NUMBER RINGS

P. Stevenhagen

Universiteit Leiden
2019

Date of this online version: November 14, 2020

Please send any comments on this text to psh@math.leidenuniv.nl.

Mail address of the author:

P. Stevenhagen
Mathematisch Instituut
Universiteit Leiden
Postbus 9512
2300 RA Leiden
Netherlands

CONTENTS

1 Introduction to number rings

A *number field* is a finite field extension of the field of rational numbers $\mathbf{Q}$, and a *number ring* is a subring of a number field. This introduction shows how number rings arise naturally when solving equations in ordinary integers.

Many basic questions about integers can be phrased as a problem of finding rational or integral solutions to equations in several indeterminates with rational coefficients. Starting for instance from the empirical observation that all small positive numbers can be written as the sum of at most 4 integral squares, one might guess that the equation $n = w^2+x^2+y^2+z^2$ admits integral solutions for all positive n. Similarly, the abundance of 'essentially different' integral solutions to the Pythagorean equation $a^2+b^2 = c^2$ makes one think that the equation $x^2 + y^2 = 1$, which describes the unit circle in the Euclidean plane, possesses infinitely many rational solutions. For higher exponents, a deep theorem of Wiles [28] confirms Fermat's belief that for $k > 2$, the curve $x^k + y^k = 1$ admits only the trivial rational solutions with $xy = 0$. All these equations, in which one restricts to integral or rational rather than real or complex solutions, are examples of *Diophantine equations*. They are named after Diophantus of Alexandria, who treated several of them in a work in 13 books called *Arithmetica* ($\pm$ 250 AD). Only six books have survived [14]. They have been a source of inspiration to later mathematicians such as Fermat (1601–1665) and Euler (1707–1783).

This introduction treats four classical examples of Diophantine equations. The reader who is interested in the history of these examples or the history of number theory in general should consult Weil's account [27] (for the period before 1800) or the appropriate chapters in [25, 13, 10].

▶ The Pell equation

We start with two special cases of a problem that was posed by Fermat as a challenge problem to the English mathematicians in 1657. It has become known as the *Pell equation* because of an erroneous attribution of its solution by Euler to the English mathematician John Pell (1611–1685).

1.1. Problem. *Find all integral solutions to the equation $x^2 - dy^2 = 1$ for $d = 3$ and for $d = 1141$.*

Problem 1.1 requires the determination of all integers y for which $1+dy^2$ is a square. If we do not know how to approach such a problem, there is always the possibility to try a few values of y and see whether we find solutions. Obviously, y gives a solution if and only if $-y$ does, so we may assume that y is non-negative. In case $d = 3$, it is not hard to see that the first few values of y for which $1 + 3y^2$ is a square are $y = 0$, 1, 4, and 15. Using a computer, one finds the next few values to be 56, 209, 780, 2911 and 10864. The corresponding non-negative x-values are $x = 1$, 2, 7, 26, 97, 362, 1351, 5042 and 18817.

A moment's reflection shows that the sequences of x and y-values that we obtained both satisfy the second order recurrence relation $s_n = 4s_{n-1} - s_{n-2}$. Provided that we are able to prove that we always obtain non-trivial solutions to our equation, we have experimentally found a way to generate infinitely many solutions. This leaves us with a statement to prove

and a completeness question: do we obtain *all* solutions by our procedure?

For $d = 1141$, we can try to follow the same procedure, but here something different happens: after the obvious value $y = 0$, we find no small values of y that yield a solution. Unlike Fermat's contemporaries, the modern reader can use a computer to look for a small solution. In this case a computer does not help: it will only tell us that there are no other solutions with $y < 10^6$ or $y < 10^{12}$. More computer time can only raise the exponent to 15 or 18, it will not change the situation. Of course, such a huge number is likely to convince us that there are no further solutions. It shouldn't:

$$1 + 1141 \cdot 30693385322765657197397208^2 = 1036782394157223963237125215^2$$

turns out to be the smallest solution.

At this point, it is clear that we need something more conceptual to approach the Pell equation. For any integer $d > 1$ that is not a square, the left hand side of the equation can be factored in the number ring $\mathbf{Z}[\sqrt{d}] = \{a + b\sqrt{d} : a, b \in \mathbf{Z}\}$. This is a subring of the real quadratic field $\mathbf{Q}(\sqrt{d})$. In $\mathbf{Z}[\sqrt{d}]$, the Pell equation takes the form

$$(x + y\sqrt{d})(x - y\sqrt{d}) = 1,$$

so every solution to the equation gives rise to a unit in the number ring $\mathbf{Z}[\sqrt{d}]$. The converse is almost true, as can be seen with the help of the norm function $N : \mathbf{Z}[\sqrt{d}] \to \mathbf{Z}$, which is defined by

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

We have $N(\alpha\beta) = N(\alpha)N(\beta)$ for $\alpha, \beta \in \mathbf{Z}[\sqrt{d}]$, so the norm gives rise to a homomorphism $N : \mathbf{Z}[\sqrt{d}]^* \to \{\pm 1\}$ on the unit groups. The solutions to Pell's equation correspond to the elements in the kernel of this homomorphism. Clearly, the kernel is a subgroup of index at most 2 in $\mathbf{Z}[\sqrt{d}]^*$.

Let us first consider the case $d = 3$. As $x^2 - 3y^2$ is never congruent to -1 mod 4 for $x, y \in \mathbf{Z}$, all units in $\mathbf{Z}[\sqrt{3}]$ have norm 1 and we conclude that the integral solutions to the equation $x^2 - 3y^2 = 1$ correspond bijectively to the units in the ring $\mathbf{Z}[\sqrt{3}]$. Apart from the 'trivial solutions' $(x, y) = (\pm 1, 0)$ corresponding to $\pm 1 \in \mathbf{Z}[\sqrt{3}]^*$, there is the small solution $(x, y) = (2, 1)$ corresponding to the unit $\varepsilon_3 = 2 + \sqrt{3}$. This unit has infinite order in $\mathbf{Z}[\sqrt{3}]^*$, and we obtain infinitely many solutions to our equation coming from the subgroup $\langle -1 \rangle \times \langle \varepsilon_3 \rangle \subset \mathbf{Z}[\sqrt{3}]^*$. One can show (cf. exercises 9–11) that $2 + \sqrt{3}$ is in fact a *fundamental unit* in $\mathbf{Z}[\sqrt{3}]$, meaning that -1 and $2 + \sqrt{3}$ generate the full group $\mathbf{Z}[\sqrt{3}]^*$. This implies that the complete set of integral solutions to the equation $x^2 - 3y^2 = 1$ is

$$\{(x_n, y_n) : n \in \mathbf{Z}\} \cup \{(-x_n, -y_n) : n \in \mathbf{Z}\},$$

where the numbers x_n and y_n are defined by $x_n + y_n\sqrt{3} = (2 + \sqrt{3})^n$. In this way, the number ring $\mathbf{Z}[\sqrt{3}]$ enables us to give a transparent description of the set of solutions of the Pell equation for $d = 3$.

Exercise 1. Show that $\{x_n\}_n$ and $\{y_n\}_n$ satisfy the second order recurrence $s_n = 4s_{n-1} - s_{n-2}$.

We now turn to the case $d = 1141 = 7 \cdot 163$. As before, we have to determine the unit group $\mathbf{Z}[\sqrt{1141}]^*$. Note that all units have norm 1, since $x^2 - 1141y^2$ is never congruent to -1 mod 7. As in the case of $\mathbf{Z}[\sqrt{3}]$, one shows that *if* there exists a unit in $\mathbf{Z}[\sqrt{1141}]$ different from ± 1, then there exists a fundamental unit ε_{1141} such that $\mathbf{Z}[\sqrt{1141}]^* = \langle -1 \rangle \times \langle \varepsilon_{1141} \rangle$. Once we have found the unit ε_{1141}, it is easy to describe the solutions of the equation $x^2 - 1141y^2 = 1$. Thus we are faced with the problem of finding ε_{1141}, if it exists. The *Dirichlet unit theorem* (theorem 5.13) implies that *every* real quadratic ring $\mathbf{Z}[\sqrt{d}]$ has a fundamental unit ε_d. This guarantees that our computer is bound to find a positive integer y for which $1 + 1141y^2$ is a square after a finite amount of time. However, one has to be extremely patient as the smallest solution given above shows that the fundamental unit equals

$$\varepsilon_{1141} = 1036782394157223963237125215 + 30693385322765657197397208\sqrt{1141}.$$

The situation can even be worse: for $d = 1000099$, the smallest number $y > 0$ giving a solution to the Pell equation has 1115 decimal digits.

Exercise 2. Making any reasonable hypothesis on computer equipment, show that no implementation of our simple trial and error method will ever find this solution.

Examples as those above make clear that we need better ways to solve the Pell equation if we want to do it in practice. Several approaches exist, and it will come as no surprise that quadratic irrationalities play an essential role in them. We will exhibit a solution, in example 7.1, by general methods for finding units, Using such algorithms, a modern computer can find a 1000-digit solution in less than a second.

► Gaussian integers

The second problem we will treat is very well known. It goes back to Fermat (1640), and the first solution known to us occurs in a 1749 letter of Euler to Goldbach.

1.2. Problem. *Determine which prime numbers can be written as the sum of two squares.*

Solution. By looking at $x^2 + y^2$ mod 4, it is easy to see that no prime $p \equiv 3$ mod 4 is a sum of two squares. The prime $2 = 1^2 + 1^2$ and the first few primes congruent to 1 mod 4 are sums of squares in an essentially unique way:

$$5 = 2^2 + 1^2 \qquad 13 = 3^2 + 2^2 \qquad 17 = 4^2 + 1^2 \qquad 29 = 5^2 + 2^2.$$

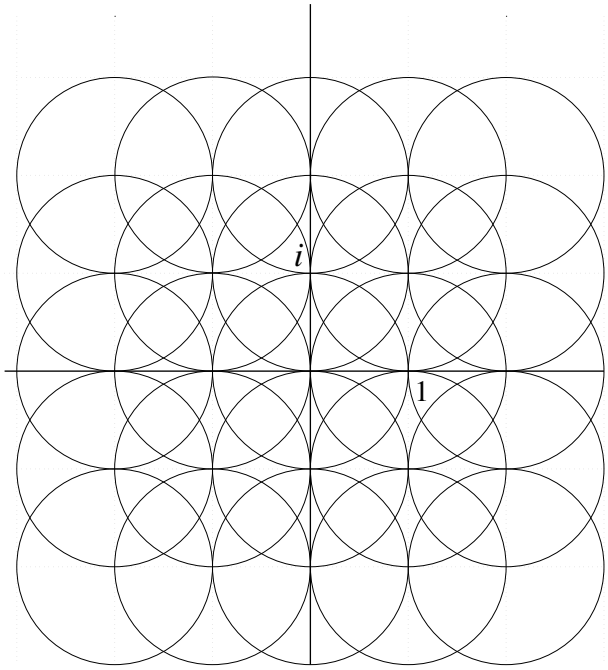
Proving that this is a general phenomenon is done most easily by regarding such identities as decompositions of prime numbers in the ring $\mathbf{Z}[i] = \mathbf{Z}[\sqrt{-1}]$ of *Gaussian integers*:

$$5 = (2+i)(2-i) \qquad 13 = (3+2i)(3-2i) \qquad 17 = (4+i)(4-i) \qquad 29 = (5+2i)(5-2i).$$

The number ring $\mathbf{Z}[i]$ is in many ways similar to the ring $\mathbf{Z}$ of ordinary integers. Just like in $\mathbf{Z}$, we have a Euclidean algorithm in $\mathbf{Z}[i]$. This means that, given any two elements $\alpha, \beta \in \mathbf{Z}[i]$ with $\beta \neq 0$, there exist elements $q, r \in \mathbf{Z}[i]$ such that $\alpha = q\beta + r$ holds and the (complex) absolute value $|r|$ of the remainder of the division is strictly smaller than $|\beta|$. Writing the identity above as

$$\alpha/\beta = q + r/\beta \qquad \text{with} \qquad |r/\beta| < 1,$$

we see that this amounts to saying that every element $\alpha/\beta \in \mathbf{Q}(i)$ can be approximated by a Gaussian integer $q \in \mathbf{Z}[i]$ in such a way that we have $|\alpha/\beta - q| < 1$. A picture shows that this is indeed the case: the open discs with radius 1 centered at the elements of $\mathbf{Z}[i]$ cover the entire complex plane.



Any integral domain admitting a Euclidean algorithm is a principal ideal domain and admits unique factorization.

Exercise 3. Check (or look up) these statements in case you have not seen them before.

Let now $p \equiv 1 \bmod 4$ be a prime number. Then -1 is the square of an element of order 4 in the cyclic group $\mathbf{F}_p^*$ of order $p-1$, so we can find an integer x for which p divides $x^2+1 = (x+i)(x-i)$. As it is clear that p divides neither $x+i$ nor $x-i$ in $\mathbf{Z}[i]$, we find that p is not a prime element in $\mathbf{Z}[i]$.

Exercise 4. Show that one can take $x = (\frac{p-1}{2})!$ in the argument above.

As in 1.1, we have a multiplicative norm $N : \mathbf{Z}[i] \to \mathbf{Z}$ that maps $a+bi$ to $(a+bi)(a-bi) = a^2+b^2$. As $a^2+b^2 = 1$ has only four integral solutions, the only units in $\mathbf{Z}[i]$ are the four powers of i.

As p is not prime in $\mathbf{Z}[i]$, there exist non-units $\pi, \pi' \in \mathbf{Z}[i]$ such that $p = \pi\pi'$. The identity $p^2 = N(p) = N(\pi)N(\pi')$ shows that π and π' both have norm p. Writing $\pi = x+yi$, we find $p = \pi\overline{\pi} = x^2+y^2$, as was to be shown. As π and $\overline{\pi} = \pi'$ are up to multiplication by powers of i the unique divisors of p, we even find that the squares in the representation $p = x^2+y^2$ are uniquely determined. As in the previous example, the introduction of a suitable number ring leads to a complete answer.

We give another application of the Gaussian integers. In geometric language, the problem to be solved deals with the integral points on a plane cubic curve.

1.3. Problem. *Find all integral solutions to the equation* $x^2 + 1 = y^3$.

Solution. If x is odd, then $x^2 + 1$ is never a cube as it is congruent to 2 mod 4. Suppose that (x, y) is a solution to our equation. We pass again to the number ring $\mathbf{Z}[i]$, where we have an equality

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

A prime element in $\mathbf{Z}[i]$ that divides both $x + i$ and $x - i$ divides their difference $2i$, so it is up to units equal to $1 + i$. However, $1 + i$ does not divide $x + i$ if x is even, so we conclude that $x + i$ and $x - i$ are coprime in $\mathbf{Z}[i]$. Their product is a cube, so unique factorization in $\mathbf{Z}[i]$ shows that each of them is the product of a unit and a cube in $\mathbf{Z}[i]$. As all units in $\mathbf{Z}[i]$ are cubes, there must be integers $a, b \in \mathbf{Z}$ such that $x + i = (a + bi)^3$. This yields the equations

$$x = a(a^2 - 3b^2) \qquad \text{and} \qquad 1 = (3a^2 - b^2)b.$$

It follows that we have $b = \pm 1$, and an inspection of both cases shows that the only solution is $(a, b) = (0, -1)$. This implies that the only solution to our original equation is $x = 0$, $y = 1$. In other words: a non-zero square is never followed by a cube. □

► Exploiting number rings

Slightly changing the cubic curve from the previous problem, we run into number rings different from $\mathbf{Z}[i]$.

1.4. Problem. *Find all integral solutions to the equation* $x^2 + 19 = y^3$.

Led by the similarity with the previous problem, we try to adapt the argument given there to our present needs. This time, we factor the left hand side of our equation in the number ring $\mathbf{Z}[\sqrt{-19}]$ as

$$(x + \sqrt{-19})(x - \sqrt{-19}) = y^3.$$

We need to check that for a hypothetical solution (x, y), the two factors on the left hand side are coprime elements in $\mathbf{Z}[\sqrt{-19}]$. By this, we mean that there exist $\alpha, \beta \in \mathbf{Z}[\sqrt{-19}]$ such that we have $\alpha(x + \sqrt{-19}) + \beta(x - y\sqrt{-19}) = 1$. Equivalently, one may show that $x + \sqrt{-19}$ is coprime to the difference $2\sqrt{-19}$ of the two factors.

If x is odd, then $x^2 + 19$ is congruent to 4 mod 8, so it cannot be a cube. If x is divisible by 19, then $x^2 + 19$ is congruent to 19 mod 19^2, so it cannot be a cube. Thus x is even and not divisible by 19, and this implies that $x^2 + 19$ and 38 are coprime. Choose $a, b \in \mathbf{Z}$ such that $a(x^2 + 19) + 38b = 1$. Then $\alpha = a(x - \sqrt{-19})$ and $\beta = -b\sqrt{-19}$ achieve what we want.

By the same argument as for $\mathbf{Z}[i]$, we deduce that $x + \sqrt{-19}$ is the product of a unit and a cube in $\mathbf{Z}[\sqrt{-19}]$. This time the norm function $N : \mathbf{Z}[\sqrt{-19}] \to \mathbf{Z}$ is defined by $N(a+b\sqrt{-19}) = a^2+19b^2$, and we have $\mathbf{Z}[\sqrt{-19}]^* = \{\pm 1\}$ as the norm equation $a^2+19b^2 = 1$ only has the trivial solutions $(\pm 1, 0)$. As before, we find that there are integers a and b such that

$$x = a(a^2 - 57b^2) \qquad \text{and} \qquad 1 = (3a^2 - 19b^2)b.$$

It is immediately obvious that this time the values $b = \pm 1$ do not lead to a solution. We conclude that the equation from problem 1.4 does not admit integral solutions.

This is a nice argument, and one would be inclined to believe it – if it weren't true that the equality

$$18^2 + 19 = 324 + 19 = 343 = 7^3$$

convincingly shows that there do exist solutions. It turns out that our argument is fallacious, and a closer inspection reveals that there is a doubtful step in our argument: we applied the 'obvious fact' that a product of two coprime elements in a number ring can only be a cube if each of the factors is the product of a unit and a cube. This is correct for the ring $\mathbf{Z}[i]$, as one sees by invoking the uniqueness of factorization in $\mathbf{Z}[i]$. For the number ring $\mathbf{Z}[\sqrt{-19}]$ however, this is no longer an obvious fact. More precisely, it is easy to find factorizations like

$$20 = (1 + \sqrt{-19})(1 - \sqrt{-19}) = 2 \cdot 2 \cdot 5$$

that are non-unique. These are factorizations into irreducible elements, as one can easily check with the help of the norm function. Apparently, the number ring $\mathbf{Z}[\sqrt{-19}]$ is rather different from $\mathbf{Z}[i]$, and we cannot indiscriminately take over arguments that are correct in $\mathbf{Z}[i]$ to $\mathbf{Z}[\sqrt{-19}]$.

Exercise 5. Find elements α and β in $\mathbf{Z}[\sqrt{-19}]$ such that $\alpha(18 + \sqrt{-19}) + \beta(18 - \sqrt{-19}) = 1$.

▶ The arithmetic of number rings

In this text, we will focus on the arithmetic of *arbitrary* number rings. As shown by our examples, we need to control the units in these rings, and to develop a sound theory of unique factorization.

Our first step will be the introduction of a suitable notion of *ideals* in number rings, for which we will prove a form of unique factorization. Although ideals and elements are not the same objects, the 'obstruction' to ideals having a generating element can be measured by the *Picard group* of the number ring. This is an abelian group, and for number rings, which we can embed in Euclidean spaces and study with methods from the *geometry of numbers*, we will show that the Picard group is always finite. For the units, techniques from the geometry of numbers also yield a finiteness theorem, the *Dirichlet unit theorem*, which describes the structure of the unit group of a number ring.

These two basic finiteness theorems are at the heart of what one might call *classical algebraic number theory*, a powerful instrument that enables us to solve many questions that cannot easily be settled in other ways. They are the content of the sections 2 through 7 of this text. Section 8 is concerned with Galois theoretic aspects of number rings and the behaviour of primes in number field extensions.

The main difference between our approach and those found in most textbooks on algebraic number theory is that we do not focus exclusively on the *rings of integers* in number fields, which have the nicest theoretical properties but may be algorithmically inaccessible. Already in the case of the quadratic rings $\mathbf{Z}[\sqrt{d}]$ occurring in this section, one may not be able to decide whether a given large integer $d > 0$ is squarefree. This is however not an essential obstruction to studying arithmetical properties of $\mathbf{Z}[\sqrt{d}]$. In fact, Picard groups of rings $\mathbf{Z}[\sqrt{d}]$ were already studied by Gauss in terms of class groups of binary quadratic forms, and for $d > 0$ the solvability of the Pell equation – by continued fractions or other

means – is not essentially different if d has square factors.

Sometimes, the applicability of algebraic number theory is not at all obvious from the problem. Nowadays, the most promising approach to the fundamental problem of finding the prime factorization of a given large integer, for which straightforward methods are far too slow to be of any practical help, is the *number field sieve* that we will treat in due time. Somewhat surprisingly, it is exactly this kind of 'practical application' that forces us to develop the theory in more generality than is customary for texts on this level. Thus, the extra amount of abstract commutative algebra that goes into our treatment is caused by the desire to obtain a theory that works in practical situations.

One should not get the impression from what we said before that classical algebraic number theory is in any sense a complete theory. First of all, there are many basic problems of both algorithmic [21] and theoretical nature in the theory that are still open. Furthermore, there are many questions of elementary number theoretic nature that nobody can currently answer. Even the development of modern algebraic number theory, which we will touch upon in the final part of these notes, has not changed this situation.

In recent years, considerable progress has been realized in arithmetical questions using methods from arithmetic algebraic geometry. In this area, one uses suitable algebraic generalizations of concepts that were originally developed by geometers working over the field of complex numbers. The most striking example of this phenomenon is without doubt the proof of Fermat's last theorem by Wiles in 1993-94 [28]. Besides algebraic number theory, this proof uses the arithmetic of *elliptic curves*, which is currently a topic of intensive research in arithmetic algebraic geometry. It has given rise to several fundamental results and conjectures, see [24, 18]. We refer to [12] for methods in arithmetic of an even more geometrical nature, such as those leading to Faltings's celebrated finiteness result (previously Mordell's conjecture) for the number of solutions to large classes of Diophantine equations. Like any text in this area, it requires a strong background in abstract algebra, cf. [15].

We finally mention that there is no such thing as a universal theory of Diophantine equations. This is the content of a theorem from mathematical logic (proved by Matiyasevich in 1970, see [22]), which states that there is no general algorithm that will decide in a finite number of steps whether a Diophantine equation admits an integral solution. This provides a negative answer to a question commonly known as *Hilbert's tenth problem*. The problem had been the tenth in the list of open problems presented by Hilbert in his famous lecture at the international congress of mathematics in Paris in 1900 [17].

Exercises.

6. Show that the set of rational solutions to the equation $x^2 + y^2 = 1$ is $\{(1,0)\} \cup \{(\frac{t^2-1}{t^2+1}, \frac{2t}{t^2+1}) : t \in \mathbf{Q}\}$.
   [Hint: intersect the unit circle with the line $y = t(x-1)$.]
7. A *Euclidean function* on a ring R is a function $g : R \setminus \{0\} \to \mathbf{Z}_{\geq 0}$ such that for any two elements a and $b \neq 0$ in R, we can write $a = qb + r$ with $q, r \in R$ in such a way that we have either $r = 0$ or $g(r) < g(b)$. Show that a domain R is a principal ideal domain if it admits a Euclidean function.
8. Show that the ring $\mathbf{Z}[\sqrt{3}]$ is a principal ideal domain.

9. Let $d > 1$ be a non-square integer with square root $\sqrt{d} \in \mathbf{R}_{>0}$, and define $L : \mathbf{Z}[\sqrt{d}]^* \to \mathbf{R}$ by $L(u) = \log|u|$. Prove the following.
   a. L is a homomorphism with kernel $\ker L = \{\pm 1\}$ and $\operatorname{im} L$ is a *discrete* subgroup of $\mathbf{R}$. [Hint: $\operatorname{im} L \cap \mathbf{R}_{>0} = \{\log(u) : u = x + y\sqrt{d} \in \mathbf{Z}[\sqrt{d}]^* \text{ with } x, y \in \mathbf{Z}_{>0}\}$.]
   b. One has $\mathbf{Z}[\sqrt{d}]^* = \{\pm 1\}$ or $\mathbf{Z}[\sqrt{d}]^* = \langle -1\rangle \times \langle \varepsilon_d\rangle$ for some unit $\varepsilon_d \in \mathbf{Z}[\sqrt{d}]^*$ of infinite order .
   c. Suppose there exists a fundamental unit ε_d as in b. Then the group $P \subset \mathbf{Z}[\sqrt{d}]^*$ of units of norm 1 equals $P = \langle -1\rangle \times \langle \varepsilon_d^k\rangle$ with $k = 1$ if ε_d is in P and $k = 2$ otherwise. [The Dirichlet unit theorem 5.13 implies that the hypothesis is always satisfied.]

10. Let d be a non-square integer and $\alpha = a + b\sqrt{d}$ an element of $\mathbf{Q}(\sqrt{d})$ of norm $u = a^2 - db^2$. Define the sequences $\{x_n\}_{n=0}^{\infty}$ and $\{y_n\}_{n=0}^{\infty}$ by $\alpha^n = x_n + y_n\sqrt{d}$. Show that these sequences have initial values $x_0 = 1$, $x_1 = a$, $y_0 = 0$ and $y_1 = b$ and satisfy the recurrence $s_{n+1} = 2as_n - us_{n-1}$ for all $n \in \mathbf{Z}_{>0}$.

11. Let $d > 1$ be a non-square integer and let y be the smallest positive integer for which dy^2 is of the form $x^2 \pm 1$. Show that $\varepsilon_d = x + y\sqrt{d}$ is a fundamental unit in $\mathbf{Z}[\sqrt{d}]$. Compute ε_d and the norm $N(\varepsilon_d)$ for all non-square $d \leq 20$.

12. Let $d > 1$ be an integer congruent to 1 mod 4 that is not a square, and let $\alpha \in \mathbf{R}$ be a zero of the polynomial $X^2 - X - \frac{d-1}{4} \in \mathbf{Z}[X]$. Show that $\mathbf{Z}[\alpha]$ is a subring of $\mathbf{R}$ that contains $\mathbf{Z}[\sqrt{d}]$ as a subring of index 2. Show also that $\mathbf{Z}[\sqrt{d}]^*$ is of finite index in $\mathbf{Z}[\alpha]^*$, and that this index is equal to 1 or 3. Give examples showing that both possibilities occur.
[If you want a large example: for $d = 1141$ the element $618715978 + 37751109\alpha$ is a fundamental unit in $\mathbf{Z}[\alpha]$.]

13. Let $R = \mathbf{Z}[\alpha] = \mathbf{Z}[\frac{1+\sqrt{-19}}{2}]$ be the ring obtained by taking $d = -19$ in the previous exercise.
   a. Show that we have $R^* = \{\pm 1\}$.
   b. We will see in exercise 36 that R is a unique factorization domain. Using this, show that the only integral solutions to the equation $x^2 + 19 = y^3$ are $(x, y) = (\pm 18, 7)$.

14. Show that the ring $R = \mathbf{Z}[\frac{1+\sqrt{-19}}{2}]$ does not admit a Euclidean function.
[Hint: pick $x \in R \setminus \{0, \pm 1\}$ with minimal function value, show that R/xR has order 2 or 3, and derive a contradiction.]

15. Let $d \in \mathbf{Z}_{\neq 1}$ be a squarefree integer and $K = \mathbf{Q}(\sqrt{d})$ the corresponding quadratic field. Show that the subset $\mathcal{O}_K \subset K$ of elements $x \in K$ that have irreducible polynomial $f_{\mathbf{Q}}^x \in \mathbf{Z}[X]$ forms a subring of K, and that we have
$$\mathcal{O}_K = \begin{cases} \mathbf{Z}[\sqrt{d}] & \text{if } d \equiv 2 \text{ or } 3 \bmod 4; \\ \mathbf{Z}[\frac{1+\sqrt{d}}{2}] & \text{if } d \equiv 1 \bmod 4. \end{cases}.$$

16. Show that for $K = \mathbf{Q}(\sqrt{d})$ as in the previous exercise and $d < 0$, we have $\mathcal{O}_K^* = \{\pm 1\}$ unless $d \in \{-1, -3\}$. What is $\mathcal{O}_K^*$ in these two exceptional cases?

17. Show that for every $\alpha \in \mathbf{Z}[i] \setminus \{0\}$, the norm $N(\alpha)$ is the cardinality of the residue class ring $\mathbf{Z}[i]/\alpha\mathbf{Z}[i]$.

18. Show that an integer $k > 0$ can be written as a sum of two squares if and only if for every prime $p \equiv 3 \bmod 4$, the number of factors p in k is *even*. Describe the number of solutions $(a, b) \in \mathbf{Z}^2$ to $k = a^2 + b^2$.

19. Determine which rational numbers can be written as the sum of two rational squares.

20. Let a, b, c be coprime integers satisfying $a^2 + b^2 = c^2$. Show that there exist integers $m, n \in \mathbf{Z}$ such that we have, after possibly interchanging a and b,

$$a = m^2 - n^2 \qquad b = 2mn \qquad c = \pm(m^2 + n^2).$$

[Hint: First method: as a and b have different parity, $c^2 = (a + bi)(a - bi)$ is the product of coprime integers in $\mathbf{Z}[i]$. Second method: if b is even, $(b/2)^2 = \frac{c-a}{2} \cdot \frac{c+a}{2}$ is a product of coprime integers. Third method: exercise 6.]

21. Let $a, b \in \mathbf{Z}$ be coprime integers satisfying $ab = c^n$ for some $n \geq 1$. Show that one has $a = \pm s^n$ for $s = \gcd(a, c)$.
[This shows that it is not necessary to factor c in order to write a and b as n-th powers.]

22. Let $p \neq 2$ be a prime number.

    a. Prove: -2 is a square in $\mathbf{F}_p^* \iff p \equiv 1, 3 \bmod 8$.
    [Hint: every primitive 8-th root of unity $\zeta_8 \in \mathbf{F}_{p^2}$ satisfies $(\zeta_8 + \zeta_8^3)^2 = -2$.]

    b. Prove:
    $$p \equiv 1, 3 \bmod 8 \iff p = x^2 + 2y^2 \quad \text{for} \quad x, y \in \mathbf{Z}.$$
    [Hint: Imitate the solution of 1.2 and write $p = \pi\bar{\pi}$ in the ring $\mathbf{Z}[\sqrt{-2}]$.]

23. Let $p \neq 3$ be a prime number. Prove:

$$p \equiv 1 \bmod 3 \iff p = x^2 + 3y^2 \quad \text{for} \quad x, y \in \mathbf{Z}.$$

[Hint: The ring $\mathbf{Z}[\sqrt{-3}]$ is *not* Euclidean, but the ring $\mathbf{Z}[\frac{-1+\sqrt{-3}}{2}]$ is.]

24. Find all integral solutions to the equation $x^2 + 4 = y^3$.

25. Find all integral solutions to the equation $x^2 + 2 = y^3$.
[In 1659, Fermat claimed he could do this exercise and the previous one.]

26. Show that the norm function $N : \mathbf{Z}[\sqrt{d}] \to \mathbf{Z}$ for $d \in \mathbf{Z}$ not a square is never surjective. Describe the prime factorizations of the elements in the image for $d \in \{-1, -2, -3, -4\}$.

27. Show that the equation $x^2 + 61 = y^3$ has integral solutions. Deduce that $\mathbf{Z}[\sqrt{-61}]$ is not a unique factorization domain.

28. Let $d < -2$ be an integer. Show that $\mathbf{Z}[\sqrt{d}]$ is not a unique factorization domain.

29. An integer T is called a *triangular number* if it is of the form

$$T = 1 + 2 + 3 + \ldots + m = \frac{1}{2}m(m + 1)$$

for some $m \geq 1$. Check that m-th triangular number is a square for the values

$$m = 1, 8, 49, 288, 1681, 9800, 57121, 332928.$$

Prove that there are infinitely many m with this property, and that the values above form a complete list of such m below 1,000,000.

30. Let q be a rational number. Prove that the following are equivalent:

    (i) there are a triangular number T and a non-zero square S with $T/S = q$;

(ii) there are infinitely many pairs (T, S) as in (i);
(iii) for each positive integer k, there is a pair (T, S) as in (i) for which k divides S;
(iv) the number $2q$ is not a rational square.

31. Let A be a commutative ring, and let $B \subset A$ be a subring for which the abelian group A/B is finite.
    a. Prove that there is an ideal I of A with $I \subset B$ for which A/I is finite.
    b. Prove that the unit groups of A and B satisfy $A^* \cap B = B^*$, and that the abelian group A^*/B^* is finite.

32. Let K be an algebraic extension of $\mathbf{Q}$, and $R \subset K$ a subring.
    a. Show that if I is a non-zero ideal of R, then $I \cap \mathbf{Z}$ is a non-zero ideal of $\mathbf{Z}$.
    b. Suppose that K is the field of fractions of R. Show that every $x \in K$ can be written as $x = r/k$, with $r \in R$ and $k \in \mathbf{Z}_{\neq 0}$.

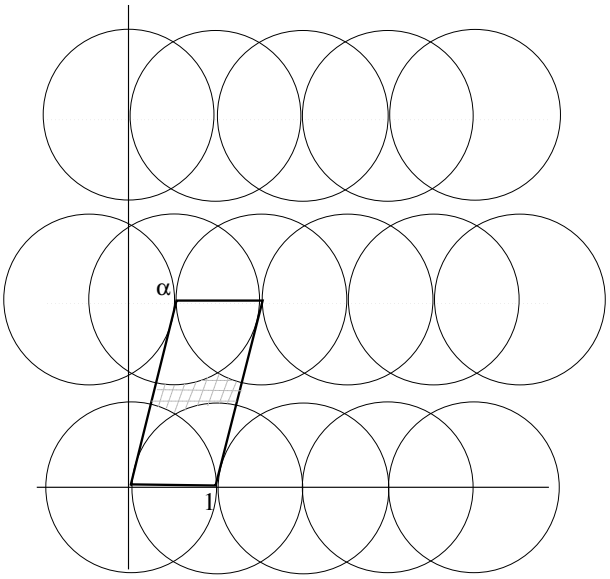
33. Let $\mathcal{P}$ denote the set of prime numbers. Show that there is a bijection

$$\begin{aligned} \{\text{subrings of } \mathbf{Q}\} &\longrightarrow \{\text{subsets of } \mathcal{P}\} \\ R &\longmapsto R^* \cap \mathcal{P}. \end{aligned}$$

34. Let K be a number field of degree $n > 1$ over $\mathbf{Q}$. Show that there are infinitely many subrings $R \subset K$ for which the additive group of R is free of rank n.

*35. Let $n \geq 2$ be an integer. Show that the equation $x^2 + 1 = y^n$ has no integral solutions with $x \neq 0$.

*36. Let $R = \mathbf{Z}[\alpha]$ with $\alpha = \frac{1+\sqrt{-19}}{2}$ be as in exercises 13 and 14, and consider R as a subring of $\mathbf{C}$. We say that $(a, b) \in R \times (R \setminus \{0\})$ allows division with remainder in R if there exist $q, r \in R$ with $a = qb + r$ and $|r| < |b|$.
    a. Show that (a, b) allows division with remainder in R if and only if $a/b \in \mathbf{C}$ lies in the union $U = \{x + d : x \in \mathbf{Z}[\alpha] \text{ and } |d| < 1\}$ of the open disks of radius 1 in the figure below.



b. Show that the sum of two complex numbers in $\mathbf{C} \setminus U$ lies in U. Deduce that if (a, b) does not allow division with remainder in R, then $(2a, b)$ and at least one of the pairs $(\alpha a, b)$ and $((1 - \alpha)a, b)$ allow division with remainder in R.
c. Show that 2 is coprime to both α and $1 - \alpha$ in R.
d. Prove that R is a principal ideal domain.

2 Ideal arithmetic

We have seen in section 1 that number rings are not in general unique factorization domains. More specifically, we saw that in the ring $\mathbf{Z}[\sqrt{-19}]$, there are coprime elements $18+\sqrt{-19}$ and $18-\sqrt{-19}$ for which 5 the product is a cube, whereas neither of the elements is up to units equal to the cube of an element in $\mathbf{Z}[\sqrt{-19}]$. This somewhat puzzling phenomenon was discovered around 1850 by the German mathematician Kummer (1820–1889), who encountered analogous phenomena in the cyclotomic number rings that arise naturally in the study of the Fermat equation $x^p + y^p = z^p$. The solution offered by Kummer consisted of the introduction of *ideale Zahlen*, and was initially regarded as extremely mysterious by his contemporaries. Only later in the 19-th century, when Kronecker and Dedekind polished Kummer's theory and generalized it to arbitrary number fields, his ideal theory found general acceptance. Abstract ideal theory became common algebraic knowledge after 1930, when the contents of the algebra courses of Hasse and E. Noether were published as a textbook by Van der Waerden [26].

▶ Ideals

Let R be a commutative ring. Then an R-ideal is an additive subgroup of R satisfying $rI \subset I$ for every $r \in R$, or, more concisely, a subset of R that is an R-module. We say that an ideal I *divides* an ideal J if I contains J. In particular, ideals 'divide' elements in the sense that I divides the principal ideal xR for all $x \in I$. Kummer originally defined R-ideals in a more restrictive way, as R-ideals I with the property that $II' = xR \neq 0$ for for some R-ideal I'. Such ideals, which will play an important role in the sequel, are nowadays said to be *invertible*.

