Algorithmic Number Theory
MSRI Publications
Volume **44**, 2008

The arithmetic of number rings

PETER STEVENHAGEN

ABSTRACT. We describe the main structural results on number rings, that is, integral domains for which the field of fractions is a number field. Whenever possible, we avoid the algorithmically undesirable hypothesis that the number ring in question is integrally closed.

CONTENTS

1. Introduction 209
2. Number rings 211
3. Localization 214
4. Invertible ideals 215
5. Ideal factorization in number rings 217
6. Integral closure 220
7. Linear algebra over $\mathbb{Z}$ 224
8. Explicit ideal factorization 228
9. Computing the integral closure 233
10. Finiteness theorems 236
11. Zeta functions 242
12. Computing class groups and unit groups 244
13. Completions 253
14. Adeles and ideles 255
15. Galois theory 258
Acknowledgments 263
References 264

1. Introduction

The ring $\mathbb{Z}$ of 'ordinary' integers lies at the very root of number theory, and when studying its properties, the concept of *divisibility* of integers naturally leads to basic notions as primality and congruences. By the 'fundamental theorem of arithmetic', $\mathbb{Z}$ admits *unique prime factor decomposition* of nonzero integers. Though one may be inclined to take this theorem for granted, its proof

is not completely trivial: it usually employs the Euclidean algorithm to show that the prime numbers, which are defined as *irreducible* elements having only 'trivial' divisors, are *prime elements* that only divide a product of integers if they divide one of the factors.

In the time of Euler, it gradually became clear that in solving problems concerning integers, it can be effective to pass from $\mathbb{Z}$ to larger rings that are not contained in the field $\mathbb{Q}$ of rational numbers but in number fields, that is, in finite field extensions of $\mathbb{Q}$. Such *number rings*, which occur everywhere in this volume, will be our objects of study. In [Lenstra 2008], we encounter the classical example of the Pell equation $x^2 - dy^2 = 1$, which can be viewed as the equation $(x + y\sqrt{d})(x - y\sqrt{d}) = 1$ in the quadratic ring $\mathbb{Z}[\sqrt{d}]$. In a similar way, writing an integer n as a sum $n = x^2 + y^2$ of two squares amounts to decomposing n as a product $n = (x + yi)(x - yi)$ of two conjugate elements in the ring $\mathbb{Z}[i]$ of Gaussian integers. The cyclotomic number ring $\mathbb{Z}[\zeta_p]$ obtained by adjoining a primitive p-th root of unity ζ_p has been fundamental in studying the Fermat equation $x^p + y^p = z^p$ since the first half of the nineteenth century, and it occurs center stage in Mihăilescu's recent treatment [2006] of the Catalan equation $x^p - 1 = y^q$. See also [Schoof 2008a].

Whereas the ring $\mathbb{Z}[i]$ is in many respects similar to $\mathbb{Z}$, an interesting property of the rings $\mathbb{Z}[\sqrt{d}]$ arising in the study of the Pell equation is that, unlike $\mathbb{Z}$, they have an *infinite* unit group. Kummer discovered around 1850 that the Fermat equation for prime exponent $p \geq 3$ has no solutions in nonzero integers if $\mathbb{Z}[\zeta_p]$ admits factorization into prime elements. As we now know [Washington 1997, Chapter 11], only the rings $\mathbb{Z}[\zeta_p]$ with $p \leq 19$ have this property. All other rings $\mathbb{Z}[\zeta_p]$, and in fact all number rings, admit factorization into irreducible elements, but this is not very useful as it is often not in any way unique. Kummer and others invented a theory of prime *ideal* factorization to salvage this situation. It lies at the heart of the algebraic number theory developed during the nineteenth century.

In the early twentieth century, Hensel showed how to *complete* the ring $\mathbb{Z}$ and other number rings at their prime ideals. This gives rise to rings in p-adic or *local* fields, which are algebraically simpler than number fields and in certain ways similar to the archimedean complete fields $\mathbb{R}$ and $\mathbb{C}$ of real and complex numbers. It led to the introduction of various 'analytic' techniques and gave rise to the insight that many questions in number rings can be studied *locally*, much like geometers study curves by focusing on neighborhoods of points. Precise formulations require the description of number theoretic objects in the language of 'abstract algebra', the language of groups, rings and fields that has become fundamental in many parts of mathematics.

Contrary to what is sometimes thought, the use of more abstract theory and language is not at all incompatible with algorithmic approaches to algebraic number theory. The recent advances with respect to 'down to earth' problems as integer factoring [Stevenhagen 2008] and primality testing [Schoof 2008c] rely on 'large' number rings and on Galois extensions of finite rings to achieve their goal. In the first case, the number rings $\mathbb{Z}[\alpha]$ one encounters are not necessarily the 'textbook rings' for which the nineteenth century theory was developed, whereas in the second case, Galois theory for rings rather than for fields is exploited. These examples show that number rings have 'concrete' algorithmic applications to problems not traditionally inside the domain of algebraic number theory, and that such applications require a slightly more general theory than is found in the classical textbooks. Fortunately, commutative algebra and, more in particular, ring theory provide us with the tools that are needed for this. In the case of number rings, the number field sieve alluded to above shows that it is undesirable to have a theory that only works for rings of integers in number fields, which may be computationally inaccessible, and that one needs to consider 'singular' number rings as well. In this paper, we impose no a priori restrictions on our number rings and define them as *arbitrary* subrings of number fields. As a consequence, the various localizations of number rings we encounter are in this same category. Special attention will be devoted to *orders* in number fields as defined in the next section, which play an important role in algorithmic practice. The analogy between number rings and algebraic curves explains the geometric flavor of much of our terminology, but we do not formally treat the case of subrings of function fields [Rosen 2002].

Number rings are the central objects in computational algebraic number theory, and algorithms in more specific areas as class field theory [Cohen and Stevenhagen 2008] assume that one can efficiently deal with them. In this paper, which is mostly a survey of more or less classical algebraic number theory, we include the modest amount of ring theory that is necessary to state and prove the results in the generality required by algorithmic practice. The next section introduces number rings and orders, and explains their relation to the classical textbook ring, the ring of integers. In addition, it outlines the further contents of this paper.

2. Number rings

A *number ring* is a domain R for which the field of fractions $K = Q(R)$ is a *number field*, that is, a field of finite degree over $\mathbb{Q}$. Note that this is a rather general definition, and that already inside $\mathbb{Q}$ there are infinitely many number rings, such as $\mathbb{Q}$ itself and $\mathbb{Z}[\frac{1}{2}, \frac{1}{3}]$. In many ways, $\mathbb{Z}$ is the 'natural' number ring in $\mathbb{Q}$ to work with, as it governs the 'arithmetic behavior' of $\mathbb{Q}$ in a sense

we will make precise. In a similar way, the arithmetic properties of an arbitrary number field K are classically described in terms of the *ring of integers*

$$\mathcal{O}_K = \{x \in K : f_{\mathbb{Q}}^x \in \mathbb{Z}[X]\} \tag{2-1}$$

of K, which consists of the elements $x \in K$ for which the monic irreducible polynomial $f_{\mathbb{Q}}^x$ over $\mathbb{Q}$, also known as the *minimal polynomial* of x over $\mathbb{Q}$, has integer coefficients. This *integral closure* of $\mathbb{Z}$ in K is a natural algebraic notion and, as will be shown just before Theorem 6.5, a *ring*; it may however be inaccessible in computational practice.

Already in the case of a quadratic field $K = \mathbb{Q}(\sqrt{d})$ associated to a nonsquare integer d, we need to write d as $d = m^2 \cdot d_0$ with d_0 squarefree in order to find $\mathcal{O}_K$, which is equal to $\mathbb{Z}[\sqrt{d_0}]$ or, in the case $d_0 \equiv 1 \bmod 4$, to $\mathbb{Z}[(1+\sqrt{d_0})/2]$. The only way we know to find d_0 proceeds by factoring d, which we may not be able to do for large d. However, even if we are unable to find a non-trivial square factor dividing d, we can often use the number ring $R = \mathbb{Z}[\sqrt{d}]$ (or $R = \mathbb{Z}[(1+\sqrt{d})/2]$) instead of $\mathcal{O}_K$ for our algorithmic purposes. Of course, we do need to know in which ways the subring R will be 'just as good' as $\mathcal{O}_K$ itself, and in which ways it may fail to behave nicely. In this quadratic case, the subrings of $\mathcal{O}_K$ are well understood, and there is a classical description of their arithmetic in terms of binary quadratic forms that goes back to Gauss. Among their algorithmic 'applications', one finds a subexponential factoring algorithm for arbitrary integers d, the *class group method* [Seysen 1987].

Our potential inability to find the square divisors of large integers is also a fundamental obstruction [Buchmann and Lenstra 1994] to computing $\mathcal{O}_K$ in other number fields K. Indeed, let K be given as $K = \mathbb{Q}(\alpha)$, with α the root of some monic irreducible polynomial $f = f_{\mathbb{Q}}^{\alpha} \in \mathbb{Q}[X]$ of degree $n = [K : \mathbb{Q}]$. Replacing α by $k\alpha$ for a suitable integer k when necessary, we may assume that f has integral coefficients. Then the index of $R = \mathbb{Z}[\alpha] = \mathbb{Z}[X]/(f)$ in $\mathcal{O}_K$ is finite, and we show in (7-7) that its square divides the discriminant $\Delta(f)$ of the polynomial f. Finding $\mathcal{O}_K$ starts with finding squares dividing $\Delta(f)$, which may not be feasible if the integer $\Delta(f)$ is too large to be factored. Such discriminants occur for the polynomials that are used in the number field sieve, and they force us to work with subrings of K that are possibly smaller than the ring of integers $\mathcal{O}_K$.

The *simple integral extensions* $\mathbb{Z}[\alpha]$ obtained by adjoining to $\mathbb{Z}$ a root α of some monic irreducible polynomial $f \in \mathbb{Z}[X]$, also known as *monogenic* number rings, are in many ways computationally convenient to work with. The 'power basis' $1, \alpha, \alpha^2, \ldots, \alpha^{n-1}$ of $K = \mathbb{Q}(\alpha)$ as a vector space over $\mathbb{Q}$ is also a basis for $\mathbb{Z}[\alpha]$ as a module over $\mathbb{Z}$. More generally, a subring $R \subset K$ that is free of rank $n = [K : \mathbb{Q}]$ over $\mathbb{Z}$ is called an *order* in K. An element $x \in K$ is integral if

and only if $\mathbb{Z}[x]$ is an order in K, so $\mathbb{O}_K$ is the union of all orders $\mathbb{Z}[x] \subset K$. The following will be proved in Section 7, as a direct corollary of formula (7-6).

THEOREM 2.2. *A number ring $R \subset K$ is an order in K if and only if it is of finite index in $\mathbb{O}_K$.*

This shows that $\mathbb{O}_K$ is the *maximal order* in K. It need not be monogenic (Example 8.6).

In an arbitrary number ring R, the role played in $\mathbb{Z}$ by the prime numbers is taken over by the nonzero prime ideals or *primes* of R. Every ideal in R containing α contains the multiples of the integer $f_{\mathbb{Q}}^{\alpha}(0)$, so nonzero ideals in R 'divide' ordinary integers in the ideal-theoretic sense of the word. As R/kR is finite of order at most $k^n = k^{[K:\mathbb{Q}]}$ for $k \in \mathbb{Z}_{\geq 1}$, with equality in the case that R is an order, every nonzero ideal in a number ring is of finite index. In particular, all R-ideals are finitely generated, and all primes of R are maximal. In ring-theoretic terms, number rings are *noetherian domains* of *dimension* at most 1. Every prime $\mathfrak{p} \subset R$ contains a unique prime number p, the characteristic of the finite field $R/\mathfrak{p}$. We say that $\mathfrak{p}$ *extends* p or *lies over* p, and call the degree $f(\mathfrak{p}/p)$ of $R/\mathfrak{p}$ over the prime field $\mathbf{F}_p$ the *residue class degree* of $\mathfrak{p}$ over p.

In the next three sections, we describe ideal factorization in arbitrary number rings R (Theorems 5.2 and 5.3), which turns out to be especially nice if R equals or contains the ring of integers $\mathbb{O}_K$ of its field of fractions (Theorems 5.7 and 6.5). Some linear algebra over $\mathbb{Z}$ (Section 7) is involved in explicit factorization (Section 8), and the local computations involved in factoring rational primes in R lead to algorithms to find $\mathbb{O}_K$ starting from an order R (Section 9).

When using ideal factorization as a replacement for element factorization, the need arises to control the difference between elements and ideals. The problem of *nonprincipality* of ideals is quantified by the Picard group of the number ring introduced in Section 4. The problem of element identities 'up to units' arising from ideal arithmetic necessitates control of the unit groups of number rings. The classical *finiteness theorems* in Section 10 show that the Picard groups of number rings are finite (Corollary 10.6) and that the unit groups of many number rings are finitely generated (Theorem 10.9). The proofs of these theorems, which do not hold for arbitrary noetherian domains of dimension 1, exploit embeddings of number rings and their unit groups as lattices in Euclidean vector spaces. They are not directly constructive, and based on the *geometry of numbers*. Section 12 presents various explicit examples showing how the relevant groups may be computed using the explicit factorization techniques from Section 8. To guarantee that no units or Picard group relations have been overlooked, one uses the *analytic* information from Section 11 on the size of Picard and unit groups for $\mathbb{O}_K$; this information is encoded by the *zeta function* of the underlying number field. Relating the Picard group of R to that of the

ring of integers is made possible by the comparison statements Theorem 6.5 and 6.7.

Although actual computations are by their finite nature bound to process rational or algebraic numbers only, many mathematical *ideas* are most elegantly expressed in terms of 'limit objects' such as real numbers, which can only be approximated by computers. Number rings are naturally embedded in *local fields* (Section 13) and *adele rings* (Section 14), which are similar in nature to real numbers and provide a conceptual clarification of our local approach to number rings. The final Section 15 deals with Galois theoretic aspects of number rings.

3. Localization

When dealing algorithmically with a number field K defined by some monic polynomial $f \in \mathbb{Z}[X]$, one often starts out with the simple order $R = \mathbb{Z}[\alpha]$ defined by f, and enlarges it to a bigger order whenever this is made possible by computations. This makes it important to carry over knowledge about, say, the primes over p in R to similar information in the larger ring. In this case, 'nothing changes' as long as the index of R in the extension ring is coprime to p. Such statements are most conveniently made precise and proved by working 'locally', in a way that was already familiar to geometers in the nineteenth century. Algebraically, the corresponding process of localization of rings and modules [Atiyah and Macdonald 1969, Chapter 2] has become a standard procedure.

For a number ring R with field of fractions K, one can form a localized ring

$$S^{-1}R = \{r/s \in K : r \in R,\ s \in S\} \subset K$$

whenever $S \subset R$ is a subset containing 1 that is closed under multiplication. There is a localization $K = Q(R)$ corresponding to $S = R \setminus \{0\}$, and, more generally, by taking $S = R \setminus \mathfrak{p}$, we have localizations

$$R_{\mathfrak{p}} = \{r/s \in K : r \in R,\ s \notin \mathfrak{p}\}$$

at all prime ideals $\mathfrak{p}$ of R. The number rings $R_{\mathfrak{p}}$ are *local number rings* in the sense that they have a unique maximal ideal

$$\mathfrak{p}R_{\mathfrak{p}} = \{r/s \in K : r \in \mathfrak{p},\ s \notin \mathfrak{p}\}$$

consisting of the complement of the unit group $R_{\mathfrak{p}}^* = \{\frac{r}{s} \in K : r, s \notin \mathfrak{p}\}$. Conversely, a local number ring R with maximal ideal $\mathfrak{p}$ is equal to its localization $R_{\mathfrak{p}}$ at $\mathfrak{p}$.

EXAMPLE 3.1. For $R = \mathbb{Z}$, the localization $\mathbb{Z}_{(p)} = \{r/s \in \mathbb{Q} : p \nmid s\}$ at the prime p is a local ring with maximal ideal $\mathfrak{p} = p\mathbb{Z}_{(p)}$. Every fraction $x \in \mathbb{Q}^*$ can

uniquely be written as $x = up^k$ with $u \in \mathbb{Z}_{(p)}^* = \{r/s \in \mathbb{Q} : p \nmid rs\}$ and $k \in \mathbb{Z}$. It follows that the ideals of $\mathbb{Z}_{(p)}$ are simply the powers of the principal ideal $\mathfrak{p}$, and this makes $\mathbb{Z}_{(p)}$ into the prototype of what is known as a *discrete valuation ring*. As will become clear in Proposition 5.4, these particularly simple rings arise as the localizations of a number ring R at all of its 'regular' primes.

Localization often enables us to reduce the complexity of a number ring R at hand by passing to a localized ring $S^{-1}R$. The ideals of $S^{-1}R$ are of the form $S^{-1}I = \{i/s : i \in I,\ s \in S\}$, with I an ideal of the *global* ring R, and whenever $I \cap S$ is nonempty we have $S^{-1}I = S^{-1}R$. The primes of $S^{-1}R$ are the ideals $S^{-1}\mathfrak{p}$ with $\mathfrak{p}$ a prime of R that does not meet S, and the natural map $R \to S^{-1}R$ induces an isomorphism between the local rings at $\mathfrak{p}$ and at $S^{-1}\mathfrak{p}$, respectively. If $R \subset R'$ is of finite index, we have $S^{-1}R = S^{-1}R' \subset K$ for all localizations for which the index is in S.

EXAMPLE 3.2. Taking R an arbitrary number ring and $S = \{x \in \mathbb{Z} : p \nmid x\}$, as in Example 3.1, we obtain a *semilocal* number ring $R_{(p)}$ having only finitely many primes $\mathfrak{p}$, all containing p. The primes of $R_{(p)}$ correspond to the primes of R lying over p. If R is of finite index in $\mathbb{O}_K$ and p is a prime number not dividing this index, the inclusion map $R \to \mathbb{O}_K$ becomes the identity when localized at S, and the local rings of R and $\mathbb{O}_K$ are naturally isomorphic at primes over p. Informally phrased, R and $\mathbb{O}_K$ are 'the same' at all primes that do not divide the index $[\mathbb{O}_K : R]$. Section 6 contains a more precise formulation of these statements.

4. Invertible ideals

As Kummer discovered, it is not in general possible to factor a nonzero element x in a number ring R into prime divisors, but something similar can be obtained when looking at 'ideal divisors' of x, that is, the ideals $I \subset R$ that satisfy $IJ = (x)$ for some R-ideal J.

For the modern reader, ideals are defined more generally as kernels of ring homomorphisms, and in this setting I is said to *divide* J whenever I contains J. For a number ring R with field of fractions K, it is convenient to slightly extend the concept of R-ideals and consider *fractional* R-ideals, that is, R-submodules $I \subset K$ with the property that rI is a *nonzero* R-ideal for some $r \in R$. If we can take $r = 1$, then I is an ordinary R-ideal, usually referred to as an *integral* R-ideal. For fractional ideals I and J, we define the *ideal quotient* as

$$I : J = \{x \in K : xJ \subset I\}.$$

A standard verification shows that the sum, intersection, product, and quotient of two fractional ideals are again fractional ideals. For every fractional R-ideal I,

the localized ideal $S^{-1}I$ is a fractional $S^{-1}R$-ideal. Moreover, localization respects the standard operations on ideals of taking sums, products, and intersections.

A fractional R-ideal I is said to be *invertible* if there exists an R-ideal J such that IJ is a nonzero principal R-ideal. These 'ideals in Kummer's sense' are precisely the ones we need to 'factor' nonzero elements of R, and for which ideal multiplication gives rise to a *group operation*. If I is invertible, we have $I \cdot I^{-1} = R$ for the fractional R-ideal

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

and its *multiplier ring*

$$\Lambda(I) = \{x \in K : xI \subset I\},$$

which clearly contains R, is actually equal to R as we have

$$\Lambda(I) = \Lambda(I)I \cdot I^{-1} \subset I \cdot I^{-1} = R.$$

The invertible fractional R-ideals form an abelian group $\mathcal{I}(R)$ under ideal multiplication. Clearly, all principal fractional R-ideals are invertible, and they form a subgroup $\mathcal{P}(R) = \{xR : x \in K^*\} = K^*/R^*$ of $\mathcal{I}(R)$.

For a principal ideal domain R such as $R = \mathbb{Z}$, *all* fractional ideals are of the form xR with $x \in K^*$, and we have $\mathcal{I}(R) = \mathcal{P}(R)$. For arbitrary number rings R, the quotient group $\mathrm{Pic}(R) = \mathcal{I}(R)/\mathcal{P}(R)$ measuring the difference between invertible and principal R-ideals is known as the *Picard group* or the *class group* of R. It fits in an exact sequence

$$1 \longrightarrow R^* \longrightarrow K^* \longrightarrow \mathcal{I}(R) \longrightarrow \mathrm{Pic}(R) \longrightarrow 1. \tag{4-1}$$

If $R = \mathbb{O}_K$ is the ring of integers of K, then $\mathrm{Pic}(\mathbb{O}_K)$, which only depends on K, is often referred to as the 'class group of K' and is denoted by Cl_K. It is a fundamental invariant of the number field K.

The Picard group of a number ring R vanishes if R is a principal ideal domain. The converse statement does not hold in general: a number ring with trivial Picard group may have noninvertible ideals that are nonprincipal.

EXAMPLES 4.2. In the quadratic field $\mathbb{Q}(\sqrt{-3})$, the ring of integers $\mathbb{O} = \mathbb{Z}[\alpha]$ with $\alpha = (1 + \sqrt{-3})/2$ is a principal ideal domain as it admits a Euclidean 'division with remainder' with respect to the complex absolute value. In other words: for nonzero $\beta, \gamma \in \mathbb{O}$ there exist $q, r \in \mathbb{O}$ with $\beta/\gamma = q + r/\gamma$ and $|r| < |\gamma|$. In a picture, this boils down to the observation that the open disks of radius 1 around the points of $\mathbb{O}$ in the complex plane cover all of $\mathbb{C}$.

Taking $R = \mathbb{Z}[\sqrt{-3}]$ instead of $\mathbb{O}$, the R-translates of α are outside the open disks of radius 1 around R, and we find that every fractional R-ideal is either

principal or of the form xI with $I = \mathbb{Z} + \mathbb{Z} \cdot \alpha$. The nonprincipal ideals xI have multiplier ring $\Lambda(xI) = \Lambda(I) = \mathbb{Z}[\alpha] \supsetneq R$, so they are not invertible, and we still have $\mathrm{Pic}(R) = 0$. The prime ideal $\mathfrak{p} = 2I = \mathbb{Z} \cdot 2 + \mathbb{Z} \cdot (1 + \sqrt{-3})$ of R of index 2 satisfies $\mathfrak{p}^2 = 2\mathfrak{p}$, which shows that $\mathfrak{p}$ is not invertible and that multiplication of arbitrary ideals in R is not a 'group-like' operation.

For the order $\mathbb{O} = \mathbb{Z}[\sqrt{-5}]$, which is the ring of integers in $\mathbb{Q}(\sqrt{-5})$, the analogous picture shows that every fractional $\mathbb{O}$-ideal is either principal or of the form xI with $I = \mathbb{Z} + \mathbb{Z} \cdot (1 + \sqrt{-5})/2$. In this case $\mathfrak{p} = 2I \subset \mathbb{O}$ satisfies $\mathfrak{p}^2 = 2\mathbb{O}$, which shows that *all* fractional $\mathbb{O}$-ideals are invertible and that $\mathrm{Pic}(\mathbb{O})$ is cyclic of order 2.

If R is a number ring and I a fractional R-ideal, the localized ideals $I_\mathfrak{p}$ at the primes of R are fractional $R_\mathfrak{p}$-ideals, and they are equal to $R_\mathfrak{p}$ for almost all $\mathfrak{p}$. The ideal I can be recovered from its localizations as we have

$$I = \bigcap_\mathfrak{p} I_\mathfrak{p}. \tag{4-3}$$

To obtain the non-trivial inclusion $\supset$, note that for $x \in \bigcap_\mathfrak{p} I_\mathfrak{p}$, the ideal $\{r \in R : rx \in I\}$ equals R as it is not contained in any prime of R.

PROPOSITION 4.4. *Let R be a number ring and I a fractional R-ideal. Then I is invertible if and only if $I_\mathfrak{p}$ is a principal $R_\mathfrak{p}$-ideal for all primes $\mathfrak{p}$.*

PROOF. If I is invertible, there exist $x_i \in I$ and $y_i \in I^{-1}$ with $\sum_{i=1}^n x_i y_i = 1$. Let $\mathfrak{p} \subset R$ be a prime. All terms $x_i y_i$ are in $R \subset R_\mathfrak{p}$, and they cannot all be in the maximal ideal of $R_\mathfrak{p}$. Suppose that we have $x_1 y_1 \in R_\mathfrak{p}^* = R_\mathfrak{p} \setminus \mathfrak{p}R_\mathfrak{p}$. Then any $x \in I$ can be written as $x = x_1 \cdot (x_1 y_1)^{-1} \cdot x y_1 \in x_1 R_\mathfrak{p}$. It follows that $I_\mathfrak{p}$ is principal with generator x_1.

For the converse, we argue by contradiction. If I is not invertible, there exists a prime $\mathfrak{p}$ containing the ideal $II^{-1} \subset R$. Let $x \in I$ be an $R_\mathfrak{p}$-generator of $I_\mathfrak{p}$. If I is generated over R by x_i for $i = 1, 2, \ldots, n$, we can write $x_i = x(r_i/s) \in R_\mathfrak{p}$, with $s \in R \setminus \mathfrak{p}$ independent of i. Then we have $sx^{-1}x_i = r_i \in R$ for all i, whence $sx^{-1}I \subset R$. We obtain $s = x \cdot sx^{-1} \in II^{-1} \subset \mathfrak{p}$, a contradiction. □

By Proposition 4.4, we may view the Picard group as a local-global obstruction group measuring the extent to which the locally principal R-ideals are globally principal.

5. Ideal factorization in number rings

It is not generally true that nonzero ideals in number rings, invertible or not, can be factored into a product of prime ideals. We can however use (4-3) to decompose $I \subset R$ into its $\mathfrak{p}$-*primary parts*

$$I_{(\mathfrak{p})} = I_\mathfrak{p} \cap R$$

at the various primes $\mathfrak{p}$ of R. We have $I_{(\mathfrak{p})} = R$ if $\mathfrak{p}$ does not divide I.

