Algebraic Number Theory

1. Introduction.

An important aspect of number theory is the study of so-called *"Diophantine"* equations. These are (usually) polynomial equations with integral coefficients. The problem is to find the integral or rational solutions. We will see, that even when the original problem involves only ordinary numbers in $\mathbf{Z}$ or in $\mathbf{Q}$, one is often led to consider more general numbers, so-called *algebraic* numbers. *Algebraic Number Theory* occupies itself with the study of the rings and fields which contain algebraic numbers. The introduction of these new numbers is natural and convenient, but it also introduces new difficulties. In this introduction we follows the historical development of the subject.

Diophantus of Alexandria lived in Egypt around 300 AD. He was interested in various problems concerning rational numbers. He wrote 13 books on the subject of which only 6 remain today. Those six books have been copied and translated over the centuries. Until the renaissance, they were the only available books treating these kind of number theoretical questions [15]. The Pythagorean equation $X^2 + Y^2 = Z^2$, long known and studied before Diophantus, is a typical example of the kind of problems that are discussed in his books. Everyone knows some solutions $X, Y, Z \in \mathbf{Z}$ of this equation: one has, for instance $3^2 + 4^2 = 5^2$ and $5^2 + 12^2 = 13^2$. Diophantus gives a complete description of the set of solutions $X, Y, Z \in \mathbf{Z}$:

Theorem 1.1. *Every solution $X, Y, Z \in \mathbf{Z}_{>0}$ with $\gcd(X, Y, Z) = 1$ of the equation*

$$X^2 + Y^2 = Z^2$$

is of the form

$$\begin{aligned} X &= a^2 - b^2, \\ Y &= 2ab, \\ Z &= a^2 + b^2, \end{aligned}$$

(or with the roles of X and Y reversed) where $a, b \in \mathbf{Z}_{>0}$ satisfy $a > b > 0$ and $\gcd(a, b) = 1$.

There is no real restriction in only considering X, Y and Z with $\gcd(X, Y, Z) = 1$: when one divides X, Y, Z by a common divisor, one still has a solution to the equation. Before proving the theorem, we prove a very important lemma.

Lemma 1.2. *Let $a, b \in \mathbf{Z}$ be two integers with $\gcd(a, b) = 1$. If the product ab is an n-th power for some positive integer n, then, upto sign, each of a and b is an n-th power.*

Proof. This follows from the fact that every non-zero integer can be written as the product of prime numbers in a unique way: let p be a prime number dividing a. Then p also divides the product ab. Let r indicate the number of times ab is divisible by p. Since $\gcd(a, b) = 1$, the prime p does not divide b. Therefore the prime number also divides a exactly r times.

Since ab is an n-th power, we see that r is divisble by n. We conclude that every prime number divides a a number of times which is divisible by n. Therefore a is, upto sign, an n-th power of an integer. The same is true for b. This proves the lemma.

Proof of Theorem 1.1. It is very easy to verify that $X = a^2 - b^2, Y = 2ab$ and $Z = a^2 + b^2$ are indeed solutions to the equation $X^2 + Y^2 = Z^2$. We have to show that every solution has this form. Let therefore $X, Y, Z \in \mathbf{Z}_{>0}$ with $\gcd(X, Y, Z) = 1$ satisfy $X^2 + Y^2 = Z^2$. Since $\gcd(X, Y, Z) = 1$, at least one of X, Y is odd. If *both* would be odd, we would have

$$Z^2 = X^2 + Y^2 \equiv 1 + 1 = 2 \pmod 4$$

which is impossible because a square is either 0 or 1 (mod 4). Therefore only one of X, Y is odd. If necessary we interchange X and Y and we assume that X is odd. We have

$$\begin{aligned} Y^2 &= Z^2 - X^2, \\ \left(\frac{Y}{2}\right)^2 &= \frac{Z-X}{2}\frac{Z+X}{2}. \end{aligned}$$

Note that both $(Z - X)/2$ and $(Z + X)/2$ are in $\mathbf{Z}$, since both X and Z are odd. A common divisor of $(Z - X)/2$ and $(Z + X)/2$ would also divide their sum Z and their difference X. Since $X^2 + Y^2 = Z^2$, it would therefore also divide Y. Since $\gcd(X, Y, Z) = 1$, we conclude that

$$\gcd\left(\frac{Z-X}{2}, \frac{Z+X}{2}\right) = 1.$$

By Lemma 1.2 and the fact that both $(Z - X)/2$ and $(Z + X)/2$ are positive we see that

$$\begin{aligned} \frac{Z-X}{2} &= a^2, \\ \frac{Z+X}{2} &= b^2. \end{aligned}$$

for some $a, b \in \mathbf{Z}_{>0}$. Since $\gcd(X, Y, Z) = 1$ also $\gcd(a, b) = 1$. Adding and subtracting the two equations one finds that $Z = a^2 + b^2$ and $X = a^2 - b^2$; this easily implies that $Y = 2ab$. Since $X > 0$ one has $a > b$. This proves Theorem 1.1.

Pierre de Fermat (1601–1665) was a magistrate in Toulouse in France. He was one of the most famous mathematicians of the 17th century [18]. He contributed to differential calculus and probability theory. He was the only mathematician of his time to be interested in number theory. The books of Diophantus were his main source of inspiration, but Fermat went further. Fermat considered problems that were, in a sense that can be made precise (see Weil [53,Ch.II]) more difficult than the ones considered by Diophantus. He usually did not publish any proofs, but it is likely, for instance, that he had a systematic method for solving equations of the type $X^2 - dY^2 = 1$ in integers ($d \in \mathbf{Z}_{>0}$). His most famous "method" is the *method of infinite descent* that he used to solve Diophantine equations: in order to show that no integral solutions of a certain kind exist, one constructs *from* a hypothetical solution another solution which is, in some sense, smaller. Since integers can not be arbitrarily small, this process cannot be repeated indefinitely and one concludes that there were no solutions to begin with. Even today Fermat's method is one of the main tools in solving Diophantine equations. The following theorem is an example of the use of the method of infinite descent. It is one of the few proofs published by Fermat himself [18]. See also [24].

Theorem 1.3. *(P. de Fermat) The only integral solutions of the equation*

$$X^4 + Y^4 = Z^2$$

are the trivial ones, i.e., the ones with $XYZ = 0$.

Proof. Suppose X, Y, Z is a non-trivial solution of this equation and let's suppose this solution is *minimal* in the sense that $|Z| > 0$ is minimal. This is easily seen to imply that $\gcd(X, Y, Z) = 1$. We may and do assume that $X, Y, Z > 0$. By considering the equation modulo 4, one sees that precisely one of X and Y is odd. Let's say that X is odd. By Theorem 1.1 there are integers $a > b > 0$ with $\gcd(a, b) = 1$ and

$$\begin{aligned} X^2 &= a^2 - b^2, \\ Y^2 &= 2ab, \\ Z &= a^2 + b^2. \end{aligned}$$

consider the first equation $X^2 + b^2 = a^2$. Since $\gcd(a, b, X) = 1$, we can apply Theorem 1.1 once more and we obtain

$$\begin{aligned} X &= c^2 - d^2, \\ b &= 2cd, \\ a &= c^2 + d^2, \end{aligned}$$

for certain integers $c > d > 0$ which satisfy $\gcd(c, d) = 1$. Substituting these expressions for a and b in the equation $Y^2 = 2ab$ above, we find

$$\begin{aligned} Y^2 &= 2ab = 2(2cd)(c^2 + d^2), \\ \left(\frac{Y}{2}\right)^2 &= c \cdot d \cdot (c^2 + d^2). \end{aligned}$$

The numbers c, d and $c^2 + d^2$ have no common divisors and their product is a square. By lemma 1.2 there exist integers U, V, W with

$$\begin{aligned} c &= U^2, \\ d &= V^2, \\ c^2 + d^2 &= W^2. \end{aligned}$$

It is easy to see that $\gcd(U, V, W) = 1$ and that

$$U^4 + V^4 = W^2.$$

We have obtained a new solution of the equation! It is easily checked that $W \neq 0$ and that $|W| \leq W^2 = c^2 + d^2 = a < a^2 < |Z|$. This contradicts the minimality of $|Z|$. We conclude that there are no non-trivial solutions of the equation, as required.

Fermat made many statements without giving a proof for them. In many cases one is tempted to believe that he actually possessed proofs, but sometimes this is not so clear. Fermat claimed, for instance that it is possible to write a prime number $p \neq 2$ as the sum of two squares if and only if it is congruent to 1 (mod 4). This fact was only proved some 100 years later by Euler in 1754. Fermat also stated that every integer is the sum of four squares. This "non inelegens theorema" (according to Euler), was not proved until 1770 by Lagrange. It is, however, conceivable that Fermat could prove this.

But Fermat also thought that for $k = 0, 1, 2, \ldots$ the numbers

$$F_k = 2^{2^k} + 1$$

are always prime. It is easily checked that $F_0, F_1, \ldots, F_4$ ar all prime, but Euler showed in 1732 that $F_5 = 4\,294\,967\,297$ is divisible by 641. Nowadays one knows that at least for $5 \leq k \leq 22$ the numbers F_k are not prime. It is unknown whether F_{23}, a number of more than 2 500 000 decimal digits, is prime or not. So, Fermat was not always right ...

The most famous claim by Fermat is the statement that for $n \geq 3$ the equation

$$X^n + Y^n = Z^n$$

does not admit any non-trivial solutions, i.e., it does not have solutions $X, Y, Z \in \mathbf{Z}$ with $XYZ \neq 0$. Fermat wrote in the his copy of Diophantus's book on number theory that he had a wonderful proof of this fact, but that, unfortunately, the margin was too narrow to contain it:

> *Cubum autem in duos cubos, aut quadratoquadratum in duos quadratoquadratos et generaliter nullam in infinitum ultra quadratum potestatem in duos eiusdem nomines fas est dividere cuius rei demonstrationem mirabilem sane detexi. Hanc marginis exiguitas non caperet.*

Sooner or later all Fermat's statements were proved or disproved, except this one, the last. It was called "Fermat's Last Theorem".

The following is an easy consequence of Theorem 1.3.

Theorem 1.4. *Fermat's Last theorem is true if and only if it for every prime number $p \neq 2$, the equation*

$$X^p + Y^p = Z^p$$

only admits trivial solutions, i.e., only solutions $X, Y, Z \in \mathbf{Z}$ with $XYZ = 0$.

Proof. If Fermat's Last Theorem is true, it is in particular true for prime exponents $p > 2$. To prove the converse, let $n \geq 3$ and let $x, y, z \in \mathbf{Z}$ be a solution to the equation $X^n + Y^n = Z^n$. We distinguish two cases: suppose first that n is divisible by an odd prime number p. Then we have

$$(x^{n/p})^p + (y^{n/p})^p = (z^{n/p})^p,$$

which is a solution to the equation $X^p + Y^p = Z^p$. So, it should be trivial: $(xyz)^{n/p} = 0$. This implies that $xyz = 0$. If n is not divisible by any odd prime number, then it is a power of 2 and hence at least 4. We have

$$(x^{n/4})^4 + (y^{n/4})^4 = (z^{n/4})^4,$$

which is a solution to the equation $X^4 + Y^4 = Z^4$. By Theorem 1.3 it should be trivial. This implies that $xyz = 0$ as required.

The most important result conerning Fermat's Last theorem was proved in 1847 by the German mathematician E.E. Kummer (1820–1889). Like Fermat, Kummer employed the method of infinite descent, but, he was led to generalize the method to rings of integers other than $\mathbf{Z}$. more precisely, let $p \neq 2$ be a prime and let ζ_p denote a primitive p-th root of unity. Kummer worked with the ring $\mathbf{Z}[\zeta_p]$ rather than with the ordinary ring of integers $\mathbf{Z}$. Since $X^p + 1 = \prod_{i=0}^{p-1}(X + \zeta_p^i)$, he could write

$$X^p + Y^p = \prod_{i=0}^{p-1}(X + \zeta_p^i Y) = Z^p.$$

He proceeded to show that the factors in the product have almost no factors in common and then he wanted to apply Lemma 1.2 to conclude that upto a unity every factor $X+\zeta_p^i Y$ is a p-th power. He then could conclude the proof in a way which is not relevant here [30]. However, as Kummer discovered, the property of unique factorizion does, in general, not hold for the rings $\mathbf{Z}[\zeta_p]$ and one can, in general, not apply Lemma 1.2. The first time it fails is for $p=23$; it fails, in fact, for every prime $p \geq 23$. Using his theory of ideal numbers [17], out of which our modern concept of "ideal" was to grow, Kummer circumvened the difficulties caused by the failure of unique factorization. For the sake of completeness we quote his famous result.

Theorem 1.5. *Let $p \neq 2$ be a prime. If p does not divide the numerators of the Bernoulli numbers $B_2, B_4, \ldots, B_{p-3}$, then the equation*

$$X^p + Y^p = Z^p$$

admits only solutions $X, Y, Z \in \mathbf{Z}$ with $XYZ = 0$.

Here the Bernoulli numbers are rational numbers defined by the Taylor series expansion

$$\frac{X}{e^X - 1} = \sum_{k=0}^{\infty} \frac{B_k}{k!} X^k.$$

Since $X/(e^X-1) + X/2 = \frac{X}{2}\coth(\frac{X}{2})$ is an even function, we see that $B_1 = -1/2$ and that the Bernoulli numbers B_k are zero for odd $k \geq 3$. The first few are:

$$\begin{array}{cccc} B_2 = \dfrac{1}{6}, & B_4 = -\dfrac{1}{30}, & B_6 = \dfrac{1}{42}, & B_8 = -\dfrac{1}{30}, \\ B_{10} = \dfrac{5}{66}, & B_{12} = -\dfrac{691}{2730}, & B_{14} = \dfrac{7}{6}, & B_{16} = -\dfrac{3617}{510}, \ldots \end{array}$$

They occur in the values of the Riemann ζ-function at even integers:

$$\zeta(k) = \sum_{n=1}^{\infty} \frac{1}{n^k} = -\frac{(2\pi i)^k}{2 \cdot k!} B_k.$$

See [1] for a table of Bernoulli numbers. From the values of the first few Bernoulli numbers one deduces that Kummer's theorem does apply for $p = 691$ or 3617. The theorem applies for all primes $p < 100$ except 37, 59 and 67.

Subsequent numerical calculations concerning Fermat's Last Theorem have always been based on Kummer's Theorem or refinements thereof. In 1992, it had in this way been checked by means of computers that Fermat's Last Theorem is correct for all exponents $n < 4\,000\,000$ (see [8]).

In the summer of 1993, the British mathematician Andrew Wiles finally announced a proof of Fermat's Last Theorem. His proof employs a variety of sophisticated techniques and builds on the work of many mathematicians. One of the principal ingredients is the abstract algebraic geometry developed by A. Grothendieck [22] in the 1960's, another is the theory of automorphic forms and representation theory developed by R. Langlands [20]. A third technique is the new method of "Euler systems" introduced by the Russian mathematician V.B. Kolyvagin [29] in the late 1980's. Wiles actually proves part of the so-called Taniyama-Shimura-Weil conjecture concerning the arithmetic of elliptic curves over $\mathbf{Q}$. It had already been shown in 1986 by the Americans K. Ribet and B. Mazur that this conjecture implies Fermat's Last Theorem. Their methods depend on the arithmetic theory of modular curves [44] and like Wiles's work, on Grothendieck's algebraic geometry. A crucial ingredient is an important result by B. Mazur [39], proved in 1976. One can interpret this result as the simultanuous solution of infinitely many Diophantine equations. Mazur's method is Fermat's method of infinite descent, couched in the language of flat cohomology.

We complete this introduction by illustrating what kinds of problems one encounters when one introduces other rings of integers when trying to solve Diophantine equations. We will do calculations in the ring $\mathbf{Z}[i]$ of Gaussian integers.

Proposition 1.6. *The ring $\mathbf{Z}[i]$ of Gaussian integers is a unique factorization domain. The unit group $\mathbf{Z}[i]^*$ of this ring is $\{1, -1, i, -i\}$.*

Proof. By Exer.1.C, the ring $\mathbf{Z}[i]$ is a Euclidean ring with respect to the norm map $\mathrm{N} : \mathbf{Z}[i] \longrightarrow \mathbf{Z}$ given by $\mathrm{N}(a + bi) = a^2 + b^2$ $(a, b \in \mathbf{Z})$. It is therefore a principal ideal ring and hence a unique factorization domain. This proves the first statement. The second statement is just Exer.1.B.

Theorem 1.7. *The only solution $X, Y \in \mathbf{Z}$ of the equation*

$$X^3 = Y^2 + 1$$

is given by $X = 1$ and $Y = 0$.

Proof. Let $X, Y \in \mathbf{Z}$ be a solution. If X were even, we would have $Y^2 = X^3 - 1 \equiv -1 \pmod 4$ and that is impossible by Exer.1.A. Therefore X is odd. We write, in the ring $\mathbf{Z}[i]$

$$X^3 = (Y + i)(Y - i).$$

A common divisor of $Y + i$ and $Y - i$ divides their difference $2i$ and hence 2. This common divisor also divides the odd number X^3 and hence the gcd of X^3 and 2, which is 1. We conclude that $Y + i$ and $Y - i$ have no common divisor. By Prop.1.6, the ring $\mathbf{Z}[i]$ is a unique factorization domain and we can apply a generalization of Lemma 1.2: since the product of $Y + i$ and $Y - i$ is a cube, each is, *upto a unit,* itself a cube. Since the unit group of $\mathbf{Z}[i]$ has order 4 by Prop.1.6, every unit is a cube and we see that, in fact,

$$Y + i = (a + bi)^3$$

for some $a + b \in \mathbf{Z}$. We do not need the analogous equation for $Y - i$. Equating real and imaginary parts, we find that

$$\begin{aligned} Y &= a^3 - 3ab^2, \\ 1 &= 3a^2b - b^3. \end{aligned}$$

The second relation says that $b(3a^2 - b^2) = 1$. Therefore $b = 1$ and $3a^2 = -1$ or $b = -1$ and $3a^2 - 1 = -1$. Only the second possibility gives rise to a solution of the equation $X^3 = Y^2 + 1$ viz., $Y = 0$ and $X = 1$ as required.

Next we consider an altogether similar equation:

$$X^3 = Y^2 + 19.$$

We solve it in a similar way: if X were even, we would have $Y^2 = X^3 - 19 \equiv 0 - 19 \equiv 5 \pmod 8$, but this is impossible, since odd squares are congruent to 1 (mod 8). If X were divisible by 19, also Y would be divisible by 19. This implies that $19 = X^3 - Y^2$ is divisble by 19^2, but that is absurd. We conclude that X is divisible by neither 19 or 2.

In the ring $\mathbf{Z}[\sqrt{-19}]$ we write

$$X^3 = (Y + \sqrt{-19})(Y - \sqrt{-19}).$$

A common divisor $\delta \in \mathbf{Z}[\sqrt{-19}]$ of $Y+\sqrt{-19}$ and $Y-\sqrt{-19}$ divides the difference $2\sqrt{-19}$ and hence $2\cdot 19$. Since $Y^2+19=X^3$, it divides also X^3. Therefore δ divides the gcd of X^3 and $2\cdot 19$ which is equal to 1. We conclude that the factors $Y+\sqrt{-19}$ and $Y-\sqrt{-19}$ have no common divisor.

By Exer.1.D, the only units of the ring $\mathbf{Z}[\sqrt{-19}]$ are 1 and -1. By a generalization of Lemma 1.2, we conclude that, since the product $(Y+\sqrt{-19})(Y-\sqrt{-19})$ is a cube, each of the factors $Y+\sqrt{-19}$ and $Y-\sqrt{-19}$ is, upto a sign, itself a cube. Since -1 is itself a cube, this means that

$$Y+\sqrt{-19}=(a+b\sqrt{-19})^3$$

for some $a,b\in\mathbf{Z}$. taking real and imaginary parts we find

$$\begin{aligned} Y &= a^3-3\cdot 19ab^2,\\ 1 &= 3a^2b-19b^3. \end{aligned}$$

it is easy to see that already the second equation $b(3a^2-19b^2)=1$ has no solutions $a,b\in\mathbf{Z}$. As in the previous example one would now like to conclude that the original equation $X^3=Y^2+19$ has no solutions either, but this is *not true at all,* as is shown by the following equality:

$$7^3=18^2+19.$$

What went wrong? The problem is, that one can only apply Lemma 1.2 or a simple generalization thereof, if the ring under consideration admits unique factorization. The ring $\mathbf{Z}[\sqrt{-19}]$ does not have this property:

$$\begin{aligned} 35 &= 5\cdot 7,\\ &= (4+\sqrt{-19})(4-\sqrt{-19}), \end{aligned}$$

are two distinct factorizations of the number 35 in the ring $\mathbf{Z}[\sqrt{-19}]$. We check that the factors are irreducible elements. By Exer.1.D the norm map

$$\mathrm{N}:\mathbf{Z}[\sqrt{-19}]\longrightarrow\mathbf{Z}$$

given by $\mathrm{N}(a+b\sqrt{-19})=a^2+19b^2$, is multiplicative. We have $\mathrm{N}(5)=25$, $\mathrm{N}(7)=49$ and $\mathrm{N}(4\pm\sqrt{-19})=4^2+19=35$. If any of these numbers were not irreducible in the ring $\mathbf{Z}[\sqrt{-19}]$, there would be elements in this ring of norm 5 or 7. Since the equations $a^2+19b^2=5$ and $a^2+19b^2=7$ have no solutions $a,b\in\mathbf{Z}$, there are no such elements. We conclude that the number 35 admits two genuinely distinct factorizations into irreducible elements. Therefore the ring $\mathbf{Z}[\sqrt{-19}]$ is not a unique factorization domain. See Exer.10.? for a proper solution of this Diophantine equation.

In this course we study number fields and their rings of integers. The rings $\mathbf{Z}[i]$ and $\mathbf{Z}[\zeta_p]$ are examples of such rings. In general, the property of unique factorization does not hold for these rings, but it can be replaced by a unique factorization property of *ideals.* This will be shown in chapter 5. There we also introduce the *classs group,* which measures the failing of the unique factorization property: it is trivial precisely when the ring of integers is a unique factorization domain. In chapter 10 we show that the class group is finite and in chapter 11 we prove Dirichlet's Unit Theorem, giving a description of the structure of the unit group of a ring of integers. The main ingredient in the proofs is Minkowski's "Geometry of Numbers". In chapter 12 we show how one can apply the theory in explicitly given cases. We discuss three elaborate examples. Finally in chapter 13, we compute the residue of the Dedekind ζ-function and obtain the "class number formula".

The present theory is discussed in a great many books. We mention the book by Ono [42], Stewart and Tall [49] and Samuel [46]. The books by Lang [32], Janusz [28] and Borevič and Shafarevič [5], cover more or less the same material, but also a great deal more.

(1.A) Let $x \in \mathbf{Z}$. Show
  (i) $x^2 \equiv 0$ or $1 \pmod 4$.
  (ii) $x^2 \equiv 0, 1$ or $4 \pmod 8$.

(1.B) Let $\mathbf{Z}[i] = \{a + bi : a, b \in \mathbf{Z}\}$ be the ring of Gaussian integers. let $\mathrm{N} : \mathbf{Z}[i] \longrightarrow \mathbf{Z}$ be the norm map defined by $\mathrm{N}(a + bi) = a^2 + b^2$. Prove
  (i) $\mathrm{N}(\alpha\beta) = \mathrm{N}(\alpha)\mathrm{N}(\beta)$ for $\alpha, \beta \in \mathbf{Z}[i]$.
  (ii) let $\alpha, \beta \in \mathbf{Z}[i]$. If α divides β then $\mathrm{N}(\alpha)$ divides $\mathrm{N}(\beta)$.
  (iii) α is a unit of $\mathbf{Z}[i]$ if and only if $\mathrm{N}(\alpha) = 1$.
  (iv) the group $\mathbf{Z}[i]^*$ is equal to $\{\pm 1, \pm i\}$.

(1.C) Show that the ring $\mathbf{Z}[i]$ is Euclidean with respect to the norm $\mathrm{N}(a + bi) = a^2 + b^2$.

(1.D) Let $\mathbf{Z}[\sqrt{-19}] = \mathbf{Z}[X]/(X^2 + 19)$. Let $\mathrm{N} : \mathbf{Z}[\sqrt{-19}] \longrightarrow \mathbf{Z}$ be the norm map defined by $\mathrm{N}(a + b\sqrt{-1}) = a^2 + 19b^2$. Show that
  (i) $\mathrm{N}(\alpha\beta) = \mathrm{N}(\alpha)\mathrm{N}(\beta)$ for $\alpha, \beta \in \mathbf{Z}[\sqrt{-19}]$.
  (ii) let $\alpha, \beta \in \mathbf{Z}[\sqrt{-19}]$. If α divides β then $\mathrm{N}(\alpha)$ divides $\mathrm{N}(\beta)$.
  (iii) α is a unit of $\mathbf{Z}[\sqrt{-19}]$ if and only if $\mathrm{N}(\alpha) = 1$.
  (iv) The group $\mathbf{Z}[\sqrt{-19}]^*$ is equal to $\{\pm 1\}$.

(1.E) Show that the ring $\mathbf{Z}[\sqrt{-2}]$ is Euclidean with respect to the norm map $\mathrm{N}(a + b\sqrt{-2}) = a^2 + 2b^2$ $(a, b \in \mathbf{Z})$.

(1.F) Show that the only solutions $X, Y \in \mathbf{Z}$ of the equation $X^2 + 2 = Y^3$ are $X = \pm 5$ and $Y = 3$. (Hint: use Exer.1.E)

(1.G) Show that the only solutions of the equation $Y^2 + 4 = X^3$ are $X = 5, Y = \pm 11$ and $X = 2, Y = \pm 2$. (Hint: distinguish the cases Y is odd and Y is even. In the second case one should divide by $2i + 2$)

(1.H) Show that $6 = 2 \cdot 3$ and $6 = (1 + \sqrt{-5})(1 - \sqrt{-5})$ are two factorizations of 6 into irreducible elements in the ring $\mathbf{Z}[\sqrt{-5}]$. Conclude that the ring $\mathbf{Z}[\sqrt{-5}]$ does not admit unique factorization.

(1.I) Show that the ring $\mathbf{Z}[(1 = \sqrt{-19})/2]$ is not Euclidean. We will see in chapter 10 that it is a unique factorization domain.

(1.J) The goal of this exercise is to show that a prime numnber $p \neq 2$ can be written as the sum of two squares if and only if $p \equiv 1 \pmod 4$. Let $p \neq 2$ be a prime number.
  (i) Show that if $p = a^2 + b^2$ for certain integers a and b, then $p \equiv 1 \pmod 4$.
  Let now $p \equiv 1 \pmod 4$. Prove:
  (ii) there exists $z \in \mathbf{Z}$ with $|z| < p/2$ and $z^2 + 1 \equiv 0 \pmod p$.
  (iii) the ideal $(z - i, p) \subset \mathbf{Z}[i]$ is generated by one element π.
  (iv) $\mathrm{N}(\pi) = p$. Conclude that $p = a^2 + b^2$ for certain $a, b \in \mathbf{Z}$.

(1.K) Show that a prime number $p \neq 3$ can be written as $p = a^2 + ab + b^2$ for certain $a, b \in \mathbf{Z}$ if and only if $p \equiv 1 \pmod 3$.

(1.L) (Fermat Numbers).
  (i) Let $n \in \mathbf{Z}_{>0}$. Show: if $2^n + 1$ is prime, then n is a power of 2.
  For $k \geq 0$ let $F_k = 2^{2^k} + 1$.
  (ii) Show that every divisor of F_k is congruent to $1 \pmod{2^{k+1}}$.
  (iii) Let $k \geq 2$. Show that the square of $2^{2^{k-2}} + 2^{-2^{k-2}}$ in $\mathbf{Z}/F_k\mathbf{Z}$ is equal to 2.
  (iv) Let $k \geq 2$. Show that every divisor of F_k is congruent to $1 \pmod{2^{k+2}}$.

2. Number fields.

In this section we discuss number fields. We define the real n-dimensional vector space $F \otimes \mathbf{R}$ associated to a number field F of degree n. We define a homomorphism $\Phi : F \longrightarrow F \otimes \mathbf{R}$ which should be seen as a generalization of the natural map $\mathbf{Q} \longrightarrow \mathbf{R}$. At the end of this section we discuss cyclotomic fields.

Definition 2.1. *A number field* F is a finite field extension of $\mathbf{Q}$. The dimension of F as a $\mathbf{Q}$-vector space is called the *degree* of F. It is denoted by $[F : \mathbf{Q}]$.

Examples of number fields are $\mathbf{Q}$, $\mathbf{Q}(i)$, $\mathbf{Q}(\sqrt[4]{2})$, $\mathbf{Q}(\sqrt[3]{3}, \sqrt{7})$ and $\mathbf{Q}(\sqrt{2}, \sqrt{1+\sqrt{2}})$ of degrees 1, 2, 4, 6 and 4 respectively. The following theorem says that every number field can be generated by one element only. This element is by no means unique.

Theorem 2.2. *(Theorem of the primitive element.) Let F be a finite extension of $\mathbf{Q}$. Then there exists $\alpha \in F$ such that $F = \mathbf{Q}(\alpha)$.*

Proof. It suffices to consider the case where $F = \mathbf{Q}(\alpha, \beta)$. The general case follows by induction. We must show that there is an element $\theta \in F$ such that $\mathbf{Q}(\alpha, \beta) = \mathbf{Q}(\theta)$.

We will take for θ a suitable linear combination of α and β: let $f(T) = f^{\alpha}_{\min}(T)$ the minimum polynomial of α over $\mathbf{Q}$. Let $n = \deg(f)$ and let $\alpha = \alpha_1, \alpha_2, \ldots, \alpha_n$ be the zeroes of f in $\mathbf{C}$. The α_i are all distinct. Similarly we let $g(T) = f^{\beta}_{\min}(T)$ the minimum polynomial of β over $\mathbf{Q}$. Let $m = \deg(g)$ and let $\beta = \beta_1, \beta_2, \ldots, \beta_m$ be the zeroes of g in $\mathbf{C}$. Since $\mathbf{Q}$ is an infinite field, we can find $\lambda \in \mathbf{Q}^*$ such that

$$\lambda \neq \frac{\alpha_i - \alpha}{\beta - \beta_j} \qquad \text{for } 1 \leq i \leq n \text{ and for } 2 \leq j \leq m,$$

or equivalently,

$$\alpha + \lambda\beta \neq \alpha_i + \lambda\beta_j \qquad \text{for } 1 \leq i \leq n \text{ and for } 2 \leq j \leq m.$$

Put

$$\theta = \alpha + \lambda\beta.$$

The polynomials $h(T) = f(\theta - \lambda T)$ and $g(T)$ are both in $\mathbf{Q}(\theta)[T]$ and they both have β as a zero. The remaining zeroes of $g(T)$ are $\beta_2, \ldots, \beta_m$ and those of $h(T)$ are $(\theta - \alpha_i)/\lambda$ for $2 \leq i \leq n$. By our choice of λ, we have that $\beta_j \neq (\theta - \alpha_i)/\lambda$ for all $1 \leq i \leq n$ and $2 \leq j \leq m$. Therefore the gcd of $h(T)$ and $g(T)$ is $T - \beta$. Since $g(T), h(T)$ are monic poynomials in $\mathbf{Q}(\theta)[T]$ we have that $T - \beta \in \mathbf{Q}(\theta)[T]$. This implies that $\beta \in \mathbf{Q}(\theta)$ and hence that $\alpha \in \mathbf{Q}(\theta)$. It follows that $\mathbf{Q}(\alpha, \beta) = \mathbf{Q}(\theta)$ as required.

Corollary 2.3. *Let F be a finite extension of degree n of $\mathbf{Q}$. There are exactly n distinct field homomorphisms $\phi : F \longrightarrow \mathbf{C}$.*

Proof. By Theorem 2.2 we can write $F = \mathbf{Q}(\alpha)$ for some α. Let f be the minimum polynomial of α over $\mathbf{Q}$. A homomorphism ϕ from F to $\mathbf{C}$ induces the identity on $\mathbf{Q}$ (see Exer.2.D). Therefore it is determined by the image $\phi(\alpha)$ of α. We have that $0 = \phi(f(\alpha)) = f(\phi(\alpha))$. In other words, $\phi(\alpha)$ is a zero of $f(T)$. Conversely, every zero $\beta \in \mathbf{C}$ of $f(T)$ gives rise to a homomorphism $\phi : F \longrightarrow \mathbf{C}$ given by $\phi(\alpha) = \beta$. This shows that there are exactly as many distinct homomorphism $F \longrightarrow \mathbf{C}$ as the degree n of f, as required.

Proposition 2.4. *Let F be a number field of degree n over $\mathbf{Q}$. Let $\omega_1, \ldots, \omega_n \in F$. Then $\omega_1, \ldots, \omega_n$ form a basis for F as a $\mathbf{Q}$-vector space if and only if $\det(\phi(\omega_i))_{\phi,i} \neq 0$. Here i runs from 1 to n and ϕ runs over all homomorphisms $\phi : F \longrightarrow \mathbf{C}$.*

Proof. First of all, note that by Cor.2.3, the matrix $(\phi(\omega_i))_{\phi,i}$ is a square matrix! Suppose that there exists a relation $\sum_i \lambda_i\omega_i = 0$ with $\lambda_i \in \mathbf{Q}$ not all zero. Since $\phi(\lambda) = \lambda$ for every $\lambda \in \mathbf{Q}$, we see that $\sum_i \lambda_i\phi(\omega_i) = 0$ for every $\phi : F \longrightarrow \mathbf{C}$. This implies that $\det(\phi(\omega_i))_{\phi,i} = 0$.

To prove the converse, we write $F = \mathbf{Q}(\alpha)$ for some α. Consider the $\mathbf{Q}$-basis $1, \alpha, \alpha^2, \ldots, \alpha^{n-1}$. For this basis the the matrix $(\phi(\omega_i))_{\phi,i} = (\phi(\alpha)^{i-1}))_{\phi,i}$ is a Vandermonde matrix (see Exer.2.E) with determinant equal to a product of terms of the form $(\phi_1(\alpha) - \phi_2(\alpha))$ with $\phi_1 \neq \phi_2$. Since the zeroes $\phi(\alpha) \in \mathbf{C}$ of the minimum polynomial of α are all distinct, this determinant is not zero.

So, for the basis $1, \alpha, \alpha^2, \ldots, \alpha^{n-1}$ the theorem is valid. For an arbitrary $\mathbf{Q}$-basis $\omega_1, \ldots, \omega_n$ there exists a matrix $M \in \mathrm{GL}_n(\mathbf{Q})$ such that

$$\begin{pmatrix} \omega_1 \\ \omega_2 \\ \vdots \\ \omega_n \end{pmatrix} = M \begin{pmatrix} 1 \\ \alpha \\ \vdots \\ \alpha^{n-1} \end{pmatrix}.$$

applying the homomorphisms $\phi : F \longrightarrow \mathbf{C}$ one obtains the following equality of $n \times n$ matrices:

$$(\phi(\omega_i))_{\phi,i} = M \cdot (\phi(\alpha^i))_{\phi,i},$$

and therefore

$$\det((\phi(\omega_i))_{\phi,i}) = \det(M) \cdot \det((\phi(\alpha^i))_{\phi,i}) \neq 0,$$

as required. This proves the proposition.

The number field $\mathbf{Q}$ admits a unique embedding into the field of complex numbers $\mathbf{C}$. The image of this embedding is contained in $\mathbf{R}$. In general, a number field F admits several embeddings in $\mathbf{C}$, and the images of these embeddings are not necessarily contained in $\mathbf{R}$. We generalize the embedding $\Phi : \mathbf{Q} \hookrightarrow \mathbf{R}$ as follows.

