in \mathbb{Z}$.

(c) Show that $\epsilon/\zeta_p^g \in \mathbb{R}$ for some $g \in \mathbb{Z}$.

(10) Let $K = \mathbb{Q}(\zeta_5)$. Show that

$$U(\mathbb{Z}_K) = \{\pm 1\} \times \langle e^{2\pi i/5} \rangle \times \left\langle \frac{1+\sqrt{5}}{2} \right\rangle.$$

21

More Minkowski magic, with a cameo appearance by Hermite

Let K be a degree n number field with real embeddings $\sigma_1, \ldots, \sigma_{r_1}$ and nonreal embeddings $\sigma_{r_1+1}, \overline{\sigma_{r_1+1}}, \ldots, \sigma_{r_1+r_2}, \overline{\sigma_{r_1+r_2}}$. In Chapter 20, we introduced the Minkowski embedding of K, defined as the map $\iota\colon K \to \mathbb{R}^{r_1} \oplus \mathbb{C}^{r_2}$ sending

$$\alpha \mapsto (\sigma_1(\alpha), \ldots, \sigma_{r_1}(\alpha), \sigma_{r_1+1}(\alpha), \ldots, \sigma_{r_1+r_2}(\alpha)).$$

We saw that ι embeds $\mathbb{Z}_K$ into

$$\mathbb{R}^{r_1} \oplus \mathbb{R}^{2r_2} = \mathbb{R}^n$$

as a full rank lattice, but we did not need to know — and so did not compute — the covolume of $\iota(\mathbb{Z}_K)$.

That computation is at the top of our agenda for this chapter; it serves as a way station on the road to the proofs of two celebrated theorems of Minkowski.

The first of these is the famous **Minkowski bound** for the smallest (in norm) representative of an ideal class. We state the result and give some examples showing how it facilitates explicit computation of class groups. But we will spend more time in the neighborhood of the second theorem, that the discriminant of any number field $K \neq \mathbb{Q}$ is larger than 1 in absolute value. That result provides a natural segue into a discussion of **Hermite's theorem**, which asserts that there only finitely many number fields K for which $|\Delta_K|$ lies below a given limit.

Covolume computations

Proposition 21.1. $\operatorname{covol}(\iota(\mathbb{Z}_K)) = 2^{-r_2}\sqrt{|\Delta_K|}$.

Proof. Let $\omega_1, \ldots, \omega_n$ be an integral basis for K. Then the covolume of $\iota(\mathbb{Z}_K)$ can be computed as $|\det(A)|$, where A is the $n \times n$ matrix whose columns are $\iota(\omega_1), \ldots, \iota(\omega_n)$; that is,

$$A = \begin{bmatrix} \sigma_1(\omega_1) & \ldots & \sigma_1(\omega_n) \\ \sigma_2(\omega_1) & \ldots & \sigma_2(\omega_n) \\ \vdots & \vdots & \vdots \\ \sigma_{r_1}(\omega_1) & \ldots & \sigma_{r_1}(\omega_n) \\ \Re\sigma_{r_1+1}(\omega_1) & \ldots & \Re\sigma_{r_1+1}(\omega_n) \\ \Im\sigma_{r_1+1}(\omega_1) & \ldots & \Im\sigma_{r_1+1}(\omega_n) \\ \vdots & \vdots & \vdots \\ \Re\sigma_{r_1+r_2}(\omega_1) & \ldots & \Re\sigma_{r_1+r_2}(\omega_n) \\ \Im\sigma_{r_1+r_2}(\omega_1) & \ldots & \Im\sigma_{r_1+r_2}(\omega_n) \end{bmatrix}.$$

For comparison, recall that $\Delta_K = \det(D_{\omega_1,\ldots,\omega_n})^2$, where $D_{\omega_1,\ldots,\omega_n}$ is the matrix with the same first r_1 rows as A, but whose final r_2 pairs of rows have the form

$$\begin{bmatrix} \sigma(\omega_1) & \ldots & \sigma(\omega_n) \\ \overline{\sigma}(\omega_1) & \ldots & \overline{\sigma}(\omega_n) \end{bmatrix} \tag{21.1}$$

instead of

$$\begin{bmatrix} \Re\sigma(\omega_1) & \ldots & \Re\sigma(\omega_n) \\ \Im\sigma(\omega_1) & \ldots & \Im\sigma(\omega_n) \end{bmatrix}. \tag{21.2}$$

One can go from (21.1) to (21.2) by a sequence of four elementary row operations; add the second row to the first, multiply the first row by $\frac{1}{2}$, subtract the first row from the second, and multiply the second row by $-i$. Since this sequence of operations is carried out r_2 times in order to transform $D_{\omega_1,\ldots,\omega_n}$ into A,

$$\det(A) = \det(D_{\omega_1,\ldots,\omega_n}) \cdot (-i/2)^{r_2}.$$

Hence,

$$\begin{aligned} \operatorname{covol}(\iota(\mathbb{Z}_K)) = |\det(A)| &= 2^{-r_2}|\det(D_{\omega_1,\ldots,\omega_n})| \\ &= 2^{-r_2}\sqrt{|\Delta_K|}, \end{aligned}$$

precisely as claimed. □

Proposition 21.1 can be generalized to arbitrary nonzero ideals of $\mathbb{Z}_K$. First we show that these ideals have the same $\mathbb{Z}$-module structure as $\mathbb{Z}_K$.

Lemma 21.2. Every nonzero ideal I of $\mathbb{Z}_K$ is free of rank n as a $\mathbb{Z}$-module.

Proof. Let α be any nonzero element of I. Then $\alpha\mathbb{Z}_K \subseteq I \subseteq \mathbb{Z}_K$. Now $\mathbb{Z}_K$ is a free $\mathbb{Z}$-module of rank n, and (as a consequence) so is $\alpha\mathbb{Z}_K$. Since I is squeezed between two free $\mathbb{Z}$-modules of rank n, Corollary 18.8 shows that I itself is free of rank n. □

Proposition 21.3. Let I be a nonzero ideal of $\mathbb{Z}_K$. Then $\iota(I)$ is a full rank lattice in $\mathbb{R}^n$, and $\mathrm{covol}(\iota(I)) = 2^{-r_2}\mathrm{N}(I)\sqrt{|\Delta_K|}$.

Proof. Let $\omega_1, \ldots, \omega_n$ and $\theta_1, \ldots, \theta_n$ be $\mathbb{Z}$-bases for $\mathbb{Z}_K$ and I, respectively. Let A be the $n \times n$ integer matrix with

$$[\theta_1, \ldots, \theta_n] = [\omega_1, \ldots, \omega_n]A.$$

By the index=determinant theorem (Theorem 13.10),

$$|\det(A)| = \mathrm{N}(I).$$

The vectors $\iota(\theta_1), \ldots, \iota(\theta_n)$ form a $\mathbb{Z}$-basis for $\iota(I)$, and

$$[\iota(\theta_1), \ldots, \iota(\theta_n)] = [\iota(\omega_1), \ldots, \iota(\omega_n)]A.$$

Hence (taking determinants and then absolute values),

$$\begin{aligned}\mathrm{covol}(\iota(I)) &= \mathrm{covol}(\iota(\mathbb{Z}_K))|\det(A)| \\ &= 2^{-r_2}\mathrm{N}(I)\sqrt{|\Delta_K|}.\end{aligned}$$

We committed a venial sin just now, speaking of the covolume of $\iota(I)$ before verifying that $\iota(I)$ is a full rank lattice. In fact, the latter statement is a byproduct of the above calculation. Indeed, since $[\iota(\theta_1), \ldots, \iota(\theta_n)]$ has nonzero determinant, the vectors $\iota(\theta_1), \ldots, \iota(\theta_n)$ are necessarily $\mathbb{R}$-linearly independent. □

The Minkowski bound

We now describe how Minkowski's theorem may be applied to estimate the smallest ideal lying in a given ideal class. We begin with a useful reformulation of the problem. Let K be an arbitrary number field.

Lemma 21.4. Let $B > 0$.

$$\begin{array}{c}\text{Every nonzero ideal } I \\ \text{contains an } \alpha \neq 0 \text{ with} \\ |\mathrm{N}\alpha| \leq B \cdot \mathrm{N}(I).\end{array} \iff \begin{array}{c}\text{Every ideal class is} \\ \text{represented by an ideal} \\ \text{of norm at most } B.\end{array}$$

Proof. The forward direction ($\Rightarrow$), which is the one important below, was shown already as Lemma 9.5. (There K is a quadratic field, but the argument carries over verbatim to general number fields.) So we only prove the backward implication ($\Leftarrow$). Let I be any nonzero ideal of $\mathbb{Z}_K$. Choose an ideal J belonging to $[I]^{-1}$ with $\mathrm{N}(J) \leq B$. Then IJ is principal. Writing $IJ = \langle\alpha\rangle$, we see that $\alpha \in I \setminus \{0\}$ and that

$$|\mathrm{N}\alpha| = \mathrm{N}(\langle\alpha\rangle) = \mathrm{N}(IJ) = \mathrm{N}(I)\mathrm{N}(J) \leq B \cdot \mathrm{N}(I). \qquad \square$$

Lemma 21.4 reduces our task to showing that nonzero ideals always contain nonzero elements of small norm, a problem that is tailor-made for Minkowskian methods! Let $\mathcal{R} \subseteq \mathbb{R}^n$ be a convex, centrally symmetric region with $\mathrm{vol}(\mathcal{R}) > 2^n \,\mathrm{covol}(\iota(I))$. Minkowski's theorem (Theorem 12.5) furnishes us with a nonzero $\alpha \in I$ having $\iota(\alpha) \in \mathcal{R}$. We will rig the game by choosing $\mathcal{R}$ so that having $\iota(\alpha) \in \mathcal{R}$ forces $|\mathrm{N}\alpha|$ to be small.

For each $X > 0$, there is a region $\mathcal{R}_0(X) \subseteq \mathbb{R}^n$ corresponding precisely to the condition that $|\mathrm{N}\alpha| \leq X$, namely

$$\{(x_1, \ldots, x_n) \in \mathbb{R}^{r_1} \oplus \mathbb{C}^{r_2} : \prod_{i=1}^{r_1} |x_i| \prod_{j=r_1+1}^{r_1+r_2} |x_j|^2 \leq X\}.$$

(Pause to convince yourself of this correspondence, if you need convincing.) Unfortunately, $\mathcal{R}_0(X)$ is in general not convex, which precludes the application of Minkowski's theorem. The fix for this is to work not with $\mathcal{R}_0(X)$ but with a convex region $\mathcal{R}$ inscribed inside $\mathcal{R}_0(X)$.

To make a sensible choice for $\mathcal{R}$, we apply the following well-known inequality comparing the arithmetic and geometric means.

Proposition 21.5 (AM-GM inequality)**.** Let $t_1, \dots, t_m$ be any nonnegative real numbers. Then the arithmetic mean of the t_i is at least as large as their geometric mean; i.e.,

$$\frac{t_1 + \cdots + t_m}{m} \geq \sqrt[m]{t_1 \cdots t_m}.$$

Proof. We cannot resist giving Pólya's slick proof.[1] The result is certainly true (but uninteresting) when all $t_i = 0$, so we assume that at least one t_i is positive. If we scale all the t_i by a factor of λ, then both the arithmetic and geometric means also scale by λ. Thus, there is no loss of generality in assuming that

$$t_1 + \cdots + t_m = m;$$

our task is then to show that

$$t_1 \cdots t_m \leq 1.$$

The function $x \mapsto e^x$ is concave up on the entire real line. Thus, its graph lies above each of its tangent lines, and so in particular above the line $y = x + 1$ (the tangent line at $x = 0$). That is,

$$e^x \geq x + 1 \qquad \text{for all real numbers } x.$$

Hence, $e^{t_i - 1} \geq t_i$ for each $i = 1, 2, \dots, m$, and so

$$1 = e^0 = e^{(t_1 + \cdots + t_m) - m} = \prod_{i=1}^{m} e^{t_i - 1} \geq \prod_{i=1}^{m} t_i. \qquad \square$$

By the AM-GM inequality,

$$\left(\prod_{i=1}^{r_1} |x_i| \prod_{j=r_1+1}^{r_1+r_2} |x_j|^2 \right)^{1/n} \leq \frac{\sum_{i=1}^{r_1} |x_i| + 2 \sum_{j=r_1+1}^{r_1+r_2} |x_j|}{n}.$$

Thus, if we set

$$\mathcal{R}_{\mathrm{Min}}(X) = \{(x_1, \dots, x_n) \in \mathbb{R}^{r_1} \oplus \mathbb{C}^{r_2} : \frac{\sum_{i=1}^{r_1} |x_i| + 2 \sum_{j=r_1+1}^{r_1+r_2} |x_j|}{n} \leq X^{1/n}\},$$

then $\mathcal{R}_{\mathrm{Min}}(X) \subseteq \mathcal{R}_0(X)$. (See Figure 21.1.) Clearly, $\mathcal{R}_{\mathrm{Min}}(X)$ is centrally symmetric, and the triangle inequality implies that $\mathcal{R}_{\mathrm{Min}}(X)$ is also convex.

[1] Pólya claimed that this proof came to him in a dream.

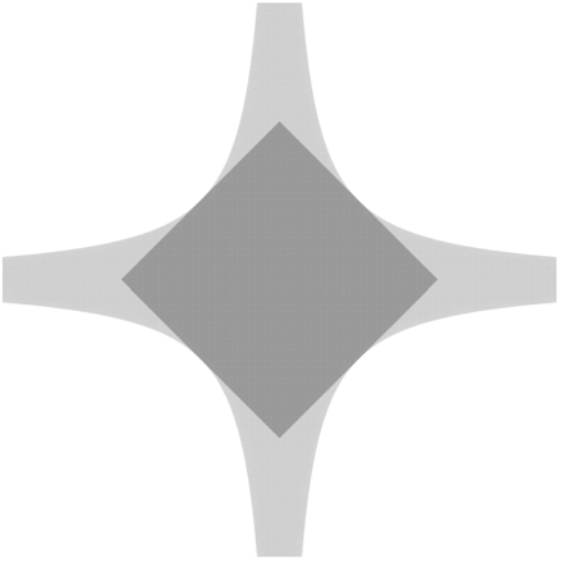


Figure 21.1. The regions $\mathcal{R}_{\mathrm{o}}$ and $\mathcal{R}_{\mathrm{Min}}$ when K is real quadratic. In that case, $\mathcal{R}_{\mathrm{o}}(X) = \{(x,y) : |xy| \le X\}$ and $\mathcal{R}_{\mathrm{Min}}(X) = \{(x,y) : \frac{|x|+|y|}{2} \le X^{1/2}\}$.

The computation of the volume of $\mathcal{R}_{\mathrm{Min}}(x)$ is deferred to the appendix. We quote the end result.

Proposition 21.6. $\mathrm{vol}(\mathcal{R}_{\mathrm{Min}}(X)) = 2^{r_1}(\pi/2)^{r_2}\frac{n^n}{n!}X$.

Combined with our earlier determination of $\mathrm{covol}(\iota(I))$ (Proposition 21.3), Proposition 21.6 shows that

$$\mathrm{vol}(\mathcal{R}_{\mathrm{Min}}(X)) > 2^n \,\mathrm{covol}(\iota(I))$$

precisely when $X > M_K \cdot \mathrm{N}(I)$, where

$$M_K := \left(\frac{4}{\pi}\right)^{r_2} \frac{n!}{n^n}\sqrt{|\Delta_K|}. \tag{21.3}$$

All the pieces are now in place for us to establish the **Minkowski bound**.[2]

[2]Minkowski, H. *Théorèmes arithmétiques.* C.R. Acad. Sci. Paris **112** (1891), 209–212.

Theorem 21.7. Every nonzero ideal I contains a nonzero α with $|\mathrm{N}\alpha| \le M_K \cdot \mathrm{N}(I)$. Thus, every ideal class has a representative of norm at most M_K.

Proof. Let X be an arbitrary real number larger than $M_K \cdot \mathrm{N}(I)$. By Minkowski's theorem, there is a nonzero $\alpha \in I$ with $\iota(\alpha) \in \mathcal{R}_{\mathrm{Min}}(X)$. By construction, $\mathcal{R}_{\mathrm{Min}}(X) \subseteq \mathcal{R}_{\mathrm{o}}(X)$, and hence $\iota(\alpha) \in \mathcal{R}_{\mathrm{Min}}(X)$ implies that $|\mathrm{N}\alpha| \le X$. Since $\mathrm{N}\alpha \in \mathbb{Z}$, in fact $|\mathrm{N}\alpha| \le \lfloor X \rfloor$. Now choose X exceeding $M_K \cdot \mathrm{N}(I)$ only slightly, so that $\lfloor X \rfloor = \lfloor M_K \cdot \mathrm{N}(I) \rfloor$. □

Two class number calculations

The following two examples illustrate how Theorem 21.7 can be used to give quick proofs that certain number fields have class number 1. More intricate class group calculations appear in the end-of-chapter exercises.

Example 21.8. Let $K = \mathbb{Q}(\sqrt[3]{3})$. Then $r_1 = 1$, $r_2 = 1$, and Δ_K divides $\Delta(x^3 - 3) = -3^5$. Hence,

$$M_K \le \frac{4}{\pi} \cdot \frac{3!}{3^3} \cdot \sqrt{3^5} = 4.41\ldots.$$

From Theorem 21.7, every nontrivial ideal class is represented by an ideal of norm 2, 3, or 4. Such an ideal factors as a product of prime ideals above $2\mathbb{Z}_K$ and $3\mathbb{Z}_K$.

The factorization of $2\mathbb{Z}_K$ may be computed with the Dedekind–Kummer Theorem (Theorem 17.2). (Note that $2^2 \nmid \Delta(x^3 - 3)$, and so $2 \nmid [\mathbb{Z}_K : \mathbb{Z}[\sqrt[3]{3}]]$.) Since

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

we have

$$2\mathbb{Z}_K = \langle 2, \sqrt[3]{3} - 1 \rangle \cdot \langle 2, \sqrt[3]{9} + \sqrt[3]{3} + 1 \rangle.$$

But

$$(\sqrt[3]{3} - 1)(\sqrt[3]{9} + \sqrt[3]{3} + 1) = (\sqrt[3]{3})^3 - 1 = 2$$

and so

$$\langle 2, \sqrt[3]{3} - 1 \rangle = \langle \sqrt[3]{3} - 1 \rangle, \quad \langle 2, \sqrt[3]{9} + \sqrt[3]{3} + 1 \rangle = \langle \sqrt[3]{9} + \sqrt[3]{3} + 1 \rangle.$$

So both prime ideals above 2 are principal.

The prime factorization of $3\mathbb{Z}_K$ is obvious: $\langle 3\rangle = \langle \sqrt[3]{3}\rangle^3$. So there is one prime ideal of norm 3, namely $\langle \sqrt[3]{3}\rangle$, which is also principal.

Since every prime above 2 or 3 is principal, $\mathrm{Cl}(\mathbb{Z}_K)$ is trivial.

Example 21.9. Let $K = \mathbb{Q}(\theta)$, where θ is a root of the irreducible quintic $f(x) = x^5 - x^3 + 1$. A quick peek at the graph shows that $f(x)$ has exactly one real root. Hence, $r_1 = 1$ and $r_2 = 2$. Moreover, $\Delta(f(x)) = 3017$, which is squarefree; thus, $\mathbb{Z}_K = \mathbb{Z}[\theta]$ and

$$\Delta_K = \Delta(f(x)) = 3017.$$

So

$$M_K = \left(\frac{4}{\pi}\right)^2 \cdot \frac{5!}{5^5} \cdot \sqrt{3017} = 3.41\ldots.$$

Hence, every nonprincipal ideal class is represented by an ideal of norm 2 or 3 (which is necessarily prime). Now $f(x)$ is irreducible mod 2, while

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

By Dedekind–Kummer, the unique prime above 2 has norm 2^5, while the primes above 3 have norm 3^2 and 3^3. In particular, there are no prime ideals of norm 2 or norm 3. So once again, $\mathrm{Cl}(\mathbb{Z}_K)$ is trivial.

A lower bound for $|\Delta_K|$

Since every ideal class contains a representative of norm at most M_K, certainly $M_K \geq 1$. Referring back to the definition (21.3), it follows that

$$|\Delta_K| \geq \left(\frac{n^n}{n!}\right)^2 \left(\frac{\pi}{4}\right)^{2r_2}. \tag{21.4}$$

We bound the right-hand side from below by the following crude argument. Since $r_1 + 2r_2 = n$, we have $r_2 \leq n/2$, and so $|\Delta_K| \geq \left(\frac{n^n}{n!}\right)^2 \left(\frac{\pi}{4}\right)^n =: B_n$ (say). For each $n \in \mathbb{Z}^+$,

$$\begin{aligned}\frac{B_{n+1}}{B_n} &= \left(1 + \frac{1}{n}\right)^{2n} \cdot \frac{\pi}{4},\\ &\geq \left(1 + \binom{2n}{1}\frac{1}{n} + \binom{2n}{2}\frac{1}{n^2} + \ldots\right) \cdot \frac{\pi}{4} \geq \frac{3\pi}{4}.\end{aligned}$$

Since $B_2 = \pi^2/4$, we conclude that if K has degree $n \geq 2$, then

$$|\Delta_K| \geq \left(\frac{\pi^2}{4}\right) \cdot \left(\frac{3\pi}{4}\right)^{n-2}. \tag{21.5}$$

Both $\pi^2/4$ and $3\pi/4$ are larger than 1, and so the following result is now immediate.

Theorem 21.10 (Minkowski)**.** If $K \neq \mathbb{Q}$, then $|\Delta_K| > 1$.

In Chapter 13, we alluded to Dedekind's theorem that the rational primes ramifying in a number field K are precisely those dividing Δ_K. (This is proved in Chapter 22.) Combining Dedekind's result with Theorem 21.10, we see that whenever K is a number field $\neq \mathbb{Q}$, the set of primes ramifying in K is nonempty.

Enter Hermite, stage left

Theorem 21.10 says that there is exactly one number field K with $|\Delta_K| < 2$, namely $K = \mathbb{Q}$. Is it natural to wonder what happens if we replace 2 with a larger bound. This is addressed by the following 1857 theorem of Hermite.[3]

Theorem 21.11. Let $X > 0$. There are only finitely many number fields K with $|\Delta_K| \leq X$.

By (21.5), an upper bound on $|\Delta_K|$ implies a corresponding bound on $n = [K : \mathbb{Q}]$. Thus, Theorem 21.11 is a consequence of the following fixed-degree variant.

Proposition 21.12. Fix $n \in \mathbb{Z}^+$. For each $X > 0$, there are only finitely many number fields K of degree n with $|\Delta_K| \leq X$.[4]

Proof. Let K be a number field of the kind described. Introduce the region $\mathcal{R} \subseteq \mathbb{R}^n$ given as[5]

$$\{(x_1, \ldots, x_n) \in \mathbb{R}^n : |x_1| \leq \frac{1}{2}, \ldots, |x_{n-1}| \leq \frac{1}{2}, |x_n| \leq T\},$$

where $T = 2^n X^{1/2}$. Then $\mathcal{R}$ is centrally symmetric, convex, and

$$\mathrm{vol}(\mathcal{R}) = (2 \cdot \frac{1}{2})^{n-1} \cdot 2T = 2^{n+1} X^{1/2},$$

[3]Hermite, C. *Extrait d'une lettre de M. C. Hermite à M. Borchardt sur le nombre limité d'irrationalités auxquelles se réduisent les racines des équations à coefficients entiers complexes d'un degré et d'un discriminant donnés.* J. reine angew. Math. **53** (1857), 182–192.

[4]In fact, while it is customary to credit Hermite with the stronger Theorem 21.11, he only claims to prove Proposition 21.12.

[5]We really do mean $\mathbb{R}^n$ here, *not* $\mathbb{R}^{r_1} \oplus \mathbb{C}^{r_2}$. So the statement that $\iota(\alpha) \in \mathcal{R}$ is a claim about the absolute values of α under the various real embeddings, as well as a claim about the absolute values of the real and imaginary parts of α under the nonreal embeddings.

while

$$2^n \operatorname{covol}(\iota(\mathbb{Z}_K)) = 2^{n-r_2}\sqrt{|\Delta_K|} \le 2^n X^{1/2}.$$

By Minkowski's theorem, there is $\alpha \in \mathbb{Z}_K$ with $\iota(\alpha) \in \mathcal{R}$. For this α, we have

$$|\sigma(\alpha)| \le \sqrt{T^2 + \frac{1}{4}} < T + 1$$

for all embeddings σ of K into $\mathbb{C}$. Now Lemma 18.2 restricts α to a finite set of candidates, depending only on n and X. (Indeed, in the notation of Lemma 18.2, α is a root of some polynomial from the finite set $\mathcal{P}_{n,T+1}$.)