LEMMA 5.1. *Let $R_{\mathfrak{p}}$ be a local number ring. Then every nonzero ideal of $R_{\mathfrak{p}}$ contains some power of the maximal ideal of $R_{\mathfrak{p}}$.*

PROOF. As $R_{\mathfrak{p}}$ is noetherian, we can apply *noetherian induction*: if there are counterexamples to the lemma, the set of such ideals contains an element I that is maximal with respect to the ordering by inclusion. Then I is not prime, as the only nonzero prime ideal of $R_{\mathfrak{p}}$ is the maximal ideal. Let $x, y \in R \setminus I$ satisfy $xy \in I$. Then $I + (x)$ and $I + (y)$ strictly contain I, so they do satisfy the conclusion of the lemma and contain a power of the maximal ideal. The same then holds for $(I + (x))(I + (y)) \subset I$. Contradiction. □

By Lemma 5.1, the $\mathfrak{p}$-primary part $I_{(\mathfrak{p})}$ of a nonzero ideal $I \subset R$ contains some power of $\mathfrak{p}$. As there are no inclusions between different primes in number rings, this implies that $\mathfrak{p}$-primary parts at different $\mathfrak{p}$ are coprime.

THEOREM 5.2. *Let R be a number ring. Then every nonzero ideal $I \subsetneq R$ has a primary decomposition $I = \prod_{\mathfrak{p} \supset I} I_{(\mathfrak{p})}$, and we have natural isomorphisms*

$$R/I \xrightarrow{\sim} \prod\nolimits_{\mathfrak{p} \supset I} R/I_{(\mathfrak{p})} \xrightarrow{\sim} \prod\nolimits_{\mathfrak{p} \supset I} R_{\mathfrak{p}}/I_{\mathfrak{p}}.$$

PROOF. We have $I = \bigcap_{\mathfrak{p}} I_{\mathfrak{p}} = \bigcap_{\mathfrak{p}} I_{(\mathfrak{p})}$ by (4-3), and we may take the intersections over those $\mathfrak{p}$ that contain I only. By the coprimality of $\mathfrak{p}$-primary parts, the finite intersection obtained is actually a *product* $I = \prod_{\mathfrak{p} \supset I} I_{(\mathfrak{p})}$.

The isomorphism $R/I \xrightarrow{\sim} \prod_{\mathfrak{p} \supset I} R/I_{(\mathfrak{p})}$ is a special case of the Chinese remainder theorem for a product of pairwise coprime ideals. The localization map $R/I_{(\mathfrak{p})} \to R_{\mathfrak{p}}/I_{\mathfrak{p}}$ is injective by the definition of $I_{(\mathfrak{p})}$; for its surjectivity, we show that every $s \in R \setminus \mathfrak{p}$ is a unit in $R/I_{(\mathfrak{p})}$. By the maximality of $\mathfrak{p}$, there is an element $s' \in R \setminus \mathfrak{p}$ such that $ss' - 1$ is in $\mathfrak{p}$. As $I_{(\mathfrak{p})}$ contains $\mathfrak{p}^n$ for some n by Lemma 5.1, the element $ss' - 1$ is nilpotent in $R/I_{(\mathfrak{p})}$, so s is a unit. □

For *invertible* ideals, we can decompose the *group* $\mathcal{I}(R)$ of invertible fractional R-ideals in a similar way into $\mathfrak{p}$-primary components. By Proposition 4.4, invertible ideals are locally principal at each $\mathfrak{p}$, giving rise to elements of $\mathcal{P}(R_{\mathfrak{p}})$.

THEOREM 5.3. *Let R be a number ring. Then we have an isomorphism*

$$\phi : \mathcal{I}(R) \xrightarrow{\sim} \bigoplus_{\mathfrak{p} \text{ prime}} \mathcal{P}(R_{\mathfrak{p}})$$

that maps I to its vector of localizations $(I_{\mathfrak{p}})_{\mathfrak{p}}$ at the primes $\mathfrak{p}$ of R. □

To proceed from primary decomposition to prime ideal factorization, it is necessary that the localizations $I_{\mathfrak{p}}$ or, equivalently, the $\mathfrak{p}$-primary parts $I_{(\mathfrak{p})}$ of an ideal I are powers of $\mathfrak{p}$. For the local rings $\mathbb{Z}_{(p)}$ of $R = \mathbb{Z}$, this is the case by

Example 3.1. For general number rings R, this depends on the nature of the local rings $R_\mathfrak{p}$.

PROPOSITION 5.4. *For a prime* $\mathfrak{p}$ *of a number ring* R, *the three following are equivalent*:

(1) $\mathfrak{p}$ *is an invertible* R*-ideal*;
(2) $R_\mathfrak{p}$ *is a principal ideal domain, and every* $R_\mathfrak{p}$*-ideal is a power of* $\mathfrak{p}R_\mathfrak{p}$;
(3) *there exists* $\pi \in R_\mathfrak{p}$ *such that every* $x \in K^*$ *can uniquely be written as* $x = u \cdot \pi^k$ *with* $u \in R_\mathfrak{p}^*$ *and* $k \in \mathbb{Z}$.

PROOF. For (1) $\Rightarrow$ (2), we use Proposition 4.4 to write $\mathfrak{p}R_\mathfrak{p} = \pi R_\mathfrak{p}$ and observe that all inclusions in the chain of principal $R_\mathfrak{p}$-ideals $R_\mathfrak{p} \supset \mathfrak{p}R_\mathfrak{p} = (\pi) \supset (\pi^2) \supset (\pi^3) \supset \ldots$ are strict: an equality $(\pi^n) = (\pi^{n+1})$ would imply $\pi^n = r\pi^{n+1}$ for some $r \in R_\mathfrak{p}$, whence $r\pi = 1$ and $\pi \in R_\mathfrak{p}^*$. We need to show there are no further $R_\mathfrak{p}$-ideals. Let $I \subset R_\mathfrak{p}$ be a nonzero ideal. As I contains all sufficiently large powers of (π) by Lemma 5.1, there is a largest value $n \geq 0$ for which we have $(\pi^n) \supset I$. Take any $r \in I \setminus (\pi^{n+1})$; then we have $r = a\pi^n$ with $a \notin (\pi)$. This implies that a is a unit in $R_\mathfrak{p}$, so we have $(r) = (\pi^n) \subset I \subset (\pi^n)$ and $I = (\pi^n)$.

For (2) $\Rightarrow$ (3), take for π a generator of $\mathfrak{p}R_\mathfrak{p}$. For every $x \in R_\mathfrak{p}$, we have $(x) = (\pi^k)$ for some uniquely determined integer $k \geq 0$, and $x = u \cdot \pi^k$ with $u \in R_\mathfrak{p}^*$. Taking quotients, we obtain (3).

For (3) $\Rightarrow$ (1), we note that we have $\pi \notin R_\mathfrak{p}^*$ and therefore

$$R_\mathfrak{p} = \{u \cdot \pi^k : u \in R_\mathfrak{p}^* \text{ and } k \geq 0\} \cup \{0\}.$$

This shows $R_\mathfrak{p}$ is local with principal maximal ideal (π); so $\mathfrak{p}$ is invertible. □

If the conditions in Proposition 5.4 are met, we call $\mathfrak{p}$ a *regular* prime of R and the local number ring $R_\mathfrak{p}$ a *discrete valuation ring*. The exponent k in (3) is then the *order* $\mathrm{ord}_\mathfrak{p}(x)$ to which $\mathfrak{p}$ occurs in $x \in K^*$, and the associated map $x \mapsto \mathrm{ord}_\mathfrak{p}(x)$ is the *discrete valuation* from which R derives its name. It is a homomorphism $K^* \to \mathbb{Z}$ satisfying

$$\begin{aligned} \mathrm{ord}_\mathfrak{p}(xy) &= \mathrm{ord}_\mathfrak{p}(x) + \mathrm{ord}_\mathfrak{p}(y), \\ \mathrm{ord}_\mathfrak{p}(x+y) &\geq \min\{\mathrm{ord}_\mathfrak{p}(x), \mathrm{ord}_\mathfrak{p}(y)\} \end{aligned} \tag{5-5}$$

for all $x, y \in K$. We formally put $\mathrm{ord}_\mathfrak{p}(0) = +\infty$. With this convention, we have

$$R_\mathfrak{p} = \{x \in K : \mathrm{ord}_\mathfrak{p}(x) \geq 0\}. \tag{5-6}$$

If $x \in K$ has negative valuation, we have $R_\mathfrak{p}[x] = K$, so a discrete valuation ring in K is a *maximal* subring of K different from K.

If all primes of a number ring R are regular, R is said to be a *Dedekind domain*. As the next section will show, all rings of integers in number fields are

Dedekind domains. For such rings, the primary decomposition from Theorems 5.2 and 5.3 becomes a true prime ideal factorization, as all localizations $I_{\mathfrak{p}}$ of any fractional R-ideal I are then of the form $\mathfrak{p}^k$ for some exponent $k = \mathrm{ord}_{\mathfrak{p}}(I) \in \mathbb{Z}$, the *valuation* of I at $\mathfrak{p}$, that is equal to 0 for almost all $\mathfrak{p}$.

THEOREM 5.7. *For a number ring R that is Dedekind, there is an isomorphism*

$$\begin{aligned} \mathcal{J}(R) &\xrightarrow{\sim} \bigoplus_{\mathfrak{p}} \mathbb{Z} \\ I &\longmapsto (\mathrm{ord}_{\mathfrak{p}}(I))_{\mathfrak{p}}, \end{aligned}$$

and every $I \in \mathcal{J}(R)$ factors uniquely as a product $I = \prod_{\mathfrak{p}} \mathfrak{p}^{\mathrm{ord}_{\mathfrak{p}}(I)}$. □

If R is Dedekind, then *all* fractional R-ideals are invertible, and the Picard group $\mathrm{Pic}(R)$ is better known as the *class group* $\mathrm{Cl}(R)$ of R. It vanishes if and only if the Dedekind domain R is a principal ideal domain.

6. Integral closure

A number ring R is Dedekind if all of its localizations $R_{\mathfrak{p}}$ are discrete valuation rings, and in this case we have prime ideal factorization as in Theorem 5.7. Algorithmically, it may not be easy to test whether a given number ring is Dedekind. Theoretically, however, every number ring R has a unique extension $R \subset \mathbb{O}$ inside its field of fractions K that is of finite index over R, and is regular at all primes. This *normalization* of R is the smallest Dedekind domain containing R, and represents what geometers would call a 'desingularization' of R.

The normalization of a number ring R is defined as the *integral closure* of R in its field of fractions K. It consists of those $x \in K$ that are *integral* over R, that is, for which there exists a monic polynomial $f \in R[X]$ with $f(x) = 0$. If R equals its integral closure, it is said to be *integrally closed*. This is a 'local property'.

PROPOSITION 6.1. *A number ring R is integrally closed if and only if all of the localizations $R_{\mathfrak{p}}$ at its primes $\mathfrak{p}$ are integrally closed.*

PROOF. Note that R and its localizations have the same field of fractions K. If $x \in K$ is integral over R, it is obviously integral over all $R_{\mathfrak{p}}$. If all $R_{\mathfrak{p}}$ are integrally closed, we then have $x \in \bigcap_{\mathfrak{p}} R_{\mathfrak{p}} = R$ by (4-3), so R is integrally closed.

Conversely, suppose $x \in K$ satisfies an integrality relation $x^n = \sum_{k=0}^{n-1} r_k x^k$ with $r_k \in R_{\mathfrak{p}}$ for some $\mathfrak{p}$. If $s \in R \setminus \mathfrak{p}$ is chosen such that we have $s r_k \in R$ for all k, multiplication by s^n yields an integrality relation $(sx)^n = \sum_{k=0}^{n-1} r_k s^{n-k} (sx)^k$ for sx with coefficients $r_k s^{n-k} \in R$. If R is integrally closed, we have $sx \in R$ and therefore $x \in R_{\mathfrak{p}}$. Thus $R_{\mathfrak{p}}$ is integrally closed. □

PROPOSITION 6.2. *A local number ring is integrally closed if and only if it is a discrete valuation ring.*

COROLLARY 6.3. *A number ring is Dedekind if and only if it is integrally closed.*

Corollary 6.3 is immediate from Propositions 6.1 and 6.2. To prove 6.2, it is convenient to rephrase the definition of integrality in the following way.

LEMMA 6.4. *An element $x \in K$ is integral over R if and only if there exists a finitely generated R-module $M \subset K$ with $M \neq 0$ and $xM \subset M$.*

PROOF. For integral x, the ring $R[x]$ is finitely generated as an R-module and yields a module M of the required sort. For the converse, observe that the inclusion $xM \subset M$ for $M = Rm_1 + \cdots + Rm_n$ gives rise to identities $xm_i = \sum_{j=1}^{n} r_{ij} m_j$ for $j = 1, 2, \ldots, n$. As the $n \times n$ matrix $A = x \cdot \mathrm{id}_n - (r_{ij})_{i,j=1}^{n}$ with entries in K maps the nonzero vector $(m_i)_i \in K^n$ to zero, we have $\det(A) = 0$, resulting in an integrality relation $x^n + \sum_{k=0}^{n-1} r_k x^k = 0$ for x. □

PROOF OF PROPOSITION 6.2. If $R \subset K$ is a discrete valuation ring, $\mathrm{ord}_{\mathfrak{p}}$ is the associated valuation, and $x \in K$ satisfies $\mathrm{ord}_{\mathfrak{p}}(x) < 0$, then a relation $x^n = \sum_{k=0}^{n-1} r_k x^k$ with $r_k \in R$ cannot hold since the valuation of the left hand side is by (5-5) and (5-6) smaller than that of the right hand side. This shows that R is integrally closed.

Conversely, let R be an integrally closed local number ring with maximal ideal $\mathfrak{p}$, and pick a nonzero element $a \in \mathfrak{p}$. By Lemma 5.1, there exists a smallest positive integer n for which $\mathfrak{p}^n$ is contained in aR. Choose $b \in \mathfrak{p}^{n-1} \setminus aR$, and take $\pi = a/b$. By construction, we have $\pi^{-1} = b/a \notin R$ and $\pi^{-1}\mathfrak{p} \subset R$. As $\mathfrak{p}$ is a finitely generated R-module and $\pi^{-1} = b/a$ is not integral over R, we see from Lemma 6.4 that we cannot have $\pi^{-1}\mathfrak{p} \subset \mathfrak{p}$. It follows that $\pi^{-1}\mathfrak{p}$ equals R, so we have $\mathfrak{p} = \pi R$, and R is a discrete valuation ring. □

Using Lemma 6.4, it is easy to see that the integral closure $\mathbb{O}$ of a number ring R is indeed a ring: for R-integral $x, y \in K$, the finitely generated module $M = R[x, y]$ is multiplied into itself by $x \pm y$ and xy. Moreover, if $x \in K$ is integral over $\mathbb{O}$ and $M \subset \mathbb{O}$ is the R-module generated by the coefficients of an integrality relation for x over $\mathbb{O}$, then $R[x] \cdot M$ is a finitely generated R-module that is multiplied into itself by x. Thus x is integral over R and contained in $\mathbb{O}$. This shows that $\mathbb{O}$, or, more generally, the integral closure in K of *any* subring of K, is integrally closed. Clearly, $\mathbb{O}$ is the smallest Dedekind domain containing R.

THEOREM 6.5. *The integral closure $\mathbb{O}$ of a number ring R in $K = Q(R)$ equals*

$$\mathbb{O} = R\mathbb{O}_K = \mathbb{O}_{K,T} = \{x \in K : \mathrm{ord}_{\mathfrak{p}}(x) \geq 0 \text{ for all } \mathfrak{p} \notin T\}$$

for some set $T = T(R)$ of primes of $\mathbb{O}_K$.

PROOF. It is clear that $\mathbb{O}$ contains R and $\mathbb{O}_K$, and therefore $R\mathbb{O}_K$. To see that $R\mathbb{O}_K$ is a Dedekind domain and therefore equal to $\mathbb{O}$, we note that any of its localizations $(R\mathbb{O}_K)_\mathfrak{p}$ contains as a subring the localization of $\mathbb{O}_K$ at $\mathbb{O}_K \cap \mathfrak{p}$. This is a discrete valuation ring and, by the maximality of discrete valuation rings, it is equal to $(R\mathbb{O}_K)_\mathfrak{p}$.

We find that the primes of $\mathbb{O}$ correspond to a subset of the primes of $\mathbb{O}_K$, and that the local rings at corresponding primes coincide. Describing these as in (5-6), we arrive at the given description of $\mathbb{O}$ as the intersection of its localizations. □

We say that the ring $\mathbb{O}_{K,T}$ in Theorem 6.5 is obtained from $\mathbb{O}_K$ by 'inverting the primes in T'. The set $T = T(R)$ consists of those primes $\mathfrak{p}$ of $\mathbb{O}_K$ for which R is not contained in the localization of $\mathbb{O}_K$ at $\mathfrak{p}$. It is empty if and only if R is an order.

The class group of the Dedekind domain $\mathbb{O}_{K,T}$ can be obtained from $\mathrm{Cl}(\mathbb{O}_K) = \mathrm{Cl}_K$. The localization map $\mathbb{O}_K \to \mathbb{O}_{K,T}$ yields a natural map $I \mapsto I \cdot \mathbb{O}_{K,T}$ from $\mathcal{I}(\mathbb{O}_K)$ to $I(\mathbb{O}_{K,T})$ which maps principal ideals to principal ideals. This induces a homomorphism between the defining sequences (4-1) for their class groups, and the 'middle map' $\mathcal{I}(\mathbb{O}_K) \to I(\mathbb{O}_{K,T})$ is by Theorem 5.7 the natural surjection $\bigoplus_\mathfrak{p} \mathbb{Z} \to \bigoplus_{\mathfrak{p} \notin T} \mathbb{Z}$ with kernel $\bigoplus_{\mathfrak{p} \in T} \mathbb{Z}$. It follows that the natural map

$$\mathrm{Cl}_K \to \mathrm{Cl}(\mathbb{O}_{K,T})$$

is surjective, and an easy application of the snake lemma [Lang 2002, Section III.9] yields the exact sequence

$$1 \longrightarrow \mathbb{O}_K^* \longrightarrow \mathbb{O}_{K,T}^* \longrightarrow \bigoplus_{\mathfrak{p} \in T} \mathbb{Z} \xrightarrow{\varphi} \mathrm{Cl}_K \longrightarrow \mathrm{Cl}(\mathbb{O}_{K,T}) \longrightarrow 1. \qquad (6\text{-}6)$$

Here φ maps the generator corresponding to $\mathfrak{p} \in T$ to the class $[\mathfrak{p}] \in \mathrm{Cl}_K$. Thus $\mathrm{Cl}(\mathbb{O}_{K,T})$ is the quotient of Cl_K modulo the subgroup generated by the ideal classes of the primes in T.

The inclusion map $R \to \mathbb{O}$ of a number ring R in its normalization $\mathbb{O}$ also gives rise to an induced map $\mathrm{Pic}(R) \to \mathrm{Cl}(\mathbb{O})$ given by $[I] \mapsto [I\mathbb{O}]$. We conclude this section by analyzing it in a similar way. As the relation between primes in R and $\mathbb{O}$ is of a different nature, the argument is slightly more involved.

At every prime $\mathfrak{p}$ of a number ring, the local ring $R_\mathfrak{p}$ is a subring of the ring $\mathbb{O}_\mathfrak{p}$ obtained by localizing the normalization $\mathbb{O}$ of R at $S = R \setminus \mathfrak{p}$. If $\mathfrak{p}$ is regular, we have $R_\mathfrak{p} = \mathbb{O}_\mathfrak{p}$ by the maximality property of discrete valuation rings in K, and R and $\mathbb{O}$ are 'locally the same' at $\mathfrak{p}$. If $\mathfrak{p}$ is noninvertible or *singular*, the inclusion $R_\mathfrak{p} \subset \mathbb{O}_\mathfrak{p}$ is strict as $\mathbb{O}_\mathfrak{p}$ is integrally closed by Proposition 6.1 and $R_\mathfrak{p}$ is not. Define the *conductor* of R in its normalization $\mathbb{O}$ as

$$\mathfrak{f}_R = \{x \in \mathbb{O} : x\mathbb{O} \subset R\}.$$

This is an ideal in both R and $\mathbb{O}$ and the largest $\mathbb{O}$-ideal contained in R. For $R = \mathbb{Z}[\sqrt{-3}] \subset \mathbb{O} = \mathbb{Z}[(1+\sqrt{-3})/2]$ from 4.2, we have $R = \mathbb{Z} + 2\mathbb{O}$ and $\mathfrak{f}_R = 2\mathbb{O}$.

For an order R the conductor is nonzero by Theorem 2.2, proved in the next section; for arbitrary R the same is true as the index of the order $R \cap \mathbb{O}_K$ in $\mathbb{O}_K$ is an integer that multiplies $\mathbb{O} = R\mathbb{O}_K$ into R. From the comparison of local rings, we have

$$\mathfrak{p} \text{ is regular} \iff R_\mathfrak{p} = \mathbb{O}_\mathfrak{p} \iff \mathfrak{p} \nmid \mathfrak{f}_R,$$

so the conductor $\mathfrak{f}_R$ is a measure of the 'singularity' of R. Note that only finitely many primes of R can be singular, just as algebraic curves only have finitely many singular points.

At the singular primes $\mathfrak{p}$, which divide $\mathfrak{f}_R$ and in particular the index $[\mathbb{O} : R]$, the local ring $R_\mathfrak{p}$ is a subring of finite index in $\mathbb{O}_\mathfrak{p}$. The primes of the *semilocal* ring $\mathbb{O}_\mathfrak{p}$ are the ideals $\mathfrak{q}\mathbb{O}_\mathfrak{p}$ coming from the primes $\mathfrak{q}$ of $\mathbb{O}$ extending $\mathfrak{p}$. As $\mathbb{O}_\mathfrak{p}$ is a Dedekind domain with only finitely many primes, it has trivial Picard group by the Chinese remainder theorem, and by Theorem 5.3 we can write its ideal group as

$$\mathcal{I}(\mathbb{O}_\mathfrak{p}) = \bigoplus_{\mathfrak{q} \supset \mathfrak{p}} \mathcal{P}(\mathbb{O}_\mathfrak{q}) = \mathcal{P}(\mathbb{O}_\mathfrak{p}) = K^*/\mathbb{O}_\mathfrak{p}^*.$$

THEOREM 6.7. *Let $R \subset \mathbb{O}$ be a number ring of conductor $\mathfrak{f}$ in its normalization $\mathbb{O}$, and $\nu : \mathrm{Pic}(R) \to \mathrm{Cl}(\mathbb{O})$ the natural map defined by $\nu([I]) = [I \cdot \mathbb{O}]$. Then we have a natural exact sequence*

$$1 \longrightarrow R^* \longrightarrow \mathbb{O}^* \longrightarrow (\mathbb{O}/\mathfrak{f})^*/(R/\mathfrak{f})^* \longrightarrow \mathrm{Pic}(R) \xrightarrow{\nu} \mathrm{Cl}(\mathbb{O}) \longrightarrow 1.$$

PROOF. Write the Picard groups of R and $\mathbb{O}$ in terms of their defining exact sequence (4-1), and express $\mathcal{I}(R)$ and $\mathcal{I}(\mathbb{O})$ as in Theorem 5.3. Using the identity for $K^*/\mathbb{O}_\mathfrak{p}^*$ preceding the theorem, we obtain a diagram

$$\begin{array}{ccccccccc}
1 & \longrightarrow & K^*/R^* & \longrightarrow & \bigoplus_\mathfrak{p} K^*/R_\mathfrak{p}^* & \longrightarrow & \mathrm{Pic}(R) & \longrightarrow & 1 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
1 & \longrightarrow & K^*/\mathbb{O}^* & \longrightarrow & \bigoplus_\mathfrak{p} K^*/\mathbb{O}_\mathfrak{p}^* & \longrightarrow & \mathrm{Cl}(\mathbb{O}) & \longrightarrow & 1
\end{array}$$

with exact rows. Again, the middle vertical map is surjective, this time with kernel $\oplus_\mathfrak{p} \mathbb{O}_\mathfrak{p}^*/R_\mathfrak{p}^*$. By the snake lemma, $\mathrm{Pic}(R) \to \mathrm{Cl}(\mathbb{O})$ is surjective and its kernel N fits in an exact sequence $1 \to \mathbb{O}^*/R^* \to \bigoplus_\mathfrak{p} \mathbb{O}_\mathfrak{p}^*/R_\mathfrak{p}^* \to N \to 1$. We are thus reduced to giving a natural isomorphism $(\mathbb{O}/\mathfrak{f})^*/(R/\mathfrak{f})^* \xrightarrow{\sim} \bigoplus_\mathfrak{p} \mathbb{O}_\mathfrak{p}^*/R_\mathfrak{p}^*$. Note that we may restrict the direct sum above to the singular primes $\mathfrak{p} \mid \mathfrak{f}$, since at regular primes we have $\mathbb{O}_\mathfrak{p} = R_\mathfrak{p}$, and therefore $\mathbb{O}_\mathfrak{p}^*/R_\mathfrak{p}^* = 1$.