Let F be a number field and let $\alpha \in F$ be such that $F = \mathbf{Q}(\alpha)$. In other words $F = \mathbf{Q}[T]/(f(T))$ where $f(T)$ denotes the minimum polynomial of α. Let $n = \deg(f)$. We put

$$F \otimes \mathbf{R} = \mathbf{R}[T]/(f(T)).$$

In these notes, $F \otimes \mathbf{R}$ is just our notation for the $\mathbf{R}$-algebra $\mathbf{R}[T]/(f(T))$. This algebra is actually the tensor product of F over $\mathbf{Q}$ with $\mathbf{R}$ and this also shows that the construction does not depend on the choice of α, but we will not use this interpretation. The natural map $\mathbf{Q}[T]/(f(T)) \longrightarrow \mathbf{R}[T]/(f(T))$ gives us a map

$$\Phi : F \longrightarrow F \otimes \mathbf{R}.$$

We compute the ring $F \otimes \mathbf{R}$ explicitly: since $\mathbf{C}$ is an algebraically closed field, the polynomial $f(T) \in \mathbf{Q}[T]$ factors completely over $\mathbf{C}$. Let's say it has precisely r_1 real zeroes $\beta_1, \ldots, \beta_{r_1}$ and r_2 pairs of complex conjugate zeroes $\gamma_1, \bar{\gamma}_1, \ldots, \gamma_{r_2}, \bar{\gamma}_{r_2}$. We have

$$r_1 + 2r_2 = n.$$

The numbers r_1 and r_2 depend only on the number field F and not on the choice of α. By the Chinese Remainder Theorem there is an isomorphism

$$F \otimes \mathbf{R} \xrightarrow{\cong} \mathbf{R}^{r_1} \times \mathbf{C}^{r_2}$$

given by $T \mapsto (\beta_1, \ldots, \beta_{r_1}, \gamma_1, \ldots, \gamma_{r_2})$. Identifying the spaces $F \otimes \mathbf{R}$ and $\mathbf{R}^{r_1} \times \mathbf{C}^{r_2}$ by means of this isomorphism, we obtain an explicit description of the map Φ:

Definition 2.5. *Let F be a number field. With the notation above, the map Φ*

$$\Phi : F \longrightarrow \mathbf{R}^{r_1} \times \mathbf{C}^{r_2}$$

is defined by

$$\Phi(x) = (\phi_1(x), \ldots, \phi_{r_1}(x), \phi_{r_1+1}(x), \ldots, \phi_{r_2+r_1}(x))$$

where the $\phi_i : F \longrightarrow \mathbf{C}$ are determined by $\phi_i(\alpha) = \beta_i$ for $1 \leq i \leq r_1$ and $\phi_{r_1+i}(\alpha) = \gamma_i$ for $1 \leq i \leq r_2$.

For completeness sake we define $\phi_{r_1+r_2+i}(\alpha) = \bar{\gamma}_i$ for $1 \leq i \leq r_2$. The map Φ is not canonical: replacing γ_i by $\bar{\gamma}_i$ would give a different map Φ. This ambiguity is not important in the sequel.

Example. Let $\alpha = \sqrt[4]{2}$ be a zero of $T^4 - 2 \in \mathbf{Q}[T]$ and let $F = \mathbf{Q}(\alpha)$. The minimum polynomial of α is $T^4 - 2$. It has two real roots $\pm\sqrt[4]{2}$ and two complex conjugate roots $\pm i\sqrt[4]{2}$. We conclude that $r_1 = 2$ and $r_2 = 1$. The homomorphisms $\phi_i : F \longrightarrow \mathbf{C}$ are determined by

$$\begin{aligned}
\phi_1(\alpha) &= \sqrt[4]{2},\\
\phi_2(\alpha) &= -\sqrt[4]{2},\\
\phi_3(\alpha) &= i\sqrt[4]{2},\\
\phi_4(\alpha) &= -i\sqrt[4]{2}.
\end{aligned}$$

The map

$$\Phi : F \longrightarrow F \otimes \mathbf{R} = \mathbf{R} \times \mathbf{R} \times \mathbf{C}$$

is, given by

$$\Phi(x) = (\phi_1(x), \phi_2(x), \phi_3(x)).$$

Theorem 2.6. *Let F be a number field of degree n.*
(i) The map $\Phi : F \longrightarrow F \otimes \mathbf{R}$ maps a $\mathbf{Q}$-basis of F to an $\mathbf{R}$-basis of $F \otimes \mathbf{R}$.
(ii) The map Φ is injective.
(iii) The image $\Phi(F)$ is a dense subset in the vector space $F \otimes \mathbf{R} = \mathbf{R}^{r_1} \times \mathbf{C}^{r_2}$, equipped with the usual Euclidean topology.

Proof. *(i)* We identify the real vectorspace $\mathbf{C}$ with $\mathbf{R}^2$ by means of the usual correspondence

$$z \leftrightarrow (\,\mathrm{Re}(z), \mathrm{Im}(z)\,).$$

Let $\omega_1, \ldots, \omega_n$ be a $\mathbf{Q}$-basis of F. Then

$$\Phi(\omega_i) = (\ldots, \phi_k(\omega_i), \ldots, \mathrm{Re}(\phi_l(\omega_i)), \mathrm{Im}(\phi_l(\omega_i)), \ldots),$$

where k denotes a "real" index whenever $1 \leq k \leq r_1$ and l denotes a "complex" index whenever $r_1 + 1 \leq l \leq r_1 + r_2$. We put the vectors $\Phi(\omega_i)$ in an $n \times n$-matrix:

$$\Phi \begin{pmatrix} \omega_1 \\ \omega_2 \\ \vdots \\ \omega_n \end{pmatrix} = \begin{pmatrix} \ldots & \phi_k(\omega_1) & \ldots & \mathrm{Re}\phi_l(\omega_1) & \mathrm{Im}\phi_l(\omega_1) & \ldots \\ \ldots & \phi_k(\omega_2) & \ldots & \mathrm{Re}\phi_l(\omega_2) & \mathrm{Im}\phi_l(\omega_2) & \ldots \\ & \vdots & & \vdots & \vdots & \\ \ldots & \phi_k(\omega_n) & \ldots & \mathrm{Re}\phi_l(\omega_n) & \mathrm{Im}\phi_l(\omega_n) & \ldots \end{pmatrix}.$$

The first r_1 columns correspond to the homomorphisms $\phi_k : F \hookrightarrow \mathbf{R}$ and the remaining $2r_2$ to the real and imaginary parts of the remaining non-conjugate homomorphisms $\phi_l : F \hookrightarrow \mathbf{C}$. Using the formula $\mathrm{Re}(z) = (z + \bar{z})/2$ and $\mathrm{Im}(z) = (z - \bar{z})/2i$ one sees that the determinant of this matrix is equal to

$$(2i)^{-r_2}\det(\phi_k(\omega_j))_{k,j}.$$

By Prop.2.4 its value is different from zero. Therefore the $\Phi(\omega_i)$ form an $\mathbf{R}$-basis for $F \otimes \mathbf{R}$.

(ii) Let $x \in F$ and $\Phi(x) = 0$. This implies, in particular, that $\phi_1(x) = 0$. Since ϕ_1 is a homomorphism of fields, it is injective and we conclude that $x = 0$, as required.

(iii) The image of Φ is a $\mathbf{Q}$-vector space and it contains an $\mathbf{R}$-basis by part *(i)*. Therefore it is dense.

Example 2.7. *(Cyclotomic fields)* For any $m \in \mathbf{Z}_{\geq 1}$ we define the *m-th cyclotomic polynomial* $\Phi_m(T) \in \mathbf{Z}[T]$ in the following inductive manner:

$$X^m - 1 = \prod_{d|m} \Phi_d(T);$$

alternatively

$$\Phi_m(T) = \prod k \in (\mathbf{Z}/m\mathbf{Z})^*(T - e^{(2\pi i k)/m}.$$

The degree of Φ_m is $\varphi(m)$, where $\varphi(m) = \#(\mathbf{Z}/m\mathbf{Z})^*$ is Euler's φ-function. See Exerc.2.K. It is rather easy to show that Φ_m is irreducible over $\mathbf{Q}$ when m is a power of a prime number, but, in general, the proof is delicate. We give it here:

Proposition 2.8. *The cyclotomic polynomial $\Phi_m(T)$ is irreducible in $\mathbf{Q}[T]$.*

Proof. Let $g(T) \in \mathbf{Q}[T]$ be a monic irreducible factor of $\Phi_m(T)$ and write $T^m - 1 = g(T)h(T)$. By Gauß's Lemma $g(T), h(T) \in \mathbf{Z}[T]$. Suppose $\alpha \in \mathbf{C}$ is a zero of g. Then α is a zero of $T^m - 1$. Let p be a prime not dividing m. Then α^p is also a zero of $T^m - 1$. If $g(\alpha^p) \neq 0$, then $h(\alpha^p) = 0$ and therefore $g(T)$ divides $h(T^p)$. This implies that $g(T)$ divides $h(T)^p$ in the ring $\mathbf{F}_p[T]$. Let $\phi(T)$ denote an irreducible divisor of $g(T)$ in $\mathbf{F}_p[T]$. Then $\phi(T)$ divides both $g(T)$ and $h(T)$ modulo p. This implies that $T^m - 1$ has a double zero mod p. But this is impossible because the derivative mT^{m-1} has, since $m \not\equiv 0 \pmod{p}$, no zeroes in common with $T^m - 1$.

Therefore $g(\alpha^p) = 0$. We conclude that for *every* prime p not dividing m and every $\alpha \in \mathbf{C}$ with $f(\alpha) = 0$, one has that $g(\alpha^p) = 0$. This implies that $g(\alpha^k) = 0$ for every integer k which is coprime to m. This shows that $\Phi_m(T)$ and $g(T)$ have the same zeroes and hence that $\Phi_m(T) = g(T)$ is irreducible. This proves the proposition.

We conclude that the *cyclotomic* fields $\mathbf{Q}[X]/(\Phi_m(X))$ are number fields of degree $\varphi(m)$. Usually one writes $\mathbf{Q}(\zeta_m)$ for these fields; here ζ_m denotes a zero of $\Phi_m(T)$, i.e., a primitive m-th root of unity.

(2.A) Compute the degrees of the number fields $\mathbf{Q}(\sqrt{2}, \sqrt{-6})$ and $\mathbf{Q}(\sqrt{-2}, \sqrt{3}, \sqrt{-6})$.
(2.B) Find an element $\alpha \in F = \mathbf{Q}(\sqrt{3}, \sqrt{-5})$ such that $F = \mathbf{Q}(\alpha)$.
(2.C) Let p be a prime. Compute the minimum polynomial of a primitive p-th root of unity ζ_p. Show that $[\mathbf{Q}(\zeta_p) : \mathbf{Q}] = p - 1$.
(2.D) Let $\phi : \mathbf{Q} \to \mathbf{C}$ be a field homomorphism. Show that $\phi(q) = q$ for every $q \in \mathbf{Q}$.
(2.E) (*VanderMonde)* Let R be a commutative ring and let $\alpha_1, \alpha_2, \ldots, \alpha_n \in R$. Show that

$$\det \begin{pmatrix} 1 & 1 & \ldots & 1 \\ \alpha_1 & \alpha_2 & \ldots & \alpha_n \\ \alpha_1^2 & \alpha_2^2 & \ldots & \alpha_n^2 \\ \vdots & \vdots & \ddots & \vdots \\ \alpha_1^{n-1} & \alpha_2^{n-1} & \ldots & \alpha_n^{n-1} \end{pmatrix} = \prod_{1 \leq i < j \leq n} (\alpha_j - \alpha_i).$$

(2.F) Consider the extension $L = \mathbf{F}_p(\sqrt[p]{X}, \sqrt[p]{Y})$ of the field $K = \mathbf{F}_p(X, Y)$. Show that the theorem of the primitive element does not hold in this case. Show that there are infinitely many distinct fields F with $K \subset F \subset L$.

(2.G) Let K be a finite extension of degree n of a finite field $\mathbf{F}_q$. Show

  (i) there exists $\alpha \in K$ such that $K = \mathbf{F}_q(\alpha)$;

  (ii) there are precisely n distinct embeddings $\phi_i : K \longrightarrow \overline{\mathbf{F}_q}$ which induce the identity map on $\mathbf{F}_q$.

(2.H) Let $F = \mathbf{Q}(\sqrt[6]{5})$. Give the homomorphism $\Phi : F \longrightarrow F \otimes \mathbf{R}$ explicitly as in Definition 2.5.

(2.I) Find a $\mathbf{Q}$-basis for $\mathbf{Q}(\sqrt{2}, \sqrt{-1})$ and $\mathbf{Q}(\sqrt[3]{2}, \zeta_3)$.

(2.J) Let F be a number field with $r_1 \geq 1$, i.e. F admits an embedding into $\mathbf{R}$. Show that the only roots of unity in F are ± 1.

(2.K) Let Φ_m denote the m-th cyclotomic polynomial.

  (i) Show that

$$\Phi_m(T) = \prod k \in (\mathbf{Z}/m\mathbf{Z})^*(T - e^{(2\pi i k)/m}.$$

  (ii) Show that

$$\begin{aligned}
\Phi_1(T) &= T - 1, \\
\Phi_2(T) &= T + 1, \\
\Phi_3(T) &= T^2 + T + 1, \\
\Phi_4(T) &= T^2 + 1, \\
\Phi_5(T) &= T^4 + T^3 + T^2 + T + 1, \\
\Phi_6(T) &= T^2 - T + 1, \\
\Phi_7(T) &= T^6 + T^5 + T^4 + T^3 + T^2 + T + 1, \\
\Phi_8(T) &= T^4 + 1, \\
\Phi_9(T) &= T^6 + T^3 + 1, \\
\Phi_{10}(T) &= T^4 - T^3 + T^2 - T + 1.
\end{aligned}$$

  (ii) Show that $\Phi_m(T) \in \mathbf{Z}[T]$ for every m.

  (iv) Show that $\deg(\Phi_m) = \varphi(m)$ where $\varphi(m) = \#(\mathbf{Z}/m\mathbf{Z})^*$ denotes the φ-function of Euler.

  (v) Let l be a prime and let $k \geq 1$. Show that

$$\Phi_{l^k}(T) = T^{l^{k-1}(l-1)} + T^{l^{k-1}(l-2)} + \ldots + T^{l^{k-1}} + 1.$$

  Show that $\Phi_{l^k}(S+1)$ is an Eisenstein polynomial with respect to l. Conclude it is irreducible over $\mathbf{Q}$.

(2.L) Let $m \geq 1$ be an integer. Compute the numbers r_1 and r_2 associated to $F = \mathbf{Q}(\zeta_m)$ in Def.2.5.

3. Norms, Traces and Discriminants.

In this section we introduce the characteristic polynomial of an element, its norm and its trace. We define the discriminant of an n-tuple of elements in a number field of degree n.

Let F be a number field of degree n and let $x \in F$. Multiplication by x is a $\mathbf{Q}$-linear map $M_x : F \longrightarrow F$. With respect to a $\mathbf{Q}$-basis of F, one can view M_x as an $n \times n$-matrix with rational coefficients.

Definition 3.1. *Let F be a number field of degree n and let $x \in F$. The characteristic polynomial $f^x_{\text{char}}(T) \in \mathbf{Q}[T]$ of x is*

$$f^x_{\text{char}}(T) = \det(T \cdot \text{Id} - M_x).$$

We have $f^x_{\text{char}}(T) = T^n + a_{n-1}T^{n-1} + \ldots + a_1 T + a_0$ with $a_i \in \mathbf{Q}$. The norm $\mathrm{N}(x)$ and the trace $\mathrm{Tr}(x)$ of x are defined by

$$\mathrm{N}(x) = \det(M_x) = (-1)^n a_0,$$
$$\mathrm{Tr}(x) = \mathrm{Trace}(M_x) = -a_{n-1}.$$

It is immediate from the definitions that $\mathrm{Tr}(x)$ and $\mathrm{N}(x)$ are rational numbers. They are well defined, because the characteristic polynomial, the norm and the trace of x do not depend on the basis with respect to which the matrix M_x has been defined. One should realize that the characteristic polynomial $f^x_{\text{char}}(T)$, and therefore the norm $\mathrm{N}(x)$ and the trace $\mathrm{Tr}(x)$ depend on the field F in which we consider x to be! We don't write $\mathrm{Tr}_F(x)$ or $\mathrm{N}_F(x)$ in order not to make the notation to cumbersome. The norm and the trace have the following, usual properties:

$$\mathrm{N}(xy) = \mathrm{N}(x)\mathrm{N}(y)$$
$$\mathrm{Tr}(x+y) = \mathrm{Tr}(x) + \mathrm{Tr}(y)$$

for $x, y \in F$.

Example. Let $F = \mathbf{Q}(\sqrt[4]{2})$ and let $x = \sqrt{2} = (\sqrt[4]{2})^2 \in F$. We take $\{1, \sqrt[4]{2}, \sqrt{2}, (\sqrt[4]{2})^3\}$ as a $\mathbf{Q}$-basis of F. With respect to this basis, the multiplication by x is given by the matrix M_x

$$\begin{pmatrix} 0 & 0 & 2 & 0 \\ 0 & 0 & 0 & 2 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix}.$$

It is easily verified that the characteristic polynomial of x is $f^x_{\text{char}}(T) = T^4 - 4T^2 + 4$, its norm is $\mathrm{N}(x) = 4$ and its trace is $\mathrm{Tr}(x) = 0$. If we consider, on the other hand, $x = \sqrt{2}$ in $F = \mathbf{Q}(\sqrt{2})$, then the characteristic polynomial of $x = \sqrt{2}$ is $f^x_{\text{char}}(T) = T^2 - 2$, its norm $\mathrm{N}(x) = 2$ and its trace $\mathrm{Tr}(x) = 0$.

Proposition 3.2. *Let F be a number field of degree n and let $x \in F$. Then*

(i)

$$f^x_{\text{char}}(T) = \prod_{\phi: F \hookrightarrow \mathbf{C}} (T - \phi(x)),$$

(ii)

$$f^x_{\text{char}}(T) = f^x_{\min}(T)^{[F:\mathbf{Q}(x)]},$$

(iii) One has $\mathrm{N}(x) = \prod_\phi \phi(x)$ and $\mathrm{Tr}(x) = \sum_\phi \phi(x)$, where the product and the sum run over all n embeddings $\phi : F \hookrightarrow \mathbf{C}$.

Proof. *(i)* We have the following commutative diagram:

$$\begin{array}{ccc} F & \xrightarrow{\Phi} & \mathbf{R}^{r_1}\times\mathbf{C}^{r_2} \\ \Big\downarrow{\scriptstyle x} & & \Big\downarrow{\scriptstyle (\phi_1(x),\ldots,\phi_{r_1+r_2}(x))} \\ F & \xrightarrow{\Phi} & \mathbf{R}^{r_1}\times\mathbf{C}^{r_2} \end{array}$$

where the righthand arrow is given by multiplication by $\phi_i(x)$ on the i-th coordinate of $F\otimes\mathbf{R} = \mathbf{R}^{r_1}\times\mathbf{C}^{r_2}$.

By Theorem 2.6*(i)*, the image of any $\mathbf{Q}$-basis of F under Φ is an $\mathbf{R}$-basis. When we write the linear map on the right as a matrix with respect to such a basis, we obtain the matrix M_x. When we do this with respect to the canonical basis of $\mathbf{R}^{r_1}\times\mathbf{C}^{r_2}$, we find a matrix which is diagonal as far as the "real" coordinates are concerned. If the i-th coordinate is "complex", we identify $\mathbf{C}$ with $\mathbf{R}^2$ via $z\leftrightarrow(\mathrm{Re}(z),\mathrm{Im}(z))$. In this way, the multiplication by $\phi_i(x)$ can be represented by a 2×2-matrix

$$\begin{pmatrix} \mathrm{Re}\phi_i(x) & \mathrm{Im}\phi_i(x) \\ -\mathrm{Im}\phi_i(x) & \mathrm{Re}\phi_i(x) \end{pmatrix}$$

with eigenvalues $\phi_i(x)$ and $\phi_{r_2+i}(x)=\overline{\phi_i(x)}$. Altogether we find an $n\times n$-matrix with eigenvalues the $\phi_i(x)$ for $1\le i\le n$. Therefore the characteristic polynomial is $\prod_{i=1}^n(T-\phi_i(x))$. Since the characteristic polynomial of M_x does not depend on the basis, the result follows.
(ii) Let $g(T)\in\mathbf{Q}[T]$ be an irreducible divisor of $f^x_{\mathrm{char}}(T)$. We conclude from *(i)* that $g(T)$ has one of the $\phi_i(x)$ as a zero. Since g has rational coefficients, we have that

$$\phi_i(g(x)) = g(\phi_i(x)) = 0$$

and hence, since ϕ_i is an injective field homomorphism, that $g(x)=0$. Therefore f^x_{min} divides g and by the irreducibility we have that $g=f^x_{\mathrm{min}}$. Since g was an arbitrary irreducible divisor of the characteristic polynomial, it follows that $f^x_{\mathrm{char}}(T)$ is a power of $f^x_{\mathrm{min}}(T)$. Finally, the degree of f^x_{char} is $n=[F:\mathbf{Q}]$ and the degree of f^x_{min} is $[\mathbf{Q}(x):\mathbf{Q}]$. This easily implies *(ii)*.
(iii) This is immediate from *(i)*. The proof of the proposition is now complete.

Next we introduce *discriminants.*

Definition 3.3. *Let F be a number field of degree n and let $\omega_1,\omega_2,\ldots,\omega_n\in F$. We define the discriminant* $\Delta(\omega_1,\omega_2,\ldots,\omega_n)\in\mathbf{Q}$ by

$$\Delta(\omega_1,\omega_2,\ldots,\omega_n) = \det(\mathrm{Tr}(\omega_i\omega_j)_{1\le i,j\le n}).$$

The discriminant depends only on the *set* $\{\omega_1,\omega_2,\ldots,\omega_n\}$ and not on the order of the elements. The basic properties of discriminants are contained in the following proposition.

Proposition 3.4. *Let F be a number field of degree n and let $\omega_1,\omega_2,\ldots,\omega_n\in F$. then*
(i)

$$\Delta(\omega_1,\omega_2,\ldots,\omega_n) = \det(\phi(\omega_i))^2_{i,\phi}\in\mathbf{Q}.$$

(ii) $\Delta(\omega_1,\omega_2,\ldots,\omega_n)\neq 0$ *if and only if* $\omega_1,\omega_2,\ldots,\omega_n$ *is a basis for F as a vector space over* $\mathbf{Q}$.
(iii) *If $\omega_i'=\sum_{j=1}^n\lambda_{ij}\omega_j$ with $\lambda_{ij}\in\mathbf{Q}$ for $1\le i,j\le n$, then one has that*

$$\Delta(\omega_1',\omega_2',\ldots,\omega_n') = \det(\lambda_{ij})^2\Delta(\omega_1,\omega_2,\ldots,\omega_n).$$

Proof. *(i)* The determinant is rational, because its entries are traces of elements in F and therefore rational numbers. From Prop.3.2*(iii)* one deduces the following equality of $n \times n$ matrices:

$$\begin{pmatrix} \phi_1(\omega_1) & \phi_2(\omega_1) & \ldots \\ \phi_1(\omega_2) & \phi_2(\omega_2) & \ldots \\ \phi_1(\omega_3) & \phi_2(\omega_3) & \ldots \\ \vdots & \vdots & \ddots \end{pmatrix} \cdot \begin{pmatrix} \phi_1(\omega_1) & \phi_1(\omega_2) & \ldots \\ \phi_2(\omega_1) & \phi_2(\omega_2) & \ldots \\ \phi_3(\omega_2) & \phi_3(\omega_2) & \ldots \\ \vdots & \vdots & \ddots \end{pmatrix} = \begin{pmatrix} \mathrm{Tr}(\omega_1^2) & \mathrm{Tr}(\omega_1\omega_2) & \ldots \\ \mathrm{Tr}(\omega_1\omega_2) & \mathrm{Tr}(\omega_2^2) & \ldots \\ \mathrm{Tr}(\omega_1\omega_3) & \mathrm{Tr}(\omega_2\omega_3) & \ldots \\ \vdots & \vdots & \ddots \end{pmatrix}$$

and *(i)* follows easily.
(ii) Immediate from Prop.2.4.
(iii) We have the following product of $n \times n$ matrices

$$(\lambda_{i,j})_{i,j}(\phi_j(\omega'_k))_{j,k} = (\phi_i(\omega_k))_{i,k},$$

and *(iii)* follows from *(i)*.

This finishes the proof of Prop.3.4.

In the sequel we will calculate several discriminants. Therefore we briefly recall the relation between discriminants in the sense of Def.3.3 and discriminants and resultants of polynomials.

Let K be a field, let $b, c \in K^*$ and let $\beta_1, \beta_2, \ldots, \beta_r \in K$ and $\gamma_1, \gamma_2, \ldots, \gamma_s \in K$. Put $g(T) = b\prod_{i=1}^r (T - \beta_i)$ and $h(T) = c\prod_{i=1}^s (T - \gamma_i)$. The *Resultant* $\mathrm{Res}(g, h)$ of g and h is defined by

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

Resultants can be calculated efficiently by means of an algorithm, which is very similar to the Euclidean algorithm in the polynomial ring $K[T]$. See Exer.3.K for the details. Discriminants of polynomials can be expressed in terms of certain resultants. Let $\alpha_1, \ldots, \alpha_n \in K$. Let $f(T) = \prod_{i=1}^n (T - \alpha_i) \in K[T]$. The *discriminant* $\mathrm{Disc}(f)$ of f is defined by

$$\mathrm{Disc}(f) = \prod_{1 \le i < j \le n} (\alpha_i - \alpha_j)^2.$$

By differentiating the relation $f(T) = \prod_{j=1}^n (T - \alpha_j)$ and substituting $T = \alpha_i$ one finds that $f'(\alpha_i) = \prod_{j \neq i}^n (\alpha_i - \alpha_j)$ and one deduces easily that

$$\mathrm{Disc}(f) = (-1)^{\frac{n(n-1)}{2}} \mathrm{Res}(f, f').$$

Proposition (3.5). *Let F be a number field of degree n. Let $\alpha \in F$ and let $f = f_{\mathrm{char}}^{\alpha}$ denote its characteristic polynomial. Then*

$$\Delta(1, \alpha, \ldots, \alpha^{n-1}) = \mathrm{Disc}(f) = (-1)^{\frac{n(n-1)}{2}} \mathrm{N}(f'(\alpha)) = (-1)^{\frac{n(n-1)}{2}} \mathrm{Res}(f, f').$$

Proof. The first equality follows from Prop.3.4*(i)* and the Vandermonde determinant in Exer.2.E. The second follows by differentiating both sides of the equation $f(T) = \prod_{j=1}^n (T - \phi_j(\alpha))$, substituting $\phi_i(\alpha)$ for T and applying Prop.3.2*(iii)*. The third equality has been explained above.

(3.A) Let F be a number field of degree n and let $x \in F$. Show that for $q \in \mathbf{Q} \subset F$ one has that

$$\begin{aligned} \mathrm{Tr}(qx) &= q\mathrm{Tr}(x), \\ \mathrm{Tr}(q) &= nq, \\ \mathrm{N}(q) &= q^n. \end{aligned}$$

Show that the map $\mathrm{Tr} : F \longrightarrow \mathbf{Q}$ is surjective. Show that the norm $\mathrm{N} : F^* \longrightarrow \mathbf{Q}^*$ is, in general, not surjective.

(3.B) Let F be a number field of degree n and let $\alpha \in F$. Show that for $q \in \mathbf{Q}$ one has that $\mathrm{N}(q-\alpha) = f_{\mathrm{char}}^{\alpha}(q)$. Show that for $q, r \in \mathbf{Q}$ one has that $\mathrm{N}(q - r\alpha) = r^n f_{\mathrm{char}}^{\alpha}(q/r)$.

(3.C) Let $\alpha = \zeta_5 + \zeta_5^{-1} \in \mathbf{Q}(\zeta_5)$ where ζ_5 denotes a primitive 5th root of unity. Calculate the characteristic polynomial of $\alpha \in \mathbf{Q}(\zeta_5)$.

(3.D) Prove that $\mathrm{Disc}(T^n - a) = n^n a^{n-1}$. Compute $\mathrm{Disc}(T^2 + bT + c)$ and $\mathrm{Disc}(T^3 + bT + c)$.

(3.E) Let $f(T) = T^5 - T + 1 \in \mathbf{Z}[T]$. Show that f is irreducible. Determine r_1, r_2 and the discriminant of f.

(3.F) Consider the field $\mathbf{Q}(\sqrt{3}, \sqrt{5})$. Compute $\Delta(1, \sqrt{3}, \sqrt{5}, \sqrt{15})$ and $\Delta(1, \sqrt{3}, \sqrt{5}, \sqrt{3} + \sqrt{5})$.

(3.G) Let K be a field and let $f \in K[T]$. Show that f has a double zero if and only if $\mathrm{Disc}(f) = 0$. Let $h \in \mathbf{Z}[T]$ be a monic polynomial. Show that it has a double zero modulo a prime p if and only if p divides $\mathrm{Disc}(f)$.

(3.H) Let F be a number field of degree n. Let $\alpha \in F$. Show that

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

Here p_k denotes the power sum $\phi_1(\alpha)^k + \ldots + \phi_n(\alpha)^k$. The ϕ_i denote the embeddings $F \hookrightarrow \mathbf{C}$.

(3.I) (*Newton's formulas*) Let K be a field and let $\alpha_1, \alpha_2, \ldots, \alpha_n \in K$. We define the *symmetric functions* s_k of the α_i by

$$\prod_{i=1}^{n}(T - \alpha_i) = T^n - s_1 T^{n-1} + s_2 T^{n-2} + \ldots + (-1)^n s_n.$$

We extend the definition by putting $s_k = 0$ whenever $k > n$. We define the *power sums* p_k by

$$p_k = \sum_{i=1}^{n} \alpha_i^k \qquad \text{for } k \ge 0.$$

Show that for every $k \ge 1$ one has that

$$(-1)^k k s_k = p_k - p_{k-1}s_1 + p_{k-2}s_2 - p_{k-3}s_3 + \ldots.$$

In particular

$$\begin{aligned} s_1 &= p_1 \\ -2s_2 &= p_2 - p_1 s_1 \\ 3s_3 &= p_3 - p_2 s_1 + p_1 s_2 \\ -4s_4 &= p_4 - p_3 s_1 + p_2 s_2 - p_1 s_3 \\ 5s_5 &= \ldots \end{aligned}$$

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

(3.J) Show that the polynomial $T^5 + T^3 - 2T + 1 \in \mathbf{Z}[T]$ is irreducible. Compute its discriminant. (Hint: use Prop.3.5)

(3.K) (*Resultants*) Let K be a field and let $\alpha_1, \ldots, \alpha_r \in K$. Put $g = b\prod_{i=1}^{r}(T - \alpha_i)$ and let $h, h' \in K[T]$ be non-zero polynomials of degree s and s' respectively. Suppose that $h \equiv h' \pmod{g}$.

(i) Show that $\mathrm{Res}(g, h) = (-1)^{rs}\mathrm{Res}(h, g)$.

(ii) Show that $\mathrm{Res}(g, h) = b^s \prod_{\alpha, g(\alpha)=0} h(\alpha)$.

(iii) Show that $b^{s'}\mathrm{Res}(g,h) = b^{s}\mathrm{Res}(g,h')$

(iv) Using parts (i) and (ii), design an efficient algorithm, similar to the Euclidean algorithm in the ring $K[T]$, to calculate resultants of polynomials.

(3.L) Let $\mathbf{F}_q$ be a finite field with q elements. Let K be a finite extension of $\mathbf{F}_q$ and let $\omega_1, \omega_2, \ldots, \omega_n \in K$. Show that the discriminant $\Delta(\omega_1, \ldots, \omega_n) = \det(\mathrm{Tr}(\omega_i\omega_j)_{i,j})$ is not zero if and only if $\omega_1, \ldots, \omega_n$ is an $\mathbf{F}_q$-basis for K. Here the definition of the trace $\mathrm{Tr}(\alpha)$ of an element $\alpha \in K$ is similar to Def.3.1. (Hint: copy the proof of Prop.3.4)

(3.M) For $n \in \mathbf{Z}_{\geq 1}$ let $\mu(n)$ denote the Möbius function:

$$\mu(n) = \begin{cases} (-1)^m; & \text{when } n \text{ is squarefree with precisely } m \text{ primefactors,} \\ 0; & \text{otherwise.} \end{cases}$$

(i) Let $\varphi(n)$ denote Euler's φ-function. Prove that for $n \geq 1$ one has $\sum_{d|n} d\mu(n/d) = \varphi(n)$.

(ii) Show that

$$\sum_{d|n} \mu(d) = \begin{cases} 1; & \text{if } n = 1, \\ 0; & \text{otherwise.} \end{cases}$$

(iii) Show that

$$\Phi_n(T) = \prod_{d|n} (T^d - 1)^{\mu(n/d)}$$

for every integer $n \geq 1$.

(3.N) The goal of this exercise is to compute the discriminant of the cyclotomic polynomial $\Phi_m(T)$.

(i) Let ζ denote a primitive m-th root of unity. Prove that

$$\Phi'_m(\zeta) \prod_{d|m, d\neq m} (\zeta^d - 1)^{-\mu(m/d)} = m\zeta^{-1}.$$

(Hint: write $T^m - 1 = \Phi_m(T)G(T)$, differentiate and put $T = \zeta$.)

(ii) Show that

$$\prod_{d|m, d\neq m} (\zeta^d - 1)^{-\mu(m/d)} = \prod_{p|m} (\zeta_p - 1)$$

where $\zeta_p = \zeta^{m/p}$; it is a primitive p-th root of unity in $\mathbf{Q}(\zeta_m)$.

(iii) For $m \geq 3$ show that

$$\mathrm{Disc}(\Phi_m(T)) = (-1)^{\frac{1}{2}\phi(m)} \left(\frac{m}{\prod_{p|m} p^{\frac{1}{p-1}}} \right)^{\phi(m)}.$$

(Hint: use Prop.3.5.)

4. Rings of integers.

In section 2 we have introduced number fields F as finite extensions of $\mathbf{Q}$. Number fields admit natural embeddings Φ into certain finite dimensional $\mathbf{R}$-algebras $F \otimes \mathbf{R}$, which are to be seen as generalizations of the embedding $\mathbf{Q} \hookrightarrow \mathbf{R}$. In this section we generalize the subring of integers $\mathbf{Z}$ of $\mathbf{Q}$: every number field F contains a unique subring O_F of *integral elements.*

Definition 4.1. *Let F be a number field. An element $x \in F$ is called integral if there exists a monic polynomial $f(T) \in \mathbf{Z}[T]$ with $f(x) = 0$. The set of integral elements of F is denoted by O_F.*

It is clear that the integrality of an element does not depend on the field F it contains. An example of an integral element is $i = \sqrt{-1}$, since it is a zero of the monic polynomial $T^2+1 \in \mathbf{Z}[T]$. Every n-th root of unity is integral, since it is a zero of $T^n - 1$. All ordinary integers $n \in \mathbf{Z}$ are integral in this new sense because they are zeroes of the polynomials $T - n$.

Lemma 4.2. *Let F be a number field and let $x \in F$. the following are equivalent*
(i) x is integral.
(ii) The minimum polynomial $f^x_{\text{min}}(T)$ of x over $\mathbf{Q}$ is in $\mathbf{Z}[T]$.
(iii) The characteristic polynomial $f^x_{\text{char}}(T)$ of x over $\mathbf{Q}$ is in $\mathbf{Z}[T]$.
(iv) There exists a finitely generated additive subgroup $M \neq 0$ of F such that $xM \subset M$.

Proof. *(i)⇒(ii)* Let x be integral and let $f(T) \in \mathbf{Z}[T]$ be a monic polynomial such that $f(x) = 0$. The minimum polynomial $f^x_{\text{min}}(T)$ divides $f(T)$ in $\mathbf{Q}[T]$. Since the minimum polynomial of x is monic, we have that $f(T) = g(T)f^x_{\text{min}}(T)$ with $g(T) \in \mathbf{Q}[T]$ monic. By Gauß's Lemma we have that both $f^x_{\text{min}}(T)$ and $g(T)$ are in $\mathbf{Z}[T]$ as required.
(ii)⇒(iii) This is immediate from Prop.3.2*(ii).*
(iii)⇒(iv) Let n be the degree of $f^x_{\text{char}}(T) = \sum_i a_i T^i$. Let M be the additive group generated by $1, x, x^2, \ldots, x^{n-1}$. The finitely generated group M satisfies $xM \subset M$ because $x \cdot x^{n-1} = x^n = -a_{n-1}x^{n-1} - \ldots - a_1 x - a_0 \in M$.
(iv)⇒(i) Let $M \neq 0$ be generated by $e_1, e_2, \ldots, e_m \in F$. Since $xM \subset M$ there exist $a_{ij} \in \mathbf{Z}$ such that

$$xe_i = \sum_{j=1}^{m} a_{ij} e_j \qquad \text{for all } 1 \leq i \leq m,$$

in other words

$$\begin{pmatrix} a_{11} & a_{12} & \ldots & a_{1m} \\ a_{21} & a_{22} & \ldots & a_{2m} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} & a_{m2} & \ldots & a_{mm} \end{pmatrix} \begin{pmatrix} e_1 \\ e_2 \\ \vdots \\ e_m \end{pmatrix} = x \begin{pmatrix} e_1 \\ e_2 \\ \vdots \\ e_m \end{pmatrix}.$$

Since $M \neq 0$, at least one of the e_i is not zero. This implies that the determinant $\det(a_{ij} - x \cdot \text{Id}) = 0$ and that the monic polynomial

$$f(T) = \det(a_{ij} - T \cdot \text{Id}) \in \mathbf{Z}[T]$$

vanishes in x. This proves the lemma.