We will argue that $K = \mathbb{Q}(\alpha)$; that is, α is a primitive element for the extension $K/\mathbb{Q}$. Since there are only finitely many possible α, there are also only finitely many possible K.

Here is the main idea of the proof. We use the form of $\mathcal{R}$ to show that the image of α under $\sigma_{r_1+r_2}$ (the final embedding appearing in the definition of ι) is different from its image under every other $\sigma\colon K \hookrightarrow \mathbb{C}$. If $\mathbb{Q}(\alpha)$ were to generate a proper subfield of K, then the embeddings of K into $\mathbb{C}$ would come in groups of $[K : \mathbb{Q}(\alpha)] > 1$, each group extending a different embedding of $\mathbb{Q}(\alpha)$, and so every element in the multiset $\{\sigma(\alpha)\}$ would occur with multiplicity at least two.

To execute this plan, we take two cases according to whether $r_2 = 0$ (so that $r_1 = n$) or $r_2 > 0$.

If $r_2 = 0$, then $|\sigma_i(\alpha)| \le \frac{1}{2}$ for all $i = 1, 2, \ldots, n-1$. On the other hand,

$$\begin{aligned} |\sigma_n(\alpha)| &= |\mathrm{N}\alpha| \cdot \prod_{i=1}^{n-1} |\sigma_i(\alpha)|^{-1} \\ &\ge |\mathrm{N}\alpha| \cdot 2^{n-1} \ge 1. \end{aligned}$$

(We used here that $|\mathrm{N}\alpha|$ and 2^{n-1} are at least 1.) Thus, $\sigma_n(\alpha)$, which is $\sigma_{r_1+r_2}(\alpha)$ in this case, is distinct from all the other $\sigma(\alpha)$.

Suppose now that $r_2 > 0$. Then $|\sigma(\alpha)| \le \frac{1}{2}$ for all real embeddings σ. Moreover, for each nonreal embedding σ different from $\sigma_{r_1+r_2}$ and $\overline{\sigma_{r_1+r_2}}$, we have $|\Re\sigma(\alpha)| \le \frac{1}{2}$ and $|\Im\sigma(\alpha)| \le \frac{1}{2}$, so that $|\sigma(\alpha)| \le \frac{\sqrt{2}}{2} <$

1. Noting that

$$\begin{aligned} |\sigma_{r_1+r_2}(\alpha)|^2 &= |\overline{\sigma_{r_1+r_2}}(\alpha)|^2 \\ &= |\mathrm{N}\alpha| \prod_{i=1}^{r_1} |\sigma(\alpha)|^{-1} \prod_{j=r_1+1}^{r_1+r_2-1} |\sigma_j(\alpha)|^{-2} \geq 1, \end{aligned} \tag{21.6}$$

we see that $\sigma_{r_1+r_2}(\alpha)$ is distinct from all other $\sigma(\alpha)$ except possibly $\overline{\sigma_{r_1+r_2}}(\alpha)$. If $\sigma_{r_1+r_2}(\alpha) = \overline{\sigma_{r_1+r_2}}(\alpha)$, then $\sigma_{r_1+r_2}(\alpha)$ is real. From the definition of $\mathcal{R}$,

$$|\Re\sigma_{r_1+r_2}(\alpha)| \leq \frac{1}{2}.$$

So we would then have $|\sigma_{r_1+r_2}(\alpha)| = |\Re\sigma_{r_1+r_2}(\alpha)| \leq \frac{1}{2}$, contradicting the lower bound (21.6). □

In recent years there has been renewed interest in quantitative refinements of Hermite's theorem. Put

$$N_d(X) = \#\{\text{number fields } K : \deg K = d \text{ and } |\Delta_K| \leq X\}.$$

It is a folk conjecture, sometimes attributed to Linnik, that for each fixed $d \geq 2$,

$$\lim_{X\to\infty} \frac{N_d(X)}{X} = \delta_d$$

for some constant $\delta_d > 0$. Gauss knew this (essentially) when $d = 2$. The $d = 3$ case was settled in 1971 by Davenport and Heilbronn[6], and the $d = 4$ and $d = 5$ cases[7][8] were recently settled by Bhargava.

When d is large, only much weaker estimates of $N_d(X)$ are known. The sharpest lower bound is due to Bhargava, Shankar, and Wang[9], who prove that for each d, there is a constant $c_d > 0$ with

$$N_d(X) > c_d X^{\frac{1}{2}+\frac{1}{d}} \qquad \text{for all } X > X_0(d).$$

In fact, they prove the same lower bound for the count of monogenic, degree d number fields whose Galois closure has Galois group the full symmetric group on d letters. The strongest upper bound is due to

---

[6]Davenport, H.; Heilbronn, H. *On the density of discriminants of cubic fields. II.* Proc. Roy. Soc. London Ser. A **322** (1971), 405–420.

[7]Bhargava, M. *The density of discriminants of quartic rings and fields.* Ann. of Math. (2) **162** (2005), 1031–1063.

[8]Bhargava, M. *The density of discriminants of quintic rings and fields.* Ann. of Math. (2) **172** (2010), 1559–1591.

[9]See the reference on p. 188.

Ellenberg and Venkatesh.[10] Their result, in slightly weakened form, is that for each $\epsilon > 0$,

$$\limsup_{X\to\infty} \frac{\log N_d(X)}{\log X} \le C_\epsilon d^\epsilon.$$

Here C_ϵ is a positive constant depending only on ϵ.

Appendix: A volume verification

We now provide a proof of Proposition 21.6. It is convenient to first state the result in terms of a parameter T that is normalized differently than X.

Proposition 21.13. Let r_1 and r_2 be nonnegative integers, not both 0, and let $n = r_1 + 2r_2$. For each $T \ge 0$, let $\mathcal{R}_{r_1,r_2}(T)$ be the region in $\mathbb{R}^n$ given by

$$\{(x_1,\dots,x_n) \in \mathbb{R}^{r_1} \oplus \mathbb{C}^{r_2} : \sum_{i=1}^{r_1} |x_i| + 2\sum_{j=r_1+1}^{r_1+r_2} |x_j| \le T\}.$$

Then

$$\mathrm{vol}(\mathcal{R}_{r_1,r_2}(T)) = 2^{r_1}\left(\frac{\pi}{2}\right)^{r_2}\frac{T^n}{n!}. \tag{21.7}$$

Proof of Proposition 21.13. The proof is by double induction on r_1 and r_2. When $r_1 = 1$ and $r_2 = 0$, the region $\mathcal{R}_{r_1,r_2}$ is an interval in $\mathbb{R}$ of "radius" T, and so

$$\mathrm{vol}(\mathcal{R}_{1,0}(T)) = 2T.$$

When $r_1 = 0$ and $r_2 = 1$, the region $\mathcal{R}_{r_1,r_2}$ is a disc in $\mathbb{R}^2$ of radius $T/2$, and

$$\mathrm{vol}(\mathcal{R}_{0,1}(T)) = \frac{\pi}{4}T^2.$$

We see that (21.7) holds in both of these cases.

Suppose now that (21.7) holds for the pair (r_1, r_2) (and every $T > 0$). We prove that it also holds for $(r_1 + 1, r_2)$ and for $(r_1, r_2 + 1)$.

Observe that $\mathcal{R}_{r_1+1,r_2}(T)$ is defined by the constraints

$$|t| + \sum_{i=1}^{r_1} |x_i| + 2\sum_{j=r_1+1}^{r_1+r_2} |x_j| \le T,$$

[10] Ellenberg, J.; Venkatesh, A. *The number of extensions of a number field with fixed degree and bounded discriminant.* Ann. of Math. **163** (2006), 723–741.

where t and the x_i are real variables, and the x_j are complex variables. By integrating the cross sectional volumes as t varies, we find that

$$\begin{aligned}\operatorname{vol}(\mathcal{R}_{r_1+1,r_2}(T)) &= \int_{-T}^{T} \operatorname{vol}(\mathcal{R}_{r_1,r_2}(T-|t|))\,dt \\ &= \frac{2^{r_1}(\pi/2)^{r_2}}{n!}\int_{-T}^{T}(T-|t|)^n\,dt.\end{aligned}$$

Since

$$\int_{-T}^{T}(T-|t|)^n = 2\int_0^T (T-t)^n = 2\frac{T^{n+1}}{n+1},$$

we conclude that

$$\operatorname{vol}(\mathcal{R}_{r_1+1,r_2}(T)) = 2^{r_1+1}\left(\frac{\pi}{2}\right)^{r_2}\frac{T^{n+1}}{(n+1)!},$$

which is consistent with (21.7).

Similarly,

$$\begin{aligned}&\operatorname{vol}(\mathcal{R}_{r_1,r_2+1}(T)) \\ &= \int_{x^2+y^2\le(T/2)^2} \operatorname{vol}(\mathcal{R}_{r_1,r_2}(T-2\sqrt{x^2+y^2}))\,dx\,dy \\ &= \frac{2^{r_1}(\pi/2)^{r_2}}{n!}\int_{x^2+y^2\le(T/2)^2}(T-2\sqrt{x^2+y^2})^n\,dx\,dy.\end{aligned}$$

To continue, we change to polar coordinates ($x = r\sin\theta$, $y = r\cos\theta$); we then see that

$$\begin{aligned}&\int_{x^2+y^2\le(T/2)^2}(T-2\sqrt{x^2+y^2})^n\,dx\,dy \\ &\qquad = \int_0^{2\pi}\int_0^{T/2}(T-2r)^n\,r\,dr\,d\theta \\ &\qquad = 2\pi\int_0^T r'^n\frac{T-r'}{4}\,dr'.\end{aligned}$$

(We made the substitution $r' = T-2r$ in the last step.) Carrying out the integration reveals that this last expression is equal to

$$\frac{\pi}{2}\left(T\frac{r'^{n+1}}{n+1}-\frac{r'^{n+2}}{n+2}\right)\Big|_0^T = \frac{\pi}{2}\frac{T^{n+2}}{(n+1)(n+2)}.$$

Putting this back in above,

$$\operatorname{vol}(\mathcal{R}_{r_1,r_2+1}(T)) = 2^{r_1}\left(\frac{\pi}{2}\right)^{r_2+1}\frac{T^{n+2}}{(n+2)!},$$

and this again agrees with (21.7). □

Proof of Proposition 21.6. Take $T = nX^{1/n}$ in Proposition 21.13. □

Exercises

(1) Use Stickelberger's criterion (Exercise 13.1), Brill's theorem (Exercise 13.2), and (21.4) to determine, for every integer $\Delta \in [-12, 21]$, whether or not $\Delta = \Delta_K$ for some number field K.

(2) (a) Show that if K and L are quadratic number fields with $\Delta_K = \Delta_L$, then $K = L$.
(b) Let $K = \mathbb{Q}(\sqrt[3]{6})$ and $L = \mathbb{Q}(\sqrt[3]{12})$. Show that $\Delta_K = \Delta_L$. (You may assume Theorem 14.7.)
(c) Show that the fields K and L in (b) are not isomorphic.

(3) Show that $\mathbb{Q}(\sqrt{17})$, $\mathbb{Q}(\sqrt{21})$, $\mathbb{Q}(\sqrt{23})$, and $\mathbb{Q}(\sqrt{29})$ have class number 1.

(4) Let $K = \mathbb{Q}(\sqrt{-26})$.
(a) By referencing either the Minkowski bound or Exercise 11.3, show that $\mathrm{Cl}(\mathbb{Z}_K)$ is generated by the classes of the prime ideals above 2, 3, and 5.
(b) Check that (with the tilde denoting conjugation)

$$\langle 2\rangle = P^2, \quad \langle 3\rangle = Q\tilde{Q}, \quad \langle 5\rangle = R\tilde{R},$$

where $P = \langle 2, \sqrt{-26}\rangle$, $Q = \langle 3, 1+\sqrt{-26}\rangle$, and $R = \langle 5, 2-\sqrt{-26}\rangle$ are prime ideals.
(c) Show that $[P]$ has order 2 in $\mathrm{Cl}(\mathbb{Z}_K)$.
(d) In Exercise 4.5, you showed that Q^3 is principal. Show that Q itself is not principal, so that $[Q]$ has order 3 in $\mathrm{Cl}(\mathbb{Z}_K)$.
(e) Find a principal ideal in $\mathbb{Z}_K$ of norm 30. By ruminating on the possibilities for its prime ideal factorization, show that $\mathrm{Cl}(\mathbb{Z}_K) \cong \mathbb{Z}/6\mathbb{Z}$.

(5) Let $K = \mathbb{Q}(\sqrt{82})$.
(a) Show that $\mathrm{Cl}(\mathbb{Z}_K)$ is generated by the classes of the prime ideals above 2, 3, 5, and 7.
(b) Show that 5 and 7 remain inert in K, that 2 ramifies, and that 3 splits.
(c) Let P be the unique prime ideal above 2. Show that P is nonprincipal by proving that there is no integer solution to

$x^2 - 82y^2 = \pm 2$. Deduce that $[P]$ has order 2 in $\mathrm{Cl}(\mathbb{Z}_K)$. *Hint:* Look back at Exercise 8.6.

(d) Let Q be either of the prime ideals above 3. Starting from $10^2 - 82 \cdot 1^2 = 18$, prove that $[P] = [Q]^{-2}$ and that $[Q]$ has order 4 in $\mathrm{Cl}(\mathbb{Z}_K)$.

(e) Conclude that $\mathrm{Cl}(\mathbb{Z}_K) \cong \mathbb{Z}/4\mathbb{Z}$.

(6) Let $K = \mathbb{Q}(\sqrt[3]{7})$.

(a) Show that $\mathrm{Cl}(\mathbb{Z}_K)$ is generated by the classes of the prime ideals above $2, 3, 5$, and 7.

(b) Show that the primes in (a) factor as follows: $\langle 2 \rangle = P_1 P_2$, $\langle 3 \rangle = Q^3$, $\langle 5 \rangle = R_1 R_2$, and $\langle 7 \rangle = S^3$.

(c) Show that $\mathrm{Cl}(\mathbb{Z}_K)$ is generated by $[Q]$. *Hint:* Show that $[S]$ is trivial, and find principal ideals of norm 6 and norm 15.

(d) Show that $[Q]$ has order 3. Conclude that $\mathrm{Cl}(\mathbb{Z}_K) \cong \mathbb{Z}/3\mathbb{Z}$.

(7) Let $K = \mathbb{Q}(\alpha)$, where α is a root of $f(x) = x^3 + x^2 - 2x + 8$. (This field was studied in Chapters 14 and 17.) Prove that K has class number 1.

(8) (Connell[11]) Let $K = \mathbb{Q}(\sqrt[3]{d})$, where d is a cubefree positive integer. Here we show that if d is divisible by a prime $q \equiv 1 \pmod 3$, then $3 \mid h_K$. (Compare with Exercise 6.)

(a) Explain why there is no loss of generality in assuming that $q \mid d$ and $q^2 \nmid d$. We will make this assumption for the rest of the exercise.

(b) Show that every element of $\mathbb{Z}_K$ is congruent, modulo q, to an element of $\mathbb{Z}[\sqrt[3]{d}]$.

(c) Let p be any prime congruent to 2 modulo 3 and not dividing $[\mathbb{Z}_K : \mathbb{Z}[\sqrt[3]{d}]]$. Show that there is a degree 1 prime ideal of $\mathbb{Z}_K$ lying above p.

(d) Show that p^{h_K} is congruent, modulo q, to the norm of an element of $\mathbb{Z}[\sqrt[3]{d}]$.

(e) Show that p^{h_K} is congruent to a cube modulo q.

(f) Suppose for a contradiction that $3 \nmid h_K$. Derive from (e) that all sufficiently large primes $p \equiv 2 \pmod 3$ are congruent to a cube modulo q. Show that this contradicts the theorem

[11] Connell, I. G. *On algebraic number fields with unique factorization.* Canad. Math. Bull. 5 (1962), 151–166.

of Dirichlet concerning primes in arithmetic progressions, quoted on p. 100.

(9) Fix a positive integer d. Use our proof of Hermite's theorem to show that there is a constant $C_d > 0$ with $N_d(X) < C_d X^d$ for all $X > 0$. (Cf. the result of Ellenberg–Venkatesh quoted in the text.)

22

Dedekind's discriminant theorem

Our goal in this chapter is laser-focused: Prove the foundational theorem of Dedekind characterizing the rational primes that ramify in a given number field.

Theorem 22.1 (Dedekind's discriminant theorem)**.** Let K be a number field. For each rational prime p,

$$p \text{ ramifies in } K \iff p \mid \Delta_K.$$

We will see that the forward direction of Theorem 22.1 can be proved reasonably quickly, while the converse implication is decidedly more delicate.

Step 0

Both directions of the proof of Theorem 22.1 depend on the following elementary lemma.

Lemma 22.2 (Discriminant divisibility criterion)**.** Let K be a number field. Let p be a rational prime. Then $p \mid \Delta_K \iff$ there is an $\alpha \in \mathbb{Z}_K$ not divisible by p with

$$\mathrm{Tr}(\alpha\beta) \equiv 0 \pmod{p} \quad \text{for all } \beta \in \mathbb{Z}_K.$$

Proof. We take the forward ($\Rightarrow$) direction first. Let n be the degree of K, and let $\omega_1, \ldots, \omega_n$ be a $\mathbb{Z}$-basis for $\mathbb{Z}_K$. Recall that $\Delta_K = \det(D)$, where $D = [\mathrm{Tr}(\omega_i\omega_j)]_{1\le i,j\le n}$ (see (13.1)). If $p \mid \Delta_K$, then the columns

of D are linearly dependent modulo p. Thus, there are integers $a_1, \ldots, a_n$, not all divisible by p, with

$$\sum_{j=1}^{n} a_j \mathrm{Tr}(\omega_i \omega_j) \equiv 0 \pmod{p} \qquad \text{for all } 1 \le i \le n.$$

So if we set $\alpha = \sum_{j=1}^{n} a_j \omega_j$, then by the linearity of the trace,

$$\mathrm{Tr}(\omega_i \alpha) \equiv 0 \pmod{p} \quad \text{for all } 1 \le i \le n.$$

Appealing again to linearity,

$$\mathrm{Tr}(\beta\alpha) \equiv 0 \pmod{p}$$

whenever β is a $\mathbb{Z}$-linear combination of the ω_i. But the ω_i are a $\mathbb{Z}$-basis for $\mathbb{Z}_K$, and hence this congruence holds for all $\beta \in \mathbb{Z}_K$. Moreover, $p \nmid \alpha$, since not all of the a_j are multiples of p. This proves the forward direction of the lemma. The backward direction ($\Leftarrow$) is proved by the same argument, run in reverse (Exercise 1). □

Uno, Dos, Trace

More groundwork must be laid before we can continue with the proof of Theorem 22.1. In particular, we need a substantially reworked notion of the "trace". The trace that we are accustomed to will emerge from our discussion as a very special case.

Let F be any perfect field (for example, a field of characteristic 0 or a finite field). Let M be a finite extension of F, say $[M : F] = n$. For each $\alpha \in M$, we define the (generalized) **field polynomial** $\phi_{M/F,\alpha}(x)$ by setting

$$\phi_{M/F,\alpha}(x) = \prod_{\sigma} (x - \sigma(\alpha)),$$

where here and below σ runs over the embeddings of M into $\bar{F}$ (an algebraic closure of F) that fix F. The proof given for Proposition 13.1 carries over to show that

$$\phi_{M/F,\alpha}(x) = \min_{F,\alpha}(x)^{[M:F(\alpha)]}, \tag{22.1}$$

where $\min_{F,\alpha}(x)$ is the minimal polynomial of α over F. In particular,

$$\phi_{M/F,\alpha}(x) \in F[x].$$

Write $\phi_{M/F,\alpha}(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0$, where the $a_i \in F$. We define the **trace of α from M down to F** by

$$\mathrm{Tr}_{M/F}(\alpha) = -a_{n-1}; \tag{22.2}$$

equivalently,

$$\mathrm{Tr}_{M/F}(\alpha) = \sum_{\sigma} \sigma(\alpha).$$

It easy to see (for example, by comparing (22.1) and Proposition 13.1) that when $F = \mathbb{Q}$ this is what we are used to referring to as the trace from M. It is also straightforward to check that when M/F is Galois, $\mathrm{Tr}_{M/F}(\alpha) = \sum_{\sigma \in \mathrm{Gal}(M/F)} \sigma(\alpha)$ (Exercise 2).

There is an alternative characterization of the trace that will play an essential role in what follows. For each $\alpha \in M$, let $m_\alpha \colon M \to M$ denote the "multiplication by α" map. That is, $m_\alpha(\beta) = \alpha\beta$ (for all $\beta \in M$). Notice that if we view M as an F-vector space, then m_α defines an F-linear transformation from M to itself.

Proposition 22.3. We have

$$\mathrm{Tr}_{M/F}(\alpha) = \mathrm{Tr}(m_\alpha),$$

where the trace on the right-hand side is the linear-algebraic trace of an F-linear transformation.

Proof. Since M is n-dimensional over F, the characteristic polynomial $\chi_\alpha(x)$ (say) of m_α is a monic polynomial of degree n.[1] We will show that $\chi_\alpha(x)$ coincides with the field polynomial $\phi_{M/F,\alpha}(x)$. Since the coefficient of x^{n-1} in the characteristic polynomial of m_α is $-\mathrm{Tr}(m_\alpha)$, the proposition then follows immediately from our definition (22.2) of $\mathrm{Tr}_{M/F}(\alpha)$.

If $f(x)$ is any polynomial over F, then plugging m_α into $f(x)$ yields $m_{f(\alpha)}$. In particular, $\mathrm{min}_{F,\alpha}(m_\alpha) = m_0$, the zero linear transformation. Since $\mathrm{min}_{F,\alpha}(x)$ is irreducible, $\mathrm{min}_{F,\alpha}(x)$ must be the minimal polynomial of the transformation m_α. The characteristic and minimal polynomials of a linear transformation always share the same irreducible factors, and so $\chi_\alpha(x)$ is a power of $\mathrm{min}_{F,\alpha}(x)$. Since $\phi_\alpha(x)$ is also a power of $\mathrm{min}_{F,\alpha}(x)$ (see (22.1)), and $\deg \chi_\alpha = n = \deg \phi_\alpha$, we must have $\chi_\alpha(x) = \phi_\alpha(x)$. □

[1] Our definition of the characteristic polynomial of T is $\det(x \cdot \mathrm{Id} - T)$.

Proposition 22.3 motivates an even more general definition of the trace. Let F be any field, and let M be an F-algebra, i.e., a ring containing F as a subring.[2] Such a ring carries an obvious F-vector space structure. Suppose that $\dim_F M < \infty$. Then for each $\alpha \in M$, we define $\mathrm{Tr}_{M/F}(\alpha)$ as the trace of the multiplication by α map, again viewed as an F-linear transformation. This last definition of the trace is the one usually found in algebra books, since it subsumes all the previous special cases.

To-may-to, to-mah-to

Let K be a degree n number field, let $\gamma \in \mathbb{Z}_K$, and let p be a rational prime. Write $\mathbb{F}_p$ for $\mathbb{Z}/p\mathbb{Z}$.

Does it make sense to talk about the trace of γ from K down to $\mathbb{F}_p$? Not directly; the (characteristic zero) field K is clearly not an algebra over the (characteristic p) field $\mathbb{F}_p$! So none of the definitions of the last section apply. Nevertheless, there are two elements of $\mathbb{F}_p$ that might reasonably be considered to deserve the title "mod p trace of γ."

The first, most obvious candidate is the reduction mod p of $\mathrm{Tr}_{K/\mathbb{Q}}(\gamma)$. Here $\mathrm{Tr}_{K/\mathbb{Q}}(\cdot)$ is just the familiar trace from K. (Keep in mind that $\mathrm{Tr}_{K/\mathbb{Q}}(\gamma)$ is a rational integer, since $\gamma \in \mathbb{Z}_K$.)

Our next contestant requires a more elaborate introduction. Let R_p be the quotient ring $\mathbb{Z}_K/p\mathbb{Z}_K$. Then R_p is an n-dimensional $\mathbb{F}_p$-algebra, where $\mathbb{F}_p$ is identified with the subring of R_p generated by 1 (equivalently, with the rational integers mod $p\mathbb{Z}_K$). Our second nominee for the "mod p trace" of γ is $\mathrm{Tr}_{R_p/\mathbb{F}_p}(\gamma \bmod p)$.