If I and J are R-ideals, the sum $I + J = \{i + j : i \in I, j \in J\}$, the intersection $I \cap J$ and the product

$$IJ = \{\textstyle\sum_{i=1}^{n} x_i y_i : x_i \in I, y_i \in J, n \in \mathbf{Z}_{\geq 0}\}$$

are again R-ideals. Note that, whereas the sum $I + J$ of the R-ideals I and J consists of elements $i + j$ with $i \in I$ and $j \in J$, the product ideal IJ is the R-ideal *generated* by the elements ij. The ideal $I + J$ is the smallest ideal containing both I and J, and we have the distributive law $H(I + J) = HI + HJ$.

Ideals I and J are said to be *coprime* if we have $I + J = R$. For principal ideals $I = Ra$ and $J = Rb$ this amounts to saying that a and b are coprime in the sense of section 1: one has $ax + by = 1$ for certain $x, y \in R$.

Exercise 1. Show that $a, b \in R$ are coprime if and only if there does not exist a ring homomorphism $f : R \to F$ with F a field and $a, b \in \ker f$.

If I and J are coprime, then so are I^n and J^n for every $n \geq 1$; one simply observes that $R = (I + J)^{2n}$ is contained in $I^n + J^n$. For coprime ideals I and J, we have $IJ = I \cap J$ and the *Chinese remainder theorem* gives a natural isomorphism $R/(IJ) \cong (R/I) \times (R/J)$.

Before we develop any ideal arithmetic at all, we show that the fallacious argument in the previous section becomes correct if we look at ideals rather than elements.

2.1. Theorem. *Let R be a ring and I and J coprime ideals of R such that IJ is the n-th power of some ideal in R. Then I and J are both n-th powers of an ideal in R.*

Proof. Suppose that $IJ = Z^n$ for some ideal Z. Using the standard multiplication rules for ideals and the coprimality of the ideals I^{n-1} and J, we obtain

$$(I+Z)^n = I^n + I^{n-1}Z + \cdots + IZ^{n-1} + IJ = I(I^{n-1} + \cdots + Z^{n-1} + J) = IR = I. \quad \square$$

2.2. Example. We have seen that in the ring $R = \mathbf{Z}[\sqrt{-19}]$, the product of the coprime ideals $I = (18 + \sqrt{-19})$ and $J = (18 - \sqrt{-19})$ equals the cube of the principal ideal (7). It follows that we have

$$(18 + \sqrt{-19}) = (18 + \sqrt{-19}, 7)^3.$$

Our computation in 1.4 implies that the ideal $P = (18 + \sqrt{-19}, 7)$ is a *non-principal* ideal, even though its cube P^3 is principal.

Exercise 2. Show that $P = (18 + \sqrt{-19}, 7)$ is a maximal ideal of index 7 in $\mathbf{Z}[\sqrt{-19}]$.

Ideals can be added and multiplied in any ring R. For a *domain* R, unrestricted division by non-zero elements can be performed inside the *field of fractions* $K = Q(R)$ of R. In order to divide the non-zero *ideals* of a domain R, one is naturally led to the following extension of the ideal concept.

2.3. Definition. *Let R be a domain with field of fractions K. Then a fractional R-ideal I is a non-zero R-submodule of K such that xI is contained in R for some $x \in K^*$.*

Saying that I is an R-submodule of K means that I is an additive subgroup of K that is mapped into itself under multiplication by elements of R. The element x in the definition can be chosen to lie in R, and if we have $xI \subset R$ then xI is an R-ideal. We say that I is *integral* if it is contained in R. Every fractional R-ideal contains non-zero elements of R. For every finite subset $\{x_1, x_2, \ldots, x_n\}$ of K^*, the R-submodule $Rx_1 + Rx_2 + \ldots + Rx_n$ of K is a fractional R-ideal. A *principal* fractional ideal is a fractional ideal of the form Rx with $x \in K^*$. If R is a principal ideal domain, then every fractional ideal is of this form. The definition of fractional ideals shows that we can divide them in an obvious way by elements of K^*. For arbitrary fractional ideals I and J we define the *ideal quotient* as

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

It is an immediate consequence of the definition that this is an R-submodule of K. If we choose $a \in I$ and $b \in K^*$ such that $bJ \subset R$, then we have $abJ \subset I$, so $I : J \neq 0$. If we take $c, d \in K^*$ such that $cI \subset R$ and $d \in J$, it follows that $cd(I : J) \subset R$. We have proved the only non-obvious case of the following proposition.

2.4. Proposition. *If I and J are fractional R-ideals, then so are the sum $I + J$, the product IJ, the intersection $I \cap J$ and the quotient $I : J$.* $\square$

If we take R equal to $\mathbf{Z}$, then all fractional ideals are of the form $I = (q) = q\mathbf{Z}$ with $q \in \mathbf{Q}^*$. The product and the quotient of such ideals are simply given by $(q_1)(q_2) = (q_1 q_2)$ and

$(q_1) : (q_2) = (q_1/q_2)$. In this case, we see that the fractional ideals form a group isomorphic to $\mathbf{Q}^*/\mathbf{Z}^* = \mathbf{Q}^*/\{\pm 1\}$. For the sum and intersection of fractional ideals in $\mathbf{Z}$ (or an arbitrary principal ideal domain) see exercise 11.

Two ideal quotients coming with a fractional R-ideal I for which we introduce a special notation are the "inverse ideal"

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

of I and the *multiplier ring*

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

of I. Note that $r(I)$ is indeed a subring of K, and that it contains R. If it is equal to R, than I is said to be *proper* for the ring R. This is not to be confused with the word 'proper' to indicate that an ideal $I \subset R$ is a proper subset of R, i.e., not equal to the full ring R.

▶ Invertible ideals

A fractional R-ideal I is said to be *invertible* if one has $IJ = R$ for some fractional R-ideal J. If such a J exists, it is contained in I^{-1}, and actually equal to I^{-1}, as we also have $I^{-1} = I^{-1} \cdot IJ \subset RJ = J$. Thus the invertible ideals are exactly those I for which we have $II^{-1} = R$. As I^{-1} is again a fractional R-ideal, we find that an ideal $I \subset R$ is invertible if and only if there exists an ideal $J \subset R$ such that IJ is a non-zero principal ideal. This means that such I occur as the "divisors of principal ideals", i.e., ideals in Kummer's original sense. Invertible ideals are not always principal, but something weaker is true.

2.5. Lemma. *Any invertible R-ideal is finitely generated.*

Proof. The equation $IJ = R$ implies that there exist $x_i \in I$ and $y_i \in J$ such that $\sum_{i=1}^n x_i y_i = 1$. Now any $x \in I$ can be written in the form $x = \sum_{i=1}^n (xy_i)x_i$. As we have $xy_i \in IJ = R$, we obtain $I = \sum_{i=1}^n Rx_i$, and we are done. □

The set $\mathcal{I}(R)$ of invertible fractional R-ideals forms a group under ideal multiplication. Principal fractional ideals, which are obviously invertible, form a subgroup $\mathcal{P}(R) \subset \mathcal{I}(R)$ that is isomorphic to K^*/R^*. The obstruction group measuring to which extent invertible R-ideals are principal is the *Picard group* of R.

2.6. Definition. *The Picard group of a domain R is defined as* $\mathrm{Pic}(R) = \mathcal{I}(R)/\mathcal{P}(R)$.

In other words, the Picard group of a domain R is defined by the long exact sequence

$$0 \longrightarrow R^* \longrightarrow K^* \xrightarrow{f} \mathcal{I}(R) \longrightarrow \mathrm{Pic}(R) \longrightarrow 0,$$

where $f(x) = xR$ for $x \in K^*$. If R is a principal ideal domain, then we have $\mathcal{I}(R) = f[K^*] = \mathcal{P}(R)$ and $\mathrm{Pic}(R) = 0$. As the condition that an ideal be invertible is rather restrictive, it is not generally true that a domain with trivial Picard group is a principal ideal domain (exercise 15).

The ring $R = \mathbf{Z}[\sqrt{-19}]$ is an example of a ring with non-trivial Picard group. As we saw in example 2.2, the class of the ideal $(18 + \sqrt{-19}, 7)$ is an element of order 3 in $\mathrm{Pic}(R)$.

This explains why our method to solve 1.4 failed: $18+\sqrt{-19}$ generates the cube of an *ideal*, but it is not the cube of an element. We will show later that in this case, $\mathrm{Pic}(R)$ is actually of order 3.

The invertible ideals of a domain R can be neatly characterized as those finitely generated R-ideals that are *locally principal*, making the Picard group into an obstruction group to a 'local-global-principle'. The precise statement is the following.

2.7. Theorem. *Let R be a domain and I a fractional R-ideal. Then I is invertible if and only if the following two conditions hold:*

(1) *I is finitely generated;*
(2) *the localization $I_{\mathfrak{m}}$ at each maximal ideal $\mathfrak{m}$ of R is a principal fractional $R_{\mathfrak{m}}$-ideal.*

▶ Localization

Before proving theorem 2.7, we spend some time on the important concept of *localization* from commutative algebra that occurs in condition (2). As we are working with domains R, we can localize inside the field of fractions $Q(R)$ of R. We will therefore avoid discussing the localization concept for arbitrary commutative rings or the geometric explanation of its 'local nature'. These are found in [9, section 3] or [15, chapter 2].

Let R be a domain and S a *multiplicative subset* of R, i.e., a subset of $R\setminus\{0\}$ that contains 1 and is closed under multiplication. Then we can define the localized ring

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

This is a subring of $K = Q(R)$ that contains R. There is the localization $K = Q(R)$ corresponding to $S = R\setminus\{0\}$. More generally, by taking $S = R\setminus\mathfrak{p}$, we have localizations

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

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

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

consisting of the complement of the unit group $R_{\mathfrak{p}}^* = \{\tfrac{r}{s} \in K : r, s \notin \mathfrak{p}\}$ consisting of all $x \in K^*$ that are 'invertible modulo $\mathfrak{p}$'. Conversely, a local domain R coincides with the localization $R_{\mathfrak{m}}$ at its maximal ideal $\mathfrak{m}$.

When dealing with the localizations of a domain R having more than one maximal ideal, one often refers to R as the *global ring*. Localization enables one to pass from R to a 'less complicated' ring $S^{-1}R$ without losing information on the ideals outside S. Informally, one can say that localizing at S maps the ideals disjoint from S to the ideals of the localized ring, and all ideals that meet S to the unit ideal of the localized ring.

2.8. Proposition. *Let R be a domain and $S \subset R\setminus\{0\}$ a multiplicative subset. Then for every R-ideal I, the image of I under the localization map $R \to S^{-1}R$ generates an ideal*

$$S^{-1}I = \{\tfrac{i}{s} : i \in I, s \in S\} \subset S^{-1}R.$$

We have $S^{-1}I \neq S^{-1}R$ if and only if $I \cap S = \emptyset$, and all ideals of $S^{-1}R$ are of the form $S^{-1}I$.

Proof. It is clear that $S^{-1}I$ is an ideal of $S^{-1}R$ that contains 1 if and only if there exists an element $s \in I \cap S$. For every ideal $J \subset S^{-1}R$, the contraction $R \cap J$ is an R-ideal with localization J. □

Exercise 3. Show that the map $I \mapsto S^{-1}I$ induces a bijection between the prime ideals of R that do not meet S and the prime ideals of $S^{-1}R$, and that the local rings at corresponding primes are isomorphic.

If I is a fractional R-ideal and $S \subset R \setminus \{0\}$ a multiplicative subset, then

$$S^{-1}I = \{\tfrac{i}{s} : i \in I, s \in S\} \subset K$$

is a fractional $S^{-1}R$-ideal. In the case $S = R \setminus \mathfrak{p}$ we denote this fractional $R_\mathfrak{p}$-ideal by $I_\mathfrak{p}$. An ideal $I \in \mathcal{I}(R)$ is determined by its localizations $I_\mathfrak{p}$, as follows.

2.9. Lemma. *Let R be a domain and I a fractional R-ideal. Then we have*

$$I = \textstyle\bigcap_\mathfrak{m} I_\mathfrak{m},$$

where the intersection is taken over the localizations at all maximal ideals $\mathfrak{m}$ of R.

Proof. It is clear that I is contained in the intersection $\bigcap_\mathfrak{m} I_\mathfrak{m}$. Given an element $x \in \bigcap_\mathfrak{m} I_\mathfrak{m}$, we consider $J = \{r \in R : rx \in I\} \subset R$. This is an ideal of R, and since we can write $x = \frac{a}{b}$ with $a \in I$ and $b \in R \setminus \mathfrak{m}$ for each maximal ideal $\mathfrak{m}$, the ideal $J \subset R$ contains, for each $\mathfrak{m}$, an element $b \notin \mathfrak{m}$. It follows that J is not contained in any maximal ideal of R, so we have $J = R$ and $x = x \cdot 1 \in I$. □

Proof of 2.7. Let I be an invertible R-ideal. Then I is finitely generated by 2.5, and there exist $x_i \in I$ and $y_i \in I^{-1}$ such that $\sum_{i=1}^n x_i y_i = 1$. Let $\mathfrak{p} \subset R$ be any 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

$$x = x_1 \cdot xy_1 \cdot (x_1 y_1)^{-1} \in x_1 R \cdot R \cdot R_\mathfrak{p} = x_1 R_\mathfrak{p}.$$

It follows that $I_\mathfrak{p}$ is principal with generator x_1.

Conversely, let $I = Rx_1 + Rx_2 + \ldots + Rx_n$ be a finitely generated R-ideal with the property that $x \in I$ generates the localization $I_\mathfrak{p} = xR_\mathfrak{p}$ at a prime $\mathfrak{p}$. Then we can write $x_i = x(r_i/s) \in R_\mathfrak{p}$, with $r_i \in R$ and $s \in R \setminus \mathfrak{p}$ independent of i. From $sx^{-1} \cdot x_i = r_i \in R$ we obtain $sx^{-1} \in I^{-1}$, so $I \cdot I^{-1}$ contains $x \cdot sx^{-1} = s \in R \setminus \mathfrak{p}$.

If I is locally principal at all maximal ideals of R, then $I \cdot I^{-1}$ is not contained in any maximal ideal of R. This means that we have $I \cdot I^{-1} = R$, and that I is invertible. □

Exercise 4. Show that we may replace 'maximal ideal' by 'prime ideal' in the second condition of 2.7.

2.10. Example. We saw in 2.2 that the principal ideal $(18 + \sqrt{-19})$ is the cube of the maximal ideal $I = (7, 3 - \sqrt{-19})$ in the ring $R = \mathbf{Z}[\sqrt{-19}]$. The ideal I is not principal, but as it is invertible our theorem implies that all its localizations $I_\mathfrak{p}$ are. For primes $\mathfrak{p}$ not containing I, we trivially find $I_\mathfrak{p} = R_\mathfrak{p}$ as I contains elements outside $\mathfrak{p}$. The only prime $\mathfrak{p} \supset I$ is $\mathfrak{p} = I$, and here we have $I_\mathfrak{p} = 7R_\mathfrak{p} = (3 - \sqrt{-19})R_\mathfrak{p}$: the quotient

$$\frac{7}{3 - \sqrt{-19}} = \frac{3 + \sqrt{-19}}{4}$$

is a unit in $R_\mathfrak{p}$ since $3+\sqrt{-19}$ and 4 are in $R \setminus \mathfrak{p} \subset R_\mathfrak{p}^*$.

The ideal $J = (2, 1+\sqrt{-19})$ of index 2 is also not principal, but here the identity $J^2 = (4, 2+2\sqrt{-19}) = 2J$ shows that J is not invertible: if it were, the identity could be multiplied by J^{-1} to prove that J is principal, and generated by 2. At the only prime $\mathfrak{p} = J$ containing J, the ideal $J_\mathfrak{p}$ needs both generators.

▶ Ideals in number rings

Suppose now that R is a number ring. Then theorem 2.7 can be simplified a bit as number rings are *noetherian*: all their ideals are finitely generated. Even more is true.

2.11. Theorem. *Every non-zero ideal in a number ring is of finite index.*

Proof. Let $K = Q(R)$ be a number field of degree $t \geq 1$ over $\mathbf{Q}$, and suppose we are given a non-zero ideal $I \subset R$. Pick any non-zero element $x \in I$. As x is algebraic over $\mathbf{Q}$, it satisfies an equation $a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0 = 0$ with $a_i \in \mathbf{Z}$, and we have $a_0 \neq 0$ as x is non-zero. This shows that $I \supset (x)$ contains the positive integer $a = |a_0|$.

Clearly R/aR maps surjectively to R/I, so it is sufficient to show that R/aR is a finite ring. To show this, let $M \subset R$ be any finitely generated subgroup of the additive group of R. As M has no elements of finite order, M is a free abelian group. Any set of more than t elements in $R \subset K$ is linearly dependent over $\mathbf{Q}$, so we see that M has to be of finite rank $k \leq t$. The natural map $M \to R/aR$ factors via the group M/aM, which is finite of order $a^k \leq a^t$. This implies that *every* finitely generated subgroup of R/aR has order at most a^t, so R/aR itself is finite of order at most a^t. □

2.12. Corollary. *A number ring is noetherian, and all of its non-zero prime ideals are maximal.*

Proof. If $I \subset R$ is a non-zero ideal, then 2.11 shows that every non-zero principal ideal $(x) \subset I$ is of finite index in I. It follows that I itself is finitely generated, so R is noetherian. The second statement is immediate from 2.11 as every finite domain $R/\mathfrak{p}$ is a field. □

The proof of 2.11 shows that for R a number ring and $n \geq 1$ any integer, the additive group of R/nR can be generated by $t = [Q(R) : \mathbf{Q}]$ elements. This does not imply that the additive group of R itself is finitely generated: the number ring $R = \mathbf{Z}[\frac{1}{2}] \subset \mathbf{Q}$ consisting of rational fractions with 2-power denominator is not finitely generated as an abelian group, but R/I is finite cyclic for all $I \neq 0$.

Exercise 5. What is the cardinality of R/nR for $R = \mathbf{Z}[\frac{1}{2}]$ and $n \in \mathbf{Z}_{>0}$?

A number ring for which the additive group is finitely generated is called an *order* in its field of fractions. As a number ring has no additive torsion elements, every order is in fact *free* of finite rank over $\mathbf{Z}$. The rank of an order R in $K = Q(R)$ is bounded by the degree $t = [K : \mathbf{Q}]$, and as we have $R \otimes_\mathbf{Z} \mathbf{Q} = K$ it has to be equal to t. This implies that we have

$$R = \mathbf{Z} \cdot \omega_1 \oplus \mathbf{Z} \cdot \omega_2 \oplus \ldots \oplus \mathbf{Z} \cdot \omega_t$$

for some $\mathbf{Q}$-basis $\{\omega_1, \omega_2, \ldots, \omega_t\}$ of K. For every monic irreducible polynomial $f \in \mathbf{Z}[X]$ of degree n, the associated order $\mathbf{Z}[\alpha] = \mathbf{Z}[X]/(f)$ obtained by adjoining a root α of f has

rank n. All number rings in the introduction are orders of the form $\mathbf{Z}[\alpha]$. If an order R is of the form $R = \mathbf{Z}[\alpha]$ for some $\alpha \in R$, then R is said to be *monogenic*.

A domain R which is not a field and in which every non-zero prime ideal of R is maximal is said to be *one-dimensional*. More generally, one defines the *Krull-dimension* of a commutative ring R as the supremum of the lengths of all chains of prime ideals in R. Here a *chain* of prime ideals in R of *length* n is a strictly increasing sequence of prime ideals $\mathfrak{p}_0 \subsetneq \mathfrak{p}_1 \subsetneq \ldots \subsetneq \mathfrak{p}_n$.

Exercise 6. Given an example of a domain R having infinite Krull dimension.

Fields and finite rings are zero-dimensional: all their prime ideals are maximal. By 2.12, number rings that are not number fields are one-dimensional. Their non-zero prime ideals, which are all maximal, are usually referred to as the *primes* of the number ring.

▶ Primary decomposition

It is not in general true that the invertible ideals of a number ring can uniquely be written as powers of prime ideals. The study of invertible ideals I of a number ring R can however be reduced to the study of its localizations $I_\mathfrak{p}$ at the primes $\mathfrak{p}$, which are *principal* and only differ from $R_\mathfrak{p}$ for finitely many $\mathfrak{p}$.

2.13. Lemma. *Let $R_\mathfrak{p}$ be a local number ring. Then every non-zero ideal of $R_\mathfrak{p}$ contains some power of its maximal ideal.*

Proof. As $R_\mathfrak{p}$ is noetherian, we can apply *noetherian induction*: if there are counterexamples to the lemma, the set of such ideals has a maximal element I (cf. exercise 26). Then I is not prime, as the maximal ideal $\mathfrak{p}$ is the only non-zero prime ideal of $R_\mathfrak{p}$. 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 $\mathfrak{p}$. The same then holds for $(I + (x))(I + (y)) \subset I$: contradiction. □

2.14. Theorem. *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 an invertible ideal I to its vector of localizations $(I_\mathfrak{p})_\mathfrak{p}$ at the primes of R.

Proof. The map ϕ is well-defined by 2.7 and the fact that, by 2.11, every non-zero ideal $I \subset R$ is contained in only finitely many primes of R. It is a homomorphism by the basic property $S^{-1}I \cdot S^{-1}J = S^{-1}(IJ)$ of localizations, and it is injective by 2.9.

In order to show ϕ is surjective it suffices to construct, for $\mathfrak{p}$ a prime of R and $J_\mathfrak{p} \in \mathcal{P}(R_\mathfrak{p})$ an integral $R_\mathfrak{p}$-ideal, some global ideal I that has localizations $I_\mathfrak{q} = R_\mathfrak{q}$ at $\mathfrak{q} \neq \mathfrak{p}$ and $I_\mathfrak{p} = J_\mathfrak{p}$. There is no choice for I by 2.9, so we let $I = J_\mathfrak{p} \cap \bigcap_{\mathfrak{q} \neq \mathfrak{p}} R_\mathfrak{q} = J_\mathfrak{p} \cap R$. It is clear that I is an integral R-ideal with localization $J_\mathfrak{p}$ at $\mathfrak{p}$. By 2.13, the ideal $I_\mathfrak{p}$ contains a power $\mathfrak{p}^n R_\mathfrak{p}$ of the maximal ideal of $R_\mathfrak{p}$. It follows that we have $\mathfrak{p}^n \subset I$. If $\mathfrak{q}$ is a prime different from $\mathfrak{p}$, we cannot have $I \subset \mathfrak{q}$ as this would imply that $\mathfrak{q}$ contains $\mathfrak{p}^n$ and therefore $\mathfrak{p}$. We find that we have $I_\mathfrak{q} = R_\mathfrak{q}$ for such $\mathfrak{q}$, as was to be shown. □

Theorem 2.14 states that for a number ring R, giving an invertible R-ideal is 'the same' as giving a principal $R_\mathfrak{p}$-ideal $I_\mathfrak{p}$ for each prime $\mathfrak{p}$ of R, provided that we take $I_\mathfrak{p} = R_\mathfrak{p}$ for almost all $\mathfrak{p}$. Note that I is an integral R-ideal if and only if all $I_\mathfrak{p}$ are integral $R_\mathfrak{p}$-ideals, and that the isomorphism ϕ 'preserves' inclusions in an obvious way.

2.15. Example. For $R = \mathbf{Z}$, the theorem reduces to unique factorization for rational numbers. In this case, the local ring $\mathbf{Z}_{(p)} = \{\frac{a}{b} \in \mathbf{Q} : p \nmid b\}$ at a prime p has unit group $\mathbf{Z}_{(p)}^* = \{\frac{a}{b} \in \mathbf{Q} : p \nmid a \text{ and } p \nmid b\}$. Any non-zero rational number can uniquely be written as $x = p^{\mathrm{ord}_p(x)} \cdot u$ with $\mathrm{ord}_p(x) \in \mathbf{Z}$ and $u \in \mathbf{Z}_{(p)}^*$, so a principal fractional $\mathbf{Z}_{(p)}$-ideal is of the form $p^k\mathbf{Z}_{(p)}$ for some unique $k \in \mathbf{Z}$. This yields $\mathcal{P}(\mathbf{Z}_{(p)}) \cong \mathbf{Z}$, and as we have $\mathcal{I}(\mathbf{Z}) = \mathbf{Q}^*/\mathbf{Z}^* = \mathbf{Q}^*/\{\pm 1\}$, theorem 2.14 yields an isomorphism

$$\mathbf{Q}^*/\{\pm 1\} \xrightarrow{\sim} \bigoplus\nolimits_{p \text{ prime}} \mathbf{Z} \qquad \text{with} \quad x \longmapsto (\mathrm{ord}_p(x))_p.$$

Looking at the definition of the function ord_p, this can be stated as: every non-zero rational number can uniquely be written as a product $\pm\prod_p p^{n_p}$, where $n_p = 0$ for almost all p.

There are more classical formulations of theorem 2.14 that work with integral ideals only, and replace the localization $I_\mathfrak{p}$ of an integral invertible R-ideal at a prime $\mathfrak{p}$ by the $\mathfrak{p}$-*primary part*

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

of I. This is an integral R-ideal with localization $I_\mathfrak{p}$, and we have $I_{(\mathfrak{p})} = R$ if $\mathfrak{p}$ does not divide I. At the primes $\mathfrak{p}$ dividing I, we have $\mathfrak{p}^n \subset I_{(\mathfrak{p})} \subset \mathfrak{p}$ for some $n \geq 0$ as $I_\mathfrak{p}$ contains some power of the maximal ideal in $R_\mathfrak{p}$ by 2.13. In particular, no prime $\mathfrak{q} \neq \mathfrak{p}$ divides the $\mathfrak{p}$-primary part of I, and the primary parts of I at distinct primes are coprime. As I is the intersection of its localizations, we have

$$I = R \cap \bigcap\nolimits_\mathfrak{p} I_\mathfrak{p} = \bigcap\nolimits_\mathfrak{p} I_{(\mathfrak{p})} = \bigcap\nolimits_{\mathfrak{p} \supset I} I_{(\mathfrak{p})}.$$

The coprimality of the various $\mathfrak{p}$-primary parts shows that the last intersection can be written as a product, where the convention is that empty ideal products and empty ideal intersections are taken equal to R. This yields the following.

2.16. Theorem. *Let R be a number ring. Then every integral ideal $I \in \mathcal{I}(R)$ has a primary decomposition $I = \prod_{\mathfrak{p} \supset I} I_{(\mathfrak{p})}$.* □

The study of $\mathfrak{p}$-primary ideals in R and ideals in the local ring $R_\mathfrak{p}$ is essentially the same, as we have a natural isomorphism

$$R/I_{(\mathfrak{p})} \xrightarrow{\sim} R_\mathfrak{p}/I_\mathfrak{p}.$$

Indeed, injectivity of the natural map is clear from the definition of $I_{(\mathfrak{p})}$. For the surjectivity, one needs to show that every $s \in R \setminus \mathfrak{p}$ is a unit in $R/I_{(\mathfrak{p})}$. To see this, one observes that by the maximality of $\mathfrak{p}$, there exists 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, the element $ss' - 1$ is nilpotent in $R/I_{(\mathfrak{p})}$. It follows that ss' and therefore s are in $(R/I_{(\mathfrak{p})})^*$.

▶ Local number rings

Whether one prefers 2.14 or the integral version 2.16, either of these theorems reduces the study of invertible R-ideals to the study of principal ideals in *local* number rings. Unique prime ideal factorization for the number ring R is obtained exactly when all primes $\mathfrak{p}$ of R are invertible.

2.17. Theorem. *Let $\mathfrak{p}$ be a prime of a number ring R. Then the 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 $k \in \mathbf{Z}$.*

Proof. For (1) ⇒ (2), we use 2.7.(2) 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

$$R_\mathfrak{p} \supset \mathfrak{p}R_\mathfrak{p} = (\pi) \supset (\pi^2) \supset (\pi^3) \supset \dots$$

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 $\pi \in R_\mathfrak{p}^*$. Let now $I \neq 0$ be an integral $R_\mathfrak{p}$-ideal. As I contains all sufficiently large powers of (π) by 2.13, 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 $I = (\pi^n)$. We conclude that $R_\mathfrak{p}$ is a principal ideal domain, and that every $R_\mathfrak{p}$-ideal is a power of (π).

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

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

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

This shows that $R_\mathfrak{p}$ is a local ring with principal maximal ideal (π), so by 2.7 we see that $\mathfrak{p}$ is invertible. □

A local ring $R_\mathfrak{p}$ satisfying the equivalent conditions (2) and (3) of 2.17 is called a *discrete valuation ring*. The terminology is explained by the existence of the homomorphism $v : K^* \to \mathbf{Z}$ in (3) that sends x to $\mathrm{ord}_\mathfrak{p}(x)$. As the notation suggests, this homomorphism does not depend on the choice of π, and it satisfies

$$(*) \qquad v(x+y) \geq \min(v(x), v(y))$$

for any two elements $x, y \in K^*$ with $x + y \neq 0$. A non-zero homomorphism $v : K^* \to \mathbf{Z}$ satisfying $(*)$ is called a *discrete valuation*. One usually extends v to K by setting $v(0) = +\infty$. With this convention, inequality $(*)$ holds unrestrictedly for $x, y \in K$. Every discrete valuation v on K gives rise to a discrete valuation ring $R_v \subset K$ with maximal ideal $\mathfrak{m}_v$ given by

$$R_v = \{x \in K : v(x) \geq 0\} \quad \text{and} \quad \mathfrak{m}_v = \{x \in K : v(x) > 0\}.$$

We have a canonical isomorphism $\mathcal{I}(R_v) = \mathcal{P}(R_v) \xrightarrow{\sim} \mathbf{Z}$ that maps $\mathfrak{m}_v$ to 1.

Exercise 7. Show that for $x, y \in K$ with valuations $v(x) \neq v(y)$, one has $v(x+y) = \min(v(x), v(y))$.

A number ring R that is not a number field, or, more generally, a one-dimensional noetherian domain R is called a *Dedekind domain* if for every prime $\mathfrak{p}$ of R, the local ring $R_\mathfrak{p}$ is a discrete valuation ring. In number rings R that are Dedekind, *every* non-zero ideal is invertible, and we obtain unique prime ideal factorization.

2.18. Theorem. *Let R be a number ring that is Dedekind. Then there is an isomorphism*

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

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

If R is Dedekind, $\mathrm{Pic}(R)$ is often called the *class group* of R and denoted by $\mathrm{Cl}(R)$.

It may seem hard to check in practice whether a number ring is Dedekind, since this imposes a condition at each prime of R. In the next section, we will see how to do this for orders of the form $R = \mathbf{Z}[\alpha]$. More generally, we will see that every number ring R is a subring of finite index of its *normalization* $\widetilde{R} \supset R$. The ring $\widetilde{R}$ is a Dedekind domain, and $R_\mathfrak{p}$ is a discrete valuation ring at all primes $\mathfrak{p}$ of R that do not divide the index $[\widetilde{R} : R]$.

Exercises.

8. Let R be a principal ideal domain different from a field, and x, $y \in R$. Prove that x and y are coprime if and only if there does not exist a prime element of R that divides both x and y. Show that this statement is incorrect if "principal ideal domain" is replaced by "unique factorization domain".

9. Let R be a domain. Call an ideal $I \subset R$ invertible if there exists an ideal $J \subset R$ such that IJ is a non-zero principal R-ideal. Show that the relation

$$I \sim I' \iff \text{there exist non-zero elements } x, y \in R \text{ such that } xI = yI'$$

is an equivalence relation on the set D of invertible R-ideals, and that the set of equivalence classes can be identified with $\mathrm{Pic}(R)$.
[This shows that $\mathrm{Pic}(R)$ can be defined in terms of 'ordinary' R-ideals.]

10. Let R be a domain. Prove that the ideal quotient of fractional R-ideals satisfies the following properties:

$$H : (I \cdot J) = (H : I) : J \qquad (\textstyle\bigcap_k I_k) : J = \bigcap_k (I_k : J) \qquad I : (\sum_k J_k) = \bigcap_k (I : J_k).$$

11. Let R be a principal ideal domain with field of fractions K, and let $a, b \in K^*$. Show that we can write $a = u \prod_p p^{n(p)}$ and $b = v \prod_p p^{m(p)}$, where u, v are units of R, the elements p range over a finite set of pairwise non-associate prime elements of R, and $n(p)$, $m(p)$ are integers. Prove that $Ra \cap Rb = Rc$, where $c = \prod_p p^{\max\{n(p), m(p)\}}$, and that $Ra + Rb = Rd$, where $d = \prod_p p^{\min\{n(p), m(p)\}}$. Are these statements correct for unique factorization domains?

12. Let R be a domain and I an invertible R-ideal. Show that I is proper, i.e. it has multiplier ring $r(I) = R$. Deduce that an additive subgroup $I \subset K = Q(R)$ is an invertible ideal for at most one subring of K.

13. Consider the integral ideal $I = (2, 1 + \sqrt{-19}) \subset R = \mathbf{Z}[\sqrt{-19}]$. Show that I is a maximal R-ideal with multiplier ring $r(I) \neq R$, and that it satisfies $I^2 = 2I$. Conclude that I is not an invertible R-ideal, and that $2R$ is not a product of prime ideals in R.

14. Let R be a local domain. Show that a fractional R-ideal is invertible if and only if it is principal. Deduce that $\mathrm{Pic}(R)$ is trivial.

15. Denote by $\sqrt{-3}$ the complex number $i\sqrt{3}$.
    a. Prove that for every $x \in \mathbf{C}$ there exists $r \in \mathbf{Z}[\sqrt{-3}]$ with $|x - r| \leq 1$, and determine for which x the equality sign is needed.
    b. Prove that every fractional $\mathbf{Z}[\sqrt{-3}]$-ideal is either of the form $\mathbf{Z}[\sqrt{-3}]a$ or of the form $\mathbf{Z}[(1 + \sqrt{-3})/2]a$, with $a \in \mathbf{Q}(\sqrt{-3})$.
    c. Prove that $\mathbf{Z}[\sqrt{-3}]$ is not a principal ideal domain, and that its Picard group is trivial.
    d. Prove that $\mathrm{Pic}\,\mathbf{Z}[(1 + \sqrt{-3})/2]$ is trivial.

16. Let R be a noetherian domain. Show that every non-zero element of $R \setminus R^*$ can be written as a product of irreducible elements.

17. Show that $(2, 3 + \sqrt{-61})$ and $(5, 3 + \sqrt{-61})$ are invertible ideals in $\mathbf{Z}[\sqrt{-61}]$, and determine the order of their classes in $\mathrm{Pic}(\mathbf{Z}[\sqrt{-61}])$.

18. Let it be given that $\mathrm{Pic}(\mathbf{Z}[\sqrt{-19}])$ is a finite group of order 3. Use this to find all integral solutions of the equation $x^2 + 19 = y^5$.

19. Let τ be a zero of an irreducible polynomial $aX^2 + bX + c \in \mathbf{Z}[X]$. Show that $R = \mathbf{Z}[a\tau]$ is an order in the quadratic field $\mathbf{Q}(\sqrt{b^2 - 4ac})$, and that $I = \mathbf{Z} + \mathbf{Z}\tau$ is an invertible R-ideal. [Hint: compute $I \cdot \sigma(I)$, where σ is the non-trivial automorphism of $\mathbf{Q}(\sqrt{b^2 - 4ac})$.]

20. Let $f \in \mathbf{Z}[X]$ be a monic irreducible polynomial of degree 3, and $A = \mathbf{Z}[\alpha]$ the cubic order generated by a root α of f.
    a. For p a prime number, show that $R = \mathbf{Z} + pA$ is a subring of A.
    b. Prove that $I = R + R\alpha$ is a fractional R-ideal with multiplier ring $r(I) = R$.
    c. Show that we have $r(I^2) = A$, and deduce that the R-ideal I is proper but *not* invertible.

21. Let R be a number ring with field of fractions K. Show that for every prime ideal $I \neq 0$ of R, the order of R/I equals p^k for a prime number p and an integer $k \leq [K : \mathbf{Q}]$.

22. Let $B > 0$ be a real number. Show that a number ring has only finitely many ideals of index at most B.

23. Let R be a ring and $\mathfrak{p}$ a prime ideal that contains a finite product of ideals $\prod_i \mathfrak{a}_i$. Show that $\mathfrak{p}$ contains some $\mathfrak{a}_i$. Do you recognize the statement for $R = \mathbf{Z}$?

24. Let R be a ring and $\mathfrak{a}$ an ideal that is contained in a finite union of prime ideals $\bigcup_i \mathfrak{p}_i$. Show that $\mathfrak{a}$ is contained in some $\mathfrak{p}_i$.
    [This is called *prime avoidance*: if $\mathfrak{a}$ contains an element outside $\mathfrak{p}_i$ for $i = 1, 2, \ldots, n$, then it contains an element that does not lie in any $\mathfrak{p}_i$.]

25. Let R be a number ring and $I \subset R$ an invertible R-ideal. Show that I is a product of prime ideals if and only if all primes $\mathfrak{p} \supset I$ are invertible.

26. Show that the following properties of a ring R are equivalent.
    (1) R is noetherian;
    (2) every ascending chain of ideals $I_1 \subset I_2 \subset I_3 \subset \ldots$ in R stabilizes;
    (3) every non-empty collection of ideals of R has a maximal element with respect to inclusion.

27. Let R be a noetherian ring and $I \subsetneq R$ an R-ideal. Show that there exist prime ideals $\mathfrak{p}_1, \mathfrak{p}_2, \ldots, \mathfrak{p}_n$ of R that contain I and satisfy $\prod_{i=1}^n \mathfrak{p}_i \subset I$. Show also that the ideals $\mathfrak{p}_i$ can be chosen such that no strict inclusions between them occur, and that with this choice, the *set* $\{\mathfrak{p}_1, \mathfrak{p}_2, \ldots, \mathfrak{p}_n\}$ is uniquely determined by I and consists of the minimal elements in the collection of prime ideals containing I.
    [Hint: noetherian induction.]