Proposition 4.3. *The set O_F of integral elements of a number field F is a subring of F.*

Proof. It is easy to see that it suffices to show that $x + y$ and xy are integral whenever x and y are integral. Let therefore $x, y \in F$ be integral. By Lemma 4.2 there exist non-trivial finitely generated subgroups M_1 and M_2 of F, such that $xM_1 \subset M_1$ and $yM_2 \subset M_2$. Let $e_1, e_2, \ldots, e_l$ be generators of M_1 and let $f_1, f_2, \ldots, f_m$ be generators of M_2. Let M_3 be the additive subgroup of F generated by the products $e_i f_j$ for $1 \le i \le l$ and $1 \le j \le m$. It is easy to see that $(x+y)M_3 \subset M_3$ and that $xyM_3 \subset M_3$. This conludes the proof of Prop.4.3

In section 5 we will encounter a more general notion of "integrality": if $R \subset S$ is an extension of commutative rings, then $x \in S$ is said to be *integral over R,* if there exists a monic polynomial $f(T) \in R[T]$ such that $f(x) = 0$. Integers of rings of number fields are, in this sense, integral over $\mathbf{Z}$.

It is, in general, a difficult problem to determine the ring of integers of a given number field. According to Thm.2.2, every number field F can be written as $F = \mathbf{Q}(\alpha)$ for some $\alpha \in F$. A similar statement for rings of integers is, in general false: there exist number fields F such that $O_F \neq \mathbf{Z}[\alpha]$ for any $\alpha \in O_F$. For example, the field $\mathbf{Q}(\sqrt[3]{20})$ has $\mathbf{Z}[\sqrt[3]{20}, \sqrt[3]{50}]$ as a ring of integers and this ring is not of the form $\mathbf{Z}[\alpha]$ for any α (see Exer.9.E). There do, in fact, exist many number fields F for which O_F is not of the form $\mathbf{Z}[\alpha]$ for any α. For instance, it was recently shown by M.-N. Gras [*], that "most" subfields of the cyclotomic fields have this property.

Number fields of degree 2 are called *quadratic number fields.* It is relatively easy to do computations in these fields. The rings of integers of quadratic fields happen to be generated by one element only:

Example 4.4. *Let F be a quadratic number field. Then*
(i) There exists a unique squarefree integer $d \in \mathbf{Z}$ such that $F = \mathbf{Q}(\sqrt{d})$.
(ii) Let d be a squarefree integer. The ring of integers O_F of $F = \mathbf{Q}(\sqrt{d})$ is given by

$$\begin{aligned} O_F &= \mathbf{Z}[\sqrt{d}] && \text{if } d \equiv 2 \text{ or } 3 \pmod 4, \\ &= \mathbf{Z}[\frac{1+\sqrt{d}}{2}] && \text{if } d \equiv 1 \pmod 4. \end{aligned}$$

Proof. *(i)* For any $\alpha \in F - \mathbf{Q}$ one has that $F = \mathbf{Q}(\alpha)$. The number α is a zero of an irreducible polynomial $f(T) \in \mathbf{Q}[T]$ of degree 2 and, it is easy to see that $F = \mathbf{Q}(\sqrt{d})$ where $d \in \mathbf{Q}$ is the discriminant of f. The field $\mathbf{Q}(\sqrt{d})$ does not change if we divide or multiply d by squares of non-zero integers. We conclude that $F = \mathbf{Q}(\sqrt{d})$ for some squarefree integer d. The uniqueness of d will be proved after the proof of part *(ii)*.
(ii) Let $\alpha \in F = \mathbf{Q}(\sqrt{d})$. Then α can be written as $\alpha = a + b\sqrt{d}$ with $a, b \in \mathbf{Q}$. The characteristic polynomial is given by

$$f^x_{\mathrm{char}}(T) = T^2 - 2aT + (a^2 - db^2).$$

Therefore, a necessary and sufficient condition for $\alpha = a + b\sqrt{d}$ to be in O_F, is that $2a \in \mathbf{Z}$ and $a^2 - db^2 \in \mathbf{Z}$.

It follows that either $a \in \mathbf{Z}$ or $a \in \frac{1}{2} + \mathbf{Z}$. We write $b = u/v$ with $u, v \in \mathbf{Z}$, $v \neq 0$ and $\gcd(u, v) = 1$. If $a \in \mathbf{Z}$, then $b^2 d \in \mathbf{Z}$. and we see that v^2 divides $u^2 d$. Since $\gcd(u, v) = 1$, we conclude that v^2 divides d. Since d is squarefree, this implies that $v^2 = 1$ and that $b \in \mathbf{Z}$. If $a \in \frac{1}{2} + \mathbf{Z}$, then $4du^2/v^2 \in \mathbf{Z}$. Since $\gcd(u, v) = 1$ and d is squarefree this implies that v^2 divides 4. Since $a \in \frac{1}{2} + \mathbf{Z}$, we have that $b \notin \mathbf{Z}$ and $v^2 \neq 1$. Therefore $v^2 = 4$ and $b \in \frac{1}{2} + \mathbf{Z}$. Now we have that $a, b \in \frac{1}{2} + \mathbf{Z}$, and this together with the fact that $a^2 - db^2 \in \mathbf{Z}$ is easily seen to imply that $(d-1)/4 \in \mathbf{Z}$.

We conclude, that for $d \equiv 1 \pmod 4$ one has that $O_F = \{a + b\sqrt{d} : a, b \in \mathbf{Z} \text{ or } a, b \in \frac{1}{2} + \mathbf{Z}\}$. Equivalently, $O_F = \mathbf{Z}[\frac{1+\sqrt{d}}{2}]$. In the other cases one has that $O_F = \mathbf{Z}[\sqrt{d}]$.
$(i)^{\mathrm{bis}}$ It remains to finish the proof of *(i)*. Suppose $F = \mathbf{Q}(\sqrt{d})$ for some squarefree integer d. The set

$$\{\mathrm{N}(x) : x \in O_F \text{ with } \mathrm{Tr}(x) = 0\}$$

is equal to $\{a^2 d : \ a \in \mathbf{Z}\}$. This shows that d is determined by O_F and hence by F.

Next we discuss *discriminants* of integral elements $\omega_1, \ldots, \omega_n \in F$.

Proposition 4.5. *Let F be a number field of degree n.*
(i) If $\omega_1, \ldots, \omega_n \in O_F$ then $\Delta(\omega_1, \ldots, \omega_n) \in \mathbf{Z}$.
(ii) Elements $\omega_1, \ldots, \omega_n \in O_F$ generate O_F as an abelian group if and only if $0 \neq \Delta(\omega_1, \ldots, \omega_n) \in \mathbf{Z}$ has minimal absolute value.
(iii) There exists $\omega_1, \ldots, \omega_n$ that generate O_F. For such a basis one has that $O_F \cong \oplus_{i=1}^n \omega_i \mathbf{Z}$. The value of $\Delta(\omega_1, \ldots, \omega_n)$ is independent of the basis and depends only on the ring O_F.

Proof. *(i)* For every i, j the element $\omega_i \omega_j$ is in O_F and hence $\mathrm{Tr}(\omega_i \omega_j) \in \mathbf{Z}$. Therefore $\Delta(\omega_1, \ldots, \omega_n)$ is in $\mathbf{Z}$.
(ii) Suppose $\omega_1, \ldots, \omega_n$ generate O_F as an abelian group. Let $\omega'_1, \ldots, \omega'_n$ be any n elements in O_F. There exist integers $\lambda_{ij} \in \mathbf{Z}$ such that $\omega'_i = \sum_{j=1}^n \lambda_{ij} \omega_j$ for $1 \leq j \leq n$. By Prop.3.4*(iii)* we have that $\Delta(\omega'_1, \ldots, \omega'_n) = \det(\lambda_{ij})^2 \Delta(\omega_1, \ldots, \omega_n)$. Since $\det(\lambda_{ij})^2$ is a positive integer, it follows that the discriminant $\Delta(\omega_1, \ldots, \omega_n)$ is minimal. Conversely, suppose $|\Delta(\omega_1, \ldots, \omega_n)|$ is minimal. If $\omega_1, \ldots, \omega_n$ do not generate the group O_F, there exists $x = \sum_i \lambda_i \omega_i \in O_F$, but not in the group generated by the ω_i. This implies that $\lambda_i \notin \mathbf{Z}$ for some i. After adding a suitable integral multiple of ω_i to x, we may assume that $0 < \lambda_i < 1$. Now we replace ω_i by x in our basis. One checks easily that $|\Delta(\omega_1, \ldots, x, \ldots, \omega_n)| = \lambda_i^2 |\Delta(\omega_1, \ldots, \omega_n)|$ which is integral by *(i)*, non-zero, but strictly smaller than $|\Delta(\omega_1, \ldots, \omega_n)|$. This contradicts the minimality and proves *(ii)*.
(iii) There exists an integral basis $\omega_1, \ldots, \omega_n$ for F over $\mathbf{Q}$. This basis has a non-zero discriminant and by *(i)* an integral one. By *(ii)* it suffices to take such a basis with minimal $|\Delta(\omega_1, \ldots, \omega_n)|$. It follows that $O_F \cong \oplus_{i=1}^n \omega_i \mathbf{Z}$. The discriminant does not depend on the basis by Prop.3.4*(iii)*.

Corollary 4.6. *let F be a number field with ring of integers O_F. Then*
(i) Every ideal $I \neq 0$ of O_F has finite index $[O_F : I]$.
(ii) Every ideal I of O_F is a finitely generated abelian group.
(iii) Every prime ideal $I \neq 0$ of O_F is maximal.

Proof. Let $I \neq 0$ be an ideal of O_F. By Exer.4.D, the ideal I contains an integer $m \in \mathbf{Z}_{>0}$. Therefore $mO_F \subset I$. By Prop.4.5*(iii)*, the additive group of O_F is isomorphic to $\mathbf{Z}^n$, where n is the degree of F. It follows that O_F/I, being a quotient of $O_F/mO_F \cong \mathbf{Z}^n/m\mathbf{Z}^n$ is finite.
(ii) Let I be an ideal of O_F. Since the statement is trivial when $I = 0$, we will assume that $I \neq 0$ and choose an integer $m \in \mathbf{Z}_{>0}$ in I. By *(i)*, the ring O_F/mO_F is finite and therefore the ideal $I \pmod{mO_F}$ can be generated, as an abelian group, by, say, $\alpha_1, \ldots, \alpha_k$. It follows easily that the ideal I is then generated by $\alpha_1, \ldots, \alpha_k$ and $m\omega_1, \ldots, m\omega_n$, where the ω_i are a $\mathbf{Z}$-basis for the ring of integers O_F.
(iii) Let $I \neq 0$ be a prime ideal of O_F. By *(i)*, the ring O_F/I is a finite domain. Since finite domains are fields, it follows that I is a maximal ideal.

As a consequence of Cor.4.6, the following definition is now justified:

Definition. *Let F be a number field and let $I \neq 0$ be an ideal of the ring of integers of O_F of F. We define the norm $\mathrm{N}(I)$ of the ideal I by*

$$\mathrm{N}(I) = [O_F : I] = \#(O_F/I).$$

Another application of Prop.4.5 is the following. Let F be a number field of degree n and let $\omega_1, \ldots, \omega_n \in F$. By Prop.3.4*(iii)* the discriminant $\Delta(\omega_1, \omega_2, \ldots, \omega_n)$ does not depend on $\omega_1, \ldots, \omega_n$, but merely on the additive group these numbers generate. This justifies the following definition.

Definition. Let F be a number field of degree n. the *discriminant* of F is the discriminant $\Delta(\omega_1, \omega_2, \ldots, \omega_n)$ of an integral basis $\omega_1, \omega_2, \ldots, \omega_n$ of O_F.

Since 1 is a **Z**-basis for **Z**, we see that the discriminant of **Q** is 1. As an example we calculate the discriminant of a quadratic field.

Example 4.7. Let F be a quadratic field. By Example 4.4 there exists a unique squarefree integer d such that $F = \mathbf{Q}(\sqrt{d})$. If $d \equiv 2$ or 3 (mod 4), the ring of integers of F is $\mathbf{Z}[\sqrt{d}]$. We take $\{1, \sqrt{d}\}$ as a **Z**-base of O_F. Then

$$\Delta_{\mathbf{Q}(\sqrt{d})} = \det\begin{pmatrix} \mathrm{Tr}(1\cdot 1) & \mathrm{Tr}(1\cdot\sqrt{d}) \\ \mathrm{Tr}(1\cdot\sqrt{d}) & \mathrm{Tr}(\sqrt{d}\cdot\sqrt{d}) \end{pmatrix} = \det\begin{pmatrix} 2 & 0 \\ 0 & 2d \end{pmatrix} = 4d.$$

If $d \equiv 1$ (mod 4), the ring of integers of F is $\mathbf{Z}[\frac{1+\sqrt{d}}{2}]$. We take $\{1, \frac{1+\sqrt{d}}{2}\}$ as a **Z**-base of O_F. Then

$$\Delta_{\mathbf{Q}(\sqrt{d})} = \det\begin{pmatrix} \mathrm{Tr}(1\cdot 1) & \mathrm{Tr}(1\cdot\frac{1+\sqrt{d}}{2}) \\ \mathrm{Tr}(1\cdot\frac{1+\sqrt{d}}{2}) & \mathrm{Tr}(\frac{1+\sqrt{d}}{2}\cdot\frac{1+\sqrt{d}}{2}) \end{pmatrix} = \det\begin{pmatrix} 2 & 1 \\ 1 & \frac{d+1}{2} \end{pmatrix} = d.$$

For $d = -4$ we find that the ring of integers of $\mathbf{Q}(i)$ is the well known ring $\mathbf{Z}[i]$ of Gaussian integers. For $d = -3$ we find the ring $\mathbf{Z}[(1+\sqrt{-3})/2]$ of *Eisenstein* integers. The latter ring is isomorphic to the ring $\mathbf{Z}[\zeta_3]$ where ζ_3 denotes a primitic root of unity.

In general, it is rather difficult to calculate the discriminant and the ring of integers of a number field. We will come back to this problem in section 9. The following proposition often comes in handy.

Proposition 4.8. *Let F be a number field of degree n. Suppose $\omega_1, \omega_2, \ldots, \omega_n \in O_F$ have the property that $\Delta(\omega_1, \omega_2, \ldots, \omega_n)$ is a squarefree integer. Then $O_F = \sum_i \omega_i \mathbf{Z}$. In particular, if there exists $\alpha \in O_F$ such that the discriminant of $f^{\alpha}_{\min}(T)$ is squarefree, then $O_F = \mathbf{Z}[\alpha]$ and $\Delta_F = \Delta(1, \alpha, \ldots, \alpha^{n-1}) = \mathrm{Disc}(f^{\alpha}_{\min})$.*

Proof. It follows from Prop.3.4*(iii)* that $\Delta(\omega_1, \omega_2, \ldots, \omega_n) = \det(M)^2\Delta_F$, where $M \in \mathrm{GL}_2(\mathbf{Z})$ is the matrix expressing the ω_i in terms of a **Z**-base of O_F. Since $\det(M)^2$ is the square of an integer, part *(i)* follows.

If we take the powers $1, \alpha, \alpha^2, \ldots, \alpha^{n-1}$ for $\omega_1, \omega_2, \ldots, \omega_n$, the result in *(ii)* follows from *(i)* and the fact, proved in Prop.3.5, that $\Delta(1, \alpha, \ldots, \alpha^{n-1}) = \mathrm{Disc}(f^{\alpha}_{\min})$.

Example. Let α be a zero of the polynomial $f(T) = T^3 - T - 1 \in \mathbf{Z}[T]$. Since $f(T)$ is irreducible modulo 2, it is irreducible over **Q**. Put $F = \mathbf{Q}(\alpha)$. By Prop.3.2*(ii)*, the characteristic polynomial of α is also equal to $f(T)$. In order to calculate the discriminant of f, one can employ various methods. See Exer.3.K for an efficient algorithm involving resultants of polynomials. Here we just use the definition of the discriminant. Let's calculate

$$\Delta(1, \alpha, \alpha^2) = \begin{pmatrix} \mathrm{Tr}(1) & \mathrm{Tr}(\alpha) & \mathrm{Tr}(\alpha^2) \\ \mathrm{Tr}(\alpha) & \mathrm{Tr}(\alpha^2) & \mathrm{Tr}(\alpha^3) \\ \mathrm{Tr}(\alpha^2) & \mathrm{Tr}(\alpha^3) & \mathrm{Tr}(\alpha^4) \end{pmatrix}.$$

The trace of 1 is 3. The trace of α is equal to -1 times the coefficient at T^2 of $F(T)$ and hence is 0. In general, the traces $\mathrm{Tr}(\alpha^k)$ are equal to the power sums $p_k = \phi_1(\alpha)^k + \phi_2(\alpha)^k + \phi_3(\alpha)^k$ for $k \geq 0$. Newton's formulas (see Exer.3.I) relate these sums to the coefficients s_k of the minimum polynomial of α.

In the notation of Exer.3.I, we have that $\mathrm{Tr}(\alpha^2) = p_2 = -2s_2 + p_1 s_1 = -2\cdot(-1) + 0 = 2$. We obtain the other values of $\mathrm{Tr}(\alpha^k)$ by using the additivity of the trace: since $\alpha^3 = \alpha + 1$, we have $\mathrm{Tr}(\alpha^3) = \mathrm{Tr}(\alpha + 1) = 0 + 3 = 3$ and $\mathrm{Tr}(\alpha^4) = \mathrm{Tr}(\alpha^2 + \alpha) = 2 + 0 = 2$. Therefore

$$\Delta(1, \alpha, \alpha^2) = \begin{pmatrix} 3 & 0 & 2 \\ 0 & 2 & 3 \\ 2 & 3 & 2 \end{pmatrix} = -23.$$

By Prop.4.8 we can now conclude that the ring of integers of $\mathbf{Q}(\alpha)$ is $\mathbf{Z}[\alpha]$ and that the discriminant $\Delta_{\mathbf{Q}(\alpha)}$ is equal to -23.

(4.A) Let F be a number field and let $\alpha \in F$. Show that there exist an integer $0 \neq m \in \mathbf{Z}$ such that $m\alpha \in O_F$.

(4.B) Show that for every number field F there exists an *integral* element $\alpha \in O_F$ such that $F = \mathbf{Q}(\alpha)$.

(4.C) Let F be a number field. Show that the field of fractions of O_F is F.

(4.D) Let F be a number field. Show that every ideal $I \neq 0$ of O_F contains a non-zero integer $m \in \mathbf{Z}$.

(4.E) Let F be a number field and let $\alpha \in O_F$. Show that $\mathrm{N}(\alpha) = \pm 1$ if and only if α is a unit of the ring O_F.

(4.F) Let $F \subset K$ be an extension of number fields. Show that $O_K \cap F = O_F$.

(4.G) Let F be a number field. Let r_1 be the number of distinct embeddings $F \hookrightarrow \mathbf{R}$ and let $2r_2$ be the number of remaining homomorphisms $F \hookrightarrow \mathbf{C}$. Show that the sign of Δ_F is $(-1)^{r_2}$.

(4.H) Determine the integers and the discriminant of the number field $\mathbf{Q}(\alpha)$ where α is given by $\alpha^3+\alpha-1=0$.

(4.I) Let F and K be two quadratic number fields. Show that if $\Delta_F = \Delta_K$, then $F \cong K$.

(4.J) let d be a negative squarefree integer. Determine the unit group of the ring of integers of the field $\mathbf{Q}(\sqrt{d})$.

(4.K) Let R be a commutative ring. An R-*algebra* A is a ring together with a ring homomorphism $R \longrightarrow A$. Alternatively, A is a ring provided with a multiplication $R \times A \longrightarrow A$ by elements of R that satisfies

$$\begin{aligned}
\lambda(x+y) &= \lambda x + \lambda y,\\
(\lambda+\mu)x &= \lambda x + \mu x,\\
(\lambda\mu)x &= \lambda(\mu x),\\
1x &= x,
\end{aligned}$$

for $\lambda, \mu \in R$ and $x, y \in A$.

(i) Show that the two definitions of an R-algebra are equivalent.

(ii) If R is a field, show that a K-algebra is a vector space over K.

(iii) Show that every ring is a $\mathbf{Z}$-algebra.

(4.L) Let K be a field.

(i) Let$A$ be a finite dimensional K-algebra (see Exer.4.K). Show: A is a domain if and only if it is a field.

(ii) Show that every prime ideal $I \neq 0$ of $K[X]$ is also maximal.

(4.M) Let $M \in \mathrm{GL}_n(\mathbf{Z})$ be an invertible matrix. Show that $\det(M) = \pm 1$.

(4.N) Let $n \geq 1$ be an integer and let ζ_n denote a primitive n-th root of unity. Show that $\zeta_n - 1$ is a unit of the ring of integers if and only if n is not the power of a prime. (Hint: substitute $T = 1$ in $(T^n-1)/(T-1) = \prod_{d|n, d\neq 1} \Phi_d(T)$ and use induction)

(4.O)*(Stickelberger 1923) Let F be a number field of degree n. Let $\{\omega_1, \omega_2, \ldots, \omega_n\}$ be a $\mathbf{Z}$-basis for the ring of integers of F. Let $\phi_i : F \hookrightarrow \mathbf{C}$ be the embeddings of F into $\mathbf{C}$. By S_n we denote the symmetric group on n symbols and by A_n the normal subgroup of *even* permutations. We define $\Delta^+ = \sum_{\tau\in A_n} \prod_{i=1}^n \phi_i(\omega_{\tau(i)})$ and $\Delta^- = \sum_{\tau\in S_n - A_n} \prod_{i=1}^n \phi_i(\omega_{\tau(i)})$. Prove, using Galois theory, that $\Delta^+ + \Delta^-$ e $\Delta^+\Delta^-$ are in $\mathbf{Z}$. Conclude that $\Delta_F = (\Delta^+ + \Delta^-)^2 - 4\Delta^+\Delta^- \equiv 0$ or $1 \pmod 4$.

5. Dedekind rings.

In this section we introduce Dedekind rings (Richard Dedekind, German mathematician 1831–1916). Rings of integers of number fields are important examples of Dedekind rings. We will show that the *fractional ideals* of a Dedekind ring admit unique factorization into prime ideals.

Definition. *A commutative ring R is called Noetherian if every sequence of ideals of R*

$$I_1 \subset I_2 \subset \ldots \subset I_i \subset \ldots$$

stabilizes, i.e. if there exists an index i_0 such that $I_i = I_{i_0}$ for all $i \geq i_0$.

Lemma 5.1. *Let R be a commutative ring. The following are equivalent:*
(i) Every R-ideal is finitely generated.
(ii) R is Noetherian.
(iii) Every non-empty collection Ω of R-ideals contains a maximal element i.e. an ideal I such that no ideal $J \in \Omega$ contains I properly.

Proof. *(i) $\Rightarrow$ (ii)* Let $I_1 \subset I_2 \subset \ldots \subset I_i \subset \ldots$ be a sequence of ideals of R. Suppose the union $I = \cup_{i \geq 1} I_i$ is generated by $\alpha_1, \ldots, \alpha_m$. For every α_k there exists an index i such that $\alpha_k \in I_i$. Writing N for the maximum of the indices i, we see that $\alpha_k \in I_N$ for all k. Therefore $I = I_N$ and the sequences stabilizes.

(ii) $\Rightarrow$ (iii) Suppose Ω is a non-empty collection without maximal elements. Pick $I = I_1 \in \Omega$. Since I_1 is not maximal, there exists an ideal $I_2 \in \Omega$ such that $I_1 \subset_{\neq} I_2$. Similarly, there exists an ideal $I_3 \in \Omega$ such that $I_2 \subset_{\neq} I_3$. In this way we obtain a sequence $I_1 \subset I_2 \subset \ldots \subset I_i \subset \ldots$ that does not stabilize. This contradicts the fact that R is Noetherian

(iii) $\Rightarrow$ (i) Let I be an ideal of R and let Ω be the collection of ideals $J \subset I$ which are finitely generated. Since $(0) \in \Omega$, we see that $\Omega \neq \emptyset$ and hence contains a maximal element J. If $J \neq I$, we pick $x \in I - J$ and we see that the ideal $J + (x)$ properly contains J and is in Ω. This contradicts the maximality of J. We conclude that $I = J$ and the proof of the lemma is complete.

Almost all rings that appear in mathematics are Noetherian (Emmy Noether, German mathematician 1882-1935). Every principal ideal ring is clearly Noetherian, so fields and the ring $\mathbf{Z}$ are Noetherian rings. According to Exer.5.A., the quotient ring R/I of a Noetherian ring R is again Noetherian. Finite products of Noetherian rings are Noetherian. The famous "Basissatz" [*] of Hilbert (David Hilbert, German mathematician 1862–1943) affirms that the polynomial ring $R[T]$ is Noetherian whenever R is.

Non-Noetherian rings are often very large and sometimes pathological. For instance, the ring $R[X_1, X_1, X_3, \ldots]$ of polynomials in countably many variables over a commutative ring R is not Noetherian.

Definition. *Let $R \subset S$ be an extension of commutative rings. An element $x \in S$ is called integral over R, if there exists a monic polynomial $f(T) \in R[T]$ with $f(x) = 0$. A domain R is called integrally closed if every integral element in the field of fractions of R is contained in R.*

Using this terminology, one can say that the integers of number fields are, in fact, integers *over* $\mathbf{Z}$. Let F be a number field. We will see in section 6 that rings of integers are integrally closed. Other examples of integrally closed rings are provided by Exer.5.D: every unique factorization domain is integrally closed.

The ring $\mathbf{Z}[2i]$ is *not* integrally closed: the element i is contained in its quotient field $\mathbf{Q}(i)$ but it is integral over $\mathbf{Z}$ and hence over $\mathbf{Z}[i]$.

Definition. *Let R be a commutative ring. The height of a prime ideal $P = P_0$ of R is the supremum of the integers n for which there exists a chain*

$$P_0 \subset P_1 \subset P_2 \subset \ldots \subset P_n \subset R$$

of distinct prime ideals in R. The Krull dimension of a ring is the supremum of the heights of the prime ideals of R.

For example, a field has Krull dimension 0 and the ring $\mathbf{Z}$ has dimension 1 (Wolfgang Krull, German mathematician 1899-1970). In general, principal ideal rings that are not fields, have dimension 1. It is easy to show that for every field K, the ring of polynomials $K[X_1, \ldots, X_n]$ has dimension at least n. The notion of dimension has its origins in algebraic geometry: the ring of regular functions on an affine variety of dimension n over a field K has Krull dimension equal to n.

Definition. *A Dedekind ring is a Noetherian, integrally closed domain of dimension at most 1.*

By Exer.5.H, every principal ideal domain R is a Dedekind ring. Its dimension is 0 if R is a field and 1 otherwise. Not all Dedekind rings are principal ideal domains. In the next section we will prove that rings of integers of number fields are Dedekind rings.

Definition. *Let R be a Dedekind ring with field of fractions K. A fractional ideal of R (or K) is an additive subgroup I of K for which there exists $\alpha \in K$ such that αI is a non-zero ideal of R.*

Proposition 5.2. *Let R be a Dedekind ring with field of fractions K. Then*
- *(i) Every non-zero ideal of R is a fractional ideal. A fractional ideal contained in R is an ideal of R.*
- *(ii) If I and J are fractional ideals, then $IJ = \{\sum_i^{<\infty} \alpha_i\beta_i : \alpha_i \in I, \beta_i \in J\}$ is a fractional ideal.*
- *(iii) For every $\alpha \in K^*$ the set $(\alpha) = \alpha R = \{\alpha r : r \in R\}$ is a fractional ideal. Such a fractional ideal is called a principal fractional ideal.*
- *(iv) For every fractional ideal I, the set $I^{-1} = \{\alpha \in K : \alpha I \subset R\}$ is a fractional ideal.*

Proof. *(i)* The first statement is obvious. If $I \subset R$ is a fractional ideal, then αI is an ideal for some $\alpha \in K^*$. It is straightforward to verify that this implies that already I is an ideal.
(ii) If $\alpha I \subset R$ and $\beta J \in R$ then $\alpha\beta IJ \subset R$.
(iii) This follows from the fact that $\alpha^{-1}(\alpha) = R$.
(iv) Let $\alpha \neq 0$ be any element in I. Then $\alpha I^{-1} \subset R$ is an ideal. This proves the proposition.

Theorem 5.3. *Let R be a Dedekind ring and let $Id(R)$ be the set of fractional ideals of R. Then*
- *(i) The set $Id(R)$ is, with the multiplication of Prop.5.2(ii), an abelian group. The neutral element is R and the inverse of a fractional ideal I is I^{-1}.*
- *(ii) We have*

$$Id(R) \cong \bigoplus_{\mathfrak{p}} \mathbf{Z}$$

where $\mathfrak{p}$ runs over the non-zero prime ideals of R. More precisely: every fractional ideal can be written as a finite product of prime ideals (with exponents in $\mathbf{Z}$) in a unique way.

Proof. Since the theorem is trivial when R is a field, we will suppose that R is not a field. We suppose, in other words, that R has Krull dimension 1.
(i) We observe that the multiplication defined in Prop.5.2*(ii)* is associative and commutative since the multiplication in R is. It is very easy to verify that $RI = I$ for every fractional ideal I. In step *(4)* of the proof of part *(ii)* we show that for every fractional ideal I, its inverse is given by I^{-1}.

(ii) The proof is given in six steps:
(1) Every non-zero ideal of R contains a product of non-zero prime ideals of R.

Suppose that there exists an ideal that does not contain a product of non-zero prime ideals. So, the collection Ω of such ideals is not empty. Since R is Noetherian, we can, by Lemma 5.1 find an ideal $I \in \Omega$ such that every ideal J that properly contains I is not in Ω. Clearly I is not prime itself. Therefore there exist $x, y \notin I$ such that $xy \in I$. The ideals $I + (x)$ and $I + (y)$ are strictly larger than I and hence contain a product of non-zero prime ideals. Say $\mathfrak{p}_1 \cdot \ldots \cdot \mathfrak{p}_r \subset I + (x)$ and $\mathfrak{p}'_1 \cdot \ldots \cdot \mathfrak{p}'_s \subset I + (y)$. Now we have $\mathfrak{p}_1 \cdot \ldots \cdot \mathfrak{p}_r \mathfrak{p}'_1 \cdot \ldots \cdot \mathfrak{p}'_s \subset (I + (x))(I + (y)) \subset I$ contradicting the fact that $I \in \Omega$.

(2) For every ideal I with $0 \neq I \neq R$ one has that $R \subset_{\neq} I^{-1}$.

Let M be a maximal ideal with $I \subset M \subset R$. Since $I^{-1} \supset M^{-1} \supset R^{-1} = R$ it suffices to prove the statement for $I = M$ a maximal ideal. Let $0 \neq a \in M$. By part *(i)* there exist prime ideals $\mathfrak{p}_i$ such that $\mathfrak{p}_1 \cdot \ldots \cdot \mathfrak{p}_r \subset (a)$. Let us assume that the number of prime ideals r in this product, is minimal. Since M itself is a prime ideal, one of the primes $\mathfrak{p}_i$, say $\mathfrak{p}_1$, is contained in M. Sinds R has Krull dimension 1, we conclude that $\mathfrak{p}_1 = M$. By minimality of r we see that $\mathfrak{p}_2 \cdot \ldots \cdot \mathfrak{p}_r \not\subset (a)$ and we can pick $b \in \mathfrak{p}_2 \cdot \ldots \cdot \mathfrak{p}_r$ but $b \notin (a)$. So, $b/a \notin R$, but $b/a \in M^{-1}$ because $bM \subset \mathfrak{p}_2 \cdot \ldots \cdot \mathfrak{p}_r M \subset (a)$. This proves *(2).*

(3) $MM^{-1} = R$ for every maximal ideal M of R.

Since $R \subset M^{-1}$ we have that $M \subset MM^{-1} \subset R$. If one would have that $M = MM^{-1}$ then every $x \in M^{-1}$ satisfies $xM \subset M$. Since M is finitely generated over R, it follows from Exer.5.E that x is integral over R. Since R is integrally closed this would imply that $M^{-1} \subset R$ contradicting the conclusion of step *(2).* We conclude that $M \neq MM^{-1}$ and hence that $MM^{-1} = R$ as required.

(4) $II^{-1} = R$ for every ideal $I \neq 0$ of R.

Suppose I is an ideal with $II^{-1} \neq R$. Suppose, moreover, that I is maximal with respect to this property. Let M be a maximal ideal containg I. Since $R \subset M^{-1}$, we have that $I \subset IM^{-1} \subset MM^{-1} \subset R$. We see that IM^{-1} is an ideal of R. If we would have that $IM^{-1} = I$, then, by Exer.5.E, M^{-1} would be integral, which is impossible. We conclude that IM^{-1} is strictly larger than I. Therefore $IM^{-1}(IM^{-1})^{-1} = R$. This implies that $M^{-1}(IM^{-1})^{-1} \subset I^{-1}$. Finally: $R = IM^{-1}(IM^{-1})^{-1} \subset II^{-1} \subset R$ whence $II^{-1} = R$ contradicting the maximality of I. This proves *(4).*

(5) Every fractional ideal is a product of prime ideals with exponents in $\mathbf{Z}$.

Suppose $I \subset R$ is an ideal which cannot be written as a product of prime ideals. Suppose that I is maximal with respect to this property. Let M be a maximal ideal $I \subset M \subset R$. Then $I \subset IM^{-1} \subset R$. Since $M^{-1} \not\subset R$ we see that $IM^{-1} \neq I$ and hence that IM^{-1} is strictly larger than I. So IM^{-1} is a product of primes and therefore, multiplying by M, so is I. This contradiction shows that every integral ideal I of R is a product of prime ideals. By definition, every fractional ideal is of the form $\alpha^{-1}I$ where $\alpha \in R$ and I is an ideal of R. We conclude that every fractional ideal is a product of prime ideals, with exponents in $\mathbf{Z}$.

(6) The decomposition into prime ideals is unique.

Suppose $\prod \mathfrak{p}^{n_\mathfrak{p}} = R$ with $n_\mathfrak{p} \neq 0$. This gives us a relation $I\mathfrak{p} = J$ where I and J are ideals in R and J is a product of primes different from $\mathfrak{p}$. However, since $\mathfrak{p}$ is prime we have that $J \subset \mathfrak{p}$ and therefore $\mathfrak{p}$ contains a non-zero prime ideal different from itself. This is impossible and the proof of Theorem 5.3 is now complete.

It is easy to see that the ideals of R are precisely the fractional ideals that have a prime ideal decomposition $\prod \mathfrak{p}^{n_\mathfrak{p}}$ with non-negative exponents. When R is a Dedekind ring and $\mathfrak{p}$ is a non-zero prime ideal in R, we denote for every fractional ideal I by

$$\mathrm{ord}_\mathfrak{p}(I)$$

the exponent $n_\mathfrak{p}$ of $\mathfrak{p}$ in the prime decomposition of I. For $x \in F^*$ we denote by

$$\mathrm{ord}_\mathfrak{p}(x)$$

the exponent $\mathrm{ord}_\mathfrak{p}((x))$ occuring in the prime decomposition of the principal fractional ideal (x).

The following corollary is a generalization of the important Lemma 1.2 used in the introduction.

Corollary 5.4. *Let R be a Dedekind domain, let $N \in \mathbf{Z}_{>0}$ and let $I_1, I_2, \ldots, I_m$ be non-zero ideals of R which are mutually coprime i.e. for which $I_i + I_j = R$ whenever $i \neq j$. If*

$$I_1 \cdot I_2 \cdot \ldots \cdot I_m = J^N$$

for some ideal J of R, then there exists for every $1 \leq i \leq m$, an ideal J_i such that $J_i^N = I_i$.

Proof. By Theorem 5.3 we can decompose the ideals I_i into a product of distinct prime ideals $\mathfrak{p}_{i,j}$:

$$I_i = \prod_{j=1}^{n_i} \mathfrak{p}_{i,j}^{e_{i,j}}.$$

We have that

$$I_1 \cdot I_2 \cdot \ldots \cdot I_m = \prod_{i=1}^{m} \prod_{j=1}^{n_i} \mathfrak{p}_{i,j}^{e_{i,j}} = J^N$$

Since the ideals I_i are mutually coprime, all the prime ideals ideals $\mathfrak{p}_{i,j}$ are distinct. By Theorem 5.3, the group of fractional ideals is a sum of copies of $\mathbf{Z}$. We conclude that all the exponents $e_{i,j}$ are divisible by N and hence that the ideals I_i are N-th powers of ideals, as required.