We first apply Theorem 5.2 to $I = \mathfrak{f}$ to obtain localization isomorphisms $R/\mathfrak{f} \cong \bigoplus_{\mathfrak{p}} R_{\mathfrak{p}}/\mathfrak{f}R_{\mathfrak{p}}$ and $\mathbb{O}/\mathfrak{f} \cong \bigoplus_{\mathfrak{p}} \bigoplus_{\mathfrak{q}\supset\mathfrak{p}} \mathbb{O}_{\mathfrak{q}}/\mathfrak{f}\mathbb{O}_{\mathfrak{q}} \cong \bigoplus_{\mathfrak{p}} \mathbb{O}_{\mathfrak{p}}/\mathfrak{f}\mathbb{O}_{\mathfrak{p}}$. Taking unit groups, we arrive at a natural isomorphism

$$(\mathbb{O}/\mathfrak{f})^*/(R/\mathfrak{f})^* \cong \bigoplus_{\mathfrak{p}\mid\mathfrak{f}} (\mathbb{O}_{\mathfrak{p}}/\mathfrak{f}\mathbb{O}_{\mathfrak{p}})^*/(R_{\mathfrak{p}}/\mathfrak{f}R_{\mathfrak{p}})^*. \tag{6-8}$$

For $\mathfrak{p} \mid \mathfrak{f}$, an element $x \in \mathbb{O}_{\mathfrak{p}}$ is invertible modulo $\mathfrak{f}\mathbb{O}_{\mathfrak{p}}$ if and only if it is not contained in any maximal ideal $\mathfrak{q}\mathbb{O}_{\mathfrak{p}} \supset \mathfrak{p}\mathbb{O}_{\mathfrak{p}} \supset \mathfrak{f}\mathbb{O}_{\mathfrak{p}}$, that is, if and only if it is in $\mathbb{O}_{\mathfrak{p}}^*$. It follows that the natural map $\mathbb{O}_{\mathfrak{p}}^* \to (\mathbb{O}_{\mathfrak{p}}/\mathfrak{f}\mathbb{O}_{\mathfrak{p}})^*$ is surjective. From the equality $\mathfrak{f}\mathbb{O} = \mathfrak{f}R$ we obtain $\mathfrak{f}\mathbb{O}_{\mathfrak{p}} = \mathfrak{f}R_{\mathfrak{p}}$, so $(R_{\mathfrak{p}}/\mathfrak{f}R_{\mathfrak{p}})^*$ is a subgroup of $(\mathbb{O}_{\mathfrak{p}}/\mathfrak{f}\mathbb{O}_{\mathfrak{p}})^*$, and the image of $x \in \mathbb{O}_{\mathfrak{p}}^*$ lies in it exactly when we have $x \in R_{\mathfrak{p}}^*$. We obtain natural maps $\mathbb{O}_{\mathfrak{p}}^*/R_{\mathfrak{p}}^* \xrightarrow{\sim} (\mathbb{O}_{\mathfrak{p}}/\mathfrak{f}\mathbb{O}_{\mathfrak{p}})^*/(R_{\mathfrak{p}}/\mathfrak{f}R_{\mathfrak{p}})^*$ at all $\mathfrak{p}$. Combining this with (6-8), we obtain the desired isomorphism. □

EXAMPLE 6.9. Let K be a quadratic field with ring of integers $\mathbb{O} = \mathbb{O}_K = \mathbb{Z}[\omega]$. For each positive integer f, there is a unique subring $R = R_f = \mathbb{Z}[f\omega] = \mathbb{Z} + \mathbb{Z} \cdot f\omega$ of index f in $\mathbb{O}$. It has conductor $\mathfrak{f}_R = f\mathbb{O}$, and its Picard group $\mathrm{Pic}(R)$ is the *ring class group* of the order of conductor f in $\mathbb{O}$. This class group can be described as a *form class group* of binary quadratic forms, and it has an interpretation in class field theory [Cohen and Stevenhagen 2008] as the Galois group of the *ring class field* of conductor f over K. By Theorem 6.7, it is the extension

$$1 \longrightarrow (\mathbb{O}/f)^*/\operatorname{im}[\mathbb{O}^*](\mathbb{Z}/f\mathbb{Z})^* \longrightarrow \mathrm{Pic}(R) \longrightarrow \mathrm{Cl}_K \longrightarrow 1$$

of Cl_K by a finite abelian group that is easily computed, especially for imaginary quadratic K, which have $\mathbb{O}^* = \{\pm 1\}$ in all but two cases.

For the order $R = \mathbb{Z}[\sqrt{-3}]$ of index 2 in $\mathbb{O} = \mathbb{Z}[\omega]$ with $\omega = (1+\sqrt{-3})/2$, the group $\mathbb{F}_4^*/\langle\omega\rangle\mathbb{F}_2^*$ vanishes, and we find as in Examples 4.2 that, just like $\mathrm{Cl}(\mathbb{O})$, the Picard group $\mathrm{Pic}(R)$ is trivial.

7. Linear algebra over $\mathbb{Z}$

Before we embark on the algorithmic approach to the ring theory of the preceding sections, we discuss the computational techniques from linear algebra that yield finiteness statements such as Theorem 2.2, and more.

Let A be a ring, and B an A-algebra that is free of finite rank n over A. For $x \in B$, let $M_x : B \to B$ denote the A-linear multiplication map $b \mapsto xb$. With respect to an A-basis of $B = \bigoplus_{i=1}^n A \cdot x_i$, the map M_x can be described by an $n \times n$ matrix with coefficients in A, and we define the *norm* and the *trace* from B to A by

$$N_{B/A}(x) = \det M_x \qquad \text{and} \qquad \mathrm{Tr}_{B/A}(x) = \operatorname{trace} M_x.$$

It follows immediately from this definition that the norm is a multiplicative map, whereas the trace $\mathrm{Tr}_{B/A} : B \to A$ is a homomorphism of the additive groups.

The notions of norm and trace are stable under *base change*. This means that if $f : A \to A'$ is *any* ring homomorphism and $f_* : B \to B' = B \otimes_A A'$ is the induced map from B to the free A'-algebra $B' = \bigoplus_{i=1}^n A' \cdot (x_i \otimes 1)$, the diagrams

$$\begin{array}{ccc} B & \xrightarrow{f_*} & B' = B \otimes_A A' \\ {\scriptstyle N_{B/A}\atop\scriptstyle \mathrm{Tr}_{B/A}}\downarrow & & \downarrow{\scriptstyle N_{B'/A'}\atop\scriptstyle \mathrm{Tr}_{B'/A'}} \\ A & \xrightarrow{f} & A' \end{array}$$

describing the 'base change' $A \to A'$ for norm and trace commute. Indeed, for an element $x \in B$ the multiplication matrix of $f_*(x)$ on B' with respect to the A'-basis $x_1 \otimes 1, x_2 \otimes 1, \ldots, x_n \otimes 1$ is obtained by applying f to the entries of M_x with respect to the A-basis $x_1, x_2, \ldots, x_n$.

Base changing a domain A to its field of fractions suffices to recover the classical 'linear algebra fact' that norms and traces do not depend on the choice of a basis for B over the domain A. In fact, the issue of dependency on a basis does not even arise if one uses *coordinatefree* definitions for the determinant and the trace of an endomorphism $M \in \mathrm{End}_A(B)$ of a free A-module B of rank n. For the determinant, one notes [Bourbaki 1989, Section III.8.1] that the n-th exterior power $\bigwedge^n B$ is a free A-module of rank 1 on which M induces scalar multiplication by $\det M \in A$. For the trace [Bourbaki 1989, Section II.4.1], one views $\mathrm{End}_A(B) = B \otimes_A B^*$ as the tensor product of B with its dual module $B^* = \mathrm{Hom}_A(B, A)$ and defines $\mathrm{Tr}_{B/A}(\sum b \otimes f) = \sum f(b)$.

For an order $B = R$ in K, base changing from $A = \mathbb{Z}$ to $\mathbb{Q}$ and to $\mathbb{F}_p$, respectively, shows that the norm and trace maps $R \to \mathbb{Z}$ are the restrictions to R of the 'field maps' $K \to \mathbb{Q}$, and that their reductions modulo p are the norm and trace maps $R/pR \to \mathbb{F}_p$ for the $\mathbb{F}_p$-algebra R/pR.

For $B = K$ a number field of degree n over $A = \mathbb{Q}$, we can use the n distinct embeddings $\sigma_i : K \to \mathbb{C}$ and the base change $\mathbb{Q} \to \mathbb{C}$ to diagonalize the matrix for M_x as $M_x = (\sigma_i(x))_{i=1}^n$, since we have an isomorphism

$$\begin{aligned} K \otimes_{\mathbb{Q}} \mathbb{C} &\xrightarrow{\sim} \mathbb{C}^n \\ x \otimes y \quad &\longmapsto (\sigma_i(x)y)_{i=1}^n. \end{aligned} \tag{7-1}$$

This yields the formulas $N_{K/\mathbb{Q}}(x) = \prod_{i=1}^n \sigma_i(x)$ and $\mathrm{Tr}_{K/\mathbb{Q}}(x) = \sum_{i=1}^n \sigma_i(x)$ for the norm and trace from K to $\mathbb{Q}$.

In a free A-algebra B of rank n, the *discriminant* of $x_1, x_2, \ldots, x_n \in B$ is defined as

$$\Delta(x_1, x_2, \ldots, x_n) = \det(\mathrm{Tr}_{B/A}(x_i x_j))_{i,j=1}^n,$$

and the *discriminant* $\Delta(B/A)$ of B over A is the discriminant of any A-basis of B. We have $(\mathrm{Tr}_{B/A}(y_i y_j))_{i,j=1}^n = T \cdot (\mathrm{Tr}_{B/A}(x_i x_j))_{i,j=1}^n \cdot T^t$ for any $n \times n$ matrix $T \in \mathrm{GL}_n(A)$ over A transforming $\{x_i\}_{i=1}^n$ to $\{y_i\}_{i=1}^n$, so the discriminant of a free A-algebra does depend on the choice of the basis, but only up to the square of a unit in A. Over a field A, it is usually the vanishing of $\Delta(B/A)$ that has intrinsic significance, and the algebras of non-vanishing discriminant are known as *separable* A-algebras. Over $A = \mathbb{Z}$, the discriminant

$$\Delta(R) = \det(\mathrm{Tr}_{R/\mathbb{Z}}(x_i x_j))_{i,j=1}^n \in \mathbb{Z} \tag{7-2}$$

of an order $R = \bigoplus_{i=1}^n \mathbb{Z} \cdot x_i$ of rank n is a well-defined integer. Considering arbitrary $\mathbb{Z}$-linear transformations of bases, one obtains, for an inclusion $R' \subset R$ of orders in K, the index formula

$$\Delta(R') = [R : R']^2 \cdot \Delta(R). \tag{7-3}$$

The discriminant of an order $R = \bigoplus_{i=1}^n \mathbb{Z} \cdot x_i$ in K can also be defined in terms of the embeddings $\sigma_i : K \to \mathbb{C}$ from (7-1) as

$$\Delta(R) = [\det(\sigma_i(x_j))_{i,j=1}^n]^2. \tag{7-4}$$

To see that (7-4) agrees with (7-2), one multiplies the matrix $X = (\sigma_i(x_j))_{i,j=1}^n$ by its transpose and uses the description of the trace map following (7-1) to find

$$X^t \cdot X = \left(\textstyle\sum_{k=1}^n \sigma_k(x_i x_j)\right)_{i,j=1}^n = \left(\mathrm{Tr}_{L/K}(x_i x_j)\right)_{i,j=1}^n.$$

Taking determinants, the desired equality follows.

For an order $\mathbb{Z}[\alpha]$ in $K = \mathbb{Q}(\alpha)$, the elements $\alpha_i = \sigma_i(\alpha)$ are the roots of $f_{\mathbb{Q}}^{\alpha}$, and by (7-4) its discriminant can be evaluated as the square of a Vandermonde determinant and equals the polynomial discriminant $\Delta(f_{\mathbb{Q}}^{\alpha})$:

$$\begin{aligned} \Delta(\mathbb{Z}[\alpha]) = \Delta(1, \alpha, \alpha^2, \ldots, \alpha^{n-1}) &= [\det(\sigma_i(\alpha^{j-1}))_{i,j=1}^n]^2 \\ &= [\det(\alpha_i^{j-1})_{i,j=1}^n]^2 = \textstyle\prod_{i>j}(\alpha_i - \alpha_j)^2 = \Delta(f_{\mathbb{Q}}^{\alpha}). \end{aligned} \tag{7-5}$$

In the same way, one shows that the discriminant over a field A of a simple field extension $A \subset A(\alpha)$ is up to squares in A^* equal to $\Delta(f_A^{\alpha})$. The extension $A \subset A(\alpha)$ is separable (as a field extension of A, or as an A-algebra) if and only if $f_{\mathbb{Q}}^{\alpha}$ is a separable polynomial.

For an order R in K containing $\mathbb{Z}[\alpha]$, the identities (7-3) and (7-5) yield

$$\Delta(f_{\mathbb{Q}}^{\alpha}) = [R : \mathbb{Z}[\alpha]]^2 \cdot \Delta(R), \tag{7-6}$$

so $\Delta(R)$ is nonzero. We also see that we have $\mathbb{Z}[\alpha] \subset R \subset d^{-1}\mathbb{Z}[\alpha]$ for every order R containing α, with d the largest integer for which d^2 divides $\Delta(f_{\mathbb{Q}}^{\alpha})$. It follows that $\mathbb{O}_K$ itself is an order contained in $d^{-1}\mathbb{Z}[\alpha]$, and in principle $\mathbb{O}_K$ can be found by a finite computation starting from $\mathbb{Z}[\alpha]$: there are finitely many

residue classes in $d^{-1}\mathbb{Z}[\alpha]/\mathbb{Z}[\alpha]$, and for each class one decides whether it is in $\mathbb{O}_K/\mathbb{Z}[\alpha]$ by computing the irreducible polynomial of an element from the class and checking whether it is integral. Finally, (7-6) implies that any order in K is of finite index in $\mathbb{O}_K$; so we have proved Theorem 2.2.

The discriminant $\Delta_K = \Delta(\mathbb{O}_K)$ is often referred to as the *discriminant of* K. It is a fundamental invariant of K, and by (7-6) it satisfies

$$\Delta(f_{\mathbb{Q}}^{\alpha}) = [\mathbb{O}_K : \mathbb{Z}[\alpha]]^2 \cdot \Delta_K \tag{7-7}$$

for every $\alpha \in \mathbb{O}_K$ of degree n. In cases where $\Delta(f_{\mathbb{Q}}^{\alpha})$ can be factored, (7-7) is used as the starting point for the computation of the extension $\mathbb{Z}[\alpha] \subset \mathbb{O}_K$. If we are lucky and $\Delta(f_{\mathbb{Q}}^{\alpha})$ can be shown to be squarefree, then we know immediately that $\mathbb{Z}[\alpha]$ is the full ring of integers $\mathbb{O}_K$, and that we have $\Delta_K = \Delta(f_{\mathbb{Q}}^{\alpha})$.

EXAMPLE 7.8. Let K be imaginary quadratic of discriminant Δ_K, and let $\tau \in K \setminus \mathbb{Q}$ be a zero of the irreducible polynomial $f_{\mathbb{Z}}^{\tau} = aX^2 + bX + c \in \mathbb{Z}[X]$. Then $I = \mathbb{Z} + \mathbb{Z} \cdot \tau$ is an invertible ideal for the order

$$R_\tau = \mathbb{Z}[a\tau] = \Lambda(I) = \{x \in K : xI \subset I\}.$$

As $a\tau$ is a zero of $X^2 + bX + ac \in \mathbb{Z}[X]$, the order R_τ has discriminant

$$\Delta(R_\tau) = b^2 - 4ac = f^2 \Delta_K$$

by (7-5) and (7-7), with f the index of R_τ in $\mathbb{O}_K$.

As any quadratic order R has field of fractions $K = \mathbb{Q}(\sqrt{\Delta(R)})$, it is determined up to isomorphism by its discriminant, which can uniquely be written as $\Delta(R) = f^2 \Delta_K$. In higher degree, there exist non-isomorphic *maximal* orders having the same discriminant.

To compute polynomial discriminants, one makes use of the *resultant*. The resultant of nonzero polynomials $g = b\prod_{i=1}^{r}(X - \beta_i)$ and $h = c\prod_{j=1}^{s}(X - \gamma_j)$ with coefficients and zeros in some field is defined as

$$R(g,h) = b^s c^r \prod_{i=1}^{r}\prod_{j=1}^{s}(\beta_i - \gamma_j).$$

It can be expressed [Lang 2002, Section IV.8] as a determinant in terms of the coefficients of g and h, but computations are usually based on the following obvious properties:

(R1) $R(g,h) = (-1)^{rs} R(h,g)$;
(R2) $R(g,h) = b^s \prod_{i=1}^{r} h(\beta_i)$;
(R3) $R(g,h) = b^{s-s_1} R(g,h_1)$ if $h_1 \neq 0$ satisfies $h_1 \equiv h \bmod g$ and $s_1 = \deg h_1$.

For an element $g(\alpha) \in K = \mathbb{Q}(\alpha)$, property (R2) yields

$$N_{K/\mathbb{Q}}(g(\alpha)) = R(f, g).$$

For $f = f_{\mathbb{Q}}^{\alpha}$ as above and $\alpha_i = \sigma_i(\alpha)$, one has $f'(\alpha_1) = \prod_{i \geq 2}(\alpha_1 - \alpha_i)$. Taking g to be the derivative f' of f, one can write the discriminant of f as

$$\Delta(f) = \prod_{i<j}(\alpha_i - \alpha_j)^2 = (-1)^{n(n-1)/2} N_{K/\mathbb{Q}}(f'(\alpha)) = (-1)^{n(n-1)/2} R(f, f').$$

This reduces the computation of norms and polynomial discriminants to the computation of resultants, which can be performed inside the field containing the coefficients of the polynomials.

EXAMPLE 7.9. The discriminant of the polynomial $X^n + a$ equals

$$(-1)^{n(n-1)/2} R(X^n + a, nX^{n-1}) = (-1)^{n(n-1)/2} n^n a^{n-1}.$$

For $f = X^3 - X^2 - 15X - 75$, long division shows that the remainder of f upon division by its derivative $f' = 3X^2 - 2X - 15$ equals $f - \frac{1}{9}(3X - 1)f' = -\frac{9}{88}(X - \frac{15}{2})$. This is a linear polynomial with zero $\frac{15}{2}$, so we find

$$\begin{aligned} \Delta(f) = -R(f', f) &= 3^2 \cdot R(f', -\tfrac{88}{9}(X - \tfrac{15}{2})) \\ &= 3^2 \cdot R(-\tfrac{88}{9}(X - \tfrac{15}{2}), f') \\ &= -3^2 \cdot (-\tfrac{88}{9})^2 \cdot f'(\tfrac{15}{2}) = -2^4 \cdot 3 \cdot 5^2 \cdot 11^2. \end{aligned}$$

8. Explicit ideal factorization

In order to factor an ideal I in a number ring R in the sense of Theorem 5.2, we have to determine for all primes $\mathfrak{p} \supset I$ the $\mathfrak{p}$-primary part $I_{(\mathfrak{p})}$ of I. Every prime $\mathfrak{p} \supset I$ divides the index $[R : I]$, so a first step towards factoring I consists of factoring $[R : I]$ in $\mathbb{Z}$ to determine the rational primes p over which the primes $\mathfrak{p} \mid I$ lie.

The index map $I \mapsto [R : I]$ for integral R-ideals extends to a *multiplicative* map $\mathcal{J}(R) \to \mathbb{Q}^*$ on invertible ideals known as the *ideal norm*. Its multiplicativity follows from Theorems 5.2 and 5.3 and the observation that for *principal* $R_{\mathfrak{p}}$-ideals, the index is a multiplicative function. At regular primes $\mathfrak{p}$, all ideals in $R_{\mathfrak{p}}$ are principal by Proposition 5.4. At singular primes this is not the case, and the behavior of the singular prime $\mathfrak{p} = (2, 1 + \sqrt{-3}) \subset R = \mathbb{Z}[\sqrt{-3}]$ in Examples 4.2 is typical: $[R : \mathfrak{p}^2] = [R : 2\mathfrak{p}] = 2^3 > 2^2 = [R : \mathfrak{p}]^2$.

If R is an order, the ideal norm of a principal ideal $xR \subset R$ equals $|N_{R/\mathbb{Z}}(x)|$ as the element norm is by definition the determinant of the multiplication map $M_x : R \to R$, and we have $[R : M_x[R]] = |\det M|$ for the $\mathbb{Z}$-module R. By

multiplicativity, this compatibility of element and ideal norms in orders extends to all $x \in K^*$.

If singular primes are encountered in R, one usually replaces R by an extension ring in which the primes over p are all regular, and then $\mathrm{ord}_{\mathfrak{p}}(I)$ can be determined to complete the factorization of I. If possible, one tries to take R to be the ring of integers $\mathbb{O}_K$, which has no singular primes at all.

Given a number field $K = \mathbb{Q}(\alpha)$ generated by an element α with irreducible monic polynomial $f \in \mathbb{Z}[X]$, we have the simple order $\mathbb{Z}[\alpha] \subset \mathbb{O}_K$ as a first approximation to $\mathbb{O}_K$, and factoring p in $\mathbb{O}_K$ or $\mathbb{Z}[\alpha]$ is 'the same' as long as p does not divide the index $[\mathbb{O}_K : \mathbb{Z}[\alpha]]$ from (7-7). For such p we have an isomorphism $\mathbb{Z}[\alpha]/p\mathbb{Z}[\alpha] \xrightarrow{\sim} \mathbb{O}_K/p\mathbb{O}_K$, and the order $\mathbb{Z}[\alpha]$ is called *p-maximal* or *regular* above p.

The primes over p in $\mathbb{Z}[\alpha]$ are the kernels of the ring homomorphisms

$$\varphi : \mathbb{Z}[\alpha] = \mathbb{Z}[X]/(f) \to \overline{\mathbf{F}}_p$$

from $\mathbb{Z}[\alpha]$ to an algebraic closure $\overline{\mathbf{F}}_p$ of the field $\mathbf{F}_p$ of p elements. As φ factors via $\mathbb{Z}[\alpha]/p\mathbb{Z}[\alpha] = \mathbf{F}_p[X]/(\bar{f})$, such kernels correspond to the irreducible factors $\bar{g} \in \mathbf{F}_p[X]$ of $\bar{f} = f \bmod p$. Pick monic polynomials $g_i \in \mathbb{Z}[X]$ such that $\bar{f}$ factors as $\bar{f} = \prod_{i=1}^{s} \bar{g}_i^{e_i} \in \mathbf{F}_p[X]$. Then the ideals in $\mathbb{Z}[\alpha]$ lying over p are the ideals

$$\mathfrak{p}_i = (p, g_i(\alpha)) \subset \mathbb{Z}[\alpha]. \tag{8-1}$$

From the isomorphism $\mathbb{Z}[\alpha]/\mathfrak{p}_i \cong \mathbf{F}_p[X]/(\bar{g}_i)$, we see that the residue class degree of $\mathfrak{p}_i$ over p equals $f(\mathfrak{p}_i/p) = \deg(g_i)$. For any polynomial $t \in \mathbb{Z}[X]$, the element $t(\alpha) \in \mathbb{Z}[\alpha]$ is in $\mathfrak{p}_i$ if and only if $\bar{g}_i$ divides $\bar{t}$ in $\mathbf{F}_p[X]$.

THEOREM 8.2 (KUMMER–DEDEKIND). *Let p and $\mathbb{Z}[\alpha]$ be as above, and define $\mathfrak{p}_i = (p, g_i(\alpha)) \subset \mathbb{Z}[\alpha]$ corresponding to the factorization $\bar{f} = \prod_{i=1}^{s} \bar{g}_i^{e_i} \in \mathbf{F}_p[X]$ as in* (8-1). *Then the inclusion*

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

of $\mathbb{Z}[\alpha]$-ideals is an equality if and only if all $\mathfrak{p}_i$ are invertible. If $r_i \in \mathbb{Z}[X]$ is the remainder of f upon division by g_i in $\mathbb{Z}[X]$, say $f = q_i g_i + r_i$, then we have

$$\mathfrak{p}_i \text{ is regular} \quad \Longleftrightarrow \quad e_i = 1 \text{ or } p^2 \nmid r_i \in \mathbb{Z}[X].$$

If $\mathfrak{p}_i$ is singular, then $\frac{1}{p} q_i(\alpha) \notin \mathbb{Z}[\alpha]$ is an integral element of $\mathbb{Q}(\alpha)$.

PROOF. Write $R = \mathbb{Z}[\alpha]$. As $\prod_{i=1}^{s} g_i(\alpha)^{e_i}$ is in $f(\alpha) + pR = pR$, the inclusion $\prod_{i=1}^{s} \mathfrak{p}_i^{e_i} \subset pR + \prod_{i=1}^{s} g_i(\alpha)^{e_i} \subset pR$ is immediate. If it is an equality, all $\mathfrak{p}_i$ are clearly invertible. Conversely, if all $\mathfrak{p}_i$ are invertible, then the invertible ideal $\prod_{i=1}^{s} \mathfrak{p}_i^{e_i}$ has index $\prod_{i=1}^{s} p^{e_i \deg(g_i)} = p^{\deg f} = [R : pR]$, so equality holds.

As the remainder r_i of f upon division by g_i in $\mathbb{Z}[X]$ is divisible by p, there are polynomials $q_i, s_i \in \mathbb{Z}[X]$ satisfying $f = q_i \cdot g_i + p s_i$ and $\deg(s_i) < \deg(g_i)$. Substitution of α yields the relation

$$p s_i(\alpha) = -q_i(\alpha) g_i(\alpha) \in \mathfrak{p}_i \qquad (*)$$

between the two R-generators p and $g_i(\alpha)$ of $\mathfrak{p}_i$. If $\bar{g}_i$ occurs with exponent $e_i = 1$ in $\bar{f}$, we have $\bar{g}_i \nmid \bar{q}_i \in \mathbb{F}_p[X]$, so $q_i(\alpha)$ is not in $\mathfrak{p}_i$. In this case $q_i(\alpha)$ is a unit in $R_{\mathfrak{p}_i}$, and $(*)$ shows that $\mathfrak{p}_i R_{\mathfrak{p}_i}$ is principal with generator p. Similarly, the hypothesis $r_i = p s_i \notin p^2\mathbb{Z}[X]$ means that $\bar{s}_i \in \mathbb{F}_p[X]$ is nonzero of degree $\deg(\bar{s}_i) < \deg(\bar{g}_i)$. This implies $\bar{g}_i \nmid \bar{s}_i$, so now $s_i(\alpha)$ is a unit in $R_{\mathfrak{p}_i}$ and $\mathfrak{p}_i R_{\mathfrak{p}_i}$ is principal with generator $g_i(\alpha)$. In either case $\mathfrak{p}_i$ is regular by Proposition 5.4.

If we have $e_i > 1$ and p^2 divides r_i in $\mathbb{Z}[X]$, then $\mathfrak{p}_i$ is singular, as the identity

$$\tfrac{1}{p} q_i(\alpha)\mathfrak{p}_i = \tfrac{1}{p} q_i(\alpha) \cdot pR + \tfrac{1}{p} q_i(\alpha) \cdot g_i(\alpha) R = q_i(\alpha) R + s_i(\alpha) R \subset \mathfrak{p}_i$$

shows that its multiplier ring $\Lambda(\mathfrak{p}_i)$ contains the integral element $\frac{1}{p} q_i(\alpha) \notin R_{\mathfrak{p}_i}$, so $R_{\mathfrak{p}_i}$ is not integrally closed. □

If $\mathbb{Z}[\alpha]$ is regular above p, we can factor p in $\mathbb{Z}[\alpha]$ or $\mathbb{O}_K$ using the Kummer–Dedekind theorem, whereas if $\mathbb{Z}[\alpha]$ is singular above p, then p divides the index $[\mathbb{O}_K : \mathbb{Z}[\alpha]]$, and p^2 divides $\Delta(f_{\mathbb{Q}}^{\alpha})$ by (7-7). For every singular prime $\mathfrak{p}_i \mid p$ of $\mathbb{Z}[\alpha]$ we encounter, an element $p^{-1} q_i(\alpha)$ is provided by Theorem 8.2 that can be adjoined to the order $\mathbb{Z}[\alpha]$ to obtain an order of smaller index in $\mathbb{O}_K$.