28. A ring is said to be *reduced* if its nilradical $N = \{x \in R : x^n = 0 \text{ for some } n > 0\}$ is the zero-ideal. Show that a reduced noetherian ring can be embedded as a subring in a finite product of noetherian domains.
    [Hint: apply the previous exercise to $I = 0$.]

*29. Let R be a domain, and suppose that every prime ideal of R is principal. Prove that R is a principal ideal domain.
    [Hint: show that the collection of non-principal ideals in any ring has maximal elements if it is non-empty, and that these are prime ideals.]

30. Let S be a multiplicatively closed subset of a domain A. Show that a ring homomorphism $\phi : A \to B$ factors via $S^{-1}A$ if and only if $\phi[S]$ is contained in B^*.
    [This is the characterizing *universal property* of localizations.]

31. Let R be a number ring. Prove that the localization of fractional R-ideals satisfies the following properties:

$$I_\mathfrak{p} + J_\mathfrak{p} = (I + J)_\mathfrak{p} \qquad I_\mathfrak{p} J_\mathfrak{p} = (IJ)_\mathfrak{p} \qquad I_\mathfrak{p} \cap J_\mathfrak{p} = (I \cap J)_\mathfrak{p}.$$

32. Let R be a domain with fractional ideals I and J, and suppose that J is finitely generated. Show that we have

$$I_\mathfrak{p} : J_\mathfrak{p} = (I : J)_\mathfrak{p}$$

    for every prime ideal $\mathfrak{p}$ of R. Deduce that a finitely generated R-ideal is invertible if and only if it is locally everywhere invertible.
    [This shows that for noetherian domains R, invertibility of R-ideals is a *local property*.]

33. Define $M \subset \mathbf{Q}$ by $M = \{\frac{a}{b} \in \mathbf{Q} : b \text{ is squarefree}\}$. Show that M is a sub-$\mathbf{Z}$-module of $\mathbf{Q}$, and that for every prime p of $\mathbf{Z}$, the localization $S_p^{-1}M$ is a principal $S_p^{-1}\mathbf{Z}$-ideal, with $S_p = \mathbf{Z} \setminus p\mathbf{Z}$. Is M an invertible $\mathbf{Z}$-ideal? If not, is there a subring $R \subset \mathbf{Q}$ for which M is an invertible R-ideal?
    In a similar way, determine for q a prime number and $M_q = \{\frac{a}{b} \in \mathbf{Q} : b \text{ is a power of } q\} \subset \mathbf{Q}$ whether each localization $S_p^{-1}M_q$ is a principal $S_p^{-1}\mathbf{Z}$-ideal. Is there a subring $R \subset \mathbf{Q}$ such that M_q is an invertible R-ideal?

34. Show that $S = 1 + p\mathbf{Z}$ is a multiplicative subset of $\mathbf{Z}$, and that $S^{-1}\mathbf{Z}$ is the local ring $\mathbf{Z}_{(p)}$ occurring in 2.15. Thus different S can yield the same localization. *Can you describe when two multiplicative subsets of a domain give rise to the same localization?
    [Hint: [9, exercise 3.7]]

35. Find for each prime $\mathfrak{p}$ in $R = \mathbf{Z}[\sqrt{-61}]$ a local generator at $\mathfrak{p}$ of the non-principal R-ideals $(2, 3+\sqrt{-61})$ and $(5, 3+\sqrt{-61})$.

36. For $R = \mathbf{Z}[\sqrt{-3}]$ and $x = (1+\sqrt{-3})/2$, show that $I = Rx$ is a fractional R-ideal that is non-integral and satisfies $I^3 = R$. Deduce that $\mathcal{I}(R)$ has a non-trivial torsion subgroup, and that R is not a Dedekind domain. Find a non-invertible R-ideal.

37. Show that the polynomial ring $\mathbf{C}[X]$ is a Dedekind domain and identify its primes. Make theorem 2.14 as explicit for this ring as we did for the ring $\mathbf{Z}$. Same questions for the polynomial ring $K[X]$ over an arbitrary field K.

38. Show that every localization $S^{-1}R$ of a Dedekind domain R different from $Q(R)$ is again a Dedekind domain. Is the same true for quotient rings R/I with $I \neq R$?

39. Show that R is a principal ideal domain if and only if R is a Dedekind domain with $\mathrm{Pic}(R) = 0$.

40. Let R be a discrete valuation ring for which the residue class field is finite. Prove that the function $N : I \mapsto [R : I]$ is a function on the set of non-zero R-ideals with values in $\mathbf{Z}_{>0}$ that satisfies $N(I \cdot J) = N(I)N(J)$.

41. Let R be a number ring that is Dedekind. Show that the norm function $N : I \mapsto [R : I]$ on R-ideals extends to a homomorphism $N : \mathcal{I}(R) \to \mathbf{Q}^*$. Is this also true for arbitrary number rings?

42. *(Semi-local rings.)* A *semi-local* ring is by definition a ring with only finitely many maximal ideals. Show that for $\mathfrak{p}_1, \mathfrak{p}_2, \ldots, \mathfrak{p}_n$ prime ideals of a ring R, the set $S = R \setminus \bigcup_{i=1}^{n} \mathfrak{p}_i$ is multiplicatively closed and the localization $S^{-1}R$ is a semi-local ring. Show also that for R a number ring and $I \neq 0$ any ideal, the quotient ring R/I is semi-local.
[Hint: exercise 23.]

43. Show that $\mathrm{Pic}(R)$ is trivial if R is a semi-local domain.
[Hint: By the Chinese remainder theorem there exist $e_{\mathfrak{m}} \in R$ such that $e_{\mathfrak{m}} \equiv 1 \bmod \mathfrak{m}$ and $e_{\mathfrak{m}} \in \mathfrak{n}$ if $\mathfrak{m} \neq \mathfrak{n}$. Choose $x_{\mathfrak{m}} \in I \setminus \mathfrak{m}I$ for each maximal $\mathfrak{m}$. Now show that $\sum_{\mathfrak{m}} x_{\mathfrak{m}} e_{\mathfrak{m}}$ generates I.]

44. Let R be a finite ring. Show that the unit group R^* has order

$$\#R^* = \#R \cdot \prod_{\mathfrak{p}} \left(1 - \frac{1}{\#(R/\mathfrak{p})}\right).$$

Here $\mathfrak{p}$ ranges over the prime ideals of R.

45. *(Approximation theorem.)* Let X be a finite set of primes of a Dedekind domain R, and suppose we are given an integer $n_{\mathfrak{p}}$ for each $\mathfrak{p} \in X$. Show there exists $x \in K = Q(R)$ such that

$$\begin{aligned} \mathrm{ord}_{\mathfrak{p}}(x) &= n_{\mathfrak{p}} \qquad \text{if } \mathfrak{p} \in X \\ \mathrm{ord}_{\mathfrak{p}}(x) &\geq 0 \qquad \text{if } \mathfrak{p} \notin X. \end{aligned}$$

[Hint: use the Chinese remainder theorem if all $n_{\mathfrak{p}}$ are positive. For the general case, apply this special case twice.]

46. Show that every ideal in a Dedekind domain can be generated by 2 elements.

47. Let X be a finite set of primes of a Dedekind domain R. Show that $\mathrm{Cl}(R)$ is generated by the classes of the primes of R that are not in X. (In particular, no generators are needed if R is semi-local.)

48. An ideal $I \neq R$ of a ring R is called *primary* if it satisfies the implication

$$xy \in I \quad \Rightarrow \quad x \in I \text{ or } y^n \in I \text{ for some } n \geq 0.$$

Show that the radical of a primary ideal is a prime ideal, and that the $\mathfrak{p}$-primary part $I_{(\mathfrak{p})}$ of an ideal I in 2.16 is a primary ideal with radical $\mathfrak{p}$.

49. *(Valuation rings.)* A subring R of a field K is said to be a *valuation ring* of K if for each $x \in K^*$, we have either $x \in R$ or $x^{-1} \in R$ (or both). Show that every valuation ring is a local ring, and that a discrete valuation ring is indeed a valuation ring.

50. Let $\mathbf{C}(X)$ be the field of rational functions with complex coefficients. For $\alpha \in \mathbf{C}$, define $\mathrm{ord}_\alpha(f)$ for a non-zero polynomial $f \in \mathbf{C}[X]$ as the order of the zero of f at α and set $\mathrm{ord}_\infty(f) = -\deg(f)$. Show that these maps extend to normalized valuations on $\mathbf{C}(X)$, and determine the corresponding valuation rings R_α and R_∞. Describe $\bigcap_{\alpha\in\mathbf{C}} R_\alpha$ and $(\bigcap_{\alpha\in\mathbf{C}} R_\alpha)\cap R_\infty$?

51. Show that *every* normalized valuation v on $\mathbf{C}(X)$ for which $v[\mathbf{C}^*] = 0$ is equal to one of the valuations from the previous exercise. Deduce that every $f \in \mathbf{C}(X)^*$ satisfies the sum formula $\sum_v v(f) = 0$, where the sum is taken over all v.
[Hint: if $v(X) \geq 0$ one has $\mathbf{C}[X] \subset R_v$ and $\mathfrak{m}_v \cap \mathbf{C}[X]$ is a prime ideal of $\mathbf{C}[X]$. Otherwise look at $1/X$.]

52. Show that every normalized valuation v on $\mathbf{Q}$ is of the form $v(x) = v_p(x) = \mathrm{ord}_p(x)$ for some prime number p.

53. Let v be a discrete valuation on a field K and R_v the corresponding discrete valuation ring. Show that the *v-adic metric*

$$d(x, y) = 2^{-v(x-y)}$$

on $K \times K$ defines a distance function on K, and that the induced *v-adic topology* makes K into a totally disconnected Hausdorff space. Is R_v closed in K?

54. Let K and v be as in the previous exercise. Show that with respect to the v-adic topology, addition and multiplication yield continuous maps $K \times K \to K$, and $x \mapsto x^{-1}$ is a continuous map on K^*. Use this to construct a *v-adic completion* K_v of K and show that K_v is a complete topological field, i.e. a field that is a complete metric space and in which all field operations are continuous.
[Hint: as when constructing $\mathbf{R}$ from $\mathbf{Q}$, let K_v be the set of equivalence classes of Cauchy sequences in K with respect to the v-adic metric.]

55. Describe the completions of $\mathbf{C}(X)$ with respect to the valuations ord_α and ord_∞.
[Hint: one obtains Laurent series in $X - \alpha$ and X^{-1}.]

56. *(Approximation theorem revisited.)* Let X be a finite set of primes of a Dedekind domain R with field of fractions K, and suppose that we are given an integer $n_\mathfrak{p}$ and an element $x_\mathfrak{p} \in K^*$ for each $\mathfrak{p} \in X$. Show that there exists $x \in K^*$ such that

$$\begin{aligned} \mathrm{ord}_\mathfrak{p}(x - x_\mathfrak{p}) &= n_\mathfrak{p} \qquad \text{if } \mathfrak{p} \in X; \\ \mathrm{ord}_\mathfrak{p}(x) &\geq 0 \qquad \text{if } \mathfrak{p} \notin X. \end{aligned}$$

Deduce that the image of K in $\prod_{\mathfrak{p}\in X} K$ under the diagonal embedding is dense if the topology on the product is obtained by giving the $\mathfrak{p}$-th component the topology coming from the $\mathfrak{p}$-adic valuation.

*57. *(p-adic numbers.)* If the completion process in the previous exercises is carried through for the field $\mathbf{Q}$ and the p-adic valuation $v = \mathrm{ord}_p$ associated to a prime number p, one obtains the p-adic number field $\mathbf{Q}_p$. The closure of $\mathbf{Z}$ in $\mathbf{Q}_p$ is the ring of p-adic integers $\mathbf{Z}_p$. Show that $\mathbf{Z}_p$ is a closed subring of $\mathbf{Q}_p$, and that we have a (topological) isomorphism

$$\mathbf{Q}_p^* \cong \langle p \rangle \times \mathbf{Z}_p^*$$

in which $\langle p \rangle \cong \mathbf{Z}$ has the discrete topology. Show that every element $x \in \mathbf{Z}_p$ has a unique representation

$$x = \textstyle\sum_{k=0}^{\infty} a_k p^k$$

in which the 'p-adic digits' a_k are chosen from the set $\{0, 1, 2, \ldots, p-1\}$.

3 Explicit ideal factorization

In order to factor an ideal I in a number ring R in the sense of 2.16, we have to determine for all prime ideals $\mathfrak{p} \supset I$ the $\mathfrak{p}$-primary part $I_{(\mathfrak{p})}$ of I. As I is of finite index in R, a prime $\mathfrak{p}$ of R divides the integer $[R : I]$, hence a prime number p. We have $\mathfrak{p} \cap \mathbf{Z} = p\mathbf{Z}$ for this prime number p, and one says that $\mathfrak{p}$ *extends* p or *lies above* or *over* p. The first step in factoring I consists of determining the primes $\mathfrak{p}$ of R lying over the primes p dividing $[R : I]$, and deciding which of them divide I. At the *regular* primes of R, i.e., the primes $\mathfrak{p}$ that are invertible, $I_{(\mathfrak{p})}$ is a power of $\mathfrak{p}$. If $\mathfrak{p}$ is non-invertible or *singular*, the situation can be more complicated.

For given p, there are only finitely many primes $\mathfrak{p}$ of R that extend p, and these $\mathfrak{p}$ correspond to the maximal ideals of the finite ring R/pR. If $\mathfrak{p}$ extends p, the degree $f(\mathfrak{p})$ of the field extension $\mathbf{F}_p \subset R/\mathfrak{p}$ is the *residue class degree* of $\mathfrak{p}$. One also says that $\mathfrak{p}$ is an ideal of *norm* $p^{f(\mathfrak{p})}$.

▶ The Kummer-Dedekind theorem

A *simple integral* extension of $\mathbf{Z}$ is a number ring of the form $\mathbf{Z}[\alpha]$, with α a zero of a monic irreducible polynomial $f \in \mathbf{Z}[X]$. Every number ring R contains subrings of this nature, and if there is a subring $\mathbf{Z}[\alpha] \subset R$ that maps surjectively to R/pR, it suffices to determine the primes over p in $\mathbf{Z}[\alpha]$ in order to obtain them in R.

Exercise 1. Show that for such $\mathbf{Z}[\alpha]$, the local rings at the primes over p in $\mathbf{Z}[\alpha]$ and R are 'the same'.

The Kummer-Dedekind theorem determines the explicit form and the regularity of the primes lying over p in number rings $\mathbf{Z}[\alpha]$.

3.1. Theorem (Kummer-Dedekind). *Let $f \in \mathbf{Z}[X]$ be a monic irreducible polynomial, $\alpha \in \overline{\mathbf{Q}}$ a zero of f and p a prime number. Let R be the ring $\mathbf{Z}[\alpha] = \mathbf{Z}[X]/(f)$, and choose monic polynomials $g_i \in \mathbf{Z}[X]$ such that the factorization of f modulo p is*

$$\overline{f} = \prod_{i=1}^{s} \overline{g}_i^{e_i} \in \mathbf{F}_p[X]$$

with $e_i \in \mathbf{Z}_{\geq 1}$ and the irreducible polynomials $\overline{g}_i = (g_i \bmod p) \in \mathbf{F}_p[X]$ pairwise distinct. Then the following holds:

(1) *the prime ideals of R that lie above p are the ideals $\mathfrak{p}_i = pR + g_i(\alpha)R$, and we have an inclusion $\prod_{i=1}^{s} \mathfrak{p}_i^{e_i} \subset pR$;*
(2) *the equality $pR = \prod_{i=1}^{s} \mathfrak{p}_i^{e_i}$ holds if and only if every prime $\mathfrak{p}_i$ is invertible;*
(3) *writing $r_i \in \mathbf{Z}[X]$ for the remainder of f upon division by g_i, one has*

$$\mathfrak{p}_i \text{ is singular } \iff e_i > 1 \text{ and } p^2 \text{ divides } r_i \in \mathbf{Z}[X].$$

Proof. (1) The ring $\mathbf{F}_p[X]$ is a principal ideal domain, so we see from the isomorphism $R/pR \cong \mathbf{F}_p[X]/(\overline{f})$ that the primes of R that lie above p correspond bijectively to the monic irreducible divisors $\overline{g}|\overline{f}$ in $\mathbf{F}_p[X]$. The prime $\mathfrak{p}_i|p$ corresponding to a factor $\overline{g}_i$ is

$$\mathfrak{p}_i = \ker[\psi_i : R \longrightarrow \mathbf{F}_p[X]/(\overline{g}_i)] = pR + g_i(\alpha)R.$$

Here ψ_i maps $t(\alpha) \in \mathbf{Z}[\alpha]$ to $\overline{t}$ mod $\overline{g}_i$, so we have

$$t(\alpha) \in \mathfrak{p}_i \Longleftrightarrow \overline{g}_i | \overline{t} \in \mathbf{F}_p[X].$$

The isomorphism $R/\mathfrak{p}_i \xrightarrow{\sim} \mathbf{F}_p[X]/(\overline{g}_i)$ induced by ψ_i shows that the residue class degree $f(\mathfrak{p}_i/p)$ is equal to the degree of g_i. As $\prod_{i=1}^s g_i(\alpha)^{e_i}$ is in $f(\alpha)+pR = pR$, we get the desired inclusion $\prod_{i=1}^s \mathfrak{p}_i^{e_i} \subset pR + \prod_{i=1}^s g_i(\alpha)^{e_i} R \subset pR$.

(2) If the inclusion in (1) is an equality, every $\mathfrak{p}_i$ is invertible as it divides the principal ideal pR in the strict sense of Kummer: we have $\mathfrak{p}_i \cdot I = pR$ for some ideal I. As R is an order of rank $\deg f$, the index of pR in R equals $p^{\deg f}$. Conversely, suppose that all primes $\mathfrak{p}_i$ over p are invertible, i.e. that the rings $R_{\mathfrak{p}_i}$ are discrete valuation rings. As we already have an inclusion, it suffices to show that $I = \prod_{i=1}^s \mathfrak{p}_i^{e_i}$ also has index $p^{\deg f}$ in R. By the Chinese remainder theorem, we have $\#(R/I) = \prod_{i=1}^s \#(R_{\mathfrak{p}_i}/\mathfrak{p}_i^{e_i} R_{\mathfrak{p}_i})$. From the description in 2.17 it is clear that all quotients $\mathfrak{p}_i^k R_{\mathfrak{p}_i}/\mathfrak{p}_i^{k+1} R_{\mathfrak{p}_i}$ in the discrete valuation ring $R_{\mathfrak{p}_i}$ are isomorphic (as R-modules) to the residue class field $R_{\mathfrak{p}_i}/\mathfrak{p}_i R_{\mathfrak{p}_i}$ of order $p^{\deg g_i}$, so the quotient ring $R_{\mathfrak{p}_i}/\mathfrak{p}_i^{e_i} R_{\mathfrak{p}_i}$ has order $p^{e_i \deg g_i}$. It follows that R/I has order p^n with $n = \sum_{i=1}^s e_i \deg(g_i)$. Comparing degrees in the factorisation $\overline{f} = \prod_{i=1}^s \overline{g}_i^{e_i}$ shows that we have $n = \deg(f)$, as was to be shown.

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

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

between the two R-generators p and $g_i(\alpha)$ of $\mathfrak{p}_i$.

Suppose that $\overline{g}_i$ occurs with exponent $e_i = 1$ in $\overline{f}$. Then $\overline{q}_i$ is not divisible by $\overline{g}_i$ in $\mathbf{F}_p[X]$, and this means that $q_i(\alpha)$ is not in $\mathfrak{p}_i$. It follows that $q_i(\alpha)$ is in $R_{\mathfrak{p}_i}^*$, so we have $g_i(\alpha) \in pR_{\mathfrak{p}_i}$, and $R_{\mathfrak{p}_i}$ is a discrete valuation ring with maximal ideal generated by p.

Similarly, the hypothesis $r_i = p s_i \notin p^2 \mathbf{Z}[X]$ means that $\overline{s}_i \in \mathbf{F}_p[X]$ is non-zero of degree $\deg(\overline{s}_i) < \deg(\overline{g}_i)$. This implies $\overline{g}_i \nmid \overline{s}_i$ and that $s_i(\alpha)$ is a unit in $R_{\mathfrak{p}_i}$. In this situation $R_{\mathfrak{p}_i}$ is a discrete valuation ring with discrete valuation ringring!discrete valuationmaximal ideal generated by $g_i(\alpha)$.

If we have both $e_i \geq 2$ and $r_i \in p^2 \mathbf{Z}[X]$, then $q_i(\alpha)$ and $s_i(\alpha)$ are both in $\mathfrak{p}_i$, and $\mathfrak{p}_i$ is not invertible as it is not locally principal. In fact, it is not a proper R-ideal as the element $p^{-1} q_i(\alpha)$ is in $r(\mathfrak{p}_i)$ but not in R: it satisfies

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

This finishes the proof of 3.1. □

3.2. Corollary. *Suppose we have $f = q_i \cdot g_i + r_i$ in 3.1.(c), and that $\mathfrak{p}_i$ is singular. Then $\frac{1}{p} q_i(\alpha)$ is in the multiplier ring of $\mathfrak{p}_i$ but not in $\mathbf{Z}[\alpha]$.*

We call a number ring R *singular* above a rational prime p if p has a singular extension in R, and *regular* above p if all extensions are regular.

Suppose that R is regular above p. Then p is called *inert* in R if p is a prime element in R, i.e. if pR is the unique prime of R lying above p. If there are different extensions of p, then p is said to *split* in R. If there is an extension $\mathfrak{p}|p$ that occurs with multiplicity $e > 1$, we say that p *ramifies* in R, or that R is *ramified above* p. The multiplicity with which a prime $\mathfrak{p}|p$ occurs in p is the *ramification index* of $\mathfrak{p}$ over p.

Exercise 2. Show that $\mathbf{Z}[\alpha]$ is regular above p if and only if the semi-local ring $\mathbf{Z}_{(p)}[\alpha]$ is Dedekind.

3.3. Example. Take $R = \mathbf{Z}[\alpha]$ with α a zero of the polynomial $f = X^3 + X + 1$. The factorizations

$$f = X^3 + X + 1 \pmod 2$$
$$f = (X-1)(X^2 + X - 1) \pmod 3$$

show that 2 is inert in R, whereas 3 splits into prime ideals $(3, \alpha - 1)$ and $(3, \alpha^2 + \alpha - 1)$ of norm 3 and 9. If f has multiple factors modulo a prime $p > 3$, then f and $f' = 3X^2 + 1$ have a common factor modulo this prime p, and this is the linear factor $f - (X/3)f' = \frac{2}{3}X + 1$ with zero $X = -3/2$. As we have $\overline{f}'(-3/2) = \overline{31/4} = \overline{0}$ only for $p = 31$, this is the unique prime for which $\overline{f}$ has multiple factors. Modulo 31, we find

$$f = (X - 14)^2(X - 3) \pmod{31},$$

and the remainder of f upon division by $X - 14$ is $f(14) = 2759 = 31 \cdot 89$. As 89 is not divisible by 31, the prime $(31, \alpha - 14)$ is regular. It follows that *all* primes of R are regular, so R is a Dedekind domain. The prime 31, which has factorization

$$31R = (31, \alpha - 14)^2(31, \alpha - 3)$$

in R, is the only rational prime that ramifies in R. The reader may check that $p = 47$ is the smallest rational prime that splits into 3 primes in $\mathbf{Z}[\alpha]$.

Example 3.3 shows that in number rings $\mathbf{Z}[\alpha]$, there is a simple relation between the residue class degrees and ramification indices of the primes above a regular rational prime. The same relation holds for arbitrary orders.

3.4. Theorem. *Let R be an order in a number field K. If R is regular above a rational prime p, we have*

$$\sum_{\mathfrak{p}|p} e(\mathfrak{p}) f(\mathfrak{p}) = [K : \mathbf{Q}].$$

Here the sum ranges over the primes of R extending p, and $e(\mathfrak{p})$ and $f(\mathfrak{p})$ denote the ramification index and residue class degree of $\mathfrak{p}$ over p.

Proof. Write $n = [K : \mathbf{Q}]$, then R is of rank n and R/pR has order p^n. Factoring pR as $pR = \prod_{\mathfrak{p}|p} \mathfrak{p}^{e(\mathfrak{p})}$, we can evaluate the order of $R/pR = \prod_{\mathfrak{p}|p} R/\mathfrak{p}^{e(\mathfrak{p})}$ as in the proof of 3.1 as $\prod_{\mathfrak{p}|p} p^{e(\mathfrak{p})f(\mathfrak{p})}$. The result follows. □

It follows from 3.4 that in an order R of rank n, a regular rational prime p has at most n extensions. If it has n extensions, we say that p is *totally split* in R. These extensions necessarily have $e(\mathfrak{p}) = f(\mathfrak{p}) = 1$. If a regular prime p has a unique extension $\mathfrak{p}$ in R with $e(\mathfrak{p}) = n$, it is said to be *totally ramified* in R.

▶ Singular primes

3.5. Lemma. *There are only finitely many rational primes p for which an order $\mathbf{Z}[\alpha]$ in 3.1 is ramified or singular above p.*

Proof. A prime p is ramified or singular in $\mathbf{Z}[\alpha]$ exactly when $\overline{f} = (f_{\mathbf{Q}}^{\alpha} \bmod p)$ has a multiple factor in $\mathbf{F}_p[X]$. This factor also divides the derivative $\overline{f}'$ of $\overline{f}$. As f and its derivative f' are coprime polynomials in $\mathbf{Q}[X]$, we can find an integer $k \neq 0$ and polynomials $g_1, g_2 \in \mathbf{Z}[X]$ satisfying $g_1 f + g_2 f' = k$. Reducing modulo p, we find that $\overline{f}$ and $\overline{f}'$ are coprime in $\mathbf{F}_p[X]$ unless p is one of the prime divisors of the non-zero integer k. □

Exercise 3. Show that one has $\mathbf{Z} \cap (f\mathbf{Z}[X] + f'\mathbf{Z}[X]) = 31\mathbf{Z}$ for $f = X^3 + X + 1$.

In cases where theorem 3.1 tells us that a ring $R = \mathbf{Z}[\alpha]$ is not Dedekind, 3.2 provides us with elements outside R that occur in the multiplier rings of these singular primes. Such elements can be used to enlarge the ring R into a ring with fewer singular primes.

3.6. Example. The ring $R = \mathbf{Z}[\sqrt{-19}]$ from section 1 is of the form $\mathbf{Z}[\alpha]$, with α a zero of the polynomial $f = X^2 + 19$. In this case f and $f' = 2X$ are coprime modulo all primes $p \notin \{2, 19\}$, so R is regular above these primes. The identity $19R = (\sqrt{-19})^2$ shows that R is regular and totally ramified above 19. As we have $f \equiv (X+1)^2 \bmod 2$ and the remainder of f upon division by $X + 1$ is $f(-1) = 20 \in 2^2\mathbf{Z}[X]$, the prime $\mathfrak{p}_2 = (2, \sqrt{-19} + 1)$ of norm 2 is the unique singular prime of R. Note that $\mathfrak{p}^2 = 2\mathfrak{p} \subsetneq 2R$ is of index 8 in R, and that $2R$ is not a product of prime ideals in R.

The identity $f = (X+1)(X-1) + 20$ shows that the multiplier ring of $\mathfrak{p}_2$ contains an element $\beta = (\sqrt{-19} - 1)/2 \notin R$. The extension ring $\widetilde{R} = \mathbf{Z}[\beta]$, which contains $R = \mathbf{Z}[\alpha]$ as a subring of index 2, is regular above 2 as the irreducible polynomial $X^2 + X + 5$ of β is irreducible modulo 2 and 2 is inert in $\widetilde{R}$. It is also regular above all primes $p \neq 2$, as we have $\mathbf{Z}_{(p)}[\alpha] = \mathbf{Z}_{(p)}[\beta]$ for these p. It follows that $\widetilde{R}$ is a Dedekind domain.

3.7. Example. The ring $R = \mathbf{Z}[\sqrt[3]{-19}]$ is of the form $\mathbf{Z}[\alpha]$ with α a zero of the polynomial $f = X^3 + 19$. This time f and $f' = 3X^2$ are coprime modulo all primes $p \notin \{3, 19\}$, so R is regular above these primes. The factorization $19R = (\alpha)^3$ shows that R is regular and totally ramified above 19. Modulo 3, we find

$$f = (X+1)^3 \pmod 3,$$

and the remainder of f upon division by $X + 1$ is $f(-1) = 18 \in 3^2\mathbf{Z}[X]$. It follows that the unique prime $\mathfrak{p}_3 = (3, \alpha + 1)$ above 3 is not invertible, and the identity

$$f = (X^2 - X + 1)(X + 1) + 18$$

shows that the multiplier ring of $\mathfrak{p}_3$ contains an element $\beta = (\alpha^2 - \alpha + 1)/3$ outside R. Note that we have $(\alpha + 1)\beta = -18/3 = -6$.

We claim that the ring $\widetilde{R} = R[\beta] = \mathbf{Z}[\alpha, \beta]$, which contains R as a subring of index 3, is a Dedekind domain. As we have $\mathbf{Z}_{(p)}[\alpha] = \mathbf{Z}_{(p)}[\alpha, \beta]$ at all primes $p \neq 3$, we know that $\widetilde{R}$ is regular at all primes $p \neq 3$. By elementary linear algebra, we compute the minimal polynomial of β as

$$f_{\mathbf{Q}}^{\beta} = X^3 - X^2 - 6X - 12.$$

The factorization $f_{\mathbf{Q}}^{\beta} = X^2(X-1) \bmod 3$ shows that the primes over 3 in $\mathbf{Z}[\beta]$ are $(3,\beta)$ and $(3,\beta-1)$. The prime $(3,\beta)$ is invertible as $f_{\mathbf{Q}}^{\beta}$ has remainder $-12 \notin 3^2\mathbf{Z}[X]$ upon division by X, so $\mathbf{Z}[\beta]$ is regular above 3. The relation $\alpha+1 = -6/\beta = (-\beta^2+\beta+6)/2$ shows that $\mathbf{Z}[\beta]$ is of index 2 in $\mathbf{Z}[\alpha,\beta]$, so locally at 3 we find $\mathbf{Z}_{(3)}[\beta] = \mathbf{Z}_{(3)}[\alpha,\beta]$. It follows that $\widetilde{R}$ is regular above 3 as well.

Exercise 4. Show that $\mathbf{Z}[\beta]$ is regular above all primes $p \neq 2$, and that above $p=2$, it has a a regular prime $(2,\beta+1)$ and a singular prime $(2,\beta)$ with multiplier ring $\widetilde{R}$.

The examples 3.6 and 3.7 show that singular primes of a number ring R may 'disappear' in suitable small extensions of R. Such extensions never introduce new singular primes.

3.8. Lemma. *Let $S \subset T$ be an extension of number rings such that T is contained in the field of fractions of S. Let $\mathfrak{q}$ be a prime of T for which $\mathfrak{p} = S \cap \mathfrak{q}$ is regular in S. Then $\mathfrak{q}$ is a regular prime of T, and it is the unique extension of $\mathfrak{p}$ to T.*

Proof. By assumption, the local ring $T_{\mathfrak{q}}$ at $\mathfrak{q}$ is a proper subring of $K = Q(S)$ that contains the discrete valuation ring $S_{\mathfrak{p}}$. If $T_{\mathfrak{q}}$ is strictly larger than $S_{\mathfrak{p}}$, then it is equal to K as we have $S_{\mathfrak{p}}[x] = K$ for every $x \in K \setminus S_{\mathfrak{p}}$. As the local ring at a prime of a number ring is not a field, we must have $S_{\mathfrak{p}} = T_{\mathfrak{q}}$, so $\mathfrak{q}$ is regular in T. This also shows that the prime $\mathfrak{q} \subset T$ is uniquely determined by $\mathfrak{p}$, as $\mathfrak{q} = T \cap \mathfrak{q}T_{\mathfrak{q}} = T \cap \mathfrak{p}S_{\mathfrak{p}}$. □

3.9. Theorem. *A number ring has only finitely many singular primes.*

Proof. Pick an element $\alpha \in R$ such that α generates the number field $Q(R)$ over $\mathbf{Q}$. Replacing α when necessary by an integral multiple $k\alpha$, we may assume that its irreducible polynomial $f_{\mathbf{Q}}^{\alpha}$ is in $\mathbf{Z}[X]$. Applied to the extension $\mathbf{Z}[\alpha] \subset R$, lemma 3.8 shows that if R is singular above a rational prime p, then the same is true for $\mathbf{Z}[\alpha]$. There are only finitely many such p by 3.5, and each of them has only finitely many extensions to R. □

▶ Quadratic and cyclotomic number rings

Before going into the general 'desingularization' of number rings, we apply the Kummer-Dedekind theorem to give two important examples of Dedekind domains.

3.10. Theorem. *Let $d \in \mathbf{Z}_{\neq 1}$ be squarefree and $R = \mathbf{Z}[\sqrt{d}]$ the corresponding quadratic order. Then R is a Dedekind domain for $d \equiv 2,3 \bmod 4$. For $d \equiv 1 \bmod 4$, it is singular only above 2, and the extension ring $\mathbf{Z}[\frac{1+\sqrt{d}}{2}] \supset R$ is a Dedekind domain.*

Proof. We take $f = X^2 - d$ in 3.1. If f has irreducible factors modulo p that occur with multiplicity greater than 1, then it has these factors in common with its derivative $\bar{f}' = 2X \in \mathbf{F}_p[X]$. Such factors can only exist when p divides $2d$. If p divides d, the multiple factor is X. The primes lying over p are then regular since the remainder $-d$ of f upon division by X is squarefree and therefore not in $p^2\mathbf{Z}[X]$.

If p divides $2d$ but not d, i.e., if $p=2$ and d is odd, we have $\overline{f} = (X+1)^2 \in \mathbf{F}_2[X]$. From $X^2 - d = (X-1)(X+1) + (1-d)$ we see that the remainder $1-d$ is in $4\mathbf{Z}[X]$ exactly when $d \equiv 1 \bmod 4$. We find that $\mathbf{Z}[\sqrt{d}]$ is Dedekind for $d \not\equiv 1 \bmod 4$, and that $\mathbf{Z}[\sqrt{d}]$ is singular only above 2 for $d \equiv 1 \bmod 4$.

In the case $d \equiv 1 \bmod 4$ the multiplier ring of the singular prime $(2, 1+\sqrt{d})$ contains an element $\alpha = \frac{\sqrt{d}-1}{2} \notin R$. The irreducible polynomial $(X+\frac{1}{2})^2 - \frac{d}{4} = X^2 + X + \frac{1-d}{4} \in \mathbf{Z}[X]$ of α has no multiple roots modulo 2, so the extension ring $\mathbf{Z}[\alpha] \supset R$ is regular above 2. As R is already regular above all odd primes, we find that $\mathbf{Z}[\alpha]$ is a Dedekind domain. □

By 3.1 and 3.10, the factorisation of an odd prime p in the ring $\mathbf{Z}[\sqrt{d}]$ can be found from the factorisation of $X^2 - d$ in $\mathbf{F}_p[X]$. It depends on the Legendre symbol $\left(\frac{d}{p}\right)$.

3.11. Corollary. *Let $d \neq 1$ be squarefree and p an odd prime. Then p is split in $\mathbf{Z}[\sqrt{d}]$ for $\left(\frac{d}{p}\right) = 1$, inert for $\left(\frac{d}{p}\right) = -1$ and ramified for $\left(\frac{d}{p}\right) = 0$.* □

Exercise 5. Show that 2 splits in $\mathbf{Z}[\frac{1+\sqrt{d}}{2}]$ for $d \equiv 1 \bmod 8$, and remains inert in $\mathbf{Z}[\frac{1+\sqrt{d}}{2}]$ for $d \equiv 5 \bmod 8$.

Let $\mathbf{Z}[\zeta]$ be the *cyclotomic number ring* obtained by adjoining a root of unity $\zeta \in \overline{\mathbf{Q}}$ to $\mathbf{Z}$. If $\zeta = \zeta_n$ is a primitive n-th root of unity, its irreducible polynomial over $\mathbf{Q}$ is the n-th cyclotomic polynomial Φ_n, which may be defined inductively for $n \geq 1$ by

$$X^n - 1 = \prod\nolimits_{d|n} \Phi_d(X).$$

The degree of Φ_n is $\phi(n)$, where ϕ is the Euler ϕ-function, and the factorization of Φ_n in the n-th cyclotomic field $\mathbf{Q}(\zeta)$ is

$$\Phi_n(X) = \prod\nolimits_{i \in (\mathbf{Z}/n\mathbf{Z})^*} (X - \zeta^i).$$

As $X^n - 1$ and its derivative nX^{n-1} are coprime in $\mathbf{F}_p[X]$ for all primes $p \nmid n$, the polynomial Φ_n is separable modulo all primes $p \nmid n$. This implies that $\mathbf{Z}[\zeta]$ is regular above all primes that do not divide n. This leaves a single prime to consider when n is a prime power.

3.12. Theorem. *Let p be prime and $\zeta \in \overline{\mathbf{Q}}$ a primitive p^k-th root of unity for some $k \geq 1$. Then $R = \mathbf{Z}[\zeta]$ is a Dedekind domain that is unramified above all $q \neq p$ and totally ramified above p.*

Denote for $q \neq p$ by f_q and g_q the order and the index of $\langle q \bmod p^k \rangle \subset (\mathbf{Z}/p^k\mathbf{Z})^*$. Then there are exactly g_q extensions of q to $\mathbf{Z}[\zeta]$, and each of them has residue class degree f_q.