Happily, everyone is a winner here; the two definitions of the "mod p trace" always yield the same element of $\mathbb{F}_p$.

Proposition 22.4. For every $\gamma \in \mathbb{Z}_K$,

$$\mathrm{Tr}_{R_p/\mathbb{F}_p}(\gamma \bmod p) = \mathrm{Tr}_{K/\mathbb{Q}}(\gamma) \bmod p.$$

[2]Remember that for us, **rings** are always commutative with 1. We also require that the subring and the ambient ring share the same 1.

Proof. Let $\omega_1, \ldots, \omega_n$ be a $\mathbb{Z}$-basis for $\mathbb{Z}_K$, and recall this implies that $\omega_1, \ldots, \omega_n$ also form a $\mathbb{Q}$-basis for K. For each $j = 1, 2, \ldots, n$, write

$$\gamma\omega_j = \sum_{i=1}^{n} c_{i,j}\omega_i, \tag{22.3}$$

where all the $c_{i,j} \in \mathbb{Z}$. Then with respect to the $\mathbb{Q}$-basis $\omega_1, \ldots, \omega_n$, the matrix $[c_{i,j}]_{1 \le i,j \le n}$ represents the $\mathbb{Q}$-linear map "multiplication by γ on K," which (consistent with our earlier notation) we will denote m_γ. Hence,

$$\mathrm{Tr}_{K/\mathbb{Q}}(\gamma) = \mathrm{Tr}(m_\gamma) = \sum_{i=1}^{n} c_{i,i}. \tag{22.4}$$

How can we get a handle on $\mathrm{Tr}_{R_p/\mathbb{F}_p}(\gamma \bmod p)$? The key is to observe that $\omega_1 \bmod p, \ldots, \omega_n \bmod p$ form an $\mathbb{F}_p$-basis for R_p. Now taking (22.3) and reducing mod p, we conclude that the $\mathbb{F}_p$-linear map of multiplication by $\gamma \bmod p$ on R_p, denoted here $m_{\gamma \bmod p}$, is represented by the matrix $[c_{i,j} \bmod p]_{1 \le i,j \le n}$. Hence,

$$\mathrm{Tr}_{R_p/\mathbb{F}_p}(\gamma \bmod p) = \mathrm{Tr}(m_{\gamma \bmod p}) = \sum_{i=1}^{n} c_{i,i} \bmod p.$$

Comparing with (22.4) proves the proposition. □

Ramified primes are discriminantal divisors

We now tackle the easier (forward) direction of Theorem 22.1. Let p be a rational prime that ramifies in K, and let $P_1, P_2, \ldots, P_g$ be the distinct prime ideals of $\mathbb{Z}_K$ that lie above p. Since some P_i appears to an exponent larger than 1 in the factorization of $p\mathbb{Z}_K$, the product $P_1 \cdots P_g$ *properly divides* $p\mathbb{Z}_K$. Thus, $P_1 \cdots P_g \supsetneq p\mathbb{Z}_K$. ("To divide is to contain.") Fix an $\alpha \in P_1 \cdots P_g$ not divisible by p. We will prove that

$$\mathrm{Tr}_{K/\mathbb{Q}}(\alpha\beta) \equiv 0 \pmod{p} \quad \text{for all } \beta \in \mathbb{Z}_K.$$

Since $p \nmid \alpha$, the discriminant divisibility criterion (Lemma 22.2) implies that $p \mid \Delta_K$, as desired.

For each $\beta \in \mathbb{Z}_K$, we write γ for the product $\alpha\beta$. By Proposition 22.4, it suffices to show that

$$\mathrm{Tr}_{R_p/\mathbb{F}_p}(\gamma \bmod p) = 0 \bmod p$$

for each $\beta \in \mathbb{Z}_K$. In other words, the $\mathbb{F}_p$-linear map $m_{\gamma \bmod p}$ (multiplication by γ mod p on R_p) has vanishing trace for every $\beta \in \mathbb{Z}_K$.

We can see this vanishing as follows. Write $p\mathbb{Z}_K = P_1^{e_1} \cdots P_g^{e_g}$, and let e be the maximum of the e_i. Since $\alpha \in P_1 \cdots P_g$, we have that

$$\langle p \rangle \mid (P_1 \cdots P_g)^e \mid \langle \alpha \rangle^e = \langle \alpha^e \rangle,$$

and hence $p \mid \alpha^e$. So if β is any element of $\mathbb{Z}_K$, then $p \mid \alpha^e \beta^e = \gamma^e$. As a consequence,

$$(m_{\gamma \bmod p})^e = m_{\gamma^e \bmod p} = m_{0 \bmod p}, \quad \text{i.e., the zero map.}$$

This shows that $m_{\gamma \bmod p}$ is nilpotent. The proof is completed by recalling that a nilpotent linear transformation always has trace 0.

Discriminantal divisors ramify

It remains to show that every prime dividing Δ_K ramifies in K. We proceed by contradiction, supposing that $p \mid \Delta_K$ but that p is unramified.

By the discriminant divisibility criterion (Lemma 22.2), we can fix an $\alpha \in \mathbb{Z}_K$, not a multiple of p, with

$$\operatorname{Tr}_{K/\mathbb{Q}}(\alpha\beta) \equiv 0 \pmod{p} \quad \text{for all } \beta \in \mathbb{Z}_K. \tag{22.5}$$

For each $\beta \in \mathbb{Z}_K$, let $\gamma = \alpha\beta$. (This is the same convention we adopted in the other direction of the proof.) Then from (22.5) and Proposition 22.4,

$$\operatorname{Tr}_{R_p/\mathbb{F}_p}(\gamma \bmod p) = 0 \bmod p \quad \text{for all } \beta \in \mathbb{Z}_K. \tag{22.6}$$

The next lemma is pivotal for understanding what (22.6) is trying to tell us. Write $p\mathbb{Z}_K = P_1 \cdots P_g$, where the P_i are distinct prime ideals. (Recall that $p\mathbb{Z}_K$ is unramified by assumption.) Put $R_{P_m} = \mathbb{Z}_K/P_m$, for $m = 1, 2, \ldots, g$. From Chapter 17, each R_{P_m} is an extension field of $\mathbb{Z}/p\mathbb{Z} = \mathbb{F}_p$ of degree $f_m := f(P_m/p)$.

Lemma 22.5. Let η be any element of $\mathbb{Z}_K$. Then

$$\operatorname{Tr}_{R_p/\mathbb{F}_p}(\eta \bmod p) = \sum_{m=1}^{g} \operatorname{Tr}_{R_{P_m}/\mathbb{F}_p}(\eta \bmod P_m). \tag{22.7}$$

Proof. By definition, the left-hand side of (22.7) is the trace of the $\mathbb{F}_p$-linear map $m_{\eta \bmod p}$ (multiplication by η on R_p). Our plan is to relate this to the right-hand side by computing said trace with respect to an $\mathbb{F}_p$-basis of R_p carefully assembled from $\mathbb{F}_p$-bases for the $\mathbb{F}_p$-algebras R_{P_m}.

The key to making all this work is the Chinese remainder theorem, which tells us that (via the canonical reduction maps)

$$\begin{aligned} R_p = \mathbb{Z}_K/p\mathbb{Z}_K &\cong \mathbb{Z}_K/P_1 \oplus \mathbb{Z}_K/P_2 \oplus \cdots \oplus \mathbb{Z}_K/P_g \\ &= R_{P_1} \oplus R_{P_2} \oplus \cdots \oplus R_{P_g}. \end{aligned} \tag{22.8}$$

We choose $\theta_1, \dots, \theta_{f_1} \in \mathbb{Z}_K$ whose mod P_1 reductions form an $\mathbb{F}_p$-basis for R_{P_1}, and whose reductions mod $P_2, \dots, P_g$ all vanish. (The existence of such θ_i follows from the surjectivity of the isomorphism in (22.8).) Next, we choose $\theta_{f_1+1}, \dots, \theta_{f_1+f_2} \in \mathbb{Z}_K$ whose mod P_2 reductions form an $\mathbb{F}_p$-basis for R_{P_2}, and whose reductions mod $P_1, P_3, \dots, P_g$ vanish. Continuing the process in the obvious way, we end up with $f_1 + \cdots + f_g = n$ elements $\theta_1, \dots, \theta_n \in \mathbb{Z}_K$. By (22.8), the mod p reductions of $\theta_1, \dots, \theta_n$ form an $\mathbb{F}_p$-basis for R_p.

What is the trace of $m_{\eta \bmod p}$ with respect to this basis? For each $j = 1, 2, \dots, n$, write

$$\eta\theta_j \equiv \sum_{i=1}^{n} c_{i,j}\theta_i \pmod{p}, \tag{22.9}$$

where the $c_{i,j}$ are rational integers. (The $c_{i,j}$ are not unique, but they are unique mod p.) Then the matrix representing $m_{\eta \bmod p}$ is $[c_{i,j} \bmod p]_{1 \le i,j \le n}$, and so

$$\mathrm{Tr}_{R_p/\mathbb{F}_p}(\eta \bmod p) = \sum_{i=1}^{n} c_{i,i} \bmod p. \tag{22.10}$$

To bring the right-hand side of (22.7) into the picture, we observe that since each P_m divides $p\mathbb{Z}_K$, the congruence (22.9) is also valid if taken mod P_m instead of mod p. The only θ_i which are nonvanishing mod P_m are those with

$$f_1 + \cdots + f_{m-1} < i \le f_1 + \cdots + f_m, \tag{22.11}$$

and these θ_i form an $\mathbb{F}_p$-basis for R_{P_m}. Interpreting (22.9) mod P_m, we conclude that the multiplication by η mod P_m map on R_{P_m} has trace

$$\sum_i c_{i,i} \bmod p,$$

where i runs over the interval (22.11). Finally, summing on m yields

$$\sum_{m=1}^{g} \mathrm{Tr}_{R_{P_m}/\mathbb{F}_p}(\eta \bmod P_m) = \sum_{i=1}^{n} c_{i,i} \bmod p;$$

comparing with (22.10) completes the proof. □

Getting back to the situation at hand, (22.6) and Lemma 22.5 together show that

$$\sum_{m=1}^{g} \mathrm{Tr}_{R_{P_m}/\mathbb{F}_p}(\gamma \bmod P_m) = 0 \bmod p, \tag{22.12}$$

for all $\beta \in \mathbb{Z}_K$. (Recall our agreement that $\gamma = \alpha\beta$.) We will use the fact that α is not divisible by p to argue that this is impossible.

Since $p \nmid \alpha$, we know that some P_i does not contain α. Without loss of generality, we can assume that $\alpha \notin P_1$. Let γ_1 be an element of $\mathbb{Z}_K$ selected so that

$$\mathrm{Tr}_{R_{P_1}/\mathbb{F}_p}(\gamma_1 \bmod P_1) \neq 0; \tag{22.13}$$

we defer the proof of the existence of γ_1 to the end of this section. Using the Chinese remainder theorem once more, we choose $\beta \in \mathbb{Z}_K$ with

$$\alpha\beta \equiv \gamma_1 \pmod{P_1}, \quad \text{and} \quad \beta \equiv 0 \pmod{P_2P_3\cdots P_g};$$

the assumption that $\alpha \notin P_1$ is used here to ensure that the first congruence has a solution. Then

$$\begin{aligned}\sum_{m=1}^{g} \mathrm{Tr}_{R_{P_m}/\mathbb{F}_p}(\gamma \bmod P_m) &= \sum_{m=1}^{g} \mathrm{Tr}_{R_{P_m}/\mathbb{F}_p}(\alpha\beta \bmod P_m)\\ &= \mathrm{Tr}_{R_{P_1}/\mathbb{F}_p}(\gamma_1 \bmod P_1) + \sum_{m=2}^{g} \mathrm{Tr}_{R_{P_m}/\mathbb{F}_p}(0 \bmod P_m)\\ &= \mathrm{Tr}_{R_{P_1}/\mathbb{F}_p}(\gamma_1 \bmod P_1) \neq 0 \bmod p.\end{aligned}$$

This contradicts (22.12) and thereby completes the proof of the theorem (phew!).

Well, almost. We have one debt outstanding, namely showing the existence of $y_1 \bmod P_1$ satisfying (22.13). That falls out as a special case of the following lemma.

Lemma 22.6. Let ℓ/k be an extension of finite fields. Then there is an $\alpha \in \ell$ with $\mathrm{Tr}_{\ell/k}(\alpha) \neq 0$.

(For our application, take $\ell = R_{P_1}$ and $k = \mathbb{F}_p$.)

Proof. Let $q = \#k$ and let $f = [\ell : k]$, so that $\#\ell = q^f$. From the theory of finite fields, ℓ/k is Galois, with the elements of $\mathrm{Gal}(\ell/k)$ given by the q^jth power maps, for $j = 0, 1, \ldots, f-1$. Hence (see Exercise 2),

$$\begin{aligned}\mathrm{Tr}_{\ell/k}(\alpha) &= \sum_{\sigma \in \mathrm{Gal}(\ell/k)} \sigma(\alpha) \\ &= \alpha + \alpha^q + \cdots + \alpha^{q^{f-1}}.\end{aligned}$$

We wish to show that this last expression is nonvanishing for some $\alpha \in \ell$. But this is clear, since the polynomial $x + x^q + \cdots + x^{q^{f-1}}$ has at most q^{f-1} roots in ℓ, whereas $\#\ell = q^f$. For a different proof (in a more general context), see Exercise 3. □

Full disclosure

Theorem 22.1 tells the truth, but not the whole truth, about ramification and the discriminant. Here is a more precise result, again due to Dedekind. Write $p\mathbb{Z}_K = \prod_{i=1}^{g} P_i^{e(P_i/p)}$, where $P_1, \ldots, P_g$ are the distinct prime ideals of $\mathbb{Z}_K$ lying above p. Then

$$p^{\sum_{i=1}^{g}(e(P_i/p)-1)f(P_i/p)} \mid \Delta_K;$$

moreover, the exponent on p is sharp if and only if all the ramification indices $e(P_i/p)$ are coprime to p. A proof can be found in §3.12 (pp. 94–101) of Koch's *Number theory*.[3]

[3] Koch, H. *Number theory. Algebraic numbers and functions.* Graduate Studies in Mathematics, **24**. American Mathematical Society, Providence, RI, 2000.

Exercises

(1) Prove the backward direction of the discriminant divisibility criterion (Lemma 22.2).

(2) Let F be a perfect field, and let M/F be a (finite) Galois extension. Prove that $\mathrm{Tr}_{M/F}(\alpha) = \sum_{\sigma \in \mathrm{Gal}(M/F)} \sigma(\alpha)$ for all $\alpha \in M$.

(3) Let F be a perfect field, and let M be a finite extension of F. In this exercise, we show that there is always an element $\gamma \in M$ with $\mathrm{Tr}_{M/F}(\gamma) \neq 0$. We proceed by contradiction, assuming that $\mathrm{Tr}_{M/F}(\cdot)$ vanishes identically.

(a) Let $\bar{F}$ be a fixed algebraic closure of F. With $n = [M : F]$, let $\sigma_1, \ldots, \sigma_n$ be the distinct embeddings of M into $\bar{F}$ fixing F. (The existence of n distinct embeddings follows from the separability of M/F.) For each n-tuple $\omega_1, \ldots, \omega_n \in M$, put

$$\Delta_{M/F}(\omega_1, \ldots, \omega_n) = \det([\sigma_i(\omega_j)]_{1 \leq i,j \leq n})^2.$$

Show that $\Delta_{M/F}(\omega_1, \ldots, \omega_n)$ is also given by

$$\det([\mathrm{Tr}_{M/F}(\omega_i \omega_j)]_{1 \leq i,j \leq n}).$$

(b) In view of (a), our assumption that $\mathrm{Tr}_{M/F}(\cdot)$ is identically zero implies that $\Delta_{M/F}(\cdot, \ldots, \cdot)$ is as well. Obtain a contradiction by showing that

$$\Delta_{M/F}(1, \alpha, \ldots, \alpha^{n-1}) \neq 0$$

if α is a primitive element for M/F. (Remember that such an α exists since M/F is separable.)

(4) (Stickelberger[4]) Let K be a degree n number field, and let p be an odd prime unramified in K. By Theorem 22.1, $p \nmid \Delta_K$. This exercise outlines a proof of the remarkable formula

$$\left(\frac{\Delta_K}{p}\right) = (-1)^{n-g}, \tag{22.14}$$

where the left-hand side is a Legendre symbol and g is the number of prime ideals of $\mathbb{Z}_K$ lying above p.

You will need the following special case of the **normal basis theorem**: *If ℓ/k is an extension of finite fields, with $\#k = q$ and*

[4]Stickelberger, L. *Über eine neue Eigenschaft der Diskriminanten algebraischer Zahlkörper.* Proceedings of the First International Congress of Mathematicians, Zürich (1897), 182–193.

$\#\ell = q^f$, then there is an $\alpha \in \ell$ for which $\alpha, \alpha^q, \ldots, \alpha^{q^{f-1}}$ form a k-basis for ℓ.[5]

(a) Write $p\mathbb{Z}_K = P_1 \cdots P_g$, where the P_i are distinct prime ideals of respective degrees f_i. Show that there are $\omega_1, \ldots, \omega_n \in \mathbb{Z}_K$ such that
- $\omega_1 \bmod p, \ldots, \omega_n \bmod p$ form an $\mathbb{F}_p$-basis for the $\mathbb{F}_p$-algebra $\mathbb{Z}_K/p\mathbb{Z}_K$,
- the pth power map on $\mathbb{Z}_K/p\mathbb{Z}_K$ acts as a permutation on $\omega_1 \bmod p, \ldots, \omega_n \bmod p$, and this permutation decomposes as a product of g disjoint cycles of lengths $f_1, \ldots, f_g$.

(b) Let $\omega_1, \ldots, \omega_n$ be as in (a). Show that

$$\Delta(\omega_1, \ldots, \omega_n) = \Delta_K \cdot u^2,$$

where u is an integer not divisible by p.

(c) Write $D_{\theta_1,\ldots,\theta_n}$ for the $n \times n$ matrix $[\sigma_i(\theta_j)]_{1\le i,j\le n}$, so that $\Delta(\theta_1, \ldots, \theta_n) = \det(D_{\theta_1,\ldots,\theta_n})^2$. Show that modulo p,

$$\det(D_{\omega_1,\ldots,\omega_n})^p \equiv (-1)^{n-g} \det(D_{\omega_1,\ldots,\omega_n}).$$

Here the congruence is meant over the ring $\bar{\mathbb{Z}}$ of all algebraic integers. *Hint:* $\det(D_{\omega_1,\ldots,\omega_n})^p \equiv \det(D_{\omega_1^p,\ldots,\omega_n^p})$.

(d) From (b) and (c), and Euler's criterion for quadratic residues, deduce that

$$\left(\frac{\Delta_K}{p}\right) \equiv (-1)^{n-g} \pmod{p},$$

where the congruence is again intended over $\bar{\mathbb{Z}}$.

(e) Explain why $1 \not\equiv -1 \pmod{p}$ in $\bar{\mathbb{Z}}$. Use this fact to complete the proof of (22.14).

The remaining exercises assume familiarity with the following fact from commutative algebra: For any ring A,

$$\{\text{nilpotent elements of } A\} = \bigcap_{P \text{ prime}} P,$$

[5]The full normal basis theorem asserts that if L/K is any (finite) Galois extension of fields, then there is an $\alpha \in L$ whose Galois conjugates form a K-basis for L. See, e.g., pp. 120–122 of: Lorenz, F. *Algebra. Vol. 1.* Universitext. Springer, New York, 2006.

where on the right P runs over all prime ideals of A.[6]

(5) Let F be a number field, and let p be a rational prime. Show that p is unramified in $F \iff$ there is a $j \in \mathbb{Z}^+$ such that $\alpha^{p^j} \equiv \alpha \pmod{p}$ for all $\alpha \in \mathbb{Z}_F$.

(6) Let K and L be number fields. Suppose that p is a rational prime unramified in both K and L.

(a) Show that

$$\{\alpha \in \mathbb{Z}_{KL} : \alpha^{p^j} \equiv \alpha \bmod p \text{ for some } j \in \mathbb{Z}^+\}$$

is a subring of $\mathbb{Z}_{KL}$ containing $\mathbb{Z}_K$ and $\mathbb{Z}_L$.

(b) Let R be the subring of $\mathbb{Z}_{KL}$ generated by $\mathbb{Z}_K$ and $\mathbb{Z}_L$. Using (a), prove that R/pR has no nonzero nilpotent elements.

(c) Show that R is free of rank $[KL : \mathbb{Q}]$ as a $\mathbb{Z}$-module. *Hint:* To bound the rank from below, show that the $\mathbb{Q}$-span of R is all of KL.

(d) Let $A = R/pR$. Let $M_1, \dots, M_g$ be the distinct maximal ideals of A. Show that $\bigcap_{i=1}^{g} M_i = \{0\}$. *Hint:* First show that there is no distinction between maximal ideals and prime ideals of A.

(e) Deduce from the Chinese remainder theorem that

$$A \cong \bigoplus_{i=1}^{g} A/M_i.$$

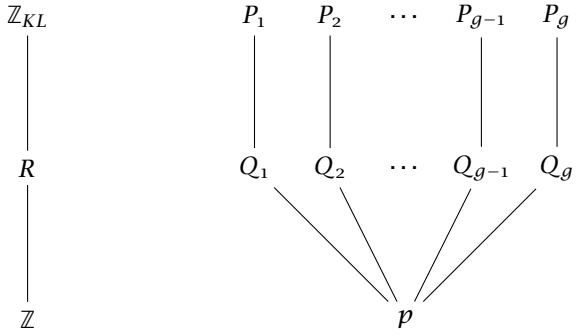
(f) Show that there are positive integers $f_1, \dots, f_g$ with $\#A/M_i = p^{f_i}$ for each i, and $f_1 + \cdots + f_g = n$.

(g) As is well-known, the maximal ideals of $A = R/pR$ correspond bijectively to the maximal ideals of R containing p. Let Q_i be the maximal ideal of R corresponding to M_i (so that Q_i is the inverse image of M_i under reduction mod p). Show that none of the extensions $Q_i\mathbb{Z}_{KL}$ (for $i = 1, 2, \dots, g$) are the unit ideal of $\mathbb{Z}_{KL}$. *Hint:* Suppose for a contradiction that $Q_i\mathbb{Z}_{KL} = \mathbb{Z}_{KL}$. Choose $\beta_1, \dots, \beta_m$ generating $\mathbb{Z}_{KL}$ as a $\mathbb{Z}$-module. Show that there is an $m \times m$ matrix U, with all entries from Q_i, having $[\beta_1, \dots, \beta_m] = [\beta_1, \dots, \beta_m]U$. Now finish as in the proof of Lemma 15.4.

---

[6] See, e.g., pp. 673–674 of: Dummit, D. S.; Foote, R. M. *Abstract algebra.* Third edition. John Wiley & Sons, Inc., Hoboken, NJ, 2004.

Figure 22.1. Diagram of maximal ideals appearing in Exercise 6. Here $Q_i \cap \mathbb{Z} = p\mathbb{Z}$ for all $i = 1, 2, \ldots, g$, while $P_i \cap R = Q_i$ for all $i = 1, 2, \ldots, g$.



(h) By (g), we can choose maximal ideals $P_1, \ldots, P_g$ of $\mathbb{Z}_{KL}$ containing $Q_1, \ldots, Q_g$, respectively. (Remember that in any ring, every nonunit ideal is contained in a maximal ideal.) Show that in any such choice, the P_i are distinct.

(i) Show that for each $i = 1, 2, \ldots, g$, there is an embedding of R/Q_i into $\mathbb{Z}_{KL}/P_i$. Deduce that $\#\mathbb{Z}_{KL}/P_i \geq p^{f_i}$.

(j) Conclude that $p\mathbb{Z}_{KL} = P_1 \cdots P_g$, and that each P_i has exact residual degree f_i (with f_i as defined in part f).

Since the P_i are distinct, one upshot of Exercise 6 is: If p is unramified in K and L, then p is unramified in their composite KL.

(7) Let F be a number field, and let p be a rational prime. Show that p splits completely in $F \iff \alpha^p \equiv \alpha \pmod{p}$ for all $\alpha \in \mathbb{Z}_F$.