EXAMPLE 8.3. Let α be a zero of $f = X^3 + 44 = X^3 + 2^2 \cdot 11 \in \mathbb{Z}[X]$, and $\mathbb{Z}[\alpha]$ the associated cubic order in $K = \mathbb{Q}(\alpha)$. Then f is separable modulo the primes $p \neq 2, 3, 11$ coprime to $\Delta(X^3 + 44) = -2^4 \cdot 3^3 \cdot 11^2$, and for these p we can factor (p) into prime ideals in $\mathbb{Z}[\alpha]$ as

$$(p) = \begin{cases} \mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3 & \text{if } p \equiv 1 \bmod 3 \text{ and } 44 \text{ is a cube modulo } p, \\ (p) & \text{if } p \equiv 1 \bmod 3 \text{ and } 44 \text{ is not a cube modulo } p, \\ \mathfrak{p}\mathfrak{P} & \text{if } p \equiv 2 \bmod 3. \end{cases}$$

In the first case, the primes $\mathfrak{p}_i = (p, \alpha - k_i)$ corresponding to the three cube roots k_i of -44 modulo p are of degree 1. In the second case, the rational prime p is called *inert* as it remains prime in $\mathbb{Z}[\alpha]$ (but becomes of degree 3). For $p \equiv 2 \bmod 3$, the element $-44 \in \mathbf{F}_p^*$ has a unique cube root k giving rise to a prime $\mathfrak{p} = (p, \alpha - k)$ of degree 1, and the irreducible quadratic polynomial $g = (X^3 + 44)/(X - k) \in \mathbf{F}_p[X]$ yields the other prime $\mathfrak{P} = (p, g(\alpha))$ of degree 2 lying over p.

For $p = 2, 11$, the triple factor X of f mod p leaves as remainder $44 = 2^2 \cdot 11$ upon division in $\mathbb{Z}[X]$. For $p = 11$, this yields the factorization $(11) = (11, \alpha)^3$.

For $p = 2$, it implies that the unique prime $\mathfrak{p}_2 = (2, \alpha)$ above 2 in $\mathbb{Z}[\alpha]$ is singular, and that $\beta = \alpha^2/2$ is an integral element outside $\mathbb{Z}[\alpha]$. We have

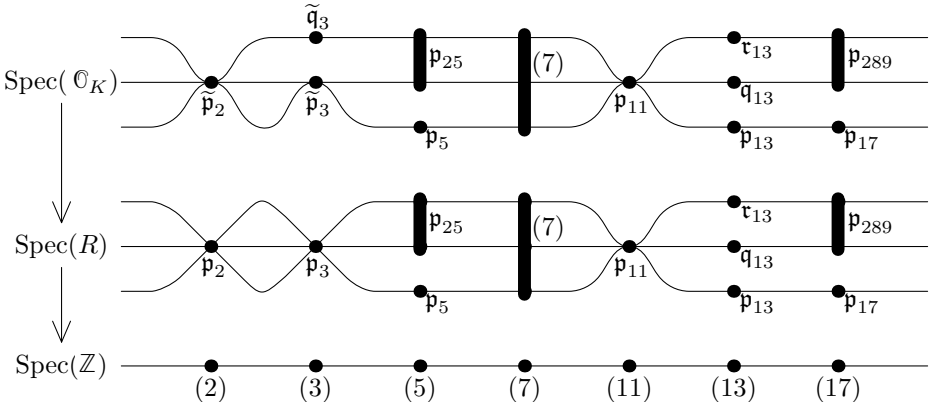
$$f_{\mathbb{Q}}^{\beta} = X^3 - 2 \cdot 11^2,$$

and $\mathbb{Z}[\beta]$ is a 2-integral ring in which we have $(2) = (2, \beta)^3$ by Theorem 8.2. This factorization also holds in $\mathbb{Z}[\alpha, \beta]$ and in $\mathbb{O}_K$.

For $p = 3$, the triple factor $X - 1$ of f mod 3 leaves remainder $45 = 3^2 \cdot 5$ upon division in $\mathbb{Z}[X]$, so the unique prime ideal $\mathfrak{p}_3 = (3, \alpha - 1)$ over 3 in $\mathbb{Z}[\alpha]$ is singular, and from $X^3 + 44 = (X - 1)(X^2 + X + 1) + 45$ we see that $\gamma = \frac{1}{3}(\alpha^2 + \alpha + 1)$ is integral. Its irreducible polynomial is the polynomial $f_{\mathbb{Q}}^{\gamma} = X^3 - X^2 + 15X - 75$ of discriminant $-2^4 \cdot 3 \cdot 5^2 \cdot 11^2$ from Example 7.9, so $\mathbb{Z}[\gamma]$ is regular above 3 and Theorem 8.2 gives us the factorization $(3) = (3, \gamma)^2(3, \gamma - 1)$ in any K-order containing γ.

In this small example, $\mathbb{Z}[\alpha]$ has index $6 = 2 \cdot 3$ in $\mathbb{O}_K = \mathbb{Z}[\alpha, \beta, \gamma]$, and we have $\Delta(\mathbb{O}_K) = \Delta_K = 6^{-2} \cdot \Delta(f) = -2^2 \cdot 3 \cdot 11^2$. The multiplier rings of the singular primes $\mathfrak{p}_2 = (2, \alpha)$ and $\mathfrak{p}_3 = (3, \alpha - 1)$ of $\mathbb{Z}[\alpha]$ contain β and γ, respectively, so $\mathfrak{f}_{\mathbb{Z}[\alpha]} = \mathfrak{p}_2\mathfrak{p}_3$ is a $\mathbb{Z}[\alpha]$-ideal of index 6 that multiplies $\mathbb{O}_K$ into $\mathbb{Z}[\alpha]$. As an $\mathbb{O}_K$-ideal, it is the regular ideal $(2, \beta)^2(3, \gamma)(3, \gamma - 1)$ of norm 36.

Having computed $\mathbb{O}_K = \mathbb{Z}[\beta, \gamma]$, one may verify that $\beta - \gamma = (\alpha^2 - 2\alpha - 2)/6$ has irreducible polynomial $X^3 + X^2 - 7X - 13$ and generates $\mathbb{O}_K$ over $\mathbb{Z}$, so in this case $\mathbb{O}_K$ is actually a simple extension of $\mathbb{Z}$. However, finding such a generator starting from $X^3 + 44$ is not immediate.



The picture above is a 'geometric' rendering of the cubic order $R = \mathbb{Z}[\sqrt[3]{44}]$ and its normalization $\mathbb{O}_K$. The inclusions $\mathbb{Z} \subset R \subset \mathbb{O}_K$ correspond to 'covering maps' $\operatorname{Spec} \mathbb{O}_K \to \operatorname{Spec} R \to \operatorname{Spec} \mathbb{Z}$. Here the *spectrum* of a number ring (see [Eisenbud and Harris 2000] for more details) is represented as a 'curve' having the primes of the ring as its points, and the covering maps intersect primes in the larger ring with the smaller ring. As suggested by the picture, Spec R is a

3-to-1 cover of $\operatorname{Spec}\mathbb{Z}$. The fiber above any rational prime different from the prime divisors 2, 3, and 11 consists of exactly three extension primes, provided that we count a prime $\mathfrak{p} \mid p$ with 'weight' $f(\mathfrak{p}/p)$. Primes of weight 2 and 3 are represented by vertical dashes intersecting 2 or 3 of the lines rather than points. The primes $\mathfrak{p}_2$ and $\mathfrak{p}_3$ over 2 and 3 in R are singular 'triple points', whereas the unique prime $\mathfrak{p}_{11} = (11, \alpha)$ in R over 11 is a regular prime in which the three lines are tangent to each other, illustrating the identity $\mathfrak{p}_{11}^3 = (11)$. The normalization $\mathbb{O}_K$ of R is locally isomorphic to R at all primes not dividing $\mathfrak{f}_{\mathbb{Z}[\alpha]} = \mathfrak{p}_2\mathfrak{p}_3$. The singular prime $\mathfrak{p}_2$ has a unique extension $\widetilde{\mathfrak{p}}_2$ in $\mathbb{O}_K$, for which we have $\mathfrak{p}_2\mathbb{O}_K = \widetilde{\mathfrak{p}}_2^2$. The singular prime $\mathfrak{p}_3$ factors in $\mathbb{O}_K$ as a product $\mathfrak{p}_3\mathbb{O}_K = \widetilde{\mathfrak{p}}_3\widetilde{\mathfrak{q}}_3$ of two primes, and we have $3\mathbb{O} = \widetilde{\mathfrak{p}}_3^2\widetilde{\mathfrak{q}}_3$ with $\widetilde{\mathfrak{p}}_3 = (3, \gamma)$.

If R is regular above p, we can factor the rational prime p in R as $pR = \prod_{\mathfrak{p} \mid p} \mathfrak{p}^{e(\mathfrak{p}/p)}$. The exponent $e(\mathfrak{p}/p) = \operatorname{ord}_{\mathfrak{p}}(pR)$ is known as the *ramification index* of $\mathfrak{p}$ over p. We say that p is *unramified* in R if all $e(\mathfrak{p}/p)$ equal 1, and *ramified* in R if we have $e(\mathfrak{p}/p) > 1$ for some $\mathfrak{p}$. Thus, the primes 2, 3 and 11 are ramified in the ring $\mathbb{O}_K$ in Example 8.3, and all other primes are unramified. This example also shows the validity of the following relation for orders, which, for orders of the form $\mathbb{Z}[\alpha]$, is immediate from the identity $f(\mathfrak{p}_i/p) = \deg g_i$ in Theorem 8.2.

THEOREM 8.4. *Let R be an order of rank n, and suppose that R is regular above p. Then we have $\sum_{\mathfrak{p} \mid p} e(\mathfrak{p}/p) f(\mathfrak{p}/p) = n$.*

PROOF. The ideal norm of pR, which is $\#(R/pR) = p^n$, is also equal to

$$\prod_{\mathfrak{p} \mid p} \#(R/\mathfrak{p}^{e(\mathfrak{p}/p)}) = \prod_{\mathfrak{p} \mid p} \#(R/\mathfrak{p})^{e(\mathfrak{p}/p)} = p^{\sum_{\mathfrak{p} \mid p} e(\mathfrak{p}/p) f(\mathfrak{p}/p)}$$

by the multiplicativity of the ideal norm for powers of regular primes. □

In the situation of Theorem 8.4, we call p *totally split* (or just *split*) in R if there are n extension primes over p, which then have $e(\mathfrak{p}/p) = f(\mathfrak{p}/p) = 1$. If there is a single prime $\mathfrak{p} \mid p$ with $e(\mathfrak{p}/p) = n$, we call p *totally ramified* in R. If $\mathfrak{p} = pR$ is a prime ideal of R, we have $f(\mathfrak{p}/p) = n$, and we say that p is *inert* in R.

For singular primes $\mathfrak{p} \mid p$, the ramification index of $\mathfrak{p}$ over p is not defined.

THEOREM 8.5. *Let R be an order and p a prime number. If R is singular above p, then p^2 divides $\Delta(R)$. If R is regular above p, we have*

$$p \text{ divides } \Delta(R) \iff p \text{ is ramified in } R.$$

PROOF. If R is singular above p, then p divides the index of R in its integral closure $\mathbb{O}$, so p^2 divides $\Delta(R) = [\mathbb{O} : R]^2 \cdot \Delta(\mathbb{O})$ by (7-3).

We have $\Delta(R) \equiv 0 \bmod p$ if and only if the discriminant $\Delta(R/pR) \in \mathbb{F}_p$ of the $\mathbb{F}_p$-algebra R/pR vanishes. If p is unramified in R, then R/pR is a product $\prod_{\mathfrak{p}\mid p} R/\mathfrak{p}$ of finite fields and $\Delta(R/pR)$ is a product of discriminants of field extensions of $\mathbb{F}_p$, each of which is nonzero by the remark following (7-5). If p is ramified in R, the $\mathbb{F}_p$-algebra R/pR has a nonzero nilradical. Taking a basis containing nilpotent elements, which have trace zero, we see that its discriminant vanishes. □

If R is an order of rank n in which some prime $p < n$ splits completely, then R is not monogenic as a monogenic ring admits at most p homomorphisms to $\mathbb{F}_p$. This makes it easy to construct examples of number fields K for which $\mathbb{O}_K$ is not monogenic, and for which every order $\mathbb{Z}[\alpha]$ has index in $\mathbb{O}_K$ divisible by p.

EXAMPLE 8.6. The ring of integers of $K = \mathbb{Q}(\sqrt{-7}, \sqrt{17})$ is generated by $\beta = (1+\sqrt{-7})/2$ and $\gamma = (1+\sqrt{17}/2)$, and $f^{\beta}_{\mathbb{Q}} = X^2 - X + 2$ and $f^{\gamma}_{\mathbb{Q}} = X^2 - X - 4$ each have two roots in $\mathbb{F}_2$. This yields *four* different maps $\mathbb{O}_K = \mathbb{Z}[\beta, \gamma] \to \mathbb{F}_2$, so 2 splits completely in $\mathbb{O}_K$. The discriminant $\Delta_K = 7^2 \cdot 17^2$ is odd, but every order $R = \mathbb{Z}[\alpha]$ in K has $\Delta(R) \equiv 0 \bmod 4$.

9. Computing the integral closure

If R is a number ring, the integral closure $\mathbb{O}$ of R in $K = Q(R)$ contains R as a subring of finite index. As the example $R = \mathbb{Z}[\sqrt{d}]$ in Section 2 shows, efficient computation of $\mathbb{O}$ from R is hampered by our inability to factor integers or, more precisely, to determine the largest squarefree divisor of a given integer. The algorithms we do have to compute $\mathbb{O}$ from R are mostly 'local at p' for a rational prime number p. They work inside the $\mathbb{F}_p$-algebra R/pR, which is finite of rank at most $[K : \mathbb{Q}]$ even in case R is not assumed to be an order. As they only use linear algebra over $\mathbb{F}_p$, they are fairly efficient. However, it may not be easy to find the primes p dividing $[\mathbb{O} : R]$ at which these computations need to be performed.

In the case of an order of discriminant $\Delta(R)$, the 'critical' primes are the primes that divide $\Delta(R)$ more than once. For such p, one wants to find a p-maximal extension

$$R \subset O_p = \{x \in \mathbb{O}_K : p^k x \in R \text{ for some } k \in \mathbb{Z}_{\geq 0}\}$$

of R inside $\mathbb{O}_K$, for which the index in $\mathbb{O}_K$ is coprime to p. The index $[O_p : R]$ is a p-power, and its square $[O_p : R]^2$ divides $\Delta(R)$. Taken together, the rings O_p with $p^2 \mid \Delta(R)$ generate $\mathbb{O}_K$ over R.

In practice one starts with a simple order $\mathbb{Z}[\alpha]$, which has $\Delta(\mathbb{Z}[\alpha]) = \Delta(f^{\alpha}_{\mathbb{Q}})$, and applies the Kummer–Dedekind theorem to determine for which critical primes p the order $\mathbb{Z}[\alpha]$ is singular above p and the inclusion $\mathbb{Z}[\alpha] \subset O_p$ is

strict. In case singular primes over p are encountered, the elements $p^{-1}q_i(\alpha) \in O_p \setminus \mathbb{Z}[\alpha]$ provided by the theorem are adjoined to $\mathbb{Z}[\alpha]$ to obtain an extension ring R for which the index $[R : \mathbb{Z}[\alpha]]$ is a power of p, and which has by (7-6) a discriminant $\Delta(R)$ having fewer factors p than $\Delta(f_{\mathbb{Q}}^{\alpha})$. If p^2 still divides $\Delta(R)$, it may be necessary to further extend the ring R to obtain O_p, and as R will not in general be simple, we now need an algorithm that is not restricted to the monogenic setting of the Kummer–Dedekind theorem to obtain the extension $R \subset O_p$. There are two ways to proceed.

The first method considers the individual primes $\mathfrak{p} \mid p$ and is also useful to compute valuations at $\mathfrak{p}$ in case $\mathfrak{p}$ is regular. It tries to compute the fractional R-ideal

$$\mathfrak{p}^{-1} = R : \mathfrak{p} = \{x \in K : x\mathfrak{p} \subset R\},$$

which clearly satisfies $R \subset \mathfrak{p}^{-1} \subset \frac{1}{p}R$. In fact, $\mathfrak{p}^{-1}$ *strictly* contains R. To see this, one picks a nonzero element $x \in \mathfrak{p}$ and notices that, by Theorem 5.2 and Lemma 5.1, the ideal (x) contains a product of prime ideals of R. We can write this product as $\mathfrak{p} \cdot I \subset (x)$ and we may assume $I \subsetneq (x)$ by taking the minimal number of primes in the product. For $y \in I \setminus (x)$, the element $a = y/x$ is in $\mathfrak{p}^{-1} \setminus R$.

Finding an element $a = \frac{1}{p}r$ in $\mathfrak{p}^{-1} \setminus R$ amounts to finding a nonzero element $\bar{r} \in R/pR$ that annihilates the ideal $\mathfrak{p}/pR \subset R/pR$, and this is a matter of linear algebra in R/pR. If we have $\mathfrak{p}$ in its 'standard form' $\mathfrak{p} = (p, \beta) \subset R$ on 2 generators, then we only need to find a nonzero element annihilating $\overline{\beta} \in R/pR$.

An element $a \in \mathfrak{p}^{-1} \setminus R$ tells us all about $\mathfrak{p}$. As $(R + Ra)\mathfrak{p} \subset R$ is an R-ideal containing the maximal ideal $\mathfrak{p}$, we have two possibilities. If $(R + Ra)\mathfrak{p}$ equals $\mathfrak{p}$, then a is in the multiplier ring $\Lambda(\mathfrak{p})$ but not in R, so $\mathfrak{p}$ is singular, and we have found an element of $\mathbb{O} \setminus R$ that we use to enlarge R. If it equals R, then $R + Ra = \mathfrak{p}^{-1}$ is the inverse of the regular ideal $\mathfrak{p}$ in $\mathcal{I}(R)$, and we can use a to determine valuations at $\mathfrak{p}$.

PROPOSITION 9.1. *Let $\mathfrak{p}$ be an invertible R-ideal, and $\mathfrak{p}^{-1} = R + Ra$ its inverse. Then the $\mathfrak{p}$-adic valuation of an ideal $I \subset R$ equals*

$$\operatorname{ord}_{\mathfrak{p}}(I) = \max\{k \geq 0 : a^k I \subset R\}.$$

PROOF. The valuation $\operatorname{ord}_{\mathfrak{p}}(I)$ of an integral ideal I is the largest integer k for which $\mathfrak{p}^{-k} I = (R + Ra)^k I$ is contained in R. □

The second method to enlarge a number ring R to a p-maximal extension is similar in nature, but does not find the individual primes over p first. Assuming that p is not a unit in R, it defines the p-radical of R as the intersection or, equivalently, the product

$$I_p = \bigcap_{p \in \mathfrak{p}} \mathfrak{p} = \prod_{p \in \mathfrak{p}} \mathfrak{p} \supset pR \tag{9-2}$$

of the primes of R lying over p. Then I_p/pR, being the intersection of all prime ideals of R/pR, is the *nilradical* $\mathrm{nil}(R/pR)$ of the finite ring R/pR. To compute it, we let $F_p : R/pR \to R/pR$ be the Frobenius map defined by $F_p(x) = x^p$. Then F_p is an $\mathbb{F}_p$-linear map that can be described by a matrix with respect to a basis of the finite $\mathbb{F}_p$-algebra R/pR. We have $I_p/pR = \mathrm{nil}(R/pR) = \ker F_p^k$ if k is chosen so that p^k exceeds $\dim_{\mathbb{F}_p}(R/pR) \leq [K:\mathbb{Q}]$. This makes the computation of $I_p/pR \subset R/pR$ a standard matter of linear algebra over $\mathbb{F}_p$.

If we find $I_p/pR = 0$, then R is regular and unramified at p, and finding the primes over p amounts to splitting the separable $\mathbb{F}_p$-algebra R/pR into a product of finite fields. This is done by finding the idempotents in R/pR, which is easy as these span the kernel of the linear map $F_p - \mathrm{id}$.

The more interesting case arises when the inclusion in (9-2) is strict, that is, when R is singular or ramified above p. To find out whether R is singular above p and the inclusion $R \subset O_p$ strict, one now considers the multiplier ring

$$R' = \Lambda(I_p) = \{x \in K : xI_p \subset I_p\}$$

of the p-radical of R. From $p \in I_p$ we obtain $R \subset R' \subset \frac{1}{p}R$, and as I_p is a finitely generated R-ideal, we have $R' \subset O_p$ by Lemma 6.4.

PROPOSITION 9.3. *Define the extensions $R \subset R' \subset O_p$ as above. If the inclusion $R \subset O_p$ is strict, then so is the inclusion $R \subset R'$.*

PROOF. Suppose we have $[O_p : R] = p^r > 1$. As all sufficiently high powers of I_p contain pR, we have $I_p^k O_p \subset R$ for large k. Let $m \geq 0$ be the largest integer for which we have $I_p^m O_p \not\subset R$, and pick $x \in I_p^m O_p \setminus R \subset O_p \setminus R$. For $y \in I_p$ we now have $xy \in I_p^{m+1} O_p \subset R \cap I_p O_p = I_p$, so x is in $R' \setminus R$. □

By Proposition 9.3, we can find O_p by repeatedly replacing R by R' until we have $R = R' = O_p$. As we can work 'modulo p' all the time, the resulting *Pohst–Zassenhaus algorithm* reduces to linear algebra over $\mathbb{F}_p$. One starts by computing $\mathbb{F}_p$-bases for I_p/pR and I_p/pI_p from a basis of R/pR. As I_p/pI_p is an R-module, we have a structure map

$$\varphi : R \to \mathrm{End}(I_p/pI_p),$$

and we find $R' = \frac{1}{p}N$ for $N = \ker\varphi$. Note that $N = \ker\varphi$ contains pR since φ factors via R/pR, and that R' is generated over R by $1/p$ times the lifts to R of an $\mathbb{F}_p$-basis for N/pR. Computing N is again a matter of linear algebra. A slight drawback of the method is that for I_p/pI_p of $\mathbb{F}_p$-dimension $n \leq [K:\mathbb{Q}]$, the endomorphism ring $\mathrm{End}(I_p/pI_p)$ is a matrix ring of dimension n^2 over $\mathbb{F}_p$. Thus, the relevant map $\overline{\varphi} : R/pR \to \mathrm{End}(I_p/pI_p)$ is described by a matrix of size $n^2 \times n$ over $\mathbb{F}_p$.

Once a p-regular ring R has been obtained, the extension primes $\mathfrak{p} \mid p$ are found by finding the idempotents of the $\mathbb{F}_p$-algebra R/pR. We refer to [Cohen 1993, Chapter 6] for further details.

10. Finiteness theorems

In order to use ideal factorization in a number ring R to establish divisibility results between *elements* as one does in $\mathbb{Z}$, there are two obstacles one has to deal with. The first is the obstruction to invertible ideals being principal, which is measured by the Picard group $\mathrm{Pic}(R)$. The second is the problem that generators of principal ideals in R are only unique up to multiplication by *units* in R. As the example of the number ring $R = \mathbb{Z}[\sqrt{d}]$ occurring in Pell's equation shows, the unit group R^* may be infinite. We do however have two basic finiteness theorems: the Picard group $\mathrm{Pic}(R)$ of a number ring R is a *finite* abelian group, and for orders R, the unit group R^* is a *finitely generated* abelian group. These are not algebraic properties of one-dimensional Noetherian domains, and the proofs use the fact that number rings allow embeddings in Euclidean vector spaces, in which techniques from the geometry of numbers can be applied.

Let V be an n-dimensional real vector space equipped with a scalar product $\langle \cdot, \cdot \rangle : V \times V \to \mathbb{R}$, that is, a positive definite bilinear form on $V \times V$. Then we define the *volume* of a parallelepiped $B = \{r_1 x_1 + r_2 x_2 + \cdots + r_n x_n : 0 \le r_i < 1\}$ spanned by $x_1, x_2, \ldots, x_n$ as

$$\mathrm{vol}(B) = |\det(\langle x_i, x_j \rangle)_{i,j=1}^n|^{1/2}.$$

Thus, the 'unit cube' spanned by an orthonormal basis for V has volume 1, and the image of this cube under a linear map T has volume $|\det(T)|$. If the vectors x_i are written with respect to an orthonormal basis for V as $x_i = (x_{ij})_{j=1}^n$, then we have

$$|\det(\langle x_i, x_j \rangle)_{i,j=1}^n|^{1/2} = |\det(M \cdot M^t)|^{1/2} = |\det(M)|$$

for $M = (x_{ij})_{i,j=1}^n$. The volume function on parallelepipeds can be extended to a Haar measure on V that, under the identification $V \cong \mathbb{R}^n$ via an orthonormal basis for V, is the well-known Lebesgue measure on $\mathbb{R}^n$.

A subgroup $L = \mathbb{Z} \cdot x_1 + \mathbb{Z} \cdot x_2 + \cdots + \mathbb{Z} \cdot x_k \subset V$ spanned by k linearly independent vectors $x_i \in V$ is called a *lattice of rank* k in V. We clearly have $k \le n$, and all discrete subgroups of V are of this form. If $L \subset V$ has maximal rank n, the *covolume* $\mathrm{vol}(V/L)$ of L in V is the volume of a parallelepiped F spanned by a basis of L. Such a parallelepiped is a *fundamental domain* for L as every $x \in V$ has a unique representation $x = f + l$ with $f \in F$ and $l \in L$. In fact, $\mathrm{vol}(V/L)$ is the volume of V/L under the induced Haar measure on the factor group V/L.

All finiteness results in this section are applications of Minkowski's 'continuous version' of Dirichlet's box principle. His theorem is simple to state and amazingly effective in the sense that *many* results can be derived from it. However, like the box principle itself, it has little algorithmic value since its proof is a pure existence proof that suggests no efficient algorithm.

THEOREM 10.1 (MINKOWSKI). *Let L be a lattice of maximal rank n in V. Then every closed bounded subset of V that is convex and symmetric and has volume* $\mathrm{vol}(X) \geq 2^n \cdot \mathrm{vol}(V/L)$ *contains a nonzero lattice point.*

PROOF. Suppose first that we have $\mathrm{vol}(X) > 2^n \cdot \mathrm{vol}(V/L)$. Then the set $\frac{1}{2}X = \{\frac{1}{2}x : x \in X\}$ has volume $\mathrm{vol}(\frac{1}{2}X) > \mathrm{vol}(V/L)$, so the map $\frac{1}{2}X \to V/L$ cannot be injective. Pick distinct points $x_1, x_2 \in X$ with $\frac{1}{2}x_1 - \frac{1}{2}x_2 = \omega \in L$. As X is symmetric, $-x_2$ is contained in X. By convexity, we find that the convex combination ω of x_1 and $-x_2 \in X$ is in $X \cap L$.