Proof. Apply 3.1 with f equal to $\Phi_{p^k}(X) = \frac{X^{p^k}-1}{X^{p^{k-1}}-1} = \sum_{i=0}^{p-1} X^{ip^{k-1}}$. Modulo p, we have $\Phi_{p^k}(X) = (X-1)^{p^k - p^{k-1}} \in \mathbf{F}_p[X]$. The remainder of Φ_{p^k} upon division by $X - 1$ equals $\Phi_{p^k}(1) = p$, which is not in $p^2\mathbf{Z}[X]$. It follows that the unique prime $\mathfrak{p} = (p, \zeta - 1)$ over p is invertible in $\mathbf{Z}[\zeta]$ and that $(p) = \mathfrak{p}^{p^k - p^{k-1}}$ is totally ramified.

We have already seen that Φ_{p^k} is separable modulo $q \neq p$, so it suffices to show that the irreducible factors of Φ_{p^k} in $\mathbf{F}_q[X]$ are of degree f_q. A finite field $\mathbf{F}_{q^t}$ of characteristic q contains a primitive p^k-th root of unity if and only if p^k divides the order $q^t - 1$ of the cyclic group $\mathbf{F}_{q^t}^*$. This happens exactly when f_q divides t, so all irreducible factors of Φ_{p^k} have degree f_q. □

The ring $\mathbf{Z}[\zeta_4] = \mathbf{Z}[i]$ of Gaussian integers and the ring $\mathbf{Z}[\zeta_3] = \mathbf{Z}[(-1+\sqrt{-3})/2]$ of Eisenstein are cyclotomic rings that are also quadratic. Comparing the description of the splitting

behavior of rational primes in them given by 3.12 (for $p^k = 3, 4$) and 3.11 (for $d = -1, -3$), we find once more the solution to problem 1.2, and deduce that -3 is a square modulo an odd prime q if and only if we have $q \equiv 1 \bmod 3$. This is a special case of the *quadratic reciprocity law*.

▶ Integral closure

For every number ring R, there exists a smallest extension ring $R \subset \widetilde{R}$ inside $K = Q(R)$ that is regular at all primes, and therefore Dedekind. It is this *integral closure* of R in K that we will discuss in the rest of this section.

3.13. Definition. *Let $A \subset B$ be an extension of rings. An element $b \in B$ is called integral over A if there exists a monic polynomial $f \in A[X]$ with $f(b) = 0$. We say that A is integrally closed in B if all $x \in B$ that are integral over A are contained in A.*

The most important case for us is the inclusion $R \subset K$ of a number ring R in its field of fractions. In this case, we simply say that R is *integrally closed* if it is integrally closed in K. The rough idea of the integrality condition for $R \subset K$ is that for an element $x \in K$, an integrality relation $x^n = \sum_{k=0}^{n-1} r_k x^k$ with $r_k \in R$ implies that x cannot have a true 'denominator' when written as a quotient of elements of R: the 'denominator' of x^n would be 'worse' than that of $\sum_{k=0}^{n-1} r_k x^k$. The following lemma makes this idea more precise.

3.14. Lemma. *A unique factorization domain is integrally closed.*

Proof. Suppose that we have $r, s \in R$ such that $x = \frac{r}{s} \in K$ satisfies an integral relation $x^n = \sum_{k=0}^{n-1} c_k x^k$ with $c_k \in R$. Multiplying by s^n, we obtain

$$r^n = \sum_{k=0}^{n-1} c_k r^k s^{n-k} = s \cdot \sum_{k=0}^{n-1} c_k r^k s^{n-1-k}.$$

If R is a unique factorization domain, this relation shows that every prime element dividing s divides r^n and therefore r. Removing common prime elements from r and s, we find $s \in R^*$ and $x \in R$. □

The argument in the preceding proof indicates that integrality is a 'local property': it can be checked locally at the prime ideals of the ring.

3.15. Proposition. *A domain R is integrally closed if and only if for every prime ideal $\mathfrak{p} \subset R$, the localization $R_\mathfrak{p}$ is integrally closed.*

Proof. Note first that R and its localizations all have the same field of fractions K. If an element $x \in K$ is integral over R, then it is obviously integral over all localizations $R_\mathfrak{p}$. If all $R_\mathfrak{p}$ are integrally closed, we have $x \in \bigcap_\mathfrak{p} R_\mathfrak{p} = R$ by 2.9, so R is integrally closed.

Conversely, suppose that $x \in K$ 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 $sr_k \in R$ 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. □

The definition of integrality in terms of monic polynomials is often replaced by one of the following equivalent formulations.

3.16. Lemma. *Let $R \subset R'$ be an extension of domains. Then the following are equivalent for an element $x \in R'$:*
(1) *x is integral over R;*
(2) *$R[x]$ is a finitely generated R-module;*
(3) *there exists a finitely generated R-module $M \subset Q(R')$ with $M \neq 0$ and $xM \subset M$.*

Proof. Suppose x satisfies an integrality relation $x^n = r_{n-1}x^{n-1} + r_{n-2}x^{n-2} + \ldots + r_1 x + r_0$. One can then express all powers of x as R-linear combinations of the elements 1, x, x^2,..., x^{n-1}. This yields $R[x] = R + R \cdot x + \ldots + R \cdot x^{n-1}$ and the implication (1) $\Rightarrow$ (2). The implication (2) $\Rightarrow$ (3) follows trivially by taking $M = R[x]$. For (3) $\Rightarrow$ (1), one writes $M = Rm_1 + \ldots + Rm_n$. The inclusion $xM \subset M$ means that we have identities

$$xm_i = \textstyle\sum_{j=1}^{n} r_{ij} m_j \qquad (i = 1, 2, \ldots, n).$$

Now the $n \times n$-matrix $A = x \cdot \mathrm{id}_n - (r_{ij})_{i,j=1}^n$ with entries in $K = Q(R')$ maps the non-zero vector $(m_i)_i \in K^n$ to zero, so we have $\det(A) = 0$. This yields the integrality relation $x^n + \sum_{k=0}^{n-1} r_k x^k = 0$ for x. □

3.17. Proposition. *If $R \subset R'$ is an extension of domains and $x, y \in R'$ are integral over R, then so are xy and $x + y$.*

Proof. If we have $xM \subset M$ and $yN \subset N$ for finitely generated R-modules M and N as in 3.16.(3), we can form the finitely generated R-module

$$MN = \{\textstyle\sum_i m_i n_i : m_i \in M, n_i \in N\} \subset Q(R').$$

It is mapped into itself by both x and y, hence also by $x + y$ and xy. □

It follows from 3.17 that for every extension of domains $R \subset R'$, the set of elements $x \in R'$ that are integral over R is a *subring* of R'. It is the *normalization* or *integral closure* of R in R'. For $R' = Q(R)$ the field of fractions of R, we obtain what is called the *normalization* or *integral closure* of R.

3.18. Proposition. *Let $R \subset R'$ be an extension of domains and $\widetilde{R}$ the normalization of R in R'. Then $\widetilde{R}$ is integrally closed in R'.*

Proof. It suffices to show that every $x \in R'$ that is integral over $\widetilde{R}$ is also integral over R. Suppose we have an integrality relation $x^n = \sum_{k=0}^{n-1} c_k x^k$ with $c_k \in \widetilde{R}$. By a repeated application of 3.16.(2), the ring $R_0 = R[c_0, c_1, \ldots, c_{n-1}]$ is finitely generated as an R-module, and $M = R_0[x]$ is finitely generated over R_0. This implies that M is finitely generated over R. As we have $xM \subset M$, it follows from 3.16.(3) that x is integral. □

3.19. Theorem. *Let R be a number ring. Then the following holds.*
(1) *R is Dedekind if and only if it is integrally closed.*
(2) *The normalization $\widetilde{R}$ of R is a Dedekind domain.*

Proof. As the normalization of a number ring is integrally closed by 3.18, (1) clearly implies (2). For (1), we note that R is by definition Dedekind when its localizations $R_\mathfrak{p}$ are discrete valuation rings, and that it is integrally closed if and only if all $R_\mathfrak{p}$ are integrally closed (3.15). It therefore suffices to show the local version of (1): a local number ring $R_\mathfrak{p}$ is a discrete valuation ring if and only if discrete valuation ringring!discrete valuationit is integrally closed.

If $R_\mathfrak{p}$ is a discrete valuation ring, it is a unique factorization domain, hence integrally closed by 3.14. Conversely, let $R_\mathfrak{p}$ be integrally closed. By 2.17, it suffices to show that its maximal ideal $\mathfrak{p}$ is principal. Take a non-zero element $a \in \mathfrak{p}$. Then there exists by 2.13 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 3.16.(3) that we cannot have $\pi^{-1}\mathfrak{p} \subset \mathfrak{p}$. It follows that $\pi^{-1}\mathfrak{p}$ equals R, so we have $\mathfrak{p} = \pi R$. □

Clearly, the normalization of a number ring is the smallest Dedekind domain containing it. More generally, we can form the integral closure of a number ring in any number field that contains it. This yields an integrally closed number ring, whence a Dedekind domain.

The integral closure of $\mathbf{Z}$ in a number field K is the *ring of integers* $\mathcal{O}_K$ of K. It is the smallest Dedekind domain with field of fractions K. Its explicit determination is a key problem in algorithmic number theory.

3.20. Theorem. *Let R be a number ring with field of fractions K, and $\mathcal{O}_K$ the ring of integers of K. Then the following holds:*

(1) $\mathcal{O}_K = \{x \in K : f^x_\mathbf{Q} \in \mathbf{Z}[X]\}$;

(2) *the normalization of R equals $\widetilde{R} = R\mathcal{O}_K$;*

(3) *R is Dedekind if and only if it contains $\mathcal{O}_K$.*

Proof. It is clear that $x \in K$ is in $\mathcal{O}_K$ if its irreducible polynomial is in $\mathbf{Z}[X]$. Conversely, if $x \in K$ is the zero of some monic polynomial $g \in \mathbf{Z}[X]$, then $f^x_\mathbf{Q}$ is a monic polynomial dividing g, so $f^x_\mathbf{Q}$ is in $\mathbf{Z}[X]$ by the Gauss lemma. This proves (1).

For (2), we note first that all primes of the ring $R\mathcal{O}_K$ are regular by 3.8, applied to the extension $\mathcal{O}_K \subset R\mathcal{O}_K$. It is therefore Dedekind, and integrally closed. As $\widetilde{R}$ contains both R and, since it is integrally closed, $\mathcal{O}_K$, we have $\widetilde{R} = R\mathcal{O}_K$. This proves (2), and (3) follows immediately. □

Exercise 6. Show that for R an order in K, we have $\widetilde{R} = \mathcal{O}_K$.

3.21. Examples. If we take $K = \mathbf{Q}(\alpha)$ with $\alpha^3 + \alpha + 1 = 0$, then α is integral over $\mathbf{Z}$ and $\mathcal{O}_K$ contains $\mathbf{Z}[\alpha]$. As $\mathbf{Z}[\alpha]$ is Dedekind by 3.3, we have $\mathcal{O}_K = \mathbf{Z}[\alpha]$.

Similarly, we can use 3.10 to deduce that the ring of integers of the quadratic field $K = \mathbf{Q}(\sqrt{d})$ for a squarefree integer $d \neq 1$ equals

$$\mathcal{O}_K = \begin{cases} \mathbf{Z}[\sqrt{d}] & \text{if } d \equiv 2 \text{ or } 3 \bmod 4; \\ \mathbf{Z}[\frac{1+\sqrt{d}}{2}] & \text{if } d \equiv 1 \bmod 4. \end{cases}$$

From this point of view, the natural ring to exploit in solving the equation $x^2 + 19 = y^3$ from problem 1.4 is not $\mathbf{Z}[\sqrt{-19}]$ but $\mathbf{Z}[\frac{1+\sqrt{-19}}{2}]$ (cf. exercise 1.13).

Exercise 7. Find $\mathcal{O}_K$ for $K = \mathbf{Q}(\sqrt{d})$ directly from 3.20 by looking at $f_{\mathbf{Q}}^x$ for $x \in K$.

EXERCISES.

8. Let $A \subset B$ be an extension of number rings. Show that for every prime $\mathfrak{p}$ of A, the ring $B_{\mathfrak{p}} = (A \setminus \mathfrak{p})^{-1}B$ is a semi-local number ring with primes corresponding to the extensions of $\mathfrak{p}$ in B.
9. Let $\mathfrak{p} = (2, 1 + \sqrt{-19})$ be the singular prime of $R = \mathbf{Z}[\sqrt{-19}]$. Compute the index of $\mathfrak{p}^k$ in R for $k = 1, 2, 3$. Conclude that $R/\mathfrak{p}$ and $\mathfrak{p}/\mathfrak{p}^2$ are not isomorphic as R-modules, and that the principal ideal $2R_{\mathfrak{p}}$ is not a power of the maximal ideal in $R_{\mathfrak{p}}$.
10. Let α be a zero of the polynomial $X^3 - X - 1$, and $R = \mathbf{Z}[\alpha]$. Show that R is a Dedekind ring, and determine all prime ideals of norm at most 30 in R. Show also that the unit group R^* is infinite.
11. Same questions as in the previous problem for the number ring $\mathbf{Z}[\sqrt[3]{2}]$.
12. Same questions for the cyclotomic ring $\mathbf{Z}[\zeta_7]$ and its subring $\mathbf{Z}[\zeta_7 + \zeta_7^{-1}]$.
13. Let R be a number ring with field of fractions K. Show that the number of extensions of a rational prime to R is at most $[K : \mathbf{Q}]$.
14. Determine the singular primes of the quadratic ring $\mathbf{Z}[\sqrt{d}]$ when d is a non-square (but not necessarily squarefree) integer.
15. Let d be an integer that is not a cube. Show that $\mathbf{Z}[\sqrt[3]{d}]$ is a Dedekind domain if and only if d is squarefree and satisfies $d \not\equiv \pm 1 \bmod 9$. Determine the singular primes in case $\mathbf{Z}[\sqrt[3]{d}]$ is not Dedekind.
16. Generalize the previous exercise to the rings $\mathbf{Z}[\sqrt[p]{d}]$, where p is an odd prime number.
17. Show that the unique prime $\mathfrak{p}|p$ in $\mathbf{Z}[\zeta_{p^k}]$ is principal with generator $1 - \zeta_{p^k}$.
18. Show that the cyclotomic ring $\mathbf{Z}[\zeta_{20}]$ is a Dedekind domain, and determine for each possible residue class p modulo 20 of a prime number p the number of primes $\mathfrak{p}$ of $\mathbf{Z}[\zeta_{20}]$ extending p, as well as their residue class field degrees $f(\mathfrak{p})$ and ramification indices $e(\mathfrak{p})$. Deduce that the irreducible polynomial $\Phi_{20} \in \mathbf{Z}[X]$ is reducible modulo every prime p.
19. Show that every quadratic ring $\mathbf{Z}[\sqrt{d}]$ is contained in some cyclotomic ring $\mathbf{Z}[\zeta]$. Given d, can you find the minimal order of ζ for which there is an inclusion?
[Hint: recall that $\mathbf{Q}(\zeta_p)$ contains a Gauss sum with square equal to $(-1)^{(p-1)/2}p$.]
20. Show that a prime $\mathfrak{p}$ of a number ring is regular if and only if it is proper, i.e., its multiplier ring $r(\mathfrak{p})$ is equal to R.
[Hint: if $\mathfrak{p}$ is singular and $a \in \mathfrak{p}$ is non-zero, we have $\mathfrak{p}_1\mathfrak{p}_2 \dots \mathfrak{p}_t \subset (a) \subset \mathfrak{p}$ by exercise 2.27. Assuming $\mathfrak{p}_1 = \mathfrak{p}$ and minimality of t, there exists $b \in \mathfrak{p}_2 \dots \mathfrak{p}_t \setminus (a)$ with $b\mathfrak{p} \subset (a)$.]
21. A domain B is said to be *integral* over a subring $A \subset B$ if every $b \in B$ is the zero of a monic polynomial in $A[X]$. Given inclusions of domains $A \subset B \subset C$, show that C is integral over A if and only if C is integral over B and B is integral over A.
22. Let R be a domain with normalization $\widetilde{R} \subset K$. Show that for every multiplicative subset $S \subset R$, the normalization of $S^{-1}R$ equals $S^{-1}\widetilde{R}$.

23. Show that every valuation ring (as in exercise 2.49) is integrally closed.

24. Let R be a number ring that is a unique factorization domain. Show that R contains $\mathcal{O}_K$, with K the field of fractions of R.

25. Show that a number ring is a unique factorization domain if and only if it is a principal ideal domain. More generally, show that a ring R is a principal ideal domain if and only if it is a unique factorization domain of dimension at most 1.
[Hint: use exercise 2.29.]

26. *(Algebraic integers.)* Let A be the integral closure of $\mathbf{Z}$ in an algebraic closure $\overline{\mathbf{Q}}$ of $\mathbf{Q}$. Show that $A \cap K = \mathcal{O}_K$ for every number field $K \subset \overline{\mathbf{Q}}$, and determine which of the characterizing properties of a Dedekind domain (integrally closed, dimension 1, noetherian) hold for A.

27. Let R be a number ring with field of fractions K, and suppose that R is Dedekind. Show that there exists a set of primes S of $\mathcal{O} = \mathcal{O}_K$ such that

$$R = \bigcap_{\mathfrak{p} \notin S} \mathcal{O}_{\mathfrak{p}} = \{x \in K : \mathrm{ord}_{\mathfrak{p}}(x) \geq 0 \text{ for all } \mathfrak{p} \notin S\}.$$

[This shows that any Dedekind domain with field of fractions K arises from $\mathcal{O}_K$ by 'inverting' some of its primes.]

28. Show that, in the situation of the previous exercise, we have a long exact sequence of abelian groups

$$1 \longrightarrow \mathcal{O}^* \longrightarrow R^* \longrightarrow \bigoplus_{\mathfrak{p} \in S} \mathbf{Z} \xrightarrow{\phi} \mathrm{Pic}(\mathcal{O}) \longrightarrow \mathrm{Pic}(R) \longrightarrow 1$$

in which ϕ maps the generator corresponding to $\mathfrak{p} \in S$ to the class $[\mathfrak{p}] \in \mathrm{Pic}(\mathcal{O})$.
[Hint: compare the exact sequences after 2.6 defining $\mathrm{Pic}(R)$ and $\mathrm{Pic}(\mathcal{O})$ using the *snake lemma* from commutative algebra.]

29. Compute the singular primes and the normalization of the order $\mathbf{Z}[\sqrt[3]{37}]$.

30. Show that $\mathbf{Z}[\sqrt{-5}]$ is a Dedekind domain, and that the identities $21 = (4+\sqrt{-5})(4-\sqrt{-5})$ and $21 = 3 \cdot 7$ represent two factorizations of 21 into pairwise non-associate irreducible elements. How does the ideal (21) factor into prime ideals in $\mathbf{Z}[\sqrt{-5}]$? Determine the order of the subgroup of $\mathrm{Cl}(\mathbf{Z}[\sqrt{-5}])$ that is generated by the classes of the primes dividing (21). Can you find an ideal in $\mathbf{Z}[\sqrt{-5}]$ for which the class is not in this subgroup?

*31. This exercise gives an example of a noetherian one-dimensional domain with infinitely many prime ideals, all of which are singular.

a. Prove that for every prime number p there exists a monic polynomial $f_p \in \mathbf{Z}[X]$ of degree p with the property that for each prime number $q \leq p$ the polynomial $(f_p \bmod q) \in \mathbf{F}_q[X]$ is irreducible.

In the rest of this exercise we let f_p be as above, we denote by α_p a zero of f_p in some given algebraic closure of $\mathbf{Q}$, and we write $\beta_p = p\alpha_p$. We let $R = \mathbf{Z}[\beta_2, \beta_3, \beta_5, \ldots]$ be the ring generated by all β_p.

a. Let $\mathfrak{p}$ be a prime ideal of the subring $\mathbf{Z}[\beta_2, \beta_3, \ldots, \beta_p]$ of R generated by all β_q with $q \leq p$. Suppose that $p \in \mathfrak{p}$. Prove that the R-ideal generated by $\mathfrak{p}$ is a finitely generated prime ideal of R.

c. Prove that R is a one-dimensional noetherian domain, that R has infinitely many non-zero prime ideals, and that none of them is invertible.

4 Linear algebra for number rings

This section provides the basic tools from linear algebra that are used in the study of number rings. They will enable us to compute the normalization of a number ring and to study its singular and ramifying primes.

▶ Norm and trace

Let $A \subset B$ be an extension of rings such that B is free of finite rank n as an A-algebra. This means that there exist $x_1, x_2, \ldots, x_n \in B$ that form an A-basis for B:

$$B = A \cdot x_1 \oplus A \cdot x_2 \oplus \ldots \oplus A \cdot x_n.$$

For $x \in B$, let $M_x : B \to B$ denote the A-linear multiplication map $b \mapsto xb$. If we choose an A-basis for B, this map can be described by an $n \times n$-matrix with coefficients in A. 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 is immediate 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 *characteristic polynomial* $f^x_{B/A}$ of $x \in B$ is the characteristic polynomial of the map M_x, i.e.,

$$f^x_{B/A}(X) = \det(X \cdot \mathrm{id}_B - M_x).$$

The polynomial $f^x_{B/A} = \sum_{k=0}^{n} a_k X^k \in A[X]$ is monic and of degree n. Its constant coefficient is $a_0 = (-1)^n N_{B/A}(x)$, and its second highest coefficient is $a_{n-1} = -\mathrm{Tr}_{B/A}(x)$.

In our examples, A will be a domain such as a number ring or a field. If A is a field, classical linear algebra tells us that norms and traces do not depend on the choice of a basis for B over A, and that we have $f^x_{B/A}(x) = 0$ by the Cayley-Hamilton theorem. The same is true for arbitrary domains A as the notions of norm, trace and discriminant are stable under *base changes* such as the inclusion map $A \subset Q(A)$ of A in its field of fractions. By this we mean that for *any* ring homomorphism $f : A \to A'$, we can form the A'-algebra $B' = B \otimes_A A'$, which is again free of rank n as the induced map $f_* : B \to B'$ maps a basis of B over A to a basis of B' over A'. For $x \in B$, the multiplication matrix for $f_*(x)$ in the A'-algebra B' is obtained by applying f to the entries of M_x, so we have commutative diagrams

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

for norm and trace. In particular, the *absolute norm* and the *absolute trace* $R \to \mathbf{Z}$ for an order R of rank n can be viewed as restrictions of the norm and trace maps for the field extension $\mathbf{Q} \subset Q(R)$ of degree n. Similarly, their reduction modulo a prime number p yield the norm and trace maps $R/pR \to \mathbf{F}_p$.

4.1. Lemma. *Let R be an order and $x \in R$. Then the index of xR in R equals $|N_{R/\mathbf{Z}}(x)|$.*

Proof. As R is free of finite rank as an abelian group, the index of the image $xR = M_x[R]$ of R under the $\mathbf{Z}$-linear map M_x equals $|\det M_x| = |N_{R/\mathbf{Z}}(x)| = |N_{K/\mathbf{Q}}(x)|$, with K the field of fractions of R. □

We already used the word *norm* for an ideal $I \subset R$ to indicate the index of I in R. For orders, the absolute norm of $x \in R$ and the ideal norm of xR coincide as $\mathbf{Z}$-ideals.

For a finite field extension $K \subset K(x)$, the Cayley-Hamilton identity $f^x_{K(x)/K}(x) = 0$ implies that the characteristic polynomial $f^x_{K(x)/K}$ is divisible by the irreducible polynomial f^x_K. As they are both of degree $[K(x) : K]$, they coincide. In case x is some element of a finite extension L of K, one can write L as a direct sum of $K(x)$-vector spaces to find $f^x_{L/K} = (f^x_K)^{[L:K(x)]}$.

Exercise 1. Deduce: $\mathrm{Tr}_{L/K}(x) = [L : K(x)] \cdot \mathrm{Tr}_{K(x)/K}(x)$ and $N_{L/K}(x) = N_{K(x)/K}(x)^{[L:K(x)]}$.

There is a different characterization of norms and traces in separable field extensions. Recall that a finite field extension $K \subset L$ is called *separable* if the set $\mathrm{Hom}_K(L, \overline{K})$ of K-homomorphisms of L into an algebraic closure $\overline{K}$ of K has cardinality $[L : K]$. Extensions in characteristic zero and extensions of finite fields are always separable. Every finite separable field extension $K \subset L$ is *primitive*, i.e., it is of the form $L = K(\alpha)$. The irreducible polynomial of an element α generating a separable extension is itself *separable* in the sense that its roots in $\overline{K}$ are simple roots.

4.2. Lemma. *Let L/K be a separable field extension of degree n. Then we have*

$$f^x_{L/K} = \prod_{\sigma \in \mathrm{Hom}_K(L,\overline{K})} (X - \sigma(x)).$$

for $x \in L$. In particular, we have $N_{L/K}(x) = \prod_\sigma \sigma(x)$ and $\mathrm{Tr}_{L/K}(x) = \sum_\sigma \sigma(x)$.

Proof. For $L = K(x)$, the K-homomorphisms $L \to \overline{K}$ map x to the various roots of the irreducible polynomial of x, so we have $\prod_\sigma (X - \sigma(x)) = f^x_K = f^x_{L/K}$, as desired. In the general case, every K-homomorphism $\sigma : K(x) \to \overline{K}$ has exactly $[L : K(x)]$ extensions to a K-homomorphism $L \to \overline{K}$ and one finds

$$\prod_{\sigma \in \mathrm{Hom}_K(L,\overline{K})} (X - \sigma(x)) = (f^x_K)^{[L:K(x)]} = f^x_{L/K}.$$

The final statements follow by inspection of the appropriate coefficients of $f^x_{L/K}$. □

4.3. Example. For the quadratic field $\mathbf{Q}(\sqrt{d})$ and the order $\mathbf{Z}[\sqrt{d}]$, we already defined the norm in various cases by $N(x + y\sqrt{d}) = x^2 - dy^2$. This is the product $(x + y\sqrt{d})(x - y\sqrt{d})$ of the two zeroes of the corresponding irreducible polynomial, and also the determinant of the matrix $\left(\begin{smallmatrix} x & dy \\ y & x \end{smallmatrix}\right)$ describing multiplication by $x + y\sqrt{d}$ with respect to the basis $\{1, \sqrt{d}\}$.

▶ Discriminant

It follows from 4.1 that the absolute norm of an integral element in a number field K is an integer measuring in some sense the 'size' of the element. For orders $R \subset K$ there is a similar notion of size that can be defined using the trace map.

4.4. Definition. *The discriminant of an order R of rank n is defined as*

$$\Delta(R) = \det(\mathrm{Tr}_{R/\mathbf{Z}}(x_i x_j))_{i,j=1}^n,$$

where $x_1, x_2, \ldots, x_n$ is some $\mathbf{Z}$-basis for R.

More generally, one defines the *discriminant* of n elements $x_1, x_2, \ldots, x_n \in B$ in a free A-algebra B of rank n as

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

If $x_1, x_2, \ldots, x_n$ is an A-basis for B and $y_1, y_2, \ldots, y_n$ some other basis defined by $y_i = \sum_{j=1}^n a_{ij} x_j$ for some $T = (a_{ij}) \in \mathrm{GL}_n(A)$, we find

$$\Delta(y_1, y_2, \ldots, y_n) = (\det T)^2 \Delta(x_1, x_2, \ldots, x_n)$$

from the relation $(\mathrm{Tr}_{B/A}(y_i y_j))_{i,j=1}^n = T \cdot (\mathrm{Tr}_{B/A}(x_i x_j))_{i,j=1}^n \cdot T^t$. Here T^t denotes the transpose of the transformation matrix T. It follows that the discriminant of a basis depends on the choice of the basis, but only up to the square of a unit in A. For $A = \mathbf{Z}$, we find that the discriminant of an order is independent of the basis chosen in 4.4.

If $R \subset \mathcal{O}$ is an inclusion of orders of the same rank n, we have $R = T[\mathcal{O}]$ for some $\mathbf{Z}$-linear map T that maps a $\mathbf{Z}$-basis of $\mathcal{O}$ to a $\mathbf{Z}$-basis of R. By the theory of finitely generated abelian groups, the index $[\mathcal{O} : R]$ is in this situation finite and equal to $|\det T|$. This yields the useful relation

$$\Delta(R) = [\mathcal{O} : R]^2 \cdot \Delta(\mathcal{O}) \tag{4.5}$$

between the discriminants of orders in the same number field.

4.6. Proposition. *Let L/K be a separable field extension of degree n and $\sigma_1, \sigma_2, \ldots, \sigma_n \in \mathrm{Hom}_K(L, \overline{K})$ the set of embeddings of L in $\overline{K}$. Then one has*

$$\Delta(x_1, x_2, \ldots, x_n) = \left[\det(\sigma_i(x_j))_{i,j=1}^n\right]^2$$

for every n elements $x_1, x_2, \ldots, x_n \in L$. If $\alpha \in L$ generates L over K, the power basis $1, \alpha, \alpha^2, \ldots, \alpha^{n-1}$ has discriminant

$$\Delta(1, \alpha, \alpha^2, \ldots, \alpha^{n-1}) = \Delta(f_K^\alpha),$$

where $\Delta(f_K^\alpha)$ denotes the discriminant of the polynomial f_K^α. One has $\Delta(x_1, x_2, \ldots, x_n) \neq 0$ if and only if $x_1, x_2, \ldots, x_n$ is a K-basis for L.

Proof. If we multiply the matrix $X = (\sigma_i(x_j))_{i,j=1}^n$ by its transpose and use the description of the trace map from 4.1, we find

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

Taking determinants, we obtain the first statement. If we have $L = K(\alpha)$, the elements $\alpha_i = \sigma_i(\alpha)$ are the roots of the polynomial f_K^α. For the basis $1, \alpha, \alpha^2, \ldots, \alpha^{n-1}$ of L/K, the associated discriminant $[\det(\sigma_i(\alpha^{j-1}))_{i,j=1}^n]^2$ is the square of the Vandermonde determinant $\det(\alpha_i^{j-1})_{i,j=1}^n = \prod_{i>j}(\alpha_i - \alpha_j)$. This yields

$$\Delta(1, \alpha, \alpha^2, \ldots, \alpha^{n-1}) = \prod\nolimits_{i>j}(\alpha_i - \alpha_j)^2 = \Delta(f_K^\alpha).$$

As f_K^α has distinct roots, the discriminant $\Delta(f_K^\alpha)$ is non-zero.

Every basis of L/K is obtained from the power basis $1, \alpha, \alpha^2, \ldots, \alpha^{n-1}$ by an invertible coordinate transformation, so the discriminant $\Delta(x_1, x_2, \ldots, x_n)$ is non-zero for every basis of L/K. For a K-linearly dependent n-tuple, the discriminant clearly vanishes. □

4.7. Corollary. *Let $f \in \mathbf{Z}[X]$ be a monic irreducible polynomial with root α. Then the order $\mathbf{Z}[\alpha]$ has discriminant $\Delta(f)$.*

Proof. We have $\Delta(\mathbf{Z}[\alpha]) = \Delta_{\mathbf{Z}[\alpha]/\mathbf{Z}}(1, \alpha, \ldots, \alpha^{n-1}) = \Delta_{\mathbf{Q}(\alpha)/\mathbf{Q}}(1, \alpha, \ldots, \alpha^{n-1}) = \Delta(f)$. □

One can reformulate the non-vanishing of the discriminant for finite separable field extensions L/K by saying that the trace form

$$\begin{aligned} \mathrm{Tr}_{L/K} : L \times L &\longrightarrow K \\ (x, y) &\longmapsto \mathrm{Tr}_{L/K}(xy) \end{aligned}$$

is a non-degenerate bilinear form, or that the map $L \to \widehat{L} = \mathrm{Hom}(L, K)$ to the dual vector space of L over K that sends x to the map $(y \mapsto \mathrm{Tr}_{L/K}(xy))$ is an isomorphism. This implies that for every basis $x_1, x_2, \ldots, x_n$ of L over K, there is a *dual basis* $y_1, y_2, \ldots y_n$ of L over K such that

$$\mathrm{Tr}_{L/K}(x_i y_j) = \delta_{ij}.$$

Here δ_{ij} denotes the Kronecker delta.

4.8. Theorem. *If K is a number field of degree n, then there exists a basis ω_1, ω_2,..., ω_n for K over $\mathbf{Q}$ for which we have*

$$\mathcal{O}_K = \mathbf{Z}\omega_1 \oplus \mathbf{Z}\omega_2 \oplus \ldots \oplus \mathbf{Z}\omega_n.$$

Proof. Choose an arbitrary basis $x_1, x_2, \ldots, x_n$ of K over $\mathbf{Q}$ consisting of integral elements, and let $y_1, y_2, \ldots, y_n$ be the dual basis. Then the abelian group $M^\dagger = \mathbf{Z}y_1 \oplus \mathbf{Z}y_2 \oplus \ldots \mathbf{Z}y_n$ is the trace dual of the abelian group $M = \mathbf{Z}x_1 \oplus \mathbf{Z}x_2 \oplus \ldots \mathbf{Z}x_n$, i.e., it can be given as

$$M^\dagger = \{x \in K : \mathrm{Tr}_{K/\mathbf{Q}}(xM) \subset \mathbf{Z}\}.$$

If $x \in \mathcal{O}_K$ is integral, then xM consists of integral elements and we have $\mathrm{Tr}_{K/\mathbf{Q}}(xM) \subset \mathbf{Z}$. This shows that we have $M \subset \mathcal{O}_K \subset M^\dagger$. As M and $M^\dagger$ are free abelian groups of rank n, the same holds for $\mathcal{O}_K$. □

A basis as in 4.8 is called an *integral basis* for $\mathcal{O}_K$. Its existence shows that $\mathcal{O}_K$ is an order in K. As every order $R \subset K$ is contained in $\mathcal{O}_K$ (cf. 3.16, or exercise 3.6), the ring of integers is the *maximal order* in K. It is the only order in K that is a Dedekind domain. Its discriminant $\Delta(\mathcal{O}_K)$ is usually referred to as the *discriminant* Δ_K of the number field K.

4.9. Theorem. *Every number ring R is of finite index in its normalization $\widetilde{R}$.*

Proof. Writing $\mathcal{O} = \mathcal{O}_K$ for the ring of integers of $K = Q(R)$, we have $\widetilde{R} = R\mathcal{O}$ by 3.20. The ring $R \cap \mathcal{O}$ is an order with field of fractions K, so its additive group is free of the same rank $[K : \mathbf{Q}]$ as $\mathcal{O}$. It follows that $R \cap \mathcal{O}$ is of finite index $k \in \mathbf{Z}_{\geq 1}$ in $\mathcal{O}$, and that $k\widetilde{R} = k\mathcal{O}R$ is contained in R. By 2.11, we conclude that R is of finite index in $\widetilde{R}$ as it contains the non-zero $\widetilde{R}$-ideal $k\widetilde{R}$. □

The rational primes p dividing the index $[\widetilde{R} : R]$ are the p that have singular extensions in R. For orders $R = \mathbf{Z}[\alpha]$, we have $\widetilde{R} = \mathcal{O}_K$ and we can detect such p using 4.7 and 4.5.

4.10. Theorem. *Let $\mathbf{Z}[\alpha]$ be an order in a number field K. Then one has*

$$\Delta(f^{\alpha}_{\mathbf{Q}}) = [\mathcal{O}_K : \mathbf{Z}[\alpha]]^2 \cdot \Delta_K.$$ □

It follows that if $f \in \mathbf{Z}[X]$ is a monic irreducible polynomial with squarefree discriminant, the order $\mathbf{Z}[\alpha]$ is the ring of integers in $\mathbf{Q}(\alpha)$. The theorem also shows the need for computational techniques to find discriminants of polynomials.

▶ Computational techniques

Let A be a domain and $f \in A[X]$ a monic polynomial. Then $B = A[\alpha] = A[X]/(f)$ with $\alpha = X \bmod f$ is a free A-algebra of rank n. In this algebra, one can compute the norm of elements of the form $a_0 + a_1\alpha$ as

$$N_{B/A}(a_0 + a_1\alpha) = (-a_1)^n f(\frac{-a_0}{a_1}).$$

For the general case, one can use resultants. The *resultant* of two non-zero polynomials $g = b\prod_{i=1}^{r}(X - \beta_i)$ and $h = c\prod_{j=1}^{s}(X - \gamma_j)$ with coefficients and zeroes in some field F is defined as

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

One directly derives from this definition that $R(g, h)$ satisfies the following 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 $h_1 \equiv h \bmod gF[X]$ and $s_1 = \deg h_1$.

It is immediate from property (R2) that for $x = g(\alpha) \in B = A[\alpha]$ in our situation above, one has

$$N_{B/A}(g(\alpha)) = R(f, g).$$

If f is separable with zeroes $\alpha_1, \alpha_2, \ldots, \alpha_n$ in $F \supset A$, one has $f'(\alpha_1) = \prod_{i\geq 2}(\alpha_1 - \alpha_i)$. Taking for g the derivative f' of f in the formula above, one finds that the discriminant of f can be written as

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

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.

4.11. Example. Let $f = X^3 - X^2 - 6X - 12$ be the irreducible polynomial of the element β occurring in 3.7. Long division shows that the remainder of f upon division by its derivative $f' = 3X^2 - 2X - 6$ equals $(X^3 - X^2 - 6X - 12) - \frac{1}{9}(3X - 1)(3X^2 - 2X - 6) = -\frac{38}{9}(X + 3)$. This is a linear polynomial with zero -3, so we can apply (R1)–(R3) to find

$$\begin{aligned}\Delta(f) &= -R(f, f') = -R(f', f) = 3^2 \cdot R(f', -\tfrac{38}{9}(X + 3)) \\ &= 3^2 \cdot R(-\tfrac{38}{9}(X + 3), f') = -3^2 \cdot (-\tfrac{38}{9})^2 \cdot f'(-3) = -2^2 \cdot 3 \cdot 19^2.\end{aligned}$$

As $\mathbf{Z}[\beta]$ has index 2 in the ring of integers of its field of fractions $K = \mathbf{Q}(\sqrt[3]{-19}) = \mathbf{Q}(\sqrt[3]{19})$, we find from 4.10 that K has discriminant $\Delta_K = -3 \cdot 19^2$.