Definition. Let R be a Dedekind ring with field of fractions K. We define a map

$$\theta : K^* \longrightarrow \mathrm{Id}(R)$$

by $\theta(\alpha) = (\alpha)$. The image of θ is the subgroup $PId(R)$ of principal fractional ideals and the kernel of θ is precisely the group of units R^* of R. The cokernel of θ is called the *class group* of R:

$$Cl(R) = \mathrm{cok}(\theta) = Id(R)/PId(R).$$

In other words, there is an exact sequence

$$0 \longrightarrow R^* \longrightarrow F^* \xrightarrow{\theta} Id(R) \longrightarrow Cl(R) \longrightarrow 0.$$

The class group of a Dedekind ring measures how far R is from being a principal ideal domain. Fields and, more generally, principal ideal domains have trivial class groups. The analogue of the class group in algebraic geometry is the *Picard group.* For a smooth algebraic curve this is the divisor group modulo its subgroup of principal divisors [*].

One can show [*], that *every* abelian group is isomorphic to the class group $Cl(R)$ of some Dedekind domain R. In section 10 we show that the class groups of rings of integers of number fields are always *finite.*

Proposition 5.5. *let R be a Dedekind ring. The following are equivalent:*
(i) The class group $Cl(R)$ is trivial.
(ii) Every fractional ideal of R is principal.
(iii) R is a principal ideal domain.
(iv) R is a unique factorization domain.

Proof. The implications *(i)* $\Rightarrow$ *(ii)* $\Rightarrow$ *(iii)* $\Rightarrow$ *(iv)* are easy or standard. To prove that *(iv)* $\Rightarrow$ *(i)* we first note that by Theorem 5.3 it suffices to show that every *prime* ideal is principal. Let, therefore, $\mathfrak{p}$ be a non-zero prime ideal and let $0 \neq x \in \mathfrak{p}$. Writing x as a product of irreducible elements and observing that $\mathfrak{p}$ is prime, we see that $\mathfrak{p}$ contains an irreducible element π. The ideal (π) is a prime ideal. Since the ring R is a Dedekind ring, it has Krull dimension 1 and we conclude that $\mathfrak{p} = (\pi)$ and hence that $\mathfrak{p}$ is principal, as required.

This completes our discussion of Dedekind rings *in general*. In the next section we apply our results to a special class of Dedekind rings: rings of integers of number fields.

(5.A) If R is a Noetherian ring, then, for every ideal I of R, the ring R/I is also Noetherian.

(5.B) Let R be a Noetherian ring. Show, without invoking the Axiom of Choice, that every ideal is contained in a maximal ideal.

(5.C) Is the ring $C^\infty(\mathbf{R}) = \{f : \mathbf{R} \to \mathbf{R} : f \text{ is a } C^\infty\text{-function}\}$ Noetherian?

(5.D) Show that every unique factorization domain is integrally closed.

(5.E) Let R be an integrally closed domain and let $f \in R[X]$ be a monic irreducible polynomial. Show that $f(T)$ is irreducible over K, the field of fractions of R.

(5.F) Show: let $R \subset S$ be an extension of commutative rings. Then an element $x \in S$ is integral over R if and only if there exists an R-module M of finite type such that $xM \subset M$ (Hint: Copy the proof of Lemma 4.2).

(5.G) Consider the properties "Noetherian", "integrally closed" and "of Krull dimension 1" that characterize Dedekind domains. Give examples of rings that have two of these properties, but not the third.

(5.H) Prove that every principal ideal domain is a Dedekind domain.

(5.I) Let I and J be two fractional ideals of a Dedekind domain.
- (i) Show that $I \cap J$ and $I + J$ are fractional ideals.
- (ii) Show that $I^{-1} + J^{-1} = (I \cap J)^{-1}$ and that $I^{-1} \cap J^{-1} = (I + J)^{-1}$.
- (iii) Show that $I \subset J$ if and only if $J^{-1} \subset I^{-1}$.

(5.J) Let R be a Dedekind ring. Show:
- (i) for $\alpha \in R$ and a fractional ideal I one has that $\alpha I \subset I$.
- (ii) every fractional ideal I is of the form $m^{-1}J$ where $m \in \mathbf{Z}$ and J is an ideal of R.
- (ii) if $I = (x)$ is a principal fractional ideal, then $I^{-1} = (x^{-1})$.

(5.K) Let I and J be fractional ideals of a Dedekind domain R. Let $n_\mathfrak{p}$ and $m_\mathfrak{p}$ be the exponents in their respective prime decompositions. Show that $I \subset J \Leftrightarrow n_\mathfrak{p} \geq m_\mathfrak{p}$ for all primes $\mathfrak{p}$.

(5.L) Let R be a Dedekind ring with only finitely many prime ideals. Show that R is a principal ideal ring. (Hint: the Chinese Remainder Theorem)

(5.M) Show that in a Dedekind ring every ideal can be generated by at most two elements.

(5.N) Let R be a Dedekind ring. Show that every class in $Cl(R)$ contains an ideal of R.

(5.O) Let R be a Dedekind ring. Let S be a set of prime ideals of R. Let R' be the subset of the quotient field K of R defined by

$$R' = \{x \in K^* : (x) = \prod_{\mathfrak{p}} \mathfrak{p}^{n_\mathfrak{p}} \quad \text{with } n_\mathfrak{p} \geq 0 \text{ for all } \mathfrak{p} \notin S\} \cup \{0\}.$$

Show that R' is a Dedekind ring.

(5.P) Let R be a Dedekind ring and let $\mathfrak{p}$ and $\mathfrak{p}'$ be two different non-zero prime ideals of R. Then $\mathfrak{p} + \mathfrak{p}' = R$.

(5.Q) Let $R \hookrightarrow S$ be an extension of Dedekind domains. Show that, if S is an R-module of finite type, the canonical map $Id(R) \longrightarrow Id(S)$ is injective.

6. The Dedekind ζ-function.

In this section we prove that the ring of integers of a number field is a Dedekind ring. We introduce the Dedekind ζ-function associated to a number field.

Proposition 6.1. *Let F be a number field. Then the ring of integers O_F of F is a Dedekind ring.*

Proof. By Cor.4.6*(ii)*, every ideal is a finitely generated abelian group. From Lemma 5.1 we conclude that O_F is a Noetherian ring. By Cor.4.6*(iii)* every non-zero prime ideal is maximal. This implies that the Krull dimension of O_F is at most 1. If $x \in F$ is integral over O_F, it satisfies an equation of the form $x^m + a_{m-1}x^{m-1} + \ldots + a_1 x + a_0 = 0$, where the coefficients a_i are in O_F. This implies that $xO_F \subset O_F$ and since O_F is a finitely generated additive group we have, by Lemma 4.2, that $x \in O_F$. This shows that O_F is integraly closed and proves the proposition.

Proposition 6.2. *Let F be a number field and let I, J be non-zero ideals of its ring of integers O_F. Then*

$$N(IJ) = N(I)N(J).$$

Proof. By Theorem 5.3 it suffices to prove that

$$N(IM) = N(I)N(M).$$

for a non-zero prime ideal M of O_F. From the exact sequence

$$0 \longrightarrow I/IM \longrightarrow R/IM \longrightarrow R/I \longrightarrow 0$$

we deduce that all we have to show, is that $\#(I/IM) = \#(R/M)$. The group I/IM is a vector space over the field R/M. Since, by Theorem 5.3 one has $MI \neq I$, it is a non-trivial vector space. Let W be a subspace of I/IM. The reciprocal image of W in R is an ideal J with $IM \subset J \subset I$. This implies that $M \subset JI^{-1} \subset R$ and hence that $JI^{-1} = M$ or $JI^{-1} = R$. In other words $J = IM$ or $J = I$ and hence $W = 0$ or $W = I/IM$. So, apparently the vector space I/IM has only trivial subspaces. It follows that its dimension is one. This proves the proposition.

Definizione. *Let F be a number field and let I be a fractional ideal of F. Suppose $I = JK^{-1}$, where J and K are two ideals of O_F. We define the norm $N(I)$ of I by*

$$N(I) = N(J)/N(K).$$

There are many ways to write a fractional ideal I as the quotient of two ideals J and K. By Prop.6.2. the norm $N(I)$ does not depend on this. The next proposition is an application of the multiplicativity of the norm map.

Proposition 6.3. *Let F be a number field of degree n.*

(i) *For every ideal $\mathfrak{p}$ of O_F there exists a prime number p such that $\mathfrak{p}$ divides p. The norm of $\mathfrak{p}$ is a power of p.*

(ii) *Let $\mathfrak{p}_1^{e_1} \cdot \ldots \cdot \mathfrak{p}_g^{e_g}$ be the prime decomposition of the ideal generated by p in O_F. Then*

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

where for every i the number f_i is defined by $N(\mathfrak{p}_i) = p^{f_i}$.

(iii) *For every prime number p there are at most n distinct prime ideals of O_F dividing p.*

(iv) *There are only finitely many ideals with bounded norm.*

Proof. *(i)* Let $\mathfrak{p}$ be a prime ideal. By Exer.4.A there exists an integer $m \neq 0$ in $\mathfrak{p}$. Since $\mathfrak{p}$ is a prime ideal, it follows that $\mathfrak{p}$ contains a prime number p. So $\mathfrak{p}$ divides p and by Prop.6.2 the norm $N(\mathfrak{p})$ divides $N(p) = p^n$.
(ii) This follows at once from the multiplicativity of the norm, by taking the norm of the prime decomposition of (p) in O_F.
(iii) This is immediate from *(ii)*.
(iv) This follows from Theorem 5.3 and *(iii)*.

The number f_i is called the *inertia index* and e_i is called the *ramification index* of the prime ideal $\mathfrak{p}_i$. We will see in section 9 that for almost all $\mathfrak{p}_i$, the index e_i is equal to 1. The prime ideals $\mathfrak{p}_i$ for which $e_i > 1$ are called *ramified.*

If for a prime p and a number field F of degree n one has that $e_i = f_i = 1$ for all g primes $\mathfrak{p}_i$ that divide p we say that p *is totally split in* F. In this case there are n different prime ideals dividing p. They all have norm p. If $g = 1$, there is only one prime ideal $\mathfrak{p}_1$ dividing p. If, in this case $f_1 = 1$, then $e_1 = n$ and we say that p is *totally ramified* in F over $\mathbf{Q}$. If, on the other hand, $e_1 = 1$ and $f_1 = n$, we say that the prime p *"remains prime"* or is *inert* in F; in this case the ideal (p) is also a prime ideal in O_F.

Example 6.5. Let $F = \mathbf{Q}(\sqrt{-5})$. By Example 4.4 the ring of integers of F is equal to $\mathbf{Z}[\sqrt{-5}]$. We will factor some small prime numbers into prime ideals.

First we study the prime 2: since $O_F/(2) = \mathbf{Z}[T]/(2, T^2+5) = \mathbf{F}_2[T]/((T+1)^2)$ is not a domain, the ideal (2) is not prime in O_F. The reciprocal image of the ideal $(T+1) \subset \mathbf{F}_2[T]/((T+1)^2)$ is just $\mathfrak{p}_2 = (2, 1+\sqrt{-5})$ in O_F. It is easily checked that $\mathfrak{p}_2^2 = (2)$. This is the decomposition of (2) into prime ideals of O_F. We see that 2 is "ramified".

The ideal $\mathfrak{p}_2$ cannot be generated by 1 element only: suppose $\mathfrak{p}_2 = (\alpha)$ where $\alpha = a + b\sqrt{-5}$ with $a, b \in \mathbf{Z}$. Then α would divide both 2 and $1+\sqrt{-5}$. By the multiplicativity of the norm, this means that $\mathrm{N}(\alpha)$ divides both $\mathrm{N}(2) = 4$ and $\mathrm{N}(1+\sqrt{-5}) = 6$. Therefore $\mathrm{N}(\alpha) = 1$ or 2. If $\mathrm{N}(\alpha) = 1$, the element α would be a unit of O_F, which is impossible since $\mathfrak{p}_2$ has index 2 in O_F. So $\mathrm{N}(\alpha) = a^2 + 5b^2 = 2$. But this equation has no solutions $a, b \in \mathbf{Z}$.

Consider the ideal (3) in O_F. Since $O_F/(3) = \mathbf{Z}[T]/(2, T^2+5) = \mathbf{F}_3[T]/((T+1)(T-1))$ is not a domain, we see that (3) is not prime. In fact, the reciprocal images of the ideals $(T+1)$ and $(T-1)$ are prime ideals that divide (3). We let $\mathfrak{p}_3 = (3, T+1)$ and $\mathfrak{p}_3' = (3, T-1)$ denote these ideals. Neither $\mathfrak{p}_3$ nor $\mathfrak{p}_3'$ are principal ideals. One verifies easily that $(3) = \mathfrak{p}_3\mathfrak{p}_3'$ which gives us the prime decomposition of (3) in O_F. The prime 3 is "totally split" in F.

One checks that 7 decomposes in a way similar to 3. The prime 11 remains prime since $O_F/(11) \cong \mathbf{F}_{11}[T]/(T^2+5)$ and the polynomial T^2+5 is irreducible modulo 11. The prime 11 is "inert" in F. The decomposition of the prime numbers less than or equal to 11 is given in the following table:

Table.

p	(p)	
2	$\mathfrak{p}_2^2$	$\mathfrak{p}_2 = (2, 1+\sqrt{-5})$
3	$\mathfrak{p}_3\mathfrak{p}_3'$	$\mathfrak{p}_3 = (3, 1+\sqrt{-5})$ and $\mathfrak{p}_3' = (3, 1-\sqrt{-5})$
5	$\mathfrak{p}_5^2$	$\mathfrak{p}_5 = (\sqrt{-5})$
7	$\mathfrak{p}_7\mathfrak{p}_7'$	$\mathfrak{p}_7 = (7, 3+\sqrt{-5})$ and $\mathfrak{p}_7' = (7, -3+\sqrt{-5})$
11	(11)	11 is inert.

The number 6 has in the ring $\mathbf{Z}[\sqrt{-5}]$ two distinct factorizations into irreducible elements:

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

The factors have norms 4, 9, 6 and 6 respectively. They are irreducible, for if they were not, than their divisors would necessarily have norm 2 or 3. But, as we have seen above, this is impossible because, for trivial reasons, the Diophantine equations $a^2 + 5b^2 = 2$ and $a^2 + 5b^2 = 3$ do not have any solutions $a, b \in \mathbf{Z}$. there exists, however, a unique factorization of the ideal (6) in "ideal" prime factors. These prime factors are non-principal ideals. The factorization refines the two factorizations above:

$$(6) = \mathfrak{p}_2^2\mathfrak{p}_3\mathfrak{p}_3'.$$

Indeed, one has, on the one hand that $\mathfrak{p}_2^2 = (2)$ and $\mathfrak{p}_3\mathfrak{p}_3'$ and on the other that $\mathfrak{p}_2\mathfrak{p}_3 = (1+\sqrt{-5})$ and $\mathfrak{p}_2\mathfrak{p}_3' = (1-\sqrt{-5})$.

Finally we will apply Theorem 5.3 to the ζ-function $\zeta_F(s)$ of a number field F. First we consider the ζ-function of Riemann (G.B. Riemann, German mathematician 1826–1866):

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s} \qquad \text{for } s \in \mathbf{C},\ \mathrm{Re}(s) > 1.$$

L. Euler (Swiss mathematician who lived and worked in Berlin and St. Petersburg 1707–1783) found an expression for $\zeta(s)$ in terms of an infinite product:

$$\zeta(s) = \prod_{p \text{ prime}} (1 - \frac{1}{p^s})^{-1} \qquad \text{for } s \in \mathbf{C},\ \mathrm{Re}(s) > 1\ .$$

This implies at once that $\zeta(s)$ does not have any zeroes in $\mathbf{C}$ with real part larger than 1. The proof of Euler's formula is as follows: let $s \in \mathbf{C}$ with $\mathrm{Re}(s) > 1$. Observe that

$$(1 - \frac{1}{p^s})^{-1} = 1 + \frac{1}{p^s} + \frac{1}{p^{2s}} + \frac{1}{p^{3s}} + \ldots$$

Since every positive integer can be written as a product of primes *in a unique way*, we find that for every $X \in \mathbf{R}_{>0}$

$$\prod_{p \le X} (1 - \frac{1}{p^s})^{-1} = \sum_n \frac{1}{n^s}$$

where n runs over the positive integers that have only prime factors less than X. Therefore

$$|\sum_{n=1}^{\infty} \frac{1}{n^s} - \prod_{p \le X} (1 - \frac{1}{p^s})^{-1}| \le \sum_{n > X} \frac{1}{n^{\mathrm{Re}(s)}} \to 0$$

when $X \to \infty$. This follows from the fact that the sum $\sum_{n=1}^{\infty} 1/n^x$ converges for $x \in \mathbf{R}_{x>1}$. This implies Euler's formula.

Definition 6.6. Let F be a number field. The Dedekind ζ-function $\zeta_F(s)$ is given by

$$\zeta_F(s) = \sum_{I \neq 0} \frac{1}{\mathrm{N}(I)^s}$$

where I runs over the non-zero ideals of O_F. We see that for $F = \mathbf{Q}$ the Dedekind ζ-function $\zeta_{\mathbf{Q}}(s)$ is just Riemann's ζ-function. We will now study for which $s \in \mathbf{C}$ this sum converges.

Proposition 6.7. *Let F be a number field. Then*

$$\zeta_F(s) = \sum_{I\neq 0} \frac{1}{\mathrm{N}(I)^s} = \prod_{\mathfrak{p}} (1 - \frac{1}{\mathrm{N}(\mathfrak{p})^s})^{-1}$$

where I runs over the non-zero ideals of O_F and $\mathfrak{p}$ runs over the non-zero prime ideals of O_F. The sum and the product converge for $s \in \mathbf{C}$ with $\mathrm{Re}(s) > 1$.

Proof. Let m be the degree of F and let $s \in \mathbf{C}$ with $\mathrm{Re}(s) > 1$. By Prop 6.3*(iii)* there are at most m prime ideals dividing a fixed prime number p. Therefore

$$|\sum_{\mathrm{N}(\mathfrak{p})\leq X} \frac{1}{\mathrm{N}(\mathfrak{p})^s}| \leq m \sum_{p\leq X} \frac{1}{p^{\mathrm{Re}(s)}} \leq m \sum_{n\leq X} \frac{1}{n^{\mathrm{Re}(s)}}$$

where $\mathfrak{p}$ runs over the primes of O_F of norm at most X, where p runs over the prime numbers at most X and where n runs over the integers from 1 to n. Since the last sum converges, the first sum converges absolutely. Hence, by Exer.6.D the product

$$\prod_{\mathfrak{p}} (1 - \frac{1}{\mathrm{N}(\mathfrak{p})^s})^{-1}$$

converges. Now we take $s \in \mathbf{R}_{>1}$. By Theorem 5.3 the ideals I admit a unique factorization as a product of prime ideals. This implies

$$\sum_{\mathrm{N}(I)\leq X} \frac{1}{\mathrm{N}(I)^s} \leq \prod_{\mathfrak{p}} (1 - \frac{1}{\mathrm{N}(\mathfrak{p})^s})^{-1}$$

and we see, since the terms $\frac{1}{N(I)^s}$ are positive, that the sum converges. Moreover

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

when $X \to \infty$. This concludes the proof.

(6.A) Let F be a number field and let I be a fractional ideal of F. Show that there is a positive integer m such that mI is an ideal.

(6.B) Show that the ideal $I = (2, 2i) \subset \mathbf{Z}[2i]$ is not invertible, i.e. $I^{-1}I \neq R$.

(6.C) Let A be an additively written abelian group, which is free with basis $\{e_\lambda : \lambda \in \Lambda\}$. Let $a_1, a_2, \ldots, a_m \in A$. Define the integers $\alpha_{i,\lambda}$ by $a_i = \sum_{\lambda\in\Lambda} \alpha_{i,\lambda} e_\lambda$. Suppose that for all $i \neq j$, the sets $\{\lambda \in \Lambda : \alpha_{i,\lambda} \neq 0\}$ and $\{\lambda \in \Lambda : \alpha_{j,\lambda} \neq 0\}$ have empty intersection. Suppose that

$$\sum_{i=1}^{m} a_i = Nv$$

from some $N \in \mathbf{Z}_{>0}$ and $v \in A$. Show that N divides every $\alpha_{i,\lambda}$.

(6.D) Let $a_i \in \mathbf{R}_{\geq 0}$ for $i = 1, 2, \ldots$. Show that $\sum_i a_i$ converges if and only if $\prod_i (1 + a_i)$ converges.

(6.E) Show that $\mathbf{Q}^*_{>0}$ and the additive group of the ring $\mathbf{Z}[T]$ are isomorphic as abelian groups.

(6.F) Let F be a number field of degree n. Show that for every $q \in \mathbf{Q}^*$, the fractional ideal generated by q has norm q^n.

(6.G) Let F be a number field. For an ideal $I \subset O_F$ we put $\Phi(I) = \#(O_F/I)^*$. Show that $\sum_{I \subset J \subset R} \Phi(J) = N(I)$ and that $\Phi(I) = N(I) \prod_{\mathfrak{p}} (1 - N(\mathfrak{p})^{-1})$. Here the product runs over the prime ideals $\mathfrak{p}$ with $I \subset \mathfrak{p} \subset R$.

(6.H) Show that

$$\zeta_{\mathbf{Q}(i)}(s) = \sum_{\substack{a,b \in \mathbf{Z} \\ a \geq 0,\, b > 0}} \frac{1}{(a^2+b^2)^s} \qquad s \in \mathbf{C} \text{ and } \mathrm{Re}(s) > 1.$$

(6.I) Show that the prime 2 is ramified in $\mathbf{Q}(i)$. Show that a prime $p > 2$ splits completely in $\mathbf{Q}(i)$ if and only if $p \equiv 1 \pmod 4$. Show that for every prime $p \equiv 3 \pmod 4$, the ideal (p) is a prime ideal of $\mathbf{Z}[i]$.

(6.J) Show that

$$\zeta_{\mathbf{Q}(i)}(s) = \left(1 - \frac{1}{2^s}\right)^{-1} \prod_{p \equiv 1 \pmod 4} \left(1 - \frac{1}{p^s}\right)^{-2} \prod_{p \equiv 3 \pmod 4} \left(1 - \frac{1}{p^{2s}}\right)^{-1};$$

here the products run over prime numbers p that are congruent to 1 and 3 modulo 4, respectively and $s \in \mathbf{C}$ with $\mathrm{Re}(s) > 1$.

(6.K) Show that

$$\frac{\zeta_{\mathbf{Q}(i)}(s)}{\zeta_{\mathbf{Q}}(s)} = \prod_p \left(1 - \frac{\chi(p)}{p}\right)^{-1}$$

where the product runs over the prime numbers p, the complex number s has $\mathrm{Re}(s) > 1$ and the function χ is defined by

$$\chi(p) = \begin{cases} 1; & \text{if } p \equiv 1 \pmod 4, \\ 0; & \text{if } p = 2, \\ -1; & \text{if } p \equiv 3 \pmod 4. \end{cases}$$

7. Finitely generated abelian groups.

The contents of this section are not of a number theoretical nature. The results will be very important in the sequel. We determine the structure of finitely generated abelian groups. We expain the relation between indices of finitely generated free groups and determinants.

An abelian group is said to be *free of rank* n, if it is isomorphic to $\mathbf{Z}^n$. A subgroup H of a free group $G \cong \mathbf{Z}^n$ is said to have rank m if the $\mathbf{Q}$-vector space generated by H in $G \otimes \mathbf{Q} \cong \mathbf{Q}^n$ has dimension m.

For any two integers α and β, the notation $\alpha|\beta$ means that α divides β.

Theorem 7.1. *Let $G \cong \mathbf{Z}^n$ be a free group of rank n and let $H \subset G$ be a subgroup. Then*
(i) The group H is free of rank $m \leq n$.
(ii) There exists a $\mathbf{Z}$-basis $e_1, \ldots, e_n$ of G and integers $\alpha_1, \ldots, \alpha_m \in \mathbf{Z}_{\geq 0}$ such that $\alpha_1|\alpha_2|\ldots|\alpha_m$ and $\alpha_1 e_1, \ldots, \alpha_m e_m$ is a basis for H. The integers $\alpha_1, \ldots, \alpha_m$ are unique.

Proof. Suppose $0 \neq H \subset G$. Consider $\mathrm{Hom}(G, \mathbf{Z})$, the group of homomorphisms $f : G \longrightarrow \mathbf{Z}$. For every $f : G \longrightarrow \mathbf{Z}$ the set $f(H)$ is an ideal in $\mathbf{Z}$. This ideal is principal and it is generated by a unique $\alpha_f \geq 0$. Since $\mathbf{Z}$ is Noetherian, there is an ideal in the collection of ideals $\{f(H) : f : G \longrightarrow \mathbf{Z}\}$ which is "maximal" in the sense that for no $g : G \longrightarrow \mathbf{Z}$ the ideal $g(H)$ strictly contains $f(H)$. Since $H \neq 0$, this ideal $f(H)$ is not 0. Let α denote a positive generator and let $a \in H$ be an element for which $f(a) = \alpha$.

Now α divides $g(a)$ for every $g \in \mathrm{Hom}(G, \mathbf{Z})$: for suppose that $d = \gcd(g(a), \alpha)$ and let $u, v \in \mathbf{Z}$ such that $u\alpha + vg(a) = d$. Then d is the value of the functional $uf + vg$ at a. Since d divides α, it follows from the maximality of α that $d = \alpha$ and hence that α divides $g(a)$.

In particular, α divides all coordinates of a. We let $b = \frac{1}{\alpha} a \in G$. We see that $f(b) = 1$ and moreover that

$$\begin{aligned} G &= b\mathbf{Z} \oplus \ker(f), \\ H &= a\mathbf{Z} \oplus (\ker(f) \cap H). \end{aligned}$$

This follows easily from the fact that for every $x \in F$ one has that $x = f(x) \cdot b + x - f(x) \cdot b$. If, moreover, $x \in H$, then $f(x) \in a\mathbf{Z}$ by definition of a. We leave the easy verifications to the reader.

Now we prove (i) by induction with respect to the rank m of H. If $m = 0$ the statement is trivially true. If $m > 0$, we can split G and H as we did in the discussion above. The group $\ker(f) \cap H \subset G \cong \mathbf{Z}^n$ obviously has rank at most m. Since $H = a\mathbf{Z} \oplus (\ker(f) \cap H)$ has clearly strictly larger rank, we conclude that the rank of $\ker(f) \cap H$ is at most $m - 1$. By induction we see that this is a free group and consequently H is free as well. This proves *(i)*

Part *(ii)* is proved by induction with respect to n. If $n = 0$ the statement is trivially true. If $n > 0$, either $H = 0$, in which case the result is clear, or $H > 0$. In the latter case we can split G and H as explained above:

$$\begin{aligned} G &= b\mathbf{Z} \oplus \ker(f), \\ H &= a\mathbf{Z} \oplus (\ker(f) \cap H). \end{aligned}$$

The group $\ker(f)$ has rank at most $n - 1$. By *(i)* it is *free* of rank at most $n - 1$. By induction there exists a basis $e_2, \ldots, e_n$ of $\ker(f)$ and integers $\alpha_2, \ldots, \alpha_m$ such that $\alpha_2 e_2, \ldots, \alpha_m e_m$ is a basis for $\ker(f) \cap H$. We now take $e_1 = b$ and $\alpha_1 = \alpha = f(a)$. To complete the proof it suffices to verify that α divides α_2. If there is no e_2, there is nothing to prove. If there is, we define $g : G \longrightarrow \mathbf{Z}$ by $g(e_1) = g(e_2) = 1$ and $g(e_i) = 0$ for $i > 2$. We see that $\alpha \in g(H)$ and therefore $f(H) \subset g(H)$. By maximality of α, this implies $g(H) = (\alpha)$. Since $\alpha_2 = g(\alpha_2 e_2) \in g(H)$ the result follows.

We leave the proof that the α_i are unique to the reader.

Corollary 7.2.

(i) *For any finitely generated abelian group A there exist unique integers $r \geq 0$ and $\alpha_1, \alpha_2, \ldots, \alpha_t \in \mathbf{Z}_{>1}$ satisfying $\alpha_1 | \alpha_2 | \ldots | \alpha_t$ and such that*

$$A \cong \mathbf{Z}^r \times \mathbf{Z}/\alpha_1\mathbf{Z} \times \ldots \times \mathbf{Z}/\alpha_t\mathbf{Z}.$$

(ii) *For any finite abelian group A there exist unique integers $\alpha_1, \alpha_2, \ldots, \alpha_t \in \mathbf{Z}_{>1}$ with the property that $\alpha_1 | \alpha_2 | \ldots | \alpha_t$, such that*

$$A \cong \mathbf{Z}/\alpha_1\mathbf{Z} \times \ldots \mathbf{Z}/\alpha_t\mathbf{Z}.$$

(iii) *Let $G \cong \mathbf{Z}^n$ be a free group of rank n and let $H \subset G$ be a subgroup of G. Then H has finite index in G if and only if* $\mathrm{rk}(H) = \mathrm{rk}(G)$.

Proof. *(i)* Let A be a finitely generated group and let n be an integer such that there is a surjective map

$$\theta : \mathbf{Z}^n \longrightarrow A.$$

By Theorem 7.1 there is a basis $e_1, \ldots, e_n$ of $\mathbf{Z}^n$ and there exist positive integers $\alpha_1 | \alpha_2 | \ldots | \alpha_m$ such that $\alpha_1 e_1 \ldots, \alpha_m e_m$ is a basis for $H = \ker(\theta)$. It follows at once that

$$A \cong \mathbf{Z}^{n-m} \times \mathbf{Z}/\alpha_1\mathbf{Z} \times \ldots \times \mathbf{Z}/\alpha_m\mathbf{Z}$$

as required. The uniqueness of the α_i's follows easily by considering A modulo $\alpha_i A$ for various i.
(ii) This is just *(i)* for a *finite* abelian group.
(iii) Choose a basis $e_1, \ldots, e_n$ of G such that the subgroup H has $\alpha_1 e_1, \ldots, \alpha_m e_m$ as a basis. We have that

$$F/H \cong \mathbf{Z}^{n-m} \times \mathbf{Z}/\alpha_1\mathbf{Z} \times \ldots \times \mathbf{Z}/\alpha_m\mathbf{Z}$$

and clearly $\mathrm{rk}(H) = \mathrm{rk}(G)$ if and only if $n = m$ if and only if $[G : H] = \#(G/H)$ is finite. This proves *(ii)*.

Corollary 7.3. *Let M be a $n \times n$-matrix with integral coefficients. Let $G = \mathbf{Z}^n$ and $H = M(G) \subset G$. Then*

(i) *The index of H in G is finite if and only if* $\det(M) \neq 0$.

(ii) *If* $\det(M) \neq 0$ *then* $[G : H] = |\det(M)|$.

Proof. According to Theorem 7.1 we can choose a basis $e_1, e_2, \ldots, e_n$ for G such that $H = A(G) = \alpha_1 e_1 \mathbf{Z} \oplus \ldots \oplus \alpha_m e_m \mathbf{Z}$. With respect to this basis the matrix M becomes

$$M = \begin{pmatrix} \alpha_1 & 0 & \ldots & 0 \\ 0 & \alpha_2 & \ldots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \ldots & \end{pmatrix}$$

and we see that G/H is infinite if and only if one of the α_i is zero. This proves *(i)*. Part *(ii)* follows from the fact that $\det(M) = \prod_i \alpha_i$.

Next we apply the results on finitely generated abelian groups to number theory.

Corollary 7.4. *Let $f \in \mathbf{Z}[T]$ be a monic irreducible polynomial. Let α denote a zero and let $F = \mathbf{Q}(\alpha)$. Then the index $[O_F : \mathbf{Z}[\alpha]]$ is finite and*

$$\mathrm{Disc}(f) = [O_F : \mathbf{Z}[\alpha]]^2 \cdot \Delta_F.$$

Proof. Let $\omega_1, \ldots, \omega_n$ denote a $\mathbf{Z}$-basis for the ring of integers of F. There is then a matrix M with integral coefficients such that

$$M(\omega_1, \ldots, \omega_n) = (1, \alpha, \alpha^2, \ldots, \alpha^{n-1}).$$

Therefore

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

and hence, by Cor.7.3 and Prop.3.4*(iii)*

$$[O_F : \mathbf{Z}[\alpha]]^2 \Delta_F = \mathrm{Disc}(f)$$

as required.

Corollary 7.5. *Let F be a number field and let $\alpha \in F$. Then the norm of the O_F-ideal generated by α is equal to the absolute value of the norm of α:*

$$\mathrm{N}((\alpha)) = |\mathrm{N}(\alpha)|.$$

Proof. Let M_α denote the matrix which expresses the multiplication by α with respect to a $\mathbf{Q}$-basis of F. The columns of M_α form a $\mathbf{Z}$-basis for the ideal (α). We have

$$\begin{aligned} |\mathrm{N}(\alpha)| &= |\det(M_\alpha)| \qquad \text{by definition,} \\ &= [O_F : \mathrm{im}(M_\alpha)] \qquad \text{by Cor.5.3,} \\ &= \#O_F/(\alpha) = N((\alpha)). \end{aligned}$$

(7.A) Let $H = \binom{3}{0}\mathbf{Z} + \binom{0}{5}\mathbf{Z} \subset \mathbf{Z}^2$. Find a basis of $\mathbf{Z}^2$ as in Theorem 7.1.

(7.B) Let H in $\mathbf{Z}^3$ be the subgroup generated by $(1, 1, 2)$, $(5, 1, 1)$ abd $(-1, -5, -3)$, What is the structure of $\mathbf{Z}^3/H$?

(7.C) Let R be a commutative ring. A *module* over R, or an R-module, is an abelian group equipped with a multiplication (by "scalars") $R \times M \longrightarrow M$ which satisfies the following axioms:

$$\begin{aligned} a(x + y) &= ax + ay, \\ (a + b)x &= ax + bx, \\ (ab)x &= a(bx), \\ 1x &= x, \end{aligned}$$

for $a, b \in R$ and $x, y \in M$.

Show that a module over a field R is the same as a vector space over R. Show that every abelian group G is a $\mathbf{Z}$-module with multiplication

$$nx = \begin{cases} x + x + \ldots + x \ (n \text{ times}); & \text{if } n \geq 0, \\ x + x + \ldots + x \ (-n \text{ times}); & \text{if } n \leq 0, \end{cases}$$

for $n \in \mathbf{Z}$ and $x \in G$.

(7.D) Let R be a commutative ring.

(i) Show that R and, more generally, every ideal in R is an R-module with the usual multiplication.

(ii) Let M and N be two R-modules. Show that the product $M \times N$ is an R-module with the multiplication:
$$a(x, y) = (ax, ay)$$
for $a \in R$ and $x, y \in R$.

(7.E) let R be a commutative ring and let M be a module over R. A subgroup $N \subset M$ is called a *submodule* if it is, with the multiplication inherited from M, itself an R-module.

(i) Show that every ideal I of R is a submodule of R.

(ii) Let I be an ideal of R. Show that the quotient R/I is an R-module with the multiplication
$$a(x + I) = ax + I$$
for every $a \in R$ and coset $a + I$ of I.

(iii) Let M be an R-module and let $N \subset M$ be a submodule of M. Show that the quotient group M/N is an R-module with multplication
$$a(x + N) = ax + N$$
for every $a \in R$ and every coset $x + N$ of N in M.

(7.F) Let R be a commutative ring. An R-module is called *finitely generated,* if there is a finite number of elements $x_1, x_2, \ldots, x_t \in M$ such that
$$M = \{\lambda_1 x_1 + \lambda_2 x_2 + \ldots + \lambda_t x_t : \lambda_1, \lambda_2, \ldots, \lambda_t \in R\}.$$

(i) Show that the R-module $R^n = R \times \ldots \times R$ is finitely generated.

(ii) Show that an abelian group is finitely generated as a group if and only if it is finitely generated as a $\mathbf{Z}$-module.

(iii) Show: if M is finitely generated and N is a submodule of M, then N/M is also finitely generated

(iv)*Give an example of a commutative ring R and a finitely generated module of R which admits a submodule which is *not* finitely generated.

(7.G) Prove the following generalization of Cor.7.2: for every finitely generated $\mathbf{Z}[i]$-module A, there exist a unique integers $r \geq 0$ and elements $\alpha_1, \alpha_2, \ldots, \alpha_t \in \mathbf{Z}[i]$ satisfying $\alpha_1 | \alpha_2 | \ldots | \alpha_t$ and such that
$$A \cong \mathbf{Z}[i]^r \times \mathbf{Z}[i]/(\alpha_1) \times \ldots \times \mathbf{Z}[i]/(\alpha_t).$$
The elements α_i are unique upto multiplication by units of $\mathbf{Z}[i]$.