Under the weaker assumption $\mathrm{vol}(X) \geq 2^n \mathrm{vol}(V/L)$, we observe that each of the sets $X_\varepsilon = (1+\varepsilon)X$ with $0 < \varepsilon \leq 1$ contains a nonzero lattice point $\omega_\varepsilon \in L$. There are only finitely many distinct lattice points $\omega_\varepsilon \in L \cap 2X$, and a point occurring for infinitely many is in the closed set $X = \cap_\varepsilon X_\varepsilon$. □

If K is a number field of degree n over $\mathbb{Q}$, the base change $\mathbb{Q} \to \mathbb{C}$ provides us with a canonical embedding of K in the n-dimensional complex vector space $K_\mathbb{C} = K \otimes_\mathbb{Q} \mathbb{C}$:

$$\begin{aligned} \Phi_K : \quad K &\longrightarrow K_\mathbb{C} \cong \mathbb{C}^n \\ x &\longmapsto (\sigma(x))_\sigma. \end{aligned}$$

Here the isomorphism $K_\mathbb{C} \cong \mathbb{C}^n$ is as in (7-1), with σ ranging over the n embeddings $K \to \mathbb{C}$. Note that Φ_K is a ring homomorphism, and that the norm and trace on the free $\mathbb{C}$-algebra $K_\mathbb{C}$ extend the norm and the trace of the field extension $K/\mathbb{Q}$. The image of K under the embedding lies in the $\mathbb{R}$-algebra

$$K_\mathbb{R} = \{(z_\sigma)_\sigma \in K_\mathbb{C} : z_{\bar{\sigma}} = \bar{z}_\sigma\}$$

consisting of the elements of $K_\mathbb{C}$ invariant under the involution $F : (z_\sigma)_\sigma \mapsto (\bar{z}_{\bar{\sigma}})_\sigma$. Here $\bar{\sigma}$ denotes the embedding of K in $\mathbb{C}$ that is obtained by composition of σ with complex conjugation.

On $K_\mathbb{C} \cong \mathbb{C}^n$, we have the standard hermitian scalar product, which satisfies $\langle Fz_1, Fz_2\rangle = \overline{\langle z_1, z_2\rangle}$. Its restriction to $K_\mathbb{R}$ is a *real* scalar product that equips $K_\mathbb{R}$ with a Euclidean structure and a *canonical* volume function.

It is customary to denote the real embeddings of K by $\sigma_1, \sigma_2, \ldots, \sigma_r$ and the pairs of complex embeddings of K by $\sigma_{r+1}, \overline{\sigma_{r+1}}, \sigma_{r+2}, \overline{\sigma_{r+2}}, \ldots, \sigma_{r+s}, \overline{\sigma_{r+s}}$.

We have $r + 2s = n$ and an isomorphism of $\mathbb{R}$-algebras

$$\begin{aligned} K_{\mathbb{R}} &\xrightarrow{\sim} \mathbb{R}^r \times \mathbb{C}^s \\ (z_\sigma)_\sigma &\longmapsto (z_{\sigma_i})_{i=1}^{r+s}. \end{aligned} \tag{10-2}$$

The inner product on $K_{\mathbb{R}}$ is taken componentwise, with the understanding that at a 'complex' component $(\sigma, \bar{\sigma})$, the inner product of $z_1 = x_1 + iy_1$ and $z_2 = x_2 + iy_2$ equals

$$\langle \tbinom{z_1}{\bar{z}_1}, \tbinom{z_2}{\bar{z}_2} \rangle = z_1\bar{z}_2 + \bar{z}_1 z_2 = 2\,\mathrm{Re}(z_1\bar{z}_2) = 2(x_1x_2 + y_1y_2).$$

This differs by a factor 2 from the inner product under the identification of $\mathbb{C}$ with the 'complex plane' $\mathbb{R}^2$, so volumes in $K_{\mathbb{R}}$ are 2^s times *larger* than they are in $\mathbb{R}^r \times \mathbb{C}^s$ with the 'standard' Euclidean structure. The following theorem shows that the 'canonical' volume is indeed canonical.

LEMMA 10.3. *Let R be an order in a number field K. Then $\Phi_K[R]$ is a lattice of covolume $|\Delta(R)|^{1/2}$ in $K_{\mathbb{R}}$.*

PROOF. Choose a $\mathbb{Z}$-basis $\{x_1, x_2, \ldots, x_n\}$ for R. Then $\Phi_K[R]$ is spanned by the vectors $(\sigma x_i)_\sigma \in K_{\mathbb{R}}$. In terms of the matrix $X = (\sigma_i(x_j))_{i,j=1}^n$ following (7-4), the covolume of $\Phi_K[R]$ equals

$$|\det(\langle (\sigma x_i)_\sigma, (\sigma x_j)_\sigma \rangle)_{i,j=1}^n|^{1/2} = |\det(X^t \cdot \overline{X})|^{1/2} = |\Delta(R)|^{1/2}. \qquad \square$$

For $I \in \mathcal{I}(R)$, the lattice $\Phi_K[I]$ has covolume $N(I) \cdot |\Delta(R)|^{1/2}$ in $K_{\mathbb{R}}$. Define the closed convex symmetric subset $X_t \subset K_{\mathbb{R}}$ by $X_t = \{(z_\sigma)_\sigma \in K_{\mathbb{R}} : \sum_\sigma |z_\sigma| \leq t\}$, and choose t such that its volume $\mathrm{vol}(X_t) = 2^r\pi^s t^n$ equals $2^n N(I) \cdot |\Delta(R)|^{1/2}$. Using the arithmetic-geometric-mean inequality, we find that X_t contains the Φ_K-image of a nonzero element $x \in I$ of absolute norm

$$|N_{K/\mathbb{Q}}(x)| = \prod_\sigma |\sigma(x)| \leq \Big(\frac{1}{n}\sum_\sigma |\sigma(x)|\Big)^n \leq \frac{t^n}{n^n} = M_R \cdot N(I),$$

where the Minkowski constant of the order R is defined as

$$M_R = \Big(\frac{4}{\pi}\Big)^s \frac{n!}{n^n} \cdot |\Delta(R)|^{1/2}. \tag{10-4}$$

It follows that xI^{-1} is integral and of norm at most M_R. As R has only finitely many ideals of norm at most M_R, we obtain our first finiteness result.

THEOREM 10.5. *Let R be an order and M_R its Minkowski constant. Then every ideal class in the Picard group* $\mathrm{Pic}(R)$ *contains an integral ideal of norm at most M_R, and* $\mathrm{Pic}(R)$ *is a finite abelian group.* $\square$

COROLLARY 10.6. *The Picard group of a number ring is finite.*

PROOF. If $\mathbb{O}$ is Dedekind, this is clear from Theorem 6.5 and (6-6). The case of a general number ring R of conductor $\mathfrak{f}$ in its normalization $\mathbb{O}$ then follows from Theorem 6.7, as $(\mathbb{O}/\mathfrak{f})^*$ is a finite group. □

As the Minkowski constant M_R in (10-4) is at least equal to 1, the absolute value of the discriminant of an order of rank n satisfies

$$|\Delta(R)| \geq \left(\frac{\pi}{4}\right)^{2s} \left(\frac{n^n}{n!}\right)^2.$$

This lower bound grows exponentially with n, and for $R \neq \mathbb{Z}$ we have $n > 1$ and $|\Delta(R)| \geq \pi^2/4 > 2$. By Theorem 8.5, it follows that *every* order $R \neq \mathbb{Z}$ has singular or ramifying primes. In particular, the ring of integers of a number field $K \neq \mathbb{Q}$ is ramified at the primes p dividing the integer $|\Delta_K| > 1$.

If we fix the value of the discriminant $\Delta(R)$ in Lemma 10.3, this puts a bound on its rank n, and one can use Theorem 10.1 to generate R by elements lying in small boxes of $K_{\mathbb{R}}$. This leads to *Hermite's theorem*: up to isomorphism, there are only finitely many orders of given discriminant D. It gives rise to the problem of finding asymptotic expressions for $x \to \infty$ for the number of number fields K, say with r real and s complex primes, for which $|\Delta_K|$ is at most x. As the suggested proof of the theorem, based on Theorem 10.1, is not at all constructive, this is a non-trivial problem for $n > 2$. For $n > 3$ there has only recently been substantial progress [Bhargava 2005; ≥ 2008].

In a more geometric direction, the finiteness of the number of curves (up to isomorphism) of given genus and 'bounded ramification' that are defined over $\mathbb{Q}$ is a 1962 conjecture of Shafarevich that was proved by Faltings [Cornell and Silverman 1986] in 1983. The *ineffective* proof yields no explicit cardinalities of any kind.

The unit group of a number ring R has a finite cyclic torsion subgroup μ_R consisting of the roots of unity in R. As R is countable, R^*/μ_R is countably generated. Not much more can be said in general, as the case $R = K$ shows, but for orders we can be more precise by considering the restriction of the ring homomorphism Φ_K to R^*:

$$\Phi_K : R^* \to K_{\mathbb{R}}^* = \{(z_\sigma)_\sigma \in K_{\mathbb{C}}^* : \bar{z}_\sigma = z_{\bar{\sigma}}\}.$$

In order to produce lattices, we apply the logarithm $z \mapsto \log|z|$ componentwise on $K_{\mathbb{C}}^* = (\mathbb{C}^*)^n$ to obtain a homomorphism $K_{\mathbb{C}}^* \to \mathbb{R}^n$ that sends $(z_\sigma)_\sigma$ to $(\log|z_\sigma|)_\sigma$.

THEOREM 10.7 (DIRICHLET UNIT THEOREM). *Let R be an order of maximal rank $n = r + 2s$ in K, with r and s as in* (10-2). *Then the homomorphism*

$$L : R^* \xrightarrow{L} \mathbb{R}^n, \quad x \longmapsto (\log|\sigma x|)_\sigma$$

has kernel μ_R and maps R^* onto a lattice of rank $r + s - 1$ in $\mathbb{R}^n$.

PROOF. For a bounded set $B = [-M, M]^n \subset \mathbb{R}^n$, the inverse image in $K_{\mathbb{R}}^*$ under the logarithmic map is the bounded set $\{(z_\sigma)_\sigma \in K_{\mathbb{R}} : e^{-M} \leq |z_\sigma| \leq e^M\}$, which has finite intersection with the lattice $\Phi(R)$. Thus $L^{-1}[B] \subset R^*$ is finite, and the discrete subgroup $L[R^*] \subset \mathbb{R}^n$ is a lattice in $\mathbb{R}^n$. Taking $M = 0$, we see that $\ker L$ is finite and equal to μ_R.

We have $\log|\sigma(x)| = \log|\bar{\sigma}(x)|$ for every $x \in K^*$, so $L[R^*]$ lies in the $(r+s)$-dimensional subspace $\{(x_\sigma)_\sigma \in \mathbb{R}^n : x_\sigma = x_{\bar{\sigma}}\} \subset \mathbb{R}^n$, and we lose no information if we replace L by its composition $L' : R^* \to \mathbb{R}^n = \mathbb{R}^{r+2s} \to \mathbb{R}^{r+s}$ of L with the linear map that *adds* the components at each of the s pairs of complex conjugate embeddings $(\sigma, \bar{\sigma})$ into a single component.

For $\eta \in R^*$ we have $[R : \eta R] = |N_{R/\mathbb{Z}}(\eta)| = \prod_\sigma |\sigma(x)| = 1$, so $L'[R^*] \cong R^*/\mu_R$ is a lattice in the 'trace-zero-hyperplane'

$$H = \{(x_i)_{i=1}^{r+s} : \textstyle\sum_i x_i = 0\} \subset \mathbb{R}^{r+s}. \tag{10-8}$$

Showing that $L'[R^*]$ has maximal rank $r + s - 1$ in H is done using Theorem 10.1. Let $E = \{(z_\sigma)_\sigma : \prod_\sigma z_\sigma = \pm 1\} \subset K_{\mathbb{R}}^*$ be the 'norm-$\pm$1-subspace' that is mapped onto H under the composition $\varphi : K_{\mathbb{R}}^* \xrightarrow{\log} \mathbb{R}^n \to \mathbb{R}^{r+s}$, and choose t such that the box $X = \{(z_\sigma)_\sigma \in K_{\mathbb{R}} : |z_\sigma| \leq t \text{ for all } \sigma\}$ has $\mathrm{vol}(X) = 2^n \cdot |\Delta_K|^{1/2}$. For every $e = (e_\sigma)_\sigma \in E$, the set

$$eX = \{ex : x \in X\} = \{(z_\sigma)_\sigma \in K_{\mathbb{R}} : |z_\sigma| < |e_\sigma| t\}$$

is a box around the origin with volume $\mathrm{vol}(eX) = \mathrm{vol}(X)$, so it contains an element $\Phi(x_e) \in \Phi[R]$ by Theorem 10.1. The norm $N(x_e)$ of $x_e \in R$ is bounded by $\prod_\sigma |e_\sigma| t = t^n$ for each e, so the set of *ideals* $\{x_e R : e \in E\}$ is finite, say equal to $\{a_i R\}_{i=1}^k$. Now

$$Y = E \cap \left(\textstyle\bigcup_{i=1}^k \Phi(a_i^{-1}) X \right)$$

is a bounded subset of E as all boxes $\Phi(a_i^{-1})X$ are bounded in $K_{\mathbb{R}}$. By the norm condition on the elements of $Y \subset E$, the absolute values $|y_\sigma|$ of $y = (y_\sigma)_\sigma \in Y$ are bounded away from zero, so $\varphi[Y]$ is a *bounded* subset of H.

To show that $L'[R^*]$ has maximal rank in H, it now suffices to show that we have $L'[R^*] + \varphi[Y] = H$ or, equivalently, $\Phi[R^*] \cdot Y = E$. For the non-trivial inclusion $\supset$, pick $e \in E$. Then there exist a nonzero element $a \in R$ such that $\Phi(a)$ is contained in $e^{-1}X$ and an element $a_i \in R$ as defined above satisfying $a_i a^{-1} = u \in R^*$. It follows that e is contained in $\Phi(a^{-1})X = \Phi(u)\Phi(a_i^{-1})X$, whence in $\Phi[R^*] \cdot Y$. □

Less canonically, Theorem 10.7 states that there exists a finite set $\eta_1, \eta_2, \ldots, \eta_{r+s-1}$ of *fundamental units* in R such that we have

$$R^* = \mu_R \times \langle \eta_1 \rangle \times \langle \eta_2 \rangle \times \cdots \times \langle \eta_{r+s-1} \rangle.$$

Such a system of fundamental units, which forms a $\mathbb{Z}$-basis for R^*/μ_R, is only unique up to $\mathrm{GL}_{r+s-1}(\mathbb{Z})$-transformations and multiplication by roots of unity.

The regulator of a set $\{\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_{r+s-1}\}$ of elements of norm ± 1 in K^* is defined as

$$\mathrm{Reg}(\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_{r+s-1}) = \left|\det(n_i \log|\sigma_i \varepsilon_j|)_{i,j=1}^{r+s-1}\right|.$$

Here the integer $n_i \in \{1, 2\}$ equals 1 if σ_i is a real embedding and 2 otherwise. The *regulator* $\mathrm{Reg}(R)$ of an order R in K is the regulator of a system of fundamental units for R^*, with $\mathrm{Reg}(R) = 1$ if R^* is finite. Its value is the covolume of the lattice $L'[R^*]$ in the trace-zero-hyperplane H from (10-8) after a projection $H \xrightarrow{\sim} \mathbb{R}^{r+s-1}$ obtained by leaving out one of the coordinates.

The regulator of the ring of integers of K is simply referred to as the *regulator* R_K of K. Unlike the discriminant Δ_K, which is an integer, R_K is a positive real number which is usually transcendental, as it is an expression in terms of *logarithms* of algebraic numbers. For an order R in K, we have $[\mathbb{O}_K^* : \mu_K R^*] = \mathrm{Reg}(R^*)/R_K$. For a subring $R \subset K$ that is not an order, we can extend Theorem 10.7 to describe R^*, even though $L[R^*] \subset H$ is a dense subset.

THEOREM 10.9. *Let R be a number ring with field of fractions K, and define r and s as in* (10-2). *Write T for the set of primes $\mathfrak{p}$ of $\mathbb{O}_K$ for which R contains elements of negative valuation. Then we have an isomorphism*

$$R^* \cong \mu_R \oplus \mathbb{Z}^{r+s-1} \oplus \mathbb{Z}^T,$$

and R^* is finitely generated if and only if T is finite.

PROOF. The unit group R^* of R is by Theorem 6.7 of finite index in the unit group $\mathbb{O}^*$ of the normalization $\mathbb{O}$ of R. By Theorem 6.5, we have $\mathbb{O} = \mathbb{O}_{K,T}$ for our set T, and (6-6) provides us with an exact sequence $1 \to \mathbb{O}_K^* \to \mathbb{O}_{K,T}^* \to \mathbb{Z}^T \to \mathrm{Cl}_K$. As subgroups of finite index in $\mathbb{Z}^T$ are free of the same rank, we have a split exact sequence $1 \to \mathbb{O}_K^* \to \mathbb{O}_{K,T}^* \to \mathbb{Z}^{\#T} \to 1$, and the result follows from Theorem 10.7. □

The r real embeddings and the s complex conjugate pairs of embeddings of K are often referred to as the *real* and *complex* primes of K, a point of view on which we will elaborate in Section 13. It is customary to include the set T_∞ of these *infinite primes* in the set T we use in Theorem 6.5 to define the ring $\mathbb{O}_{K,T}$. With this convention, Theorem 10.9 states that the group $\mathbb{O}_{K,T}^*$ of *T-units* is the product of μ_K and a free abelian group of rank $\#T - 1$.

The group μ_K of roots of unity is easily found. For $r > 0$ we simply have $\mu_K = \mu_{\mathbb{R}} = \{\pm 1\}$, and for totally complex K the group μ_K reduces injectively modulo all odd unramified primes of K. This implies that the order w_K of μ_K is an integer dividing $\#(\mathbb{O}_K/\mathfrak{p})^* = p^{f(\mathfrak{p}/p)} - 1$ for all primes $\mathfrak{p} \nmid 2\Delta_K$.

As w_K is actually the greatest common divisor of these orders, a few well-chosen primes are usually enough to determine w_K and the maximal cyclotomic subfield $\mathbb{Q}(\mu_K) \subset K$.

11. Zeta functions

Although our approach to number rings has been mostly algebraic, we do need a few results from analytic number theory that play an important role in the verification of the *correctness* of any computation of Picard and unit groups. We do not give the proofs of these results.

For a number field K, the *Dedekind zeta function* ζ_K is the complex analytic function defined on the half plane $\mathrm{Re}(t) > 1$ by

$$\zeta_K(t) = \textstyle\sum_{I \neq 0} N_{K/\mathbb{Q}}(I)^{-t}, \tag{11-1}$$

where the sum ranges over all nonzero ideals $I \subset \mathbb{O}$ of the ring of integers $\mathbb{O}_K$ of K. For $K = \mathbb{Q}$, this is the well-known Riemann zeta function $\zeta(t) = \sum_{n=1}^{\infty} n^{-t}$. The sum defining $\zeta_K(t)$ converges absolutely and uniformly on compact subsets of $\mathrm{Re}(t) > 1$, and the holomorphic limit ζ_K can be expanded into an Euler product

$$\zeta_K(t) = \prod\nolimits_{\mathfrak{p}} (1 - N_{K/\mathbb{Q}}(\mathfrak{p})^{-t})^{-1} = \prod\nolimits_{\mathfrak{p}} (1 - p^{-f(\mathfrak{p}/p)t})^{-1} \tag{11-2}$$

over the primes of $\mathbb{O}_K$; this shows that ζ_K is zero-free on $\mathrm{Re}(t) > 1$. To see this, note first that for each rational prime number p, there are at most $n = [K : \mathbb{Q}]$ primes $\mathfrak{p} \mid p$ by Theorem 8.4, and each of these has $N_{K/\mathbb{Q}}(\mathfrak{p}) = p^{f(\mathfrak{p}/p)} \geq p$. The resulting estimate

$$\sum\nolimits_{N_{K/\mathbb{Q}}(\mathfrak{p}) \leq X} |N_{K/\mathbb{Q}}(\mathfrak{p})^{-t}| \leq n \sum\nolimits_{p \leq X} p^{-\mathrm{Re}(t)}$$

shows that $\sum_{\mathfrak{p}} N_{K/\mathbb{Q}}(\mathfrak{p})^{-t}$ converges absolutely and uniformly in every half plane $\mathrm{Re}(t) > 1 + \varepsilon$, so the same is true for the right hand side of (11-2). Multiplication of the geometric series

$$(1 - N_{K/\mathbb{Q}}(\mathfrak{p})^{-t})^{-1} = \textstyle\sum_{k=0}^{\infty} N_{K/\mathbb{Q}}(\mathfrak{p})^{-kt}$$

for all primes $\mathfrak{p}$ reduces (11-2) to (11-1), as every ideal I has a unique factorization as a product of prime ideal powers.

Hecke proved that ζ_K can be extended to a holomorphic function on $\mathbb{C} \setminus \{1\}$, and that it has particularly nice properties when Euler factors are added in (11-2) for the r real and s complex primes of K. More precisely, the function

$$Z(t) = |\Delta_K|^{t/2} \big(\Gamma(t/2)\pi^{-t/2}\big)^r \big(\Gamma(t)(2\pi)^{-t}\big)^s \zeta_K(t) \tag{11-3}$$

satisfies the simple functional equation $Z(t) = Z(1-t)$. In [Lang 1994, Chapter XIII and XIV], one can find both Hecke's classical proof and Tate's 1959 adelic proof of this result. More details on Tate's approach are found in [Ramakrishnan and Valenza 1999].

Hecke's techniques have been used by Zimmert to show that not only Δ_K but also the regulator R_K grows exponentially with the degree. An explicit lower bound [Skoruppa 1993] is

$$R_K / w_K \geq .02 \cdot \exp(.46r + .1s), \tag{11-4}$$

with $w_K = \#\mu_K$ the number of roots of unity in K. Depending on the degree and the size of the discriminant, there are better lower bounds [Friedman 1989]. For all but nine explicitly known fields, one has $R_K / w_K \geq 1/8$.

The functional equation shows that the meromorphic extension of ζ_K to $\mathbb{C}$ has 'trivial zeros' at all negative integers $k \in \mathbb{Z}_{<0}$: for k odd the multiplicity of the zero equals s, whereas for k even the multiplicity equals $r + s$. All other zeros ρ satisfy $0 < \mathrm{Re}(\rho) < 1$, and one of the deepest open problems in number theory, the *Generalized Riemann Hypothesis (GRH)*, predicts that we actually have $\mathrm{Re}(\rho) = 1/2$ for these non-trivial zeros.

At $t = 1$, the Dedekind zeta function ζ_K has a simple pole. Its residue

$$2^r (2\pi)^s \frac{h_K R_K}{w_K |\Delta_K|^{1/2}}$$

at $t = 1$ can be found using extensions of the techniques in the previous section [Lang 1994, Section VIII.2, Theorem 5]. It gives us information on the fundamental invariants h_K, R_K, and Δ_K of K we have defined before. For $K = \mathbb{Q}$ the residue equals 1, and for general K we can approximate it by evaluating the limit $\lim_{t \to 1} \zeta_K(t)/\zeta_{\mathbb{Q}}(t)$ using (11-2) to obtain

$$\frac{h_K R_K}{w_K} = 2^{-r} (2\pi)^{-s} |\Delta_K|^{1/2} \prod\nolimits_p E(p), \tag{11-5}$$

where the Euler factor $E(p)$ at the rational prime p is defined by

$$E(p) = \frac{1 - p^{-1}}{\prod_{\mathfrak{p} \mid p} (1 - p^{-f(\mathfrak{p}/p)})}.$$

Identity (11-5) allows us to approximate $h_K R_K$ by multiplying the Euler factors $E(p)$ for sufficiently many p. Convergence is slow, but we will only need single digit precision. In fixed degree n, it suggests that $h_K R_K$ is a quantity of order of magnitude $|\Delta_K|^{1/2}$. In an asymptotic sense, this is made precise by the *Brauer–Siegel theorem* [Lang 1994, Section XIII.4, Theorem 4], which states that the quotient of the *logarithms* $\log(h_K R_K)$ and $\frac{1}{2} \log |\Delta_K|$ tends to 1 in any sequence of pairwise non-isomorphic normal number fields K of some fixed

degree. The condition of normality can be dispensed with under assumption of GRH, and for the degree it actually suffices to assume that $[K : \mathbb{Q}]/\log|\Delta_K|$ tends to 0. Unfortunately, the theorem is not *effective*.

At $t = 0$, the functional equation shows that ζ_K has a zero of order $r + s - 1$ with leading coefficient $-h_K R_K / w_K$ in the Taylor expansion. The idea that such a coefficient should 'factor over χ-eigenspaces', much like zeta functions themselves factor into L-functions, underlies the largely conjectural theory of *Stark units* [Tate 1984].

12. Computing class groups and unit groups

The actual computations of class groups and units groups are inextricably linked, in the sense that one uses a single algorithm yielding both the class group and the unit group. The complexity of the calculation is exponential in any reasonable measure for the size of the number field, and for number rings that do allow explicit calculations of the type discussed in this section, factoring discriminants and computing normalizations are not expected to pose great difficulties. For this reason, we will focus on the computation of the class group and unit group of a number field K. For other number rings $R \subset K$, the results from Section 5 can be used to relate $\mathrm{Pic}(R)$ and R^* to Cl_K and $\mathbb{O}_K^*$.

The kind of computation that yields Cl_K and $\mathbb{O}_K^*$ has become standard in algorithmic number theory: it factors smooth elements over a suitably chosen factor base and produces relations using linear algebra over $\mathbb{Z}$. In this volume, it occurs in [Lenstra 2008; Pomerance 2008a; 2008b; Stevenhagen 2008; Schirokauer 2008; Schoof 2008b].

Suppose we are given a number field

$$K = \mathbb{Q}[X]/(f)$$

of degree $n = r + 2s$ by means of a defining monic polynomial $f \in \mathbb{Z}[X]$ having r real and s complex conjugate pairs of roots. Computing r and s from f is classical and easy: one counts sign changes in a *Sturm sequence* that can be obtained as a by-product of the computation of the discriminant $\Delta(f)$ from the resultant $R(f, f')$ as in Example 7.9 [Cohen 1993, Theorem 4.1.10]. We take the order $\mathbb{Z}[\alpha]$ defined by $f = f_{\mathbb{Q}}^{\alpha}$, and extend it to $\mathbb{O} = \mathbb{O}_K$ using the methods of Sections 8 and 9. Note that this requires factoring $\Delta(f)$. We then select a smoothness bound B such that Cl_K is generated by the primes $\mathfrak{p}$ in $\mathbb{O}$ of norm at most B. One can take for B the Minkowski constant

$$M_K = \left(\frac{4}{\pi}\right)^s \frac{n!}{n^n} \cdot |\Delta_K|^{1/2}$$

from (10-4) or use the asymptotically *much* smaller *Bach bound*

$$B_K = 12(\log|\Delta_K|)^2,$$

which is good enough if one is willing to assume GRH [Bach 1990]. In practice even the Bach bound is usually overly pessimistic, and correct results may be obtained using even smaller values of B.