Exercise 2. Derive the same conclusion starting from the order $\mathbf{Z}[\sqrt[3]{-19}]$ of discriminant $\Delta(X^3 + 19)$.

4.12. Example. Let $p > 2$ be a prime and $K = \mathbf{Q}(\zeta_p)$ the p-th cyclotomic field. Then we have $\Delta_K = \Delta(\Phi_p) = (-1)^{(p-1)/2} N_{K/\mathbf{Q}}(\Phi_p'(\zeta_p))$. Every difference of two distinct p-th roots of unity is a product of a root of unity and a conjugate of $1 - \zeta_p$. As we have $N_{K/\mathbf{Q}}(\zeta_p) = 1$ and $N_{K/\mathbf{Q}}(1 - \zeta_p) = \Phi_p(1) = p$, we find $\Delta_{\mathbf{Q}(\zeta_p)} = (-1)^{(p-1)/2} p^{p-2}$.

Example 4.11 indicates how one can find $\mathcal{O}_K$ for a small number field $K = \mathbf{Q}(\alpha)$. After replacing α when necessary by a suitable multiple $k\alpha$, we may suppose that α is integral. One computes the discriminant $\Delta(f^\alpha_{\mathbf{Q}})$ of the order $\mathbf{Z}[\alpha]$ using either the resultant or the values of the *power sums* of α (exercises 19– 21). For each prime number p for which p^2 divides $\Delta(f^\alpha_{\mathbf{Q}})$, one has to check whether p divides the index $[\mathcal{O}_K : \mathbf{Z}[\alpha]]$. The primes p that divide the index are exactly the primes for which the semi-local ring $\mathbf{Z}_{(p)}[\alpha]$ is not integrally closed, i.e. the primes p for which there is a prime ideal $\mathfrak{p}|p$ in $\mathbf{Z}[\alpha]$ that is not invertible. These primes can be found using the Kummer-Dedekind theorem 3.1, and for each of them we find an element of $x \in \mathcal{O}_K$ outside $\mathbf{Z}[\alpha]$. After adjoining all these elements to $\mathbf{Z}[\alpha]$ we obtain a subring $R \subset \mathcal{O}_K$ with fewer singular primes than $\mathbf{Z}[\alpha]$. If there are primes $p|[R : \mathbf{Z}[\alpha]]$ for which p^2 divides $\Delta(f^\alpha_{\mathbf{Q}})/[R : \mathbf{Z}[\alpha]]^2$, one still has to check whether $R_{(p)}$ is integrally closed. If it is not, then for one of the finitely many non-zero elements in $\overline{x} \in \frac{1}{p}R/R$ the lift $x \in \frac{1}{p}R$ is integral over $\mathbf{Z}$. This shows that we find $\mathcal{O}_K$ after a finite computation.

4.13. Example. Consider the order $R = \mathbf{Z}[\sqrt[4]{-19}] \subset K = \mathbf{Q}(\sqrt[4]{-19})$. As we have $R = \mathbf{Z}[\alpha]$ with $f^\alpha_{\mathbf{Q}} = X^4 + 19$, we can apply 3.1. Just as in 3.7, we easily find that R is regular and unramified above $p \neq 2, 19$, and that R is regular and totally ramified above 19. The unique prime $(2, \alpha - 1)$ in R above 2 is singular: from

$$X^4 + 19 = (X - 1)(X^3 + X^2 + X + 1) + 2^2 \cdot 5$$

we find an integral element $\beta = (\alpha^3 + \alpha^2 + \alpha + 1)/2$ and an integral extension $R \subset R[\beta]$ of index 2. As R has discriminant $\Delta(X^4 + 19) = 2^8 \cdot 19^3$, the discriminant of $R[\beta]$ is $2^{-2}\Delta(R) = 2^6 \cdot 19^3$. In order to see whether $R[\beta]$ is regular above 2, we have to check whether there are integral elements in $\frac{1}{2}R[\beta] \setminus R[\beta]$. In this case, such an element is easily found: the generator $\gamma = (\alpha^2 + 1)/2 = (\sqrt{-19} + 1)/2$ of the ring of integers of the subfield $\mathbf{Q}(\sqrt{-19}) \subset K$ is not in $R[\beta]$. Note that we have $(\alpha + 1)\gamma = \beta$. This gives us an order $B = \mathbf{Z}[\alpha, \beta, \gamma] = \mathbf{Z}[\alpha, \gamma]$ in K of discriminant $4^{-2}\Delta(R) = 2^4 \cdot 19^3$. One can check that none of the 15 non-zero elements in $\frac{1}{2}B/B$ has an integral lift in K, so we have $B = \mathcal{O}_K$ and $\Delta_K = 2^4 \cdot 19^3$. A more efficient way to see this proceeds by applying a *relative* version of the Kummer-Dedekind theorem 3.1 to the extension $A \subset B = A[\alpha]$ of the Dedekind domain $A = \mathbf{Z}[\gamma]$ – see exercises 31 and 32.

▶ Ramification

If a prime p divides the discriminant $\Delta(f^\alpha_{\mathbf{Q}})$ of an order $R = \mathbf{Z}[\alpha]$, then $f^\alpha_{\mathbf{Q}} \bmod p$ has multiple factors and it follows from 3.1 that either p is regular and ramified in R, or p is singular in R and a divisor of the index $[\mathcal{O}_K : \mathbf{Z}[\alpha]]$. In view of 4.10, this strongly suggests the following result.

4.14. Theorem. *A rational prime p ramifies in the ring of integers $\mathcal{O}_K$ of K if and only if it divides the discriminant Δ_K.*

As not every ring of integers is of the form $\mathbf{Z}[\alpha]$, we cannot derive this result from 3.1. The proof is based on the following elementary lemma.

4.15. Lemma. *Let $M = M_1 \times M_2 \times \ldots M_t$ be a product of free R-algebras of finite rank. Then we have $\mathrm{Tr}_{M/R}((m_i)_{i=1}^t) = \sum_{i=1}^t \mathrm{Tr}_{M_i/R}(m_i)$ and $\Delta(M/R) = \prod_{i=1}^t \Delta(M_i/R)$.*

Proof. It suffices to prove the lemma for $M = M_1 \times M_2$, the general case then follows by induction. View the R-algebras M_1 and M_2 as R-submodules of M and choose R-bases X of M_1 and Y of M_2. Then $X \cup Y$ is a basis for M, and we have $xy = 0$ for $x \in X$ and $y \in Y$. The trace of an element $m_i \in M_i$ as an element of M_i and as an element of $M \supset M_i \times \{0\} = M_i$ coincides, so we have the general identity $\mathrm{Tr}_{M/R}(m_1, m_2) = \mathrm{Tr}_{M_1/R}(m_1) + \mathrm{Tr}_{M_2/R}(m_2)$. One deduces that the discriminant of the basis $X \cup Y$ of M is the determinant of a block matrix in which the blocks are the discriminant matrices for M_1 and M_2. This yields $\Delta(M/R) = \Delta(M_1/R)\Delta(M_2/R)$. □

Proof of 4.14. In order to study $\Delta_K \bmod p$, we apply the base extension $\mathbf{Z} \to \mathbf{F}_p$. This simply means that we reduce everything modulo p and look at the $\mathbf{F}_p$-algebra $\mathcal{O}/p\mathcal{O} = \mathcal{O} \otimes_{\mathbf{Z}} \mathbf{F}_p$. This algebra has discriminant $\Delta(\mathcal{O}_K) \cdot \mathbf{F}_p = (\Delta_K \bmod p)$ over $\mathbf{F}_p$. We have $p\mathcal{O} = \prod_{\mathfrak{p}|p} \mathfrak{p}^{e(\mathfrak{p}/p)}$ in $\mathcal{O}$, so the Chinese remainder theorem for $\mathcal{O}/p\mathcal{O}$ and 4.15 yield

$$\Delta_K \bmod p = \prod\nolimits_{\mathfrak{p}|p} \Delta((\mathcal{O}/\mathfrak{p}^{e(\mathfrak{p}/p)})/\mathbf{F}_p).$$

If p is unramified in $\mathcal{O}$, all discriminants $\Delta((\mathcal{O}/\mathfrak{p}^{e(\mathfrak{p}/p)})/\mathbf{F}_p) = \Delta((\mathcal{O}/\mathfrak{p})/\mathbf{F}_p)$ are non-zero by 4.6, since $\mathbf{F}_p \subset \mathcal{O}/\mathfrak{p}$ is a separable field extension. In this case we find that $\Delta_K \bmod p$ is non-zero, so p does not divide Δ_K.

If p is ramified in $\mathcal{O}$, there exists $\mathfrak{p}|p$ in $\mathcal{O}$ with $e = e(\mathfrak{p}/p) \geq 2$. In this case we can choose a basis for $\mathcal{O}/\mathfrak{p}^e$ over $\mathbf{F}_p$ that contains an element $x \in \mathfrak{p} \setminus \mathfrak{p}^2$. As the element x is nilpotent in $\mathcal{O}/\mathfrak{p}^e$, we have $\mathrm{Tr}(xy) = 0 \in \mathbf{F}_p$ for all $y \in \mathcal{O}/\mathfrak{p}^e$. It follows that the discriminant of every basis containing x vanishes, so we have $\Delta((\mathcal{O}/\mathfrak{p}^e)/\mathbf{F}_p) = 0$ and $\Delta_K = 0 \bmod p$. □

The examples we have treated so far, such as $K = \mathbf{Q}(\zeta_p), \mathbf{Q}(\sqrt[3]{-19})$ or $\mathbf{Q}(\sqrt[4]{-19})$, show that the *exponent* with which p divides Δ_K tends to be high if the ramification indices of the primes over p are high. The precise relation involves the *different* of K.

4.16. Definition. *The different $\mathfrak{D}_K$ of a number field K is the integral $\mathcal{O}_K$-ideal whose inverse*

$$\mathfrak{D}_K^{-1} = \{x \in K : \mathrm{Tr}_{K/\mathbf{Q}}(x\mathcal{O}_K) \subset \mathbf{Z}\}.$$

is the trace dual of $\mathcal{O}_K$.

Note that $\mathfrak{D}_K^{-1}$ is indeed a fractional $\mathcal{O}_K$-ideal, and that its inverse is integral as we have $\mathfrak{D}_K^{-1} \supset \mathcal{O}_K$. If $\omega_1, \omega_2, \ldots, \omega_n$ is a $\mathbf{Z}$-basis for $\mathcal{O}_K$, the *co-different* $\mathfrak{D}_K^{-1}$ has $\mathbf{Z}$-basis $\omega_1^*, \omega_2^*, \ldots, \omega_n^*$.

4.17. Theorem. *The different $\mathfrak{D}_K$ of K is an $\mathcal{O}_K$-ideal of norm $[\mathcal{O}_K : \mathfrak{D}_K] = |\Delta_K|$ that is divisible only by the ramified primes of $\mathcal{O}_K$. For every prime $\mathfrak{p}$ of $\mathcal{O}_K$ one has $\mathfrak{p}^{e(\mathfrak{p}/p)-1}|\mathfrak{D}_K$.*

Proof. Choose a basis $\omega_1, \omega_2, \ldots, \omega_n$ of $\mathcal{O}_K$, and let $T : \mathfrak{D}_K^{-1} \to \mathcal{O}_K$ be a $\mathbf{Z}$-linear map sending the $\mathbf{Z}$-basis $\omega_1^*, \omega_2^*, \ldots, \omega_n^*$ of $\mathfrak{D}_K^{-1}$ to the basis of $\mathcal{O}_K$ by $T\omega_i^* = \omega_i$. Then $\mathcal{O}_K$ has index $|\det T|$ in $\mathfrak{D}_K^{-1}$, and we find

$$1 = \det(\mathrm{Tr}_{K/\mathbf{Q}}(\omega_i\omega_j^*))_{i,j=1}^n = \det(T^{-1}) \cdot \det(\mathrm{Tr}_{K/\mathbf{Q}}(\omega_i\omega_j)_{i,j=1}^n) = \det(T^{-1}) \cdot \Delta_K.$$

It follows that we have $[\mathcal{O}_K : \mathfrak{D}_K] = [\mathfrak{D}_K^{-1} : \mathcal{O}_K] = |\det(T^{-1})| = |\Delta_K|$.

Suppose that $\mathfrak{p}|p$ is a prime of $\mathcal{O} = \mathcal{O}_K$ that ramifies with index $e > 1$. Then every element x in the integral $\mathcal{O}$-ideal $\mathfrak{p}^{1-e}p$ reduces modulo p to an element in $\mathcal{O}/p\mathcal{O}$ that is contained in all prime ideals of $\mathcal{O}/p\mathcal{O}$. It follows that $\overline{x}$ is a nilpotent element in $\mathcal{O}/p\mathcal{O}$, so we have $\overline{0} = \mathrm{Tr}_{(\mathcal{O}/p\mathcal{O})/\mathbf{F}_p}(\overline{x}) = \mathrm{Tr}_{K/\mathbf{Q}}(x) \bmod p$. This proves the inclusion

$$\mathrm{Tr}_{K/\mathbf{Q}}(\mathfrak{p}^{1-e}p) \subset p\mathbf{Z}.$$

As $\mathrm{Tr}_{K/\mathbf{Q}}$ is $\mathbf{Z}$-linear, we obtain $\mathrm{Tr}_{K/\mathbf{Q}}(\mathfrak{p}^{1-e}) \subset \mathbf{Z}$, whence $\mathfrak{p}^{1-e} \subset \mathfrak{D}_K^{-1}$ and $\mathfrak{p}^{e-1}|\mathfrak{D}_K$.

The preceding argument shows that for every prime $\mathfrak{p}$ above p dividing $\mathfrak{D}_K$, we have $\mathrm{Tr}_{K/\mathbf{Q}}(\mathfrak{p}^{-1}p) \subset p\mathbf{Z}$ and, reducing modulo p, the identity $\mathrm{Tr}_{(\mathcal{O}/p\mathcal{O})/\mathbf{F}_p}(\mathfrak{p}^{-1}p/p\mathcal{O}) = \overline{0}$. If $\mathfrak{p}$ is unramified, the ideal $\mathfrak{p}^{-1}p/p\mathcal{O} \subset \mathcal{O}/p\mathcal{O}$ is the summand

$$\mathcal{O}/\mathfrak{p} \subset \mathcal{O}/p\mathcal{O} \ = \mathcal{O}/\mathfrak{p} \times \prod_{\mathfrak{q}|p, \mathfrak{q}\neq\mathfrak{p}} \mathcal{O}/\mathfrak{q}^{e(\mathfrak{q}/p)},$$

and $\mathrm{Tr}_{(\mathcal{O}/p\mathcal{O})/\mathbf{F}_p}$ is by 4.15 the field trace $\mathrm{Tr} : \mathcal{O}/\mathfrak{p} \to \mathbf{F}_p$. As the trace does not vanish in a separable field extension, we find $\mathfrak{p} \nmid \mathfrak{D}_K$ for unramified $\mathfrak{p}$. □

One can show that $\mathfrak{p}^{e(\mathfrak{p}/p)-1}$ is the exact power of $\mathfrak{p}$ dividing $\mathfrak{D}_K$ if and only if the ramification index $e(\mathfrak{p}/p)$ is not divisible by p. In this case one says that $\mathfrak{p}$ is *tamely ramified* over p. If p does divide the ramification $e(\mathfrak{p}/p)$, the ramification is said to be *wild*.

Theorem 4.17 shows that the different is a finer measure for ramification than the discriminant as it detects the primes in $\mathcal{O}_K$ that are ramified, not just the rational primes lying below them. As a consequence, it lives in $\mathcal{O}_K$ and not in $\mathbf{Z}$.

In a similar way, the index $[\widetilde{R} : R]$ has as its prime divisors the primes p above which R is singular. For the *conductor* of R measuring the singular primes themselves, we refer to exercise 25.

Exercises.

3. Show that the norm and the trace are transitive in towers of separable field extensions, i.e., for a tower $K \subset L \subset M$ we have $N_{L/K} \circ N_{M/L} = N_{M/K}$ and $\mathrm{Tr}_{L/K} \circ \mathrm{Tr}_{M/L} = \mathrm{Tr}_{M/K}$.
4. Let $\mathcal{O}_K$ be the ring of integers of K and $N_{K/\mathbf{Q}} : \mathcal{I}(\mathcal{O}_K) \to \mathbf{Q}^*$ the ideal norm, i.e., the homomorphism that maps a prime $\mathfrak{p}$ of $\mathcal{O}_K$ to $N_{K/\mathbf{Q}}\mathfrak{p} = p^{f(\mathfrak{p}/p)}$. Show the compatiblity
$$|N_{K/\mathbf{Q}}(x)| = N_{K/\mathbf{Q}}(x\mathcal{O}_K)$$
of the ideal norm of a principal ideal $x\mathcal{O}_K$ with the element norm $N_{K/\mathbf{Q}}(x)$ of x.
5. Let R be a number ring. Show by an example that the norm map $I \mapsto N(I) = [R : I]$ on the set of integral R-ideals is not necessarily multiplicative.
6. Let K be a field and $f = \sum_{i=0}^{n} a_i X^i \in K[X]$ a monic irreducible polynomial. Define $L = K[X]/(f)$ and $x = X \bmod (f)$. Write the multiplication map $M_x : L \to L$ as a matrix with respect to the basis $1, x, x^2, \ldots, x^{n-1}$ of L/K and verify that M_x has characteristic polynomial f.
7. Let K be a number field of degree n. Show that there is an isomorphism $K \otimes_{\mathbf{Q}} \mathbf{C} \cong \mathbf{C}^n$ mapping $k \otimes z$ to $(z\sigma(k))_{\sigma \in \mathrm{Hom}(K,\mathbf{C})}$. Deduce: $N_{K/\mathbf{Q}}(x) = \prod_\sigma \sigma(x)$ and $\mathrm{Tr}_{K/\mathbf{Q}}(x) = \sum_\sigma \sigma(x)$.
8. Let $\{x_1, x_2, \ldots, x_n\}$ be a basis for the separable field extension L/K and $\{x_1^*, x_2^*, \ldots, x_n^*\}$ the dual basis. Prove: $\Delta(x_1, x_2, \ldots, x_n) \cdot \Delta(x_1^*, x_2^*, \ldots, x_n^*) = 1$.
9. Show that for a squarefree integer $d \neq 1$, the corresponding quadratic field $K = \mathbf{Q}(\sqrt{d})$ has discriminant
$$\Delta_K = \begin{cases} 4d & \text{if } d \equiv 2 \text{ or } 3 \bmod 4; \\ d & \text{if } d \equiv 1 \bmod 4. \end{cases}$$
10. A free A-algebra of finite rank B is *separable* over A if $\Delta(B/A)$ is a unit in A.
    a. When is a finite field extension separable in this sense?
    b. Show that B is separable over A if and only if the natural map $B \to \mathrm{Hom}_A(B, A)$ sending b to the homomorphism $x \mapsto \mathrm{Tr}_{B/A}(xb)$ is an isomorphism of A-modules.
    c. Show that if B is separable over A, then $B' = B \otimes_A A'$ is separable over A' for any base change $A \to A'$. Does the converse hold?
11. Let K be a number field and $\alpha \in \mathcal{O}_K$ an element such that $\alpha \notin k\mathcal{O}_K$ for any $k \in \mathbf{Z}_{>1}$. Show that there exists an integral basis for $\mathcal{O}_K$ containing α. Deduce that we can choose $\omega_1 = 1$ in every integral basis.

12. Let K be a number field and $2s$ the number of embeddings $\sigma : K \to \mathbf{C}$ with $\sigma[K] \not\subset \mathbf{R}$. Show that we have $\mathrm{sign}(\Delta_K) = (-1)^s$.

13. *(Stickelberger's criterion.)* Show that the discriminant of an order R satisfies

$$\Delta(R) \equiv 0 \text{ or } 1 \bmod 4.$$

[Hint: the discriminant is of the form $(P-N)^2$, where $P = \sum_\pi \prod_{i=1}^n \sigma_i(\omega_{\pi(i)})$ with π ranging over the even permutations of $\{1, 2, \ldots, n\}$.]

14. Let $K = \mathbf{Q}(\alpha)$ be of degree n with $\alpha \in \mathcal{O}_K$ integral. Show the following:
    a. $\mathbf{Z}[\alpha]$ is regular above p if and only if the natural map $\mathbf{Z}[\alpha] \to \mathcal{O}_K/p\mathcal{O}_K$ is surjective;
    b. $\mathbf{Z}[\alpha]$ is not regular above a prime $p < n$ that splits completely in $\mathcal{O}_K$;
    c. $\mathcal{O}_K$ is not of the form $\mathbf{Z}[x]$ for any $x \in K$ if some prime $p < n$ splits completely in $\mathcal{O}_K$.

15. Let $K = \mathbf{Q}(\alpha)$ with $\alpha^3+\alpha^2-2\alpha+8 = 0$. Show that we have $\mathcal{O}_K = \mathbf{Z}[\alpha, \frac{\alpha+\alpha^2}{2}]$ and $\mathcal{O}_K \neq \mathbf{Z}[\beta]$ for every $\beta \in \mathcal{O}_K$. (This example is due to Dedekind.)

16. Determine the ring of integers and the discriminant of the field $K = \mathbf{Q}(\sqrt[3]{20})$. Show that there is no $\alpha \in \mathcal{O}_K$ such that $\mathcal{O}_K = \mathbf{Z}[\alpha]$.
[Hint: the equation $2a^3 - 5b^3 = \pm 1$ has no solutions modulo 7.]

17. Let d be an integer that is not a cube. Compute the ring of integers of $K = \mathbf{Q}(\sqrt[3]{d})$.
[You may want to start with the easier cases $3 \nmid d$ or d squarefree.]

18. Prove the identities

$$\Delta(X^3 - aX - b) = 4a^3 - 27b^2 \qquad \text{and} \qquad \Delta(X^n + a) = (-1)^{\frac{1}{2}n(n-1)} n^n a^{n-1}$$

for $n \in \mathbf{Z}_{>0}$ and a, b in some field K.

19. *(Power sums.)* Let K be a field and $f = \prod_{i=1}^n (X - \alpha_i) \in K[X]$ a separable polynomial. Define the *power sums* p_k of f for $k \in \mathbf{Z}$ by $p_k = \sum_{i=1}^n \alpha_i^k$. Show that the discriminant of f equals

$$\Delta(f) = \det(p_{i+j-2})_{i,j=1}^n.$$

20. *(Newton's formulas.)* Let K be a field and $f = \prod_{i=1}^n (X - \alpha_i) = \sum_{k=0}^n a_k X^{n-k} \in K[X]$ a monic polynomial of degree n with zeroes $\alpha_1, \alpha_2, \ldots, \alpha_n \in \overline{K}$. Put $a_k = 0$ whenever $k > n$, and define the power sums of f by $p_k = \sum_{i=1}^n \alpha_i^k$ as in the previous exercise. Show that for every $k \geq 1$ one has

$$k a_k + \sum_{j=0}^{k-1} a_j p_{k-j} = 0.$$

[Hint: Compute the logarithmic derivative of $\prod_{i=1}^n (1 - \alpha_i T)$.]

21. Set $f = X^4+X^2+X+1$. Compute the power sums p_k of f for $0 \leq k \leq 6$ and the discriminant $\Delta(f)$. Show also that f is irreducible over $\mathbf{Q}$, and that $\mathbf{Z}[X]/(f)$ is a Dedekind domain.

22. Let p be a prime number. Compute the discriminant of the cyclotomic field $\mathbf{Q}(\zeta_{p^k})$.

23. Compute the different $\mathfrak{D}_K$ for a quadratic number field.

24. Same question for $\mathbf{Q}(\sqrt[3]{-19})$.

25. Let R be a number ring with normalization $\widetilde{R}$. The *conductor* of R is defined as

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

Show that $\mathfrak{f}_R$ is the largest $\widetilde{R}$-ideal that is contained in R, and that a prime $\mathfrak{p}$ of R divides $\mathfrak{f}_R$ if and only if it is singular.

26. Compute the singular primes, the conductor and the normalization of the order $\mathbf{Z}[\sqrt[3]{37}]$.

27. Let R be an order in a quadratic field K. Show that we have $R = \mathbf{Z} + f\mathcal{O}_K$ for some unique non-negative integer $f \in \mathbf{Z}$. Express the conductor $\mathfrak{f}_R$ in terms of f.

28. Let $\mathcal{O}$ be the ring of integers of a real quadratic field K of odd discriminant, and $R \subset \mathcal{O}$ the order of index 2 in $\mathcal{O}$. Suppose that we have $R^* \neq \mathcal{O}^*$. Prove: $[\mathcal{O}^* : R^*] = 3$ and $K = \mathbf{Q}(\sqrt{d})$ for some positive squarefree integer $d \equiv 5 \bmod 8$.
[Compare with exercise 1.12.]

29. *(Euler's identities.)* Let $K = \mathbf{Q}(\alpha)$ be a number field of degree n.

    a. Show that the $\mathbf{Q}$-basis of K that is trace dual to the power basis $\{\alpha^i\}_{i=0}^{n-1}$ equals $\{b_i\}_{i=0}^{n-1}$, with $b_i \in K$ defined by

$$\frac{f(X)}{f'(\alpha)(X-\alpha)} = b_0 + b_1 X + \ldots + b_{n-1}X^{n-1} \in K[X].$$

    b. Suppose that α is integral. Show that we have $\mathbf{Z}[\alpha]^\dagger = f'(\alpha)^{-1}\mathbf{Z}[\alpha]$. Deduce that we have $\mathfrak{D}_K = f'(\alpha)\mathcal{O}_K$ if $\mathbf{Z}[\alpha]$ is the ring of integers of K.

    [Hint: Show that the polynomial $g = \frac{\alpha^r f(X)}{f'(\alpha)(X-\alpha)} \in K[X]$ satisfies $\mathrm{Tr}_{K/\mathbf{Q}}\, g = X^r$, where the trace of the polynomial is taken coefficientwise.]

30. *(Linear independence of group characters, Artin-Dedekind.)* Show that distinct group homomorphisms $\sigma_i : G \to C^*$ from a group G to the unit group of a field C are linearly independent over C, i.e. the expression

$$a_1\sigma_1(g) + a_2\sigma_2(g) + \ldots + a_n\sigma_n(g)$$

with $a_i \in C$ is non-zero for some $g \in G$ unless $a_1 = a_2 = \ldots = a_n = 0$. Deduce that the discriminant of a basis in a finite separable extension is non-zero.
[Hint: Assume we have a dependence relation with n minimal. Then $n > 1$, and for $g, g' \in G$ we can subtract $\sigma_1(g')$ times the relation for g from the relation for gg' to obtain a relation without σ_1.]

31. Let A be a number ring and $B = A[\alpha]$ a simple integral extension obtained by adjoining a zero in an extension of $K = Q(A)$ of a polynomial $f \in A[X]$ that is irreducible in $K[X]$. Let $\mathfrak{p}$ be a regular prime of A. Formulate and prove the analogue of 3.1 for the primes in B extending $\mathfrak{p}$.

32. Show that the normalization of $R = \mathbf{Z}[\sqrt[4]{-19}]$ is $\widetilde{R} = R[\gamma]$ with $\gamma = (\sqrt{-19}+1)/2$.
[Hint: put $A = \mathbf{Z}[\gamma]$ and $B = A[\sqrt[4]{-19}]$ and apply the theorem in the previous exercise.]

5 Geometry of numbers

In this section, we prove the classical finiteness theorems for a number ring R: the Picard group $\mathrm{Pic}(R)$ is a *finite* group, and the unit group R^* is in many cases finitely generated. These are not properties of arbitrary Dedekind domains, and the proofs rely on the special fact that number rings can be embedded in a natural way as lattices in a finite dimensional real vector space. The key ingredient in the proofs is non-algebraic: it is the theorem of Minkowski on the existence of lattice points in symmetric convex bodies given in 5.1.

▶ Minkowski's theorem

Let V be a vector space of finite dimension n over the field $\mathbf{R}$ of real numbers, and $\langle \cdot, \cdot \rangle : V \times V \to \mathbf{R}$ a scalar product, i.e., a positive definite bilinear form on $V \times V$. The scalar product induces a notion of volume on V, which is also known as the *Haar measure* on V. For a parallelepiped

$$B = \{r_1 x_1 + r_2 x_2 + \ldots + r_n x_n : 0 \leq r_i < 1\}$$

spanned by $x_1, x_2, \ldots, x_n$, the volume is defined by

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

This definition shows that the 'unit cube' spanned by an orthonormal basis for V has volume 1, and that 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 $x_i = (x_{ik})_{k=1}^n$, 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 uniquely extended to a measure on V. Under the identification $V \cong \mathbf{R}^n$ via an orthonormal basis for V, this is the Lebesgue measure on $\mathbf{R}^n$. We usually summarize these properties by saying that V is an n-dimensional *Euclidean space*.

A *lattice* in V is a subgroup of V of the form

$$L = \mathbf{Z} \cdot x_1 + \mathbf{Z} \cdot x_2 + \ldots + \mathbf{Z} \cdot x_k,$$

with $x_1, x_2, \ldots, x_k \in V$ linearly independent. The integer k is the *rank* of L. It cannot exceed $n = \dim V$, and we say that L is *complete* or has *maximal rank* if it is equal to n. For a complete lattice $L \subset V$, the *co-volume* $\mathrm{vol}(V/L)$ of L is defined as the volume of the 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.

A subset $X \subset V$ is said to be *symmetric* if it satisfies $-X = \{-x : x \in X\} = X$.

5.1. Minkowski's theorem. *Let L be a complete lattice in an n-dimensional Euclidean space V and $X \subset V$ a bounded, convex, symmetric subset satisfying*

$$\mathrm{vol}(X) > 2^n \cdot \mathrm{vol}(V/L).$$

Then X contains a non-zero lattice point. If X is closed, the same is true under the weaker assumption $\mathrm{vol}(X) \geq 2^n \cdot \mathrm{vol}(V/L)$.

Proof. By assumption, the set $\frac{1}{2}X = \{\frac{1}{2}x : x \in X\}$ has volume $\mathrm{vol}(\frac{1}{2}X) = 2^{-n}\,\mathrm{vol}(X) > \mathrm{vol}(V/L)$. This implies that the map $\frac{1}{2}X \to V/L$ cannot be injective, so there are 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 volume $\mathrm{vol}(X) \geq 2^n\,\mathrm{vol}(V/L)$, each of the sets $X_k = (1 + 1/k)X$ with $k \in \mathbf{Z}_{\geq 1}$ contains a non-zero lattice point $\omega_k \in L$. As all ω_k are contained in the bounded set $2X$, there are only finitely many different possibilities for ω_k. It follows that there is a lattice element $\omega \in \bigcap_k X_k$, and for closed X we have $\bigcap_k X_k = X$. □

▶ Number rings as lattices

Let K be a number field of degree n. Then K is an n-dimensional $\mathbf{Q}$-vector space, and by base extension we can map K into the complex vector space

$$K_{\mathbf{C}} = K \otimes_{\mathbf{Q}} \mathbf{C} \cong \prod_{\sigma : K \to \mathbf{C}} \mathbf{C} = \mathbf{C}^n$$

by the canonical map $\Phi_K : x \mapsto (\sigma(x))_\sigma$. Note that Φ_K is a ring homomorphism, and that the norm and trace on the free $\mathbf{C}$-algebra $K_{\mathbf{C}}$ extend the norm and the trace of the field extension $K/\mathbf{Q}$. The image $\Phi_K[K]$ of K under the embedding lies in the $\mathbf{R}$-algebra

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

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

On $K_{\mathbf{C}} \cong \mathbf{C}^n$, we have the standard hermitian scalar product $\langle \cdot, \cdot \rangle$. It satisfies $\langle Fz_1, Fz_2 \rangle = \overline{\langle z_1, z_2 \rangle}$, so its restriction to $K_{\mathbf{R}}$ is a real scalar product that equips $K_{\mathbf{R}}$ with a Euclidean structure. In particular, we have a *canonical* volume function on $K_{\mathbf{R}}$. It naturally leads us to the following fundamental observation.

5.2. Lemma. *Let R be an order in a number field K. Then $\Phi_K[R]$ is a lattice of co-volume $|\Delta(R)|^{1/2}$ in $K_{\mathbf{R}}$.*

Proof. Choose a $\mathbf{Z}$-basis $\{x_1, x_2, \ldots, x_n\}$ for R. Then $\Phi_K[R]$ is spanned by the vectors $(\sigma x_i)_\sigma \in K_{\mathbf{R}}$, and using the matrix $X = (\sigma_i(x_j))_{i,j=1}^n$ from the proof of 4.6, we see that the co-volume of $\Phi_K[R]$ equals

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

If $I \subset R$ is a non-zero ideal of norm $N(I) = [R : I] \in \mathbf{Z}$, then 5.2 implies that $\Phi_K[I]$ is a lattice of co-volume $N(I) \cdot |\Delta(R)|^{1/2}$ in $K_{\mathbf{R}}$. To this lattice in $K_{\mathbf{R}}$ we will apply Minkowski's theorem 5.1, which states that every sufficiently large symmetric box in $K_{\mathbf{R}}$ contains a non-zero element of $\Phi_K[I]$.

In order to compute volumes in $K_{\mathbf{R}}$, we have a closer look at its Euclidean structure. Denote the real embeddings of K in $\mathbf{C}$ by $\sigma_1, \sigma_2, \ldots, \sigma_r$ and the pairs of complex embeddings of K by $\sigma_{r+1}, \overline{\sigma_{r+1}}, \sigma_{r+2}, \overline{\sigma_{r+2}}, \ldots, \sigma_{r+s}, \overline{\sigma_{r+s}}$. Then we have $r + 2s = n = [K : \mathbf{Q}]$, and an isomorphism of $\mathbf{R}$-algebras

$$\begin{aligned} K_{\mathbf{R}} &\longrightarrow \mathbf{R}^r \times \mathbf{C}^s \\ (z_\sigma)_\sigma &\longmapsto (z_{\sigma_i})_{i=1}^{r+s}. \end{aligned} \tag{5.3}$$

The inner product on $K_{\mathbf{R}}$ is taken componentwise, with the understanding that at a complex component, the inner product of elements $z_1 = x_1 + iy_1$ and $z_2 = x_2 + iy_2 \in \mathbf{C}$ equals

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

Note that this differs by a factor 2 from the inner product under the 'standard identification' $\mathbf{C} = \mathbf{R}^2$ of $\mathbf{C}$ as the 'complex plane'. For this reason, volumes in $K_{\mathbf{R}}$ are 2^s times *larger* than they are in $\mathbf{R}^r \times \mathbf{C}^s$ with the 'standard' Euclidean structure.

▶ Finiteness of Picard groups

As a direct application of Minkowski's theorem, we can show that in a number ring R that is an *order*, every ideal $I \subset R$ contains an element $x \neq 0$ that is not much larger than $N(I)$. As a consequence, we deduce that the Picard group $\mathrm{Pic}(R)$ is finite.

5.4. Theorem. *Let R be an order in a number field K with s pairs of complex embeddings. Then every ideal class in the Picard group $\mathrm{Pic}(R)$ contains an integral ideal of norm at most $\left(\frac{2}{\pi}\right)^s |\Delta(R)|^{1/2}$, and $\mathrm{Pic}(R)$ is a finite abelian group.*

Proof. Let $I \subset R$ be an ideal and $X_t \subset K_{\mathbf{R}}$ the closed box consisting of elements $(z_\sigma)_\sigma$ with $|z_\sigma| \leq t$ for all σ. Then $X_t \subset \mathbf{R}^r \times \mathbf{C}^s$ is a product of r real intervals $[-t, t]$ and s disks in $\mathbf{C}$ of radius t, so its *canonical* volume in $K_{\mathbf{R}}$ equals

$$\mathrm{vol}(X_t) = 2^s \cdot (2t)^r (\pi t^2)^s = 2^{r+s}\pi^s t^n.$$

Minkowski's theorem 5.1 implies that X_t contains a non-zero element $\Phi_K(x) \in \Phi_K[I] \cap X_t$, provided that we have $2^{r+s}\pi^s t^n \geq 2^n N(I)|\Delta(R)|^{1/2}$. We therefore choose $t \in \mathbf{R}_{>0}$ to satisfy

$$t^n = \left(\tfrac{2}{\pi}\right)^s N(I) \cdot |\Delta(R)|^{1/2}.$$

The norm of the element $x \in I$ obtained satisfies $|N_{K/\mathbf{Q}}(x)| = \prod_\sigma |\sigma(x)| \leq t^n$ since all $|\sigma(x)|$ are bounded by t, so we conclude that every integral R-ideal I contains a non-zero element x of norm $|N_{K/\mathbf{Q}}(x)| \leq \left(\frac{2}{\pi}\right)^s N(I) \cdot |\Delta(R)|^{1/2}$.

If I is invertible, the element $x \in I$ we just found gives rise to an integral ideal xI^{-1} in the ideal class $[I^{-1}] \in \mathrm{Pic}(R)$ of norm at most $\left(\frac{2}{\pi}\right)^s |\Delta(R)|^{1/2}$. As I was arbitrary, this implies that *every* ideal class in $\mathrm{Pic}(R)$ contains an integral ideal satisfying this norm bound. There are only finitely many ideals in R having norm below a given bound, so we find that $\mathrm{Pic}(R)$ is finite. □

For $R = \mathcal{O}_K$ the ring of integers of a number field K, the Picard group $\mathrm{Pic}(R)$ is the class group

$$\mathrm{Cl}(K) = \mathrm{Cl}(\mathcal{O}_K)$$

of K, and its order is known as the *class number* h_K of K. It is a fundamental invariant of the number field K.

Exercise 1. Show that $\mathrm{Pic}(R)$ is finite for every Dedekind domain $R \subset K$. [Hint: use exercise 3.28.]