(7.H) Prove the following generalization of Cor.7.2: let F be a field. For every finitely generated $F[T]$-module A, there exist a unique integers $r \geq 0$ and unique monic polynomials $f_1, f_2, \ldots, f_t \in F[T]$ satisfying $f_1 | f_2 | \ldots | f_t$ and such that
$$A \cong F[T]^r \times F[T]/(f_1) \times \ldots \times F[T]/(f_t).$$

(7.I) Let F be a field and let n be a positive integer.

(i) Suppose that F^n is an $F(T)$-module. Show that multiplication by T is given by multiplication by an $n \times n$-matrix M with coefficients in F.

(ii) Conversely, if M is an $n \times n$-matrix with coefficients in F, then F^n admits the structure of an $F[T]$-module, where multiplication by T is given by multplication by M.

(7.J)**(Theorem of Jordan-Hölder)* Let M be an $n \times n$-matrix with coefficients in $\mathbf{C}$. Show that M is conjugate to a matrix of the form
$$\begin{pmatrix} (\quad) & 0 & \ldots & 0 \\ 0 & (\quad) & \ldots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \ldots & (\quad) \end{pmatrix}$$

where the small "submatrices" have the form

$$\begin{pmatrix} \lambda & 1 & 0 & \dots & 0 \\ 0 & \lambda & 1 & \dots & 0 \\ 0 & 0 & \lambda & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & & \dots & \lambda \end{pmatrix}$$

for some $\lambda \in \mathbf{C}$.
(Hint. Turn $\mathbf{C}^n$ into a $\mathbf{C}[T]$-module by means of the matrix M. Then apply Exer.7.H.)

8. Lattices.

This section concerns *lattices.* Lattices are finitely generated groups with additional structure. Many of the finitely generated groups that arise in algebraic number theory are, in natural way, equipped with the structure of a lattice.

We show that the ring of integers O_F of an algebraic number field F admits a natural lattice structure. In section 11 we will see that, in a certain sense, the unit group O_F^* admits a lattice structure as well.

Definition 8.1. *Let V be a vector space over $\mathbf{R}$. A subset $L \subset V$ is called a lattice if there exist $e_1, \ldots, e_n \in L$ such that*
(i) $L = \sum_i \mathbf{Z} e_i$,
(ii) The e_i are a basis for V over $\mathbf{R}$.

An easy example of a lattice is the group $\mathbf{Z}^n$ contained in the vector space $\mathbf{R}^n$. The following example is very important.

Example 8.2. *Let F be a number field. The image under Φ of the ring of integers O_F of F in $F \otimes \mathbf{R} = \mathbf{R}^{r_1} \times \mathbf{C}^{r_2}$ is a lattice.*

Proof. By Theorem 2.6 the map Φ maps a $\mathbf{Q}$-base of F to an $\mathbf{R}$-base of $F \otimes \mathbf{R}$. In particular, every $\mathbf{Z}$-base of O_F is mapped to an $\mathbf{R}$-base of $F \otimes \mathbf{R}$. This implies that $\Phi(O_F)$ is a lattice in $F \otimes \mathbf{R}$.

Proposition 8.3. *Let V be a real vector space and let $L \subset V$ be a subgroup. Then*
(i) L is a lattice.
(ii) L is discrete and cocompact.
(iii) L generates V over $\mathbf{R}$ and for every bounded set $B \subset V$ one has that $B \cap L < \infty$.

Proof. *(i) $\Rightarrow$ (ii)* The set L is clearly discrete. We have that $V = \sum_i e_i \mathbf{R}$ and therefore V/L, being a continuous image of the compact space $\sum_i e_i[0,1]$ is compact. In other words, L is *cocompact.*
(ii) $\Rightarrow$ (iii) Suppose L is discrete and cocompact. If L generates $W \subset_{\neq} V$ then there is a continuous surjection $V/L \longrightarrow V/W$. The vector space V/W is not compact and this contradicts the fact that V/L is compact. If there would be a bounded set B with $B \cap L$ infinite, then L could not be discrete.
(iii) $\Rightarrow$ (i) Since L generates V over $\mathbf{R}$, there is an $\mathbf{R}$-basis $e_1, \ldots, e_n \in L$ of V. The set $B = \sum_i e_i[0,1]$ is bounded and therefore L can be written as a finite union:

$$L = \bigcup_{x \in B \cap L} (x + \sum_i e_i \mathbf{Z}).$$

We conclude that the index $[L : \sum_i e_i \mathbf{Z}] = m$ is finite and that $mL \subset \sum_i e_i \mathbf{Z}$. By Theorem 7.1 the group mL is free and by Cor.7.2 it is of rank n. We conclude that L is free of rank m as well. This proves the proposition.

Corollary 8.4. *Let F be a number field. The image of a fractional ideal I under $\Phi : F \longrightarrow F \otimes \mathbf{R}$ is a lattice.*

Proof. Let $n \neq 0$ be an integer such that nI is an ideal. Let $0 \neq m \in nI$ be an integer. We have that

$$\frac{m}{n} O_F \subset I \subset \frac{1}{n} O_F.$$

Since the image of O_F in $F \otimes \mathbf{R}$ is a lattice, so is the image of qO_F for every $q \in \mathbf{Q}^*$. We conclude that $\frac{m}{n} O_F$ and therefore I is cocompact and that $\frac{1}{n} O_F$ and therefore I is discrete. By Prop.8.3 the image of I is a lattice, as required.

Definition. *Let V be a real vectore space provided with a Haar measure. Let $L \subset V$ be a lattice. The covolume* $\mathrm{covol}(L)$ *of* L *is defined by*

$$\mathrm{covol}(L) = \mathrm{vol}(V/L)$$

where the volume is taken with respect to the Haar measure induced on the quotient group V/L.

It is easy to see that the covolume of $L = \sum_i \mathbf{Z} v_i \subset \mathbf{R}^n$ is also the volume of a socalled *fundamental domain* of V for L:

$$\mathrm{covol}(L) = \mathrm{vol}(\{\sum_{i=1}^{n} \lambda_i v_i : 0 \leq \lambda_i < 1\}).$$

Lemma 8.5. *Let $e_1, \ldots, e_n$ be the standard basis of $\mathbf{R}^n$, provided with the usual Haar measure. Let M be an $n \times n$-matrix with real coefficients. Let L be the subgroup generated by the image $M(e_1 \ldots e_n)$ of the basis. Then*
(i) L is a lattice if and only if $\det(M) \neq 0$.
(ii) If L is a lattice, then $\mathrm{covol}(L) = |\det(M)|$.

Proof. Clearly $\det(M) \neq 0$ if and only if the vectors $M(e_1), \ldots, M(e_n)$ span $\mathbf{R}^n$ and, therefore, if and only if L is a lattice. This proves *(i)*. Part *(ii)* is a standard fact from linear algebra: For any n vectors $v_1, \ldots, v_n \in \mathbf{R}^n$ the parallelopepid $\{\sum \lambda_i v_i : 0 \leq \lambda_i < 1 \text{ for } 1 \leq i \leq n\}$ has volume $|\det(M)|$.

For instance, the lattice $\binom{2}{0}\mathbf{Z} + \binom{1}{-2}\mathbf{Z} \in \mathbf{R}^2$ has covolume $\left|\det\begin{pmatrix} 2 & 1 \\ 0 & -2 \end{pmatrix}\right| = 4$. The next proposition gives the covolumes of the lattices $\Phi(O_F)$ and $\Phi(I)$ in $F \otimes \mathbf{R}$.

Proposition 8.6. *Let F be a number field of degree n. Let r_1 denote the number of distinct homomorphisms $F \hookrightarrow \mathbf{R}$ and $2r_2$ the number of remaining homomorphisms $F \hookrightarrow \mathbf{C}$.*
(i) The covolume of the lattice O_F or rather $\Phi(O_F)$ in $F \otimes \mathbf{R}$ is given by

$$\mathrm{covol}(O_F) = 2^{-r_2} |\Delta_F|^{1/2}.$$

(ii) Let I be a fractional ideal, the covolume of I in $F \otimes \mathbf{R}$ is given by

$$\mathrm{covol}(I) = \mathrm{N}(I) 2^{-r_2} |\Delta_F|^{1/2}.$$

Proof. As usual we identify the 2-dimensional vector space $\mathbf{C}$ with $\mathbf{R}^2$ via $z \mapsto (\mathrm{Re}(z), \mathrm{Im}(z))$. In this way we have that $F \otimes \mathbf{R} \cong \mathbf{R}^n$ and we find that

$$\Phi(O_F) = \begin{pmatrix} \phi_1(\omega_1) & \ldots & \mathrm{Re}\,\phi_k(\omega_1) & \mathrm{Im}\,\phi_k(\omega_1) & \ldots & \\ \phi_1(\omega_2) & \ldots & \mathrm{Re}\,\phi_k(\omega_2) & \mathrm{Im}\,\phi_k(\omega_2) & \ldots & \\ \vdots & \vdots & & \vdots & \vdots & \end{pmatrix}$$

here $\omega_1, \ldots, \omega_n$ denotes a $\mathbf{Z}$-basis for O_F and the ϕ_j denote the embeddings $F \hookrightarrow \mathbf{C}$ upto complex conjugation. In the proof of Theorem 2.6 the determinant of this $n \times n$-matrix has been calculated:

$$\begin{aligned}|\det| &= |(2i)^{-r_2}\det(\phi_i(\omega_j))| \\ &= 2^{-r_2}|\Delta_F|^{1/2}\end{aligned}$$

and hence, by Lemma 8.5,

$$\mathrm{covol}(O_F) = 2^{-r_2}|\Delta_F|^{1/2}.$$

(ii) Using the notation of part *(i)* let $I \neq 0$ be a fractional ideal in O_F. By Exer.4.A there exists a non-zero integer m such that mI is an ideal in O_F. The ideal mI, being a subgroup of finite index of the free group O_F, is free of rank n. Let A be a matrix with integral coefficients such that

$$mI = A\begin{pmatrix}\omega_1\\ \vdots \\ \omega_n\end{pmatrix}.$$

By Cor.7.3*(ii)* the absolute value of the determinant of A is equal to $[O_F : mI] = \mathrm{N}(mI) = m^n\mathrm{N}(I)$. As in *(i)*, we have that

$$\mathrm{covol}(mI) = \det\left(A \cdot \Phi(O_F)\right) = m^n N(I)2^{-r_2}|\Delta_F|^{1/2}.$$

By Exer.8.B we have that $\mathrm{covol}(mI) = m^n\mathrm{covol}(I)$, and the result follows.

(8.A) Let $L = \{(x, y, z) \in \mathbf{Z}^3 : 2x + 3y + 4z \equiv 0 \pmod 7\}$. Show that $L \subset \mathbf{R}^3$ is a lattice. Find a $\mathbf{Z}$-basis and calculate its covolume.

(8.B) Let $L \subset \mathbf{R}^n$ be a lattice. Let A be an invertible $n \times n$-matrix. Show that $A(L)$ is a lattice. Show that $\mathrm{covol}(A(L)) = |\det(A)|\mathrm{covol}(L)$. Let $m \in \mathbf{Z}_{>0}$; show that $\mathrm{covol}(mL) = m^n\mathrm{covol}(L)$.

(8.C) Identify the quaternions $\mathbf{H} = \{a+bi+cj+dk : a, b, c, d \in \mathbf{R}\}$ with $\mathbf{R}^4$ via $a+bi+cj+dk \leftrightarrow (a, b, c, d)$. What is the covolume of the ring of Hurwitz integers

$$\mathbf{Z}[i, j, k, \frac{1+i+j+k}{2}]$$

in $\mathbf{H} \cong \mathbf{R}^4$?

(8.D) Let F be a number field. Suppose $R \subset F$ is a subring with the property that its image in $F \otimes \mathbf{R}$ is a lattice. Show that $R \subset O_F$.

(8.E) *(Euclidean imaginary quadratic rings.)* Let F be an imaginary quadratic number field. We identify O_F with its Φ-image in $F \otimes \mathbf{R} = \mathbf{C}$.

(i) Show that O_F is Euclidean for the norm if and only if the disks with radius 1 and centers in O_F cover $\mathbf{C}$.

(ii) Show that O_F is Euclidean for the norm if and only if $\Delta_F = -3, -4, -7, -8$ or -11.

(iii) For real quadratic fields F (with $F \otimes \mathbf{R} = \mathbf{R}^2$) there is a similar result: the ring O_F of integers of a real quadratic field F is Euclidean for the norm if and only if $\Delta_F = 5$, 8, 12, 13, 17, 21, 24, 28, 29, 33, 37, 41, 44, 57, 73 or 76. This result is due to Chatland and Davenport [13] and much harder to prove. The following is easier: show that the rings of integers of the rings of integers of the quadratic fields F with $\Delta_F = 5, 8$ and 12 are Euclidean for the norm.

(8.F)*Let L be a free abelian group of rank r. Let $Q(x)$ be a positive definite quadratic form on L. Supppose that for every $B \in \mathbf{R}$ there are only finitely many $x \in L$ with $Q(x) < B$. Then there is an injective map $I : L \hookrightarrow \mathbf{R}^r$ such that $i(L)$ is a lattice and $\|i(x)\| = Q(x)$. Here $\|v\|$ denotes the usual length of a vector $v \in \mathbf{R}^r$.

(8.G) Let $L \subset \mathbf{R}^n$ be a lattice. Show that

$$\lim_{t\to\infty} \frac{1}{t^n} \#\{(v_1, \dots, v_n) \in L : |v_i| \le t \quad \text{for all } 1 \le i \le n\} = \frac{2^n}{\text{covol}(L)}.$$

(8.H) Show that the rings $\mathbf{Z}[\zeta_3]$ and $\mathbf{Z}[\zeta_4]$ are Euclidean for the norm. It was shown by H.W. Lenstra [**,**] that the ring $\mathbf{Z}[\zeta_m]$ is Euclidean for the norm when $\varphi(m) \le 10$ (except for the case $m = 16$, which was done by Ojala [*]).

9. Discriminants and ramification.

Any number field F can be written as $\mathbf{Q}(\alpha)$ where α is an algebraic integer. Consequently, the ring $\mathbf{Z}[\alpha]$ is a subring of O_F, which is of finite index by Cor.7.4. In this section we investigate under which conditions $\mathbf{Z}[\alpha] = O_F$, or more generally, which primes divide the index $[O_F : \mathbf{Z}[\alpha]]$. For primes that do *not* divide this index, one can find the prime ideals of O_F that divide p, from the decomposition of the minimum polynomial $f(T)$ of α in the ring $\mathbf{F}_p[T]$. This is the content of the Factorization Lemma.

Theorem 9.1. *(Factorization Lemma or Kummer's Lemma) Suppose $f \in \mathbf{Z}[T]$ is an irreducible polynomial. Let α denote a zero of f and let $F = \mathbf{Q}(\alpha)$. Let p be a prime number not dividing the index $[O_F : \mathbf{Z}[\alpha]]$. Suppose the polynomial f factors in $\mathbf{F}_p[T]$ as*

$$f(T) = h_1(T)^{e_1} \cdot \ldots \cdot h_g(T)^{e_g}$$

where the polynomials $h_1, \dots, h_g$ are the distinct irreducible factors of f modulo p. Then the prime factorization of the ideal (p) in O_F is given by

$$(p) = \mathfrak{p}_1^{e_1} \cdot \ldots \cdot \mathfrak{p}_g^{e_g},$$

where the $\mathfrak{p}_i = (h_i(\alpha), p)$ are distinct prime ideals with $N(\mathfrak{p}_i) = p^{\deg(h_i)}$.

Proof. We observe first that for any prime p we have that

$$\mathbf{Z}[\alpha]/(h_i(\alpha), p) \cong \mathbf{F}_p[T]/(h_i(T), f(T), p) \cong \mathbf{F}_{p^{\deg(h_i)}}.$$

Let $d = [O_F : \mathbf{Z}[\alpha]]$ and suppose p is a prime not dividing d. Let $a, b \in \mathbf{Z}$ such that $ap + bd = 1$. We claim that the map

$$O_F/\mathfrak{p}_i \xrightarrow{*bd} \mathbf{Z}[\alpha]/(g_i(\alpha), p)$$

is an isomorphism of rings. Note that $\mathfrak{p}_i$ is the ideal generated by p and $g_i(\alpha)$ *in* O_F. To prove our claim we first observe that the map is clearly well defined. It is a homomorphism since $(bdx)(bdy) - bdxy = bdxy(1 - bd) = bdxyap$ for $x, y \in O_F$ and this is 0 modulo the ideal $(g_i(\alpha), p) \subset \mathbf{Z}[\alpha]$. The map is injective since, whenever $bdx \in (g_i(\alpha), p)$ then $x = (ap + bd)x = apx + bdx \in \mathfrak{p}_i$. Finally, the map is surjective since any $x \in \mathbf{Z}[\alpha]$ satisfies $x = (ap + bd)x \equiv bdx$.

We conclude that $\mathfrak{p}_i$ is a prime ideal of norm $p^{\deg(h_i)}$. Therefore

$$\mathrm{N}(\prod_i \mathfrak{p}_i^{e_i}) = p^{\sum_i \deg(h_i)e_i} = p^n$$

where $n = \deg(f)$. On the other hand, we have that

$$\prod_i \mathfrak{p}_i^{e_i} = \prod_i (h_i(\alpha), p)^{e_i} \subset (p).$$

Since $\mathrm{N}((p)) = p^n$, we conclude that $(p) = \prod_i \mathfrak{p}_i$. Finally, the ideals $\mathfrak{p}_i$ are mutually distinct since $(h_i(T), h_j(T), p) = O_F$ for $i \ne j$. This proves the theorem.

Corollary 9.2. *Let F be a number field. If p is a prime number that ramifies in F, then p divides the discriminant Δ_F or p divides the index $[O_F : \mathbf{Z}[\alpha]]$ for some integral α which generates F over $\mathbf{Q}$. In particular, only finitely many primes p are ramified in F.*

Proof. Suppose p ramifies and does not divide the index $[O_F : \mathbf{Z}[\alpha]]$. By the Factorization Lemma 6.1 the prime (p) splits as

$$(p) = \prod (g_i(\alpha), p)^{e_i}$$

where the e_i are the exponents occurring in the prime decomposition of $f(T) = \prod_i h_i(T)^{e_i}$ in $\mathbf{F}_p[T]$. We conclude that $e_i > 1$ for some index i and hence that the polynomial $f(T) \in \mathbf{F}_p[T]$ is not squarefree. This implies that its discriminant is 0. In other words p divides $\mathrm{Disc}(f)$ as required.

Example. Let $F = \mathbf{Q}(\alpha)$ where α is a zero of the polynomial $f(T) = T^3 - T - 1$. We have seen in section 2 that the discriminant of f is -23. Therefore the ring of integers of F is just $\mathbf{Z}[\alpha]$. By the Factorization Lemma, a prime number p factors in $O_F = \mathbf{Z}[\alpha]$ in the same way as the polynomial $f(T) = T^3 - T - 1$ factors in the ring $\mathbf{F}_p[T]$.

Modulo 2 and 3, the polynomial $f(T)$ is irreducible; we conclude that the ideals (2) and (3) in O_F are prime. Modulo 5 the polynomial $f(T)$ has a zero and f factors as $T^3 - T - 1 = (T-2)(T^2 + 2T - 2)$ in $\mathbf{F}_5[T]$. We conclude that $(5) = \mathfrak{p}_5\mathfrak{p}_{25}$ where $\mathfrak{p}_5 = (5, \alpha - 2)$ is a prime of norm 5 and $\mathfrak{p}_{25} = (5, \alpha^2 + 2\alpha - 2)$ is a prime of norm 25. The prime 7 is again prime in O_F and the prime 11 splits, like the prime 5, into a product of a prime of norm 11 and of one of norm 121.

The following table contains this and some more factorizations of prime numbers. The indices denote the norms of the prime ideals. Notice the only ramified prime: 23. There are also primes that split completely in F over $\mathbf{Q}$. The prime 59 is the smallest example.

Table.

p	(p)	
2	(2)	
3	(3)	
5	$\mathfrak{p}_5\mathfrak{p}_{25}$	$\mathfrak{p}_5 = (\alpha - 2, 5)$ and $\mathfrak{p}_{25} = (\alpha^2 + 2\alpha - 2, 5)$
7	(7)	
11	$\mathfrak{p}_{11}\mathfrak{p}_{121}$	$\mathfrak{p}_{11} = (\alpha + 5, 11)$ and $\mathfrak{p}_{121} = (\alpha^2 - 5\alpha + 2, 11)$
13	(13)	
17	$\mathfrak{p}_{17}\mathfrak{p}_{289}$	$\mathfrak{p}_{17} = (\alpha - 5, 17)$ and $\mathfrak{p}_{289} = (\alpha^2 + 5\alpha - 10, 17)$
19	$\mathfrak{p}_{19}\mathfrak{p}_{361}$	$\mathfrak{p}_{19} = (\alpha - 6, 19)$ and $\mathfrak{p}_{361} = (\alpha^2 + 6\alpha - 3, 19)$
23	$\mathfrak{p}_{23}^2\mathfrak{p}'_{23}$	$\mathfrak{p}_{23} = (\alpha - 10, 23)$ and $\mathfrak{p}'_{23} = (\alpha - 3, 23)$
59	$\mathfrak{p}_{59}\mathfrak{p}'_{59}\mathfrak{p}''_{59}$	$\mathfrak{p}_{59} = (\alpha - 4, 59)$, $\mathfrak{p}'_{59} = (\alpha - 13, 59)$ and $\mathfrak{p}''_{59} = (\alpha + 17, 59)$

Proposition 9.3. *Let p be a prime and let $f(T) \in \mathbf{Z}[T]$ be an Eisenstein polynomial for the prime p. Let π be a zero of f and let $F = \mathbf{Q}(\pi)$ be the number field generated by π. Then $\mathbf{Z}[\pi]$ has finite index in O_F and p does not* divide this index.

Proof. By Cor.7.4 the index $[O_F : \mathbf{Z}[\pi]]$ is finite. Suppose that p divides the index. Consider the $\mathbf{F}_p[T]$-ideal

$$I = \{g \in \mathbf{F}_p[T] : \frac{1}{p} g(\pi) \in O_F\}.$$

Note that this ideal is well defined and that it contains $f(T) \equiv T^n \pmod{p}$. Here $n = \deg(f) = [F : \mathbf{Q}]$. Since p divides the index $[O_F : \mathbf{Z}[\pi]]$, there exists an element $x \in O_F - \mathbf{Z}[\alpha]$ such that $px \in \mathbf{Z}[\pi]$. So words $px = \sum_{i=0}^{n-1} a_i \pi^i$ where $a_i \in \mathbf{Z}$ not all divisibale by p. This implies that

$\sum_{i=0}^{n-1} a_i T^i$ is a non zero polynomial contained in the ideal I and we see that the ideal I is a *proper* divisor of T^n. Therefore $\frac{\pi^{n-1}}{p}$ is in O_F or, equivalently, p divides π^{n-1}.

Let $f(T) = T^n + a_{n-1}T^{n-1} + \ldots + a_1 T + a_0 \in \mathbf{Z}[T]$ be the Eisenstein polynomial. Then πp divides

$$-a_0 = \pi^n + a_{n-1}\pi^{n-1} + \ldots + a_2\pi^2 + a_1\pi.$$

This implies that π divides a_0/p and hence that p divides π^{n-1} and $(a_0/p)^{n-1}$. This contradicts the fact that a_0/p is prime to p and we conclude that p does not divide the index $[O_F : \mathbf{Z}[\pi]]$ as required.

Example 9.4. *Let p^n be a power of a prime p and let $F = \mathbf{Q}(\zeta_{p^n})$. The ring of integers of F is $\mathbf{Z}[\zeta_{p^n}]$.*

Proof. Clearly $\mathbf{Z}[\zeta_p]$ is contained in the ring of integers of $\mathbf{Q}(\zeta_{p^n})$. By Exercise 3.N, the discriminant of $\Phi_{p^n}(T)$ is a power of p. By Cor.7.4 we see that the only prime that could divide the index $[O_F^* : \mathbf{Z}[\zeta_p]]$ is p. Consider the minimum polynomial of ζ_{p^n}:

$$f_{\min}^{\zeta_p}(T) = \Phi_{p^n}(T) = T^{(p-1)p^{n-1}} + \ldots + T^{p^{n-1}} + 1.$$

It is easy to see that $\Phi_{p^n}(T+1)$ is an Eisenstein polynomial. We conclude from Prop.9.3 that p does not divide the index $[O_F^* : \mathbf{Z}[\zeta_p]]$. This completes the example.

The following two theorems will not be used in the sequel. They are included because they give complete answers to natural questions and because the proofs can easily be given using only the theory we have developed sofar. Theorem 9.5 is an extension of Prop.9.3. Theorem 9.6 makes part of Cor.9.2 more precise.

Theorem 9.5. *(Dedekind's Criterion.) Suppose α is an algebraic integer with minimum polynomial over $f(T) \in \mathbf{Z}[T]$. Let $F = \mathbf{Q}(\alpha)$. For p be a prime number, let $f_1, \ldots, f_g \in \mathbf{Z}[T]$ and $e_1, \ldots, e_g \in \mathbf{Z}_{\geq 1}$ such that $f = f_1^{e_1} \cdot \ldots \cdot f_g^{e_g}$ is the decomposition of f into distinct irreducible polynomials f_i modulo p. Then*

$$p \text{ divides the index } [O_F : \mathbf{Z}[\alpha]]$$

if and only if there is an index j such that

$$f_j \text{ divides } \left(\frac{f(T) - \prod_j f_j(T)^{e_j}}{p}\right) \quad \text{in } \mathbf{F}_p[T] \qquad \text{and} \qquad e_j \geq 2.$$

Proof. We put

$$u(T) = \frac{f(T) - \prod_j f_j(T)^{e_j}}{p} \in \mathbf{Z}[T]$$

and for every index j we define the polynomial $F_j(T) \in \mathbf{Z}[T]$ by

$$F_j(T) = \frac{1}{f_j(T)} \prod_{j=1}^{g} f_j(T)^{e_j}.$$

Finally we let

$$x_j = \frac{1}{p} F_j(\alpha) = \frac{u(\alpha)}{f_j(\alpha)} \in F.$$

"if": Suppose that $f_j(T)$ divides $u(T)$ in $\mathbf{F}_p[T]$ and that $e_j \geq 2$ for some index j. Consider $x = x_j$. Clearly $px \in \mathbf{Z}[\alpha]$, but since $\deg(F_j) < \deg(f)$, we have that $x \notin \mathbf{Z}[\alpha]$. To prove that p divides the index $[O_F : \mathbf{Z}[\alpha]]$ it suffices to show that $x \in O_F$.

Consider the ideal $I = (f_j(\alpha), p) \subset \mathbf{Z}[\alpha]$. We have that $xp = F_j(\alpha)$ which is a $\mathbf{Z}[\alpha]$-multiple of $f_j(\alpha)$ because $e_j \geq 2$. We have that $xf_j(\alpha) = u(\alpha)$ which is a $\mathbf{Z}[\alpha]$-multiple of $f_j(\alpha)$ by assumption. The ideal I is a finitely generated abelian group. Lemma 3.1*(iii)* implies that x is integral. This proves the sufficiency.

"only if": Suppose that p divides the index of $\mathbf{Z}[\alpha]$ in O_F. Consider the $\mathbf{F}_p[T]$-ideal $J = \{h \in \mathbf{F}_p[T] : \frac{1}{p}h(\alpha) \in O_F\}$. This ideal clearly contains $f(T)$, but, by our assumption on the index, it is strictly larger than (f). Let ϕ be a generator of J and let j be an index such that

$$f_j(T) \text{ divides } \frac{f(T)}{\phi(T)} \qquad \text{in } \mathbf{F}_p[T].$$

We claim that this index j satisfies the conditions of the theorem.

To show this we consider again

$$x = x_j = \frac{1}{p}F_j(\alpha) = \frac{u(\alpha)}{f_j(\alpha)}.$$

Since ϕ divides F_j, we have that $x \in O_F$. We conclude that there exists a monic polynomial in $\mathbf{Z}[T]$ with $u(\alpha)/f_j(\alpha)$ as a zero. Therefore $f_j(\alpha)$ divides $u(\alpha)^m$ in $\mathbf{Z}[\alpha]$ for some integer $m \geq 1$. We conclude that there exists polynomials $h_1, h_2 \in \mathbf{Z}[T]$ such that

$$u(T)^m = f_j(T)h_1(T) + f(T)h_2(T)$$

and hence that $f_j(T)$ divides $u(T)^m$ in the ring $\mathbf{F}_p[T]$. Since $f_j(T)$ is irreducible modulo p, this implies that $f_j(T)$ divides $u(T)$ modulo p.

It remains to prove that $e_j \geq 2$. From $f_j(\alpha)x = u(\alpha)$ one concludes that $F_j\alpha) + f_j(\alpha)x = F_j\alpha) + u(\alpha)$ and hence that

$$x = \frac{u(\alpha) + F_j(\alpha)}{p + f_j(\alpha)}.$$

Exactly the same proof as before, now gives that $f_j(T)$ divides $u(T) + F_j(T)$ modulo p. Therefore $f_j(T)$ divides $F_j(T)$ and $e_j \geq 2$ as required.

Theorem 9.6. *(R. Dedekind 1920) Let F be a number field and let p be a prime. Then p is ramified in F over $\mathbf{Q}$ if and only if p divides Δ_F.*

Proof. We introduce a slightly more general concept of "discriminant": let K be a field and let A be an n-dimensional commutative K-algebra, that is, a vector space over K of dimension n which is also a commutative ring satisfying $\lambda(ab) = (\lambda a)b = a(\lambda b)$ for all $a, b \in A$ and $\lambda \in K$. In section 2 we have studied the special case $K = \mathbf{Q}$ and A a number field F.

On A we define the *trace* $\mathrm{Tr}(x)$ of an element $x \in A$ by $\mathrm{Tr}(x) = \mathrm{Tr}(M_x)$ where M_x denotes the matrix of the multiplication-by-x-map with respect to some K-base of A. For $\omega_1, \ldots, \omega_n \in A$ we let

$$\Delta(\omega_1, \ldots, \omega_n) = \det(\mathrm{Tr}(\omega_i\omega_j))_{1 \leq i,j \leq n}.$$

In contrast to the situation in section 3, or Exer.3.L, it may happen, in general that $\Delta(\omega_1, \ldots, \omega_n) = 0$ even if the ω_i constitute a K-basis for A. However, if this happens, it happens for *every* basis of A: as in section 3, the discriminant $\Delta(\omega_1, \ldots, \omega_n)$ of a *basis* $\omega_1, \ldots, \omega_n$ depends on the basis, but whether the discriminant is zero or not doesn't: the discriminant differs by a multiplicative factor $\det(M)^2$ where $M \in \mathrm{GL}_n(K)$ is the matrix transforming one basis into the other.

Using the fact that the non-nullity of the discriminant of a basis does not depend on the basis, we define the *discriminant of* A by

$$\Delta(A/K) = \Delta(\omega_1, \ldots, \omega_n)$$

for some K-basis $\omega_1, \ldots, \omega_n$ of A. It is only well defined upto a unit in K^*.

In Exer.9.J it is shown that for two finite dimensional K-algebras A and B one has that

$$\Delta(A \times B/K) = \Delta(A/K)\Delta(B/K).$$

Now we start the proof. Let F be a number field of degree n and let p be a prime number. Consider the field $K = \mathbf{F}_p$ and the n-dimensional K-algebra $O_F/(p)$. We are going to calculate the discriminant of $O_F/(p)$. First by reducing a $\mathbf{Z}$-basis of the ring of integers O_F modulo p:

$$\Delta(O_F/(p)/\mathbf{F}_p) \equiv \Delta_F \pmod{p}.$$

Next we decompose $O_F/(p)$ into a product of $\mathbf{F}_p$-algebras. Suppose p factors in O_F as

$$(p) = \mathfrak{p}_1^{e_1} \cdot \ldots \cdot \mathfrak{p}_g^{e_g}.$$

By the Chinese Remainder Theorem (Exer.4.G) we have that

$$O_F/(p) \cong O_F/\mathfrak{p}_1^{e_1} \times \ldots \times O_F/\mathfrak{p}_g^{e_g}$$

and hence that

$$\Delta(O_F/(p)) = \Delta((O_F/\mathfrak{p}_1^{e_1})/\mathbf{F}_p) \cdot \ldots \cdot \Delta((O_F/\mathfrak{p}_g^{e_g})/\mathbf{F}_p).$$

By Exer.2.Q the discriminant $\Delta(\mathbf{F}_q/\mathbf{F}_p)$ is non-zero for every finite field extension $\mathbf{F}_q$ of $\mathbf{F}_p$. This shows that p does not divide Δ_F whenever p is not ramified.

To show the converse, it suffices to show that $\Delta((O_F/\mathfrak{p}^e)/\mathbf{F}_p) = 0$ whenever $\mathfrak{p}$ divides p and $e > 1$. Let therefore $e > 1$ and put $A = O_F/\mathfrak{p}^e$ and let $\pi \in \mathfrak{p}$ but not in $\mathfrak{p}^2$. Then π is nilpotent. Since it is not zero, we can use it as the first element in an $\mathbf{F}_p$-basis $\omega_1, \ldots, \omega_k$ of A. Clearly $\pi\omega_i$ is nilpotent for every $\omega_i \in A$. Since a nilpotent endomorphism has only eigenvalues 0, we see that the first row of the matrix $(\mathrm{Tr}(\omega_i\omega_j))_{1 \le i,j \le n}$ is zero. This concludes the proof of the Theorem.

(9.A) Let $F = \mathbf{Q}(\alpha)$ where α be a zero of the polynomial $T^3 - T - 1$. Show that the ring of integers of F is $\mathbf{Z}[\alpha]$. Find the factorizations in $\mathbf{Z}[\alpha]$ of the primes less than 10.

(9.B) Let d be a squarefree integer and let $F = \mathbf{Q}(\sqrt{d})$ be a quadratic field. Show that for *odd* primes p one has that p splits (is inert, ramifies) in F over $\mathbf{Q}$ if and only if d is a square (non-square, zero) modulo p.

(9.C) Let ζ_5 denote a primitive 5th root of unity. Determine the decomposition into prime factors in $\mathbf{Q}(\zeta_5)$ of the primes less than 14.

(9.D) Show that the following three polynomials have the same discriminant:

$$T^3 - 18T - 6,$$
$$T^3 - 36T - 78,$$
$$T^3 - 54T - 150.$$

Let α, β and γ denote zeroes of the respective polynomials. Show that the fields $\mathbf{Q}(\alpha)$, $\mathbf{Q}(\beta)$ and $\mathbf{Q}(\gamma)$ have the same discriminants, but are not isomorphic. (Hint: the splitting behavior of the primes is not the same.)

(9.E) Show that $\mathbf{Z}[\sqrt[3]{20}, \sqrt[3]{50}]$ is the ring of integers of $F = \mathbf{Q}(\sqrt[3]{20})$. Show there is no $\alpha \in O_F$ such that $O_F = \mathbf{Z}[\alpha]$.

(9.F) *(Samuel) Let $f(T) = T^3 + T^2 - 2T + 8 \in \mathbf{Z}[T]$. Show that f is irreducible.

(i) Show that $\mathrm{Disc}(f) = -4 \cdot 503$. Show that the ring of integers of $F = \mathbf{Q}(\alpha)$ admits $1, \alpha, \beta = (\alpha^2 - \alpha)/2$ as a $\mathbf{Z}$-basis.

(ii) Show that O_F has precisely three distinct ideals of index 2. Conclude that 2 splits completely in F over $\mathbf{Q}$.

(iii) Show that there is no $\alpha \in F$ such that $O_F = \mathbf{Z}[\alpha]$. Show that for every $\alpha \in O_F - \mathbf{Z}$, the prime 2 divides the index $[O_F : \mathbf{Z}[\alpha]]$.

(9.G)*Let $m \in \mathbf{Z}_{>0}$. Let K be a field, let A be the K-algebra $K[T]/(T^m)$. Compute the discriminant of A.

(9.H)*Let K be a field and let A and B be two finite dimensional K-algebras. Show that $\Delta(A \times B) = \Delta(A) \times \Delta(B)$.

10. The Theorem of Minkowski.

In this section we prove the most important finiteness results of algebraic number theory. We prove that the class group of the ring of integers is finite. This result is due to to P. Lejeune Dirichlet (German mathematician 1805–1859) [45]. We will prove it by means of techniques from the "Geometry of Numbers" a subject created by Hermann Minkowski (German mathematician 1864–1909) [56,57]. For a very thorough discussion of the geometry of numbers and its history see the book by Lekkerkerker and Gruber [46].