EXAMPLE 12.1. For $f = X^3+44$ from Example 8.3, we have $\Delta_K = -2^2\cdot 3\cdot 11^2$ and $r = s = 1$. In this case the Minkowski constant $M_K < 11$ is so small that all calculations can be done by hand. As 44 as not a cube modulo 7, the prime 7 is inert in K, and Cl_K is generated by the primes over 2, 3, and 5. We factored these primes explicitly in Theorem 8.4 as $(2) = \mathfrak{p}_2^3$, $(3) = \mathfrak{p}_3^2\mathfrak{q}_3$ and $(5) = \mathfrak{p}_5\mathfrak{p}_{25}$, where the subscripts denote the norms of the primes involved. Using $g = X^3 + X^2 - 7X - 13$, the irreducible polynomial of the generating element $\delta = \beta - \gamma = (\alpha^2 - 2\alpha - 2)/6$ of $\mathbb{O}_K$ we found in Example 8.3, it suffices to tabulate a few smooth values of g and compute the factorization of those principal ideals $(k-\gamma)$ of norm $N_{K/\mathbb{Q}}(k-\gamma) = g(k)$ that are 5-smooth.

k	-3	-2	-1	0	1	2	3
$g(k)$	$-2\cdot 5$	-3	$-2\cdot 3$	13	$-2\cdot 3^2$	$-3\cdot 5$	2
$(k-\delta)$	$\mathfrak{p}_2\mathfrak{p}_5$	$\mathfrak{q}_3$	$\mathfrak{p}_2\mathfrak{p}_3$	$-$	$\mathfrak{p}_2\mathfrak{q}_3^2$	$\mathfrak{p}_3\mathfrak{p}_5$	$\mathfrak{p}_2$

Note that g has a double zero modulo 3 at $k = -1 \bmod 3$ giving rise to the ramified prime $\mathfrak{p}_3 = (3, \delta+1)$ dividing $(-1-\delta)$, whereas the unramified prime $\mathfrak{q}_3 = (3, \delta+2)$ divides $(k-\delta)$ at the values $k \equiv 1 \bmod 3$. The table shows that $\mathfrak{p}_2 = (3-\delta)$ and $\mathfrak{q}_3 = (2+\delta)$ are principal, and by the entries for $k = -1$ and $k = -3$, the other generators $\mathfrak{p}_3 = (1+\delta)/(3-\delta)$ and $\mathfrak{p}_5 = (3+\delta)/(3-\delta)$ of Cl_K are principal as well, so without any further computation we have $\mathrm{Cl}_K = 0$. The unused entries $k = 1, 2$ now yield *different* generators for $(1-\delta)$ and $(2-\delta)$, namely $(3-\delta)(2+\delta)^2$ and $(1+\delta)(3+\delta)/(3-\delta)^2$. Their quotients are the unit $(1-\delta)(3-\delta)^{-1}(2+\delta)^{-2} = -1$ and the non-trivial unit

$$\varepsilon = (2-\delta)(1+\delta)^{-1}(3+\delta)^{-1}(3-\delta)^2 = -5\delta^2 + 17\delta - 7.$$

In terms of the root α of $f = X^3 + 44$, we have $\varepsilon = \frac{1}{6}(17\alpha^2 - 4\alpha - 226)$. The unit ε is actually fundamental, so we have $\mathbb{O}_K^* = \langle -1\rangle \times \langle \varepsilon\rangle$. To *prove* this fact, we have several options.

One can generate more units using the prime ideal factorizations of 5-smooth ideals such as (2), (3), (5), and $(8+\delta) = \mathfrak{q}_3^4\mathfrak{p}_5$, find that they are all up to sign a power of ε, and decide on *probabilistic* grounds that ε must be fundamental. Alternatively, one can divide the regulator $\mathrm{Reg}(\varepsilon) \approx 8.3$ by the absolute lower bound for R_K following from (11-4) to obtain $[\mathbb{O}_K^* : \langle -1\rangle \times \langle \varepsilon\rangle] \geq 33$, and show that $-\varepsilon$, which has norm 1, is not a p-th power for any prime number $p \leq 31$.

For this, it suffices to find a prime $\mathfrak{p}$ of norm $N\mathfrak{p} \equiv 1 \bmod p$ in $\mathbb{O}_K$ and to show that we have $\varepsilon^{(N\mathfrak{p}-1)/p} \neq 1 \in \mathbb{O}_K/\mathfrak{p}$. If ε is *not* a p-th power in K, such $\mathfrak{p}$ are usually abundant. A third possibility consists in approximating the Euler product (11-5) to precision sufficient to convince oneself that R_K is not equal to $\mathrm{Reg}(\varepsilon)/k$ for some $k > 1$. We will do this in the case of a larger example in Example 12.4.

For a 'small' number field $K = \mathbb{Q}[X]/(f)$ defined by a monic polynomial $f \in \mathbb{Z}[X]$, the basic invariants of K can be found from a small table of factored values of f.

EXAMPLE 12.2. We take $f = X^3 + X^2 + 5X - 16$, which gives rise to the values in Table 1. As f has no zeros modulo 11, 13, and 17, it is irreducible modulo these primes, and in $\mathbb{Z}[X]$. The discriminant $\Delta(f) = -R(f, f')$ can be computed as in Example 7.9, and equals

$$\begin{aligned} -R(X^3+X^2+5X-16, 3X^2+2X+5) &= -3^2\,R(\tfrac{28}{9}X - \tfrac{149}{9}, 3X^2+2X+5) \\ &= -3^2\cdot\left(\tfrac{28}{9}\right)^2\cdot\left(3\left(\tfrac{149}{28}\right)^2+2\left(\tfrac{149}{28}\right)+5\right) \\ &= -8763 \\ &= -3\cdot 23\cdot 127. \end{aligned}$$

As $\Delta(f)$ is squarefree, $K = \mathbb{Q}[X]/(f)$ has $\Delta_K = -8763$ and $\mathbb{O} = \mathbb{O}_K = \mathbb{Z}[\alpha]$. As f has a single real root, we have $r = s = 1$, and Minkowski's constant equals

$$M_K = \frac{3!}{3^3}\frac{4}{\pi}\sqrt{8763} \approx 26.5.$$

The primes in $\mathbb{O}$ of norm at most 25 can be found by factoring the rational primes up to 23 in $\mathbb{O}$. This is an application of Theorem 8.2 using the values of f in

k	$f(k)$	k	$f(k)$
-10	$-2\cdot 3\cdot 7\cdot 23$	0	-2^4
-9	-709	1	-3^2
-8	$-2^3\cdot 3^2\cdot 7$	2	$2\cdot 3$
-7	$-3\cdot 5\cdot 23$	3	$5\cdot 7$
-6	$-2\cdot 113$	4	$2^2\cdot 3\cdot 7$
-5	$-3\cdot 47$	5	$3\cdot 53$
-4	$-2^2\cdot 3\cdot 7$	6	$2\cdot 7\cdot 19$
-3	-7^2	7	$3\cdot 137$
-2	$-2\cdot 3\cdot 5$	8	$2^3\cdot 3\cdot 5^2$
-1	$-3\cdot 7$	9	839

Table 1. Values of $f = X^3 + X^2 + 5X - 16$.

our table. Leaving out the inert primes 11, 13, and 17, we obtain factorizations

$$\begin{aligned}
2\mathbb{O} &= \mathfrak{p}_2\mathfrak{p}_4 = (2,\alpha)\cdot(2,\alpha^2+\alpha+1)\\
3\mathbb{O} &= \mathfrak{p}_3^2\mathfrak{q}_3 = (3,\alpha+1)^2\cdot(3,\alpha-1)\\
5\mathbb{O} &= \mathfrak{p}_5\mathfrak{p}_{25} = (5,\alpha+2)\cdot(5,x_5)\\
7\mathbb{O} &= \mathfrak{p}_7\mathfrak{q}_7\mathfrak{r}_7 = (7,\alpha+1)(7,\alpha-3)(7,\alpha+3)\\
19\mathbb{O} &= \mathfrak{p}_{19}\mathfrak{p}_{361} = (19,\alpha-4)\cdot(19,x_{19})\\
23\mathbb{O} &= \mathfrak{p}_{23}^2\mathfrak{q}_{23} = (23,\alpha+7)^2(23,\alpha+10)
\end{aligned}$$

in which x_5 and x_{19} denote elements that we do not bother to compute. This shows that Cl_K is generated by the classes of the primes $\mathfrak{p}_2$, $\mathfrak{p}_3$, $\mathfrak{p}_5$, $\mathfrak{p}_{19}$, $\mathfrak{p}_{23}$, and two of the primes over 7. We can express the classes of the large primes in those of smaller primes using the factorizations of principal ideals $(k-\alpha)$ resulting from the values of $f(k)$ in our table.

The entry $k=-7$ yields $(-7-\alpha)=\mathfrak{p}_3\mathfrak{p}_5\mathfrak{p}_{23}$, so we can omit $[\mathfrak{p}_{23}]$ from our list of generators. Similarly, we can omit $[\mathfrak{p}_{19}]$ as the entry $k=6$ gives $(6-\alpha)=\mathfrak{p}_2\mathfrak{p}_7\mathfrak{p}_{19}$. The primes over 7 can be dealt with using the identities $(-1-\alpha)=\mathfrak{p}_3\mathfrak{p}_7$ and $(3-\alpha)=\mathfrak{p}_5\mathfrak{q}_7$. The relation $(-2-\alpha)=\mathfrak{p}_2\mathfrak{q}_3\mathfrak{p}_5=3\mathfrak{p}_2\mathfrak{p}_3^{-2}\mathfrak{p}_5$ takes care of $[\mathfrak{p}_5]$, and finally $(2-\alpha)=\mathfrak{p}_2\mathfrak{p}_3$ shows that the class group of K is generated by $[\mathfrak{p}_2]$. The order of this class divides 4 since we have $(\alpha)=\mathfrak{p}_2^4$, and further relations do not indicate that it is smaller.

To show that $\mathfrak{p}_2^2$ is not principal and that $\mathrm{Cl}_K=\langle[\mathfrak{p}_2]\rangle$ is cyclic of order 4, we need to know the group $\mathbb{O}^*/(\mathbb{O}^*)^2$. As in Example 12.1, we can produce a non-trivial unit from the fact that the factorizations of 3, (α), $(\alpha-1)$, and $(\alpha-2)$ involve only $\mathfrak{p}_2$ and the primes over 3. One deduces that

$$\eta=\frac{(\alpha-1)(\alpha-2)^4}{9\alpha}=4\alpha^2+\alpha-13$$

is a unit of norm $N(\eta)=1$. From the Dirichlet unit theorem (with $r=s=1$) we have $\mathbb{O}^*\cong\langle-1\rangle\times P$, where $P\cong\mathbb{Z}$ can be taken to be the group of units of norm 1. In order to prove that η generates P/P^2, it suffices to show that η is not a square in $\mathbb{O}^*$. This is easy: reducing modulo $\mathfrak{p}_3$ we find $\eta\equiv 4-1-13\equiv -1$, and -1 is not a square in $\mathbb{O}/\mathfrak{p}_3=\mathbb{F}_3$.

Suppose now that $\mathfrak{p}_2^2=(y)$ is principal. Then y^2 and α are both generators of $\mathfrak{p}_2^4$, so there exists a unit ε with $y^2=\varepsilon\cdot\alpha$. As the norm $N(\varepsilon\cdot\alpha)=16N(\varepsilon)=N(y)^2$ is positive, we have $\varepsilon\in P$. If ε is in P^2, then $\alpha=\varepsilon^{-1}y^2$ is a square, contradicting that we have $\alpha\equiv -2 \bmod \mathfrak{p}_5$. If ε is in ηP^2, then $\eta\cdot\alpha$ is a square, and this is contradicted by the congruence

$$\eta\cdot\alpha\equiv(4(-2)^2+(-2)-13)\cdot -2\equiv 3 \bmod \mathfrak{p}_5.$$

We conclude that no unit ε exists, and that $\mathfrak{p}^2$ has order 2 in $\mathrm{Cl}_K \cong \mathbb{Z}/4\mathbb{Z}$. As in Example 12.1, we can show in various ways that η is actually a fundamental unit, and that we have $\mathcal{O}^* = \langle -1 \rangle \times \langle \eta \rangle$.

In number fields $K = \mathbb{Q}(\alpha)$ that are bigger than the two baby examples we just did, more work is involved, but the underlying idea remains the same. Having chosen a factor bound B, one explicitly obtains the factorization of all primes $p \leq B$ using the Kummer–Dedekind theorem for $\mathbb{Z}[\alpha]$. For those primes p dividing the index of $\mathbb{Z}[\alpha]$ in $\mathcal{O}_K$, some extra work is needed as $\mathcal{O}/p\mathcal{O}$ may not be monogenic over $\mathbb{F}_p$. However, everything can be determined using the techniques of Section 9, using linear algebra over $\mathbb{F}_p$. One is left with a factor base consisting of the set T of primes of norm at most B.

Next, one tries to factor sufficiently many principal ideals $(x) \subset \mathcal{O}_K$ over the chosen factor base. The B-smooth elements $x \in \mathcal{O}_K \setminus \{0\}$ for which this is possible generate the subgroup $\mathcal{O}_{K,T}^* \subset K^*$ of T-units, and we have an exact sequence

$$1 \to \mathcal{O}_K^* \longrightarrow \mathcal{O}_{K,T}^* \xrightarrow{F} \mathbb{Z}^T \xrightarrow{C} \mathrm{Cl}_K \to 0.$$

Here F is the 'factorization map' that sends $x \in \mathcal{O}_{K,T}^*$ to its exponent vector $(\mathrm{ord}_{\mathfrak{p}}(x\mathcal{O}_K))_{\mathfrak{p} \in T}$, and C is the natural map sending the characteristic function of $\mathfrak{p} \in T$ to the ideal class of $[\mathfrak{p}]$. As $\mathcal{O}_{K,T}^*$ is a free abelian group of rank $\#T + r + s - 1$ by Theorem 10.9, we expect it to be generated by any 'random' subset of its elements of cardinality substantially larger than its rank.

EXAMPLES 12.3. In $K = \mathbb{Q}(\sqrt[3]{44})$ from Example 12.1, the set T of primes of norm at most 5 consists of 4 primes, and $\#T + r + s - 1$ equals 5. The 6 elements $k - \delta$ with $|k| \in \{1, 2, 3\}$ already generate $\mathcal{O}_{K,T}^* \cong \langle -1 \rangle \times \mathbb{Z}^5$.

In Example 12.2, with T consisting of the 3 primes of norm at most 3, the elements 3, (α), $(\alpha - 1)$, and $(\alpha - 2)$ are independent in $\mathcal{O}_{K,T}^* \cong \langle -1 \rangle \times \mathbb{Z}^4$.

For a subset $X \subset \mathcal{O}_{K,T}^*$ generating a subgroup of maximal rank, it is a matter of linear algebra over $\mathbb{Z}$ to reduce the matrix of exponent vectors $(F(x))_{x \in X}$ and to compute the group $\mathbb{Z}^T / F[X]$, which will be of finite order

$$h' = [F[\mathcal{O}_{K,T}^*] : F[X]] \cdot h_K$$

if X is sufficiently large. The dependencies found between the vectors give rise to elements $u \in \mathcal{O}_K^* = \ker(F)$ generating a subgroup $U \subset \mathcal{O}_K^*$. For these elements we compute their log-vectors $L'(u) \in H \subset \mathbb{R}^{r+s}$ as in Theorem 10.7. Linear algebra over $\mathbb{R}$ will give us $r + s - 1$ independent units generating the lattice $L[U]$ if X is sufficiently large, and the associated regulator is

$$R' = [\mathcal{O}_K^* : L[U]] \cdot R_K.$$

If our set X truly generates $\mathbb{O}_{K,T}^*$, then we have $h' = h_K$ and $R' = R_K$, so

$$\mathrm{Cl}_K \cong \mathbb{Z}^T / F[X]$$

and $\mathbb{O}_K^* = U$. If this is not the case, $h'R' > h_K R_K$ will be an integral multiple of $h_K R_K$, and we discover this by comparing our value $h'R'$ with the analytic estimate of $h_K R_K$ obtained by approximating (11-5) with a truncated Euler product. The factors $E(p)$ in (11-5) are computed from the 'factorization type' of p in $\mathbb{O}_K$, which we know already for $p < B$, and which follows for more p, if desired, from the factorization type of the defining polynomial f modulo p.

The description of the fundamental units furnished by the algorithm is a *power product representation* in terms of T-units in X. Although the set X we pick to generate $\mathbb{O}_{K,T}^*$ usually consists of elements that are relatively small, the units obtained from them can be huge when written out on a basis of K over $\mathbb{Q}$. This is unavoidable in view of the order of magnitude $|\Delta_K|^{1/2}$ of $h_K R_K$: in many cases h_K appears to be rather small, and this means that the regulator measuring the *logarithmic* size of the unit group will be of size $|\Delta_K|^{1/2}$. In such cases the units themselves require a number of bits that is exponential in $\log|\Delta_K|$. Already in the simplest non-trivial case of real quadratic fields, the phenomenon of the smallest solution of the Pell equation $x^2 - dy^2 = 1$ being very large in comparison to $d > 0$ was noticed 350 years ago by Fermat.

This paper does not intend to present cutting-edge examples of the performance of the algorithm above, which involve serious linear algebra to reduce large matrices over $\mathbb{Z}$. The final example below is small and 'hands-on' like the cubic Examples 12.1 and 12.2. It illustrates the use of log-vectors in the determination of the unit group, and the analytic confirmation of the algebraically obtained output.

EXAMPLE 12.4. Let K be the quartic field generated by a root α of the polynomial

$$f = X^4 - 2X^2 + 3X - 7 \in \mathbb{Z}[X]$$

of prime discriminant $\Delta(f) = -98443$. Then we have $\mathbb{O}_K = \mathbb{Z}[\alpha]$, an order with $r = 2$, $s = 1$ and Minkowski constant $M_K \approx 37.4$. To deal with all primes of norm up to 37, we tabulate consecutive values of f in Table 2 on the next page.

This shows that f has no roots modulo the primes $p = 2, 3, 17, 23, 29$, and also modulo 37 once we check $37 \nmid f(18)$. In fact, f is irreducible modulo 2 and 3, and the factorization $(5) = \mathfrak{p}_5\mathfrak{q}_5\mathfrak{p}_{25}$ shows that Cl_K is generated by the ideals of prime norm $p \in [5, 31]$, which all 'occur' in Table 2.

n	$f(n)$	n	$f(n)$	n	$f(n)$
-18	$127\cdot 821$	-6	$11\cdot 109$	6	$5\cdot 13\cdot 19$
-17	$5\cdot 11^2\cdot 137$	-5	$7\cdot 79$	7	$7\cdot 331$
-16	64969	-4	$5\cdot 41$	8	$5\cdot 797$
-15	50123	-3	47	9	$7^2\cdot 131$
-14	$5^2\cdot 7^2\cdot 31$	-2	-5	10	$11\cdot 19\cdot 47$
-13	$19\cdot 1483$	-1	-11	11	$5^2\cdot 577$
-12	$5\cdot 7\cdot 11\cdot 53$	0	-7	12	20477
-11	$83\cdot 173$	1	-5	13	$5\cdot 5651$
-10	$13\cdot 751$	2	7	14	$7\cdot 5437$
-9	$5\cdot 19\cdot 67$	3	$5\cdot 13$	15	$149\cdot 337$
-8	$31\cdot 127$	4	229	16	$5\cdot 7\cdot 11\cdot 13^2$
-7	$5^2\cdot 7\cdot 13$	5	$11\cdot 53$	17	$31\cdot 2677$

Table 2. Values of $f = X^4 - 2X^2 + 3X - 7 \in \mathbb{Z}[X]$.

In case $f(n) = \pm p$ is prime, the prime ideal $(p, \alpha - n)$ is principal and generated by $\alpha - n$. The following list of ideals of prime norm $p \leq 31$ results.

$$\begin{aligned} \mathfrak{p}_5 &= (\alpha - 1) & \mathfrak{q}_5 &= (\alpha + 2) \\ \mathfrak{p}_7 &= (\alpha) & \mathfrak{q}_7 &= (\alpha - 2) \\ \mathfrak{p}_{11} &= (\alpha + 1) & \mathfrak{q}_{11} &= (11, \alpha - 5) \\ \mathfrak{p}_{13} &= (13, \alpha - 3) & \mathfrak{q}_{13} &= (13, \alpha - 6) \\ \mathfrak{p}_{19} &= (19, \alpha - 6) & \mathfrak{q}_{19} &= (19, \alpha + 9) \\ \mathfrak{p}_{31} &= (31, \alpha + 8) & \mathfrak{q}_{31} &= (31, \alpha + 14) \end{aligned}$$

The primes lying over 5 and 7 are all principal, and so is $\mathfrak{p}_{11}$. This suggests strongly that $\mathrm{Cl}(\mathcal{O})$ is trivial. In order to prove this, we try to express all primes in the table in terms of the principal ideals. From the entry with $k = 3$ in our table we obtain $(3 - \alpha) = \mathfrak{p}_{13}\mathfrak{q}_5$, showing that $\mathfrak{p}_{13}$ is principal. The relation $(16 - \alpha) = \mathfrak{p}_5\mathfrak{q}_7\mathfrak{q}_{11}\mathfrak{p}_{13}^2$ then shows that $\mathfrak{q}_{11}$ is also principal. Similarly, we have principality of $\mathfrak{q}_{13}$ from $(-7 - \alpha) = \mathfrak{q}_5^2\mathfrak{p}_7\mathfrak{q}_{13}$ and of $\mathfrak{p}_{19}$ from $(6 - \alpha) = \mathfrak{p}_5\mathfrak{q}_{13}\mathfrak{p}_{19}$. Finally, we use $(-14 - \alpha) = \mathfrak{p}_5^2\mathfrak{p}_7^2\mathfrak{q}_{31}$ to eliminate $\mathfrak{q}_{31}$. This exploits all useful relations from our table, leaving us with the primes $\mathfrak{q}_{19}$ and $\mathfrak{p}_{31}$. In order to prove that these primes are also principal, we factor a small element in them. Modulo $\mathfrak{q}_{19} = (19, \alpha + 9)$ we have $\alpha = -9 \in \mathbb{F}_{19}$, and $1 - 2\alpha$ is therefore a small element in the ideal. Similarly, we have $\alpha = -8 \in \mathbb{F}_{31}$ when working modulo $\mathfrak{p}_{31} = (31, \alpha + 8)$, so $1 + 4\alpha$ is in $\mathfrak{p}_{31}$. The norms of these elements are $N(1 - 2\alpha) = 2^4 f(1/2) = -5 \cdot 19$ and $N(1 + 4\alpha) = (-4)^4 f(-1/4) = 5 \cdot 13 \cdot 31$, which implies that $\mathfrak{q}_{19}$ and $\mathfrak{p}_{31}$ are principal. The corresponding explicit factorizations are $(1 - 2\alpha) = \mathfrak{q}_5\mathfrak{q}_{19}$ and $(1 + 4\alpha) = \mathfrak{p}_5\mathfrak{p}_{13}\mathfrak{p}_{31}$. This proves that $\mathrm{Cl}(\mathcal{O})$ is trivial.

At this stage, we have produced explicit generating elements for all prime ideals of norm below the Minkowski bound. Although we do not need all of these generators, we list them for completeness sake.

$$\begin{aligned}
\mathfrak{p}_5 &= (\alpha - 1) & \mathfrak{q}_5 &= (\alpha + 2)\\
\mathfrak{p}_7 &= (\alpha) & \mathfrak{q}_7 &= (\alpha - 2)\\
\mathfrak{p}_{11} &= (\alpha + 1) & \mathfrak{q}_{11} &= (32\alpha^3 + 53\alpha^2 + 25\alpha + 138)\\
\mathfrak{p}_{13} &= (\alpha^3 - 2\alpha^2 - 2\alpha - 2) & \mathfrak{q}_{13} &= (2\alpha^3 - 4\alpha^2 + 5\alpha - 6)\\
\mathfrak{p}_{19} &= (\alpha^3 + \alpha^2 + \alpha + 8) & \mathfrak{q}_{19} &= (\alpha^3 - 2\alpha^2 + 2\alpha - 3)\\
\mathfrak{p}_{31} &= (2\alpha^3 + 3\alpha^2 + 2\alpha + 11) & \mathfrak{q}_{31} &= (\alpha^3 + \alpha^2 + 6)
\end{aligned}$$

These generators are not necessarily the smallest or most obvious generators of the ideals in question, they happen to come out of the arguments by which we eliminated all generators of the class group. The search for units that is to follow will provide other generators, and one can for instance check that the large coefficients of our generator for $\mathfrak{q}_{11}$ are not necessary as we have $\mathfrak{q}_{11} = (\alpha^2 - 3)$.

From now on every further factorization of a principal ideal (x) as a product of primes in this table will give us a unit in $\mathbb{O}$: since both x and a product of generators from our table generate (x), this means that their quotient is a unit. Trying some elements $a + b\alpha$, for which we can easily compute the norm $N_{K/\mathbb{Q}}(a + b\alpha) = b^4 f(-a/b)$, one quickly generates a large number of units. The rank of the unit group $\mathbb{O}^*$ for our field K equals $r + s - 1 = 2$, so some administration is needed to keep track of the subgroup of $\mathbb{O}^*$ generated by these units. As in the proof of the Dirichlet unit theorem, one looks at the lattice in $\mathbb{R}^2$ generated by the 'log-vectors' $L(u) = (\log|\sigma_1(u)|, \log|\sigma_2(u)|)$ for each unit u. Here σ_1 and σ_2 are taken to be the real embeddings $K \to \mathbb{R}$, so they send α to the real roots $\alpha_1 \approx -2.195$ and $\alpha_2 \approx 1.656$ of f.

The table below lists a couple of units obtained from small elements $a + b\alpha$.

relation	u	$L(u)$
$(2\alpha + 1) = \mathfrak{q}_{11}\mathfrak{q}_{13}$	$\alpha^3 - 2\alpha^2 + 3\alpha - 4$	$(3.4276, -3.7527)$
$(2\alpha - 3) = \mathfrak{q}_{31}$	$\alpha^3 - 2\alpha^2 + 3\alpha - 4$	$(3.4276, -3.7527)$
$(2\alpha + 3) = \mathfrak{p}_5^2\mathfrak{q}_7$	$-3\alpha^3 - 5\alpha^2 - 2\alpha - 12$	$(-3.4276, \quad 3.7527)$
$(3\alpha + 1) = \mathfrak{q}_5\mathfrak{q}_7\mathfrak{p}_{19}$	$5\alpha^3 - 11\alpha^2 + 14\alpha - 16$	$(5.0281, -1.2731)$
$(3\alpha - 5) = \mathfrak{q}_{13}$	$\alpha^3 - 4\alpha + 2$	$(-1.6005, -2.4796)$
$(3\alpha - 4) = \mathfrak{q}_5^2\mathfrak{q}_{11}$	$-4743\alpha^3 + 10412\alpha^2$ $-13371\alpha + 15124$	$(11.8833, -8.7785)$
$(4\alpha - 7) = \mathfrak{q}_5\mathfrak{p}_7\mathfrak{p}_{11}$	$-\alpha^3 + 2\alpha^2 - 3\alpha + 4$	$(3.4276, -3.7527)$

We see that

$$\eta_1 = \alpha^3 - 2\alpha^2 + 3\alpha - 4 \qquad \text{and} \qquad \eta_2 = \alpha^3 - 4\alpha + 2$$

are likely to be fundamental. From the log-vectors, the units in the fourth and sixth lines of the table are easily identified (up to sign) as being equal to $\eta_1\eta_2^{-1}$ and $\eta_1^3\eta_2^{-1}$.