As the primary ideals occurring in the factorization of an invertible integral ideal $I \subset R$ have norm at most $N(I)$, it follows from 5.4 that for an order R, the Picard group is generated by primary ideals of norm at most $\left(\frac{2}{\pi}\right)^s |\Delta(R)|^{1/2}$. For the ring of integers of K, we find that $\mathrm{Cl}(\mathcal{O}_K)$ is generated by prime ideals of norm at most $\left(\frac{2}{\pi}\right)^s |\Delta_K|^{1/2}$. This enables us to find an explicit set of generators of the class group by factoring the rational primes up to this bound.

5.5. Examples. For the Dedekind domain $R = \mathbf{Z}[\sqrt{-5}]$ we have $\Delta(R) = -20$, so $\mathrm{Pic}(R)$ is generated by the ideal classes of the primes of norm at most $\left(\frac{2}{\pi}\right)\sqrt{20} < 3$. The unique prime $\mathfrak{p} = (2, 1+\sqrt{-5})$ of norm 2 in R is non-principal, but its square is generated by 2. We find that $\mathrm{Pic}(R) \cong \mathbf{Z}/2\mathbf{Z}$ is generated by $[\mathfrak{p}_2]$, and that $\mathbf{Q}(\sqrt{-5})$ is a field of class number 2.

The ring $R = \mathbf{Z}[\sqrt{-19}]$ is not a Dedekind domain. By 3.11 the prime 3 is inert in R, so the only primary R-ideals of norm at most $\left(\frac{2}{\pi}\right)\sqrt{4 \cdot 19} < 6$ are the non-invertible prime $\mathfrak{p}_2 = (2, 1+\sqrt{-19})$, the principal ideal (2) and the prime ideals $\mathfrak{p}_5 = (5, 1+\sqrt{-19})$ and $\mathfrak{q}_5 = (5, 1-\sqrt{-19})$ lying over 5. As $\mathfrak{p}_5\mathfrak{q}_5 = (5)$ is principal, we find that $\mathrm{Pic}(R)$ is generated by $\mathfrak{p}_5$. As $\mathfrak{p}_5$ is non-principal with cube $\mathfrak{p}_5^3 = (7+2\sqrt{-19})$, the Picard group $\mathrm{Pic}(R)$ is cyclic of order 3.

Let $\mathcal{O} = \mathbf{Z}[(1+\sqrt{-19})/2]$ be the integral closure of the ring $\mathbf{Z}[\sqrt{-19}]$ just considered. Then 2 is inert in $\mathcal{O}$, so there are no primes in $\mathcal{O}$ of norm smaller than $\frac{2}{\pi}\sqrt{19} < 3$. It follows that no primes are needed to generate the class group, so $\mathrm{Pic}(\mathcal{O})$ is trivial and $\mathbf{Q}(\sqrt{-19})$ has class number 1.

▶ Minkowski's constant

The constant $\left(\frac{2}{\pi}\right)^s$ in 5.4 can be improved if we can replace X_t by a box of the same volume containing elements of *smaller* norm. A look at the real quadratic case in the pictures below suggests that we should take $X_t \subset K_{\mathbf{R}}$ of the form

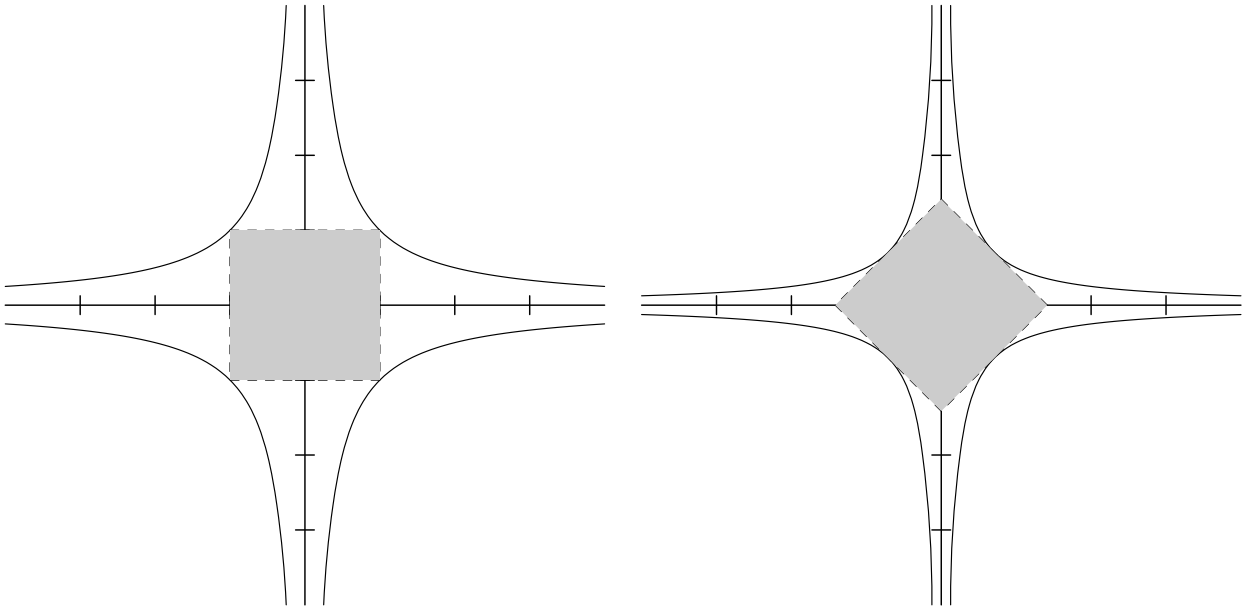
$$X_t = \{(z_\sigma)_\sigma \in K_{\mathbf{R}} : \sum_\sigma |z_\sigma| \leq t\}. \tag{5.6}$$

Computing the volume of the box X_t in (5.6) is an exercise in integration.

5.7. Lemma. *The box $X_t \subset K_{\mathbf{R}}$ in (5.6) has canonical volume* $\mathrm{vol}(X_t) = 2^r\pi^s\frac{t^n}{n!}$.

Proof. Inside $\mathbf{R}^r \times \mathbf{C}^s$, our box takes the shape

$$X_t = \{((x_i)_i, (z_j)_j) \in \mathbf{R}^r \times \mathbf{C}^s : \sum\nolimits_i |x_i| + 2\sum\nolimits_j |z_j| \leq t\},$$



and we need to show that this box has 'standard volume' $V_{r,s}(t) = 2^r \left(\frac{\pi}{2}\right)^s t^n n!$. As the volume function is a real valued function depending on two integral parameters r and s, we can apply induction with respect to each of these parameters.

We note first that $V_{1,0}(t) = \mathrm{vol}([-t,t]) = 2t$ and $V_{0,1}(t) = \mathrm{vol}(\{|z| \le t/2\}) = \pi t^2/4$ have the required value. For $V_{r+1,s}(t)$ we use the induction hypothesis to obtain

$$V_{r+1,s}(t) = \int_{x=-t}^{t} V_{r,s}(t-|x|)dx = 2^r \left(\frac{\pi}{2}\right)^s \cdot 2 \int_{x=0}^{t} \frac{(t-x)^n}{n!} dx = 2^{r+1} \left(\frac{\pi}{2}\right)^s \frac{t^{n+1}}{(n+1)!}.$$

For $V_{r,s+1}(t)$ the method is similar, but we have to integrate with respect to a complex variable $z = x + iy = \rho e^{i\theta}$ to obtain its value

$$V_{r,s+1}(t) = \int_{|z|<t/2} V_{r,s}(t-2|z|)dxdy = 2^r \left(\frac{\pi}{2}\right)^s \cdot 2\pi \int_{\rho=0}^{t/2} \frac{(t-2\rho)^n}{n!} \rho d\rho = 2^r \left(\frac{\pi}{2}\right)^{s+1} \frac{t^{n+2}}{(n+2)!}.$$

This establishes the result. □

5.8. Theorem. *Let R be an order in a number field K of degree n with s pairs of complex embeddings. Then every ideal class of* $\mathrm{Pic}(R)$ *contains an integral ideal of norm not exceeding the Minkowski constant*

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

of the order R.

Proof. As in the proof of 5.4, we need to bound the absolute value of the norm of an element $x = (z_\sigma)_\sigma \in X_t$, where t is chosen such that $\mathrm{vol}(X_t) = 2^n N(I)|\Delta_K|^{1/2}$. Using the value $\mathrm{vol}(X_t) = 2^r \pi^s \frac{t^n}{n!}$ from 5.7 and the fact that the geometric mean $(\prod_\sigma |z_\sigma|)^{1/n}$ does not exceed the arithmetic mean $\frac{1}{n}\sum_\sigma |z_\sigma|$, we obtain

$$|N(x)| = \prod_\sigma |z_\sigma| \le (\frac{1}{n}\sum_\sigma |z_\sigma|)^n \le \frac{t^n}{n^n} = \left(\tfrac{4}{\pi}\right)^s \frac{n!}{n^n} \cdot |\Delta(R)|^{1/2}.$$

The result follows as in 5.4. □

5.9. Corollary. *The class group of a number field K is generated by the classes of the prime ideals of norm at most $M_K = \left(\frac{4}{\pi}\right)^s \frac{n!}{n^n}|\Delta_K|^{1/2}$.* □

A second corollary of 5.8 is the existence of a lower bound for discriminants of orders in terms of their rank.

5.10. Corollary. *Let R be an order of rank n over $\mathbf{Z}$. Then we have*

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

One has $b_n \geq \pi^n/4$ for all n, and $\lim_{n\to\infty} b_n^{1/n} = \pi e^2/4 \approx 5.803$.

Proof. As every integral R-ideal has integral norm, we must have $M_R \geq 1$ in 5.8. This yields the inequality. From the identity $b_{n+1}/b_n = (\pi/4)\cdot(1+\frac{1}{n})^{2n} \geq \pi$ we obtain both the lower bound for b_n and the limit behavior $\lim_{n\to\infty} b_n^{1/n} = \lim_{n\to\infty} \frac{b_{n+1}}{b_n} = \pi e^2/4$. □

Better lower bounds for discriminants have been derived around 1975 by complex analytic methods [23]. Our bounds already imply the famous result of Minkowski that there are no number fields $K \neq \mathbf{Q}$ of discriminant 1.

5.11. Corollary. *Let $K \neq \mathbf{Q}$ be a number field. Then there exists a prime p that is ramified in K.*

Proof. For $K \neq \mathbf{Q}$ we have $n \geq 2$ and $|\Delta_K| \geq \pi^2/4 > 2$, so there is a prime dividing Δ_K. This prime ramifies in $K/\mathbf{Q}$ by 4.14. □

▶ Hermite's theorem

It follows from 5.11 and 4.5 that the discriminant of any order $R \neq \mathbf{Z}$ in a number field satisfies $|\Delta(R)| > 1$. There are other restrictions on the values of discriminants, such as the *Stickelberger criterion* $\Delta(R) \equiv 0, 1 \bmod 4$ from exercise 4.13. If R is quadratic over $\mathbf{Z}$, it is uniquely determined by its discriminant. This is not true for orders of higher rank (exercise 18), but the geometry of numbers yields the following finiteness result for orders 'with bounded ramification'.

5.12. Hermite's theorem. *Let $D \in \mathbf{Z}$ be an integer. Then there are, up to isomorphism, only finitely many orders R of discriminant $\Delta(R) = D$.*

Proof. As the ring of integers $\mathcal{O}_K$ of a number field K contains only finitely many orders of bounded index, it suffices in view of 4.10 to show that there are only finitely many isomorphism classes of number fields of discriminant $\Delta_K = D$. The degree n of such K is bounded by 5.10, so we may assume that both D and n are fixed.

Suppose K is a field of degree n with absolute discriminant D. Then we construct a box $X \subset K_{\mathbf{R}}$ that is bounded in terms of D and contains an element $\Phi(x)$ with $K = \mathbf{Q}(x)$ as follows. If K has a real embedding $\tau : K \to \mathbf{R}$ we let X consist of the elements $(z_\sigma)_\sigma \in K_{\mathbf{R}}$ satisfying

$$|z_\tau| \leq C \qquad \text{and} \qquad |z_\sigma| < 1 \quad \text{if } \sigma \neq \tau,$$

where $C \in \mathbf{R}_{>0}$ is chosen to have $\mathrm{vol}(X) > 2^n\sqrt{|D|}$. If K has only complex embeddings and $\tau : K \to \mathbf{C}$ is one of them, we define X as consisting of the elements with

$$z_\tau, z_{\overline{\tau}} \in [-1,1] + [-C,C]i \subset \mathbf{C} \qquad \text{and} \qquad |z_\sigma| \leq 1 \quad \text{if } \sigma \neq \tau, \overline{\tau},$$

with $C \in \mathbf{R}_{>0}$ such that again $\mathrm{vol}(X) = 2^n\sqrt{|D|}$. In both cases, X is symmetric and convex and C depends on D but not on K.

By 5.1 and 5.2, there exists a non-zero element $x \in \mathcal{O}_K$ such that $\Phi(x) = (\sigma(x))_\sigma$ is contained in X. We will show that $K = \mathbf{Q}(x)$ for this x. As the embeddings $\sigma : K \to \mathbf{C}$ are the $[K : \mathbf{Q}(x)]$ extensions to K of each of the $[\mathbf{Q}(x) : \mathbf{Q}]$ embeddings $\mathbf{Q}(x) \to \mathbf{C}$, it suffices to show that for our chosen τ, we have $\sigma(x) \neq \tau(x)$ whenever $\sigma \neq \tau$. In the case that τ is a real embedding, we cannot have $\tau(x) = \sigma(x)$ for any $\sigma \neq \tau$ as this would imply $|\sigma(x)| < 1$ for *all* embeddings $\sigma : K \to \mathbf{C}$ and therefore $|N_{K/\mathbf{Q}}(x)| = \prod_\sigma |\sigma(x)| < 1$. This obviously cannot happen for the non-zero integer $N_{K/\mathbf{Q}}(x) \in \mathbf{Z}$. In the case that τ is a complex embedding, the same argument shows that $\tau(x) \neq \sigma(x)$ if $\sigma \neq \tau, \overline{\tau}$. We also cannot have $\tau(x) = \overline{\tau}(x)$, since this would imply that $\tau(x)$ is a real element in $(-1,1) + (-C,C)i$, which leads to the same impossible estimate $|\tau(x)| < 1$.

We conclude that K is generated over $\mathbf{Q}$ by an element $x \in \mathcal{O}_K$ with $\Phi(x) \in X$. This means that the zeroes $\sigma(x) \in \mathbf{C}$ of the irreducible polynomial $f^x_{\mathbf{Q}} \in \mathbf{Z}[X]$ have an absolute value that can be bounded in terms of D. As the degree n of $f^x_{\mathbf{Q}}$ is fixed, we can also bound the coefficients of $f^x_{\mathbf{Q}}$ in $\mathbf{Z}$. It follows that, given D, there are only finitely many possibilities for $f^x_{\mathbf{Q}}$, and therefore the number of possible $K \subset \overline{\mathbf{Q}}$ is also finite. □

Given $r, s \in \mathbf{Z}_{\geq 0}$, it is a challenging problem to *count* up to isomorphism the number $S_{r,s}(X)$ of number fields K having r real and $2s$ complex embeddings and satisfying $|\Delta_K| < X$. One can do this exactly for given X, or asymptotically for $X \to \infty$. Hermite's theorem, though in principle constructive, does not provide a direct answer to these questions. Only recently one has been able to obtain answers in cases with $n = r + 2s > 3$.

Exercise 2. Find asymptotic expressions for $S_{2,0}(X)$ and $S_{0,1}(X)$.

▶ Dirichlet's unit theorem

As a final application of Minkowski's theorem, we show that the unit group of an order R in a number field with r real and $2s$ complex embeddings is *finitely generated* of free rank $r + s - 1$. The classical formulation of this result is as follows.

5.13. Dirichlet unit theorem. *Let R be an order admitting r real and $2s$ complex embeddings, and write μ_R for the group of roots of unity in R. Then μ_R is finite, and R^*/μ_R is a free abelian group of rank $r + s - 1$.*

More explicitly but less canonically, 5.13 states that there exists a finite set $\eta_1, \eta_2, \ldots, \eta_{r+s-1}$ of *fundamental units* such that we have

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

Such a system of fundamental units, which forms a $\mathbf{Z}$-basis for R^*/μ_R, is only unique up to coordinate transformations and multiplication by roots of unity. In the real quadratic case

$R = \mathbf{Z}[\sqrt{d}]$, we saw already that the fundamental unit solving the Pell equation $x^2 - dy^2 = \pm 1$ is only unique up to sign and inversion.

In case $r > 0$ we have $\mu_R = \{\pm 1\}$ as there are no other roots of unity in $\mathbf{R}$. In general one has $\mu_R \subset \mu_K = \langle \zeta_m \rangle$ with m the largest integer for which the m-th cyclotomic field $\mathbf{Q}(\zeta_m)$ can be embedded in K. For such m, the degree $[\mathbf{Q}(\zeta_m) : \mathbf{Q}] = \phi(m)$ divides $[K : \mathbf{Q}]$ and the odd prime factors of m all divide Δ_K. This severely restricts m, and in practice the groups μ_K and μ_R are also easily determined in the *totally complex* case $r = 0$.

In order to prove 5.13, we reformulate it in terms of our $\mathbf{R}$-algebra $K_{\mathbf{R}}$. As we are now dealing with a subgroup the *multiplicative* group K^*, we consider the embedding

$$\Phi : K^* \to K_{\mathbf{R}}^* = \{(z_\sigma)_\sigma \in K_{\mathbf{C}}^* : \overline{z}_\sigma = z_{\overline{\sigma}}\}.$$

As the geometry of numbers with its lattices prefers to work with additive groups, we apply the logarithm componentwise on the unit group $K_{\mathbf{C}}^* = (\mathbf{C}^*)^n$ of $K_{\mathbf{C}}$ to obtain a homomorphism $\mathrm{Log}\colon K_{\mathbf{C}}^* \to \mathbf{R}^n$ that sends $(z_\sigma)_\sigma$ to $(\log|z_\sigma|)_\sigma$. Write $L : R^* \to \mathbf{R}^n$ for the composition of Φ with this logarithmic map. With this notation, the Dirichlet unit theorem can be phrased as follows.

5.14. Theorem. *Let R be an order admitting r real and $2s$ complex embeddings. Then the homomorphism $L : R^* \to \mathbf{R}^n$ that sends $x \in R^*$ to $(\log|\sigma x|)_\sigma$ has a finite cyclic kernel μ_R consisting of the roots of unity in R^* and maps R^* to a lattice of rank $r + s - 1$ in $\mathbf{R}^n$.*

Proof. For every bounded set $B = [-M, M]^n \subset \mathbf{R}^n$, the inverse image in $K_{\mathbf{R}}^*$ under the logarithmic map is the bounded set $\{(z_\sigma)_\sigma \in K_{\mathbf{R}} : e^{-M} \leq |z_\sigma| \leq e^M\}$. The intersection of this set with the lattice $\Phi(R)$ is finite, so the inverse image $L^{-1}[B] \subset R^*$ is also finite. This implies first of all that $L[R^*]$ is a discrete subgroup of $\mathbf{R}^n$, i.e. a lattice in $\mathbf{R}^n$. Secondly, taking $M = 0$, we see that $\ker L$ is a finite subgroup of R^*. The elements in this group have finite order, so they are roots of unity. As every root of unity in R is clearly in $\ker L$, we have $\ker L = \mu_R$. As this is a finite subgroup of K^*, it is cyclic.

It is easy to see that the image $L[R^*]$ is a lattice in an $r + s - 1$ dimensional subspace of $\mathbf{R}^n$. First of all, we have $\log|\sigma(x)| = \log|\overline{\sigma}(x)|$ for every $x \in K^*$, so $L[R^*]$ lies in the $(r + s)$-dimensional subspace

$$\mathrm{Log}[K_{\mathbf{R}}^*] = \{(x_\sigma)_\sigma \in \mathbf{R}^n : x_\sigma = x_{\overline{\sigma}}\} \subset \mathbf{R}^n.$$

Secondly, the absolute value $|N(\eta)|$ of the norm of a unit η equals $[R : \eta R] = 1$, so the sum of the coordinates of $L(\eta)$ equals

$$\textstyle\sum_\sigma \log|\sigma(x)| = \log \prod_\sigma |\sigma(x)| = \log|N(\eta)| = 0.$$

We can take the first restriction into account by composing $L : R^* \to \mathbf{R}^n = \mathbf{R}^{r+2s}$ with the surjection $\mathbf{R}^{r+2s} = \mathbf{R}^r \times (\mathbf{R}^2)^s \to \mathbf{R}^{r+s}$ that maps each component $\mathbf{R}^2$ corresponding to a pair of complex conjugate embeddings to $\mathbf{R}$ by *adding* the components. The composition $L' : R^* \to \mathbf{R}^{r+s}$ has the same kernel as L, and its image lies again in the 'trace-zero-hyperplane' $H \subset \mathbf{R}^{r+s}$ consisting of elements $(x_i)_{i=1}^{r+s}$ satisfying $\sum_{i=1}^{r+s} x_i = 0$. The difficult part of the theorem consists in showing that $L'[R^*]$ is a lattice in H of *maximal* rank.

Let $E \subset K_{\mathbf{R}}^*$ be defined as the 'norm-1-subspace'

$$E = \{(z_\sigma)_\sigma : \textstyle\prod_\sigma z_\sigma = \pm 1\}.$$

Under the composition Log' of the logarithmic map $\mathrm{Log}\colon K_{\mathbf{R}}^* \to \mathbf{R}^n$ with our surjection $\mathbf{R}^n \to \mathbf{R}^{r+s}$, we have $\mathrm{Log}'[E] = H$. We will construct a subset $Y \subset E$ such that $\mathrm{Log}'[Y] \subset H$ is *bounded* and satisfies $L[R^*] + \mathrm{Log}'[Y] = H$. By exercise 5, this implies that $L[R^*]$ has maximal rank in H, as we want to show.

Let $X = X_t = \{(z_\sigma)_\sigma \in K_{\mathbf{R}} : |z_\sigma| \leq t \text{ for all } \sigma\}$ be our standard box in $K_{\mathbf{R}}$, and choose t such that we have $\mathrm{vol}(X) = 2^n \cdot |\Delta_K|^{1/2}$. By Minkowski's theorem, X contains a non-zero element of the lattice $\Phi[R]$. For every $e = (e_\sigma)_\sigma \in E$, the set

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

is a box around the origin with volume $\mathrm{vol}(eX) = \mathrm{vol}(X)$, so it also contains an element $\Phi(x_e) \in \Phi[R]$. 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. Suppose that it consists of $\{a_i R\}_{i=1}^k$. We claim that

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

is the required subset of E.

We note first that all boxes $\Phi(a_i^{-1})X$ are bounded in $K_{\mathbf{R}}$, so their union is bounded as well. The absolute values $|y_\sigma|$ of the coordinates of an element $y = (y_\sigma)_\sigma \in Y$ are bounded away from zero since each $|y_\sigma|$ is bounded from above and we have $\prod_\sigma |y_\sigma| = 1$. This implies that $\mathrm{Log}'[Y]$ is a bounded subset of $\mathbf{R}^{r+s}$.

Now let $e \in E$ be arbitrary. Then there exist a non-zero 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 $\Phi(a^{-1})X = \Phi(u)\Phi(a_i^{-1})X$ for some a_i. This proves the inclusion $E \subset \Phi[R^*] \cdot Y$. Applying Log' yields $L[R^*] + \mathrm{Log}'[Y] = H$. □

As the proof of 5.14 relies on Minkowski's theorem 5.1, it is not directly constructive and cannot be used to explicitly find unit groups. Our explicit methods in section 7 will therefore be of a different nature.

The L'-image of R^* is a complete lattice in the 'trace-zero-hyperplane' $H \subset \mathbf{R}^{r+s}$. The co-volume of the lattice obtained by *any* projection $\mathbf{R}^{r+s} \to \mathbf{R}^{r+s-1}$ that leaves out one of the coordinates is called the *regulator* $\mathrm{Reg}\, R$ of R. The proof of 5.14 yields the following explicit definition.

5.15. Definition. *Let K be a number field and $\{\sigma_i\}_{i=1}^{r+s}$ a complete set of pairwise non-conjugate embeddings of K in $\mathbf{C}$. Then the regulator of a set $\{\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_{r+s-1}\}$ of $r+s-1$ elements in K^* of norm ± 1 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^*. We put $\mathrm{Reg}(R) = 1$ if R^* is finite, i.e., if R is either $\mathbf{Z}$ or an imaginary quadratic order. The regulator $R_K = \mathrm{Reg}(\mathcal{O}_K)$ of the ring of integers of K is known as the *regulator* of the number field K. By the Dirichlet unit theorem, regulators of orders do not vanish. Unlike the discriminant of the order, which is an integer, the regulator of an order is a positive real number that is usually transcendental as it is an expression in terms of *logarithms* of algebraic numbers.

Exercise 3. Show that the unit group R^* of an order $R \subset K$ is a subgroup of finite index in $\mathcal{O}_K^*$, and that we have $[\mathcal{O}_K^* : \mu_K R^*] = \mathrm{Reg}(R)/\mathrm{Reg}(\mathcal{O}_K)$.

To conclude this section, we briefly look at the case of number rings R that are not necessarily orders. Any number ring R is by 4.9 of finite index in its normalization $\widetilde{R}$, and if k is this index, then the kernel of the natural map

$$\widetilde{R}^* \longrightarrow (\widetilde{R}/k\widetilde{R})^* \tag{5.16}$$

is a subgroup of finite index of $\widetilde{R}^*$ that is contained in R^* as we have $1 + k\widetilde{R} \subset R$. This implies that R^* is of finite index in $\widetilde{R}^*$, and if $\widetilde{R}^*$ is finitely generated abelian of free rank t, then so is R^*. It may however be that $\widetilde{R}^*$ is not finitely generated – think of the case $R = K$.

EXERCISES.

4. Let $R = \oplus_{i=1}^{n} \mathbf{Z} \cdot \omega_i$ be an order in a number field K. This exercise shows how to prove $\mathrm{Pic}(R)$ finite without any volume computations.
   a. Show that there exists a constant $C = C(K)$ such that
   $$|N_{K/\mathbf{Q}}(\textstyle\sum_{i=1}^{n} a_i\omega_i)| < C \cdot (\max |a_i|)^n.$$
   b. Show that there exists a constant $M = M(R)$ such that for every $x \in K^*$, we can find $\omega \in R$ and $t \in \{1, 2, \ldots, M\}$ with
   $$|N_{K/\mathbf{Q}}(tx - \omega)| < 1.$$
   [Hint: for large M, there exist $1 \leq t_1 < t_2 < M$ for which $t_1 x$ and $t_2 x$ are 'close' in K/R. Take $t = t_2 - t_1$.]
   c. Show that every non-zero ideal $I \subset R$ contains an element α such that αI^{-1} divides $M! \cdot R$. Deduce that $\mathrm{Pic}(R)$ is finite.
   [Hint: take $\alpha \in I$ non-zero with $|N_{K/\mathbf{Q}}(\alpha)|$ minimal. Then every $\beta \in I$ satisfies $t\beta = \alpha\omega \in I$ for some t and ω as in b.]
5. Prove that a subgroup $L \subset \mathbf{R}^n$ is a lattice if and only if it is discrete. For $n = 1$, show that L is either a lattice or a dense subgroup.
6. Show that a lattice $L \subset \mathbf{R}^n$ has maximal rank if and only if the following equivalent conditions hold
   (i) the factor group $\mathbf{R}^n/L$ is compact in the quotient topology;
   (ii) there exists a bounded subset $B \subset \mathbf{R}^n$ such that $L + B = \mathbf{R}^n$.
7. Let V be the set of non-zero lattices $L \subset \mathbf{C}$ that satisfy $x \cdot L \subset L$ for every $x \in \mathbf{Z}[\frac{1+\sqrt{-23}}{2}]$. Show that V becomes an abelian group if we set $L_1 \cdot L_2 = \{\sum x_i y_i \in \mathbf{C} : x_i \in L_1, y_i \in L_2\}$. Let $P \subset V$ be the set of lattices of the form $L_z = \mathbf{Z} \cdot z + \mathbf{Z} \cdot \frac{(1+\sqrt{-23})z}{2}$ with $z \in \mathbf{C}^*$. Show that P is a subgroup of V and that $V/P \cong \mathbf{Z}/3\mathbf{Z}$.
8. *(Minkowski's theorem on linear forms)* Suppose that n linear forms on $\mathbf{R}^n$ with real coefficients are given by $L_i(x) = \sum_{j=1}^{n} a_{ij} x_j$, and that $A = (a_{ij})_{i,j=1}^{n}$ has non-zero determinant. Show that there exists a non-zero element $x \in \mathbf{Z}^n$ satisfying
   $$|L_i(x)| < c_i \quad \text{for } i = 1, 2, \ldots, n$$
   if the constants $c_i \in \mathbf{R}_{>0}$ satisfy $\prod_{i=1}^{n} c_i > |\det A|$.
   Can you find positive integers x, y satisfying
   $$|x\sqrt{7} - y\sqrt{6}| + |x\sqrt{15} - y\sqrt{13}| < 2\sqrt{\sqrt{91} - \sqrt{90}} = 0.458515\ldots?$$
9. Find all integral solutions to the equation $X^2 = Y^3 - 13$.
10. Determine the class number of $\mathbf{Q}(\sqrt{d})$ for $d = -41, -47, -163$.
11. Show that all real quadratic fields of discriminant $\Delta < 40$ have class number 1. What is the class number of $\mathbf{Q}(\sqrt{10})$?

12. *(Lagrange's four squares theorem.)* Let p be a prime number.
    a. Show that there exist $u, v \in \mathbf{Z}$ such that $u^2 + v^2 + 1 \equiv 0 \bmod p$, and that the corresponding lattice
    $$L_{u,v} = \{(a,b,c,d) \in \mathbf{Z}^4 : c \equiv ua + vb \bmod p \quad \text{and} \quad d \equiv ub - va \bmod p\}$$
    has co-volume p^2 in $\mathbf{R}^4$.
    b. Show that every positive integer is the sum of four squares.
    [Hint: for a prime number p this can be deduced from the fact that an open ball of radius $\sqrt{2p}$ in $\mathbf{R}^4$ contains a non-zero lattice point from $L_{u,v}$. Then use the multiplicativity of the norm $N : \mathbf{R}[i,j,k] \to \mathbf{R}$ on the quaternion-algebra.]

13. Apart from the involution F on $K_{\mathbf{C}}$ defined in the text, there is also the 'component-wise' complex conjugation on $K_{\mathbf{C}}$ sending $(z_\sigma)_\sigma$ to $(\overline{z}_\sigma)_\sigma$. We denote it by an overhead bar. Prove that the following conditions are equivalent.
    (i) The automorphism $\overline{\ }$ of $K_{\mathbf{C}}$ maps K to itself;
    (ii) There is a field automorphism τ of K such that for all $x \in K$ and all embeddings $\sigma : K \to \mathbf{C}$ one has $\sigma\tau x = \overline{\sigma x}$;
    (iii) Either K is totally real, or K is a totally imaginary quadratic extension of a totally real field.

    An algebraic number field K is called a *CM-field* if the above three conditions are satisfied. The abbreviation stands for "complex multiplication". This has its origin in a connection with endomorphism rings of elliptic curves and abelian varieties. Give an example of an algebraic number field that is not a CM-field.

14. Let $f \in \mathbf{Z}[X]$ be a monic polynomial. Prove that $|\Delta(f)| = 1$ if and only if there exists $k \in \mathbf{Z}$ such that $f = X - k$ or $f = X^2 - (2k+1)X + k(k+1)$.

15. Let L be a lattice in an n-dimensional Euclidean space V. Prove:
    $$\lim_{t\to\infty} \frac{\#\{x \in L : \sqrt{\langle x, x\rangle} \leq t\}}{t^n} = \frac{\omega_n}{\mathrm{vol}(V/L)},$$
    where $\omega_n = \pi^{n/2}/\Gamma(\frac{n}{2}+1)$ denotes the volume of the unit ball in V.

16. Let R be an order in a number field K. Show that we have $R = \mathcal{O}_K$ if and only if all primes $\mathfrak{p} \subset R$ of index at most the Minkowski constant M_R of R are invertible.

17. Let K be a number field with Minkowski constant $M < 2$.
    a. Prove that $\mathcal{O}_K$ is a principal ideal domain.
    b. Prove that for each $x \in K$ there exists $\omega \in \mathcal{O}_K$ with $|N(x - \omega)| < 1$.
    [Hint: let X be the box in 5.6 with $t = n/2 = [K : \mathbf{Q}]/2$, and set $Y = X \cup (\Phi_K(x) + X)$. Then the map $Y \to K_{\mathbf{R}}/\Phi_K[\mathcal{O}_K]$ is not injective.]
    c. Prove that $\mathcal{O}_K$ is a Euclidean ring.

18. Show that the three cubic fields that are obtained by adjoining to $\mathbf{Q}$ a root of one of the polynomials
    $$X^3 - 18X - 6, \qquad X^3 - 36X - 78, \qquad X^3 - 54X - 150$$
    all have the same discriminant, but that no two of them are isomorphic.

*19. Let K be a a number field of degree n.

a. Let m be a positive integer. Prove that the number of non-zero ideals $I \subset \mathcal{O}_K$ of norm m is less than or equal to the number of vectors $(x_i)_{i=1}^n$ with $x_i \in \mathbf{Z}$, $x_i > 0$, $\prod_{i=1}^n x_i = m$.

b. Let M be the Minkowski constant of K. Prove that the class number h of K satisfies

$$\begin{aligned} h &\leq \mathrm{vol}\{(x_i)_{i=1}^n \in \mathbf{R}_{>0}^n : \textstyle\prod_{i=1}^n \max\{1, x_i\} \leq M\} \\ &\leq M \cdot \frac{(n-1+\log M)^{n-1}}{(n-1)!}. \end{aligned}$$

20. Let R be a subring of a ring A, and suppose that A is integral over R. Show that the unit groups satisfy $A^* \cap R = R^*$. Can the integrality condition be omitted?

21. *(Artin.)* Let K be a cubic field with a single real embedding $\sigma : K \to \mathbf{R}$. Show that the group of units of $\mathcal{O}_K$ that have positive image under σ is isomorphic to $\mathbf{Z}$, and let $u > 1$ be the σ-image of a generator. Show that Δ_K is a negative integer that satisfies

$$|\Delta_K| \leq 4u^3 + 24.$$

[Hint: write the conjugates of the generator as $u = x^2$ and $x^{-1}e^{\pm iy}$ and estimate the function $\phi(x, y) = |\Delta(1, u, u^2)|^{1/2}$ for fixed x.]

22. Let $a \geq 2$ be an integer for which $4a^3 + 27$ is squarefree. Show that the unit group of the ring of integers of the field $\mathbf{Q}(\alpha)$ with $\alpha^3 + a\alpha - 1 = 0$ has rank 1, and that $\alpha \in \mathcal{O}_K^*$ is a fundamental unit.

23. Let $K = \mathbf{Q}(\alpha)$ with $\alpha^3 = \alpha + 1$. Prove that the elements

$$\alpha, \quad \alpha - 1, \quad \alpha^2 - 1, \quad \alpha^3 - 1, \quad (\alpha - 2)^2/(\alpha + 3), \quad (2\alpha - 1)^2/(\alpha + 5)$$

belong to $\mathcal{O}_K^*$ and find a minimal set of generators for the subgroup U generated by these units. Is U equal to $\mathcal{O}_K^*$?

24. Determine the class number and the unit group $\mathcal{O}_K^*$ for each of the following number fields K:

$$\mathbf{Q}(\sqrt[3]{2}), \qquad \mathbf{Q}[X]/(X^3 - X + 2), \qquad \mathbf{Q}(\sqrt{5}, \sqrt{-5}), \qquad \mathbf{Q}(\sqrt{-7}, \sqrt{21}).$$

25. Let $K \subset \mathbf{R}$ be a number field. Show that $\mathcal{O}_K^*$ lies dense in $\mathbf{R}$ if and only if K is either totally real cubic or of degree $n \geq 4$.

26. Let K be a number field and $\Phi : K \to K_{\mathbf{R}}$ the canonical embedding. Show that for any non-zero $x \in \mathcal{O}_K$, the square of the length of $\Phi(x) \in K_{\mathbf{R}}$ satisfies $\langle \Phi(x), \Phi(x) \rangle \geq [K : \mathbf{Q}]$, with equality if and only if x is in μ_K.

27. Let $k > 0$ and $l \geq 0$ be integers and denote by φ the Euler function. Prove that there exists an algebraic number field K for which $\mathcal{O}_K^*$ is isomorphic to $(\mathbf{Z}/k\mathbf{Z}) \oplus \mathbf{Z}^l$ if and only if k is even and $\varphi(k)$ divides $2(l + 1)$.

28. Let n be a positive integer. Suppose one has an equilateral polygon in the Euclidean plane with the property that all angles, with the possible exception of two consecutive ones, are integral multiples of π/n. Show that the remaining two angles are integral multiples of π/n as well.

29. Show that $\mathbf{Z}[\zeta_5]$ is a Euclidean ring with unit group $\mathbf{Z}[\zeta_5]^* = \langle\zeta_{10}\rangle \times \langle\eta\rangle$, where η denotes a fundamental unit in the ring of integers of $\mathbf{Q}(\sqrt{5})$. Express $1+\zeta_5$, $1+\zeta_5+\zeta_5^2$ and $1+\zeta_5+\zeta_5^2+\zeta_5^3$ on this basis.

30. Let K_1 be a real quadratic field and K_2 an imaginary quadratic field. Prove:

$$[\mathcal{O}^*_{K_1K_2} : \mu_{K_1K_2}\mathcal{O}^*_{K_1}] \in \{1, 2\}.$$

Do both values occur?