Theorem 10.1. *(Minkowski's convex body theorem) Let $V \cong \mathbf{R}^n$ be a real vector space and let $L \subset V$ be a lattice. Let X be a bounded, convex, symmetric subset of V. If*

$$\mathrm{vol}(X) > 2^n \mathrm{covol}(L)$$

then there exists a non-zero vector $\lambda \in L \cap X$.

Proof. Consider the measure preserving natural map

$$X \longrightarrow V/2L.$$

Since $\mathrm{covol}(2L) = 2^n \mathrm{covol}(L)$ we see that $\mathrm{vol}(X) > \mathrm{vol}(V/2L)$. Therefore there are two points $x_1 \neq x_2$ in X which have the same image in $V/2L$. In other words $x_1 - x_2 \in 2L$. We conclude that $0 \neq y = (x_1 - x_2)/2 \in L$. By symmetry we have that $-x_2 \in X$ and hence, by convexity, that $y = (x_1 - x_2)/2 \in X$. So $0 \neq y \in X \cap L$ as required.

In the proof of the following lemma, we will calculate a certain volume. This will be useful in the proof of Theorem 10.3.

Lemma 10.2. *Let $r_1, r_2 \in \mathbf{Z}_{>0}$ and put $n = r_1 + 2r_2$. For every $R \geq 0$ put*

$$W(r_1, r_2, R) = \{(x_1, \ldots, x_{r_1}, y_1, \ldots, y_{r_2}) \in \mathbf{R}^{r_1} \times \mathbf{C}^{r_2} : |x_1| + \ldots + |x_{r_1}| + 2|y_1| + \ldots + 2|y_{r_2}| \leq R\}.$$

Then

$$\mathrm{vol}(W(r_1, r_2, R)) = 2^{r_1} \left(\frac{\pi}{2}\right)^{r_2} \frac{R^n}{n!}.$$

Proof. The proof is by induction with respect to n. If $r_1 = 1$ and $r_2 = 0$ and if $r_1 = 0$ and $r_2 = 1$, the result is easily verified. We will next discuss the two steps $r_1 \to r_1 + 1$ and $r_2 \to r_2 + 1$.

Case $r_1 \to r_1 + 1$

$$\begin{aligned}\mathrm{vol}(W(r_1+1, r_2, R)) &= \int_{-R}^{R} \mathrm{vol}(r_1, r_2, R - |t|)dt \\ &= 2^{r_1} \left(\frac{\pi}{2}\right)^{r_2} \frac{1}{n!} \int_{-R}^{R} (R-|t|)^n dt \\ &= 2^{r_1+1} \left(\frac{\pi}{2}\right)^{r_2} \frac{1}{n!} \int_{0}^{R} t^n dt \\ &= 2^{r_1+1} \left(\frac{\pi}{2}\right)^{r_2} \frac{R^{n+1}}{(n+1)!}.\end{aligned}$$

Case $r_2 \to r_2 + 1$

$$\begin{aligned}\mathrm{vol}(W(r_1, r_2+1, R)) &= \int_{\substack{z \in \mathbf{C} \\ |z| \le R/2}} \mathrm{vol}(r_1, r_2, R - |z|)d\mu(z) \\ &= \int_0^{2\pi} \int_0^{R/2} 2^{r_1} \left(\frac{\pi}{2}\right)^{r_2} \frac{1}{n!} (R - 2\rho)^n \rho d\rho d\phi \\ &= 2\pi 2^{r_1} \left(\frac{\pi}{2}\right)^{r_2} \frac{1}{n!} \int_0^R t^n \frac{(R-t)}{2} \frac{dt}{2} \\ &= 2^{r_1} \left(\frac{\pi}{2}\right)^{r_2} \frac{R^{n+2}}{(n+2)!}\end{aligned}$$

This proves the lemma.

Theorem 10.3. *(H .Minkowski) Let F be a number field of degree n. Let r_1 denote the number of embeddings $F \hookrightarrow \mathbf{R}$ and $2r_2$ the remaining number of embeddings $F \hookrightarrow \mathbf{C}$. Then every non-zero ideal I of O_F contains an element x with*

$$|\mathrm{N}(x)| \le \frac{n!}{n^n} \left(\frac{4}{\pi}\right)^{r_2} |\Delta_F|^{1/2} \mathrm{N}(I).$$

Proof. We view the ideal I via the map $\Phi : O_F \longrightarrow V_F$ as a lattice in $V_F = \mathbf{R}^{r_1} \times \mathbf{C}^{r_2}$. By Prop.8.6*(ii)* the covolume of I in V_F is

$$\mathrm{covol}(I) = 2^{-r_2} \mathrm{N}(I) |\Delta_F|^{1/2}.$$

For any positive real number R we put

$$X(R) = \{(x_1, \ldots, x_{r_1}, y_1, \ldots, y_{r_2}) \in \mathbf{R}^{r_1} \times \mathbf{C}^{r_2} : |x_1| + \ldots + |x_{r_1}| + 2|y_1| + \ldots + 2|y_{r_2}| \le R\}.$$

Using the triangle inequality one easily verifies that $X(R)$ is a convex, symmetric and bounded set. By Lemma 10.2 its volume is given by

$$\mathrm{vol}(X(R)) = \frac{R^n}{n!} \left(\frac{\pi}{2}\right)^{r_2} 2^{r_1}.$$

From Minkowski's convex body Theorem 10.1 we conclude that *if*

$$\frac{R^n}{n!} \left(\frac{\pi}{2}\right)^{r_2} 2^{r_1} > 2^n \cdot 2^{-r_2} \mathrm{N}(I) |\Delta_F|^{1/2}$$

then there exists a non-zero element $x \in I \cap X(R)$. Since for every R the set $X(R)$ is bounded, and since the set $I \cap X(R)$ is finite, it follows that there is a vector $x \in I$ such that $x \in X(R)$ for *every* R satisfying this inequality. Since $X(R_0)$ is closed, this vector x is also contained in $X(R_0)$ where R_0 satisfies the equality

$$\frac{R_0^n}{n!}\left(\frac{\pi}{2}\right)^{r_2} 2^{r_1} = 2^n \cdot 2^{-r_2} N(I)|\Delta_F|^{1/2}.$$

By Prop.3.2*(iii)* and the arithmetic-geometric-mean-inequality (Exer.10.D), we have that

$$\begin{aligned}|\mathrm{N}(x)| &= |x_1| \cdot \ldots |x_{r_1}||y_1|^2 \cdot \ldots \cdot |y_{r_2}|^2,\\ &\leq \left(\frac{|x_1| + \ldots + |x_{r_1}| + 2|y_1| + \ldots + 2|y_{r_2}|}{n}\right)^n,\\ &\leq \frac{R_0^n}{n^n} = \frac{n!}{n^n}\left(\frac{4}{\pi}\right)^{r_2} |\Delta_F|^{1/2}\mathrm{N}(I)\end{aligned}$$

as required.

Corollary 10.4. *Let F be a number field of degree n. Then*
(i)

$$|\Delta_F| \geq \left(\frac{n^n}{n!}(\frac{\pi}{4})^{r_2}\right)^2.$$

(ii) $|\Delta_F| \geq \frac{\pi^n}{4}$. *In particular,* $|\Delta_F| > 1$ *whenever* $F \neq \mathbf{Q}$.
(iii) Every ideal class contains an ideal I with

$$|N(I)| \leq \frac{n!}{n^n}\left(\frac{4}{\pi}\right)^{r_2} |\Delta_F|^{1/2}.$$

(iv) The class group $Cl(O_F)$ is finite.

Proof. *(i)* It follows from the multiplicativity of the norm (Prop.6.2) that for every ideal I and $x \in I$, one has that $|\mathrm{N}(x)| \geq \mathrm{N}(I)$. Combining this with Theorem 10.3 gives *(i)*
(ii) One verifies (by induction) that $n^n \geq 2^{n-1}n!$ for all $n \geq 1$. It follows from *(i)* that

$$|\Delta_F| \geq \left(\frac{n^n}{n!}\right)^2 \left(\frac{\pi}{4}\right)^{2r_2} \geq (2^{n-1})^2 \left(\frac{\pi}{4}\right)^n = \frac{\pi^n}{4}.$$

(iii) Let c be an ideal class. Every ideal class contains integral ideals. Pick an integral ideal J in the inverse of the class of I. By Theorem 10.3 there exists an element $x \in J$ with

$$\left|N(xJ^{-1})\right| \leq \frac{n!}{n^n}\left(\frac{\pi}{4}\right)^{-r_2} |\Delta_F|^{1/2}.$$

Since the ideal xJ^{-1} is integral and in c, the result follows.
(iv) By Prop.6.3*(iii)* there are only a finite number of prime ideals of a given norm. Therefore, for every number B, there are only a finite number of integral ideals of norm less than B. The result now follows from *(iii)*.

The cardinality of the class group $Cl(O_F)$ is called the *class number* of O_F, or of F. It is denoted by

$$h_F = \#Cl(O_F).$$

The expression
$$\frac{n!}{n^n}\left(\frac{4}{\pi}\right)^{r_2}\sqrt{|\Delta_F|}$$
associated to a number field F, with the usual notations, is called the *Minkowski constant* associated to F. Although $n!/n^n \approx e^{-n}\sqrt{2\pi n}$, it grows rapidly with the degree n of F.

The estimate in Cor.10.4*(i)* can be drastically improved when the degree n is large. We only mention the most recent *asymptotic* estimates, i.e. when $n \to \infty$, since these are the easiest to state. Using Stirling's formula is is easy to see that Cor.10.4*(i)* implies that
$$\begin{aligned}|\Delta_F|^{1/n} &\geq \left(\frac{e^2\pi}{4}\right)\left(\frac{4}{\pi}\right)^{\frac{r_1}{n}}\\ &\geq (5.803)(1.273)^{\frac{r_1}{n}}.\end{aligned}$$
Using the Dedekind ζ-function $\zeta_F(s)$ of the number field F and especially its functional equation (see section ?) these estimates were improved by A.M. Odlyzko in 1976:
$$\begin{aligned}|\Delta_F|^{1/n} &\geq (4\pi e^{\gamma})e^{\frac{r_1}{n}},\\ &\geq (22.37)(2.718)^{\frac{r_1}{n}}.\end{aligned}$$
here $\gamma = 0.57721566490153\ldots$ is Euler's constant: $\gamma = \lim_{n\to\infty}(\sum_{k=1}^{n}\frac{1}{k} - \log(n))$.

Odlyzko's estimates are even better if the truth of certain generalized Riemann hypotheses (GRH) is assumed. See Serre's Note [66] and Poitou's Bourbaki talk [60] for more details.
$$\begin{aligned}|\Delta_F|^{1/n} &\geq (8\pi e^{\gamma})(e^{\frac{\pi}{2}})^{\frac{r_1}{n}} \qquad \text{(GRH)},\\ &\geq (44.76)(4.810)^{\frac{r_1}{n}} \qquad \text{(GRH)}.\end{aligned}$$
J. Martinet [51] exhibited an infinite number of totally complex fields F (i.e. with $r_2 = 0$), with $\Delta_F|^{1/n}| = 2^{3/2}11^{4/5}23^{4/5} = 92.37\ldots$. This indicates that Odlyzko's bounds are close to being optimal.

Odlyzko's methods can be used to obtain estimates for discriminants of number fields of *finite* degree as well. This has been done by F. Diaz y Diaz, who published his results in a table [20].

Minkowski's Theorem can be used to calculate class groups of rings of integers of number fields. In the next section we will give some elaborate examples. Here we give two small examples.

Examples. *(i)* Take $F = \mathbf{Q}(\alpha)$ where α is a zero of the polynomial $f(T) = T^3 - T - 1$. In section 2 we have calculated the discriminant Δ_F of F. We have that $\Delta_F = \mathrm{Disc}(f) = -23$. It is easily verified that the polynomial $T^3 - T - 1$ has precisely one real zero. So $r_1 = 1$ and $r_2 = 1$. The bound in Minkowski's Theorem is now
$$\frac{3!}{3^3}\left(\frac{4}{\pi}\right)\sqrt{23} \approx 1.356942.$$
Therefore, by Cor.10.4*(iii)*, every ideal class contains an integral ideal of norm less than or equal to 1. This shows, at once, that the class group of F is trivial. (By Exer.10.R the ring of integers $\mathbf{Z}[\alpha]$ is even Euclidean!)

(ii) Take $F = \mathbf{Q}(\sqrt{-47})$. By the example in section 2, the ring of integers of F is $\mathbf{Z}[\frac{1+\sqrt{-47}}{2}]$ and the discriminant of F satisfies $\Delta_F = -47$. Since $r_1 = 0$ and $r_2 = 1$ we find that the Minkowski constant is equal to
$$\frac{2!}{2^2}\left(\frac{4}{\pi}\right)\sqrt{47} \approx 4.36444.$$

Therefore the class group is generated by the prime ideals of norm less than or equal to 4. To find these prime ideals explicitly, we decompose the primes 2 and 3 in O_F. Let $\alpha = \frac{1+\sqrt{-47}}{2}$. Then $\alpha^2 - \alpha + 12 = 0$. By the Factorization Lemma (Theorem 9.1) we see that $(2) = \mathfrak{p}_2\mathfrak{p}_2'$ where $\mathfrak{p}_2 = (2, \alpha)$ and $\mathfrak{p}_2' = (2, \alpha - 1)$. Similarly $(3) = \mathfrak{p}_3\mathfrak{p}_3'$ where $\mathfrak{p}_3 = (3, \alpha)$ and $\mathfrak{p}_3' = (3, \alpha - 1)$. We conclude that the only ideals of O_F of norm less than 4.36444 are O_F, $\mathfrak{p}_2$, $\mathfrak{p}_2'$, $\mathfrak{p}_3$, $\mathfrak{p}_3'$, $\mathfrak{p}_2^2$, $\mathfrak{p}_2'^2$, $\mathfrak{p}_2\mathfrak{p}_2'$. Therefore the class number is at most 8.

Since $(2) = \mathfrak{p}_2\mathfrak{p}_2'$, the ideal classes of $\mathfrak{p}_2$ and $\mathfrak{p}_2'$ are each others inverses: $\mathfrak{p}_2' \sim \mathfrak{p}_2^{-1}$. Similarly $\mathfrak{p}_3' \sim \mathfrak{p}_3^{-1}$. We conclude that the class group is generated by the classe of $\mathfrak{p}_2$ and $\mathfrak{p}_3$.

In order to determine the class group, we decompose some principal ideals into prime factors. Principal ideals (β) can be factored, by first factoring their norm $N(\beta) \in \mathbf{Z}$ and then determining the prime ideal divisors of (β). For the sake of convenience we take elements β of the form $\beta = \alpha - k$ where $k \in \mathbf{Z}$ is a small integer. By Exer.2.F we have that $\mathrm{N}(\beta) = \mathrm{N}(k - \alpha) = k^2 - k + 12$.

We find

Table.

	k	$\beta =$	$\mathrm{N}(\beta) = k^2 - k + 12$	(β)
(i)	1	$1 - \alpha$	$12 = 2^2 \cdot 3$	$\mathfrak{p}_2'^2\mathfrak{p}_3'$
(ii)	2	$2 - \alpha$	$14 = 2 \cdot 7$	$\mathfrak{p}_2\mathfrak{p}_7$
(iii)	3	$3 - \alpha$	$18 = 2 \cdot 3^2$	$\mathfrak{p}_2'\mathfrak{p}_3^2$
(iv)	4	$4 - \alpha$	$24 = 2^3 \cdot 3$	$\mathfrak{p}_2^3\mathfrak{p}_3$
(v)	5	$5 - \alpha$	$32 = 2^5$	$\mathfrak{p}_2'^5$

From entry (i), we see that the ideal class of $\mathfrak{p}_2'^2\mathfrak{p}_3' \sim (1)$ is trivial. The relation implies that

$$\mathfrak{p}_3 \sim \mathfrak{p}_2^{-1}.$$

We conclude that the class group is *cyclic*. It is generated by the class of $\mathfrak{p}_2$. We will now determine the order of this class. The second entry tells us that $\mathfrak{p}_7 \sim \mathfrak{p}_2^{-1}$ and is not of much use to us. Relation (iii) implies that

$$\mathfrak{p}_2 \sim \mathfrak{p}_3^2.$$

Combining this with the relation obtained from the first entry of our table, gives at once that

$$\mathfrak{p}_2^5 \sim 1.$$

This relation can also be deduced directly from entry (v) of the table. It follows that the class group is cyclic of order 5 or 1. The latter case occurs if and only if the ideal $\mathfrak{p}_2$ is principal. Suppose that for $a, b \in \mathbf{Z}$ the element $\gamma = a + b(1 + \sqrt{-47})/2 \in O_F$ is a generator of $\mathfrak{p}_2$. Since the norm of $\mathfrak{p}_2$ is 2, we must have that

$$2 = \mathrm{N}(\mathfrak{p}_2) = |\mathrm{N}(\gamma)| = a^2 + ab + 12b^2.$$

Writing this equation as $(2a + b)^2 + 47b^2 = 8$, it is immediate that there are no solutions $a, b \in \mathbf{Z}$. We conclude that $\mathfrak{p}_2$ is not principal and that $Cl_{\mathbf{Q}(\sqrt{-47})} \cong \mathbf{Z}/5\mathbf{Z}$.

Corollary 10.6. *(J. uy, French mathematician 1822-1901) For any integer Δ, there are upto isomorphism only finitely many number fields F with $|\Delta_F| = \Delta$.*

Proof. Let $\Delta \in \mathbf{Z}$. By Cor.10.4*(ii)* there are only finitely many possible values for the degree n of F. There is, therefore, no loss in assuming that the degree n is fixed. Let F be a number field of degree n and discriminant Δ. Consider the following, bounded, convex and symmetric box B in $F \otimes \mathbf{R} = \{\mathbf{x} = (x_1, \ldots, x_{r_1}, z_1, \ldots, z_{r_2}) \in \mathbf{R}^{r_1} \times \mathbf{C}^{r_2}\}$:

$$B = \begin{cases} \{\mathbf{x} : |x_1| \le \sqrt{|\Delta|} + 1 \text{ and } |x_i| < 1 \text{ for } i \ne 1\} & \text{if } r_1 > 0, \\ \{\mathbf{x} : |\mathrm{Re}(z_1)| \le 1,\ |\mathrm{Im}(z_1)| \le \sqrt{|\Delta|} + 1 \text{ and } |z_i| < 1 \text{ for } i \ne 1\} & \text{if } r_1 = 0. \end{cases}.$$

It is easily checked that the volume of B is $\pi^{r_2-1}(\sqrt{|\Delta|}+1)$ if $r_1 = 0$ and $2^n(\sqrt{|\Delta|}+1)$ otherwise. In each case $\mathrm{vol}(B)$ exceeds $2^n \mathrm{covol}(O_F)$. By Minkowski's Theorem 10.1, there exists $0 \ne \alpha \in O_F \cap B$. Since $\alpha \ne 0$, we have that $\mathrm{N}(\alpha) \ge 1$. Since $\alpha \in B$, we have that $|\phi_i(\alpha)| < 1$ for all $i > 1$. We conclude that $|\phi_1(\alpha)| \ge 1$.

We claim that $\phi_1(\alpha) \ne \phi_i(\alpha)$ for all $i \ge 2$. This is immediate if $r_1 > 0$, for all $\phi_i(\alpha)$ have absolute values strictly larger than $|\phi_1(\alpha)|$. If $r_1 = 0$, only $\phi_{r_2+1}(\alpha) = \overline{\phi_1(\alpha)}$ has the same absolute value as $\phi_1(\alpha)$. But, if $\phi_{r_2+1}(\alpha) = \phi_1(\alpha)$, then $\phi_1(\alpha)$ would be in $\mathbf{R}$ and hence $|\phi_1(\alpha)| = |\mathrm{Re}(\phi_1(\alpha))| < 1$, which leads to a contradiction.

Let $f(T)$ denote the minimum polynomial $f^{\alpha}_{\mathrm{char}}(T)$ of α. By Prop.2.7*(i)*, the polynomial f has no double zeroes and we conclude from part *(ii)* of the same proposition that $f = f^{\alpha}_{\mathrm{min}}$ and that $F = \mathbf{Q}(\alpha)$.

Since the zeroes $\phi_i(\alpha)$ of $f(T) = f^{\alpha}_{\mathrm{char}}(T) = \prod_i (T - \phi_i(\alpha))$ have absolute values bounded by $\sqrt{|\Delta|}+1$, the coefficients of f can be bounded as well. Since the coefficients are in $\mathbf{Z}$, there are only finitely many possibilities for f and therefore, upto isomorphism, for F. This proves the corollary.

(10.A) Show that $\mathbf{Q}(\sqrt{86})$ has class group isomorphic to $\mathbf{Z}/10\mathbf{Z}$.

(10.B) Show that $\mathbf{Q}(\sqrt{-163})$ has trivial class group and the closely related fact that

$$e^{\pi\sqrt{163}} = 262\,537\,412\,640\,768\,743.999\,999\,999\,999\,2\ldots$$

is "almost" an integer.

(10.C) Compute the structure of the class groups of $\mathbf{Q}(\sqrt{-30})$ and $\mathbf{Q}(\sqrt{-114})$.

(10.D) Show that the class group of $\mathbf{Q}(\alpha)$ where α is a zero of the polynomial $T^3 + T - 1$ is trivial.

(10.E) Compute the class group of $F = \mathbf{Q}(\sqrt{101})$.

(10.F) Prove the arithmetic-geometric-mean inequality: let $a_1, \ldots, a_n \in \mathbf{R}_{\ge 0}$ then

$$(a_1 \cdot \ldots \cdot a_n)^{1/n} \le \frac{a_1 + \ldots + a_n}{n}.$$

The equality holds if and only if $a_1 = \ldots = a_n$.(Hint: let $A = \frac{a_1 + \ldots + a_n}{n}$. Show that $e^{\frac{a_i}{A} - 1} \ge \frac{a_i}{A}$ for every i, with equality if and only if $a_i = A$.)

(10.G) Show that the class group of $\mathbf{Q}(\zeta_{11})$ is trivial.

(10.H) Let $f(T) \in \mathbf{Z}[T]$. Show: if $\mathrm{Disc}(f) = 1$, then $f(T) = (T - k)(T - k - 1)$ for some $k \in \mathbf{Z}$.

(10.I) Show that the ring $\mathbf{Z}[(1 + \sqrt{19})/2]$ is *not* Euclidean, but admits unique factorization.

(10.J) Find all solution $X, Y \in \mathbf{Z}$ of the equation that we encountered in the introduction: $Y^2 = X^3 - 19$.

(10.K) Prove Stirling's Formula:

$$n! = n^n e^{-n} \sqrt{2\pi n} e^{\theta/12n} \qquad \text{for some } \theta \text{ with } 0 < \theta < 1.$$

(10.L) Show that the Diophantine equation $Y^2 = X^3 - 5$ has no solutions $X, Y \in \mathbf{Z}$. (Hint: show that the class group of $\mathbf{Z}[\sqrt{-5}]$ has order 2.)

(10.M)*Show that for every number field F there is a prime that is ramified in F over $\mathbf{Q}$.

(10.N)*Let F be a number field. Show that if

$$\frac{n!}{n^n} \left(\frac{4}{\pi}\right)^{r_2} |\Delta_F|^{1/2} < 2$$

then the ring of integers O_F is a Euclidean for the norm $|\mathrm{N}(x)|$. (Hint: Let $x \in F \otimes \mathbf{R}$. Show, using the notation of the proof of Theorem 10.3, that the set $X(R) \cup (X(R) + x)$ with $R = n$ has a volume which is larger than $2^n \mathrm{covol}(O_F)$. Show that it contains a lattice point.)

11. The Theorem of Dirichlet.

In this section we prove Dirichlet's famous Unit Theorem. Just as in the previous section, this will be done by means of Minkowski's techniques. Dirichlet's original proof (18??) exploited the so-called "box principle".

We introduce *modified* absolute values $\|x\|$ on $\mathbf{R}$ and $\mathbf{C}$:

$$\|x\| = \begin{cases} |x|, & \text{on } \mathbf{R}; \\ |x|^2, & \text{on } \mathbf{C}. \end{cases}$$

Definition. Let F be a number field of degree n with r_1 embeddings $\phi_i : F \hookrightarrow \mathbf{R}$ and r_2 remaining embeddings $\phi_i : F \hookrightarrow \mathbf{C}$. Let the homomorphism Ψ be given by:

$$\begin{aligned} \Psi : O_F^* &\longrightarrow \mathbf{R}^{r_1+r_2} \\ \varepsilon &\mapsto (\log\|\phi_1(\varepsilon)\|, \ldots, \log\|\phi_{r_1+r_2}(\varepsilon)\|) \end{aligned}$$

where $\phi_1, \ldots, \phi_{r_1}$ denote the real embeddings and $\phi_{r_1+1}, \ldots, \phi_{r_1+r_2}$ denote a set of mutually non-conjugate complex embeddings.

Theorem 11.1. *(P. Lejeune-Dirichlet) Using the notation above:*

(i) The kernel of Ψ is finite and equal to μ_F, the group of the roots of unity of F.

(ii) The image of Ψ is a lattice in the space $\{x \in \mathbf{R}^{r_1+r_2} :$ the sum of the coordinates of x is zero$\}$, which is of codimension 1 in $\mathbf{R}^{r_1+r_2}$.

Proof. *(i)* Let $\zeta \in \mu_F$ be a root of unity in F. Then there is an integer $n \neq 0$ such that $\zeta^n = 1$. this implies that $n\Psi(\zeta) = 0$ and hence that $\Psi(\zeta) = 0$. This shows that the roots of unity are in the kernel. Next we show that the kernel of Ψ is finite. This implies that $\ker(\Psi) = \mu_F$.

For any $\varepsilon \in \ker(\Psi)$ we have that $\|\phi(\varepsilon)\| = 1$ for all embeddings $\phi : F \longrightarrow \mathbf{C}$. Viewing O_F via the map Φ of section 2 as a lattice inside the vector space $F \otimes \mathbf{R}$, we see that the kernel of Ψ is contained in the *bounded* set B of points $(x_1, \ldots, x_{r_1}, y_1, \ldots, y_{r_2}) \in \mathbf{R}^{r_1} \times \mathbf{C}^{r_2}$ for which

$$\begin{aligned} |x_i| &\leq 1 \qquad \text{for } 1 \leq i \leq r_1, \\ |y_i| &\leq 1 \qquad \text{for } 1 \leq i \leq r_2. \end{aligned}$$

Example 8.2 implies that $B \cap \Phi(O_F)$ is finite and therefore that $\ker(\Psi)$ is finite as required.

(ii) Let B be any bounded set in $\mathbf{R}^{r_1+r_2}$. Let $B' \subset \mathbf{R}^{r_1+r_2}$ be the box

$$\{(x_1, \ldots, x_{r_1+r_2}) : \quad |x_i| \leq R \quad \text{for } 1 \leq i \leq r_1 + r_2\}$$

where R is so large that $B \subset B'$. The elements $\varepsilon \in O_F^*$ that have $\Psi(\varepsilon) \in B'$ satisfy

$$|\phi_i(\varepsilon)| \leq \begin{cases} \exp(R), & \text{for real immersions } \phi_i; \\ \exp(R/2), & \text{for complex immersions } \phi_i. \end{cases}$$

Viewing O_F via Φ as a lattice in $F \otimes \mathbf{R}$, we see that the elements $\varepsilon \in O_F^*$ that satisfy $\Psi(\varepsilon) \in B'$ are in a bounded box in $F \otimes \mathbf{R}$. Therefore there are only finitely many such ε and a fortiori there are only finitely many elements in $B' \cap \Psi(O_F^*)$. We conclude that $\Psi(O_F^*)$ is *discrete.*

By Exer.4.E, every unit $\varepsilon \in O_F^*$ has $N(\varepsilon) = \pm 1$. Therefore

$$\begin{aligned} 1 = |N(\varepsilon)| &= \prod_{\sigma : F \to \mathbf{C}} |\sigma(\varepsilon)| \\ &= \prod_{i=1}^{r_1+r_2} \|\sigma_i(\varepsilon)\| \end{aligned}.$$

This easily implies that $\Psi(O_F^*)$ is contained in the subspace of $\mathbf{R}^{r_1+r_2}$ of vectors that have the sum of their coordinates equal to zero.

To complete the proof, we must show that $\Psi(O_F^*)$ spans this vector space. This will be done by invoking two lemmas that will be stated and proved *after* the proof of this theorem.

Let $1 \leq i \leq r_1+r_2$. By Lemma 11.2 there exist non-zero integral elements $x_1, x_2, x_3, \ldots \in O_F$, such that $|\mathrm{N}(x_i)|$ is bounded by $\sqrt{|\Delta_F|}+1$ and

$$\|\phi_j(x_1)\| > \|\phi_j(x_2)\| > \|\phi_j(x_3)\| > \ldots \qquad \text{for all } j \neq i.$$

By Prop.6.3*(iv)* there are only finitely many ideals in O_F with bounded norm. This implies that the collection of principal ideals (x_k) is finite. Therefore there exist at least two indices $j < j'$ such that $(x_j) = (x_{j'})$. We define the unit ε_i by

$$\varepsilon_i = \frac{x_{j'}}{x_j}.$$

By construction, ε_i satisfies

$$\|\phi_j(\varepsilon_i)\| < 1 \qquad \text{for all } j \neq i.$$

Consider the matrix with entries $a_{ij} = \log\|\phi_j(\varepsilon_i)\|$ where $1 \leq i, j \leq r_1 + r_2$. It satisfies $a_{ij} < 0$ whenever $i \neq j$ and it satisfies $\sum_j a_{ij} = 0$. Therefore Lemma 11.3 implies that any $(r_1 + r_2 - 1) \times (r_1+r_2-1)$-minor is invertible. This implies that the rank of $(a_{ij})_{i,j}$ is r_1+r_2-1 and the theorem is proved.

Lemma 11.2. *Let F be a number field of degree n. Let $\phi_1, \ldots, \phi_{r_1}$ denote the different homorphisms $F \longrightarrow \mathbf{R}$ and $\phi_{r_1+1}, \ldots, \phi_{r_1+r_2}$ the remaining, pairwise non-conjugate, embeddings $F \longrightarrow \mathbf{C}$. Then there exists for each index $1 \leq i \leq r_1+r_2$ a sequence of integers $\alpha_1, \alpha_2, \alpha_3, \ldots \in O_F - \{0\}$, with $|\mathrm{N}(\alpha_j)| \leq \sqrt{|\Delta_F|}+1$ and*

$$\|\phi_j(\alpha_1)\| > \|\phi_j(\alpha_2)\| > \|\phi_j(\alpha_3)\| > \ldots$$

for all indices $j \neq i$.

Proof. Let i be an index with $1 \leq i \leq r_1 + r_2$. The existence of the α_j is proved by applying Minkowski's theorem to boxes that are "thin" in every direction except in the direction of the i-th coordinate. In this direction the box is so large that its volume is larger than $2^n\mathrm{covol}(O_F)$. We will contruct the integers $\alpha_j \in O_F$ inductively. We take $\alpha_1 = 1$. Suppose that $\alpha_1, \ldots, \alpha_m$ have been constructed. Let $\beta_j = \frac{1}{2}\|\phi_j(\alpha_m)\|$ for $j \neq i$ and let $\beta_i \in \mathbf{R}$ be defined by the relation $\prod_j \beta_j = \sqrt{|\Delta_F|}+1$.

Consider the box

$$B = \{(x_1, \ldots, x_{r_1+r_2}) \in \mathbf{R}^{r_1} \times \mathbf{C}^{r_2} : \|x_j\| \leq \beta_j \text{ for all } j \neq i\}.$$

This is a bounded, symmetric and convex subset of $\mathbf{R}^{r_1} \times \mathbf{C}^{r_2}$. It has volume

$$\mathrm{vol}(B) = \prod_{j=1}^{r_1}(2\beta_j) \prod_{j=r_1+1}^{r_1+r_2}(\pi\beta_j) = 2^{r_1}\pi^{r_2}\left(\sqrt{|\Delta_F|}+1\right)$$

which is easily seen to exceed $2^n 2^{-r_2}\sqrt{|\Delta_F|} = 2^n\mathrm{covol}(O_F)$.

By Minkowski's Theorem 10.1, there is a non-zero element x in $B \cap O_F$, where we view, as usual, O_F as a lattice in the vector space $\mathbf{R}^{r_1} \times \mathbf{C}^{r_2}$ via the map Φ of section 2. We take $\alpha_{m+1} = x$ and we verify that

$$|\mathrm{N}(\alpha_{m+1})| = \prod_{j=1}^{r_1+r_2} \|\phi_j(\alpha_{m+1})\| \leq \prod_{j=1}^{r_1+r_2} \beta_j = \sqrt{|\Delta_F|} + 1,$$
$$\|\phi_j(\alpha_{m+1})\| \leq \beta_j = \frac{1}{2}\|\phi_j(\alpha_m)\| < \|\phi_j(\alpha_m)\|$$

This proves the theorem.

Lemma 11.3. *Let $(a_{ij})_{i,j}$ be an $m \times m$-matrix with real entries. Suppose that*

$$\begin{aligned} a_{ij} &< 0 \qquad \text{when } i \neq j, \\ \sum_j a_{ij} &> 0 \qquad \text{for all } i. \end{aligned}$$

Then $(a_{ij})_{i,j}$ has rank m.

Proof. Suppose that the rank of $(a_{ij})_{i,j}$ is less than m. Then there is a non-trivial relation $\sum_i \lambda_i a_{ij} = 0$ with not all $\lambda_i \in \mathbf{R}$ equal to zero. Suppose λ_k has the largest absolute value of the λ_i. Since we can multiply the relation by -1, we may assume that $\lambda_k > 0$. We have that $\lambda_k \geq \lambda_i$ for all indices i. Therefore $\lambda_k a_{ik} \leq \lambda_i a_{ik}$ for *all* indices i, including $i = k$. Taking the sum over i, we find

$$0 < \lambda_k \sum_{i=1}^{m} a_{ik} = \sum_{i=1}^{m} \lambda_k a_{ik} \leq \sum_{i=1}^{m} \lambda_i a_{ik} = 0.$$

This contradiction proves the lemma.

Corollary 11.4. *Let F be a number field with precisely r_1 distinct embeddings $F \hookrightarrow \mathbf{R}$ and $2r_2$ remaining embeddings $F \hookrightarrow \mathbf{C}$. Then*

(i) There exist a set of so-called fundamental units $\varepsilon_1, \ldots, \varepsilon_{r_1+r_2-1} \in O_F^*$ such that

$$O_F^* = \{\zeta^m \varepsilon_1^{n_1} \cdot \ldots \cdot \varepsilon_{r_1+r_2-1}^{n_{r_1+r_2-1}} : n_1, \ldots, n_{r_1+r_2-1}, m \in \mathbf{Z}\}.$$

(ii) There is an isomorphism of abelian groups

$$O_F^* \cong (\mathbf{Z}/w_F\mathbf{Z}) \times \mathbf{Z}^{r_1+r_2-1}.$$

here w_F denotes the number of roots of unity in F.

Proof. By Theorem 10.6, we can choose $r_1 + r_2 - 1$ units ε_i in O_F^* such that the vectors $\Psi(\varepsilon_i)$ span the lattice $\Psi(O_F^*)$. For an arbitrary unit $u \in O_F^*$ there exist integers $n_1, \ldots, n_{r_1+r_2-1}$ such that

$$\Psi(u) = n_1\Psi(\varepsilon_1) + \ldots + n_{r_1+r_2-1}\Psi(\varepsilon_{r_1+r_2-1})$$

By Theorem 7.6*(i)* we see that $u\varepsilon^{-n_1} \cdot \ldots \cdot \varepsilon_{r_1+r_2-1}^{-n_{r_1+r_2-1}}$ is in the kernel of Ψ and therefore a root of unity. This proves *(i)*. Part *(ii)* follows from the fact that the roots of unity are algebraic integers and form a cyclic group.

Definition 11.5. Let F be a number field of degree n and let $\phi_1, \ldots, \phi_{r_1+r_2}$ be the homomorphisms $F \longrightarrow \mathbf{C}$ as in Definition 2.5. The *regulator* R_F of F is defined by

$$|\det(\log\|\phi_j(\varepsilon_i)\|)_{i,j}|$$

where $\varepsilon_1, \ldots, \varepsilon_{r_1+r_2-1}$ are a set of fundamental units and the ϕ_j run over the homomorphisms in the set $\{\phi_1, \ldots, \phi_{r_1+r_2}\}$ except one.

The regulator R_F of a number field F is well defined. See Exer.11.H*(i)* for a proof that the value of R_F does not depend on the homomorphism ϕ_i that one leaves out in Definition.11.5.