(8) Let K and L be number fields. Show that if p is a rational prime that splits completely in both K and L, then p splits completely in KL. *Hint:* Since "split completely" $\Rightarrow$ "unramified", we can apply the results of Exercise 6. In the notation of that problem, show that every element of A/M_i is its own pth power, for all $i = 1, 2, \ldots, g$. Deduce that $f_1 = f_2 = \cdots = f_g = 1$.

23

The quadratic Gauss sum

> What is written [in the *Disquisitiones*] is rigorously proved there, but what follows, i.e., the determination of the sign, is exactly what has tortured me all the time. This shortcoming spoiled everything else that I found; and hardly a week passed during the last four years where I have not made this or that vain attempt to untie that knot — especially vigorously during recent times. But all this brooding and searching was in vain, sadly I had to put the pen down again. Finally, a few days ago, it has been achieved — but not by my cumbersome search, rather through God's good grace, I am tempted to say. As the lightning strikes the riddle was solved; I myself would be unable to point to a guiding thread between what I knew before, what I had used in my last attempts, and what made it work. – Gauss to Olbers, 1805[1]

Let q be an odd prime, and let $\zeta = e^{2\pi i/q}$. The **quadratic Gauss sum** attached to q is the complex number

$$G := \sum_{a \bmod q} \left(\frac{a}{q}\right) \zeta^a.$$

[1]Translation from: Patterson, S. J. *Gauss sums.* In: The shaping of arithmetic after C. F. Gauss's Disquisitiones arithmeticae, 505–528, Springer, Berlin, 2007.

Here the subscript on the sum indicates that a runs over an arbitrary complete residue system modulo q.

G makes its first appearance in the seventh (and final) section of Gauss's *Disquisitiones*, where can also read a proof of the next proposition.[2] In what follows, we write q^* for $(-1)^{(q-1)/2}q$; thus, $q^* = \pm q$, with the sign chosen so that $q^* \equiv 1 \pmod 4$.

Proposition 23.1. $G^2 = q^*$.

Proof. We expand the squared sum;

$$\begin{aligned} G^2 &= \left(\sum_{a \bmod q} \left(\frac{a}{q}\right)\zeta^a \right) \cdot \left(\sum_{b \bmod q} \left(\frac{b}{q}\right)\zeta^b \right) \\ &= \sum_{c \bmod q} \zeta^c \sum_{\substack{a,b \bmod q \\ a+b\equiv c \pmod q}} \left(\frac{ab}{q}\right) \\ &= \sum_{c \bmod q} \zeta^c \sum_{\substack{a \bmod q \\ a\not\equiv 0 \pmod q}} \left(\frac{a(c-a)}{q}\right). \end{aligned}$$

In the last step, we have removed the term $a \equiv 0 \pmod q$, which makes a vanishing contribution. When $c \equiv 0$, each of the $q-1$ terms of the final inner sum takes the value $\left(\frac{-1}{q}\right)$. Thus,

$$G^2 = \left(\frac{-1}{q}\right)(q-1) + \sum_{\substack{c \bmod q \\ c\not\equiv 0 \pmod q}} \zeta^c \sum_{\substack{a \bmod q \\ a\not\equiv 0 \pmod q}} \left(\frac{a(c-a)}{q}\right). \tag{23.1}$$

To evaluate the new inner sum, notice that

$$\left(\frac{a(c-a)}{q}\right) = \left(\frac{a^2}{q}\right)\left(\frac{a^{-1}(c-a)}{q}\right) = \left(\frac{ca^{-1}-1}{q}\right),$$

where inverses here are meant modulo q. As a runs through the nonzero residue classes mod q, so does ca^{-1}. Hence, the quantity

[2] See Art. 356. There he writes that "these theorems are so elegant they deserve special note."

$ca^{-1} - 1$ runs over the residue classes $\not\equiv -1 \pmod q$, and

$$\sum_{\substack{a \bmod q \\ a \not\equiv 0 \pmod q}} \left(\frac{a(c-a)}{q}\right) = \left(\left(\frac{0}{q}\right) + \left(\frac{1}{q}\right) + \cdots + \left(\frac{q-1}{q}\right)\right) - \left(\frac{-1}{q}\right) = -\left(\frac{-1}{q}\right).$$

Putting this in above,

$$\sum_{\substack{c \bmod q \\ c \not\equiv 0 \pmod q}} \zeta^c \sum_{\substack{a \bmod q \\ a \not\equiv 0 \pmod q}} \left(\frac{a(c-a)}{q}\right) = -\left(\frac{-1}{q}\right) \sum_{\substack{c \bmod q \\ c \not\equiv 0 \pmod q}} \zeta^c = \left(\frac{-1}{q}\right).$$

(The last step follows from the Vieta relations, since the numbers ζ^c are the roots of $x^{q-1} + x^{q-2} + \cdots + 1$.) Inserting this into (23.1), and recalling that $\left(\frac{-1}{q}\right) = (-1)^{(q-1)/2}$, shows that $G^2 = \left(\frac{-1}{q}\right) q = q^*$, as desired. □

Quadratic reciprocity

Section VII of Gauss's *Disquisitiones* is a detailed investigation into what have come to be called "Gaussian periods", of which our friend G is one example (after renormalization).[3] By developing the properties of Gaussian periods, Gauss was led to his own version of Galois theory for the subfields of $\mathbb{Q}(\zeta)$ a decade before Galois was born. As an application, he proved the following theorem, which has become a staple of many a course in modern algebra: The regular n-gon is constructible by straightedge and compass whenever $\varphi(n)$ (Euler's totient) is a power of 2.[4]

Gauss's investigations in §VII were also motivated by a passionate interest in higher reciprocity laws. Quite early in his mathematical

[3] Let d be a divisor of $q-1$. Then there is a unique subfield F of $\mathbb{Q}(\zeta)$ with $[\mathbb{Q}(\zeta) : F] = d$. What Gauss calls the **fundamental d-nomial period** $\eta_0^{(d)}$ is the trace of ζ from $\mathbb{Q}(\zeta)$ down to F; a general d-nomial period is any conjugate of $\eta_0^{(d)}$. Our G is $2\eta_0^{(q-1)/2} + 1$.

[4] For a recent exposition of this material, following Gauss's approach, see Chapter 2 of: Pollack, P. *Not always buried deep: A second course in elementary number theory.* American Mathematical Society, Providence, RI, 2009.

career, Gauss realized that the quadratic Gauss sums studied in this chapter could be used to fashion a simple proof of the law of quadratic reciprocity. (A proof along these lines was written for the *Disquisitiones*, but was cut when the manuscript was abridged prepublication.) Gauss was convinced that understanding generalized sums of this sort would pave the way for proofs of higher reciprocity laws. As usual, his instincts were spot on. In the first half of the 19th century, cubic and biquadratic reciprocity laws were proved (by Eisenstein, Jacobi, and — the history is a bit murky — possibly Gauss himself), and generalized Gauss sums play the central role in the arguments. A masterful exposition of this material can be found in the book of Ireland and Rosen.[5] (Cf. Exercises 6–8.)

In this section, we use Proposition 23.1 to give a quick proof of the quadratic reciprocity law. The argument we present is a version of Gauss's sixth proof of that law and is taken from §6.3 of Ireland and Rosen's book (ibid.).

Theorem 23.2 (Law of quadratic reciprocity)**.** Let p and q be distinct odd primes. Then

$$\left(\frac{p}{q}\right) = \left(\frac{q^*}{p}\right). \tag{23.2}$$

This form of the reciprocity law may be initially strange-seeming, but it is easily seen to be equivalent to the more familiar symmetric version. Indeed, applying once more Euler's result that $\left(\frac{-1}{r}\right) = (-1)^{(r-1)/2}$, we find that

$$\left(\frac{q^*}{p}\right) = \left(\frac{(-1)^{\frac{q-1}{2}}q}{p}\right) = \left(\frac{-1}{p}\right)^{\frac{q-1}{2}}\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}\left(\frac{q}{p}\right).$$

Substituting this for the right-hand side of (23.2), Theorem 23.2 reduces to the usual textbook statement of quadratic reciprocity.

The proof of Theorem 23.2 requires an observation about the effect on G incurred by replacing ζ with a different primitive qth root

[5] Ireland, K.; Rosen, M. *A classical introduction to modern number theory.* Second edition. Graduate Texts in Mathematics, **84**. Springer-Verlag, New York, 1990.

of 1. For each integer m prime to q, put

$$G_m = \sum_{a \bmod q} \left(\frac{a}{q}\right)\zeta^{am}.$$

Since q is prime and $q \nmid m$, as a runs through a complete residue system modulo q, so does am. Hence,

$$\left(\frac{m}{q}\right)G_m = \sum_{a \bmod q} \left(\frac{am}{q}\right)\zeta^{am} = G;$$

multiplying through by $\left(\frac{m}{q}\right)$ yields

$$G_m = \left(\frac{m}{q}\right)G. \tag{23.3}$$

Now let p be an odd prime, $p \neq q$. We work in the ring of integers $\mathbb{Z}_K$ of $K = \mathbb{Q}(\zeta_q)$. Then, with the congruence being mod p,

$$\begin{aligned} G^p &= \left(\sum_{a \bmod q} \left(\frac{a}{q}\right)\zeta^a\right)^p \\ &\equiv \sum_{a \bmod q} \left(\frac{a}{q}\right)^p \zeta^{ap} = G_p = \left(\frac{p}{q}\right)G. \end{aligned} \tag{23.4}$$

On the other hand, Proposition 23.1 implies that

$$G^p = (q^*)^{(p-1)/2}G;$$

hence, applying Euler's criterion for quadratic residues,

$$G^p \equiv \left(\frac{q^*}{p}\right)G \pmod{p}. \tag{23.5}$$

Comparing (23.4) and (23.5) shows that $\left(\frac{p}{q}\right)G \equiv \left(\frac{q^*}{p}\right)G$, mod p. We multiply through by G and then by the inverse of q^* mod p to conclude that

$$\left(\frac{p}{q}\right) \equiv \left(\frac{q^*}{p}\right) \pmod{p}.$$

To prove Theorem 23.2, it remains to promote this congruence modulo p to an equality of integers. Since both $\left(\frac{p}{q}\right)$ and $\left(\frac{q^*}{p}\right)$ are ± 1, this amounts to showing that

$$1 \not\equiv -1 \pmod{p}.$$

Of course, this last assertion is obvious in $\mathbb{Z}$, but we are working in $\mathbb{Z}_K$. Even so, it is not so bad: If $1 \equiv -1 \pmod{p}$, then $p \mid 2$ in $\mathbb{Z}_K$, and so

$$\frac{2}{p} \in \mathbb{Z}_K \cap \mathbb{Q} \subseteq \bar{\mathbb{Z}} \cap \mathbb{Q} = \mathbb{Z}.$$

But this is clearly impossible since p is an odd prime. This completes the proof of Theorem 23.2.

A similar method allows one to prove the supplementary law characterizing when 2 is a square modulo an odd prime p, namely

$$\left(\frac{2}{p}\right) = \begin{cases} 1 & \text{if } p \equiv \pm 1 \pmod{8}, \\ -1 & \text{if } p \equiv \pm 3 \pmod{8}. \end{cases} \tag{23.6}$$

We sketch the argument. Let $\zeta_8 = e^{2\pi i/8}$. It is straightforward to check that

$$\zeta_8 + \zeta_8^{-1} = \pm\sqrt{2}.$$

(Square both sides. In fact, elementary trigonometry shows that the $+$ sign is correct, but that is not needed for the argument.) View this identity as taking place in $\mathbb{Z}_K$, where $K = \mathbb{Q}(\zeta_8)$. Raise both sides to the pth power and analyze the results modulo p. The details are left as Exercise 1.

Signs and wonderings

Recall our convention that when $n < 0$, the symbol "$\sqrt{-n}$" denotes the complex number $i\sqrt{n}$.

By Proposition 23.1, for any odd prime q,

$$G = \pm\sqrt{q^*}.$$

It is natural to wonder which choice of sign is correct. In his *Disquisitiones* (Art. 356), Gauss asserts that the $+$ sign should always be taken. That is:

Theorem 23.3. $G = \sqrt{q^*}$.

No proof is given:

> These matters are on a higher level of investigation, and we will reserve their consideration for another occasion.

We know — both from Gauss's letter to Olbers quoted at the start of this chapter, and from his mathematical diary[6] — that Gauss had no proof of Theorem 23.3 until four years later, in 1805.

One explanation for the difficulties is that any proof of Theorem 23.3 must use not only algebraic ideas but also analytic ones. Indeed, ζ and ζ^m, when $q \nmid m$, are algebraically indistinguishable, both being roots of the irreducible polynomial $\Phi_q(x)$. But replacing ζ with ζ^m has the effect of replacing G with $G_m = \left(\frac{m}{q}\right)G$, so that the analogue of Theorem 23.3 becomes false when m is a quadratic nonresidue.

In the remainder of this chapter, we present a proof of Theorem 23.3 based on ideas of Cauchy and Kronecker. See Chapter 11 of Rademacher's *Lectures on elementary number theory* for a clean exposition of Gauss's original argument.[7] Four more proofs (due to Dirichlet, Kronecker, Schur, and Mertens) are discussed in the first volume of Landau's *Vorlesungen*.[8] Some applications of Theorem 23.3 are presented in Chapter 26.

A warm-up

For each odd prime q, define the **mock Gauss sum** $\tilde{G}$ by

$$\tilde{G} = \prod_{k=1}^{(q-1)/2} (\zeta^{2k-1} - \zeta^{-(2k-1)}).$$

(One reason for the adjective "mock" is that this is a product, not a sum!) The next result is the "mock" analogue of Proposition 23.1.

Lemma 23.4. $\tilde{G}^2 = q^*$.

Proof. It is an easy exercise to check that the numbers $\pm(4k-2)$, for $k = 1, 2, \ldots, \frac{q-1}{2}$, run over a complete set of nonzero residue classes

[6] see: Gray, J. J. *A commentary on Gauss's mathematical diary, 1796–1814*, with an English translation. Exposition. Math. **2** (1984), no. 2, 97–130. Entry [123] from 1805 reads: "The proof of the most charming theorem recorded above, May 1801, which we have sought to prove for 4 years and more with every effort, at last perfected."

[7] Rademacher, H. *Lectures on elementary number theory.* Blaisdell, New York-Toronto-London, 1964.

[8] See Chapter VI in: Landau, E. *Elementary number theory.* Translated by J. E. Goodman. Chelsea Publishing Co., New York, N.Y., 1958.

modulo q. Thus,

$$\prod_{k=1}^{(q-1)/2} (1-\zeta^{4k-2})(1-\zeta^{-(4k-2)}) = \prod_{j=1}^{q-1}(1-\zeta^j) = q.$$

Take the kth pair of factors in the leftmost product and multiply the first term in each pair by $-\zeta^{-(2k-1)}$ and the second by ζ^{2k-1}. Since $-\zeta^{-(2k-1)} \cdot \zeta^{2k-1} = -1$, this results in $\frac{q-1}{2}$ sign changes, so that

$$\prod_{k=1}^{(q-1)/2} (\zeta^{2k-1} - \zeta^{-(2k-1)})^2 = (-1)^{(q-1)/2} q = q^*;$$

this is precisely the claim of the lemma. □

Thus, $\tilde{G} = \pm\sqrt{q^*}$. We now show that in the "mock" setting, the + sign always holds.

Lemma 23.5 (sign of the mock Gauss sum)**.** $\tilde{G} = \sqrt{q^*}$.

It should not be surprising that Lemma 23.5 is simpler to prove than Theorem 23.3. After all, signs of products are easier to understand than signs of sums.

Proof. The kth factor in the definition of $\tilde{G}$ is

$$\begin{aligned}\zeta^{2k-1} - \zeta^{-(2k-1)} &= e^{(4k-2)\pi i/q} - e^{-(4k-2)\pi i/q} \\ &= 2i \sin\frac{(4k-2)\pi}{q}.\end{aligned}$$

Hence,

$$\prod_{k=1}^{(q-1)/2} (\zeta^{2k-1} - \zeta^{-(2k-1)}) = 2^{(q-1)/2} i^{(q-1)/2} \prod_{k=1}^{(q-1)/2} \sin\frac{(4k-2)\pi}{q}.$$

The sin factors are positive for $k \le \frac{q+2}{4}$ and negative for $\frac{q+2}{4} < k \le \frac{q-1}{2}$. (This is the only "analysis" needed for the proof.) If q has the form $4j+1$, then $i^{(q-1)/2} = i^{2j} = (-1)^j$, while

$$\operatorname{sgn} \prod_{k=1}^{(q-1)/2} \sin\frac{(4k-2)\pi}{q} = (-1)^{\lfloor \frac{q-1}{2} \rfloor - \lfloor \frac{q+2}{4} \rfloor} = (-1)^{2j-j} = (-1)^j.$$

Therefore, $\prod_{k=1}^{(q-1)/2}(\zeta^{2k-1} - \zeta^{-(2k-1)})$ is a positive real number. Now Lemma 23.4 implies that $\tilde{G} = \sqrt{q}$.

When $q = 4j + 3$, similar arguments show that $\tilde{G}$ is a positive multiple of i. By Lemma 23.4, $\tilde{G} = i\sqrt{q} = \sqrt{q^*}$. □

Think globally, act locally

We know that $G = \pm\tilde{G}$, since both square to q^*. To prove Theorem 23.3, it suffices (in view of Lemma 23.5) to show that the + sign is correct. This will be accomplished by proving that G and $\tilde{G}$ agree modulo a large power of $\pi := \zeta - 1$. In the subsequent arguments, K always denotes the field $\mathbb{Q}(\zeta)$.

Lemma 23.6. $\langle\pi\rangle$ is a prime ideal of $\mathbb{Z}_K$ lying above q. Moreover,

$$\langle q\rangle = \langle\pi\rangle^{q-1}.$$

Proof. Our starting point is the familiar factorization

$$q = \prod_{k=1}^{q-1}(\zeta^k - 1). \tag{23.7}$$

(With $1 - \zeta^k$ instead of $\zeta^k - 1$, we have seen (23.7) many times; the sign changes are inconsequential since $(-1)^{q-1} = 1$.) Since $\frac{\zeta^k-1}{\zeta-1} = \zeta^{k-1} + \zeta^{k-2} + \cdots + 1 \in \mathbb{Z}_K$, each factor in (23.7) is a multiple of π, and so

$$\langle\pi\rangle^{q-1} \mid \langle q\rangle. \tag{23.8}$$

As k runs from 1 to $q - 1$, the numbers ζ^k run over the roots of $\Phi_q(x) = \min_\zeta(x)$. So with $\mathrm{N}(\cdot)$ denoting the norm from $K = \mathbb{Q}(\zeta)$ down to $\mathbb{Q}$, (23.7) expresses the fact that $\mathrm{N}(\pi) = q$. Consequently,

$$\mathrm{N}(\langle q\rangle) = q^{q-1} = \mathrm{N}(\langle\pi\rangle^{q-1}),$$

which with (23.8) implies that $\langle q\rangle = \langle\pi\rangle^{q-1}$. Finally, since $\langle\pi\rangle$ has norm q with q prime, $\mathbb{Z}_K/\langle\pi\rangle$ is isomorphic to the field (!) $\mathbb{Z}/q\mathbb{Z}$. So $\langle\pi\rangle$ is a prime ideal of $\mathbb{Z}_K$. □

If we suppose that $G \neq \tilde{G}$, then

$$G - \tilde{G} = -2\sqrt{q^*}. \tag{23.9}$$

Since $\langle\sqrt{q^*}\rangle^2 = \langle q\rangle$, Lemma 23.6 implies that $\pi^{(q-1)/2} \parallel \sqrt{q^*}$. As $\pi \nmid 2$, we deduce from (23.9) that

$$\pi^{(q-1)/2} \parallel G - \tilde{G}.$$

The rest of our arguments are devoted to showing that actually

$$G \equiv \tilde{G} \pmod{\pi^{(q+1)/2}};$$

hence, $G = \tilde{G} = \sqrt{q^*}$, as desired.

The proof of the next lemma is deferred to the end of this section.

Lemma 23.7. Let j be a nonnegative integer. Then, modulo q,

$$\sum_{a=0}^{q-1} a^j \equiv \begin{cases} -1 & \text{if } j \text{ is a nonzero multiple of } q-1, \\ 0 & \text{otherwise.} \end{cases}$$

We will compute G and $\tilde{G}$ modulo $\pi^{(q+1)/2}$ and show that the same result is obtained in both cases. Working modulo $\pi^{(q+1)/2}$ in the ring $\mathbb{Z}_K$,

$$\begin{aligned} G &= \sum_{a \bmod q} \left(\frac{a}{q}\right)(\pi+1)^a \\ &\equiv \sum_{a=0}^{q-1} \left(\frac{a}{q}\right) \sum_{j=0}^{(q-1)/2} \binom{a}{j} \pi^j. \end{aligned}$$

Here a binomial coefficient $\binom{a}{j}$ with $j > a$ is to be interpreted as 0. Since $\pi^{(q+1)/2}$ divides q, Euler's criterion yields

$$\left(\frac{a}{q}\right) \equiv a^{(q-1)/2}.$$

Now inverting the order of summation, the last expression for G is seen to be[9]

$$\equiv \sum_{j=0}^{(q-1)/2} \pi^j \sum_{a=0}^{q-1} \frac{a^{(q-1)/2} a(a-1)\cdots(a-j+1)}{j!}.$$

[9] We use here that $\binom{a}{j} = \frac{a(a-1)\cdots(a-j+1)}{j!}$ for every pair of nonnegative integers a and j, even in the degenerate case $j > a$.

By Lemma 23.7, the summands corresponding to $j < \frac{q-1}{2}$ vanish mod q, and so also mod $\pi^{(q+1)/2}$. The same result shows that when $j = \frac{q-1}{2}$,

$$\sum_{a=0}^{q-1} \frac{a^{(q-1)/2} a(a-1)\cdots(a-j+1)}{j!} \equiv -(\text{coefficient of } a^{q-1}) \equiv -\frac{1}{\frac{q-1}{2}!} \pmod{q}.$$

(Here and below, when $\frac{1}{((q-1)/2)!}$ appears in a congruence, it denotes the congruential inverse of $\frac{q-1}{2}!$.) As a consequence,

$$G \equiv -\frac{\pi^{(q-1)/2}}{\frac{q-1}{2}!} \pmod{\pi^{(q+1)/2}}. \tag{23.10}$$

We turn now to the evaluation of $\tilde{G}$ modulo $\pi^{(q+1)/2}$. Keeping in mind that $1 + \pi = \zeta$, we see that

$$\begin{aligned}(1+\pi)^{-1} = (1+\pi)^{q-1} &\equiv 1 + (q-1)\pi \pmod{\pi^2} \\ &\equiv 1 - \pi \pmod{\pi^2}.\end{aligned}$$

Thus,

$$\begin{aligned}\zeta^{2k-1} - \zeta^{-(2k-1)} &= \left((1+\pi)^{(2k-1)} - (1+\pi)^{-(2k-1)}\right) \\ &\equiv \left((1+\pi)^{(2k-1)} - (1-\pi)^{2k-1}\right) \\ &\equiv (1 + (2k-1)\pi) - (1 - (2k-1)\pi) \\ &\equiv 2(2k-1)\pi \pmod{\pi^2}\end{aligned}$$

for each $k = 1, 2, \ldots, \frac{q-1}{2}$. Hence,

$$\begin{aligned}\tilde{G}/\pi^{(q-1)/2} &= \prod_{k=1}^{(q-1)/2} \frac{(\zeta^{(2k-1)} - \zeta^{-(2k-1)})}{\pi} \\ &\equiv \prod_{k=1}^{(q-1)/2} 2(2k-1) \pmod{\pi}.\end{aligned}$$

Therefore, modulo $\pi^{(q+1)/2}$,

$$\begin{aligned}\tilde{G} &\equiv \pi^{(q-1)/2} 2^{(q-1)/2} \cdot (1 \cdot 3 \cdots (q-2)) \\ &\equiv \pi^{(q-1)/2} 2^{(q-1)/2} \cdot \frac{(q-1)!}{2 \cdot 4 \cdot \cdots \cdot (q-1)} \\ &\equiv \pi^{(q-1)/2} \frac{(q-1)!}{\frac{q-1}{2}!} \\ &\equiv -\frac{\pi^{(q-1)/2}}{\frac{q-1}{2}!}, \qquad (23.11)\end{aligned}$$

using Wilson's theorem in the last step.

Comparing (23.10) and (23.11) yields

$$G \equiv \tilde{G} \pmod{\pi^{(q+1)/2}}.$$

As explained above, Theorem 23.3 follows.