31. Let $K \subsetneq L$ be an extension of number fields. Show that $[\mathcal{O}_L^* : \mathcal{O}_K^*]$ is finite if and only if L is a totally imaginary CM-field with maximal real subfield K. Show also that if the index is finite, we have

$$[\mathcal{O}_L^* : \mu_L\mathcal{O}_K^*] = 2^{1-[K:\mathbf{Q}]}R_K/R_L.$$

32. Suppose $[\mathcal{O}_L^* : \mathcal{O}_K^*]$ is finite. Show that there is a group homomorphism $\psi\colon \mathcal{O}_L^* \to \mu_L$ that maps $u \in \mathcal{O}_L^*$ to $u/\sigma(u)$, with σ the non-trivial K automorphism of L. Prove also that

$$\ker\psi = \mathcal{O}_K^*, \qquad \#\operatorname{coker}\psi \cdot [\mathcal{O}_L^* : \mathcal{O}_K^* \cdot \mu_L] = 2.$$

33. Let $n > 1$ be an integer, $n \not\equiv 2 \bmod 4$, and $\zeta_n \in \overline{\mathbf{Q}}$ a primitive n-th root of unity.

    a. Prove that the number of roots of unity in $\mathbf{Z}[\zeta_n]$ equals $\operatorname{lcm}(n, 2)$.

    b. Prove that

$$\mathbf{Z}[\zeta_n]^* = \langle\zeta_n\rangle \cdot \mathbf{Z}[\zeta_n + \zeta_n^{-1}]^*$$

    if n is a prime power, and that

$$[\mathbf{Z}[\zeta_n]^* : \langle\zeta_n\rangle \cdot \mathbf{Z}[\zeta_n + \zeta_n^{-1}]^*] = 2,$$
$$\mathbf{Z}[\zeta_n]^* = \langle 1 \pm \zeta_n\rangle \cdot \mathbf{Z}[\zeta_n + \zeta_n^{-1}]^*$$

    if n is not a prime power.

34. Let $K_1 = \mathbf{Q}(\sqrt{d_1})$ and $K_2 = \mathbf{Q}(\sqrt{d_2})$ be distinct real quadratic fields. Define $K_3 = \mathbf{Q}(\sqrt{d_1d_2})$ and $K = K_1K_2$.

    a. Show that $\mathcal{O}^*_{K_1}\mathcal{O}^*_{K_2}\mathcal{O}^*_{K_3}$ is of finite index in $\mathcal{O}_K^*$.

    b. Take $d_1 = 2$ and $d_2 = 3$. Is $\sqrt{2} + \sqrt{3}$ in $\mathcal{O}^*_{K_1}\mathcal{O}^*_{K_2}\mathcal{O}^*_{K_3}$?

6 Zeta functions

In its present form, this section contains just the definition of the zeta function of a number field and, without proof, in 6.3 and 6.5, two of its properties. All we need for the moment is the identity (6.4), which will serve as an independent check to verify the correctness of our computations in of Picard groups and unit groups in the next section.

▶ Dedekind zeta function

The Dedekind zeta-function ζ_K of a number field K is a complex analytic function which, despite its simple definition, encodes a lot of fundamental information on the number field. For $K = \mathbf{Q}$, this zeta function is the well known Riemann zeta-function, which is defined on the complex right half-plane $\mathrm{Re}(t) > 1$ by the formula $\zeta(t) = \sum_{n=1}^{\infty} n^{-t}$. This sum can be viewed as a sum over the non-zero ideals $n\mathbf{Z}$ of the ring of integers $\mathbf{Z}$ of $\mathbf{Q}$, and for arbitrary K, the function ζ_K is defined in a similar way as

$$\zeta_K(t) = \sum_{I \neq 0} (N_{K/\mathbf{Q}}(I))^{-t}, \tag{6.1}$$

where the sum ranges over all non-zero ideals $I \subset \mathcal{O}$ of the ring of integers $\mathcal{O}_K$ of K. The convergence properties of the sum are just as for the Riemann zeta function, and it also has a representation as an *Euler product* over prime ideals, as follows.

6.2. Lemma. *Let $t \in \mathbf{C}$ be a complex number with $\mathrm{Re}(t) > 1$. Then we have an identity*

$$\zeta_K(t) = \sum_{I \neq 0} (N_{K/\mathbf{Q}}(I))^{-t} = \prod_{\mathfrak{p} \text{ prime}} (1 - (N_{K/\mathbf{Q}}(\mathfrak{p}))^{-t})^{-1}$$

in which the sum over $I \neq 0$ and the Euler product over $\mathfrak{p}$ are absolutely convergent. The function $\zeta_K(t)$ is a holomorphic function without zeroes in the half plane $\mathrm{Re}(t) > 1$.

Proof. For each rational prime number p, there are at most $n = [K : \mathbf{Q}]$ primes $\mathfrak{p}|p$, and these primes have $N_{K/\mathbf{Q}}(\mathfrak{p}) \geq p$. The estimate

$$\sum_{N(\mathfrak{p}) \leq X} |N(\mathfrak{p})^{-t}| \leq n \sum_{p \leq X} p^{-\mathrm{Re}(t)}$$

shows that $\sum_{\mathfrak{p}} N(\mathfrak{p})^{-t}$ converges absolutely in the half plane $\mathrm{Re}(t) > 1$, and this implies that the product $\prod_{\mathfrak{p} \text{ prime}} (1 - (N_{K/\mathbf{Q}}(\mathfrak{p}))^{-t})^{-1}$ also converges absolutely for these t. From the geometric series

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

and the fact that every ideal I has a unique factorization as a product of prime ideal powers, it is easily seen that for $t \in \mathbf{R}_{>1}$, the sum $\sum_{I \neq 0} N_{K/\mathbf{Q}}(I)^{-t}$ has positive terms and is bounded by $\prod_{\mathfrak{p}} (1 - (N_{K/\mathbf{Q}}(\mathfrak{p}))^{-t})^{-1}$. It follows that the sum converges absolutely whenever $\mathrm{Re}(t) > 1$. The estimate

$$|\sum_{I \neq 0} N(I)^{-t} - \prod_{N(\mathfrak{p}) \leq X} (1 - N(\mathfrak{p})^{-t})^{-1}| \leq \sum_{N(I) > X} N(I)^{-\mathrm{Re}(t)} \to 0$$

for $X \to \infty$ implies that sum and product coincide. The convergence is uniform on compact subsets of the half plane $\mathrm{Re}(t) > 1$, so the limit function ζ_K is holomorphic on this half plane. The product representation shows that there are no zeroes in this region. □

▶ Analytic class number formula

The sum in (6.1) diverges for $t = 1$, but ζ_K does have a meromorphic continuation to the left of the half space $\mathrm{Re}(t) > 1$ such that $t = 1$ becomes a simple pole for this extended function. Its residue at $t = 1$ involves all basic invariants of the number field, including the class number of $\mathcal{O}_K$.

6.3. Theorem. *Let K be a number field of degree n with r real and $2s$ complex embeddings. Then the zeta-function ζ_K of K admits a meromorphic extension to the half-plane $\mathrm{Re}(t) > 1 - 1/n$. It is holomorphic except for a single pole at $t = 1$ with residue*

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

Here $w_K = \#\mu_K$ is the number of roots of unity in K.

Proof. See [5, Chapter 5, section 1]. □

The formula for the residue $\zeta_K^*(1)$ at $t = 1$ is known as the *analytic class number formula*. It shows that $\zeta_K^*(1)$, and therefore the product $h_K R_K$, can be computed analytically from the limit

$$\zeta_K^*(1) = \lim_{t \to 1} (t-1)\zeta_K(t).$$

As the Riemann zeta function $\zeta_{\mathbf{Q}}$ has a pole with residue 1 at $t = 1$, one can compute $\lim_{t\to 1}(t-1)\zeta_K(t)$ as the limit $\lim_{t\to 1} \zeta_K(t)/\zeta_{\mathbf{Q}}(t)$ of a quotient of zeta functions that is holomorphic at $t = 1$. The quotient of their Euler products is convergent at $t = 1$, and one obtains

$$\frac{2^r(2\pi)^s h_K R_K}{w_K |\Delta_K|^{1/2}} = \prod_p E(p), \tag{6.4}$$

where the Euler factor at the rational prime p is defined by

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

We will see in the following section how this formula can be applied.

▶ Functional equation

Just like the Riemann zeta function, the Dedekind zeta-function can be extended to a meromorphic function ζ_K on all of $\mathbf{C}$ which is holomorphic except for a simple pole at $t = 1$. It has a functional equation relating its values at t and $1 - t$ which most clearly shows its symmetries if we complete ζ_K with Euler factors 'at infinity' coming from the complex embeddings of K.

6.5. Theorem. *Let K be a number field of degree n with r real and $2s$ complex embeddings. Then ζ_K can be extended to a holomorphic function on $\mathbf{C}\setminus\{1\}$. The completed zeta function*

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

satisfies the functional equation $Z_K(t) = Z_K(1-t)$.

The Γ-function occurring in the definition of the completed zeta function Z_K was already defined by Euler as

$$\Gamma(t) = \int_0^\infty x^{t-1}e^{-x}dx.$$

As it satisfies the functional equation $\Gamma(t+1) = t\Gamma(t)$ and has the easily computed value $\Gamma(1) = 1$, we see that the Γ-function has simple poles at integers $k \in \mathbf{Z}_{\leq 0}$, and satifies $\Gamma(k+1) = k!$ for integers $k \geq 0$. It then follows from the functional equation that ζ_K has 'trivial zeroes' at all negative integers $k \in \mathbf{Z}_{<0}$. At odd integers k the multiplicity of the zero equals s, at even k the multiplicity equals $r+s$. At $k=0$, the zeta function ζ_K has a zero of order $r+s-1$ with leading coefficient $\zeta_K^*(0) = -h_K R_K/w_K$ in its Taylor expansion. All other zeroes ρ of ζ_K satisfy $0 < \mathrm{Re}(\rho) < 1$.

The first proof of 6.5 was given by Hecke in 1910. A more elegant proof using harmonic analysis on adelic groups, which shows how the Γ-factors in Z_K can be seen as Euler factors at the 'infinite primes' of K, was given by Tate in 1959. These proofs can both be found in [7, Chapter XIII and XIV]. As indicated there, the techniques of Hecke have been used recently by Zimmert and Skoruppa to show that not only the discriminant (cf. 5.10), but also the regulator grows exponentially with the degree. An explicit lower bound is

$$R_K/w_K \geq .02 \cdot \exp(.46r + .1s). \tag{6.6}$$

The famous *generalized Riemann hypothesis* (GRH—seegeneralized Riemann hypothesis) states that all zeroes ρ of ζ_K in the *critical strip* $0 < \mathrm{Re}(t) < 1$ satisfy $\mathrm{Re}(\rho) = 1/2$. This is the most important open conjecture in analytic number theory. There are many other unproved conjectures concerning special values of the zeta function that go back to Stark, Beilinson and others.

7 Computing units and class groups

This section is devoted to the actual computation of Picard groups and unit groups of number rings. This is actually *one* problem, since finding class group relations and units is done in exactly the same way. Moreover, one needs information on the unit group of a number ring in order to *prove* that the orders of elements in the Picard group are what they appear to be.

Both from a theoretical and from an algorithmic point of view, the computations are by no means easy. Calculations by hand or using only a simple calculator are necessarily restricted to fields of small degree, usually not exceeding 5, and of fairly small discriminant. Computer packages as Pari and Magma that have been developed over the last 20 years can handle slightly larger fields, of degree up to about 20, if the discriminant is of moderate size. One very soon runs into fundamental problems: the discriminant can be so large that it becomes impossible to find its factorization, and the units can be so large that simply writing them down is already not feasible. These are important problems in practice, and we will have to deal with them when discussing the *number field sieve* for factoring integers in section **, which employs number rings of moderate degree but with huge discriminant. We refer to [21] for a more detailed discussion of these fundamental issues.

▶ Pell revisited

We start with the quadratic order $\mathbf{Z}[\sqrt{1141}]$ occurring in problem 1.1.

7.1. Example. *Find the unit group R^* for the real quadratic order $R = \mathbf{Z}[\sqrt{1141}]$.*

In this case, we know by 3.21 that R is an order of index 2 in the ring of integers $\mathcal{O} = \mathbf{Z}[\frac{1+\sqrt{1141}}{2}]$ of $\mathbf{Q}(\sqrt{1141})$. It is usually easier to find unit groups and Picard groups of integral extensions of a number ring, since these have smaller Minkowski constants. We therefore compute the class group $\mathrm{Cl} = \mathrm{Cl}(\mathcal{O})$ and the unit group $\mathcal{O}^*$ of $\mathcal{O}$ first.

The ring $\mathcal{O}$ is of the form $\mathcal{O} = \mathbf{Z}[\alpha]$ with $\alpha = (1+\sqrt{1141})/2$ a zero of $f = f^{\alpha}_{\mathbf{Q}} = X^2 - X - 285$, and its discriminant equals $\Delta(\mathcal{O}) = 1141 = 7 \cdot 163$. The Minkowski constant $M_{\mathcal{O}} = \frac{1}{2}\sqrt{1141}$ of $\mathcal{O}$ is smaller than 17, so Cl is generated by the primes of norm at most 13. We easily deduce from 3.11 that 2 and 11 are inert in $\mathcal{O}$, so we can restrict our attention to the primes over 3, 5, 7 and 13. Applying 3.1, we find the following factorizations:

$$\begin{aligned} 3\mathcal{O} &= \mathfrak{p}_3\mathfrak{q}_3 = (3,\alpha)\cdot(3,\alpha-1) \\ 5\mathcal{O} &= \mathfrak{p}_5\mathfrak{q}_5 = (5,\alpha)\cdot(5,\alpha-1) \\ 7\mathcal{O} &= \mathfrak{p}_7^2 = (7,\alpha-4)^2 \\ 13\mathcal{O} &= \mathfrak{p}_{13}\mathfrak{q}_{13} = (13,\alpha-4)\cdot(13,\alpha+3). \end{aligned}$$

In order to determine Cl, we have to find relations between these seven generators. In line with the 'linear algebraic' nature of most class group computations, we write Cl as an additive group. From the factorizations above we find relations $[\mathfrak{p}_i] + [\mathfrak{q}_i] = 0$ for $i = 3, 5, 13$ and $2[\mathfrak{p}_7] = 0$. In order to find additional relations, we factor suitable principal ideals in $\mathcal{O}$ into prime ideals.

We usually try to factor ideals of the form $(k-\alpha)$ with $k \in \mathbf{Z}$, since in that case the norm of $k-\alpha$ is easily computed as $N_{K/\mathbf{Q}}(k-\alpha) = f(k)$. As we need relations between prime ideals of small norm, we take values of k for which $f(k)$ is not too large. From the primes dividing $f(k)$ it is easy to determine which prime ideals occur in the factorization of $(k-\alpha)$. Note that no rational prime divides $k-\alpha$, so only primes $\mathfrak{p}$ of degree $f(\mathfrak{p}/p) = 1$ can occur, and if such a prime occurs the other prime $\mathfrak{q}|p$ does not occur. Moreover, if $\mathfrak{p}|p$ divides $(k-\alpha)$, then it divides all ideals $(k'-\alpha)$ with $k' \equiv k \bmod p$. We compile the following small table of factorizations in $\mathcal{O}$.

k	15	16	17	18	19	20	21
$f(k)$	-75	-45	-13	21	57	95	135
$(k-\alpha)$	$\mathfrak{p}_3\mathfrak{p}_5^2$	$\mathfrak{q}_3^2\mathfrak{q}_5$	$\mathfrak{p}_{13}$	$\mathfrak{p}_3\mathfrak{p}_7$	$\mathfrak{q}_3\mathfrak{p}_{19}$	$\mathfrak{p}_5\mathfrak{q}_{19}$	$\mathfrak{p}_3^3\mathfrak{q}_5$

We have written $\mathfrak{p}_{19} = (19, \alpha)$ and $\mathfrak{q}_{19} = (19, \alpha - 1)$ for the primes over 19. The entry for $k = 17$ tells us that $\mathfrak{p}_{13}$ is principal. The same is then true for its inverse $\mathfrak{q}_{13}$ in Cl. The entry for $k = 18$ shows that $\mathfrak{p}_7$ and $\mathfrak{p}_3$ are in ideal classes that are inverse to each other. As we know already that $\mathfrak{p}_7^2 = (7)$ is principal, the square of $\mathfrak{p}_3$ is also principal. As we have $[\mathfrak{p}_{19}] + [\mathfrak{q}_{19}] = 0$, multiplication of the entries for $k = 19$ and $k = 20$ yields $[\mathfrak{p}_5] = -[\mathfrak{q}_3] = [\mathfrak{p}_3]$. We deduce that Cl is generated by $[\mathfrak{p}_3]$. From the entry $k = 15$ we find $[\mathfrak{p}_3] + 2[\mathfrak{p}_5] = 3 \cdot [\mathfrak{p}_3] = 0$, and as we know already that $2 \cdot [\mathfrak{p}_3] = 0$ we conclude that Cl is the trivial group, i.e., $\mathcal{O}$ is a principal ideal domain.

Exercise 1. Find explicit generators for all primes in $\mathcal{O}$ of norm at most 13.

In order to find a non-trivial unit in $\mathcal{O}$, we employ the fact that our table has 3 entries involving only primes over 3 and 5. As we have $\mathfrak{q}_3 = 3\mathfrak{p}_3^{-1}$ and $\mathfrak{q}_5 = 5\mathfrak{p}_5^{-1}$, we can write all factorizations in terms of $\mathfrak{p}_3$ and $\mathfrak{p}_5$ as

$$(15-\alpha) = \mathfrak{p}_3\mathfrak{p}_5^2 \qquad (15+\alpha) = \mathfrak{p}_3^2\mathfrak{p}_5 \qquad (21-\alpha)/5 = \mathfrak{p}_3^3\mathfrak{p}_5^{-1}.$$

The principal ideal generated by the element

$$\eta = (15-\alpha)^a(15+\alpha)^b(21-\alpha)^c 5^{-c}$$

factors as $\mathfrak{p}_3^{a+2b+3c}\mathfrak{p}_5^{2a+b-c}$, and this is the unit ideal if we choose a, b and c satisfying $a + 2b + 3c = 2a + b - c = 0$. We can take $(a, b, c) = (-5, 7, -3)$ and compute the resulting unit $\eta = -618715978 - 37751109\alpha$. It remains to prove that η is fundamental, so that we have

$$\mathcal{O}^* = \langle -1 \rangle \times \langle 618715978 + 37751109\alpha \rangle.$$

If $\varepsilon = 618715978 + 37751109\alpha$ is not fundamental, there exists a unit $\varepsilon_0 = t + u\alpha \in \mathbf{Z}[\alpha]$ and $k \in \mathbf{Z}_{>1}$ such that $\varepsilon_0^k = \varepsilon$. Note that t and u are non-negative since ε is a unit with positive coefficients on the basis $\{1, \alpha\}$. In order to bound the index k, we take the embedding $\mathcal{O} \to \mathbf{R}$ under which α is positive. For the fundamental unit $\varepsilon_0 = t + u\alpha$, we have a trivial lower bound like $\varepsilon_0 > \alpha$ or, after checking that $t + u\alpha$ of norm $t^2 - tu - 285u^2$ can not be a unit for $u = 1, 2, 3$, the slightly better bound $\varepsilon_0 > 4\alpha$ to find

$$k = \frac{\mathrm{Reg}(\varepsilon)}{\mathrm{Reg}(\varepsilon_0)} = \frac{\log(\varepsilon)}{\log(\varepsilon_0)} \leq \frac{\log(\varepsilon)}{\log(4\alpha)} \approx 4.94.$$

This shows that we have $\varepsilon = \varepsilon_0^k$ with k at most 4. It now suffices to show that ε is not a square or a cube in $\mathcal{O}$, and this can be shown most easily by reducing $\mathcal{O}$ modulo suitable primes and checking that ε does not map to a square or cube. The unit ε is congruent to 1 modulo both $\mathfrak{p}_3$ and $\mathfrak{q}_3$, but modulo $\mathfrak{p}_5$ we find that $\overline{\varepsilon} = 3 \in \mathcal{O}/\mathfrak{p}_5 = \mathbf{F}_5$ is not a square. Thus ε is not a square. For cubes we have to look at splitting primes congruent to 1 mod 3, and one finds that ε is a cube modulo the primes over 7 and 13, but that $\overline{\varepsilon} = 16 \in \mathcal{O}/\mathfrak{p}_{19} = \mathbf{F}_{19}$ is not a cube. This proves that ε is fundamental in $\mathcal{O}^*$.

The fundamental unit of $\mathcal{O}$ does not lie in $R = \mathbf{Z} + 2\mathcal{O}$, but (cf. 5.16) the index of R^* in $\mathcal{O}^*$ is bounded by the order of $(\mathcal{O}/2\mathcal{O})^* = \mathbf{F}_4^*$. We conclude that ε^3 is a fundamental unit in $R = \mathbf{Z}[\sqrt{1141}]$, and it is an easy calculator check to see that this corresponds to the smallest solution to $x^2 - 1141y^2 = 1$ that appeared out of the blue in section 1. □

We list the observation occurring in this example in slightly greater generality for the ease of future reference.

7.2. Proposition. *Let $f \in \mathbf{Z}[X]$ be a monic irreducible polynomial and $R = \mathbf{Z}[\alpha]$ the order obtained by adjoining a root α of f. Let p be a prime number and $k \in \mathbf{Z}$ an integer. Then there is a prime ideal $\mathfrak{p}|p$ dividing the principal ideal $(k-\alpha)$ if and only if p divides $f(k)$. If such a $\mathfrak{p}$ exists, it is the ideal $\mathfrak{p} = (p, k-\alpha)$ of residue class degree $f(\mathfrak{p}/p) = 1$. In particular, there is at most one prime over p dividing $(k-\alpha)$.*

Proof. A homomorphism $\phi : R \to F$ to a finite field F of characteristic p with kernel $\ker\phi \supset (k-\alpha)$ maps α to $k \in \mathbf{F}_p \subset F$, so it is uniquely determined and has image $\mathbf{F}_p$. There exists $\phi : R \to \mathbf{F}_p$ with $\phi(\alpha) = k \bmod p$ if and only if k is a zero of $f \bmod p$. □

▶ A cubic example

Our next example is the cubic number ring of the form $\mathbf{Z}[\alpha, \beta]$ that we encountered in 3.7. This forces us to apply the Kummer-Dedekind theorem 3.1 to more than one polynomial.

7.3. Example. *Find the class group and the unit group of the maximal order in $\mathbf{Q}(\sqrt[3]{19})$.*

We determined the maximal order $\mathcal{O} = \mathbf{Z}[\alpha, \beta]$ for this field in 3.7, and we computed its discriminant $\Delta(\mathcal{O}) = -3 \cdot 19^2$ in 4.11. The Minkowski constant $M_{\mathcal{O}} = \frac{4}{\pi} \cdot \frac{6}{27} \cdot \sqrt{3 \cdot 19^2} \approx 9.3$ shows that $\mathrm{Cl}(\mathcal{O})$ is generated by the primes of norm ≤ 7. From the irreducible polynomials $f_{\mathbf{Q}}^{\alpha} = X^3 + 19$ and $f_{\mathbf{Q}}^{\beta} = X^3 - X^2 - 6X - 12$ one derives by 3.1 the factorizations

$$\begin{aligned} 2\mathcal{O} &= \mathfrak{p}_2\mathfrak{p}_4 = (2, \alpha - 1) \cdot (2, \alpha^2 + \alpha + 1) \\ 3\mathcal{O} &= \mathfrak{p}_3^2\mathfrak{q}_3 = (3, \beta)^2 \cdot (3, \beta - 1) \\ 5\mathcal{O} &= \mathfrak{p}_5\mathfrak{p}_{25} = (5, \alpha - 1) \cdot (5, \alpha^2 + \alpha + 1) \\ 7\mathcal{O} &= \mathfrak{p}_{343} = (7). \end{aligned}$$

From our set of generators $\{\mathfrak{p}_2, \mathfrak{p}_4, \mathfrak{p}_3, \mathfrak{q}_3, \mathfrak{p}_5\}$ we can discard $\mathfrak{p}_4$ and $\mathfrak{q}_3$, since the factorizations of 2 and 3 yield the relations $[\mathfrak{p}_4] = -[\mathfrak{p}_2]$ and $[\mathfrak{q}_3] = -2[\mathfrak{p}_3]$ in $\mathrm{Cl}(\mathcal{O})$. We have $N(\alpha - 1) = -f_{\mathbf{Q}}^{\alpha}(1) = -20 = -2^2 \cdot 5$, and it is clear that $\alpha - 1$ is contained in $\mathfrak{p}_2$ and $\mathfrak{p}_5$. We deduce that there is a factorization $(\alpha - 1) = \mathfrak{p}_2^2\mathfrak{p}_5$, and this allows us to discard the generator $[\mathfrak{p}_5]$. The element $\beta = (\alpha^2 - \alpha + 1)/3$ is contained in $\mathfrak{p}_3$ and $\mathfrak{p}_4$ and of norm $N(\beta) = -f_{\mathbf{Q}}^{\beta}(0) = 12$,

so we have $(\beta) = \mathfrak{p}_3\mathfrak{p}_4$ and a resulting relation $[\mathfrak{p}_3] = -[\mathfrak{p}_4] = [\mathfrak{p}_2]$. It follows that $\mathrm{Cl}(\mathcal{O})$ is cyclic and generated by $[\mathfrak{p}_2]$. The factorization of $(\alpha+3) = \mathfrak{p}_2^3$ or $(\beta+1) = \mathfrak{p}_2^3$ show that $\mathrm{Cl}(\mathcal{O})$ has order 1 or 3. Factoring additional elements yield no new relations: we have $(\alpha-2) = \mathfrak{p}_3\mathfrak{q}_3^2$ in the class of $-3[\mathfrak{p}_3]$ and $(\beta-3) = \mathfrak{p}_2^2\mathfrak{p}_3$ in the class of $3[\mathfrak{p}_3]$. This suggests that $\mathrm{Cl}(\mathcal{O})$ has order 3.

Showing that an ideal is *not* principal involves the knowledge of the unit group. In this case, finding a unit is easy as the 8 elements $\beta+i$ with $i \in \mathbf{Z}$ between -4 and 3 and the 5 elements $\alpha+j$ with $j \in \{\pm 1, -2, 3, 4\}$ all factor into primes lying over 2, 3 and 5.

Exercise 2. Find these factorizations, and use them to produce a few units in $\mathcal{O}$. Check how they are related to the unit η we will now construct.

As $\alpha+3$ and $\beta+1$ both generate $\mathfrak{p}_2^3$, the element $\eta = (\alpha+3)/(\beta+1) = 1-\alpha-\beta$ is a unit in $\mathcal{O}^*$. Before showing that η is fundamental, let us see how we can apply this to prove that the order of $[\mathfrak{p}_2]$ in the class group is 3.

Suppose that $\mathfrak{p}_2 = (x)$ is a principal ideal. Then x^3 and $\alpha+3$ generate the same ideal in $\mathcal{O}$, so we have

$$\alpha + 3 = \varepsilon \cdot x^3$$

for some unit $\varepsilon \in \mathcal{O}^*$. We have $\mathcal{O}^* = \langle -1 \rangle \times \langle \eta \rangle$ by our assumption that η is fundamental, so $\varepsilon = \pm\eta^k$ for some $k \in \mathbf{Z}$. In order to derive a contradiction, we reduce the equation modulo a suitable prime of norm $p \equiv 1 \bmod 3$. Modulo $\mathfrak{p}_{19} = (\alpha)$, we find that β maps to $1/3 = -6 \in \mathcal{O}/\mathfrak{p}_{19} = \mathbf{F}_{19}$ and $\eta = 1-\alpha-\beta$ to $7 \in \mathbf{F}_{19}$. As 7 is a cube in $\mathbf{F}_{19}$, we find that $\varepsilon \cdot x^3$ maps to a cube in $\mathcal{O}/\mathfrak{p}_{19}$ for all k. However, $\alpha+3$ maps to 3, which is not a cube in $\mathbf{F}_{19}$. This shows that $\mathfrak{p}_2$ is not principal, and that $\mathrm{Cl}(\mathcal{O})$ has order 3.

It remains to show that η is a fundamental unit in $\mathcal{O}$. In fact, the argument above only uses that η generates the cyclic group $\mathcal{O}^*/(\mathcal{O}^*)^3$, and this can again be proved by exhibiting a prime $\mathfrak{p}$ in $\mathcal{O}$ for which η is not a cube in $\mathcal{O}/\mathfrak{p}$.

Exercise 3. Check that η maps modulo $\mathfrak{p}_{97} = (97, \alpha - 60)$ to the non-cube $54 \in \mathbf{F}_{97}^*$.

In order to prove that η is fundamental, we need a lower bound on the regulator of $\mathcal{O}$. From problem 5.21, we have $\mathrm{Reg}(\mathcal{O}) \geq \frac{1}{3}\log(\frac{3\cdot 19^2-24}{4}) \approx 1.86$. Under the unique embedding $\mathcal{O} \to \mathbf{R}$ we have $\log(\eta) \approx -2.63$, so the inequality $\mathrm{Reg}(\eta)/\mathrm{Reg}(\mathcal{O}) < 2$ shows that η is fundamental.

The method employed in 7.3 to show that an ideal that appears to be non-principal is indeed of some order $k > 1$ in the Picard group works in general number rings in the following way. Suppose we know that $\mathfrak{a}^k = (x)$ is a principal ideal, and that we want to show that $[\mathfrak{a}]$ has order k in the Picard group. We need to show that $\mathfrak{a}^{k/p}$ is non-principal for all prime divisors p of k. If $\mathfrak{a}^{k/p} = (y)$ is principal, we have $x = \varepsilon \cdot y^p$ for some unit ε. As y can be changed by an arbitrary unit, it suffices to show that this equation cannot hold for ε ranging over a set of representatives of the cosets of $(\mathcal{O}^*)^p$ in $\mathcal{O}^*$. By the Dirichlet unit theorem, there are only finitely many cosets, so this yields finitely many equations. Showing that $x = \varepsilon \cdot y^p$ is not solvable for fixed ε is done by reducing modulo sufficiently many primes of prime norm congruent to 1 mod p. If $x\varepsilon^{-1}$ is not a p-th power, one is bound to find such a prime after a finite amount of time. It is often possible to deal with many (or even all) cases at one time

by exhibiting primes modulo which all units are p-th powers, but x is not. This is what we did in 7.3.

▶ A larger cubic example

Any cubic field that is not totally real, and for which the unit rank is therefore equal to 1, can be dealt with in a way similar to the one we employed for the pure cubic field $\mathbf{Q}(\sqrt[3]{19})$. As the Minkowski constant is larger in this example, we proceed in a more systematic way.

7.4. Example. *Find the class group and the unit group of the maximal order in $K = \mathbf{Q}(\alpha)$ with $\alpha^3 + \alpha^2 + 5\alpha - 16 = 0$.*

Before anything else, we tabulate a few values of the polynomial $f = X^3 + X^2 + 5X - 16$ in factored form.

n	$f(n)$
-10	$-2 \cdot 3 \cdot 7 \cdot 23$
-9	-709
-8	$-2^3 \cdot 3^2 \cdot 7$
-7	$-3 \cdot 5 \cdot 23$
-6	$-2 \cdot 113$
-5	$-3 \cdot 47$
-4	$-2^2 \cdot 3 \cdot 7$
-3	-7^2
-2	$-2 \cdot 3 \cdot 5$
-1	$-3 \cdot 7$

n	$f(n)$
0	-2^4
1	-3^2
2	$2 \cdot 3$
3	$5 \cdot 7$
4	$2^2 \cdot 3 \cdot 7$
5	$3 \cdot 53$
6	$2 \cdot 7 \cdot 19$
7	$3 \cdot 137$
8	$2^3 \cdot 3 \cdot 5^2$
9	839

This table shows that f has no zeroes modulo 11, 13 and 17, so it is irreducible modulo these primes. In particular, it is irreducible in $\mathbf{Z}[X]$.

Its discriminant can be computed from the resultant $R(f, f')$ as

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

As $\Delta(f)$ is squarefree, we have $\Delta_K = -8763$ and $\mathcal{O} = \mathcal{O}_K = \mathbf{Z}[\alpha]$. As $\Delta(f)$ is negative, the cubic polynomial f has a single real root. This gives $r = s = 1$ for our field, so Minkowski's constant equals

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

and the class group is generated by the classes of the primes of norm at most 25. We can factor the rational primes up to 23 by simply looking at the values of f in our table. Leaving

out the inert primes 11, 13 and 17, we obtain factorizations

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

in which x_5 and x_{19} denote elements which we do not bother to compute. These factorizations show that the class group 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 $(k-\alpha)$. In view of 7.2, these can be derived 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 $(\alpha)=\mathfrak{p}_2^4$.

It turns out that we do not find relations indicating that the order of $[\mathfrak{p}_2]$ is smaller than 4, so we try to prove this. This comes down to showing that the ideal $\mathfrak{p}_2^2$ is not principal. We need to know the group $\mathcal{O}^*/(\mathcal{O}^*)^2$ in order to show this. As in 7.1, 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 $\mathcal{O}^*\cong\langle-1\rangle\times P$, where $P\cong\mathbf{Z}$ 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 $\mathcal{O}^*$. This is easy: reducing modulo $\mathfrak{p}_3$ we find $\eta\equiv 4-1-13\equiv -1$, and -1 is not a square in $\mathcal{O}/\mathfrak{p}_3=\mathbf{F}_3$.

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 the fact 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 $\mathfrak{p}^2$ is not principal. It follows that Cl is cyclic of order 4 with generator $[\mathfrak{p}_2]$.

The question remains whether η is a fundamental unit. This can be decided as in 7.3. Under the unique real embedding $K\to\mathbf{R}$ the image of η has absolute logarithm $\mathrm{Reg}(\eta)\approx 7.684$. From the lower bound $R_K\geq\frac{1}{3}\log(\frac{|\Delta_K|-24}{4})\approx 2.563$ we obtain $[P:\langle\eta\rangle]=\mathrm{Reg}(\eta)/R_K<3$, so η is fundamental if it is not a square in $\mathcal{O}$. We saw this already, so we have indeed $\mathcal{O}^*=\langle-1\rangle\times\langle\eta\rangle$. □

▶ An example with unit rank 2

When dealing with number rings of unit rank 2 and higher, a more detailed administration of units is necessary in order to keep track of the unit group that is generated by the units we produce from factorizations of principal ideals.

7.5. Example. *Find the class group and the unit group of the maximal order in* $K = \mathbf{Q}(\alpha)$ *with* $\alpha^4 - 2\alpha^2 + 3\alpha - 7 = 0$.

Note first that the polynomial $f = X^4 - 2X^2 + 3X - 7 \in \mathbf{Z}[X]$ is irreducible as it is irreducible modulo 2. We begin again by tabulating a list of small values of f in factored form.

n	$f(n)$
-15	50123
-14	$5^2 \cdot 7^2 \cdot 31$
-13	$19 \cdot 1483$
-12	$5 \cdot 7 \cdot 11 \cdot 53$
-11	$83 \cdot 173$
-10	$13 \cdot 751$
-9	$5 \cdot 19 \cdot 67$
-8	$31 \cdot 127$
-7	$5^2 \cdot 7 \cdot 13$
-6	$11 \cdot 109$
-5	$7 \cdot 79$
-4	$5 \cdot 41$
-3	47
-2	-5
-1	-11
0	-7

n	$f(n)$
1	-5
2	7
3	$5 \cdot 13$
4	229
5	$11 \cdot 53$
6	$5 \cdot 13 \cdot 19$
7	$7 \cdot 331$
8	$5 \cdot 797$
9	$7^2 \cdot 131$
10	$11 \cdot 19 \cdot 47$
11	$5^2 \cdot 577$
12	20477
13	$5 \cdot 5651$
14	$7 \cdot 5437$
15	$149 \cdot 337$
16	$5 \cdot 7 \cdot 11 \cdot 13^2$

For a change, we compute the discriminant of f from the power sums p_k of the roots of f. We have $p_0 = 4$ and $p_1 = 0$, and from Newton's formula's (exercise 4.20) we find

$$\begin{aligned}
p_2 &= -2a_2 - p_1a_1 = -2 \cdot 2 + 0 = 4 \\
p_3 &= -3a_3 - p_2a_1 - p_1a_2 = 3 \cdot (-3) + 0 + 0 = -9 \\
p_4 &= 2p_2 - 3p_1 + 7p_0 = 2 \cdot 4 - 0 + 7 \cdot 4 = 36 \\
p_5 &= 2p_3 - 3p_2 + 7p_1 = 2 \cdot (-9) - 3 \cdot 4 + 0 = -30 \\
p_6 &= 2p_4 - 3p_3 + 7p_2 = 2 \cdot 36 - 3 \cdot (-9) + 7 \cdot 4 = 127.
\end{aligned}$$

The discriminant is then by exercise 4.19 equal to the determinant

$$\Delta(f) = \det \begin{pmatrix} 4 & 0 & 4 & -9 \\ 0 & 4 & -9 & 36 \\ 4 & -9 & 36 & -30 \\ -9 & 36 & -30 & 127 \end{pmatrix} = -98443,$$

which is a prime number. This implies $\Delta_K = -98443$ and $\mathcal{O} = \mathcal{O}_K = \mathbf{Z}[\alpha]$. We deduce from the sign of Δ_K that K has $r = 2$ real embeddings and $s = 1$ pair of complex embeddings (cf. exercise 4.12). Minkowski's constant is then equal to

$$\frac{4!}{4^4}\frac{4}{\pi}\sqrt{98443} \approx 37.4,$$

so the class group is generated by the classes of the primes of norm at most 37. The table shows that f has no zeroes modulo p for the primes $p = 2, 3, 17, 23$ and 29. Computing a few additional values we see that f has no zeroes modulo 37 either. This implies that there are no prime ideals of norm p for these primes p. It is easily checked that f is irreducible modulo 2 and 3 and that it factors modulo 5 as

$$f \equiv (X-1)(X+2)(X^2-X+1) \pmod 5.$$

This implies that 2 and 3 are inert in K and that 5 factors as a product $(5) = \mathfrak{p}_5\mathfrak{q}_5\mathfrak{p}_{25}$, where $\mathfrak{p}_5$ and $\mathfrak{q}_5$ have norm 5 and $\mathfrak{p}_{25}$ is a prime of norm 25. All other primes of norm less than the Minkowski bound have prime norm, so they can be found from our table.