In order to show that $\mathbb{O}^*$ is equal to $\langle -1\rangle \times \langle \eta_1\rangle \times \langle \eta_2\rangle$, we have to check that the regulator of K is equal to

$$\mathrm{Reg}(\eta_1,\eta_2) = \begin{vmatrix} \log|\sigma_1(\eta_1)| & \log|\sigma_1(\eta_2)| \\ \log|\sigma_2(\eta_1)| & \log|\sigma_2(\eta_2)| \end{vmatrix} \approx \begin{vmatrix} 3.4276 & -1.6005 \\ -3.7527 & -2.4796 \end{vmatrix} \approx 14.506.$$

If this is the case, the residue in $t = 1$ of the zeta function $\zeta_K(t)$ of K should equal

$$\frac{2^r(2\pi)^s h_K R(\eta_1,\eta_2)}{w_K\sqrt{|\Delta|}} \approx \frac{2^2(2\pi)\cdot 1\cdot 14.506}{2\cdot\sqrt{98443}} \approx 0.5810.$$

We can approximate this residue using (11-5), using the Euler product $\prod_p E(p)$, with

$$E(p)^{-1} = \frac{\prod_{\mathfrak{p}\mid p}(1 - N_{K/\mathbb{Q}}(\mathfrak{p})^{-1})}{1 - p^{-1}}.$$

The factor $E(p)^{-1}$ is a polynomial expression in p^{-1} that depends only on the residue class degrees of the primes $\mathfrak{p} \mid p$, that is, on the degrees of the irreducible factors of the defining polynomial f modulo p. If we disregard the single ramified prime 98443, there are 5 possible factorization types of f modulo p. If the number n_p of zeros of f mod p equals 4, 2, or 1, we immediately know the degree of all irreducible factors of f mod p. For $n_p = 0$, the polynomial f is either irreducible modulo p or a product of two quadratic irreducibles, and we can use the fact that the *parity* of the number g of irreducible factors of f mod p can be read off from $\left(\frac{\Delta(f)}{p}\right) = (-1)^{n-g}$ for $p \nmid \Delta(f)$. It follows that we have

$$E(p)^{-1} = \begin{cases} (1-p^{-1})^3 & \text{if } n_p = 4; \\ (1-p^{-1})(1-p^{-2}) & \text{if } n_p = 2; \\ 1-p^{-3} & \text{if } n_p = 1; \\ (1+p^{-1})(1-p^{-2}) & \text{if } n_p = 0 \text{ and } \left(\frac{\Delta(f)}{p}\right) = 1; \\ 1+p^{-1}+p^{-2}+p^{-3} & \text{if } n_p = 0 \text{ and } \left(\frac{\Delta(f)}{p}\right) = -1. \end{cases}$$

The following data indicate the speed of convergence of this product.

N	$\prod_{p<N} E(p)$	N	$\prod_{p<N} E(p)$
100	0.625211	5000	0.579408
200	0.595521	10000	0.579750
500	0.581346	20000	0.581892
1000	0.584912	50000	0.581562
2000	0.585697	100000	0.581423

We see that the convergence is non-monotonous and slow, but all values are close to the expected value 0.5810. If our units η_1 and η_2 were not fundamental, the Euler product should be at least twice as small as 0.5810, which is highly unlikely. Under GRH, one can effectively bound the error of a finite approximation [Buchmann and Williams 1989, Theorem 3.1] and *prove* the correctness of the result obtained.

13. Completions

We have seen in Section 5 that a regular prime $\mathfrak{p}$ of a number ring R gives rise to a discrete valuation ring $R_\mathfrak{p} \subset R$ with maximal ideal containing $\mathfrak{p}$. If $\mathfrak{p}$ is singular, there is a discrete valuation ring with this property for every prime $\widetilde{\mathfrak{p}}$ over $\mathfrak{p}$ in the normalization of R from Theorem 6.5. Thus, the discrete valuation rings having a given number field K as their field of fractions correspond bijectively to the primes of the ring of integers $\mathbb{O}_K$ of K. One may even follow the example of the geometers in their definition of *abstract non-singular curves* [Hartshorne 1977, Section I.6] and say that these discrete valuation rings *are* the *primes* or *places* of K.

For each prime $\mathfrak{p}$ of $\mathbb{O}_K$, one can use the discrete valuation $\mathrm{ord}_\mathfrak{p} : K \to \mathbb{Z} \cup \{\infty\}$ to define a $\mathfrak{p}$-adic *absolute value* or *exponential valuation* on K by

$$|x - y|_\mathfrak{p} = N_{K/\mathbb{Q}}(\mathfrak{p})^{-\mathrm{ord}_\mathfrak{p}(x-y)}. \tag{13-1}$$

By (5-5), it satisfies $|xy|_\mathfrak{p} = |x|_\mathfrak{p}|y|_\mathfrak{p}$ for $x, y \in K$ and the *ultrametric inequality*

$$|x + y|_\mathfrak{p} \le \max\{|x|_\mathfrak{p}, |y|_\mathfrak{p}\}. \tag{13-2}$$

Instead of $N_{K/\mathbb{Q}}(\mathfrak{p}) = \#(\mathbb{O}_K/\mathfrak{p})$, we could have taken any real number $c > 1$ in (13-1) to get an equivalent metric inducing the same topology on K, but our normalization will be natural in view of (13-4) and the remark following it.

One may now *complete* the number field K as in [Weiss 1963, Section I.7] with respect to the metric in (13-1) to obtain a field $K_\mathfrak{p}$ that is complete with respect to the $\mathfrak{p}$-adic absolute value, using a process similar to the construction of the field of real numbers $\mathbb{R}$ as consisting of *limits* of Cauchy sequences of rational numbers. If we choose a *uniformizer* $\pi \in K$ of order $\mathrm{ord}_\mathfrak{p}(\pi) = 1$ as

in Proposition 5.4(3) and some finite set $S \subset \mathbb{O}$ of representatives of the cosets of $\mathfrak{p}$ in $\mathbb{O}$, then every $x \in K_\mathfrak{p}$ can *uniquely* be written as a converging Laurent series

$$x = \sum_{k=k_0}^{\infty} a_k \pi^k \in K_\mathfrak{p}$$

with 'digits' $a_k \in S$. The field operations can be performed as for real numbers represented in terms of their decimal expansions, so effective computations in $K_\mathfrak{p}$ are possible to any given $\mathfrak{p}$-adic *precision*.

Topologically, the fields $K_\mathfrak{p}$ are locally compact fields, but their topology is different from that of the more familiar *archimedean* locally compact fields $\mathbb{R}$ and $\mathbb{C}$. As a result of the *non-archimedean* ultrametric inequality (13-2), small quantities do not become large when repeatedly added to themselves in $K_\mathfrak{p}$, so all open disks $\{x \in K_\mathfrak{p} : |x|_\mathfrak{p} < \varepsilon\}$ around $0 \in K_\mathfrak{p}$ are additive subgroups of $K_\mathfrak{p}$. By the discreteness of the absolute value, these open disks are also closed in $K_\mathfrak{p}$, and $K_\mathfrak{p}$ is a *totally disconnected* topological space.

The closure $O_\mathfrak{p}$ of the ring of integers $\mathbb{O}_K$ in $K_\mathfrak{p}$, which is equal to the closed unit disk of radius 1 in $K_\mathfrak{p}$, is a compact *ring* consisting of the $\mathfrak{p}$-*adic integers*, that is, elements of the form $\sum_{k\geq 0} a_k \pi^k$.

For $K = \mathbb{Q}$, the completion at primes leads as in [Gouvêa 1993; Koblitz 1984] to the rings $\mathbb{Z}_p$ of p-adic integers and the p-adic fields $\mathbb{Q}_p$ from [Buhler and Wagon 2008, Section 4.3]. Just like the field of real numbers, the field $\mathbb{Q}_p$ is algebraically 'simpler' than $\mathbb{Q}$: the number of extensions of $\mathbb{Q}_p$ of fixed degree n (inside an algebraic closure) is a *finite* number. In fact, defining such extensions by a monic polynomial from $\mathbb{Z}_p[X]$, one can derive this from the compactness of $\mathbb{Z}_p$ by showing (*Krasner's lemma* [Lang 1994, Proposition II.2.3]) that irreducible polynomials in $\mathbb{Z}_p[X]$ that are coefficientwise sufficiently close define the same extension of $\mathbb{Q}_p$. In particular, all finite extensions of $\mathbb{Q}_p$ arise as completions of number fields at primes over $\mathfrak{p}$.

For a number field $K = \mathbb{Q}(\alpha)$ defined by a monic polynomial $f = f_\mathbb{Q}^\alpha \in \mathbb{Z}[X]$, finding the primes of K lying over a rational prime p amounts to factoring f over $\mathbb{Q}_p$, as a factorization $f = \prod_{i=1}^s f_i \in \mathbb{Q}_p[X]$ yields an isomorphism

$$K \otimes_\mathbb{Q} \mathbb{Q}_p = \mathbb{Q}_p[X]/(f) \xrightarrow{\sim} \prod_{i=1}^s \mathbb{Q}_p[X]/(f_i) = \prod_{i=1}^s K_{\mathfrak{p}_i} \qquad (13\text{-}3)$$

that maps the subring $\mathbb{Z}[\alpha] \otimes_\mathbb{Z} \mathbb{Z}_p = \mathbb{Z}_p[X]/(f)$ into $\prod_{i=1}^s O_{\mathfrak{p}_i}$, with equality if and only if $\mathbb{Z}[\alpha]$ is regular over p.

By Hensel's lemma [Buhler and Wagon 2008, Section 4.3], the factorization of f over $\mathbb{Q}_p$ can be found by factoring f modulo a sufficiently high power of p and lifting the factors by a Newton-type algorithm. Finite precision is enough to determine the nature of the extension field $K_{\mathfrak{p}_i}$ corresponding to a factor f_i in (13-3), and in this light the Kummer–Dedekind Theorem 8.2 is a first step that exploits the factorization of $(f \mod p) \in \mathbb{F}_p[X]$. In case $f \mod p$ is separable,

Hensel's lemma yields the 'unramified case' of the Kummer–Dedekind theorem (Theorem 8.2), and $K_{\mathfrak{p}_i} = \mathbb{Q}_p[X]/(f_i)$ is *the* unramified extension of $\mathbb{Q}_p$ of degree $f(\mathfrak{p}_i/p) = \deg(f_i)$.

Apart from the completions at the primes $\mathfrak{p}$ of the ring of integers, we also have completions of K arising from the embeddings $\sigma : K \to \mathbb{C}$ occurring in (10-2). Up to complex conjugation, there are r real and s complex embeddings known as the *infinite* primes of K, and the completion is either $\mathbb{R}$ or $\mathbb{C}$ for these primes. We normalize the absolute values at an infinite prime $\mathfrak{p}$ corresponding to σ in each of these cases by putting $|x|_{\mathfrak{p}} = |\sigma(x)|$ if $\mathfrak{p}$ is real, and $|x|_{\mathfrak{p}} = |\sigma(x)|^2$ if $\mathfrak{p}$ is complex.

The normalization of infinite absolute values is actually *the same* as for the finite absolute values in (13-1). To explain this, we note that each *local field* $K_{\mathfrak{p}}$ obtained by completing K at a prime $\mathfrak{p}$ is locally compact, and comes with a translation invariant measure [Ramakrishnan and Valenza 1999, Theorem 1.8] that is unique up to a scalar factor; this is the *Haar measure* $\mu_{\mathfrak{p}}$. For the infinite primes, $\mu_{\mathfrak{p}}$ is a multiple of the familiar Lebesgue measure on $\mathbb{R}$ or $\mathbb{C}$ that we used implicitly in the volume computations in the $\mathbb{R}$-algebra $K_{\mathbb{R}} = \prod_{\mathfrak{p}\,|\,\infty} K_{\mathfrak{p}}$ from (10-2). The normalization of the infinite absolute values is inspired by the fact that for $x \in K_{\mathfrak{p}}$, we have $\mu_{\mathfrak{p}}(xB_{\mathfrak{p}}) = |x|_{\mathfrak{p}}\mu_{\mathfrak{p}}(B_{\mathfrak{p}})$ for all measurable subsets $B_{\mathfrak{p}} \subset K_{\mathfrak{p}}$. For finite $\mathfrak{p}$, the very same identity gives rise to the normalization (13-1): multiplication by x increases all volumes in $K_{\mathfrak{p}}$ by a factor $|x|_{\mathfrak{p}}$.

With our normalization, the product $\prod_{\mathfrak{p}\,|\,\infty} |x|_{\mathfrak{p}}$ of the infinite absolute values of x equals $|N_{K/\mathbb{Q}}(x)|$ by the remark following (7-1). In view of (13-1) and the compatibility of element and ideal norm, we arrive at the *product formula*

$$\prod_{\mathfrak{p}} |x|_{\mathfrak{p}} = 1 \qquad \text{for } x \in K^*, \tag{13-4}$$

where the product is taken over *all* primes of K, both finite and infinite. It is the arithmetic analogue of the complex geometric fact that functions on curves have 'as many zeros as they have poles' when we count them with multiplicity and all 'points at infinity' are included in our (projective) curves.

14. Adeles and ideles

Despite the intrinsic differences between finite and infinite primes, the product formula already indicates that it is often useful to treat them equally, in order to obtain a closer analogy with the geometric situation, where all 'places' of a curve are of the same finite nature. This has given rise to the concept of the *adele ring* $\mathbf{A}_K = \prod'_{\mathfrak{p}} K_{\mathfrak{p}}$ of K, a global object obtained by taking a restricted direct product of *all* completions $K_{\mathfrak{p}}$, both finite and infinite. The restriction means that we deal only with elements that are in the local ring of integers $O_{\mathfrak{p}}$

at almost all finite $\mathfrak{p}$, that is,

$$\mathbf{A}_K = \{(x_\mathfrak{p})_\mathfrak{p} \in \textstyle\prod_\mathfrak{p} K_\mathfrak{p} : |x_\mathfrak{p}|_\mathfrak{p} \leq 1 \text{ for almost all } \mathfrak{p}\}.$$

With this restriction, the adele ring is naturally a locally compact ring whose topology is generated by sets of the form $\prod_{\mathfrak{p}\in T} X_\mathfrak{p} \times \prod_{\mathfrak{p}\notin T} O_\mathfrak{p}$. Here T is a finite set of primes containing the infinite primes, $X_\mathfrak{p}$ is some open subset of the locally compact field $K_\mathfrak{p}$, and $O_\mathfrak{p}$ is the compact ring of integers in $K_\mathfrak{p}$ at finite $\mathfrak{p}$. The diagonal embedding $K \to \mathbf{A}_K$ defined by $x \mapsto (x)_\mathfrak{p}$ makes K into a subring of $\mathbf{A}_K$.

For $A_\mathbb{Q} = \mathbb{R} \times \prod_p' \mathbb{Q}_p$, the compact open neighborhood $W = [-\frac{1}{2}, \frac{1}{2}] \times \prod_p \mathbb{Z}_p$ of 0 satisfies $W \cap \mathbb{Q} = \{0\}$ and $\mathbb{Q} + W = \mathbf{A}_\mathbb{Q}$. It follows that $\mathbb{Q}$ is discrete in $\mathbf{A}_\mathbb{Q}/\mathbb{Q}$ and that the quotient group $\mathbf{A}_\mathbb{Q}/\mathbb{Q}$ is compact. The same statements hold for $K \subset \mathbf{A}_K$ and the quotient group $\mathbf{A}_K$, as (13-3) shows that the adele ring $\mathbf{A}_K \cong \mathbf{A}_\mathbb{Q} \otimes_\mathbb{Q} K$ is obtained from $\mathbf{A}_\mathbb{Q}$ by applying the base change $\mathbb{Q} \to K$. One can show that the locally compact group $\mathbf{A}_K$ is naturally isomorphic to its Pontryagin dual, and that isomorphism makes K into its own annihilator. This lies at the basis of the adelic proof of the functional equation of the zeta function alluded to after (11-3).

The unit group $\mathbf{A}_K^* = \prod_\mathfrak{p}' K_\mathfrak{p}^*$ of the adele ring of K is the *idele group*

$$\mathbf{A}_K^* = \{(x_\mathfrak{p})_\mathfrak{p} \in \textstyle\prod_\mathfrak{p} K_\mathfrak{p}^* : |x_\mathfrak{p}|_\mathfrak{p} = 1 \text{ for almost all } \mathfrak{p}\}. \tag{14-1}$$

This is naturally a locally compact group, when its topology is generated as above by sets of the form $\prod_{\mathfrak{p}\in T} Y_\mathfrak{p} \times \prod_{\mathfrak{p}\notin T} O_\mathfrak{p}^*$. The idele group contains K^* diagonally as a discrete subgroup of *principal ideles*. We define the *norm* of an idele by

$$\|(x_\mathfrak{p})_\mathfrak{p}\| = \textstyle\prod_\mathfrak{p} |x_\mathfrak{p}|_\mathfrak{p}, \tag{14-2}$$

which is well defined by (14-1), and we note that the norm map factors by the product formula (13-4) via the *idele class group* $C_K = \mathbf{A}_K^*/K^*$. The idele class group is of fundamental importance in class field theory, which describes the Galois group of the maximal abelian extension of K over K as a quotient of C_K under the *Artin map* [Cohen and Stevenhagen 2008]. In the most classical case where K is imaginary quadratic and the class field theory goes under the name of *complex multiplication*, ideles have proved to be a most convenient tool even in a computational setting [Gee and Stevenhagen 1998].

For every prime $\mathfrak{p}$, the local unit group $U_\mathfrak{p} = \{x_\mathfrak{p} \in K_\mathfrak{p}^* : |x_\mathfrak{p}|_\mathfrak{p} = 1\}$ is a maximal compact subgroup of $K_\mathfrak{p}^*$. It is equal to $O_\mathfrak{p}^*$ if $\mathfrak{p}$ is finite, and to the group $\{z : |z| = 1\}$ in $\mathbb{R}^*$ or $\mathbb{C}^*$ if $\mathfrak{p}$ is infinite and $K_\mathfrak{p}$ is isomorphic to $\mathbb{R}$ or $\mathbb{C}$. The subgroup $U_K = \prod_\mathfrak{p} U_\mathfrak{p}$ is a maximal compact subgroup of $\mathbf{A}_K^*$ that intersects K^* in the group μ_K of roots of unity of K. It is the kernel of the

surjective homomorphism

$$\begin{aligned} \mathbf{A}_K^* &\xrightarrow{\delta} \mathrm{Div}_K = \bigoplus\nolimits_{\mathfrak{p}<\infty} \mathbb{Z} \times \bigoplus\nolimits_{\mathfrak{p}\,|\,\infty} \mathbb{R} \\ (x_\mathfrak{p})_\mathfrak{p} &\longmapsto ((\mathrm{ord}_\mathfrak{p}(x_\mathfrak{p}))_\mathfrak{p}, (-\log|x_\mathfrak{p}|)_\mathfrak{p}) \end{aligned}$$

to the *Arakelov divisor group* Div_K of K. The elements of Div_K are usually represented as finite formal sums $D = \sum_\mathfrak{p} n_\mathfrak{p}\mathfrak{p}$, with $n_\mathfrak{p} \in \mathbb{Z}$ if $\mathfrak{p}$ is finite and $n_\mathfrak{p} \in \mathbb{R}$ if $\mathfrak{p}$ is infinite. One can think of Div_K as a 'completion' of the group $\mathcal{J}(\mathbb{O}_K) = \bigoplus_{\mathfrak{p}<\infty} \mathbb{Z}$ of finite divisors from Theorem 5.7 by $\bigoplus_{\mathfrak{p}\,|\,\infty} \mathbb{R} = \mathbb{R}^{r+s}$, the group of infinite divisors occurring in (10-8). In these terms, every $x \in K^*$ gives rise to a *principal* Arakelov divisor $\delta(x) = (x\mathbb{O}_K, -L'(x)) \in \mathrm{Div}_K$, with L' the homomorphic extension to K^* of the logarithmic map $L' : R^* \to \mathbb{R}^{r+s}$ from the proof of the Dirichlet unit theorem (Theorem 10.7). The quotient Pic_K of Div_K modulo its subgroup of principal divisors fits in an exact sequence

$$1 \to \mu_K \longrightarrow K^* \xrightarrow{\delta} \mathrm{Div}_K \longrightarrow \mathrm{Pic}_K \to 1$$

that is analogous to (4-1), and much closer to the definition of the Picard group of a *complete* algebraic curve.

Just as for functions on an algebraic curve, we define a *degree map* $\deg : \mathbf{A}_K^* \to \mathbb{R}$ in terms of the norm (14-2) by $\deg(x) = -\log\|x\|$. As ideles in U_K and principal ideles have degree 0, this gives rise to a homomorphism $\deg : \mathrm{Pic}_K \to \mathbb{R}$. Its kernel Pic_K^0 is the *Arakelov class group* of K that occurs center stage in [Schoof 2008b]. As in [Proposition 2.2] there, it is an extension

$$0 \to H/L'[\mathbb{O}_K^*] \to \mathrm{Pic}_K^0 \to \mathrm{Cl}_K \to 0 \tag{14-3}$$

of the ordinary class group Cl_K of K by the 'unit torus' obtained by taking the trace-zero-hyperplane $H \subset \mathbb{R}^{r+s}$ from (10-8) modulo the unit lattice $L'[\mathbb{O}_K^*]$ of covolume the regulator R_K of K. The algorithm in Section 12 for computing class groups and unit groups in K can be viewed as an algorithm for computing the Arakelov class group Pic_K^0, and it is in these terms that a proper analysis of the algorithm can be given; see [Lenstra 1992, Section 6] and [Schoof 2008b, Section 12].

By (14-3), the compactness of the Arakelov class group Pic_K^0 is tantamount to the finiteness of Cl_K and the compactness of $H/L'[\mathbb{O}_K^*]$ expressed by the Dirichlet unit theorem (Theorem 10.7). As Pic_K^0 is the quotient of the group $C_K^1 = \ker[\deg : C_K \to \mathbb{R}]$ of idele classes of norm 1 (and degree zero) by the compact group U_K, the compactness of Pic_K^0 implies the compactness of C_K^1. One can also go in the reverse direction, prove the compactness of C_K^1 directly as in [Cassels and Fröhlich 1967, Section II.16], and derive from this the finiteness results of Corollary 10.6 and Theorem 10.7.

15. Galois theory

Let K be a number field that is Galois over $\mathbb{Q}$ with group $G = \mathrm{Gal}(K/\mathbb{Q})$. Then G acts on every object that is 'intrinsically defined' in terms of K. Examples of such objects are the ring of integers $\mathbb{O}_K$, its unit group $\mathbb{O}_K^*$, and its class group Cl_K, and in each of these examples the natural problem of determining their *Galois module structure* over $\mathbb{Z}[G]$ was and is an area of active research [Fröhlich 1983; Weiss 1996].

A number ring with field of fractions K does not necessarily have an action of G, but the number ring R generated by all G-conjugates of the original ring is a *Galois number ring* that does. For an order $\mathbb{Z}[\alpha]$, this amounts to passing to the 'Galois order' R generated by *all* roots of $f = f_{\mathbb{Q}}^{\alpha}$. The invariant ring

$$R^G = \{x \in R : \sigma(x) = x \text{ for all } \sigma \in G\} = R \cap \mathbb{Q}$$

is equal to $\mathbb{Z}$ for such an order, and the fundamental observation that we have a *transitive* G-action on the primes of R extending a given rational prime is true in great generality.

LEMMA 15.1. *Let A be a commutative ring and $G \subset \mathrm{End}(A)$ a finite group of automorphisms. If $\varphi, \psi : A \to k$ are homomorphisms to a domain k that coincide on the invariant ring A^G, then φ equals $\psi \circ \sigma$ for some $\sigma \in G$.*

PROOF. Extend φ and ψ coefficientwise to homomorphisms $\varphi, \psi : A[X] \to k[X]$. An element $a \in A$ is a zero of the polynomial $f = \prod_{\sigma \in G}(X - \sigma a) \in A^G[X]$ on which φ and ψ coincide, so $\varphi(a)$ is a zero of $\varphi(f) = \psi(f) = \prod_{\sigma \in G}(X - \psi\sigma a) \in k[X]$, and we have $\varphi(a) = (\psi\sigma)(a)$ for some $\sigma \in G$ since k is a domain. Now σ depends on a, but our argument shows that the union over $\sigma \in G$ of

$$A_\sigma = \{a \in A : \varphi(a) = (\psi\sigma)(a)\}$$

equals A. To show that we have $A = A_\sigma$ for some σ, as stated by the lemma, we repeat the previous argument starting with the maps $\varphi, \psi : A[X] \to k[X]$ to obtain

$$A[X] = \bigcup_{\sigma \in G}(A[X])_\sigma = \bigcup_{\sigma \in G} A_\sigma[X].$$

If $a_\sigma \in A \setminus A_\sigma$ exists for all $\sigma \in G$, all polynomials $\sum_{\sigma \in G} a_\sigma X^{n_\sigma}$ that are sums of monomials of *different* degrees n_σ are in $A[X]$ but not in $A_\sigma[X]$ for any $\sigma \in G$. □

The primes over p in a Galois number ring R are kernels of homomorphisms $R \to k$, with $k = \overline{\mathbb{F}}_p$ an algebraic closure of $\mathbb{F}_p$, and they extend the homomorphism $R^G = \mathbb{Z} \to \mathbb{F}_p$. By Lemma 15.1, they are transitively permuted by the Galois group. As a consequence, the residue class degree $f_p = f(\mathfrak{p}/p)$ for a prime $\mathfrak{p} \mid p$ does not depend on the choice of the extension prime $\mathfrak{p}$ in R. If

R is regular above p, the same is true for the ramification index $e_p = e(\mathfrak{p}/p)$, and, with g_p the number of primes in R lying over p, Theorem 8.4 for Galois number rings becomes

$$e_p f_p g_p = [K : \mathbb{Q}]. \tag{15-2}$$

Identity (15-2) is actually an identity for the primes over p in a Galois number field K. It also holds for the infinite prime $p = \infty$ of $\mathbb{Q}$, as does Theorem 8.4, if we set $f_\infty = 1$ and $e_\infty = [K_\mathfrak{p} : \mathbb{R}] \in \{1, 2\}$.