Proof of Lemma 23.7. When $j = 0$, the left-hand sum consists of q 1s, and thus is $\equiv 0 \pmod{q}$. When j is a nonzero multiple of $q-1$, each $a \not\equiv 0 \pmod{q}$ makes a contribution $\equiv 1 \pmod{q}$, while $0^j \equiv 0 \pmod{q}$. Hence, the sum is $\equiv q - 1 \equiv -1 \pmod{q}$ in that case. It remains to show that the sum vanishes mod q when $q-1$ does not divide j. Let g mod q be a generator of the cyclic group $\mathbb{F}_q^\times$. Then

$$\sum_{a=0}^{q-1} a^j \equiv \sum_{\ell=0}^{q-2} g^{\ell j} \equiv \frac{g^{j(q-1)} - 1}{g^j - 1} \pmod{q}.$$

The numerator is a multiple of q but the denominator is not. Therefore the sum on a vanishes mod q, as desired. □

Exercises

We keep the same notation as earlier in the chapter: q is an odd prime, $q^* = (-1)^{(q-1)/2}q$, and $\zeta = e^{2\pi i/q}$.

(1) Complete the indicated proof of (23.6).

(2) (a) Show that $\mathbb{Q}(\zeta)$ is a Galois extension of $\mathbb{Q}$.
(b) Show that for each integer a coprime to q, there is a unique automorphism σ_a of $\mathbb{Q}(\zeta)/\mathbb{Q}$ with $\sigma_a(\zeta) = \zeta^a$. Then prove that the map

$$\begin{aligned} U(\mathbb{Z}/q\mathbb{Z}) &\to \mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q}) \\ a \bmod q &\mapsto \sigma_a \end{aligned}$$

is an isomorphism of groups.

(3) (Look ma, no Gauss sums!) Prove the field containment $\mathbb{Q}(\sqrt{q^*}) \subseteq \mathbb{Q}(\zeta)$ by "pure thought". Proceed as follows.
(a) Show that the nonzero squares modulo q comprise the unique index 2 subgroup of $U(\mathbb{Z}/q\mathbb{Z})$.
(b) Deduce from (a) and the Galois correspondence that $\mathbb{Q}(\zeta)$ has a unique quadratic subfield.
(c) Show that q is the unique rational prime that ramifies in $\mathbb{Q}(\zeta)$.
(d) Show that a quadratic field where all primes not equal to q are unramified is necessarily $\mathbb{Q}(\sqrt{q^*})$.
(e) Conclude that $\mathbb{Q}(\sqrt{q^*}) \subseteq \mathbb{Q}(\zeta)$.

(4) We can now eliminate Gauss sums from our earlier proof of quadratic reciprocity. Let p be an odd prime, $p \neq q$.
(a) Show that $\sigma_p(\alpha) \equiv \alpha^p \bmod p$ for all $\alpha \in \mathbb{Z}[\zeta]$. (Here σ_p has the same meaning indicated in Exercise 2(b).)
(b) Since $\mathbb{Z}[\zeta]$ is the ring of integers of $\mathbb{Q}(\zeta)$ (Theorem 14.6), and $\mathbb{Q}(\sqrt{q^*}) \subseteq \mathbb{Q}(\zeta)$, we have that $\sqrt{q^*} \in \mathbb{Z}[\zeta]$. Show that $\sigma_p(\sqrt{q^*}) \equiv \left(\frac{q^*}{p}\right)\sqrt{q^*} \pmod p$.
(c) Promote (b) from a congruence to an equality. That is, prove that $\sigma_p(\sqrt{q^*}) = \left(\frac{q^*}{p}\right)\sqrt{q^*}$.
(d) It is clear from part (c) that

$$\left(\frac{q^*}{p}\right) = 1 \iff \sigma_p \in \mathrm{Gal}\left(\mathbb{Q}(\zeta)/\mathbb{Q}(\sqrt{q^*})\right).$$

Finish the proof of quadratic reciprocity by explaining why

$$\sigma_p \in \mathrm{Gal}\left(\mathbb{Q}(\zeta)/\mathbb{Q}(\sqrt{q^*})\right) \iff \left(\frac{p}{q}\right) = 1.$$

Hint: Look back at your solution to Exercise 3.

(5) Work out the $q = 2$ versions of Exercises 3 and 4. In other words, give a computation-free proof that $\mathbb{Q}(\sqrt{2}) \subseteq \mathbb{Q}(\zeta_8)$, and deduce the law (23.6) governing the quadratic character of 2.

(6) Let q be a prime, $q \equiv 1 \pmod 3$. Since $\mathbb{F}_q^\times$ is a cyclic group whose order is a multiple of 3, the cubic residues mod q form a subgroup of index 3. Let n be a fixed cubic nonresidue modulo q. Then the image of $n \bmod q$ generates the quotient group $\mathbb{F}_q^\times/(\mathbb{F}_q^\times)^3$. Introduce a cubic residue symbol mod q as follows. Let $\omega = e^{2\pi i/3}$ and $\zeta = e^{2\pi i/q}$. For each integer a not divisible by q, put

$$\left(\!\left(\frac{a}{q}\right)\!\right) = \begin{cases} 1 & \text{if } a \equiv \square\square\square \pmod q, \\ \omega & \text{if } a \equiv n \cdot \square\square\square \pmod q, \\ \omega^2 & \text{if } a \equiv n^2 \cdot \square\square\square \pmod q, \end{cases}$$

and put $\left(\!\left(\frac{a}{q}\right)\!\right) = 0$ when q divides a. Define the corresponding cubic Gauss sum by

$$G_{(3)} = \sum_{a \bmod q} \left(\!\left(\frac{a}{q}\right)\!\right) \zeta^a.$$

Note that our definition of $\left(\!\left(\frac{\cdot}{q}\right)\!\right)$ is not canonical. We could have chosen our fixed nonresidue from the coset of $n^2 \bmod q$ rather than the coset of $n \bmod q$; then $\left(\!\left(\frac{\cdot}{q}\right)\!\right)$ would be replaced with $\left(\!\left(\frac{\cdot}{q}\right)\!\right)^2$. To account for this ambiguity, we let

$$G'_{(3)} = \sum_{a \bmod q} \left(\!\left(\frac{a}{q}\right)\!\right)^2 \zeta^a.$$

(a) Show that $\left(\!\left(\frac{a}{q}\right)\!\right)\left(\!\left(\frac{b}{q}\right)\!\right) = \left(\!\left(\frac{ab}{q}\right)\!\right)$ for every pair of integers a and b, and that $\sum_{a \bmod q} \left(\!\left(\frac{a}{q}\right)\!\right) = 0$.

(b) Following the method used in the text to evaluate G^2, prove that $G_{(3)} \cdot \overline{G_{(3)}} = q = G'_{(3)} \cdot \overline{G'_{(3)}}$. (Bars denote complex conjugation.) *Hint:* $\overline{\left(\!\left(\frac{a}{q}\right)\!\right)} = \left(\!\left(\frac{a}{q}\right)\!\right)^{-1}$ if $q \nmid a$.

(c) Prove that $G_{(3)}^2 = G'_{(3)} \cdot J$, where

$$J = \sum_{a \bmod q} \left(\left(\frac{a(1-a)}{q}\right)\right).$$

Conclude that $J \cdot \bar{J} = q$.

(7) (continuation) Let $K = \mathbb{Q}(\sqrt{-3})$. Since $\omega = \frac{-1+\sqrt{-3}}{2} \in \mathbb{Z}_K$, it is immediate that $J \in \mathbb{Z}_K$. From part (c) of the last exercise, $\mathrm{N}J = q$.

(a) Show that $1 + 2\left(\left(\frac{r}{q}\right)\right) \equiv 0 \pmod{\sqrt{-3}}$ for each integer r not divisible by q.

(b) Use (a) to prove that $J \equiv -1 \pmod 3$. *Hint:* Prove that $\sum_{a \bmod q}(1 + 2\left(\left(\frac{a}{q}\right)\right))(1 + 2\left(\left(\frac{a+1}{q}\right)\right)) \equiv 0 \bmod 3$. How is this sum related to J?[10]

(c) Show that $J \equiv \left(\left(\frac{2}{q}\right)\right) \pmod 2$. *Hint:* Pair a and $1-a$ in the definition of J.

(8) (continuation)

(a) Show that the six units of $\mathbb{Z}_K$ are pairwise incongruent mod 3.

(b) Show that there are exactly two elements of $\mathbb{Z}_K$ congruent to -1 mod 3 with norm q, namely J and $\bar{J}$.

(c) (Gauss[11]) Show that $\left(\left(\frac{2}{q}\right)\right) = 1 \iff q = x^2 + 27y^2$ for some integers x and y.

(9) (Louisiana State University Problem Solving Group[12]) Let q be a prime, $q \equiv 1 \pmod 4$. Show that

$$1 + q^n + q^{2n} + \cdots + q^{(q-1)n}$$

is composite for every positive integer n. *Hint:* Write down a nontrivial factorization of $q^n - \zeta$ in $\mathbb{Z}_K$, where $K = \mathbb{Q}(\zeta)$. Then take norms.

(10) (the Pólya–Vinogradov inequality for the Legendre symbol[13]) Let q be an odd prime and let $n \in \mathbb{Z}^+$.

---

[10] This argument is taken from: Williams, K. S. *Note on a cubic character sum.* Aequationes Math. **12** (1975), no. 2–3, 229–231.

[11] Gauss, C. F. *Notizen über cubische und biquadratische Reste.* Nachlaß, Werke VIII (1900), 5–14.

[12] Amer. Math. Monthly **109** (2002), 476; solution in **111** (2004), 362–363.

[13] See: Pólya, G. *Über die Verteilung der quadratischen Reste und Nichtreste.* Gött. Nachr. (1918), 21–29; Vinogradov, I. M. *On the distribution of quadratic residues and nonresidues.* (Russian) J. Soc. Phys. Math. Univ. Permi **2** (1919), pp. 1–14. The proof sketched here follows: Schur, I. *Einige Bemerkungen zu der vorstehenden Arbeit des Herrn G. Pólya: Über die Verteilung der quadratischen Reste und Nichtreste.* Gött. Nachr. (1918), 30–36.

(a) Show that

$$\left| \sum_{m=1}^{n} \left(\frac{m}{q}\right) \right| = \frac{1}{\sqrt{q}} \left| \sum_{\substack{|a|<q/2 \\ a\neq 0}} \left(\frac{a}{q}\right) \sum_{m=1}^{n} \zeta^{am} \right|.$$

Hint: First solve for $\left(\frac{m}{q}\right)$ in (23.3).

(b) Show that for each nonzero a with $|a| < q/2$,

$$\left| \sum_{m=1}^{n} \zeta^{am} \right| = \frac{|\sin(\pi an/q)|}{|\sin(\pi a/q)|} \leq \frac{1}{|\sin(\pi a/q)|}.$$

(c) Prove that $|\sin(\theta)| \geq \frac{2}{\pi}|\theta|$ whenever $|\theta| \leq \frac{\pi}{2}$.

(d) Prove that

$$\sum_{0<a<q/2} \frac{1}{a} < \log q.$$

Hint: First show that $\frac{1}{a} < \log \frac{1+\frac{1}{2a}}{1-\frac{1}{2a}}$.

(e) Conclude that

$$\left| \sum_{m=1}^{n} \left(\frac{m}{q}\right) \right| < \sqrt{q} \log q.$$

(11) Show that if q is any sufficiently large prime, then every list of $3q^{1/2} \log q$ consecutive integers m contains at least one with $\left(\frac{m}{q}\right) = 1$ and another with $\left(\frac{m}{q}\right) = -1$.

24

Ideal density in quadratic number fields

Fix a number field K. We have seen in previous chapters that for any $X > 0$, there are only finitely many $I \in \mathrm{Id}(\mathbb{Z}_K)$ with $\mathrm{N}(I) \leq X$. Let $Z(X)$ be the corresponding counting function; i.e.,

$$Z(X) = \sum_{\substack{I \in \mathrm{Id}(\mathbb{Z}_K) \\ \mathrm{N}(I) \leq X}} 1.$$

Then $Z(X)$ is nonnegative and (weakly) increasing, and clearly $Z(X) \to \infty$ as $X \to \infty$. So from an analytic perspective, the following question naturally presents itself.

Question 24.1. Can we obtain a precise estimate for the rate of growth of $Z(X)$, as $X \to \infty$?

In the special case when K is a quadratic field, an affirmative answer to this question was given by Dirichlet in 1839.[1] In this chapter, we work through his arguments and derive an asymptotic formula for $Z(X)$. In the next chapter, we will see how Dirichlet's results can be used to establish surprising expressions for the class number h_K.

[1] See: Dirichlet, P. G. L. *Recherches sur diverses applications de l'Analyse infinitesimale à la théorie des Nombres.* J. reine angew. Math. **19** (1839), 324–369. There Dirichlet formulates his results in the language of binary quadratic forms, not quadratic fields, but this is more-or-less equivalent.

Dedekind would later generalize Dirichlet's results to all number fields and would include his findings in his 11th supplement to Dirichlet's lectures on number theory. We state (without proof) Dedekind's general formula at the end of the chapter.

Divide and conquer

We split the problem of estimating $Z(X)$ into h_K subproblems. For each ideal class $C \in \mathrm{Cl}(\mathbb{Z}_K)$, set

$$Z(X;C) = \sum_{\substack{I \in C \\ \mathrm{N}(I) \le X}} 1;$$

clearly,

$$Z(X) = \sum_{C \in \mathrm{Cl}(\mathbb{Z}_K)} Z(X;C).$$

The reason for this subdivision is found in the following lemma, which will allow us to interpret $Z(X;C)$ as a certain lattice point count.

Lemma 24.2. Let C be an ideal class. Fix a representative J for the class C^{-1}. Then

$$Z(X;C) = \#\{\text{ideals } \langle\alpha\rangle : \alpha \in J,\ 0 < |\mathrm{N}\alpha| \le \mathrm{N}(J) \cdot X\}. \tag{24.1}$$

Proof. If I belongs to C and $\mathrm{N}(I) \le X$, then $IJ = \langle\alpha\rangle$, where $\alpha \in J$ and where $|\mathrm{N}\alpha| = \mathrm{N}(\langle\alpha\rangle) = \mathrm{N}(IJ) = \mathrm{N}(I)\mathrm{N}(J) \le \mathrm{N}(J) \cdot X$. Conversely, suppose that $\alpha \in J$ and that $|\mathrm{N}\alpha| \le \mathrm{N}(J) \cdot X$. Then $\langle\alpha\rangle = IJ$ for some I ("to contain is to divide"); moreover, $I \in C$ and $\mathrm{N}(I) = \mathrm{N}(\langle\alpha\rangle)\mathrm{N}(J)^{-1} \le (\mathrm{N}(J) \cdot X) \cdot \mathrm{N}(J)^{-1} = X$. □

The analysis now forks off in two different directions, depending on the sign of Δ_K.

Counting ideals in imaginary quadratic fields

The finiteness of the unit group when $\Delta_K < 0$ makes this case the simpler of the two. Each ideal $\langle\alpha\rangle$ counted on the right of (24.1) arises from $w_K := \#U(\mathbb{Z}_K)$ distinct elements α (namely, all associates of any one generator). Hence,

$$w_K \cdot Z(X;C) = \#\{\alpha \in J,\ 0 < |\mathrm{N}\alpha| \le \mathrm{N}(J) \cdot X\}, \tag{24.2}$$

so that we have converted our count of ideals into a count of elements.

Let $\iota\colon K \to \mathbb{C}$ denote the Minkowski embedding of K, as defined in Chapter 20. We can assume (relabeling the embeddings of K into $\mathbb{C}$ if necessary) that ι is the identity map. Then identifying $\mathbb{C}$ with $\mathbb{R}^2$, we have that $\iota(\alpha) = (\Re\alpha, \Im\alpha)$. Thus, $\mathrm{N}\alpha = \alpha\bar{\alpha} = (\Re\alpha)^2 + (\Im\alpha)^2 = \|\iota(\alpha)\|^2$, so that the right-hand side of (24.2) can be reinterpreted geometrically as follows:

$$\#\{\alpha \in J,\ 0 < |\mathrm{N}\alpha| \le \mathrm{N}(J)\cdot X\} = \sum_{\mathbf{v}\in\iota(J)\cap\mathcal{R}(X)} 1, \tag{24.3}$$

where

$$\mathcal{R}(X) = \{\mathbf{v} \in \mathbb{R}^2 : 0 < \|v\|^2 \le \mathrm{N}(J)\cdot X\}.$$

Recall that $\iota(J)$ is a lattice in $\mathbb{R}^2$ (Proposition 21.3). Moreover, as $X \to \infty$, the region $\mathcal{R}(X)$ is "expanding" in the sense of Chapter 12. Specifically, if we let

$$\mathcal{B} = \{\mathbf{x} \in \mathbb{R}^2 : 0 < \|\mathbf{x}\|^2 \le 1\}$$

(the punctured unit ball), then $\mathcal{R}(X)$ is the dilation of $\mathcal{B}$ by the factor $(\mathrm{N}(J)\cdot X)^{1/2}$. Thus, the stage is perfectly set for an application of the fundamental point counting principle.

Clearly (for those of us living post-Archimedes), $\mathrm{vol}(\mathcal{B}) = \pi$, while Proposition 21.3 tells us that

$$\mathrm{covol}(\iota(J)) = 2^{-1}\cdot \mathrm{N}(J)\sqrt{|\Delta_K|}.$$

So by the point counting principle (in the form of Proposition 13.13),

$$\frac{1}{\mathrm{N}(J)\cdot X}\sum_{\mathbf{v}\in\iota(J)\cap\mathcal{R}(X)} 1 \to \frac{\pi}{2^{-1}\mathrm{N}(J)\sqrt{|\Delta_K|}}, \qquad \text{as } X \to \infty.$$

Cleaning this up a bit,

$$\frac{1}{X}\sum_{\mathbf{v}\in\iota(J)\cap\mathcal{R}(X)} 1 \to \frac{2\pi}{\sqrt{|\Delta_K|}}.$$

Putting this together with (24.2) and (24.3), we conclude that

$$\frac{Z(X;C)}{X} \to \frac{2\pi}{w_K\sqrt{|\Delta_K|}}. \tag{24.4}$$

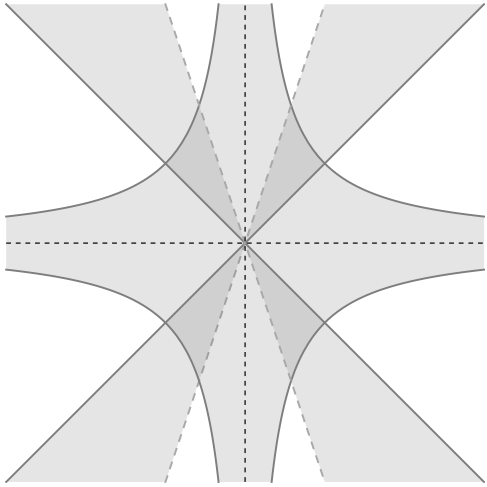


Figure 24.1. $\mathcal{R}(X)$ is the doubly-shaded, four-armed region bounded by $xy = \pm X$ and the lines $y = \pm x$ and $y = \pm\epsilon^2 x$.

Counting ideals in real quadratic fields

When $\Delta_K > 0$, the Minkowski embedding $\iota\colon K \to \mathbb{R}^2$ can be assumed to send α to $(\alpha, \tilde{\alpha})$.[2] So in this case, $\mathrm{N}\alpha$ is the product of the components of $\iota(\alpha)$. This implies that (24.1) counts $\alpha \in J$ for which $\iota(\alpha)$ belongs to the hyperbolic region

$$\{(x, y) \in \mathbb{R}^2 : 0 < |xy| \le \mathrm{N}(J) \cdot X\},$$

with the crucial caveat that we count each associate of α only once.

Lemma 24.3. Let ϵ be the fundamental unit of $\mathbb{Z}_K$. Every nonzero $\alpha \in \mathbb{Z}_K$ has an associate β satisfying

$$1 \le |\tilde{\beta}/\beta| < \epsilon^2. \tag{24.5}$$

Moreover, (24.5) determines β up to sign.

Proof. The associates β of α each have the form $\pm\epsilon^j\alpha$. Since $|\mathrm{N}\epsilon| = |\epsilon\tilde{\epsilon}| = 1$,

$$\left|\frac{\tilde{\beta}}{\beta}\right| = \left|\frac{\tilde{\epsilon}^j\tilde{\alpha}}{\epsilon^j\alpha}\right| = \epsilon^{-2j}\left|\frac{\tilde{\alpha}}{\alpha}\right|.$$

[2]Here we use a tilde for the nontrivial automorphism of $K/\mathbb{Q}$.

The value of j is now uniquely determined by (24.5), while the choice of sign is arbitrary. □

Lemma 24.3 motivates us to define

$$\mathcal{R}(X) = \{(x, y) : 0 < |xy| \le \mathrm{N}(J) \cdot X \text{ and } 1 \le \left|\frac{y}{x}\right| < \epsilon^2\}.$$

(Figure 24.1 shows the shape of $\mathcal{R}(X)$. In that illustration, $\epsilon^2 \approx 3$.) We see then that

$$\#\{\langle\alpha\rangle : \alpha \in J,\ 0 < |\mathrm{N}\alpha| \le \mathrm{N}(J) \cdot X\} = \frac{1}{2} \sum_{\mathbf{v} \in \iota(J) \cap \mathcal{R}(X)} 1. \tag{24.6}$$

As before, $\mathcal{R}(X)$ is a region expanding with X; letting

$$\mathcal{R}_0 = \{(x, y) : 0 < |xy| \le 1 \text{ and } 1 \le \left|\frac{y}{x}\right| < \epsilon^2\},$$

we have that $\mathcal{R}(X) = (\mathrm{N}(J) \cdot X)^{1/2} \mathcal{R}_0$. So by the fundamental point counting principle,

$$\frac{1}{\mathrm{N}(J) \cdot X} \sum_{\mathbf{v} \in \iota(J) \cap \mathcal{R}(X)} 1 \to \frac{\mathrm{vol}(\mathcal{R}_0)}{\mathrm{covol}(\iota(J))}. \tag{24.7}$$

The value of the denominator on the right-hand side is given to us by Proposition 21.3:

$$\mathrm{covol}(\iota(J)) = \mathrm{N}(J)\sqrt{\Delta_K}. \tag{24.8}$$

To compute the numerator, we take advantage of the four-fold symmetry of $\mathcal{R}_0$. From Figure 24.2,

$$\begin{aligned} \frac{1}{4}\mathrm{vol}(\mathcal{R}_0) &= \int_0^{\epsilon^{-1}} (\epsilon^2 x - x)\, dx + \int_{\epsilon^{-1}}^1 \left(\frac{1}{x} - x\right) dx \\ &= \log \epsilon \qquad \text{(Calculus to the rescue!)}. \end{aligned} \tag{24.9}$$

Putting (24.1) together with (24.6)–(24.9) shows that

$$\frac{Z(X; C)}{X} \to \frac{2 \log \epsilon}{\sqrt{\Delta_K}}, \qquad \text{as } X \to \infty. \tag{24.10}$$

Summing up

The limit of $Z(X)/X$, as $X \to \infty$, can now be obtained simply by summing (24.4) and (24.10) over the h_K ideal classes.

Theorem 24.4 (Ideal density in quadratic fields)**.** Let K be a quadratic field.

(a) If $\Delta_K < 0$, then

$$\lim_{X\to\infty} \frac{Z(X)}{X} = \frac{2\pi \cdot h_K}{w_K\sqrt{|\Delta_K|}},$$

where w_K is the number of units of $\mathbb{Z}_K$.

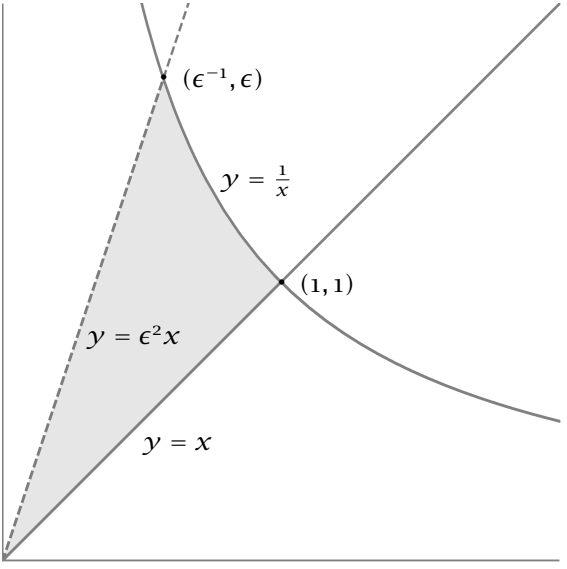
(b) If $\Delta_K > 0$, then

$$\lim_{X\to\infty} \frac{Z(X)}{X} = \frac{2h_K \log \epsilon}{\sqrt{\Delta_K}},$$

where ϵ is the fundamental unit of $\mathbb{Z}_K$.