Example 11.6. Consider the field $F = \mathbf{Q}(\sqrt{d})$ where $d \in \mathbf{Z}_{>0}$ We have that $r_1 = 2$ and $r_2 = 0$. It follows from Dirichlet's Unit Theorem that the unit group O_F^* is *larger* than $\{\pm 1\}$. It is easy to see that $\varepsilon = X + Y\sqrt{d} \in O_F$ for some $X, Y \in \mathbf{Z}$ is a unit if and only if $\mathrm{N}(\varepsilon) = X^2 - dY^2 = \pm 1$. Therefore, at least when $d \equiv 2, 3 \pmod 4$, Dirichlet's Unit Theorem implies that the Diophantine Equation

$$X^2 - 94Y^2 = \pm 1$$

has non-trivial solutions $X, Y \in \mathbf{Z}$, i.e., solutions different from the ones with $Y = 0$. This equation is usually called *Pell's Equation.* It is by no means obvious to actually *find* these non-trivial solutions. When $d = 94$, the smallest ones are $X = 2143295$ and $Y = 221064$. Equivalently, the unit group $\mathbf{Z}[\sqrt{94}]^*$ is generated by -1 and $\varepsilon = 2143295 + 221064\sqrt{94}$.

Example 11.7. Consider the field $F = \mathbf{Q}(\sqrt{257})$. We have $r_1 = 2$ and $r_2 = 0$. Since F admits embeddings into $\mathbf{R}$, the group of roots of unity in F is $\{\pm 1\}$. By Dirichlet's Unit Theorem we therefore have that

$$O_F^* \cong \varepsilon^{\mathbf{Z}} \times \{\pm 1\}.$$

We will determine the class group $Cl(O_F)$ and the unit group of O_F together. By Example 4.4, the ring of integers of F is equal to $\mathbf{Z}[\alpha]$ where $\alpha = (1 + \sqrt{257})/2$. By Example 4.7, the discriminant of F is 257. Minkowski's constant for F is easily calculated to be equal to

$$\frac{2!}{2^2}\sqrt{257} \approx 8.01.$$

The minimum polynomial of α is easily seen to be $f(T) = T^2 - T - 64$. We first substitute a few integers n into f. In order to obtain small values of $f(n)$, we choose n close to the zero $(1 + \sqrt{257})/2 \approx 8.5 \in \mathbf{R}$:

Table.

	n	β	$f(n) = \mathrm{N}(\beta)$	(β)
(i)	5	$\alpha - 5$	$-44 = -4 \cdot 11$	${\mathfrak{p}_2'}^2\mathfrak{p}_{11}'$
(ii)	6	$\alpha - 6$	$-34 = -2 \cdot 17$	$\mathfrak{p}_2\mathfrak{p}_{17}$
(iii)	7	$\alpha - 7$	$-22 = -2 \cdot 11$	$\mathfrak{p}_2'\mathfrak{p}_{11}$
(iv)	8	$\alpha - 8$	$-8 = -2^3$	${\mathfrak{p}_2}^3$
(v)	9	$\alpha - 9$	$8 = 2^3$	${\mathfrak{p}_2'}^3$
(vi)	10	$\alpha - 10$	$26 = 2 \cdot 13$	$\mathfrak{p}_2\mathfrak{p}_{13}$
(vii)	11	$\alpha - 11$	$46 = 2 \cdot 23$	$\mathfrak{p}_2'\mathfrak{p}_{23}$

Since none of the numbers $f(n)$ is divisible by 3, 5 or 7, we conclude that f has no zeroes modulo 3, 5 or 7. By the Factorization Lemma 9.1, we conclude that the ideals (3), (5) and (7) are prime in O_F. Therefore, the only primes having norm less than 8.01 in O_F are the prime divisors $\mathfrak{p}_2$ and $\mathfrak{p}_2'$ of 2. From the Factorization Lemma we deduce that $\mathfrak{p}_2 = (\alpha, 2)$ and $\mathfrak{p}_2' = (\alpha - 1, 2)$.

Since the classes of $\mathfrak{p}_2$ and $\mathfrak{p}_2'$ are inverse to one another in the class group, we conclude that the class group of O_F is cyclic. It is generated by the class of $\mathfrak{p}_2$. From entry (iv) or (v) of the table, it is immediate that

$$\mathfrak{p}_2^3 \sim 1$$

and we see that $Cl(O_F)$ is cylic of order 3 or 1. The class group is trivial if and only if $\mathfrak{p}_2$ is principal. If $\mathfrak{p}_2$ were principal and $\gamma = a + b(1+\sqrt{257})/2$, with $a, b \in \mathbf{Z}$ would be a generator, we would have the following equation:

$$\pm 2 = \mathrm{N}(\gamma) = a^2 + ab - 64b^2.$$

This Diophantine equation is not so easy to solve directly, so we proceed in a different way. We will need to know the unit group O_F^* first.

From the 4th and 5th line of the table we deduce the following decomposition into prime ideals:

$$((\alpha - 8)(\alpha - 9)) = {\mathfrak{p}_2}^3 {\mathfrak{p}_2'}^3$$

Since we also have that $(8) = {\mathfrak{p}_2}^3 {\mathfrak{p}_2'}^3$, we see that the principal ideals $((\alpha - 8)(\alpha - 9))$ and (8) are equal. Therefore their generators differ by a unit $\varepsilon \in O_F$. Taking norms, we see that $\mathrm{N}(\varepsilon) = -1$ and we conclude that $\varepsilon \neq \pm 1$. We find, in fact, that

$$\varepsilon = \frac{(\alpha - 8)(\alpha - 9)}{8} = -2\alpha + 17 = 16 - \sqrt{257}.$$

However, it is not clear that ε is a fundamental unit in the sense of Dirichlet's Unit Theorem. It could be that there is another unit $u \in O_F^*$ such that $\varepsilon = \pm u^k$ form some $k \geq 2$. The absolute values of $|\phi_1(\varepsilon)|$ and $|\phi_2(\varepsilon)|$ are $32.0312\ldots$ and $0.0312\ldots$ respectively. If $\varepsilon = \pm u^k$ for $|k| \geq 2$, we would have that $|\phi_1(u)| \leq \sqrt{32.04} \leq 5.7$ and $|\phi_2(u)| \leq \sqrt{0.0312} \leq 0.18$.

Therefore u is contained in the intersection of the lattice $\Phi(O_F) \subset F \otimes \mathbf{R} = \mathbf{R} \times \mathbf{R}$ with the box

$$\{(x_1, x_2) \in \mathbf{R}^2 : |x_1| \leq 5.7 \text{ and } |x_2| \leq 0.18\}.$$

By drawing a picture it easily checked that this intersection contains only the number 0 and we conclude that u cannot exist and that ε and -1 generate the unit group O_F^*.

Suppose the class group $Cl(O_F)$ is trivial. Then we have that $\mathfrak{p}_2 = (\gamma)$ and by entry (iv) of the table that $\gamma^3 = u(\alpha - 8)$ for some unit $u \in O_F^*$. Here γ is only determined upto a unit and, consequently, the unit u is only determined upto a cube of a unit. Since -1 is a cube, we may assume that

$$\gamma^3 = \varepsilon^k(\alpha - 8) \qquad \text{for some } k \in \mathbf{Z}.$$

This implies that for every ideal $I \subset O_F$, which is prime to $\mathfrak{p}_2$, we have that

$$\alpha - 8 = \varepsilon^k \text{ in } (O_F/I)^*/H$$

where H is the subgroup of cubes $((O_F/I)^*)^3$. We test this modulo the ideal $I = (5)\mathfrak{p}_{13}$. Here $\mathfrak{p}_{13} = (13, \alpha - 10) = (13, \alpha + 3)$ as in the table above.

By the Chinese Remainder Theorem we have the following isomorphism of groups

$$(O_F/I)^*/((O_F/I)^*)^3 \cong \mathbf{F}_{13}^*/(\mathbf{F}_{13}^*)^3 \times \mathbf{F}_{25}^*/(\mathbf{F}_{25}^*)^3 \cong \mathbf{Z}/3\mathbf{Z} \times \mathbf{Z}/3\mathbf{Z}.$$

The last isomorphism is not very natural. We first observe that raising to the 4th power induces an isomorphism
$$\mathbf{F}_{13}^*/(\mathbf{F}_{13}^*)^3 \xrightarrow{\cong} \mu_3 = \{1,3,9\} \subset \mathbf{F}_{13}^*$$
and then we choose an isomorphism $\mathbf{Z}/3\mathbf{Z} \cong \mu_3$, for instance by mapping x to 3^x. Similarly, raising to the power 8 gives an isomorphism

$$\mathbf{F}_{25}^*/(\mathbf{F}_{25}^*)^3 \xrightarrow{\cong} \mu_3 = \{1,-\alpha,\alpha^2\} \subset \mathbf{F}_{25}^*.$$

Here we used that $\alpha^2-\alpha+1 \equiv 0 \pmod 5$, so that $-\alpha$ is a primitive cube root of unity. The map $x \mapsto (-\alpha)^x$ gives an isomorphism $\mu_3 \cong \mathbf{Z}/3\mathbf{Z}$.

We want to test whether the image of $\alpha-8$ in $\mathbf{Z}/3\mathbf{Z} \times \mathbf{Z}/3\mathbf{Z}$ under this isomorphism is a multiple of the image of $\varepsilon = -2\alpha+17$.

First we compute the image of $\alpha-8$: modulo $\mathfrak{p}_{13}$ it is congruent to $-3-8 \equiv 2$. Raising this to the 4th power gives $16 \equiv 3$, which maps to $1 \in \mathbf{Z}/3\mathbf{Z}$ by our choice of the isomorphism. Modulo 5, we have that $\alpha-8 \equiv \alpha+2 \in \mathbf{F}_{25} = \mathbf{F}_5(\alpha)$. To compute its 8th power, we observe that $\alpha^2-\alpha+1 \equiv 0 \pmod 5$, so that $\overline{\alpha}+\alpha = 1$ and $\overline{\alpha}\alpha = 1$. Here $\overline{\alpha} = \alpha^5$ is the conjugate of α over $\mathbf{F}_5$. We find
$$\begin{aligned}(\alpha+2)^8 &= (\alpha+2)(\alpha+2)^5(\alpha+2)^2,\\ &= (\alpha+2)(\overline{\alpha}+2)(\alpha^2+4\alpha+4),\\ &= (\alpha\overline{\alpha}+2(\alpha+\overline{\alpha})+4)(\alpha-1+4\alpha+4),\\ &= (1+2+4)(-1+4) = 1.\end{aligned}$$

Since 1 maps to $0 \in \mathbf{Z}/3\mathbf{Z}$, we find that the image of $\alpha-8$ in $\mathbf{Z}/3\mathbf{Z} \times \mathbf{Z}/3\mathbf{Z}$ is equal to $\binom{1}{0}$.

The computation for $\varepsilon = -2\alpha+17$ is entirely similar. We leave it to the reader. The result is that the image of ε is $\binom{1}{1}$. Since this vector is not a scalar multiple of $\binom{1}{0}$, we conclude that $\alpha-8$ is not of the form $u\gamma^3$ for any unit $u \in O_F^*$. Therefore the class group is not trivial and hence cyclic of order 3.

(11.A) Show that the unit group of the ring of integers of $\mathbf{Q}(\sqrt{5})$ is generated by the "golden ratio" $(1+\sqrt{5})/2$.
(11.B) Compute the units of $\mathbf{Q}(\sqrt{229})$ and of $\mathbf{Q}(\sqrt{19})$
(11.C) Show that if the rank of the unit group O_F^* of a number field F is 1, then $[F:\mathbf{Q}] = 2$, 3 or 4.
(11.D) (*Pell's equation.*) Show that for every positive integer d the equation

$$X^2 - dY^2 = 1$$

has solutions $X, Y \in \mathbf{Z}_{>0}$.
(11.E) Let $f(T) \in \mathbf{Z}[T]$ be a monic polynomial all of whose roots in $\mathbf{C}$ are on the unit circle. Show that all roots of f are roots of unity.
(11.F) Let $\eta \in \mathbf{C}$ be a sum of roots of unity. Show that if $|\eta| = 1$, then η is a root of unity.
(11.G) Let F be a number field of degree n. Show that $R_F\sqrt{n} = \mathrm{covol}(O_F^*)$. here we view O_F^* via the map Ψ as a lattice in the subspace of vectors in $\mathbf{R}^{r_1+r_2}$ that have the sum of their
(11.H) Let F be a number field.
(i) Show that the regulator R_F is well defined, i.e. it does not depend on the choice of the embedding $\phi_i : F \to \mathbf{C}$ that was left out in Definiton 11.5.
(ii) For $1 \le i \le r_1+r_2$, let π_i denote the projection of $\mathbf{R}^{r_1+r_2}$ onto the subspace generated by all basis vectors except the i-th. Show that π_i restricted to $\Psi(O_F^*)$ is injective.
(11.I) Show that $\mathbf{Q}(\sqrt{2})^*$ and $\mathbf{Q}(\sqrt[3]{2})^*$ are isomorphic abelian groups.

12. Examples.

In this section we illustrate the theory of the preceding sections by means of three elaborate examples.

Example 12.1. Let $g(T) \in \mathbf{Z}[T]$ be the polynomial

$$g(T) = T^3 + T^2 + 5T - 16.$$

It is easily checked that g has no zeroes in $\mathbf{Z}$. By Gauß's lemma it is therefore irreducible in $\mathbf{Q}[T]$. Let F be the field $\mathbf{Q}[T]/(g(T))$ or, equivalently, let $F = \mathbf{Q}(\alpha)$ where α denotes a zero of $g(T)$. We will calculate the ideal class group of the ring of integers of F.

As we will see below, most of our information about the arithmetic of F will be deduced from the values of g at the first few small integers. Therefore we begin our calculation by computing a table of the values $g(k)$ at the integers k with $-10 \le k \le 9$. The contents of the last column will be explained below.

Table I.

	k	$g(k)$	$(\alpha - k)$
(i)	0	-2^4	$\mathfrak{p}_2^4$
(ii)	1	-3^2	${\mathfrak{p}'_3}^2$
(iii)	2	$2 \cdot 3$	$\mathfrak{p}_2\mathfrak{p}_3$
(iv)	3	$5 \cdot 7$	$\mathfrak{p}_5\mathfrak{p}'_7$
(v)	4	$2^2 \cdot 3 \cdot 7$	$\mathfrak{p}_2^2\mathfrak{p}'_3\mathfrak{p}''_7$
(vi)	5	$3 \cdot 53$	
(vii)	6	$2 \cdot 7 \cdot 19$	$\mathfrak{p}_2\mathfrak{p}_7\mathfrak{p}_{19}$
(viii)	7	$3 \cdot 137$	
(ix)	8	$2^3 \cdot 3 \cdot 5^2$	$\mathfrak{p}_2^3\mathfrak{p}_3{\mathfrak{p}_5}^2$
(x)	9	839	

	k	$g(k)$	$(\alpha - k)$
(xi)	-1	$-3 \cdot 7$	$\mathfrak{p}_3\mathfrak{p}_7$
(xii)	-2	$-2 \cdot 3 \cdot 5$	$\mathfrak{p}_2\mathfrak{p}'_3\mathfrak{p}_5$
(xiii)	-3	-7^2	${\mathfrak{p}''_7}^2$
(xiv)	-4	$-2^2 \cdot 3 \cdot 7$	$\mathfrak{p}_2^2\mathfrak{p}_3\mathfrak{p}'_7$
(xv)	-5	$-3 \cdot 47$	
(xvi)	-6	$-2 \cdot 113$	
(xvii)	-7	$-3 \cdot 5 \cdot 23$	$\mathfrak{p}_3\mathfrak{p}_5\mathfrak{p}_{23}$
(xviii)	-8	$-2^3 \cdot 3^2 \cdot 7$	$\mathfrak{p}_2^3{\mathfrak{p}'_3}^2\mathfrak{p}_7$
(xix)	-9	-709	
(xx)	-10	$-2 \cdot 3 \cdot 7 \cdot 23$	$\mathfrak{p}_2\mathfrak{p}_3\mathfrak{p}''_7\mathfrak{p}'_{23}$

For instance, the fact that none of the values $g(0), g(1), g(2), \ldots, g(10)$ is divisible by 11 implies that g has no zeroes modulo 11. Therefore it is irreducible in $\mathbf{F}_{11}[T]$ and we have another proof that g is irreducible in $\mathbf{Q}[T]$.

To evaluate the *discriminant* of $g(T)$, we compute the sums p_i of the ith powers of its roots. Using Newton's relations (Exer.3.I), these can be expressed in terms of the symmetric polynomials $s_1 = -1$, $s_2 = 5$ and $s_3 = 16$ in the roots of $g(T)$. We have

$$\begin{aligned}
p_0 &= 3,\\
p_1 &= s_1 = -1,\\
p_2 &= -2s_2 + p_1 s_1 = -2 \cdot 5 + (-1) \cdot (-1) = -9,\\
p_3 &= 3s_3 + p_2 s_1 - p_1 s_2 = 3 \cdot 16 + (-9) \cdot (-1) - (-1) \cdot 5 = 62,\\
p_4 &= -4s_4 + p_3 s_1 - p_2 s_2 + p_1 s_3 = -4 \cdot 0 + 62 \cdot (-1) - (-9) \cdot 5 + (-1) \cdot 16 = -33.
\end{aligned}$$

This gives us

$$\det \begin{pmatrix} 3 & -1 & -9 \\ -1 & -9 & 62 \\ -9 & 62 & -33 \end{pmatrix} = -8763 = -3 \cdot 23 \cdot 127$$

Since 8763 is squarefree, the discriminant Δ_F is, by Prop.4.8, equal to -8763, and the ring of integers O_F is equal to $\mathbf{Z}[\alpha]$. It is easily verified that the polynomial $g(T)$ has precisely one zero in $\mathbf{R}$. Therefore $r_1 = 1$ and $r_2 = 1$ as well. We conclude that Minkowski's constant is equal to

$$\frac{3!}{3^3}\frac{4}{\pi}\sqrt{8763} = 26.4864\ldots$$

This implies that the class group of O_F is generated by the classes of the prime ideals of norm less than 26. By Prop.6.3, the prime ideals of O_F all occur in the factorization of the principal ideals (p) of O_F, where p is an ordinary prime number.

With the aid of the values of the polynomial $g(T)$ at the first few integers, given in table I above, we easily find the zeroes of g modulo p. This gives us the factorization of $g(T)$ modulo p. Using the Factorization Lemma 9.1, it is then easy to obtain the factorizations of the ideals (p) in the ring O_F:

Table II.

p	(p)	
2	$\mathfrak{p}_2\mathfrak{p}_4$	$\mathfrak{p}_2 = (\alpha, 2)$ and $\mathfrak{p}_4 = (\alpha^2 + \alpha + 1, 2)$
3	$\mathfrak{p}_3^2\mathfrak{p}_3'$	$\mathfrak{p}_3 = (\alpha + 1, 3)$ and $\mathfrak{p}_3' = (\alpha - 1, 3)$
5	$\mathfrak{p}_5\mathfrak{p}_{25}$	$\mathfrak{p}_5 = (\alpha + 2, 5)$ and $\mathfrak{p}_{25} = (\alpha^2 - \alpha + 2, 5)$
7	$\mathfrak{p}_7\mathfrak{p}_7'\mathfrak{p}_7''$	$\mathfrak{p}_7 = (\alpha + 1, 7)$, $\mathfrak{p}_7' = (\alpha - 3, 7)$ and $\mathfrak{p}_7'' = (\alpha + 3, 7)$
11	(11)	
13	(13)	
17	(17)	
19	$\mathfrak{p}_{19}\mathfrak{p}_{361}$	$\mathfrak{p}_{19} = (\alpha - 6, 19)$
23	$\mathfrak{p}_{23}^2\mathfrak{p}_{23}'$	$\mathfrak{p}_{23} = (\alpha + 7, 23)$ and $\mathfrak{p}_{23}' = (\alpha + 10, 23)$

Now we explain the contents of the third column of Table I. For $k \in \mathbf{Z}$ one has that $g(k) = \mathrm{N}(k-\alpha)$ and hence that $|g(k)|$ is the norm of the principal ideal $(k-\alpha)$. Using these norms and the explicit descriptions of the prime ideals of O_F, given in Table II, it is easy to find the factorization of the principal ideals $(k - \alpha)$.

For instance, since $g(4) = 84 = 2^2 \cdot 3 \cdot 7$, the principal ideal $(\alpha - 4)$ is only divisible by prime ideals with norm a power of 2 or 3 or 7. It remains to decide *which* prime ideals actually occur. Since, by Table II, we have $\alpha - 4 \in \mathfrak{p}_2$ but $\alpha - 4 \notin \mathfrak{p}_4$ we see that $\mathfrak{p}_2$ divides $\alpha - 4$, but $\mathfrak{p}_4$ does not. Similarly, $\mathfrak{p}_3$ does not divide $\alpha - 4$, but $\mathfrak{p}_3'$ does. Finally, the only prime of norm 7 that contains $\alpha - 4$ is $\mathfrak{p}_7''$. We conclude that the factorization of $(\alpha - 4)$ is given by

$$(\alpha - 4) = \mathfrak{p}_2^2\mathfrak{p}_3'\mathfrak{p}_7''.$$

As we have seen above, the class group is generated by the classes of the prime ideals of norm less than 26. Using the relations that are implied by the factorizations of the principal ideals $(\alpha - k)$, we can reduce the number of generators of the class group. For example, entry (xx) tells us that

$$\mathfrak{p}_{23}' \sim (\mathfrak{p}_2\mathfrak{p}_3\mathfrak{p}_7'')^{-1},$$

i.e the ideals $\mathfrak{p}_{23}'$ and $(\mathfrak{p}_2\mathfrak{p}_3\mathfrak{p}_7'')^{-1}$ belong to the same ideal class. This implies that the class of $\mathfrak{p}_{23}'$ is in the group generated by the classes of $\mathfrak{p}_2$, $\mathfrak{p}_3$, and $\mathfrak{p}_7''$. Similarly, entry (xvii) says that

$$\mathfrak{p}_{23} \sim (\mathfrak{p}_3\mathfrak{p}_5)^{-1}.$$

We conclude that the class group is already generated by the classes of the prime ideals dividing the primes $p \leq 19$. Continuing in this way, we can eliminate many of the generators, each time expressing the class of a prime ideal as a product of classes of primes of smaller norm.

By entry (vi), we eliminate $\mathfrak{p}_{19}$; by means of the entries (iii), (iv) and (xi) we eliminate the primes over 7. Entry (xii) implies that $\mathfrak{p}_5$ can be missed as a generator. Since $\mathfrak{p}_{25} \sim \mathfrak{p}_5^{-1}$, we see that $\mathfrak{p}_{25}$ can be missed as well. The prime $\mathfrak{p}_3$ is taken care of by the relation implied by entry (ii). Since $\mathfrak{p}_3' \sim \mathfrak{p}_3^{-2}$ we don't need the prime $\mathfrak{p}_3'$ either. Finally $\mathfrak{p}_4 \sim \mathfrak{p}_2^{-1}$.

We conclude that the class group of O_F is generated by the class of the prime $\mathfrak{p}_2$. Entry (i) implies that

$$\mathfrak{p}_2^4 \sim (1).$$

This shows that the class group is a quotient of $\mathbf{Z}/4\mathbf{Z}$.

Further attempts turn out not to give any new relations This leads us to believe that the class group is perhaps isomorphic to $\mathbf{Z}/4\mathbf{Z}$. To *prove* this, it suffices to show that the ideal $\mathfrak{p}_2^2$ is not principal. Since, by entry (ii) we have that $\mathfrak{p}_3' \sim \mathfrak{p}_3^{-2} \sim \mathfrak{p}_2^2$, this is equivalent to showing that the ideal $\mathfrak{p}_3'$ is not principal.

Suppose $\mathfrak{p}_3' = (\gamma)$ for some $\gamma \in O_F$. By entry (ii) of Table I, we would have that $(\gamma)^2 = (\alpha - 1)$. Therefore

$$\gamma^2 \cdot u = \alpha - 1 \qquad \text{for some unit } u \in O_F^*.$$

In order to show that this cannot happen, we need to know the unit group O_F^*, or, at least, the units modulo squares. By Dirichlet's Unit Theorem, the unit group has rank $r_1 + r_2 - 1$. Since F admits an embedding into $\mathbf{R}$, the only roots of unity in F are ± 1. Therefore

$$O_F^* = \{\pm \varepsilon^k : k \in \mathbf{Z}\}$$

for some unit $\varepsilon \in O_F^*$.

To find a unit different from ± 1, we exploit the *redundancy* in the relations implied by Table I. Consider the principal ideals generated by $(\alpha - 1)(\alpha - 2)^4$ and 9α. Entries (i), (ii) and (iii) of the table imply that both these ideals factor as

$$\mathfrak{p}_2^4 \mathfrak{p}_3^4 {\mathfrak{p}_3'}^2.$$

Therefore $((\alpha - 1)(\alpha - 2)^4) = (9\alpha)$ and

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

is a unit. In fact, its multiplicative inverse is equal to $129\alpha^2 + 346\alpha + 1227$, but we won't use this fact.

Consider the images of ε and -1 under the following homomorphism:

$$\begin{array}{ccccccc} O_F^*/(O_F^*)^2 & \longrightarrow & (O_F/\mathfrak{p}_3)^* \times (O_F/\mathfrak{p}_7)^*/((O_F/\mathfrak{p}_7)^*)^2 & \cong & \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z} \\ \varepsilon & \mapsto & (-1, 4) & \mapsto & (1, 0) \\ -1 & \mapsto & (-1, -1) & \mapsto & (1, 1) \end{array}$$

Since the vectors $\binom{1}{0}$ and $\binom{1}{1}$ are independent, we conclude that ε and -1 generate the unit group O_F^* modulo squares.

Therefore the unit u is, modulo squares, of the form

$$u = \pm \varepsilon^k$$

for some $k \in \mathbf{Z}$. The equation satisfied by α now becomes

$$\pm\varepsilon^k \cdot \gamma^2 = \alpha - 1 \qquad \text{for some } \gamma \in O_F \text{ and } k \in \mathbf{Z}.$$

Consider this equation modulo $\mathfrak{p}_5$. More precisely consider the image in the following group of order 2:

$$(O_F^*/\mathfrak{p}_5)^*/((O_F^*/\mathfrak{p}_5)^*)^2.$$

Since -1 is a square mod 5 and since $\varepsilon \equiv 4 \cdot (-2)^2 - 2 - 13 \equiv 1$ is square modulo $\mathfrak{p}_5$ as well, the left hand side of this equation is trivial. The right hand side, however, is congruent to $-2-1 \equiv 2$ which is *not* a square.

We conclude that the equation has no solutions and hence that the ideal class group is cyclic of order 4.

Example 12.3. (*The Number Field Sieve*) Let $F = \mathbf{Q}(\sqrt[5]{2})$. This number field $\mathbf{Q}(\sqrt[5]{2})$ and its ring of integers have been exploited to factor the 9th Fermat number $2^{512}+1$ into prime factors [*]. See the course on Galois theory for some more details. The discriminant of the minimum polynomial $T^5 - 2$ of $\sqrt[5]{2}$ is easily seen to be equal to $50\,000 = 2^4 5^5$. Since $T^5 - 2$ is an Eisenstein polynomial for the prime 2 and $(T+2)^5 - 2$ is Eisenstein for 5, we conclude from Prop.9.3 that $\mathbf{Z}[\sqrt[5]{2}]$ is the ring of integers of F.

Since the roots of $T^5 - 2$ differ by 5th roots of unity, there is only one embedding $F \hookrightarrow \mathbf{R}$. Therefore $r_1 = 1$ and $r_2 = 2$. Minkowski's constant is equal to

$$\frac{5!}{5^5}\left(\frac{4}{\pi}\right)^2 \sqrt{50\,000} = 13.919\ldots.$$

By Cor.10.4*(iii)*, the class group of F is generated by the ideal classes of the primes of norm less than 13.919. We use the Factorization Lemma 9.1 to determine those primes: we already observed that $T^5 - 2$ and $(T-2)^5 - 2$ are Eisenstein polynomials with respect to the primes 2 and 5 respectively. We conclude that both 2 and 5 are totally ramified in F over $\mathbf{Q}$:

$$(2) = \mathfrak{p}_2^5 \qquad \text{and} \qquad (5) = \mathfrak{p}_5^5.$$

To find the prime ideals of small norm, we study the decomposition of the other primes p in F. This can be done in as in Examle 12.1, but here we proceed differently. Consider the map $\mathbf{F}_p^* \longrightarrow \mathbf{F}_p^*$ given by $x \mapsto x^5$. If $p \not\equiv 1 \pmod 5$, this is a bijection. This implies that in this case the polynomial $T^5 - 2$ has precisely one zero in $\mathbf{F}_p$.In fact,

$$(p) = \begin{cases} \mathfrak{p}_p \mathfrak{p}_{p^2} \mathfrak{p}'_{p^2}, & \text{if } p \equiv -1 \pmod 5. \\ \mathfrak{p}_p \mathfrak{p}_{p^4}, & \text{if } p \equiv 2, 3 \pmod 5. \end{cases}$$

Here $\mathfrak{p}_{p^k}$ denotes a prime ideal of norm p^k.

On the other hand, if $p \equiv 1 \pmod 5$, the map $x \mapsto x^5$ is not bijective. If 2 is a 5th power in $\mathbf{F}_p^*$, then $T^5 - 2$ decomposes as a product of linear factors modulo p. If not, $T^5 - 2$ is irreducible. For instance, $T^5 - 2$ is irreducible mod 11.

We conclude that for $p = 2$, 3, 5, 7 and 13 there is precisely one prime ideal ($\mathfrak{p}_2$, $\mathfrak{p}_3$, $\mathfrak{p}_5$, $\mathfrak{p}_7$ and $\mathfrak{p}_{13}$ respectively) of norm p. These are all the prime ideals of norm less than 13.919. They generate the class group. In order to determine the structure of the class group, we factor some elements of small norm.

Table III.

	p/q	$\beta = p - q\alpha$	$\mathrm{N}(\beta) = p^5 - 2q^5$	(β)
(i)	0	α	-2	$\mathfrak{p}_2$
(ii)	1	$1-\alpha$	-1	(1)
(iii)	-1	$1+\alpha$	-3	$\mathfrak{p}_3$
(iv)	2	$2-\alpha$	$-30 = -2\cdot 3\cdot 5$	$\mathfrak{p}_2\mathfrak{p}_3\mathfrak{p}_5$
(v)	-2	$2+\alpha$	$34 = 2\cdot 17$	$\mathfrak{p}_2\mathfrak{p}_{17}$
(vi)	3	$3-\alpha$	241	$\mathfrak{p}_{241}$
(v)	-3	$3+\alpha$	$-245 = -5^27$	${\mathfrak{p}_5}^2\mathfrak{p}_7$
(vii)	$1/2$	$1-2\alpha$	$-63 = -3^27$	${\mathfrak{p}_3}^2\mathfrak{p}_7$
(viii)	$-1/2$	$1+2\alpha$	$65 = 5\cdot 13$	$\mathfrak{p}_5\mathfrak{p}_{13}$

By relation (viii), the ideal $\mathfrak{p}_{13}\mathfrak{p}_5$ is principal. This implies that

$$\mathfrak{p}_{13} \sim \mathfrak{p}_5^{-1}$$

i.e. the ideal class of $\mathfrak{p}_{13}$ is equal to the class of $\mathfrak{p}_5^{-1}$. Therefore, the ideal class group of F is already generated by the classes of $\mathfrak{p}_2$, $\mathfrak{p}_3$, $\mathfrak{p}_5$ and $\mathfrak{p}_7$. In a similar way, by considering the relations (vii) and (iv), we see that $Cl(O_F)$ is, in fact, generated by $\mathfrak{p}_2$ and $\mathfrak{p}_3$. But both these ideals are principal: it follows form entries (i) and (iii) that they are generated by α and $\alpha+1$ respectively. We conclude that the class group of O_F is trivial.

By Dirichlet's Unit Theorem the unit group O_F^* has rank $r_1 + r_2 - 1 = 1 + 2 - 1 = 2$. From the table we obtain one unit $\alpha - 1 = \sqrt[5]{2} - 1$. It does not seem easy to obtain independent units with small absolute values by extending the table further. Therefore we search, by brute force, among elements of the form $x = a + b\alpha + c\alpha^2$ with $a, b, c \in \mathbf{Z}$. By Prop.3.2*(iii)* one has that

$$\mathrm{N}(x) = \left(a + b\sqrt[5]{2} + c\sqrt[5]{4}\right)\left|a + b\sqrt[5]{2}e^{\frac{2\pi i}{5}} + c\sqrt[5]{4}e^{\frac{4\pi i}{5}}\right|^2\left|a + b\sqrt[5]{2}e^{\frac{4\pi i}{5}} + c\sqrt[5]{4})e^{\frac{8\pi i}{5}}\right|^2.$$

Calculating a few values of $\mathrm{N}(a + b\alpha + c\alpha^2)$ with $|a|, |b|, |c| \le 1$, one finds that $\mathrm{N}(1 - \alpha + \alpha^2) = -3$. It follows from the table that

$$\frac{1 - \alpha + \alpha^2}{\alpha + 1} = \alpha^4 - \alpha^3 + \alpha^2 - 1$$

is a unit.

Example 12.4. Consider the following (randomly selected, Trento, december 1990) polynomial

$$f(T) = T^4 - 2T^2 + 3T - 7 \qquad \in \mathbf{Z}[T].$$

This polynomial is irreducible modulo 2. This follows from the fact that it is an Artin-Schreier polynomial, but it can also, easily, be checked directly. We will study the number field $F = \mathbf{Q}(\alpha)$, where α is a zero of $f(T)$.

First of all we substitute all integers n with $-18 \le n \le 18$ in $f(T)$ and factor the result into a product of prime numbers:

Table IV.

n	$f(n)=\mathrm{N}(n-\alpha)$
0	-7
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	$149\cdot 337$

n	$f(n)=\mathrm{N}(n-\alpha)$
0	-7
-1	-11
-2	-5
-3	47
-4	$5\cdot 41$
-5	$7\cdot 79$
-6	$11\cdot 109$
-7	$5^2\cdot 7\cdot 13$
-8	$31\cdot 127$
-9	$5\cdot 19\cdot 67$
-10	$13\cdot 751$
-11	$83\cdot 173$
-12	$5\cdot 7\cdot 11\cdot 53$
-13	$19\cdot 1483$
-14	$5^2\cdot 7^2\cdot 31$
-15	50123

To evaluate the discriminant of $f(T)$, we compute the sums p_i of the ith powers of its roots in $\mathbf{C}$ using Newton's relations (Exer.3.I):

$$\begin{aligned}
p_1 &= 0\\
p_2 &= -2s_2 + p_1 s_1 = -2\cdot 2 + 0 = 4\\
p_3 &= 3s_3 + p_2 s_1 - p_1 s_2 = 3\cdot(-3) + 0 + 0 = -9\\
p_4 &= 2p_2 - 3p_1 + 7p_0 = 2\cdot 4 - 0 + 7\cdot 4 = 36\\
p_5 &= 2p_3 - 3p_2 + 7p_1 = 2\cdot(-9) - 3\cdot 4 + 0 = -30\\
p_6 &= 2p_4 - 3p_3 + 7p_2 = 2\cdot 36 - 3\cdot(-9) + 7\cdot 4 = 127
\end{aligned}$$

We have that

$$\mathrm{Disc}(f) = \det\begin{pmatrix} 4 & 0 & 4 & -9\\ 0 & 4 & -9 & 36\\ 4 & -9 & 36 & -30\\ -9 & 36 & -30 & 127\end{pmatrix} = -98443$$

which is a prime number. We conclude from Prop.4.8 that $\Delta_F = -98443$ and that $O_F = \mathbf{Z}[\alpha]$. From Exer.4.G we deduce that $(-1)^{r_2} = -1$ and we conclude that $r_2 = 1$ and hence that $r_1 = 2$. Minkowski's constant is equal to

$$\frac{4!}{4^4}\frac{4}{\pi}\sqrt{98443} = 37.45189\ldots.$$

By Minkowski's Theorem, the ideal class group $Cl(O_F)$ is generated by the primes of norm less than $37.451\ldots$. In order to calculate the class group, we determine the primes of small norm first.

We see in Table IV that the polynomial $f(T)$ has no zeroes modulo p for the primes $p = 2, 3, 17, 23$ and 29. We leave the verification that $f(T)$ has no zeroes modulo 37 either, to the reader. By the Factorization Lemma we conclude that there are no prime ideals of norm p for these primes p. It is easily checked that $f(T)$ is irreducible modulo 2 and 3 and that $f(T) \equiv (T-1)(T+2)(T^2-T+1) \pmod 5$. The polynomial T^2-T+1 is irreducible mod 5.