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

Here we use the fact that $(p, \alpha - k)$ is already generated by $(\alpha - k)$ when $f(k) = \pm p$.

The class group is generated by the classes of the primes in this table and the class $[\mathfrak{p}_{25}]$. The primes lying over 5 and 7 are all principal (note that we have $\mathfrak{p}_{25} = 5\mathfrak{p}_5^{-1}\mathfrak{q}_5^{-1}$), 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 $k = 3$ 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 $\alpha = -9 \in \mathbf{F}_{19}$ and $1 - 2\alpha$ is therefore a small element in the ideal. Similarly, we have $\alpha = -8 \in \mathbf{F}_{31}$ 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.

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

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 $\mathcal{O}$, 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, one quickly generates a large number of units. The rank of the unit group $\mathcal{O}^*$ for our field K equals $r + s - 1 = 2$, so some administration is needed to keep track of the subgroup of $\mathcal{O}^*$ generated by these units. As in the proof of the Dirichlet unit theorem, one looks at the lattice in $\mathbf{R}^2$ 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 $K \to \mathbf{R}$, so they send α to the the real roots $\alpha_1 \approx -2.195$ and $\alpha_2 \approx 1.656$ of f. The following units are obtained in this way.

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

From the table 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. This impression can be confirmed by factoring more elements of small norm. Note that the log-vectors are very useful to make a relation like

$$5\alpha^3 - 11\alpha^2 + 14\alpha - 16 = \pm(\alpha^3 - 2\alpha^2 + 3\alpha - 4)(\alpha^3 - 4\alpha + 2)^{-1} = \pm\eta_1\eta_2^{-1}$$

that is otherwise non-obvious immediately visible.

Exercise 4. Express the unit $-4743\alpha^3 + 10412\alpha^2 - 13371\alpha + 15124$ in terms of η_1 and η_2.

In order to prove that the unit group is indeed equal to $\mathcal{O}^* = \langle -1 \rangle \times \langle \eta_1 \rangle \times \langle \eta_2 \rangle$, we have to check that the regulator of K is equal to

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

There are two ways to proceed. The first way is to bound the index $[\mathcal{O}^* : \langle -1, \eta_1, \eta_2 \rangle] = \mathrm{Reg}(\eta_1, \eta_2)/R_K$ as in the previous examples, and show modulo suitable primes of $\mathcal{O}$ that η_1 and η_2 generate $\mathcal{O}^*/\{\pm 1\}$ modulo p-th powers for all primes p below the index bound. As f has degree 4, we have to use the lower bound (6.6) for R_K to achieve this.

The second way, which is more efficient and generally shows that R_K *and* h_K equal the values obtained, proceeds numerically by approximating the residue in $t = 1$ of the zeta function $\zeta_K(t)$ of K. If η_1 and η_2 are fundamental, the residue should equal

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

From the previous section, we know that this residue can be computed from the Euler product $\prod_p E(p)$, where

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

The factor $E(p)^{-1}$ is a polynomial expression in p^{-1} that depends only on the residue class degrees of the primes $\mathfrak{p}|p$, i.e. on the degrees of the irreducible factors of the defining polynomial f modulo p. In this case, it is not even necessary to factor $\overline{f} \in \mathbf{F}_p[X]$ to determine the degrees of the irreducible factors: it suffices to count the number of zeroes of f in $\mathbf{F}_p[X]$. If we disregard the single ramified prime 98443, there are 5 possible factorization types of f modulo p. If the number n_p of zeroes 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. We can distinguish the two cases for $n_p = 0$ using exercise 15, which states that the parity of the number of irreducible factors of f mod p can be read off from the Legendre symbol $\left(\frac{\Delta(f)}{p}\right)$. It follows that we have

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

A simple computer program enables us to evaluate the Euler product with some precision. The following data indicate the speed of convergence of this product.

N	$\prod_{p<N} E(p)$
100	0.625211
200	0.595521
500	0.581346
1000	0.584912
2000	0.585697

N	$\prod_{p<N} E(p)$
5000	0.579408
10000	0.579750
20000	0.581892
50000	0.581562
100000	0.581423

We see that the convergence is non-monotonous and slow, but certainly close to the value .5810 we found before. 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. This convinces us that we have found the full unit group. A rigorous proof would involve a more detailed analysis on the convergence of the Euler product.

EXERCISES.

5. Find the smallest integral solution $y > 0$ to the Pell equation $x^2 - 61y^2 = 1$.
6. Find the smallest integral solution $y > 0$ to the Pell equation $x^2 - 109y^2 = 1$.
7. Compute the class group and the unit group of the maximal order in $\mathbf{Q}(\sqrt{229})$.
8. Find the fundamental units of the number rings $\mathbf{Z}[\alpha]$ and $\mathbf{Z}[\beta]$ contained in the order $\mathcal{O}$ of example 7.3.
9. Determine for the twelve prime ideals $\mathfrak{p}$ in example 7.4 of norm at most 25 the class of $[\mathfrak{p}] \in \mathrm{Cl}(\mathcal{O}) = \langle \mathfrak{p}_2 \rangle$.
10. Compute the Picard group and the unit group of the order $\mathbf{Z}[\sqrt[3]{7}]$.
11. Compute the Picard group and the unit group of the order $\mathbf{Z}[\sqrt[3]{37}]$.
12. Compute the Picard group and the unit group of the order $\mathbf{Z}[\sqrt[3]{-19}]$.
    [Hint: use 4.13 and the fact that the quadratic subring $A \subset \widetilde{R}$ of discriminant -19 has class number 1.]
13. Pick integers a, b, c and d of absolute value at most 4 such that $f = X^4 + aX^3 + bX^2 + cX + d$ is irreducible in $\mathbf{Z}[X]$. Compute the class group and the unit group of the field $\mathbf{Q}[X]/(f)$.
14. Let F be a field and $f \in F[X]$ a separable polynomial. Write $n = \deg f$, and denote by α_1, α_2, …, α_n the zeroes of f in a splitting field of f over F. We put

$$e(f) = \sum_{\sigma \in A_n} \prod_{i=1}^{n} \alpha_{\sigma(i)}^{i-1}, \qquad e'(f) = \sum_{\sigma \in S_n - A_n} \prod_{i=1}^{n} \alpha_{\sigma(i)}^{i-1},$$

    where S_n is the symmetric group of degree n and $A_n \subset S_n$ the alternating group. We view the Galois group $\mathrm{Gal}(f)$ of f over F as a subgroup of S_n, via its action on α_1, α_2, …, α_n.

    a. Prove that $(X - e(f))(X - e'(f)) \in F[X]$ and that $(e(f) - e'(f))^2$ equals the discriminant of f. Deduce that $e(f) \neq e'(f)$.
    b. Show that $e(f)$ and $e'(f)$ belong to F if and only if $\mathrm{Gal}(f) \subset A_n$.
    c. Prove that for F of characteristic different from 2, the discriminant of f is a square in F if and only if $\mathrm{Gal}(f) \subset A_n$.
    d. Prove that for $F = \mathbf{F}_2$, one has $e(f)e'(f) = 0$ if and only if $\mathrm{Gal}(f) \subset A_n$.
    e. Suppose that F is finite, and denote the number of irreducible factors of f in $F[X]$ by t. Prove that $\mathrm{Gal}(f) \subset A_n$ if and only if $n \equiv t \bmod 2$.
15. Let $f \in \mathbf{Z}[X]$ be a monic irreducible polynomial, n its degree, α a zero of f in some extension field of $\mathbf{Q}$, and p a prime number not dividing the discriminant $\Delta(f)$ of f. Denote by t the number of prime ideals $\mathfrak{p}$ of $\mathbf{Z}[\alpha]$ with $p \in \mathfrak{p}$. Prove that $\left(\frac{\Delta(f)}{p}\right) = (-1)^{n-t}$. (Here $\left(\frac{\Delta(f)}{p}\right)$ denotes the Kronecker symbol if $p = 2$.)

16. Let $\mathcal{O} = \mathbf{Z}[\alpha]$ with $\alpha^3 + \alpha + 1 = 0$ be the order of example 3.3, and p a prime number. Show that p is the product of two prime ideals in $\mathcal{O}$ if $\left(\frac{-31}{p}\right) = -1$, and that $p\mathcal{O}$ is either inert or the product of three prime ideals if $\left(\frac{-31}{p}\right) = 1$. Do both possibilities for $\left(\frac{-31}{p}\right) = 1$ occur? Determine the 5 smallest primes that split completely in $\mathcal{O}$.

17. Show that the maximal order in $\mathbf{Q}(\sqrt{-31})$ has class number 3. Show that a rational prime p has a *principal* extension of norm p in this order if and only if p is of the form $p = x^2 + 31y^2$. Determine the 5 smallest primes p of this form. *Can you explain the relation with the previous exercise?

8 Galois theory for number fields

In the previous section, we have seen how to compute, starting from an irreducible polynomial $f \in \mathbf{Z}[X]$, the fundamental arithmetic invariants of the number field $K = \mathbf{Q}[X]/(f)$ defined by f. A basic algorithmic tool here is the Kummer-Dedekind theorem, which tells us how to derive the explicit splitting of a rational prime p in K (more precisely: in $\mathcal{O}_K$) from the splitting of f modulo p.

In Galois!theory, a theory (or theorem) of which we assume the basic notions to be known, one learns that the polynomial f gives rise to a finite group $\mathrm{Gal}(f)$, the automorphism group of the splitting field $\Omega_{\mathbf{Q}}^f$ of f over $\mathbf{Q}$. This section discusses the interplay between the Galois group $\mathrm{Gal}(f)$ and the splitting of rational primes p in K and in $\Omega_{\mathbf{Q}}^f$. It will ultimately lead us to various results describing the 'average splitting behavior' of f mod p if f is fixed and p varies.

▶ Galois action on extension primes

Let K be a number field that is Galois over $\mathbf{Q}$ with group $G = \mathrm{Gal}(K/\mathbf{Q})$. Then G acts naturally on all intrinsically defined objects and invariants related to K that we have encountered in the previous sections.

Exercise 1. Check this for $\mathcal{O}_K$ and $\mathrm{Cl}(K)$, and for the set of primes in $\mathcal{O}_K$ extending a rational prime p.

For K as above, any choice of an embedding $\phi \in \mathrm{Hom}_{\mathbf{Q}}(K, \overline{\mathbf{Q}})$ leads to an identification $G \leftrightarrow \mathrm{Hom}_{\mathbf{Q}}(K, \overline{\mathbf{Q}})$ given by $\sigma \mapsto \phi \circ \sigma$. In particular, we can use this identification in 4.2 to rewrite the products and sums defining norms and traces as ranging over all $\sigma \in G$.

8.1. Theorem. *Let K be a number field that is Galois over $\mathbf{Q}$ with group G, and p a rational prime. Then G acts transitively on the primes $\mathfrak{p}$ of K extending p.*

Proof. Suppose there exist extensions $\mathfrak{p}$ and $\mathfrak{p}'$ of p that are in different G-orbits. Then we can use the Chinese remainder theorem to construct an element $x \in \mathfrak{p}$ satisfying $x \notin \sigma\mathfrak{p}'$ for all $\sigma \in G$. The norm $N_{K/\mathbf{Q}}(x) = \prod_{\sigma \in G} \sigma(x)$ is then by construction in $\mathfrak{p}$ but not in $\mathfrak{p}'$. As it lies in $\mathfrak{p} \cap \mathbf{Z} = p\mathbf{Z} = \mathfrak{p}' \cap \mathbf{Z}$, we arrive at a contradiction. □

8.2. Corollary. *All extensions $\mathfrak{p}$ of p in K are isomorphic, and the residue class degree $f_p = f(\mathfrak{p}/p)$ and the ramification index $e_p = e(\mathfrak{p}/p)$ only depend on p. If g_p is the number of extensions of p in K, we have*

$$e_p f_p g_p = [K : \mathbf{Q}].$$

8.3. Example. Take $K = \mathbf{Q}(\zeta_3, \sqrt[3]{-19})$ to be the splitting field of $X^3 + 19$. Then K is Galois over $\mathbf{Q}$ with non-abelian Galois group of order 6. The prime 3 ramifies in the quadratic subfield $\mathbf{Q}(\zeta_3) = \mathbf{Q}(\sqrt{-3})$, so the primes in K over 3 have even ramification index e_3. As 3 has two extensions to $\mathbf{Q}(\sqrt[3]{-19})$ by 3.7, 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 $(3) = \mathfrak{p}^2\mathfrak{q}$ in $\mathbf{Q}(\sqrt[3]{-19})$ factor in the quadratic extension K of $\mathbf{Q}(\sqrt[3]{-19})$ as $\mathfrak{p}\mathcal{O}_K = \mathfrak{P}_1\mathfrak{P}_2$ and $\mathfrak{q}\mathcal{O}_K = \mathfrak{Q}^2$.

The prime 2 is inert in $\mathbf{Q}(\zeta_3)$ and splits as $(2) = \mathfrak{p}_2\mathfrak{p}_4$ in $\mathbf{Q}(\sqrt[3]{-19})$. For this prime f_2 is even and g_2 is at least 2, so we have $e_2 = 1$, $f_2 = 2$ and $g_2 = 3$. We conclude that $\mathfrak{p}_2$ is inert in $\mathbf{Q}(\sqrt[3]{-19}) \subset K$, giving rise to a prime $\mathfrak{P}$ of norm 4, and that $\mathfrak{p}_4$ splits into two primes $\mathfrak{Q}$ and $\mathfrak{R}$ of norm 4 each.

▶ Decomposition and inertia groups

In the situation of 8.1, the stabilizer

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

of a prime $\mathfrak{p}$ of K extending p is known as the *decomposition group* of $\mathfrak{p}$. As G acts transitively on the primes extending p, 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. By 8.2, the order of $G_\mathfrak{p}$ equals e_pf_p.

If $\mathfrak{p}'$ is another extension of p to K, we have $\mathfrak{p}' = \sigma\mathfrak{p}$ for some $\sigma \in G$ and consequently $G_{\mathfrak{p}'} = G_{\sigma\mathfrak{p}} = \sigma G_\mathfrak{p}\sigma^{-1}$. This shows that the various decomposition groups of the primes above a rational prime p are all conjugate in G. If G is abelian, or, more generally, if $G_\mathfrak{p}$ is normal in G, the decomposition group is independent of the choice of the extension $\mathfrak{p}|p$ and can be denoted by G_p.

The decomposition group $G_\mathfrak{p}$ acts naturally as a group of automorphisms of the residue class field extension $\mathbf{F}_p = \mathbf{Z}/p\mathbf{Z} \subset k_\mathfrak{p} = \mathcal{O}_K/\mathfrak{p}$, which is an extension of finite fields of degree $f(\mathfrak{p}/p)$. In particular, $\mathbf{F}_p \subset k_\mathfrak{p}$ is a cyclic Galois extension of order $f(\mathfrak{p}/p)$ with group generated by the *Frobenius automorphism* $\mathrm{Frob}_p : x \mapsto x^p$ on $k_\mathfrak{p}$.

8.4. Lemma. *The natural map $G_\mathfrak{p} \to \mathrm{Gal}(k_\mathfrak{p}/\mathbf{F}_p)$ is surjective.*

Proof. Choose an element $x \in \mathcal{O}_K$ that is contained in all primes $\mathfrak{p}' \neq \mathfrak{p}$ over p and for which the reduction $\overline{x} = x \bmod \mathfrak{p}$ satisfies $\mathbf{F}_p(\overline{x}) = k_\mathfrak{p}$. Then $\sigma(x)$ is in $\mathfrak{p}$ for all $\sigma \in G\setminus G_\mathfrak{p}$, so the characteristic polynomial $f = \prod_{\sigma\in G}(X - \sigma(x))$ of x factors in $k_\mathfrak{p}[X]$ as $\overline{f} = X^{\#(G-G_\mathfrak{p})} \cdot h_\mathfrak{p}$ for some polynomial $h_\mathfrak{p} \in k_\mathfrak{p}[X]$. As $\overline{f}$ is in $\mathbf{F}_p[X]$ we also have $h_\mathfrak{p} \in \mathbf{F}_p[X]$, and the identity $\overline{f}(\overline{x}) = 0 = h_\mathfrak{p}(\overline{x})$ implies that the irreducible polynomial of $\overline{x}$ over $\mathbf{F}_p$ divides $h_\mathfrak{p}$. This shows that all conjugates of $\overline{x}$ over $\mathbf{F}_p$ can be obtained as the reduction of an element $\sigma(x)$ with $\sigma \in G_\mathfrak{p}$, and that every element of $\mathrm{Gal}(k_\mathfrak{p}/\mathbf{F}_p)$ comes from some $\sigma \in G_\mathfrak{p}$. □

The kernel of the map $G_\mathfrak{p} \to \mathrm{Gal}(k_\mathfrak{p}/\mathbf{F}_p)$ is the *inertia group* $I_\mathfrak{p} \subset G_\mathfrak{p}$ of $\mathfrak{p}$ in G. It is a normal subgroup of $G_\mathfrak{p}$, and we have an exact sequence

$$0 \longrightarrow I_\mathfrak{p} \longrightarrow G_\mathfrak{p} \longrightarrow \mathrm{Gal}(k_\mathfrak{p}/\mathbf{F}_p) \longrightarrow 0 \tag{8.5}$$

showing that the group $G_\mathfrak{p}$ of order $e(\mathfrak{p}/p)f(\mathfrak{p}/p)$ has a normal subgroup $I_\mathfrak{p}$ of order $e(\mathfrak{p}/p)$ for which the quotient $G_\mathfrak{p}/I_\mathfrak{p}$ is cyclic of order $f(\mathfrak{p}/p)$.

8.6. Example. Let $K = \mathbf{Q}(\zeta_3, \sqrt[3]{19})$ be as in example 8.3. Then the decomposition groups at the primes over 3 in $\mathrm{Gal}(K/\mathbf{Q})$ are the three subgroups of order 2. Note that these are conjugate subgroups, and that we have $G_\mathfrak{Q} = I_\mathfrak{Q} = \mathrm{Gal}(K/\mathbf{Q}(\sqrt[3]{19}))$.

The prime 19 has two extensions $(4 \pm \sqrt{-3})$ in $\mathbf{Q}(\zeta_3)$ that are both totally ramified in $K/\mathbf{Q}(\zeta_3)$. Their decomposition group $G_{19} = I_{19}$ is the normal subgroup of order 3. It does not depend on the choice of the extension.

The decomposition groups of the primes over 2 are again the three subgroups of order 2. The prime $\mathfrak{P}$ in 8.3 has $G_{\mathfrak{P}} = \mathrm{Gal}(K/\mathbf{Q}(\sqrt[3]{19}))$.

Everything we have done so far for the Galois extension $\mathbf{Q} \subset K$ can immediately be generalized to an arbitrary Galois extension $K \subset L$ of number fields. The Galois group $G = \mathrm{Gal}(L/K)$ acts transitively on the set of primes $\mathfrak{q}$ of L extending a prime $\mathfrak{p}$ of K as in 8.1, and the stabilizer of $\mathfrak{q}$ in G is the decomposition group $G_{\mathfrak{q}} = G_{\mathfrak{q}/\mathfrak{p}}$ of $\mathfrak{q}$ over $\mathfrak{p}$. It acts on the residue class field extension $k_{\mathfrak{p}} \subset k_{\mathfrak{q}}$, and as in 8.5 we obtain an exact sequence

$$0 \longrightarrow I_{\mathfrak{q}/\mathfrak{p}} \longrightarrow G_{\mathfrak{q}/\mathfrak{p}} \longrightarrow \mathrm{Gal}(k_{\mathfrak{q}}/k_{\mathfrak{p}}) \longrightarrow 0 \tag{8.7}$$

showing that $G_{\mathfrak{q}/\mathfrak{p}}$ is the extension of a cyclic group of order $f(\mathfrak{q}/\mathfrak{p})$ by the inertia group $I_{\mathfrak{q}/\mathfrak{p}}$ of order $e(\mathfrak{q}/\mathfrak{p})$.

Exercise 2. Formulate and prove the analogues of 8.1 and 8.4 for the extension $K \subset L$.

If H is a subgroup of $G = \mathrm{Gal}(L/K)$ corresponding to the intermediate field E and $\mathfrak{q}_E$ is the restriction of $\mathfrak{q}$ to E, then it is immediate from the definitions that the decomposition and inertia group of $\mathfrak{q}$ in the Galois extension $E \subset L$ equal

$$H_{\mathfrak{q}} = G_{\mathfrak{q}} \cap H \qquad \text{and} \qquad I_{\mathfrak{q}/\mathfrak{q}_E} = I_{\mathfrak{q}} \cap H.$$

Moreover, if H is normal in G, the extension $K \subset E$ is Galois with group G/H and the natural map $G_{\mathfrak{q}/\mathfrak{p}} \to G/H$ induces isomorphisms

$$\begin{aligned} G_{\mathfrak{q}}/H_{\mathfrak{q}} = G_{\mathfrak{q}/\mathfrak{p}}/(G_{\mathfrak{q}/\mathfrak{p}} \cap H) &\xrightarrow{\sim} (G/H)_{\mathfrak{q}_E/\mathfrak{q}} \\ I_{\mathfrak{q}/\mathfrak{p}}/I_{\mathfrak{q}/\mathfrak{q}_E} = I_{\mathfrak{q}/\mathfrak{p}}/(I_{\mathfrak{q}/\mathfrak{p}} \cap H) &\xrightarrow{\sim} I_{\mathfrak{q}_E/\mathfrak{q}}. \end{aligned}$$

To see this, it suffices to observe that both maps are clearly injective, and therefore surjective by the transitivity relations $f(\mathfrak{q}/\mathfrak{p}) = f(\mathfrak{q}/\mathfrak{q}_E)f(\mathfrak{q}_E/\mathfrak{p})$ and $e(\mathfrak{q}/\mathfrak{p}) = e(\mathfrak{q}/\mathfrak{q}_E)e(\mathfrak{q}_E/\mathfrak{p})$.

The subfields $L^{G_{\mathfrak{q}}}$ and $L^{I_{\mathfrak{q}}}$ corresponding to the decomposition and inertia groups of $\mathfrak{q}$ over $\mathfrak{p}$ are the *decomposition field ('Zerlegungskörper')* and the *inertia field ('Trägheitskörper')* of $\mathfrak{q}$ in $K \subset L$. By the functorial properties of decomposition and inertia groups, we see that the inclusions $G \supset G_{\mathfrak{q}} \supset I_{\mathfrak{q}} \supset 1$ lead to a tower of fields that relates to the extension behavior of $\mathfrak{q}$ in the following way:

	K	$\subset$	$L^{G_{\mathfrak{q}}}$	$\subset$	$L^{I_{\mathfrak{q}}}$	$\subset$	L
residue class degree		1		$f(\mathfrak{q}/\mathfrak{p})$		1	
ramification index		1		1		$e(\mathfrak{q}/\mathfrak{p})$	

One finds that the decomposition field $L^{G_{\mathfrak{q}}}$ is the maximal subextension E of $K \subset L$ for which we have $e(\mathfrak{q}_E/\mathfrak{p}) = f(\mathfrak{q}_E/\mathfrak{p}) = 1$, and the inertia field $L^{I_{\mathfrak{q}}}$ is the maximal subextension E of $K \subset L$ for which $\mathfrak{q}_E$ is unramified over $\mathfrak{p}$.

Exercise 3. Prove these statements, and describe the respective subgroups of G corresponding to the maximal subextension of $K \subset L$ for which $\mathfrak{p}$ is totally split (unramified) in $K \subset E$.

▶ The Frobenius symbol

If $\mathfrak{q}$ is *unramified* over $\mathfrak{p}$ in 8.7, then the inertia group $I_{\mathfrak{q}/\mathfrak{p}}$ is trivial and we see that $G_{\mathfrak{q}/\mathfrak{p}}$ itself has a 'Frobenius of $\mathfrak{q}$ over $\mathfrak{p}$' as its canonical generator. This automorphism is the *Frobenius symbol* $\mathrm{Fr}_{\mathfrak{q}} \in G_{\mathfrak{q}/\mathfrak{p}} \subset G$ of $\mathfrak{p}$ in G, and it is characterized by the identity $\mathrm{Fr}_{\mathfrak{q}}(x) = x^{\#k_{\mathfrak{p}}} \bmod \mathfrak{q}$ for all $x \in \mathcal{O}_L$. If $\mathfrak{q}' = \sigma\mathfrak{q}$ is some other prime over p, we have $\mathrm{Fr}_{\sigma\mathfrak{q}} = \sigma \,\mathrm{Fr}_{\mathfrak{q}}\, \sigma^{-1}$, so the Frobenius elements at the primes over $\mathfrak{p}$ are conjugate elements in G. If G is *abelian*, we can speak of the Frobenius element of $\mathfrak{p}$ in G. This element, which is also known as the *Artin symbol* of $\mathfrak{p}$ in G, plays a key role in class field theory.

8.8. Example. The cyclotomic field $K = \mathbf{Q}(\zeta_n)$ is Galois over $\mathbf{Q}$ with abelian Galois group $(\mathbf{Z}/n\mathbf{Z})^*$, with $a \in (\mathbf{Z}/n\mathbf{Z})^*$ corresponding to the automorphism of K defined by $\zeta_n \mapsto \zeta_n^a$.

Let p be a prime number, and write $n = p^k m$ with $p \nmid m$. Then $\mathbf{Q}(\zeta_m)$ is the inertia field of p, since p is unramified in $\mathbf{Q}(\zeta_m)$ with extensions that are totally ramified in $\mathbf{Q}(\zeta_m) \subset \mathbf{Q}(\zeta_n)$. In particular, we have

$$I_p = (\mathbf{Z}/p^k\mathbf{Z})^* \times (1 \bmod m) \subset (\mathbf{Z}/p^k\mathbf{Z})^* \times (\mathbf{Z}/m\mathbf{Z})^* = (\mathbf{Z}/n\mathbf{Z})^*.$$

If p does not divide n, we have $m = n$ and p is unramified in $\mathbf{Q}(\zeta_n)$. In this case the Frobenius element Fr_p in $(\mathbf{Z}/n\mathbf{Z})^*$ satisfies $\mathrm{Fr}(\zeta_n) \equiv \zeta_n^p$ modulo all primes over p. As Φ_n is separable in characteristic $p \nmid n$, this shows that we have $\mathrm{Fr}_p(\zeta_n) = \zeta_n^p$ and $G_p = \langle p \bmod n \rangle \subset (\mathbf{Z}/n\mathbf{Z})^*$. The prime p splits completely in $\mathbf{Q}(\zeta_n)^{G_p}$—this explains the name decomposition field—and its extensions remain inert in the extension $\mathbf{Q}(\zeta_n)^{G_p} \subset \mathbf{Q}(\zeta_n)$.

Exercise 4. Show that the prime 2 has decomposition field $\mathbf{Q}(\sqrt{-7})$ and inertia field $\mathbf{Q}(\zeta_7)$ in $\mathbf{Q}(\zeta_{28})$. Determine the decomposition fields of the primes 3, 5, 7, 13 and 29, and show that no prime is inert in $\mathbf{Q} \subset \mathbf{Q}(\zeta_{28})$.

▶ The non-Galois case

Even if the extension $\mathbf{Q} \subset K$ one is dealing with is not Galois, one can effectively apply Galois theory to obtain the splitting behavior of primes. This is because there is a Galois action on the *fundamental set* $X_K = \mathrm{Hom}(K, \overline{\mathbf{Q}})$ of embeddings of K in an algebraic closure $\overline{\mathbf{Q}}$ of $\mathbf{Q}$ for *every* number field K. The set X_K has $n = [K : \mathbf{Q}]$ elements, and the images $\sigma[K] \subset \overline{\mathbf{Q}}$ for $\sigma \in X_K$ generate the *normal closure* L of K in $\overline{\mathbf{Q}}$. The extension $\mathbf{Q} \subset L$ is Galois, say with group G, and the natural left action of G given by composition is transitive. If $K = \mathbf{Q}(\alpha)$ is generated over $\mathbf{Q}$ by a root α of $f \in \mathbf{Z}[X]$, then L is the splitting field of the polynomial f in $\overline{\mathbf{Q}}$, and the natural action of $G = \mathrm{Gal}(f) = \mathrm{Gal}(L/\mathbf{Q})$ on the n-element set X_K identifies G with a subgroup of S_n. As the map $\sigma \mapsto \sigma(\alpha)$ identifies the elements $\sigma \in X_K$ with the zeroes of f in $\overline{\mathbf{Q}}$, this is nothing but the classical Galois action of $\mathrm{Gal}(f)$ on the n roots of f in $\overline{\mathbf{Q}}$.

8.9. Theorem. *Let X_K be the fundamental set of a number field K of degree n and $G = \mathrm{Gal}(L/\mathbf{Q})$ the Galois group over $\mathbf{Q}$ of the normal closure L of K. Given integers $e_i, f_i > 0$ for $i = 1, 2, \ldots, t$ such that $\sum_{i=1}^t e_i f_i = n$, the following are equivalent:*

(1) *the prime p has t distinct extensions $\mathfrak{p}_1, \mathfrak{p}_2, \ldots, \mathfrak{p}_t$ in K with ramification indices $e(\mathfrak{p}_i/p) = e_i$ and residue class field degrees $f(\mathfrak{p}_i/p) = f_i$;*

(2) *for every decomposition group $G_\mathfrak{q} \subset G$ of a prime $\mathfrak{q}$ above p in L, there are t different $G_\mathfrak{q}$-orbits $X_i \subset X_K$ of length $\#X_i = e_i f_i$. Under the action of the inertia group $I_\mathfrak{q} \subset G_\mathfrak{q}$ on X_i, there are f_i orbits of length e_i each.*

Proof. **to be supplied** □

8.10. Corollary. *A prime number p is unramified (totally split) in K if and only if it is unramified (totally split) in the normal closure of K.*

Proof. A subgroup $H \subset G = \mathrm{Gal}(L/\mathbf{Q})$ that acts trivially on X_K is necessarily trivial as the normal closure L is generated by the subfields $\sigma[K]$ with $\sigma \in X_K$. Now apply this with H the inertia (decomposition) group of a prime $\mathfrak{q}$ over p in L. □

8.11. Corollary. *Let $f \in \mathbf{Z}[X]$ be a monic irreducible polynomial and p a prime number. Suppose that $f \bmod p$ factors as a product of k distinct irreducible factors of degrees $d_1, d_2, \ldots, d_k$. Then $\mathrm{Gal}(f)$, viewed as a permutation group on the roots of f, contains a permutation that is the product of k disjoint cycles of lengths $d_1, d_2, \ldots, d_k$.*

Proof. The hypothesis means that $f \bmod p$ is separable, and that p does not divide $\Delta(f)$. The number ring $\mathbf{Z}[\alpha] = \mathbf{Z}[X]/(f)$ obtained by adjoining a root of f to $\mathbf{Z}$ is then regular and unramified at p. By the Kummer-Dedekind theorem 3.1, the primes extending p in the ring of integers of $K = \mathbf{Q}(\alpha)$ have residue class degrees $d_1, d_2, \ldots, d_k$. If $\mathrm{Fr}_\mathfrak{q}$ is the Frobenius element of a prime over p in $G = \mathrm{Gal}(f)$, then the lengths of the disjoint cycles of $\mathrm{Fr}_\mathfrak{q}$ are the lengths of the orbits under the action of $G_\mathfrak{q} = \langle \mathrm{Fr}_\mathfrak{q} \rangle \subset G$ on X_K or – equivalently – the roots of f. By 8.9, these lengths are $d_1, d_2, \ldots, d_k$. □

8.12. Example. Take $f = X^4 + X + 1$. Then f is irreducible modulo 2 and factors as a linear times a cubic polynomial modulo 3. It follows that $\mathrm{Gal}(f)$ is a permutation group on 4 elements containing a cycle of length 4 and a cycle of length 3. We immediately deduce that $\mathrm{Gal}(f)$ is the full symmetric group S_4 of order 24.

Exercises.

5. For each residue class $a \in (\mathbf{Z}/20\mathbf{Z})^*$, determine the decomposition group G_p of a prime $p \equiv a \bmod 20$ in $\mathrm{Gal}(\mathbf{Q}(\zeta_{20})/\mathbf{Q})$ and the corresponding decomposition field.
6. Determine the decomposition and inertia fields for the primes $p < 20$ in the splitting field of $f = X^4 - 19$.
7. Let $f \in \mathbf{Z}[X]$ be monic and irreducible of degree $n \in \mathbf{Z}_{\geq 1}$. Show that $\mathrm{Gal}(f)$, when viewed as a permutation group on the roots of f, is contained in A_n if and only if $\Delta(f)$ is a square in $\mathbf{Z}$.
8. Let $\mathbf{Q} \subset K$ be Galois with group G. Show that G is generated by the inertia groups of the primes of $\mathcal{O}_K$.
9. Determine the Galois groups of the polynomials $X^4 + 3X + 1$ and $X^4 + 3X^2 + 1$.
10. Determine the isomorphism types of Galois groups of irreducible polynomials $f \in \mathbf{Z}[X]$ of degree 4 that exist, and find a polynomial with that Galois group for each type.
11. Determine the isomorphism types of Galois groups of irreducible polynomials $f \in \mathbf{Z}[X]$ of degree 5 that exist, and find a polynomial with that Galois group for each type.

Literature

There are several texts covering a large part of the material in these notes. We list a few of them, roughly in ascending order of difficulty, and indicate their most striking features.

1. I. Stewart, D.O. Tall, *Algebraic Number Theory*, Chapman and Hall 1979. Second edition 1987.
   A very readable, somewhat elementary account. Many examples, exercises and motivating remarks.
2. K. Ireland, M. Rosen, *A classical introduction to modern number theory,* Springer GTM 84, 1982. Second edition, 1990.
   Short and very readable chapters. Contains many attractive special topics not covered in our notes.
3. P. Samuel, *Algebraic theory of numbers,* translation of *Théorie algébrique des nombres* (1967), Hermann, 1970.
   A very clear and logical presentation in the style of Bourbaki.
4. A. Fröhlich, M.J. Taylor, *Algebraic Number Theory*, Cambridge University Press, 1991.
   Classical in spirit, with special attention to explicit computations in number fields of low degree.
5. Z. I. Borevich, I. R. Shafarevich, *Number theory,* translation of *Teoria čisel* (1964), Academic Press 1967.
   An unconventional classic.
6. J. Neukirch, *Algebraische Zahlentheorie,* Springer, 1992.
   A modern account stressing the analogy between algebraic number theory and algebraic geometry that has given rise to the fruitful area of arithmetic algebraic geometry. Contains class field theory in Neukirch's own axiomatic set up and an extensive chapter on zeta functions and L-series.
7. S. Lang, *Algebraic number theory,* Addison Wesley, 1970. Reprinted by Springer (GTM 110, 1986).
   More succinct than all preceding texts, no exercises. Contains class field theory and a lot of analytic number theory as well.
8. J. W. S. Cassels, A. Fröhlich (eds), *Algebraic Number Theory*, Academic Press, 1967.
   Proceedings of a 1965 instructional conference. The first chapters provide a concise introduction to algebraic number theory. Cohomological class field theory is found in the later chapters.

References

9. M. F. Atiyah, I. G. Macdonald, *Introduction to commutative algebra*, Addison-Wesley, 1969.
10. N. Bourbaki, *Elements of the history of mathematics*, Springer, 1994?. Translation of *Éléments d'histoire des mathématiques*, Masson, Paris, 1984.

11. J. Buchmann, H. W. Lenstra, Jr., *Computing maximal orders and decomposing primes in number fields*.
12. G. Cornell, J. H. Silverman, *Arithmetic Geometry*, Springer, 1986.
13. J. Dieudonné, *Abrégé d'histoire des mathématiques, 1700–1900,* Hermann, nouvelle édition 1986.
14. Diophantus, *Arithmetica*.
15. D. Eisenbud, *Commutative algebra with a viewpoint towards algebraic geometry*, Springer GTM 153, 1995.
16. R. Hartshorne, *Algebraic Geometry*, Springer GTM 52, 1977.
17. D. Hilbert, *Mathematische Probleme*, Gesammelte Abhandlungen Band III, 290–329, Springer Verlag, 1970.
18. Anthony W. Knapp, *Elliptic Curves*, Princeton University Press 1992.
19. S. Lang, *Algebra*, Addison-Wesley. Third edition 1993.
20. A. K. Lenstra, H. W. Lenstra, Jr. (eds), *The development of the number field sieve*, Springer LNM 1554, 1993.
21. H. W. Lenstra, Jr., *Algorithms in algebraic number theory*, Bull. AMS **26**(2), 211–244 (1992).
22. Yu. I. Manin, *A course in mathematical logic*, Springer GTM 53, 1977.
23. J.-P. Serre, *Minorations de discriminants*, Collected Works, vol III, 240–243, Springer, 1986.
24. J. H. Silverman, *The Arithmetic of Elliptic Curves*, Springer GTM 106, 1986.
25. J. Stilwell, *Mathematics and its history*, Undergraduate Text in Mathematics, Springer, 1989.
26. B. L. van der Waerden, *Moderne Algebra*, 1930-31. Later editions: *Algebra I&II*. English translation edited by Springer, 1991.
27. A. Weil, *Number Theory, an approach through history; from Hammurapi to Legendre*, Birkhäuser, 1984.
28. A. Wiles, *Modular elliptic curves and Fermat's last theorem*, Annals of Mathematics **142**, 443–551 (1995).

Index