The limiting value of $\frac{Z(X)}{X}$ is called the **ideal density** of K.

Figure 24.2. The first-quadrant "arm" of $\mathcal{R}_0$.



Ideal density in arbitrary number fields

To state Dedekind's grand generalization of Theorem 24.4, we need one more definition. Let $\epsilon_1, \ldots, \epsilon_{r_1+r_2-1}$ be any system of "fundamental units" of $\mathbb{Z}_K$, meaning that

$$U(\mathbb{Z}_K) = \mu_K \times \prod_{i=1}^{r_1+r_2-1} \langle \epsilon_i \rangle.$$

Consider the $(r_1 + r_2) \times (r_1 + r_2 - 1)$ matrix whose columns are the vectors $\operatorname{Log} \epsilon_i$. The **regulator of** K, denoted R_K, is defined as the absolute value of the determinant of any of the $(r_1+r_2-1)\times(r_1+r_2-1)$ minors. It is not hard to check that R_K is independent of how the fundamental units are selected and of which minor is chosen.

Theorem 24.5 (Dedekind's ideal density theorem)**.** Let K be any number field. With $Z(X)$ the number of nonzero ideals of $\mathbb{Z}_K$ of norm not exceeding X,

$$\lim_{X\to\infty} \frac{Z(X)}{X} = \frac{2^{r_1}(2\pi)^{r_2} R_K h_K}{w_K \cdot \sqrt{|\Delta_K|}},$$

where $w_K = \#\mu_K$.

The proof in the general case is the same in spirit as the proof when K is quadratic, but it is significantly more painful to write down the regions analogous to $\mathcal{B}$ and $\mathcal{R}_0$ and to compute their volumes. See Chapter 6 of Marcus's book for a careful treatment.[3]

Exercises

(1) (Partial summation) Let $\{a_N\}_{N=1}^{\infty}$ be an infinite sequence of real numbers. For each real $T \geq 1$, let $A(T) = \sum_{N\leq T} a_N$ (the **summatory function** of $\{a_N\}$).

Let $X \geq 1$. Show that if f is a real-valued function with f' continuous on $[1, X]$, then

$$\sum_{N\leq X} a_N f(N) = A(X)f(X) - \int_1^X A(T)f'(T)\,dT.$$

[3] Marcus, D. A. *Number fields.* Universitext. Springer-Verlag, New York-Heidelberg, 1977.

Hint: Establish that

$$\int_1^X A(T)f'(T)\,dT = \sum_{N\le X} a_N \int_N^X f'(T)\,dT.$$

(2) Suppose now that $\{a_N\}_{N=1}^{\infty}$ is a sequence of real numbers with mean value λ, meaning that

$$\lim_{X\to\infty} \frac{A(X)}{X} = \lambda. \tag{24.11}$$

(a) Show that the series $\sum_{N=1}^{\infty} a_N/N^s$ converges for all $s > 1$ and that in fact

$$\sum_{N=1}^{\infty} \frac{a_N}{N^s} = s\int_1^{\infty} \frac{A(T)}{T^{s+1}}\,dT.$$

Hint: Apply partial summation with $f(T) = T^{-s}$.

(b) Check that for $s > 1$,

$$s\int_1^{\infty} \frac{\lambda T}{T^{s+1}}\,dT = \lambda\frac{s}{s-1}.$$

(c) Write $A(T) = \lambda T + E(T)$. By (24.11), $E(T)/T \to 0$ as $T \to \infty$. Use this to prove that

$$\lim_{s\downarrow 1} \frac{s\int_1^{\infty} E(T)/T^{s+1}\,dt}{1/(s-1)} = 0.$$

Hint: For each $\epsilon > 0$, there is a constant $C = C(\epsilon)$ with $|E(T)| \le C + \epsilon T$ for all $T \ge 1$. (Why?) Use this to show that

$$\limsup_{s\downarrow 1} \left| \frac{s\int_1^{\infty} E(T)/T^{s+1}\,dT}{1/(s-1)} \right| \le \epsilon.$$

(d) Conclude that

$$\lim_{s\downarrow 1} \frac{\sum_{N=1}^{\infty} a_N/N^s}{1/(s-1)} = \lambda.$$

(3) (Dedekind's class number formula) For this exercise, assume Dedekind's ideal density theorem (Theorem 24.5). For each number field K, define the **Dedekind zeta function** $\zeta_K(s)$ for real $s > 1$ by the formula

$$\zeta_K(s) = \sum_I \frac{1}{\mathrm{N}(I)^s},$$

where I runs over all nonzero ideals of $\mathbb{Z}_K$.

First, show that this definition makes sense by proving that the series converges for all $s > 1$, and that its value does not depend on how the ideals I are ordered. Then prove that

$$\lim_{s \downarrow 1} \frac{\zeta_K(s)}{1/(s-1)} = \frac{2^{r_1}(2\pi)^{r_2} R_K h_K}{w_K \cdot \sqrt{|\Delta_K|}}.$$

25

Dirichlet's class number formula

In the same 1839 paper discussed in Chapter 24, Dirichlet expresses the ideal density of a quadratic field as the sum of a weighted variant of the harmonic series, where the weights encode the splitting behavior of the rational primes. In this chapter, we prove this remarkable **class number formula** in the special case of the fields $K = \mathbb{Q}(\sqrt{q^*})$, where q is an odd prime and (as in Chapter 23) $q^* = (-1)^{(q-1)/2}q$. Note that since $q^* \equiv 1 \pmod 4$, we always have $\Delta_K = q^*$.

Theorem 25.1 (Dirichlet's class number formula for the fields $\mathbb{Q}(\sqrt{q^*})$)**.** Let q be an odd prime, and let $K = \mathbb{Q}(\sqrt{q^*})$. Then the ideal density of K is represented by the series

$$\sum_{m=1}^{\infty} \frac{1}{m}\left(\frac{m}{q}\right).$$

Thus, by Theorem 24.4,

$$\sum_{m=1}^{\infty} \frac{1}{m}\left(\frac{m}{q}\right) = \begin{cases} \dfrac{2\pi h_K}{w_K\sqrt{q}} & \text{if } q \equiv 3 \pmod 4, \\ \dfrac{2h_K \log \epsilon}{\sqrt{q}} & \text{if } q \equiv 1 \pmod 4. \end{cases}$$

Here $w_K = \#U(\mathbb{Z}_K)$ when $q^* < 0$ (corresponding to $q \equiv 3 \pmod 4$), and ϵ is the fundamental unit of $\mathbb{Z}_K$ when $q^* > 0$ (corresponding to $q \equiv 1 \pmod 4$).

For example, let $q = 3$. Then $K = \mathbb{Q}(\sqrt{-3})$. K is Euclidean, and so $h_K = 1$. From Chapter 8, $w_K = 6$. The Legendre symbol $\left(\frac{n}{3}\right)$ vanishes

when $3 \mid n$ and otherwise alternates between 1 and -1. Thus,

$$1 - \frac{1}{2} + \frac{1}{4} - \frac{1}{5} + \frac{1}{7} - \frac{1}{8} + \cdots = \frac{\pi}{3\sqrt{3}}.$$

A formal affair

For each $N \in \mathbb{Z}^+$, let $R(N)$ denote the number of ideals of $\mathbb{Z}_K$ of norm N. As in the last chapter, write $Z(X)$ for the total number of nonzero ideals of $\mathbb{Z}_K$ of norm not exceeding X. Clearly,

$$Z(X) = \sum_{N \le X} R(N).$$

We proceed to analyze the terms $R(N)$ by studying the **formal Dirichlet series**[1]

$$\frac{R(1)}{1^s} + \frac{R(2)}{2^s} + \frac{R(3)}{3^s} + \ldots.$$

Here "formal" means that you should think of the denominators 1^{-s}, 2^{-s}, 3^{-s}, ... as analogous to the symbols $1, x, x^2, \ldots$ in the theory of formal power series. To borrow an image from Herb Wilf, these symbols provide

> a clothesline on which we hang up a sequence of numbers;[2]

nothing is being claimed about what happens when one plugs in a real or complex number s![3]

To start off our manipulations, the definition of $R(N)$ immediately yields

$$\sum_{N=1}^{\infty} \frac{R(N)}{N^s} = \sum_{N=1}^{\infty} \frac{1}{N^s} \sum_{\substack{I \in \mathrm{Id}(\mathbb{Z}_K) \\ \mathrm{N}(I)=N}} 1 = \sum_{I \in \mathrm{Id}(\mathbb{Z}_K)} \frac{1}{\mathrm{N}(I)^s}.$$

[1] In general, a **Dirichlet series** is an expression of the form $\sum_{N=1}^{\infty} a_N / N^s$, where $\{a_N\}$ is a sequence of real or complex numbers.

[2] Wilf, H. S. *generatingfunctionology*. Third edition. A K Peters, Wellesley, MA, 2006.

[3] This is in contrast to the Dirichlet series that appeared in the exercises to Chapter 24 and that appear in the exercises to this chapter. In those examples, it is essential to view the series as functions of s.

Since nonzero ideals enjoy unique factorization,

$$\begin{aligned}\sum_{I\in \mathrm{Id}(\mathbb{Z}_K)} \frac{1}{\mathrm{N}(I)^s} &= \prod_P \left(1 + \frac{1}{\mathrm{N}(P)^s} + \frac{1}{\mathrm{N}(P^2)^s} + \dots\right) \\ &= \prod_P \left(\sum_{j=0}^{\infty} \frac{1}{\mathrm{N}(P)^{js}}\right) = \prod_P \frac{1}{1-\frac{1}{\mathrm{N}(P)^s}}; \end{aligned} \tag{25.1}$$

here P is understood to run over the nonzero prime ideals of $\mathbb{Z}_K$. (The idea behind (25.1) goes back to Euler. Of course, nothing special about quadratic fields is being used here; analogous manipulations are valid for any number field. Cf. Exercise 7.) Grouping prime ideals P lying above the same rational prime p, we find that

$$\prod_{P\mid\langle p\rangle} \frac{1}{1-\frac{1}{\mathrm{N}(P)^s}} = \begin{cases} (1-\frac{1}{p^s})^{-1} & \text{if } p \text{ ramifies,} \\ (1-\frac{1}{p^s})^{-2} & \text{if } p \text{ splits,} \\ (1-\frac{1}{p^{2s}})^{-1} & \text{if } p \text{ is inert.} \end{cases} \tag{25.2}$$

By the quadratic case of the Dedekind–Kummer criterion (Theorem 7.3; see also Corollaries 7.7 and 7.8),

$$p \text{ ramifies} \iff p = q \iff \left(\frac{p}{q}\right) = 0,$$

$$p \text{ splits} \iff \left(\frac{q^*}{p}\right) = 1 \overset{\text{quad. recip.}}{\iff} \left(\frac{p}{q}\right) = 1,$$

$$p \text{ is inert} \iff \left(\frac{q^*}{p}\right) = -1 \iff \left(\frac{p}{q}\right) = -1.$$

We see that in all three cases, the factor on the right-hand side of (25.2) matches up with

$$\left(1-\frac{1}{p^s}\right)^{-1}\left(1-\left(\frac{p}{q}\right)\frac{1}{p^s}\right)^{-1}.$$

Substituting this back in above,

$$\sum_{N=1}^{\infty} \frac{R(N)}{N^s} = \prod_p \frac{1}{1-\frac{1}{p^s}} \frac{1}{1-\left(\frac{p}{q}\right)\frac{1}{p^s}}. \tag{25.3}$$

Since positive integers factor uniquely into primes,

$$\prod_p \frac{1}{1-\frac{1}{p^s}} = \prod_p \left(1 + \frac{1}{p^s} + \frac{1}{p^{2s}} + \dots\right)$$

$$= \sum_{n=1}^{\infty} \frac{1}{n^s}.$$

(Euler's idea again!) Similarly, taking advantage of the multiplicativity relation $\left(\frac{m_1}{q}\right)\left(\frac{m_2}{q}\right) = \left(\frac{m_1 m_2}{q}\right)$, we find that

$$\prod_p \frac{1}{1-\left(\frac{p}{q}\right)\frac{1}{p^s}} = \sum_{m=1}^{\infty} \left(\frac{m}{q}\right)\frac{1}{m^s}.$$

Putting these expressions back into (25.3),

$$\sum_{N=1}^{\infty} \frac{R(N)}{N^s} = \left(\sum_{n=1}^{\infty} \frac{1}{n^s}\right)\left(\sum_{m=1}^{\infty} \left(\frac{m}{q}\right)\frac{1}{m^s}\right).$$

Multiplying out the right-hand side and equating coefficients of N^{-s}, we conclude that

$$R(N) = \sum_{mn=N} \left(\frac{m}{q}\right). \tag{25.4}$$

The identity (25.4) will be the key to deriving the expression for the ideal density of K given in Theorem 24.4.

It's how you count that counts

Sum both sides of (25.4) over $N \le X$ to find that

$$Z(X) = \sum_{m \le X} \left(\frac{m}{q}\right) \sum_{n \le X/m} 1.$$

The inner sum here is $\lfloor X/m \rfloor = X/m - \{X/m\}$. Inserting this into the last display and dividing by X,

$$\frac{Z(X)}{X} = \sum_{m \le X} \left(\frac{m}{q}\right)\frac{1}{m} - \frac{1}{X}\sum_{m \le X} \left(\frac{m}{q}\right)\left\{\frac{X}{m}\right\}. \tag{25.5}$$

To understand the two right-hand sums, we require a lemma of Dirichlet about special infinite series. A proof is given in the appendix.

Lemma 25.2 (Dirichlet's test for convergence)**.** Suppose that $\{a_n\}_{n=1}^{\infty}$ and $\{b_n\}_{n=1}^{\infty}$ are sequences of real and complex numbers, respectively. Assume that $\{a_n\}$ is decreasing with limit 0, and that the partial sums of $\{b_n\}$ are bounded. Then $\sum_{n=1}^{\infty} a_n b_n$ converges.

We apply Lemma 25.2 with $a_m = 1/m$ and $b_m = \left(\frac{m}{q}\right)$. Clearly, $\{a_m\}$ meets the given conditions. Moreover, if m runs over any q consecutive integers, then

$$\begin{aligned}\sum\nolimits_m b_m &= \sum_{m:\,\left(\frac{m}{q}\right)=1} 1 - \sum_{m:\,\left(\frac{m}{q}\right)=-1} 1 \\ &= \frac{q-1}{2} - \frac{q-1}{2} = 0.\end{aligned}$$

Since $|b_m| \le 1$, it follows that the sum of the b_m, with m running over any interval, is always smaller than q in absolute value. This estimate applies, in particular, to the partial sums of the b_m. So by Dirichlet's convergence test,

$$\sum_{m \le X} \left(\frac{m}{q}\right) \frac{1}{m}$$

tends to a finite limit as $X \to \infty$.

Having understood the limiting behavior of the first piece in (25.5), we turn attention to the subtracted term. We will argue that this piece tends to zero as $X \to \infty$.

Let J be a large, fixed integer. We split the range of summation in this second piece into $J+1$ intervals: the ranges where $\lfloor \frac{X}{m} \rfloor = j$ for some $j = 1, 2, \dots, J$, together with the range where $\frac{X}{m} \ge J+1$. When $\lfloor \frac{X}{m} \rfloor = j$, we have $\left\{\frac{X}{m}\right\} = \frac{X}{m} - j$, and thus

$$\begin{aligned}\frac{1}{X} \sum_{m \le X} \left(\frac{m}{q}\right) \left\{\frac{X}{m}\right\} &= \frac{1}{X} \sum_{j=1}^{J} \sum_{\frac{X}{j+1} < m \le \frac{X}{j}} \left(\frac{m}{q}\right) \left(\frac{X}{m} - j\right) \\ &\quad + \frac{1}{X} \sum_{m \le \frac{X}{J+1}} \left(\frac{m}{q}\right) \left\{\frac{X}{m}\right\}.\end{aligned}$$

Since each term $\left(\frac{m}{q}\right)\{\frac{X}{m}\}$ is bounded by 1 in absolute value, it is trivial that

$$\left| \frac{1}{X} \sum_{m \le \frac{X}{J+1}} \left(\frac{m}{q}\right) \left\{\frac{X}{m}\right\} \right| \le \frac{1}{J+1}.$$

Moreover,

$$\frac{1}{X} \sum_{j=1}^{J} \sum_{\frac{X}{j+1} < m \le \frac{X}{j}} \left(\frac{m}{q}\right) \left(\frac{X}{m} - j\right)$$

$$= \sum_{\frac{X}{J+1} < m \le X} \left(\frac{m}{q}\right) \frac{1}{m} - \sum_{j=1}^{J} \frac{j}{X} \sum_{\frac{X}{j+1} < m \le \frac{X}{j}} \left(\frac{m}{q}\right).$$

The first right-hand sum on m tends to 0 as $X \to \infty$, by the Cauchy convergence criterion for infinite series. (Remember, we already know that $\sum_{m=1}^{\infty} \left(\frac{m}{q}\right) \frac{1}{m}$ converges.) Also,

$$\left| \sum_{j=1}^{J} \frac{j}{X} \sum_{\frac{X}{j+1} < m \le \frac{X}{j}} \left(\frac{m}{q}\right) \right| \le \sum_{j=1}^{J} \frac{j}{X} \left| \sum_{\frac{X}{j+1} < m \le \frac{X}{j}} \left(\frac{m}{q}\right) \right|$$

$$\le \frac{1}{X} \sum_{j=1}^{J} jq < \frac{qJ^2}{X},$$

and this also tends to 0 as $X \to \infty$.

Hence, the subtracted term in (25.5) satisfies

$$\limsup_{X \to \infty} \left| \frac{1}{X} \sum_{m \le X} \left(\frac{m}{q}\right) \left\{\frac{X}{m}\right\} \right| \le \frac{1}{J+1}.$$

But J can be taken arbitrarily large, and hence this second term in fact goes to zero as X tends to infinity.

Putting everything together shows that

$$\lim_{X \to \infty} \frac{Z(X)}{X} = \sum_{m=1}^{\infty} \left(\frac{m}{q}\right) \frac{1}{m},$$

exactly as claimed in Theorem 25.1.

The class number formula for an arbitrary quadratic field

Now let K be an arbitrary quadratic field. The **Kronecker character** of K is the function $\chi_K : \mathbb{Z} \to \{-1, 0, 1\}$ defined by the following recipe. For each prime p, let

$$\chi_K(p) = \begin{cases} 0 & \text{if } p \text{ ramifies in } K, \\ 1 & \text{if } p \text{ splits in } K, \\ -1 & \text{if } p \text{ is inert in } K. \end{cases}$$

Further, set

$$\chi_K(-1) = \begin{cases} 1 & \text{if } K \text{ is real}, \\ -1 & \text{if } K \text{ is imaginary}. \end{cases}$$

This uniquely determines χ_K once we add the condition that χ_K be **totally multiplicative**, i.e., that

$$\chi_K(mn) = \chi_K(m)\chi_K(n)$$

for all integers m and n.[4] Dirichlet's general class number formula is the statement one obtains from Theorem 25.1 by replacing $\left(\frac{m}{q}\right)$ with $\chi_K(m)$ and q with $|\Delta_K|$.

Theorem 25.3 (Dirichlet's class number formula; general case)**.** Let K be a quadratic field. Then

$$\sum_{m=1}^{\infty} \frac{\chi_K(m)}{m} = \begin{cases} \dfrac{2\pi h_K}{w_K\sqrt{|\Delta_K|}} & \text{if } K \text{ is imaginary quadratic}, \\ \dfrac{2h_K \log \epsilon}{\sqrt{\Delta_K}} & \text{if } K \text{ is real quadratic}. \end{cases}$$

Here $w_K = \#U(\mathbb{Z}_K)$ in the imaginary case and ϵ is the fundamental unit of $\mathbb{Z}_K$ in the real case.[5]

It is a straightforward exercise using the quadratic reciprocity law (and the supplementary laws governing the quadratic character of -1

[4] Caveat lector: χ_K is more usually denoted $\left(\frac{\Delta_K}{\cdot}\right)$ and referred to as a **Kronecker symbol**.

[5] We noted in Chapter 11 that analytic methods show that $h_K \to \infty$ as $\Delta_K \to -\infty$, but that when $\Delta_K \to +\infty$, these methods only establish the weaker result that $h_K \log \epsilon \to \infty$ (equations 11.6 and 11.7). The class number formula explains this initially puzzling dichotomy, as both results are derived from lower bounds on $\sum_{m=1}^{\infty} \frac{\chi_K(m)}{m}$. See the Davenport book referenced on p. 112.

and 2) to see that if $K = \mathbb{Q}(\sqrt{q^*})$, then $\chi_K(m) = \left(\frac{m}{q}\right)$ (Exercise 1). So Theorem 25.1 is a special case of Theorem 25.3 (as expected).

Without entering into the technicalities, we say a few words about the proof of Theorem 25.3. Getting started is straightforward; the same manipulations with formal Dirichlet series that prove (25.4) prove the analogue for a general quadratic field K, namely: With $R(N)$ the number of ideals of $\mathbb{Z}_K$ of norm N,

$$R(N) = \sum_{mn=N} \chi_K(m). \tag{25.6}$$

To carry over our subsequent arguments, we need to know that the partial sums of χ_K are bounded. The law of quadratic reciprocity can be shown to imply that χ_K is a periodic function modulo $|\Delta_K|$ and that $\chi_K(m) = -1$ for some integer m. From this, it is not hard to deduce (Exercise 5) that the sum of χ_K vanishes over any $|\Delta_K|$ consecutive integers, which allows the rest of our proof to be run as before. We leave the reader to work out the details; alternatively, they will find this (and much more) in Zagier's beautifully written book on quadratic fields.[6]

As a particularly nice example, one can (should!) check that if K is the Gaussian field $\mathbb{Q}(i)$, then

$$\chi_K(n) = \begin{cases} 0 & \text{if } n \text{ is even,} \\ 1 & \text{if } n \equiv 1 \pmod 4, \\ -1 & \text{if } n \equiv 3 \pmod 4. \end{cases} \tag{25.7}$$

From this, they may deduce from Theorem 25.3 that the famous Gregory–Leibniz identity

$$\frac{\pi}{4} = 1 - \frac{1}{3} + \frac{1}{5} - \frac{1}{7} + \dots \tag{25.8}$$

is equivalent to the existence of unique factorization in the ring $\mathbb{Z}[i]$!

Appendix: Dirichlet's test for convergence

We now give the short proof of Lemma 25.2. We will show the convergence of $\sum_{n=1}^{\infty} a_n b_n$ by proving that the associated sequence of

[6] Zagier, D. B. *Zetafunktionen und quadratische Körper*. Hochschultext. Springer-Verlag, Berlin-New York, 1981.

partial sums obeys Cauchy's criterion. For each positive integer n, let

$$B_n = b_1 + b_2 + \cdots + b_n,$$

and let $B_0 = 0$. By assumption, the sequence $\{B_n\}$ is bounded; thus, we may fix a real number K with

$$|B_n| \leq K \quad \text{for all natural numbers } n.$$

We now apply the method of Abel summation. For any positive integers N and M with $N \leq M$,

$$\begin{aligned}\sum_{n=N}^{M} a_n b_n &= \sum_{n=N}^{M} a_n (B_n - B_{n-1}) \\ &= a_M B_M + \sum_{n=N}^{M-1} a_n B_n - \sum_{n=N-1}^{M-1} a_{n+1} B_n \\ &= a_M B_M - a_N B_{N-1} + \sum_{n=N}^{M-1} (a_n - a_{n+1}) B_n.\end{aligned}$$

Invoke the triangle inequality. Since $\{a_n\}$ is nonnegative and decreasing,

$$\begin{aligned}\left| \sum_{n=N}^{M} a_n b_n \right| &\leq 2K \cdot a_N + K \sum_{n=N}^{M-1} (a_n - a_{n+1}) \\ &\leq 2K \cdot a_N + K \cdot a_N = 3K \cdot a_N.\end{aligned}$$

Since $\{a_n\}$ goes to zero, $3K \cdot a_N \to 0$ as $N \to \infty$, and so the Cauchy criterion is satisfied.