EXAMPLE 15.3. Let $f = X^3 + 44$ be as in Example 8.3, and $K = \mathbb{Q}(\zeta_3, \sqrt[3]{44})$ a splitting field of f over $\mathbb{Q}$. Then K is Galois over $\mathbb{Q}$ with nonabelian Galois group of order 6. The prime 3 ramifies in the quadratic subfield $\mathbb{Q}(\zeta_3) = \mathbb{Q}(\sqrt{-3})$, so the primes in K over 3 have even ramification index e_3. As 3 has two extensions in $\mathbb{Q}(\sqrt[3]{44})$ by Example 8.3, we have $g_3 \geq 2$. From $e_3 f_3 g_3 = 6$ we find $e_3 = 2$, $f_3 = 1$, and $g_3 = 3$. This shows without any explicit computation that the primes occurring in the factorization $(3) = \mathfrak{p}_3^2 \mathfrak{q}_3$ in $\mathbb{Q}(\sqrt[3]{44})$ factor in the quadratic extension K of $\mathbb{Q}(\sqrt[3]{44})$ as $\mathfrak{p}_3 \mathcal{O}_K = \mathfrak{P}_3 \mathfrak{P}_3'$ and $\mathfrak{q}_3 \mathcal{O}_K = \mathfrak{Q}_3^2$. A similar argument leads to the same values of e, f, and g for describing the 'ramification' of the infinite prime $p = \infty$.

The prime 5 is inert in $\mathbb{Q}(\zeta_3)$ and splits as $(5) = \mathfrak{p}_5 \mathfrak{p}_{25}$ in $\mathbb{Q}(\sqrt[3]{44})$. For this prime, f_5 is even and g_5 is at least 2, so we have $e_5 = 1$, $f_5 = 2$, and $g_5 = 3$. We conclude that $\mathfrak{p}_5$ is inert in $\mathbb{Q}(\sqrt[3]{44}) \subset K$, giving rise to a prime $\mathfrak{P}_{25}$ of norm 25, and that $\mathfrak{p}_{25}$ splits into two primes $\mathfrak{Q}_{25}$ and $\mathfrak{R}_{25}$ of norm 25 each.

Let K be Galois over $\mathbb{Q}$, and $\mathfrak{p} \mid p$ a prime of K. Then the stabilizer

$$G_\mathfrak{p} = \{\sigma \in G : \sigma \mathfrak{p} = \mathfrak{p}\} \subset G$$

of $\mathfrak{p}$ is the *decomposition group* of $\mathfrak{p}$. It is the subgroup of automorphisms in G that leave the $\mathfrak{p}$-adic absolute value on K invariant, and it may be identified with the Galois group $\mathrm{Gal}(K_\mathfrak{p}/\mathbb{Q}_p)$ of the $\mathfrak{p}$-adic completion over $\mathbb{Q}_p$. For $p = \infty$, read $\mathbb{Q}_\infty = \mathbb{R}$.

As G acts transitively on the primes over p, all decomposition groups of primes over p are conjugate in G. The G-set $G/G_\mathfrak{p}$ of left cosets of $G_\mathfrak{p}$ in G may be identified with the set of extensions of p to K. As $G/G_\mathfrak{p}$ has cardinality g_p, the order of $G_\mathfrak{p}$ equals $e_p f_p$ by (15-2).

For finite primes, the decomposition group $G_\mathfrak{p}$ acts naturally as a group of automorphisms on the residue class field extension $\mathbb{F}_p \subset k_\mathfrak{p} = \mathcal{O}_K/\mathfrak{p}$, which is cyclic of degree f_p and has a canonical generator of its Galois group in the *Frobenius automorphism* $\mathrm{Frob}_\mathfrak{p} : x \mapsto x^p$ on $k_\mathfrak{p}$.

LEMMA 15.4. *For every prime $\mathfrak{p} \mid p$ in K, there exists $\sigma_\mathfrak{p} \in \mathrm{Gal}(K/\mathbb{Q})$ inducing the Frobenius automorphism $\mathrm{Frob}_\mathfrak{p}$ on $k_\mathfrak{p}$.*

PROOF. Applying Lemma 15.1 with $\psi : \mathbb{O}_K \to k_\mathfrak{p}$ the reduction map and $\varphi = \mathrm{Frob}_\mathfrak{p} \circ \psi$, we find that there exists $\sigma_\mathfrak{p} \in G$ that induces $\mathrm{Frob}_\mathfrak{p}$. □

Denoting the kernel of reduction modulo $\mathfrak{p}$ in $G_\mathfrak{p}$ by $I_\mathfrak{p}$, we obtain an exact sequence

$$1 \longrightarrow I_\mathfrak{p} \longrightarrow G_\mathfrak{p} \longrightarrow \mathrm{Gal}(k_\mathfrak{p}/\mathbb{F}_p) \longrightarrow 1. \tag{15-5}$$

The *inertia group* $I_\mathfrak{p}$ is a normal subgroup of $G_\mathfrak{p}$ of order e_p. Its invariant field $K^{I_\mathfrak{p}}$ is the largest subfield of K on which the $\mathfrak{p}$-adic valuation is an *unramified* prime over p. The invariant subfield $K^{G_\mathfrak{p}}$ of the decomposition group itself is the largest subfield of K for which the completion under the $\mathfrak{p}$-adic valuation is equal to $\mathbb{Q}_p$. For infinite primes $\mathfrak{p}$, we use the convention $I_\mathfrak{p} = G_\mathfrak{p}$ to make this correct.

EXAMPLE 15.6. Take $K = \mathbb{Q}(\zeta_3, \sqrt[3]{44})$ as in Example 15.3. The primes 2 and 11 are unramified and inert in $\mathbb{Q} \subset \mathbb{Q}(\zeta_3)$, with extensions that are totally ramified in $K/\mathbb{Q}(\zeta_3)$. Their decomposition groups are equal to G itself, and their inertia groups are equal to the normal subgroup of index 2 in $G \cong S_3$.

The decomposition groups at the three primes over 3 in G are the three subgroups of order 2. Note that these are conjugate subgroups, and that $G_{\mathfrak{Q}_3} = I_{\mathfrak{Q}_3}$ is the subgroup with invariant field $\mathbb{Q}(\sqrt[3]{44})$. For the three unramified primes over 5, we have the same three decomposition groups of order 2, and $G_{\mathfrak{P}_{25}}$ is the one with invariant field $\mathbb{Q}(\sqrt[3]{44})$.

The prime 7 splits in $\mathbb{Q}(\zeta_3)$ into two primes that remain inert in $K/\mathbb{Q}(\zeta_3)$. Their decomposition group is the normal subgroup of order 3 in G. The decomposition groups of the six extension primes of the totally splitting prime 13 are trivial.

For unramified primes $\mathfrak{p}$, the decomposition group $G_\mathfrak{p} \cong \mathrm{Gal}(k_\mathfrak{p}/\mathbb{F}_p)$ in (15-5) is cyclic of order f_p with *canonical* generator $\sigma_\mathfrak{p}$, the *Frobenius at* $\mathfrak{p}$ in G. The elements $\mathrm{Frob}_\mathfrak{p} \in G$ for the primes $\mathfrak{p} \mid p$ form a conjugacy class $C_p \subset G$ in case p is unramified in K. In the case of Example 15.6, the three conjugacy classes of $G \cong S_3$ are realized by the smallest unramified primes 5, 7, and 13. It is even true that every conjugacy class occurs as the *Frobenius class* for infinitely many p, in the following precise sense.

THEOREM 15.7 (CHEBOTAREV DENSITY THEOREM). *Let $\mathbb{Q} \subset K$ be Galois with group G and $C \subset G$ a conjugacy class. Then the set of rational primes p that are unramified in K and have C as their Frobenius class is infinite and has natural density $\#C/\#G$ in the set of all primes.*

EXAMPLE 15.8. In the case of the degree 6 field K from Example 15.6, the totally splitting primes p having 'trivial' Frobenius class $C_p = \{\mathrm{id}\} \subset G$ form a set of density $1/6$, whereas the unramified primes $p \equiv 2 \bmod 3$ having the

three elements of order 2 in G in their Frobenius class form, as expected, a set of density $1/2$. The primes p modulo which X^3+44 is irreducible have the two elements of order 3 in G in their Frobenius class and form a set of density $1/3$.

The cyclotomic field $\mathbb{Q}(\zeta_n)$ is abelian over $\mathbb{Q}$ with Galois group

$$\begin{aligned} &\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \cong (\mathbb{Z}/n\mathbb{Z})^* \\ &(\sigma_a : \zeta_n \mapsto \zeta_n^a) \leftrightarrow (a \bmod n). \end{aligned} \tag{15-9}$$

Here $\{\sigma_p\}$ is the Frobenius class of p, and Theorem 15.7 reduces to Dirichlet's theorem on primes in arithmetic progressions: the primes $p \nmid n$ are equidistributed over $(\mathbb{Z}/n\mathbb{Z})^*$. Chebotarev's original proof (1924) of Theorem 15.7 reduces the general case by a clever trick (see [Stevenhagen and Lenstra 1996, Appendix]) to the cyclotomic case, and forms a key ingredient in the proof of *Artin's reciprocity law* in class field theory [Cohen and Stevenhagen 2008], a far reaching generalization of Example 15.8 to arbitrary abelian extensions of number fields. Assuming class field theory, there are shorter proofs [Lang 1994, Theorem VIII.4.10] of Theorem 15.7.

If K is not Galois over $\mathbb{Q}$, the absolute Galois group $G_{\mathbb{Q}} = \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ of $\mathbb{Q}$ acts not on K itself but on its *fundamental set* $X_K = \mathrm{Hom}(K, \overline{\mathbb{Q}})$ of embeddings of K in $\overline{\mathbb{Q}}$. Choosing $\overline{\mathbb{Q}}$ as a subfield of $\mathbb{C}$, the elements of X_K are the n embeddings $\sigma : K \to \mathbb{C}$ considered in Section 10. The images $\sigma[K] \subset \overline{\mathbb{Q}}$ for $\sigma \in X_K$ generate the *normal closure* L of K in $\overline{\mathbb{Q}}$, which is Galois over $\mathbb{Q}$. The natural left action of $G_{\mathbb{Q}}$ on X_K by composition factors via the finite quotient $\mathrm{Gal}(L/\mathbb{Q})$. Writing $K = \mathbb{Q}(\alpha)$, one may, more classically, identify X_K with the $G_{\mathbb{Q}}$-set of roots of $f_{\mathbb{Q}}^{\alpha}$ in $\overline{\mathbb{Q}}$ under $\sigma \mapsto \sigma(a)$, and view L as the splitting field over $\mathbb{Q}$ of the polynomial $f_{\mathbb{Q}}^{\alpha}$. The splitting of a prime p in K can be described in terms of the Galois action on X_K of the decomposition and inertia groups $G_{\mathfrak{P}}$ and $I_{\mathfrak{P}}$ in $\mathrm{Gal}(L/\mathbb{Q})$ of a prime $\mathfrak{P} \mid p$ in L.

THEOREM 15.10. *Let K be a number field with fundamental set X_K and normal closure L over $\mathbb{Q}$. Given a prime p and integers $e_i, f_i > 0$ for $i = 1, 2, \ldots, t$ with $\sum_{i=1}^{t} e_i f_i = [K : \mathbb{Q}]$, the following are equivalent*:

(1) *there are t different primes $\mathfrak{p}_1, \mathfrak{p}_2, \ldots, \mathfrak{p}_t$ over p in K having $e(\mathfrak{p}_i/p) = e_i$ and $f(\mathfrak{p}_i/p) = f_i$;*
(2) *for any prime $\mathfrak{P}$ over p in L, there are t different $G_{\mathfrak{P}}$-orbits $X_i \subset X_K$ of length $\#X_i = e_i f_i$; under the action of $I_{\mathfrak{P}}$ on X_i, there are f_i orbits of length e_i.*

We will merely sketch the proof, stressing once more the analogy between finite and infinite primes. For the infinite prime $p = \infty$, we embed $\overline{\mathbb{Q}}$ in the algebraic closure $\mathbb{C}$ of the completion $\mathbb{R}$ of $\mathbb{Q}$ at p to view X_K as the set of embeddings

of K in $\mathbb{C}$. Then the absolute Galois group $G_{\mathbb{R}} = \mathrm{Gal}(\mathbb{C}/\mathbb{R})$ of $\mathbb{R}$ acts on X_K, and embeddings in $\mathbb{C}$ give rise to the same infinite prime on K if and only if they are complex conjugate, as in Section 10, and we see that the $G_{\mathbb{R}}$-orbits of X_K of length 1 and 2 correspond to the real and complex primes of K.

For finite p, we embed $\overline{\mathbb{Q}}$ in an algebraic closure $\overline{\mathbb{Q}}_p$ of $\mathbb{Q}_p$, to which the p-adic absolute value extends uniquely [Weiss 1963, Corollary 2-2-11], and we have $G_{\mathbb{Q}_p} = \mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$ act on X_K. Again, two embeddings of K in $\overline{\mathbb{Q}}_p$ give rise to the same $\mathfrak{p}$-adic value on K if and only if they are in the same $G_{\mathbb{Q}_p}$-orbit, and the length of such an orbit is

$$\mathrm{Hom}_{\mathbb{Q}_p}(K_{\mathfrak{p}}, \overline{\mathbb{Q}}_p) = [K_{\mathfrak{p}} : \mathbb{Q}_p] = e(\mathfrak{p}_i/p)\, f(\mathfrak{p}_i/p).$$

A concrete application of Theorem 15.10 is the following classical method to obtain $\mathrm{Gal}(L/\mathbb{Q})$ for the normal closure L of a field $K = \mathbb{Q}(\alpha)$ generated by the root α of a monic irreducible polynomial $f \in \mathbb{Z}[X]$.

COROLLARY 15.11. *Let f, K and L be as above. Then the following are equivalent*:

(1) *there exists a prime p for which $f \bmod p$ factors as a product of t distinct irreducible factors of degrees $d_1, d_2, \ldots, d_t$.*
(2) $\mathrm{Gal}(L/\mathbb{Q})$, *viewed as a permutation group on X_K, contains a permutation that is the product of t disjoint cycles of lengths $d_1, d_2, \ldots, d_t$.*

PROOF. For a prime as in (1), apply the Kummer–Dedekind theorem (Theorem 8.2) to the number ring $\mathbb{Z}[\alpha] = \mathbb{Z}[X]/(f)$ to deduce that the primes over p in $K = \mathbb{Q}(\alpha)$ are unramified with residue class degrees $d_1, d_2, \ldots, d_t$. The Frobenius of such a prime, which generates the decomposition group, will act on X_K as a product of t disjoint cycles of lengths $d_1, d_2, \ldots, d_t$, as these are the orbit lengths under the action of Frobenius by Theorem 15.10. Conversely, every element of $\mathrm{Gal}(L/\mathbb{Q})$ is the Frobenius of some prime over $p \nmid \Delta(f)$ by Theorem 15.7, so all cycle types can be obtained from the factorization of $f \bmod p$ for a suitable prime p in 1. □

EXAMPLES 15.12. An irreducible cubic polynomial $f \in \mathbb{Z}[X]$ has S_3 as the Galois group of its splitting field if and only if it splits as a product of a linear and an irreducible quadratic factor modulo some prime p.

For the quartic polynomial $f = X^4 - 2X^2 + 3X - 7$ from Example 12.4, we noticed that it was irreducible modulo 2 and 3, and had exactly two zeros modulo 5. The Galois group of its splitting field is therefore a subgroup of S_4 containing a 4-cycle and a 2-cycle. As the value $f(-4) = 5 \cdot 41$ is the only root of f modulo 41, the factorization modulo 41 shows that the Galois group contains a 3-cycle as well, and is therefore equal to the full symmetric group S_4.

More generally, one can show that the Galois group $\mathrm{Gal}(f)$ over $\mathbb{Q}$ of the splitting field of *any* polynomial $f \in \mathbb{Z}[X]$ of squarefree discriminant is the full symmetric group. This is because a prime p that divides $\Delta(f)$ only once has a unique ramified extension $\mathfrak{p}$ to $K = \mathbb{Q}[X]/(f)$, with $e(\mathfrak{p}/p) = 2$. By Theorem 15.10, we deduce that all non-trivial inertia groups in $\mathrm{Gal}(f)$ are generated by a single 2-cycle in their action on the fundamental set X_K. Now the Galois group of a number field over $\mathbb{Q}$ is generated by its inertia groups, as every proper extension of $\mathbb{Q}$ ramifies at some finite prime. We can then apply the group theoretical fact that $\mathrm{Gal}(f)$, as a transitive subgroup of the symmetric group that is generated by transpositions, is equal to the full symmetric group.

EXAMPLE 15.13. From Theorem 15.7 and Corollary 15.11, it follows that the *factorization type* of an irreducible polynomial $f \in \mathbb{Z}[X]$ modulo rational primes p occurs with a frequency that depends on the group $\mathrm{Gal}(f)$ of its splitting field over $\mathbb{Q}$. We illustrate this for the quartic polynomial $f = X^4 - 2X^2 + 3X - 7$ from Example 12.4, which has group S_4.

X	# primes	4	1-3	2-2	1-1-2	1-1-1-1
10^3	194	.27976	.35714	.10119	.23810	.02381
10^4	1229	.26688	.34255	.11391	.23759	.03905
10^5	9592	.25378	.33208	.12407	.24617	.04390
10^6	78498	.25063	.33377	.12448	.25048	.04064
10^7	664579	.24962	.33366	.12517	.25003	.04152
∞	∞	.25000	.33333	.12500	.25000	.04167

There are five (separable) factorization types of polynomials of degree 4, just like there are five cycle types in S_4. They correspond to the partitions of 4. In the table above, we have counted the fractions of the primes up to some bound X yielding a given factorization type. For increasing X, the fractions tend to the limit fractions $\frac{1}{4}$, $\frac{1}{3}$, $\frac{1}{8}$, $\frac{1}{4}$ and $\frac{1}{24}$ in the bottom line that come from the five conjugacy classes in $\mathrm{Gal}(f) \cong S_4$. In fact, the general density result for 'factorization types' of a polynomial in $\mathbb{Z}[X]$ modulo primes is a weak version of Theorem 15.7 that is due to Frobenius, and Theorem 15.7 can be seen as a common generalization of this result and Dirichlet's theorem on primes in arithmetic progressions.

Acknowledgments

Useful comments on earlier versions of this paper were provided by Reinier Bröker, Joe Buhler, Capi Corrales, Eduardo Friedman, René Schoof and William Stein.

References

[Atiyah and Macdonald 1969] M. F. Atiyah and I. G. Macdonald, *Introduction to commutative algebra*, Addison-Wesley, MA–London–Don Mills, Ont., 1969.

[Bach 1990] E. Bach, "Explicit bounds for primality testing and related problems", *Math. Comp.* **55**:191 (1990), 355–380.

[Bhargava 2005] M. Bhargava, "The density of discriminants of quartic rings and fields", *Ann. of Math.* (2) **162**:2 (2005), 1031–1063.

[Bhargava $\geq$ 2008] M. Bhargava, "The density of discriminants of quintic rings and fields", *Ann. of Math.* (2). To appear.

[Bourbaki 1989] N. Bourbaki, *Algebra. I. Chapters 1–3*, Elements of Mathematics (Berlin), Springer, Berlin, 1989.

[Buchmann and Lenstra 1994] J. A. Buchmann and H. W. Lenstra, Jr., "Approximating rings of integers in number fields", *J. Théor. Nombres Bordeaux* **6**:2 (1994), 221–260.

[Buchmann and Williams 1989] J. Buchmann and H. C. Williams, "On the computation of the class number of an algebraic number field", *Math. Comp.* **53**:188 (1989), 679–688.

[Buhler and Wagon 2008] J. P. Buhler and S. Wagon, "Basic algorithms in number theory", pp. 25–68 in *Surveys in algorithmic number theory*, edited by J. P. Buhler and P. Stevenhagen, Math. Sci. Res. Inst. Publ. **44**, Cambridge University Press, New York, 2008.

[Cassels and Fröhlich 1967] J. W. S. Cassels and A. Fröhlich (editors), *Algebraic number theory: Proceedings of an instructional conference* (Brighton, 1965), Academic Press, London, 1967.

[Cohen 1993] H. Cohen, *A course in computational algebraic number theory*, Graduate Texts in Mathematics **138**, Springer, Berlin, 1993.

[Cohen and Stevenhagen 2008] H. Cohen and P. Stevenhagen, "Computational class field theory", pp. 497–534 in *Surveys in algorithmic number theory*, edited by J. P. Buhler and P. Stevenhagen, Math. Sci. Res. Inst. Publ. **44**, Cambridge University Press, New York, 2008.

[Cornell and Silverman 1986] G. Cornell and J. H. Silverman (editors), *Arithmetic geometry* (Storrs, CT, 1984), Springer, New York, 1986.

[Eisenbud and Harris 2000] D. Eisenbud and J. Harris, *The geometry of schemes*, Graduate Texts in Mathematics **197**, Springer, New York, 2000.

[Friedman 1989] E. Friedman, "Analytic formulas for the regulator of a number field", *Invent. Math.* **98**:3 (1989), 599–622.

[Fröhlich 1983] A. Fröhlich, *Galois module structure of algebraic integers*, vol. 1, Ergebnisse der Mathematik und ihrer Grenzgebiete (3), Springer, Berlin, 1983.

[Gee and Stevenhagen 1998] A. Gee and P. Stevenhagen, "Generating class fields using Shimura reciprocity", pp. 441–453 in *Algorithmic number theory* (Portland, OR,

1998), edited by J. P. Buhler, Lecture Notes in Comput. Sci. **1423**, Springer, Berlin, 1998.

[Gouvêa 1993] F. Q. Gouvêa, *p-adic numbers: An introduction*, Universitext, Springer, Berlin, 1993.

[Hartshorne 1977] R. Hartshorne, *Algebraic geometry*, Graduate Texts in Mathematics **52**, Springer, New York, 1977.

[Koblitz 1984] N. Koblitz, *p-adic numbers, p-adic analysis, and zeta-functions*, 2nd ed., Graduate Texts in Mathematics **58**, Springer, New York, 1984.

[Lang 1994] S. Lang, *Algebraic number theory*, 2nd ed., Graduate Texts in Mathematics **110**, Springer, New York, 1994.

[Lang 2002] S. Lang, *Algebra*, 3rd ed., Graduate Texts in Mathematics **211**, Springer, New York, 2002.

[Lenstra 1992] H. W. Lenstra, Jr., "Algorithms in algebraic number theory", *Bull. Amer. Math. Soc.* (*N.S.*) **26**:2 (1992), 211–244.

[Lenstra 2008] H. W. Lenstra, Jr., "Solving the Pell equation", pp. 1–23 in *Surveys in algorithmic number theory*, edited by J. P. Buhler and P. Stevenhagen, Math. Sci. Res. Inst. Publ. **44**, Cambridge University Press, New York, 2008.

[Mihăilescu 2006] P. Mihăilescu, "On the class groups of cyclotomic extensions in presence of a solution to Catalan's equation", *J. Number Theory* **118**:1 (2006), 123–144.

[Pomerance 2008a] C. Pomerance, "Elementary thoughts on discrete logarithms", pp. 385–396 in *Surveys in algorithmic number theory*, edited by J. P. Buhler and P. Stevenhagen, Math. Sci. Res. Inst. Publ. **44**, Cambridge University Press, New York, 2008.

[Pomerance 2008b] C. Pomerance, "Smooth numbers and the quadratic sieve", pp. 69–81 in *Surveys in algorithmic number theory*, edited by J. P. Buhler and P. Stevenhagen, Math. Sci. Res. Inst. Publ. **44**, Cambridge University Press, New York, 2008.

[Ramakrishnan and Valenza 1999] D. Ramakrishnan and R. J. Valenza, *Fourier analysis on number fields*, Graduate Texts in Mathematics **186**, Springer, New York, 1999.

[Rosen 2002] M. Rosen, *Number theory in function fields*, Graduate Texts in Mathematics **210**, Springer, New York, 2002.

[Schirokauer 2008] O. Schirokauer, "The impact of the number field sieve on the discrete logarithm problem in finite fields", pp. 397–420 in *Surveys in algorithmic number theory*, edited by J. P. Buhler and P. Stevenhagen, Math. Sci. Res. Inst. Publ. **44**, Cambridge University Press, New York, 2008.

[Schoof 2008a] R. Schoof, *Catalan's Conjecture*, Springer, New York, 2008.

[Schoof 2008b] R. J. Schoof, "Computing Arakelov class groups", pp. 447–495 in *Surveys in algorithmic number theory*, edited by J. P. Buhler and P. Stevenhagen, Math. Sci. Res. Inst. Publ. **44**, Cambridge University Press, New York, 2008.

[Schoof 2008c] R. J. Schoof, "Four primality testing algorithms", pp. 101–125 in *Surveys in algorithmic number theory*, edited by J. P. Buhler and P. Stevenhagen, Math. Sci. Res. Inst. Publ. **44**, Cambridge University Press, New York, 2008.

[Seysen 1987] M. Seysen, "A probabilistic factorization algorithm with quadratic forms of negative discriminant", *Math. Comp.* **48**:178 (1987), 757–780.

[Skoruppa 1993] N.-P. Skoruppa, "Quick lower bounds for regulators of number fields", *Enseign. Math.* (2) **39**:1-2 (1993), 137–141.

[Stevenhagen 2008] P. Stevenhagen, "The number field sieve", pp. 83–100 in *Surveys in algorithmic number theory*, edited by J. P. Buhler and P. Stevenhagen, Math. Sci. Res. Inst. Publ. **44**, Cambridge University Press, New York, 2008.

[Stevenhagen and Lenstra 1996] P. Stevenhagen and H. W. Lenstra, Jr., "Chebotarëv and his density theorem", *Math. Intelligencer* **18**:2 (1996), 26–37.

[Tate 1984] J. Tate, *Les conjectures de Stark sur les fonctions L d'Artin en s* $= 0$, Progress in Mathematics **47**, Birkhäuser, Boston, 1984.

[Washington 1997] L. C. Washington, *Introduction to cyclotomic fields*, 2nd ed., Graduate Texts in Mathematics **83**, Springer, New York, 1997.

[Weiss 1963] E. Weiss, *Algebraic number theory*, McGraw-Hill, New York, 1963.

[Weiss 1996] A. Weiss, *Multiplicative Galois module structure*, Fields Institute Monographs **5**, American Mathematical Society, Providence, RI, 1996.

PETER STEVENHAGEN
MATHEMATISCH INSTITUUT
UNIVERSITEIT LEIDEN
POSTBUS 9512
2300 RA LEIDEN
THE NETHERLANDS
psh@math.leidenuniv.nl