Exercises

(1) Let q be an odd prime. Check that when $K = \mathbb{Q}(\sqrt{q^*})$, we have $\chi_K(m) = \left(\frac{m}{q}\right)$ for all integers m.

(2) Verify that when $K = \mathbb{Q}(i)$, the Kronecker character χ_K takes the values specified in (25.7) and that the class number formula corresponds to the Gregory–Leibniz identity (25.8).

(3) Use (25.6) to prove **Jacobi's two squares theorem**: The number of ordered pairs $(x, y) \in \mathbb{Z}^2$ with $x^2 + y^2 = N$ is given by

$$4(d_1(N) - d_3(N)),$$

where $d_i(N)$ counts the number of divisors of N congruent to i modulo 4.

(4) Determine χ_K explicitly for both $K = \mathbb{Q}(\sqrt{2})$ and $K = \mathbb{Q}(\sqrt{-2})$. (Remember that both functions are supposed to be periodic modulo 8.) Write down the corresponding identities output by the class number formula.

(5) Let K be a quadratic field. Assume as known that

- $\chi_K(n + \Delta_K) = \chi_K(n)$ for all integers n,
- there is an $m \in \mathbb{Z}$ with $\chi_K(m) = -1$.

Prove that the sum of χ_K over any $|\Delta_K|$ consecutive integers vanishes. *Hint:* Show that $\gcd(m, \Delta_K) = 1$ and then argue that

$$\chi_K(m) \sum_{n=1}^{|\Delta_K|} \chi_K(n) = \sum_{n=1}^{|\Delta_K|} \chi_K(n).$$

(6) Let q be an odd prime. For each integer $j \geq 0$, put

$$u_j = \sum_{jq<m<(j+1)q,\ \left(\frac{m}{q}\right)=1} \frac{1}{m}, \quad v_j = \sum_{jq<m<(j+1)q,\ \left(\frac{m}{q}\right)=-1} \frac{1}{m},$$

so that

$$\sum_{m=1}^{\infty} \left(\frac{m}{q}\right) \frac{1}{m} = u_0 - v_0 + u_1 - v_1 + \dots.$$

(a) Show that $u_{j+1} \leq v_j$ for all j. Deduce that $\sum_{m=1}^{\infty} \left(\frac{m}{q}\right) \frac{1}{m} \leq u_0$.

(b) Show that $u_0 < \log q$. Thus, $\sum_{m=1}^{\infty} \left(\frac{m}{q}\right) \frac{1}{m} < \log q$. *Hint:* Exercise 23.10(d) will be useful.[7]

[7] The argument sketched in parts (a, b) is due to S. Louboutin.

(c) Now assume additionally that $q \equiv 1 \pmod 4$. Appealing to the class number formula, derive the upper bound

$$\epsilon^h < q^{\frac{1}{2}\sqrt{q}},$$

where ϵ and h are the fundamental unit and class number of $\mathbb{Z}[\frac{1+\sqrt{q}}{2}]$, respectively.

Supplement: Kronecker's density theorems. The following exercises provide a glimpse of how analytic methods can be applied to study the distribution of algebraically special sets of primes.[8] Let K be any number field. Recall from Exercise 24.3 that the Dedekind zeta function $\zeta_K(s)$ is defined by the convergent series $\sum_I 1/\mathrm{N}(I)^s$ in the region $s > 1$. Moreover,

$$\lim_{s \downarrow 1} \frac{\zeta_K(s)}{1/(s-1)} = \frac{2^{r_1}(2\pi)^{r_2} R_K h_K}{w_K \cdot \sqrt{|\Delta_K|}}. \tag{25.9}$$

We will see that that (25.9) — or really, the mere existence of a nonzero, finite limit for $(s-1)\zeta_K(s)$, as $s \downarrow 1$ — has far-reaching arithmetic consequences.

(7) (Euler factorization of $\zeta_K(s)$) As discussed earlier in this chapter, the identity

$$\zeta_K(s) = \prod_P \frac{1}{1 - \mathrm{N}(P)^{-s}} \tag{25.10}$$

is formally valid, as a consequence of unique factorization. It will be important for us to know that (25.10) also expresses an identity of real-valued functions on the domain $(1, \infty)$. This exercise outlines a proof. We fix $s > 1$, and we write P_X for the partial product

$$\prod_{\mathrm{N}(P) \leq X} \frac{1}{1 - \mathrm{N}(P)^{-s}},$$

where P runs over the nonzero prime ideals of norm not exceeding X. Our task is to show that

$$\lim_{X \to \infty} P_X = \zeta_K(s).$$

[8] For an enthralling discussion of deeper, closely related results, see: Stevenhagen, P.; Lenstra, H. W., Jr. *Chebotarëv and his density theorem.* Math. Intelligencer **18** (1996), no. 2, 26–37.

(a) Show that for each $X \geq 2$,

$$P_X = \sum_{\substack{I \\ P \mid I \Rightarrow \mathrm{N}(P) \leq X}} \frac{1}{\mathrm{N}(I)^s}.$$

(Here the sum is over nonzero ideals I divisible only by prime ideals P with $\mathrm{N}(P) \leq X$.)

(b) Deduce that for each $X \geq 2$,

$$0 \leq \zeta_K(s) - P_X \leq \sum_{\substack{I \\ \mathrm{N}(I) > X}} \frac{1}{\mathrm{N}(I)^s}.$$

(c) Conclude that $\lim_{X \to \infty} P_X = \zeta_K(s)$, as desired.

(8) (a) Use (25.10) to show that for $s > 1$,

$$\log \zeta_K(s) = \sum_P \frac{1}{\mathrm{N}(P)^s} + O(1).$$

Here and below, we write $O(1)$ to denote a quantity bounded (in absolute value) for all $s \in (1, 2]$, by a constant depending at most on K. *Hint:* $X \leq \log \frac{1}{1-X} \leq X + X^2$ for $0 \leq X \leq \frac{1}{2}$.

(b) Combining part (a) with (25.9), prove that

$$\sum_P \frac{1}{\mathrm{N}(P)^s} = \log \frac{1}{s-1} + O(1). \tag{25.11}$$

(9) The remaining exercises exhibit some spectacular consequences of (25.11) due essentially to Kronecker.[9]

If $\{a_p\}$ is a sequence of complex numbers indexed by rational primes, we define the **Dirichlet average** $\delta(\{a_p\})$ of $\{a_p\}$ by

$$\delta(\{a_p\}) := \lim_{s \downarrow 1} \frac{\sum_p a_p p^{-s}}{\log \frac{1}{s-1}},$$

if the limit exists.

(a) Show that if $a_p = c$ (a constant) for all primes p, then $\delta(\{a_p\}) = c$. *Hint:* Apply (25.11) with $K = \mathbb{Q}$.

(b) Suppose that the Dirichlet averages of $\{a_p\}$ and $\{b_p\}$ both exist. Show that any linear combination of $\{a_p\}$ and $\{b_p\}$ also has a Dirichlet average, namely the corresponding linear combination of $\delta(\{a_p\})$ and $\delta(\{b_p\})$.

---

[9] Kronecker, L. *Über die Irreductibilität von Gleichungen.* Monatsb. Kgl. Akad. d. Wiss. Berlin (1880), 155–162.

(c) Show that if $a_p = b_p$ for all but finitely many primes p, then $\delta(\{a_p\}) = \delta(\{b_p\})$, provided that either is defined.

(10) (continuation) If $f(x) \in \mathbb{Z}[x]$ and p is a rational prime, we let

$$N_{f,p} = \#\{\text{distinct roots of } f \text{ modulo } p\}.$$

(a) Let $g(x)$ be a monic polynomial with integer coefficients, irreducible over $\mathbb{Q}$. Let $K = \mathbb{Q}(\theta)$, where θ is a complex root of g. Show that $N_{g,p}$ is — with the possible exception of finitely many primes p — the number of nonzero prime ideals P of $\mathbb{Z}_K$ lying above p with $f(P/p) = 1$.

(b) Show that the estimate (25.11) continues to hold with P restricted to primes of residual degree 1. That is, prove that

$$\sum_{p} \sum_{\substack{P \mid p\mathbb{Z}_K \\ f(P/p)=1}} \frac{1}{\mathrm{N}(P)^s} = \log \frac{1}{s-1} + O(1).$$

Hint: First argue that for each prime p, and each real $s > 1$,

$$\sum_{\substack{P \mid p\mathbb{Z}_K \\ f(P/p)>1}} \frac{1}{\mathrm{N}(P)^s} \leq \frac{1}{2}[K : \mathbb{Q}]p^{-2}.$$

(c) Use (a) and (b) to prove that $\{N_{g,p}\}$ has Dirichlet average 1. (In other words: An irreducible polynomial has on average one root per prime!)

(d) Suppose now that $f(x) = g_1(x) \cdots g_\ell(x)$ for distinct monic irreducible polynomials $g_i(x) \in \mathbb{Z}[x]$. Show that for all but finitely many p,

$$N_{f,p} = \sum_{i=1}^{\ell} N_{g_i,p},$$

and conclude that $N_{f,p}$ has Dirichlet average ℓ. *Hint:* Discard p dividing $\Delta(f(x))$.

(11) Let K be a degree n number field and suppose that $K/\mathbb{Q}$ is Galois.

(a) Write $K = \mathbb{Q}(\alpha)$, where $\alpha \in \bar{\mathbb{Z}}$. Let $f(x) = \min_\alpha(x)$. Show that — apart from finitely many exceptional primes p — either $N_{f,p} = n$ or $N_{f,p} = 0$, according to whether or not p splits completely in K. *Hint:* Combine Exercise 17.7 with the Dedekind–Kummer theorem.

(b) Say that a set of rational primes has **Dirichlet density** δ if the corresponding characteristic function has Dirichlet average δ. Deduce from (a) that the rational primes that split completely in K have Dirichlet density $1/n$. This is sometimes called **Kronecker's density theorem**.

(12) Let K be any number field. Show that if p is a rational prime, then

$$p \text{ splits completely in } K \iff p \text{ splits completely in } L, \text{ the Galois closure of } K/\mathbb{Q}.$$

Thus, from Exercise 11, the Dirichlet density of primes splitting completely in K is $1/[L:\mathbb{Q}]$. *Hint:* L is the compositum of the fields $\sigma(K)$, where σ runs over the embeddings of K into $\mathbb{C}$. Now apply Exercises 17.8 and 22.8.

(13) Let $f(x)$ be a monic polynomial with integer coefficients, irreducible over $\mathbb{Q}$. Show that if f has degree at least 2, then the set of primes p with $N_{f,p} > 0$ does *not* have Dirichlet density 1.

26

Three miraculous appearances of quadratic class numbers

> Recently Dirichlet, applying Fourier series to number theory, has found results touching the pinnacle of human ingenuity. — C. G. J. Jacobi to his brother M. H. Jacobi, extolling Dirichlet's work on quadratic class numbers

Life isn't fair, but sometimes mathematics is. Let q be a prime congruent to 1 modulo 4. Then $\left(\frac{a}{q}\right) = \left(\frac{q-a}{q}\right)$ for every a. Hence,

$$\sum_{\substack{1\le a\le q-1\\ \left(\frac{a}{q}\right)=1}} a = \sum_{\substack{1\le a\le q-1\\ \left(\frac{a}{q}\right)=1}} (q-a),$$

so that

$$2\sum_{\substack{1\le a\le q-1\\ \left(\frac{a}{q}\right)=1}} a = \sum_{\substack{1\le a\le q-1\\ \left(\frac{a}{q}\right)=1}} q = q\cdot\frac{q-1}{2}.$$

Exactly the same argument, with precisely the same conclusion, goes through with the condition $\left(\frac{a}{q}\right) = 1$ replaced by $\left(\frac{a}{q}\right) = -1$. So when $q \equiv 1 \pmod 4$:

(26.1) The quadratic residues in $[1, q-1]$ and the nonresidues in $[1, q-1]$ share the same sum.

Similarly, still under the assumption that $q \equiv 1 \pmod 4$,

$$\sum_{a=1}^{(q-1)/2}\left(\frac{a}{q}\right) = \sum_{a=1}^{(q-1)/2}\frac{1}{2}\left(\left(\frac{a}{q}\right)+\left(\frac{q-a}{q}\right)\right) = \frac{1}{2}\sum_{a=1}^{q-1}\left(\frac{a}{q}\right) = 0.$$

Hence:

(26.2) The half-interval $[1, \frac{q-1}{2}]$ contains an equal number of quadratic residues and nonresidues.

So far, so easy. But what happens when $q \equiv 3 \pmod 4$? It is not hard to see (thinking about parity) that both (26.1) and (26.2) are now impossible; the ties between the residues and nonresidues must be broken. The following astonishing theorem of Dirichlet[1] says that in both problems, the tiebreaker always goes in the same direction, independent of the particular prime q.

Theorem 26.1. Suppose that $q \equiv 3 \pmod 4$.

(a) The sum of the quadratic nonresidues in $[1, q-1]$ exceeds the corresponding sum of residues.

(b) The half-interval $[1, \frac{q-1}{2}]$ has more quadratic residues than nonresidues.

The proof shows that in both cases, the excess is measured by the class number of $\mathbb{Q}(\sqrt{-q})$; see (26.7) and (26.10).

Theorem 26.1 is the first of three results discussed in this chapter where class numbers make a surprise appearance. The remaining two are motivated by a classical observation of Lagrange. By Wilson's theorem,

$$\begin{aligned} -1 &\equiv \left(1 \cdot 2 \cdots \frac{q-1}{2}\right) \cdot \left((-1) \cdot (-2) \cdots (-\frac{q-1}{2})\right) \\ &\equiv (-1)^{(q-1)/2} \left(\frac{q-1}{2}!\right)^2. \end{aligned}$$

Hence,

$$\left(\frac{q-1}{2}!\right)^2 \equiv (-1)^{(q+1)/2} \pmod q. \tag{26.3}$$

Lagrange was the first to publish a proof of Wilson's theorem, and (26.3) appears in the very same 1771 paper.[2]

---

[1] Dirichlet, P. G. L. *Sur l'usage des séries infinies dans la théorie des nombres.* J. reine angew. Math. **18** (1838), 259–274.

[2] Lagrange, J. L. *Demonstration d'un théorème nouveau concernant les nombres premiers.* Nouv. Mém. Acad. Berlin **2** (1771), 125–137.

When $q \equiv 3 \pmod 4$, (26.3) is telling us that $\frac{q-1}{2}!$ squares to 1; therefore,

$$\frac{q-1}{2}! \equiv \pm 1 \pmod q.$$

What is the correct choice of sign? This question was raised by Dirichlet in 1828.[3] Within the next decade, he himself had developed all the tools necessary to write down the answer. But as far as I am aware, the solution does not appear in the literature until a century later, in an elementary number theory textbook authored by B. A. Venkov.[4] The result was subsequently rediscovered by Mordell and Chowla (independently).[5]

Theorem 26.2. Suppose that $q \equiv 3 \pmod 4$. Then the class number h of $\mathbb{Q}(\sqrt{-q})$ is odd, and when $q > 3$,

$$\frac{q-1}{2}! \equiv (-1)^{(h+1)/2} \pmod q.$$

Thus, the answer to Dirichlet's question depends on $h_{\mathbb{Q}(\sqrt{-q})}$ modulo 4. It is interesting to note that Theorem 26.2 and Theorem 26.1(a) (in the quantitatively precise form in which it is proved below) were conjectured by Jacobi already in 1832, on the basis of empirical evidence.[6]

When $q \equiv 1 \pmod 4$, (26.3) tells us that $\frac{q-1}{2}!$ is a square root of -1 modulo q. Again, it is possible to pinpoint which root. Our third and final result, due to Chowla, exhibits this root in terms of the class number and the fundamental unit of $\mathbb{Q}(\sqrt{q})$.[7]

Theorem 26.3. Suppose that $q \equiv 1 \pmod 4$. Then the class number h of $\mathbb{Q}(\sqrt{q})$ is odd, the fundamental unit $\epsilon = \frac{1}{2}(u + v\sqrt{q})$ of $\mathbb{Q}(\sqrt{q})$

---

[3] Dirichlet, P. G. L. *Aufgaben. Question d'analyse indéterminée.* J. reine angew. Math. **3** (1828), 407–409.

[4] Venkov, B. A. *Elementary number theory.* (Russian) ONTI, Moscow, 1937; English translation by Helen Alderson, Wolters–Noordhoff, Groningen, 1970.

[5] See: Mordell, L. J. *The congruence* $\frac{p-1}{2}! \equiv \pm 1 \pmod p$. Amer. Math. Monthly **68** (1961), 145–146. Mordell writes: "Professor Chowla informs me that he found the result about the same time that I did."

[6] Jacobi, C. G. J. *Observatio arithmetica de numero classium divisorum quadraticorum formae* $yy + Azz$, *designante* A *numerum primum formae* $4n + 3$. J. reine angew. Math. **9** (1832), 189–192.

[7] Chowla, S. *On the class number of real quadratic fields.* Proc. Nat. Acad. Sci. U.S.A. **47** (1961), 878.

has norm -1, and

$$2 \cdot \frac{q-1}{2}! \equiv (-1)^{(h+1)/2} u \pmod{q}.^{8}$$

A fundamental identity

The proofs of all three main theorems share the same starting point. Let q be an odd prime, and let $\zeta = e^{2\pi i/q}$. We bring back on stage two principal players from earlier chapters, the quadratic Gauss sum G attached to q, defined by

$$G = \sum_{a \bmod q} \left(\frac{a}{q}\right) \zeta^a,$$

and Dirichlet's series representing ideal density in $\mathbb{Q}(\sqrt{q^*})$,

$$\sum_{m=1}^{\infty} \left(\frac{m}{q}\right) \frac{1}{m}.$$

These two lead actors, from Chapters 23 and 25 respectively, have great chemistry; in fact, magic happens in the act of multiplication.

From Chapter 23 (equation (23.3)), we have that for each integer m coprime to q,

$$G \cdot \left(\frac{m}{q}\right) = \sum_{a \bmod q} \left(\frac{a}{q}\right) \zeta^{am}.$$

Thus,

$$G \cdot \sum_{m=1}^{\infty} \left(\frac{m}{q}\right) \frac{1}{m} = \sum_{m=1}^{\infty} \frac{1}{m} \sum_{a \bmod q} \left(\frac{a}{q}\right) \zeta^{am}. \tag{26.4}$$

To proceed, recall that when $|z| \le 1$ and $z \ne 1$,

$$-\operatorname{Log}(1-z) = \sum_{m=1}^{\infty} \frac{z^m}{m}, \tag{26.5}$$

where Log denotes the principal branch of the natural logarithm.[9] Inverting the order of summation in (26.4) and applying (26.5), we

[8] In both this result and Theorem 26.2, only the congruence for $\frac{q-1}{2}!$ is to be attributed to the listed authors. The other statements are included for completeness but are much older.

[9] For $|z| < 1$, (26.5) follows from the theory of complex Taylor series. The identity can be extended to $|z| = 1$, $z \ne 1$ by Abel's theorem.

arrive at our fundamental identity:

$$G \cdot \sum_{m=1}^{\infty} \left(\frac{m}{q}\right) \frac{1}{m} = -\sum_{a=1}^{q-1} \left(\frac{a}{q}\right) \operatorname{Log}(1-\zeta^a). \tag{26.6}$$

Dirichlet

Assume now that $q \equiv 3 \pmod 4$. From Theorem 23.3 (the determination of the Gauss sum) and Theorem 25.1 (the class number formula),

$$G \cdot \sum_{m=1}^{\infty} \left(\frac{m}{q}\right) \frac{1}{m} = i\sqrt{q} \cdot \frac{2\pi h}{w\sqrt{q}} = \frac{2\pi h}{w} i,$$

where h is the class number of $\mathbb{Q}(\sqrt{-q})$ and w is the number of units in the corresponding ring of integers. In particular, the common value in (26.6) is purely imaginary.

We now compare imaginary parts in (26.6). It is an amusing exercise (draw a picture!) to check that

$$\begin{aligned} \Im(\operatorname{Log}(1-\zeta^a)) &= \operatorname{Arg}(1-\zeta^a) \\ &= \frac{\pi a}{q} - \frac{\pi}{2}. \end{aligned}$$

It follows that

$$\frac{2\pi h}{w} = -\sum_{a=1}^{q-1} \left(\frac{a}{q}\right)\left(\frac{\pi a}{q} - \frac{\pi}{2}\right) = -\frac{\pi}{q} \sum_{a=1}^{q-1} a\left(\frac{a}{q}\right).$$

Hence,

$$\begin{aligned} -\frac{2qh}{w} &= \sum_{a=1}^{q-1} a\left(\frac{a}{q}\right) \\ &= \sum_{\substack{1\le a\le q-1 \\ \left(\frac{a}{q}\right)=1}} a - \sum_{\substack{1\le a\le q-1 \\ \left(\frac{a}{q}\right)=-1}} a. \end{aligned} \tag{26.7}$$

Since $-2qh/w < 0$, Theorem 26.1(a) follows immediately. (Incidentally, equation (26.7) also gives a simple, finite procedure for the calculation of h.)

We deduce part (b) of Theorem 26.1 from (26.7) by an elementary, self-contained argument of Uspensky and Heaslet.[10]

[10] See Exercise 7 on p. 284 in: Uspensky, J. V.; Heaslet, M. A. *Elementary Number Theory.* McGraw-Hill Book Company, Inc., New York, 1939.

Lemma 26.4. For primes $q \equiv 3 \pmod 4$,

$$\sum_{a=1}^{(q-1)/2} \left(\frac{a}{q}\right) = -\frac{1}{q}\left(2 - \left(\frac{2}{q}\right)\right) \cdot \sum_{a=1}^{q-1} a\left(\frac{a}{q}\right).$$

Proof. We evaluate $\sum_{a=1}^{q-1} a\left(\frac{a}{q}\right)$ in two different ways. Since $\left(\frac{q-a}{q}\right) = -\left(\frac{a}{q}\right)$, we have

$$\begin{aligned}\sum_{a=1}^{q-1} a\left(\frac{a}{q}\right) &= \sum_{a=1}^{(q-1)/2} a\left(\frac{a}{q}\right) + \sum_{a=1}^{(q-1)/2} (q-a)\left(\frac{q-a}{q}\right) \\ &= 2\sum_{a=1}^{(q-1)/2} a\left(\frac{a}{q}\right) - q\sum_{a=1}^{(q-1)/2}\left(\frac{a}{q}\right). \qquad (26.8)\end{aligned}$$

On the other hand, decomposing $\{1, 2, \ldots, q-1\}$ as

$$\{2a : 1 \le a \le \frac{q-1}{2}\} \cup \{q - 2a : 1 \le a \le \frac{q-1}{2}\},$$

we find that

$$\begin{aligned}\sum_{a=1}^{q-1} a\left(\frac{a}{q}\right) &= \sum_{a=1}^{(q-1)/2} 2a\left(\frac{2a}{q}\right) + \sum_{a=1}^{(q-1)/2} (q-2a)\left(\frac{q-2a}{q}\right) \\ &= 4\left(\frac{2}{q}\right)\sum_{a=1}^{(q-1)/2} a\left(\frac{a}{q}\right) - \left(\frac{2}{q}\right) q\sum_{a=1}^{(q-1)/2}\left(\frac{a}{q}\right). \qquad (26.9)\end{aligned}$$

Multiplying (26.8) by $2\left(\frac{2}{q}\right)$ and subtracting the result from (26.9) yields

$$\left(1 - 2\left(\frac{2}{q}\right)\right)\sum_{a=1}^{q-1} a\left(\frac{a}{q}\right) = \left(\frac{2}{q}\right) q\sum_{a=1}^{(q-1)/2}\left(\frac{a}{q}\right).$$

To conclude, multiply both sides by $\frac{1}{q}\left(\frac{2}{q}\right)$. □

From Lemma 26.4 and (26.7),

$$\sum_{a=1}^{(q-1)/2} \left(\frac{a}{q}\right) = 2\left(2 - \left(\frac{2}{q}\right)\right)\frac{h}{w}. \qquad (26.10)$$

The right-hand side is positive, proving Theorem 26.1(b).

Venkov

We continue to assume that $q \equiv 3 \pmod 4$. From (26.10),

$$\left(2 - \left(\frac{2}{q}\right)\right) h = \frac{w}{2} \sum_{a=1}^{(q-1)/2} \left(\frac{a}{q}\right).$$

Since $w = 6$ when $q = 3$, and $w = 2$ for $q > 3$, we have that $w/2$ is always odd. Moreover, the sum on a is also odd (it involves an odd number of odd terms). It follows that h is odd, which was the first assertion of Theorem 26.2.

For the rest of the argument, we restrict to $q > 3$.

Let $n_1, \dots, n_N$ be a list of the quadratic nonresidues in $[1, \frac{q-1}{2}]$ and $r_1, \dots, r_R$ be a list of the quadratic residues from the same interval. Then the remaining quadratic residues in $[1, q-1]$ are

$$q - n_1, \quad \dots, \quad q - n_N.$$

Thus, the product of all of the residues in $[1, q-1]$ is

$$r_1 \cdots r_R (q - n_1) \cdots (q - n_N)$$

$$\equiv (-1)^N r_1 \cdots r_R \cdot n_1 \cdots n_N \equiv (-1)^N \cdot \frac{q-1}{2}! \pmod q.$$

The quadratic residues in $[1, q-1]$ can also be described as the mod q reductions of $1^2, 2^2, \dots, \left(\frac{q-1}{2}\right)^2$. From this perspective, their product is seen to be

$$\equiv \frac{q-1}{2}!^2 \equiv 1 \pmod q.$$

Equating these two evaluations shows that

$$\frac{q-1}{2}! \equiv (-1)^N \pmod q. \tag{26.11}$$

The congruence (26.11) was observed already by Dirichlet in his 1828 note (op. cit.). However, he did not (then) have the means to evaluate N modulo 2.

We do: equation (26.10) ! Since we are assuming that $q > 3$, we have $w = 2$. So (26.10) gives

$$R - N = \left(2 - \left(\frac{2}{q}\right)\right) h.$$

Since $R + N = \frac{q-1}{2}$,

$$2N = \frac{q-1}{2} - \left(2 - \left(\frac{2}{q}\right)\right) h. \tag{26.12}$$

When $q \equiv 3 \pmod 8$, (26.12) implies that

$$2N = \frac{q-1}{2} - 3h \equiv 1 + h \pmod 4.$$

Thus,

$$N \equiv \frac{1+h}{2} \pmod 2,$$

and (26.11) yields the main claim of Theorem 26.2. When $q \equiv 7 \pmod 8$, (26.12) shows that

$$2N = \frac{q-1}{2} - h \equiv 3 - h \equiv 3 + 3h \pmod 4,$$

and so

$$N \equiv 3 \cdot \frac{1+h}{2} \equiv \frac{1+h}{2} \pmod 2.$$

So the theorem holds in that case as well.

Chowla

From now on, we assume that $q \equiv 1 \pmod 4$. The following gorgeous identity plays a key role in the proof of Theorem 26.3.

Lemma 26.5. We have

$$\sqrt{q} \cdot \epsilon^h = \prod_{\substack{1 \le a \le q-1 \\ \left(\frac{a}{q}\right) = -1}} (1 - \zeta^a). \tag{26.13}$$

Proof. Since now $q \equiv 1 \pmod 4$, Theorems 23.3 and 25.1 yield

$$G \cdot \sum_{m=1}^{\infty} \frac{1}{m} \left(\frac{m}{q}\right) = \sqrt{q} \cdot \frac{2h \log \epsilon}{\sqrt{q}} = 2h \log \epsilon.$$

Substituting this into our fundamental identity (26.6) and exponentiating,

$$\epsilon^{2h} = \prod_{a=1}^{q-1} (1 - \zeta^a)^{-\left(\frac{a}{q}\right)}.$$

Thus,

$$q\epsilon^{2h} = \prod_{a=1}^{q-1}(1-\zeta^a)\cdot\prod_{a=1}^{q-1}(1-\zeta^a)^{-\left(\frac{a}{q}\right)}$$

$$= \prod_{\substack{1\le a\le q-1\\ \left(\frac{a}{q}\right)=-1}}(1-\zeta^a)^2,$$

so that

$$\prod_{\substack{1\le a\le q-1\\ \left(\frac{a}{q}\right)=-1}}(1-\zeta^a) = \pm\sqrt{q}\cdot\epsilon^h.$$

To show that the + sign should be taken, we pair the terms corresponding to a and $q-a$ in the left-hand product. (This makes sense, since $\left(\frac{a}{q}\right) = \left(\frac{q-a}{q}\right)$.) Each of the $\frac{q-1}{4}$ pairs contributes a factor of the form

$$(1-\zeta^a)(1-\zeta^{q-a}) = |1-\zeta^a|^2,$$

and thus the product is positive. □

We can now justify the claims of Theorem 26.3 about the parity of h and the sign of ϵ. Let n_0 be a fixed quadratic nonresidue modulo q. The automorphism σ (say) of $\mathbb{Q}(\zeta)$ sending ζ to ζ^{n_0} maps G to $\left(\frac{n_0}{q}\right)G = -G$. (This is just equation (23.3) again, with n_0 in place of m.) In other words,

$$\sigma(\sqrt{q}) = -\sqrt{q}.$$

Hence, $\sigma|_{\mathbb{Q}(\sqrt{q})}$ is the nontrivial automorphism of $\mathbb{Q}(\sqrt{q})$, which we will also denote with a tilde. Applying σ to both sides of (26.13) yields

$$-\sqrt{q}\cdot\tilde{\epsilon}^h = \prod_{\substack{1\le b\le q-1\\ \left(\frac{b}{q}\right)=1}}(1-\zeta^b). \tag{26.14}$$

(Here we used that $b := an_0$ runs through the quadratic residues as a runs through the nonresidues.) Multiplying (26.13) and (26.14) shows that, with $\mathrm{N}(\cdot)$ denoting the norm on $\mathbb{Q}(\sqrt{q})$,

$$-q\cdot\mathrm{N}(\epsilon)^h = \prod_{1\le k\le q-1}(1-\zeta^k) = q,$$

so that

$$\mathrm{N}(\epsilon)^h = -1.$$

This last equation does double duty, showing simultaneously that $N\epsilon = -1$ and that h is odd.

In the course of determining the sign of G in Chapter 23, we showed that, with $\pi = \zeta - 1$,

$$\sqrt{q} = G \equiv -\frac{\pi^{(q-1)/2}}{\frac{q-1}{2}!} \pmod{\pi^{(q+1)/2}}.$$

Inserting this into (26.13) and rearranging,

$$-\epsilon^h \cdot \pi^{(q-1)/2} \equiv \frac{q-1}{2}! \cdot \prod_{\substack{1 \le a \le q-1 \\ \left(\frac{a}{q}\right)=-1}} (1-\zeta^a) \pmod{\pi^{(q+1)/2}}. \tag{26.15}$$

The great unknown here (besides $\frac{q-1}{2}!$, which is what we are trying to solve for) is the right-hand product on a. Let us determine that product modulo $\pi^{(q+1)/2}$. Since

$$\begin{aligned} 1-\zeta^a &= (1-(1+\pi)^a) \\ &\equiv 1-(1+a\pi) \equiv -a\pi \pmod{\pi^2}, \end{aligned}$$

we have

$$\frac{1-\zeta^a}{\pi} \equiv -a \pmod{\pi},$$

and thus

$$\prod_{\substack{1 \le a \le q-1 \\ \left(\frac{a}{q}\right)=-1}} \frac{1-\zeta^a}{\pi} \equiv \prod_{\substack{1 \le a \le q-1 \\ \left(\frac{a}{q}\right)=-1}} (-a) \pmod{\pi}. \tag{26.16}$$

Since $q \equiv 1 \pmod 4$, as a runs through the quadratic nonresidues mod q, so does $-a$. The product of the quadratic *residues* modulo q is

$$\equiv 1^2 2^2 \cdots \left(\frac{q-1}{2}\right)^2 = \frac{q-1}{2}!^2 \equiv -1 \pmod{q}.$$

Hence, the product of the nonresidues modulo q is

$$\equiv \frac{(q-1)!}{\frac{q-1}{2}!^2} \equiv \frac{-1}{-1} \equiv 1 \pmod{q}.$$

Since $\langle \pi \rangle$ lies above q, this last congruence is also valid modulo π. Putting this back in (26.16) and multiplying through by $\pi^{(q-1)/2}$, we

conclude that

$$\prod_{\substack{1\le a\le q-1\\ (\frac{a}{q})=-1}} (1-\zeta^a) \equiv \pi^{(q-1)/2} \pmod{\pi^{(q+1)/2}}. \tag{26.17}$$

Putting (26.15) together with (26.17), we now deduce that

$$\frac{q-1}{2}! \equiv -\epsilon^h \mod \pi. \tag{26.18}$$

The congruence (26.18) is rather elegant as it stands, but it can be simplified somewhat. Since $\epsilon = \frac{1}{2}(u + v\sqrt{q})$ and π divides $\sqrt{q}$,

$$2\epsilon \equiv u \equiv 2\tilde{\epsilon} \pmod{\pi}.$$

Thus, $\epsilon \equiv \tilde{\epsilon} \pmod{\pi}$, and

$$-1 = \mathrm{N}\epsilon = \epsilon\tilde{\epsilon} \equiv \epsilon^2 \pmod{\pi}.$$

Since h is odd, (26.18) implies that

$$\frac{q-1}{2}! \equiv -(-1)^{(h-1)/2}\epsilon \pmod{\pi},$$

and so

$$2 \cdot \frac{q-1}{2}! \equiv (-1)^{(h+1)/2} \cdot u \pmod{\pi}.$$

At present, this congruence takes place in the ring $\mathbb{Z}[\zeta]$. But both sides are rational integers, and so the congruence in fact holds in $\mathbb{Z}$, modulo $\pi\mathbb{Z}[\zeta] \cap \mathbb{Z} = q\mathbb{Z}$. This completes the proof of Theorem 26.3.

Exercises

(1) This exercise presents Dirichlet's original derivation of the fundamental identity (26.6). The symbols q and ζ retain their earlier meanings, while (as in Chapter 23) we write G_a for $\sum_{n \bmod q} \left(\frac{n}{q}\right)\zeta^{an}$.

(a) For each complex number z with $|z| < 1$, let

$$L_q(z) = \sum_{m=1}^{\infty} \left(\frac{m}{q}\right) \frac{z^m}{m}.$$

Show that $L_q(z)$ is analytic for $|z| < 1$ and that

$$L_q'(z) = \sum_{n=1}^{q-1} \left(\frac{n}{q}\right) \frac{z^{n-1}}{1 - z^q}.$$

(b) Establish the partial fraction decomposition

$$\sum_{n=1}^{q-1} \left(\frac{n}{q}\right) \frac{z^{n-1}}{1 - z^q} = \sum_{a=1}^{q-1} \frac{\gamma_a}{1 - \zeta^a z},$$

where each $\gamma_a = \zeta^a \cdot G_{-a} \cdot q^{-1}$.

(c) By Abel's theorem on power series,

$$\sum_{m=1}^{\infty} \left(\frac{m}{q}\right) \frac{1}{m} = \lim_{u \uparrow 1} L_q(u);$$

equivalently, noting that $L_q(0) = 0$, we have $\sum_{m=1}^{\infty} \left(\frac{m}{q}\right) \frac{1}{m} = \lim_{u \uparrow 1} \int_{[0,u]} L_q'(z)\, dz$. Deduce from (a) and (b) that

$$\sum_{m=1}^{\infty} \left(\frac{m}{q}\right) \frac{1}{m} = -\frac{1}{q} \sum_{a=1}^{q-1} G_{-a} \operatorname{Log}(1 - \zeta^a).$$

(d) Show that $G_{-a} = \left(\frac{a}{q}\right) \cdot qG^{-1}$ and use this to complete the proof of (26.6).

(2) Let q be a prime, $q \equiv 1 \pmod 4$. Write ϵ and h for the fundamental unit and class number of $\mathbb{Z}[\frac{1+\sqrt{q}}{2}]$.

(a) Dividing (26.13) by (26.14), prove that

$$\left(\frac{\prod_n \sin(\pi n/q)}{\prod_r \sin(\pi r/q)}\right)^2 = \epsilon^{2h},$$

where n, r run over the quadratic nonresidues and residues (respectively) from $[1, \frac{q-1}{2}]$.

Hint: $(1 - \zeta^a)(1 - \zeta^{-a}) = 4 \sin^2(\pi a/q)$.

(b) In one line or less, deduce from (a) that

$$\frac{\prod_n \sin(\pi n/q)}{\prod_r \sin(\pi r/q)} = \epsilon^h. \tag{26.19}$$

In particular, the left-hand side is always larger than 1 — not at all obvious!

(3) (cf. Chowla and Chowla[11]) Let q be a prime, $q \equiv 1 \pmod 4$. Let ϵ and h denote the fundamental unit and class number of $\mathbb{Z}[\frac{1+\sqrt{q}}{2}]$, respectively. Write $\epsilon^h = \frac{1}{2}(U + V\sqrt{q})$, where $U, V \in \mathbb{Z}$.

(a) Deduce from (26.13) and (26.14) that

$$qV = \prod_{\substack{1\le n\le q-1\\ (\frac{n}{q})=-1}} (1-\zeta^n) + \prod_{\substack{1\le r\le q-1\\ (\frac{r}{q})=1}} (1-\zeta^r).$$

(b) Show that in the ring $\mathbb{Z}[x]$,

$$qV \equiv \prod_{\substack{1\le n\le q-1\\ (\frac{n}{q})=-1}} (1-x^n) + \prod_{\substack{1\le r\le q-1\\ (\frac{r}{q})=1}} (1-x^r) \pmod{\Phi_q(x)}.$$

Making the substitution $x = 2$, conclude that

$$qV \equiv \prod_{\substack{1\le n\le q-1\\ (\frac{n}{q})=-1}} (1-2^n) + \prod_{\substack{1\le r\le q-1\\ (\frac{r}{q})=1}} (1-2^r) \pmod{2^q-1}.$$

(c) Using the bound for ϵ^h appearing in Exercise 25.6, show that $qV < 2^q - 1$. Hence, qV is in fact the least nonnegative remainder of the preceding right-hand side when taken modulo $2^q - 1$.

(d) Use the result of (c) along with a computer to determine a unit > 1 in the ring of integers of $\mathbb{Q}(\sqrt{337})$.

(4) Many of the results of this chapter have variants that apply to quadratic fields not of the form $\mathbb{Q}(\sqrt{q^*})$. Here is one example: Let K be any imaginary quadratic field not $\mathbb{Q}(i)$ or $\mathbb{Q}(\sqrt{-3})$. Let χ be the Kronecker character associated to K (as defined in Chapter 25). Then, generalizing (26.10), one can show[12] that the class number

[11] Chowla, P.; Chowla, S. *Formulae for the units and class-numbers of real quadratic fields.* J. reine angew. Math. **230** (1968), 61–65.

[12] See, e.g., Chapter 26 in: Ribenboim, P. *Classical theory of algebraic numbers.* Universitext. Springer-Verlag, New York, 2001.

h of K is given by

$$h = \frac{1}{2 - \chi(2)} \sum_{1 \le n < \frac{1}{2}|\Delta_K|} \chi(n).$$

Here we outline an application of this formula to the fields $K = \mathbb{Q}(\sqrt{-q})$, where $q \equiv 1 \pmod 4$ is prime.

(a) Show that $\chi(n) = 0$ when n is even and $\chi(n) = (-1)^{(n-1)/2}\left(\frac{n}{q}\right)$ when n is odd.

(b) Use the formula for h quoted above to prove that

$$h = \sum_{\substack{0<a<q \\ a \equiv 1 \pmod 4}} \left(\frac{a}{q}\right) - \sum_{\substack{0<a<q \\ a \equiv 3 \pmod 4}} \left(\frac{a}{q}\right).$$

(c) Show that $\sum_{\substack{0<a<q \\ a \text{ odd}}} \left(\frac{a}{q}\right) = 0$ and conclude that

$$\sum_{\substack{0<a<q \\ a \equiv 1 \pmod 4}} \left(\frac{a}{q}\right) = \frac{1}{2}h.$$

(d) Making the substitution $a = q - 4m$, deduce from (c) that

$$\sum_{1 \le m \le \frac{q-1}{4}} \left(\frac{m}{q}\right) = \frac{1}{2}h.$$

In particular, there are more quadratic residues than non-residues mod q in the initial quarter interval $[1, \frac{q-1}{4}]$.[13]

(5) (Lewittes and Kolyvagin[14]) Let q be an odd prime, and let g be a primitive root mod q (meaning that g mod q generates $U(\mathbb{Z}/q\mathbb{Z})$). Then the map

$$x \mapsto g^x \bmod q$$

induces a permutation of $\{1, 2, \ldots, q-1\}$. In this exercise, we relate the sign of this permutation to the value of $\frac{q-1}{2}! \bmod q$. It will be convenient to recall that if $\sigma \in S_n$, then

$$\operatorname{sgn}(\sigma) = \prod_{1 \le i < j \le n} \frac{x_{\sigma(j)} - x_{\sigma(i)}}{x_j - x_i},$$

[13] Several variations on this theme are discussed in: Berndt, B. C. *Classical theorems on quadratic residues.* Enseignement Math. (2) **22** (1976), no. 3–4, 261–304 and Schinzel, A.; Urbanowicz, J.; Van Wamelen, P. *Class numbers and short sums of Kronecker symbols.* J. Number Theory **78** (1999), no. 1, 62–84.

[14] Lewittes, J.; Kolyvagin, V. *Primes, permutations and primitive roots.* New York J. Math. **16** (2010), 387–398.

where the quotient is calculated in $\mathbb{Z}[x_1, \dots, x_n]$. (In fact, this is sometimes taken as the definition of $\operatorname{sgn}(\sigma)$.)

(a) Show that

$$\prod_{1 \le i < j \le q-1} (j - i) \equiv -\left(\frac{2}{q}\right) \cdot \frac{q-1}{2}! \pmod{q}.$$

Hint: First group terms according to the common value k of $j - i$. Then pair the contributions from k and $q - k$.

(b) Prove that $\prod_{1 \le i < j \le q-1} (g^j - g^i) \equiv \left(\frac{2}{q}\right)$ when $q \equiv 3 \pmod 4$, and is $\equiv -\left(\frac{2}{q}\right) \cdot g^{(q-1)/4} \pmod q$ when $q \equiv 1 \pmod 4$.

Hint: First, factor out g^i from every term. Then group the factors $g^{j-i} - 1$ according to the common of value k of $j - i$, and pair the contributions from k and $q - 1 - k$.

(c) Deduce from (a), (b), and the formula for sgn that $\operatorname{sgn}(\sigma) \equiv -\frac{q-1}{2}! \pmod q$ when $q \equiv 3 \pmod 4$, and is $\equiv -\frac{q-1}{2}! \cdot g^{(q-1)/4} \pmod q$ when $q \equiv 1 \pmod 4$.

(6) (Aguirre and Peral[15]) Let q be a prime, $q \equiv 3 \pmod 4$. Consider the first quadrant region of points on or underneath the curve $y = x^2/q$ for $0 < x \le q$; i.e., the region

$$\mathcal{R} = \{(x, y) : 0 < x \le q, 0 < y \le x^2/q\}.$$

As explained in Chapter 12, we expect the area of $\mathcal{R}$ to be closely approximated by the count of lattice points lying in $\mathcal{R}$. See Figure 26.1 for the picture when $q = 11$.

(a) Prove that this count of lattice points is exactly

$$\frac{(q+1)(2q+1)}{6} - \sum_{n=1}^{q} \left\{ \frac{n^2}{q} \right\}.$$

(b) Show that

$$\sum_{k=1}^{q} \frac{k}{q} \left(1 + \left(\frac{k}{q}\right)\right) = \sum_{n=1}^{q} \left\{ \frac{n^2}{q} \right\} + 1.$$

Hint: $1 + \left(\frac{k}{q}\right)$ is the number of distinct solutions n modulo q to $n^2 \equiv k \pmod q$.

---

[15] Aguirre, J.; Peral, J. C. *Sobre el número de clases y las raíces primitivas.* Gac. R. Soc. Mat. Esp. **11** (2008), no. 4, 705–720.

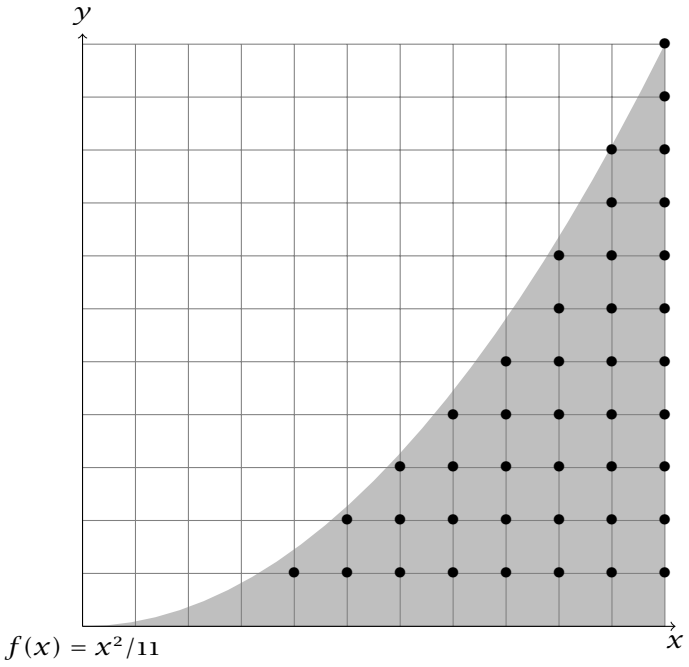


Figure 26.1. First quadrant lattice points lying on or under the curve $y = x^2/11$, for $0 < x \le 11$.

(c) Conclude that the number of lattice points always overshoots the area, and that for each $q \ge 7$ the excess is given by $\frac{2}{3} + h$, where h is the class number of $\mathbb{Q}(\sqrt{-q})$.

Exercises 7 and 8 are based on a charming American Math. Monthly article of Kurt Girstmair.[16]

(7) (Expanding $1/n$ in base g) Let g and n be coprime integers, both at least 2. For each $k \in \mathbb{Z}$, let g_k be the least nonnegative residue of g^k mod n, and for $k = 1, 2, 3, \ldots$, set $x_k = \dfrac{g g_{k-1} - g_k}{n}$.

(a) Explain why each $x_k \in \mathbb{Z}$.

(b) Show that $-1 < x_k < g$ for each k. Hence, by (a), each $x_k \in \{0, 1, \ldots, g-1\}$.

[16] Girstmair, K. *A "popular" class number formula.* Amer. Math. Monthly **101** (1994), no. 10, 997–1001.

(c) Show that $\sum_{k=1}^{\infty} x_k g^{-k} = 1/n$.

(d) Parts (a)–(c) demonstrate that $x_1, x_2, x_3, \ldots$ are the successive digits in *one* base g expansion of $1/n$. Show that this is the only base g expansion of $1/n$.

(e) Prove that the sequence of x_k is purely periodic with (not necessarily minimal) period $\varphi(n)$.

(8) (continuation) We now suppose that $n = q$, where q is an odd prime. From Exercise 7, the (unique!) base g expansion of $1/q$ can be written in the form

$$\frac{1}{q} = 0.\overline{x_1 x_2 \ldots x_{q-1}}.$$

(We are keeping the assumptions of the last exercise, so that $g \geq 2$ and g is prime to q.) Let

$$S_{g,q} = -x_1 + x_2 - x_3 + \cdots - x_{q-2} + x_{q-1}$$

be the alternating sum of the digits $x_1, \ldots, x_{q-1}$.

(a) Show that

$$S_{g,q} = -\frac{g}{q} \sum_{k=1}^{q-1} (-1)^{k-1} g_{k-1} - \frac{1}{q} \sum_{k=1}^{q-1} (-1)^k g_k.$$

(b) Show that the two sums on k have the same value, say K. Thus, $S_{g,q} = -(g+1)K/q$.

(c) Now tack on the assumption that g is a primitive root modulo q. Show that

$$K = \sum_{a=1}^{q-1} a \left(\frac{a}{q}\right).$$

(d) Conclude that $S_{g,q} = 0$ when $q \equiv 1 \pmod 4$, and that $S_{g,q} = (g+1)h_{\mathbb{Q}(\sqrt{-q})}$ when $q \equiv 3 \pmod 4$ and $q > 3$. What is $S_{g,3}$?

Example: Taking $g = 10$ and $q = 7$, we see that the trivial-seeming relation

$$-1 + 4 - 2 + 8 - 5 + 7 = 11$$

encodes that $\mathbb{Z}[\frac{1+\sqrt{-7}}{2}]$ is a UFD!

(9) Pat yourself on the back. Then head to your local library and return with another book on algebraic number theory.

Hint: QA247.

Index