This gives us the following list of all prime ideals of norm less than 37.45...: the ideals (2) and (3) are prime and $(5) = \mathfrak{p}_5\mathfrak{p}'_5\mathfrak{p}_{25}$, where $\mathfrak{p}_5$ and $\mathfrak{p}'_5$ have norm 5 and $\mathfrak{p}_{25}$ is a prime of norm 25. The other primes $\mathfrak{p}_p$ and $\mathfrak{p}'_p$ of norm less 37.45... have prime norm p. They are listed in Table II and are easily computed from Table I.

Table V.

$\mathfrak{p}_5 = (5, \alpha - 1)$	$\mathfrak{p}'_5 = (5, \alpha + 2)$
$\mathfrak{p}_7 = (7, \alpha)$	$\mathfrak{p}'_7 = (7, \alpha - 2)$
$\mathfrak{p}_{11} = (11, \alpha + 1)$	$\mathfrak{p}'_{11} = (11, \alpha - 5)$
$\mathfrak{p}_{13} = (13, \alpha - 3)$	$\mathfrak{p}'_{13} = (13, \alpha - 6)$
$\mathfrak{p}_{19} = (19, \alpha - 6)$	$\mathfrak{p}'_{19} = (19, \alpha + 9)$
$\mathfrak{p}_{31} = (31, \alpha + 8)$	$\mathfrak{p}'_{31} = (31, \alpha + 14)$

The class group is generated by the classes of these primes and the class of $\mathfrak{p}_{25}$. There exist, however, many relations between these classes. In the following table we list the factorizations of some numbers of the form $q - p\alpha$, where $p, q \in \mathbf{Z}$. We have chosen numbers of this form because $\mathrm{N}(q-p\alpha) = p^4 f(q/p)$ can be computed so easily. The factorizations into prime ideals of the principal ideals $(q-p\alpha)$ give rise to relations in the class group. For instance $\mathrm{N}(1-4\alpha) = -2015 = -5\cdot 13\cdot 31$ and $(1 - 4\alpha) = \mathfrak{p}_5\mathfrak{p}_{13}\mathfrak{p}_{31}$. This shows that the ideal class of $\mathfrak{p}_5\mathfrak{p}_{13}\mathfrak{p}_{31}$ is trivial. Therefore the class of $\mathfrak{p}_{31}$ can be expressed in terms of classes of prime ideals of smaller norm:

$$\mathfrak{p}_{31} \sim \mathfrak{p}_5^{-1}\mathfrak{p}_{13}^{-1}.$$

We conclude that the ideal $\mathfrak{p}_{31}$ is not needed to generate the ideal class group. In a similar way one deduces from Table VI below that the ideal classes of the primes of norm 31,19,13 and 11, can all be expressed in terms of ideal classes of primes of smaller norm.

Table VI.

	β	$\mathrm{N}(\beta)$	(β)
(i)	$4\alpha + 1$	$-5 \cdot 31 \cdot 13$	$\mathfrak{p}_5\mathfrak{p}_{13}\mathfrak{p}_{31}$
(ii)	$3\alpha - 2$	-31	$\mathfrak{p}'_{31}$
(iii)	$\alpha - 6$	$5 \cdot 13 \cdot 19$	$\mathfrak{p}_5\mathfrak{p}'_{13}\mathfrak{p}_{19}$
(iv)	$2\alpha - 1$	$-5 \cdot 19$	$\mathfrak{p}'_5\mathfrak{p}'_{19}$
(v)	$\alpha + 7$	$5^2 \cdot 7 \cdot 13$	${\mathfrak{p}'_5}^2\mathfrak{p}'_7\mathfrak{p}'_{13}$
(vi)	$3\alpha - 5$	13	$\mathfrak{p}'_{13}$
(vii)	$\alpha - 3$	$-5 \cdot 13$	$\mathfrak{p}'_5\mathfrak{p}_{13}$
(viii)	$\alpha + 1$	-11	$\mathfrak{p}_{11}$
(ix)	$3\alpha - 4$	$5^2 \cdot 11$	${\mathfrak{p}'_5}^2\mathfrak{p}'_{11}$

We conclude that $Cl(O_F)$ is generated by the primes $\mathfrak{p}_5$, $\mathfrak{p}'_5$, $\mathfrak{p}_7$, $\mathfrak{p}'_7$ and $\mathfrak{p}_{25}$. One does not need entry (vi) to conclude this, but this entry will be useful later.

The primes of norm 5 and 7 are all principal. This follows form the first few lines of Table I. Finally, since $\mathfrak{p}_5\mathfrak{p}'_5\mathfrak{p}_{25} = (5)$, one concludes that $\mathfrak{p}_{25}$ is principal. We have proved that the class group of $\mathbf{Q}(\alpha)$ is trivial.

By Dirichlet's Unit Theorem, the unit group has rank $r_1 + r_2 - 1 = 2 + 1 - 1 = 2$. The group of roots of unity is just $\{\pm 1\}$. In all our calculations, we have not encountered a single unit yet! To find units, it is convenient to calculate the norms of some elements of the form $a + b\alpha + c\alpha^2$ with $a, b, c \in \mathbf{Z}$. This can be done as follows: one calculates approximations of the roots $\alpha_1, \alpha_2, \alpha_3, \overline{\alpha_3}$

of f in $\mathbf{C}$:

$$\begin{aligned}\alpha_1 &= -2.195251731\ldots\\ \alpha_2 &= 1.655743097\ldots\\ \alpha_3 &= .269754317\ldots \pm 1.361277001\ldots i\end{aligned}$$

By Prop.2.7*(iii)* one has that

$$\mathrm{N}(a+b\alpha+c\alpha^2) = \left(a+b\alpha_1+c\alpha_1^2\right)\left(a+b\alpha_2+c\alpha_2^2\right)\left|a+b\alpha_3+c\alpha_3^2\right|^2.$$

Calculating norms of some small elements of the form $a+b\alpha+c\alpha^2$ one soon finds that $\mathrm{N}(1+\alpha-\alpha^2)=5$. This shows that the ideals $1+\alpha-\alpha^2$ and $\mathfrak{p}_5'$ are equal. In Table IV, we read that $\mathfrak{p}_5'=(\alpha+2)$. We conclude that

$$\varepsilon_1 = \frac{1+\alpha-\alpha^2}{\alpha+2} = \alpha^3-2\alpha^2+3\alpha-4$$

is a unit. Similarly one finds that $\mathrm{N}(2-2\alpha+\alpha^2)=65$. One easily checks that $(2-2\alpha+\alpha^2)=\mathfrak{p}_5'\mathfrak{p}_{13}'$. In Table III(vi) we see that $\mathfrak{p}_{13}'=(3\alpha-5)$. We conclude that the principal ideals $(2-2\alpha+\alpha^2)$ and $((\alpha+2)(3\alpha-5))$ are equal. This implies that

$$\varepsilon_2 = \frac{2-2\alpha+\alpha^2}{(3\alpha-5)(\alpha+2)} = \alpha^3+\alpha^2+\alpha+3$$

is a unit.

Rather then proving that the units $\varepsilon_1,\varepsilon_2$ and -1 generate the unit group, we provide merely evidence that these units generate the whole group. For this we use the main results of the *next* section. We use the ζ-function of the field F. Theorem 13.4 gives us an expression for the residue of the Dedekind ζ-function $\zeta_F(s)$ associated to F at $s=1$. Since the Riemann ζ-function $\zeta_{\mathbf{Q}}(s)$ has a residue equal to 1 at $s=1$, one can express the content of Theorem 13.4 as follows

$$\lim_{s\to 1}\frac{\zeta_F(s)}{\zeta_{\mathbf{Q}}(s)} = \frac{2^{r_1}(2\pi)^{r_2}h_F R_F}{w_F\sqrt{|\Delta|}}.$$

Using the Euler product formula for the ζ-functions and ignoring problems of convergence this gives rise to

$$\prod_p \frac{\prod_{\mathfrak{p}|p}\left(1-\frac{1}{\mathrm{N}(\mathfrak{p})}\right)^{-1}}{\left(1-\frac{1}{p}\right)^{-1}} = \frac{2^{r_1}(2\pi)^{r_2}h_F R_F}{w_F\sqrt{|\Delta|}}.$$

We can compute the right hand side: $r_1=2$, $r_2=1$, $w_F=2$ and $\Delta=-98443$. By the calculation above we have that $h_F=1$.

Next we calculate more explicitly the factors in the Euler product on the left hand side. For a given prime p, the factor is

$$\prod_{\mathfrak{p}|p}\left(1-\frac{1}{\mathrm{N}(\mathfrak{p})}\right)^{-1}.$$

To determine it, we must find the way the prime p splits in the extension F over $\mathbf{Q}$. Apart from the ramified prime 98443, there are five possibilities. Using the Factorization Lemma they can be distinguished by the factorization of $f(T)\in\mathbf{F}_p[T]$:

$$(p) = \begin{cases} \textit{(i)}\quad \mathfrak{p}_p\mathfrak{p}_p'\mathfrak{p}_p''\mathfrak{p}_p''', & \text{if } f(T) \text{ has 4 zeroes mod } p,\\ \textit{(ii)}\quad \mathfrak{p}_p\mathfrak{p}_p'\mathfrak{p}_{p^2}, & \text{if } f(T) \text{ has exactly 2 zeroes mod } p,\\ \textit{(iii)}\quad \mathfrak{p}_p\mathfrak{p}_{p^3}, & \text{if } f(T) \text{ has only one zero mod } p,\\ \textit{(iv)}\quad \mathfrak{p}_{p^2}\mathfrak{p}_{p^2}' & \text{if } f(T) \text{ has two irreducible quadratic factors mod } p,\\ \textit{(v)}\quad (p), & \text{if } f(T) \text{ is irreducible mod } p.\end{cases}$$

here $\mathfrak{p}_p$, $\mathfrak{p}_{p^2}$, etc. denote primes of norm p, p^2 etc. We find that

$$\prod_p F(p)^{-1} = \frac{4\pi}{\sqrt{98443}} R_F$$

where

$$\begin{aligned} F(p) &= \left(1-\frac{1}{p}\right)^3 && \text{in case } \textit{(i)},\\ &= \left(1-\frac{1}{p}\right)\left(1-\frac{1}{p^2}\right) && \text{in case } \textit{(ii)},\\ &= \left(1-\frac{1}{p^3}\right) && \text{in case } \textit{(iii)},\\ &= \left(1+\frac{1}{p}\right)\left(1-\frac{1}{p^2}\right) && \text{in case } \textit{(iv)},\\ &= \left(1+\frac{1}{p}+\frac{1}{p^2}+\frac{1}{p^3}\right) && \text{in case } \textit{(v)}. \end{aligned}$$

If we *assume* that the units $\varepsilon_1, \varepsilon_2$ are fundamental, we can compute the regulator using the two real embeddings $\phi_1, \phi_2 : F \hookrightarrow \mathbf{R}$ given by $\alpha \mapsto \alpha_1$ and $\alpha \mapsto \alpha_2$ respectively. This gives

$$R_F = \det\begin{pmatrix} \log|\phi_1(\varepsilon_1)| & \log|\phi_1(\varepsilon_2)| \\ \log|\phi_2(\varepsilon_1)| & \log|\phi_2(\varepsilon_2)| \end{pmatrix} \approx \det\begin{pmatrix} 3.427619209 & 1.600462837 \\ -3.752710586 & 2.479594524 \end{pmatrix} \approx 14.50597965$$

So, assuming that the units $\varepsilon_1, \varepsilon_2$ are fundamental we find that the right hand side of the equation is equal to

$$\frac{4\pi}{\sqrt{98443}} \cdot 14.50597965 \approx 0.5809524077.$$

If the units would *not* be fundamental, the regulator would be k times as small, for some positive integer k. This would imply that the value 0.5809524077 would be replaced by 0.2904762039 or 0.1936508026 or ... etc.

We compute the left hand side by simply evaluating the contribution of the primes less than a certain moderately large number. A short computer program enables one to evaluate this product with some precision. It suffices to count the zeroes of $f(T)$ modulo p. To distinguish between cases *(iv)* and *(v)* one observes that in case *(iv)*, the discriminant of $f(T)$ is a square modulo p, while in case *(v)* it isn't. See Exer.12.?

Using the primes less than 1657 one finds 0.5815983 for the value of the Euler product. This is close to the number 0.5809524077 that we found above. In view of the slow convergence of the Euler product, the error is not unusually large. It is rather unlikely that the final value will be two times, three times or even more times as small. This indicates, but does not prove, that the units ε_1 and ε_2 are indeed fundamental. To *prove* that they are fundamental, one should employ different techniques, related to methods to search for short vectors in lattices.

(12.A) Pick integers $A, B, C, D \in \mathbf{Z}$, satisfying $|A|, |B|, |C|, |D| \leq 4$ until the polynomial $f(T) = T^4 + AT^3 + BT^3 + CT + D$ is irreducible. Let α denote a zero of $F(T)$. Determine the class group of $\mathbf{Q}(\alpha)$.

(12.B) Determine which of the prime ideals in table IV are in which of the four ideal classes of O_F of example 8.3.

(12.C) Exercise on the distinction of the cases *(iv)* and *(v)* above.

(12.D) Exercise on testing whether x is a square modulo p or not.

(12.E) (Lenstra) Determine the class group of the field generated by a zero of the polynomial $T^4 + \ldots$.

(12.F) More polynomials for computations.

13. The class number formula.

In this section we compute the residue in $s = 1$ of the Dedekind ζ-function $\zeta_F(s)$ assoctiated to a number field F. The result involves the class number of the number field and several other arithmetical invariants that we have studied. It is often called the *class number formula.*

The Riemann ζ-function

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s} \qquad (s \in \mathbf{C},\ \mathrm{Re}(s) > 1),$$

is not defined for $s = 1$. In order to study its behavior as $s \to 1$ we consider the partial sums $\sum_{n=1}^{N} n^{-s}$ for $s \in \mathbf{R}_{>1}$ and $N \in \mathbf{Z}_{>0}$. We have

$$\int_1^N \frac{dx}{x^s} \leq \sum_{n=1}^{N} \frac{1}{n^s} \leq 1 + \int_1^N \frac{dx}{x^s}$$

and therefore

$$\frac{1}{s-1}(1 - N^{1-s}) \leq \sum_{n=1}^{N} \frac{1}{n^s} \leq 1 + \frac{1}{s-1}(1 - N^{1-s}).$$

Multiplying by $s - 1$ and letting first N tend to infinity and then s tend to 1, we obtain

$$\lim_{s \to 1} (s-1) \sum_{n=1}^{\infty} \frac{1}{n^s} = 1.$$

In fact, the Riemann ζ-function admits a meromorphic continuation to all of $\mathbf{C}$ with a single pole of order 1 at 1, but we will neither prove nor use this.

In this section we generalize this result to the Dedekind ζ-function $\zeta_F(s)$ associated to a number field F:

$$\zeta_F(s) = \sum_{0 \neq I} \frac{1}{\mathrm{N}(I)^s} = \prod_{\mathfrak{p}} \left(1 - \frac{1}{\mathrm{N}(\mathfrak{p})^s}\right)$$

for $s \in \mathbf{C}$, $\mathrm{Re}(s) > 1$. Here the sum runs over the non-zero ideals of the ring of integers O_F The techniques will be analytical in nature. See Heilbronn's article in [*] or Davenport's book [*] for similar techniques. Like the Riemann ζ-function, the Dedekind ζ-functions admit meromorphic continuations to $\mathbf{C}$ with only a simple pole at 1. The limit $\lim_{s \to 1}(s-1)\zeta_F(s)$, which is given in Theorem 13.1, is equal to the residue of $\zeta_F(s)$ at $s = 1$. See Hecke's Theorem 13.5 for a more complete statement.

Theorem 13.1. *(The Class Number Formula) Let F be a number field and let $\zeta_F(s)$ denote its Dedekind ζ-function. Then*

$$\lim_{s \to 1}(s-1)\zeta_F(s) = \frac{2^{r_1}(2\pi)^{r_2} h_F R_F}{w_F \sqrt{|\Delta_F|}}$$

Here r_1 is the number of homomorphism $F \hookrightarrow \mathbf{C}$ which have their image in $\mathbf{R}$ and $2r_2$ the remaining number of homomorphism $F \hookrightarrow \mathbf{C}$. By h_F we denote the class number of F, by R_F its regulator, by Δ_F, the discriminant and, finally, by w_F, the number of roots of unity in F.

Proof. Let $s \in \mathbf{C}$ with $\mathrm{Re}(s) > 1$. By Prop.6.7, the sum

$$\zeta_F(s) = \sum_{J \neq 0} \frac{1}{\mathrm{N}(J)^s}$$

is absolutely convergent. We rewrite it as

$$\zeta_F(s) = \sum_{C \in Cl(O_F)} \zeta_C(s)$$

where

$$\zeta_C(s) = \sum_{J \in C} \frac{1}{\mathrm{N}(J)^s}.$$

Let C be an ideal class and let $I \in C^{-1}$. The map $J \mapsto IJ$ gives a bijection between the class C and the set of principal ideals (α) contained in I. Therefore we can write

$$\zeta_C(s) = \sum_{(\alpha) \subset I} \frac{1}{\mathrm{N}(\alpha I^{-1})^s} = \mathrm{N}(I) \sum_{(\alpha) \subset I} \frac{1}{|\mathrm{N}\alpha|^s}.$$

In order to calculate this sum, we view the ideal I via the map $\Phi : F \longrightarrow F \otimes \mathbf{R}$ as a lattice in the $\mathbf{R}$-algebra $F \otimes \mathbf{R} = \mathbf{R}^{r_1} \times \mathbf{C}^{r_2}$.

The units of the algebra $F \otimes \mathbf{R}$ are precisely the vectors that have all their coordinates non-zero. We extend the map $\Psi : O_F^* \longrightarrow \mathbf{R}^{r_1+r_2}$ to $(F \otimes \mathbf{R})^*$:

$$\Psi : (\mathbf{R}^{r_1} \times \mathbf{C}^{r_2})^* \longrightarrow \mathbf{R}^{r_1+r_2}$$

by

$$\Psi(x_1, \ldots, x_{r_1}, z_1, \ldots, z_{r_2}) = (\log\|x_1\|, \ldots, \log\|x_{r_1}\|, \log\|z_1\|, \ldots \log\|z_{r_2}\|)$$

and we extend the norm $\mathrm{N} : F \longrightarrow \mathbf{R}$ to $F \otimes \mathbf{R}$ by

$$\mathrm{N}(x_1, \ldots, x_{r_1}, z_1, \ldots, z_{r_2}) = |x_1| \cdot \ldots \cdot |x_{r_1}| \cdot |z_1|^2 \cdot \ldots \cdot |z_{r_2}|^2.$$

The norm is a homogenous polynomial of degree n. Clearly it does not vanish on $(F \otimes \mathbf{R})^*$.

We choose a basis E for the real vector space $\mathbf{R}^{r_1+r_2}$. Choose a system of fundamental units $\varepsilon_1, \ldots, \varepsilon_{r_1+r_2-1}$ and apply the map Ψ. This gives us $r_1 + r_2 - 1$ independent vectors $\Psi(\varepsilon_i)$ that span the subspace of vectors that have the sum of their coordinates equal to zero. The basis E will consist of the vectors $\Psi(\varepsilon_i)$ plus the vector $\mathbf{v} = (1, 1, \ldots, 1, 2, 2, \ldots, 2)$ that has 1's on the real coordinates and 2's on the complex coordinates.

The proof will be a fairly straightforward consequence of three lemmas that will be stated and proved after the proof of Theorem 13.1.

Consider the following set $\Gamma \subset \mathbf{R}^{r_1} \times \mathbf{C}^{r_2}$:

$$\begin{aligned}\Gamma = \{\mathbf{x} \in \mathbf{R}^{r_1} \times \mathbf{C}^{r_2} : {} & \text{the coordinates } \xi_i \text{ of the vectors } \Psi(\mathbf{x}) \text{ with respect to} \\ & \text{the basis } E \text{ satisfy } 0 \leq \xi_i < 1 \text{ for } 1 \leq i \leq r_1 + r_2 - 1; \\ & \text{the first coordinate } x_1 \text{ of } \mathbf{x} \text{ satisfies } 0 \leq \arg(x_1) < \tfrac{2\pi}{w_F}\}.\end{aligned}$$

If $r_1 > 0$, i.e. if the first coordinate x_1 is real, the condition $0 \leq \arg(x_1) < \frac{2\pi}{w_F}$ should be interpreted as $x_1 > 0$. By Lemma 13.2, we have that

$$\zeta_C = \mathrm{N}(I)^s \sum_{\alpha \in I \cap \Gamma} \frac{1}{|\mathrm{N}(\alpha)|^s} \qquad \text{for } s \in \mathbf{C},\ \mathrm{Re}(s) \geq 1.$$

The set Γ is a *cone,* i.e. for all $\mathbf{x} \in \Gamma$ and $\lambda > 0$ also $\lambda\mathbf{x} \in \Gamma$. This can be seen as follows: From

$$\Psi(\lambda\mathbf{x}) = \Psi(\lambda) + \Psi(\mathbf{x}) = \lambda\mathbf{v} + \Psi(\mathbf{x})$$

it follows that, with respect to the basis E, the coordinates of $\Psi(\lambda\mathbf{x})$ and $\Psi(\mathbf{x})$ are equal, except possibly the last. Since $\lambda > 0$, the argument of the first coordinate of $\mathbf{x}$ is also unchanged. This shows that Γ is a cone.

The subset $\Gamma_1 = \{\gamma \in \Gamma : |\mathrm{N}(\gamma)| \le 1\}$ is bounded and has finite volume. Therefore, by Lemmas 13.3 and 13.4, we have that

$$\begin{aligned}\lim_{s\to 1}(s-1)\zeta_C(s) &= \lim_{s\to 1}(s-1)\mathrm{N}(I)^s \sum_{\alpha\in I\cap\Gamma} \frac{1}{|\mathrm{N}(\alpha)|^s}\\ &= \mathrm{N}(I)\frac{\mathrm{vol}(\Gamma_1)}{\mathrm{covol}(I)} = \mathrm{N}(I)\frac{2^{r_1}\pi^{r_2}R_F}{w_F}\frac{2^{r_2}}{\mathrm{N}(I)\sqrt{|\Delta_F|}}.\end{aligned}$$

We see that the result does *not* depend on the ideal class C. Therefore, since there are h_F different ideal classes, we find that

$$\lim_{s\to 1}(s-1)\zeta_F(s) = \sum_C \lim_{s\to 1}(s-1)\zeta_C(s) = h_F\frac{2^{r_1}\pi^{r_2}R_F}{w_F\sqrt{|\Delta|}}$$

as required

It remains to prove the three Lemma's.

Lemma 13.2. *Let F be a number field and let $\Gamma \subset F\otimes\mathbf{R}$ be the cone defined above. Then for a fractional ideal I of F we have that*

$$\sum_{(\alpha)\subset I}\frac{1}{|\mathrm{N}(\alpha)|^s} = \sum_{\alpha\in I\cap\Gamma}\frac{1}{|\mathrm{N}(\alpha)|^s}.$$

(Note that the first sum runs over the principal ideals (α), while the second runs over *elements* α.*)*

Proof. We show first that $(F\otimes\mathbf{R})* = O_F^*\cdot\Gamma$: let $(\mathbf{x} \in F\otimes\mathbf{R})^*$. Write $\Psi(\mathbf{x})$ with respect to the besis E introduced above.

$$\Psi(\mathbf{x}) = \xi_1\Psi(\varepsilon_1) + \ldots + \xi_{r_1+r_2-1}\Psi(\varepsilon_{r_1+r_2-1}) + \xi_{r_1+r_2}\mathbf{v}.$$

Define the unit ε by

$$\varepsilon = \varepsilon_1^{m_i}\ldots\varepsilon_{r_1+r_2}^{m_{r_1+r_2}},$$

where m_i denotes the integral part of ξ_i. As a consequence, the first r_1+r_2-1 coordinates of $\Psi(\varepsilon^{-1}\mathbf{x})$ are between 0 and 1. Next consider the first coordinate y_1 of $\varepsilon^{-1}\mathbf{x}$. Pick a root of unity $\zeta \in F^*$, such that the argument ϕ of ζy_1 satisfies $0 \le \phi < 2\pi/w_F$. We conclude that $\zeta\varepsilon^{-1}\mathbf{x} \in \Gamma$ and hence that $\mathbf{x} \in O_F^*\cdot\Gamma$ as required.

Moreover, this representation of $\mathbf{x} \in (F\otimes\mathbf{R})^*$ is unique: suppose that $\varepsilon\gamma = \varepsilon'\gamma'$ for $\varepsilon\varepsilon' \in O_F^*$ and $\gamma,\gamma' \in \Gamma$. Then $u = \varepsilon/\varepsilon' = \gamma'/\gamma \in O_F^*\cap\Gamma$. This implies at once that the first r_1+r_2-1 coeficients of $\Psi(u)$ are zero. Since u is a unit, the sum of the coefficients is zero and therefore the last coefficient is also zero. this implies that $u \in \ker(\Psi) = \mu_F$. Since the arguments of the first coordinate in $F\otimes\mathbf{R}$ of both γ and γ' are between 0 and $2\pi/w_F$, we conclude that $u = 1$ and the unicity follows.

The lemma now follows from the fact that every principal ideal $(\alpha) \subset F\otimes\mathbf{R}$ has precisely one generator in Γ. Indeed, $\alpha \in (F\otimes\mathbf{R})^*$, so by the above, there is a unique unit ε such that $\varepsilon\alpha \in \Gamma$.

Lemma 13.3. *Let L be a lattice in $\mathbf{R}^n$ and let $\Gamma \subset \mathbf{R}^n$ be a cone. Let N be a homogeneous polynomial of degree, that does not vanish on Γ. Assume that $\Gamma_1 = \{\gamma \in \Gamma : |\mathrm{N}(\gamma)| \leq 1\}$ is bounded and has finite volume. Then*

$$\lim_{s\to 1} \sum_{x\in L\cap\Gamma} \frac{1}{|\mathrm{N}(x)|^s} = \frac{\mathrm{vol}(\Gamma_1)}{\mathrm{covol}(L)}.$$

Proof. Let

$$\nu(r) = \#(\frac{1}{r}L \cap \Gamma_1) = \#\{x \in L : |\mathrm{N}(x)| \leq r^n\}.$$

Since Γ_1 is bounded, $\nu(r)$ is finite. The equality follows from the fact that $\mathrm{N}(x)$ is homogeneous of degree n. By the definiton of the Riemann integral we have that

$$\mathrm{vol}(\Gamma_1) = \lim_{r\to\infty} \nu(r)\mathrm{covol}(\frac{1}{r}L)$$

and, equivalenlty

$$\lim_{r\to\infty} \frac{\nu(r)}{r^n} = \frac{\mathrm{vol}(\Gamma_1)}{\mathrm{covol}(L)}.$$

Next, we enumerate the vectors $\mathbf{x}_1$, $\mathbf{x}_2$, $\mathbf{x}_3$ ... in $\Gamma \cap L$:

$$0 < |\mathrm{N}(\mathbf{x}_1)| \leq |\mathrm{N}(\mathbf{x}_2)| \leq |\mathrm{N}(\mathbf{x}_3)| \leq \ldots$$

and for $k \geq 1$ we put

$$r_k = |\mathrm{N}(\mathbf{x}_k)|^{\frac{1}{n}}.$$

It is immediate that $k \leq \nu(r_k)$ and that for every $\varepsilon > 0$ one has that $\nu(r_k - \varepsilon) \leq k - 1 < k$. Therefore

$$\frac{\nu(r_k-\varepsilon)}{(r_k-\varepsilon)^n}\left(\frac{r_k-\varepsilon}{r_k}\right)^n < \frac{k}{r_k^n} \leq \frac{\nu(r_k)}{r_k^n}$$

and letting $\varepsilon \to 0$ we find that

$$\lim_{k\to\infty} \frac{k}{r_k^n} = \lim_{k\to\infty} \frac{k}{r_k^n} = \lim_{k\to\infty} \frac{v(r_k)}{r_k^n} = \frac{\mathrm{vol}(\Gamma_1)}{\mathrm{covol}(L)} > 0.$$

It follows that for $\varepsilon > 0$ suficiently small and $k_0 \in \mathbf{Z}_{>0}$ sufficiently large, we have for all $k \geq k_0$ that

$$\left(\frac{\mathrm{vol}(\Gamma_1)}{\mathrm{covol}(L)} - \varepsilon\right)\frac{1}{k} < \frac{1}{|\mathrm{N}(\mathbf{x}_k)|} < \left(\frac{\mathrm{vol}(\Gamma_1)}{\mathrm{covol}(L)} + \varepsilon\right)\frac{1}{k}$$

and hence for $s \in \mathbf{R}_{>1}$ that

$$\left(\frac{\mathrm{vol}(\Gamma_1)}{\mathrm{covol}(L)} - \varepsilon\right)^s (s-1)\sum_{k\geq k_0}\frac{1}{k^s} < (s-1)\sum_{k\geq k_0}\frac{1}{|\mathrm{N}(\mathbf{x}_k)|^s} < \left(\frac{\mathrm{vol}(\Gamma_1)}{\mathrm{covol}(L)} + \varepsilon\right)^s (s-1)\sum_{k\geq k_0}\frac{1}{k^s}.$$

Now we let s tend to 1. Since $\lim_{s\to 1}(s-1)\sum_{1\leq k<k_0} 1/k^s = 0$, and the fact that the Riemann ζ-function $\zeta(s) = \sum_{k=1}^{\infty} 1/k^s$ has a pole of order 1 at $s = 1$ with residue 1, we obtain that for sufficiently small $\varepsilon > 0$

$$\frac{\mathrm{vol}(\Gamma_1)}{\mathrm{covol}(L)} - \varepsilon < \lim_{s\to 1}\sum_{k=1}^{\infty}\frac{1}{|\mathrm{N}(\mathbf{x}_k)|^s} < \frac{\mathrm{vol}(\Gamma_1)}{\mathrm{covol}(L)} + \varepsilon.$$

This proves the lemma.

Lemma 13.3. *Let F be a number field and let $\Gamma \subset F \otimes \mathbf{R}$ be the cone defined above. Then*
(i)
$$\mathrm{vol}(\Gamma_1) = \frac{2^{r_1}\pi^{r_2} R_F}{w_F}.$$

(ii) Let I be a fractional ideal in F, then the image of I in $F \otimes \mathbf{R}$ satisfies

$$\mathrm{covol}(I) = 2^{-r_2}\mathrm{N}(I)\sqrt{|\Delta_F|}.$$

Proof. The set Γ_1 consists of those vectors $\mathbf{x} = (x_1, \ldots, x_{r_1}, y_1, \ldots, y_{r_2}) \in (F \otimes \mathbf{R})^*$, for which $0 \le \arg(x_1) < \pi/w_F$, for which $\mathrm{N}(\mathbf{x}) \le 1$ and for which $0 \le \xi_1, \ldots, \xi_{r_1+r_2-1} \le 1$, where the ξ_i are defined by

$$\Psi(\mathbf{x}) = \xi_1\Psi(\varepsilon_1) + \ldots + \xi_{r_1+r_2-1}\Psi(\varepsilon_{r_1+r_2-1}) + \xi_{r_1+r_2}\mathbf{v}.$$

It is clear that, if we drop the condition that $0 \le \arg(x_1) < \pi/w_F$, the volume of Γ_1 is multiplied by w_F. If, moreover, we add the conditions that $x_i > 0$ for all real coordinates i, i.e. for $1 \le i \le r_1$, the volume is multiplied by 2^{-r_1}:

$$\begin{aligned}\mathrm{vol}(\Gamma_1) = \frac{2^{r_1}}{w_F}\mathrm{vol}\{\mathbf{x} \in (F \otimes \mathbf{R})^* :& 0 \le \xi_1, \ldots, \xi_{r_1+r_2-1} \le 1 \text{ and } x_1, \ldots, x_{r_1} > 0 \\ & |x_1| \cdot \ldots \cdot |x_{r_1}| \|y_1\| \cdot \ldots \cdot \|y_{r_2}\| \le 1\}.\end{aligned}$$

We use polar coordinates for the complex coordinates: write $z_k = \rho_k e^{i\phi_k}$ and it is convenient to work with $x_{r_1+k} = \rho_k^2$ rather than ρ_k. We find that

$$\mathrm{vol}(\Gamma_1) = \frac{2^{r_1}\pi^{r_2}}{w_F}\int_W dx_1 \cdot \ldots \cdot dx_{r_1+r_2-1}$$

where W is the set of vectors $\mathbf{x} = (x_1, \ldots, x_{r_1+r_2}) \in (F \otimes \mathbf{R})^*$ for which $x_1, \ldots, x_{r_1+r_2} > 0$ and $\sum_{i=1}^{r_1+r_2}\log(x_i) < 0$ and for which

$$\begin{pmatrix} \log(x_1) \\ \vdots \\ \log(x_{r_1+r_2}) \end{pmatrix} = \xi_1\Psi(\varepsilon_1) + \ldots + \xi_{r_1+r_2-1}\Psi(\varepsilon_{r_1+r_2-1}) + \xi_{r_1+r_2}\mathbf{v}$$

with $0 \le \xi_1, \ldots, \xi_{r_1+r_2-1} < 1$.

Observe that $\xi_{r_1+r_2-1} = -\sum_i \log(x_i)$. Clearly, the above integral is most conveniently evaluated by integration with respect to the variables ξ_i. So, we make the change of variables according to the formulas given in the description of the set W. It is not difficult to calculate the Jacobian J of this transformation. One finds

$$\mathrm{vol}(\Gamma_1) = \frac{2^{r_1}\pi^{r_2}}{w_F}\int_0^1 \ldots \int_0^1 \int_{-\infty}^0 |\det(J)| d\xi_1 \ldots d\xi_{r_1+r_2}$$

where

$$J = \begin{pmatrix} x_1\log\|\phi_1(\varepsilon_1)\| & \ldots & x_1\log\|\phi_1(\varepsilon_{r_1+r_2-1})\| & x_1 \\ \vdots & & \vdots & \vdots \\ x_{r_1+r_2}\log\|\phi_{r_1+r_2}(\varepsilon_1)\| & \ldots & x_{r_1+r_2}\log\|\phi_{r_1+r_2}(\varepsilon_{r_1+r_2-1})\| & 2x_{r_1+r_2} \end{pmatrix}.$$

We conclude that

$$\begin{aligned}\mathrm{vol}(\Gamma_1) &= \frac{2^{r_1}\pi^{r_2}}{w_F} R_F \int_0^1 \cdots \int_0^1 \int_{-\infty}^0 n x_1 \cdot \ldots \cdot x_{r_1+r-2} d\xi_1 \ldots d\xi_{r_1+r_2} \\ &= \frac{2^{r_1}\pi^{r_2}}{w_F} R_F n \int_{-\infty}^0 e^{n\xi_{r_1+r_2}} d\xi_{r_1+r_2} = \frac{2^{r_1}\pi^{r_2} R_F}{w_F}.\end{aligned}$$

as required.

Finally, we formulate, without proof, Hecke's Theorem (German mathematician 1887–1947) [26]. Hecke's proof is elaborate. It exploits Θ-functions and their functional equations. Later in 1959, J.T. Tate gave a simpler proof, based on harmonic analysis on adelic groups [9,32]. The Γ-function $\Gamma(s)$ below, is for $s \in \mathbf{C}$, $\mathrm{Re}(s) > 0$ is defined by

$$\Gamma(s) = \int_0^\infty e^{-t} t^s \frac{dt}{t}.$$

Theorem 13.5. *(E. Hecke 1910) Let F be a number field and let $\zeta_F(s)$ denote its Dedekind ζ-function.*

(i) (Euler product.)

$$\zeta_F(s) = \sum_{0 \neq I} \frac{1}{\mathrm{N}(I)^s} = \prod_{\mathfrak{p}} \left(1 - \frac{1}{\mathrm{N}(\mathfrak{p})^s}\right)$$

for $s \in \mathbf{C}$, $\mathrm{Re}(s) > 1$. Here the sum runs over the non-zero ideals of the ring of integers O_F and the product runs over the non-zero prime ideals $\mathfrak{p}$ of this ring.

(ii) (Analytic continuation.) The function $\zeta_F(s)$ admits a meromorphic extension to $\mathbf{C}$. It has only one pole of order 1 at $s = 1$. The residue is

$$\frac{2^{r_1}(2\pi)^{r_2} h_F R_F}{w_F \sqrt{|\Delta|}}$$

where the notation is as in Theorem 13.1.

(iii) (Functional equation.) The function

$$Z(s) = |\Delta_F|^{s/2} \left(\Gamma(\frac{s}{2})\pi^{-s/2}\right)^{r_1} \left(\Gamma(s)(2\pi)^{-s}\right)^{r_2} \zeta_F(s)$$

satisfies $Z(s) = Z(1-s)$.

(iv) (Zeroes.) The ζ-function has zeroes at the negative integers: at the odd ones with multiplicity R_2 and at the even ones with multiplicity r_1+r_2. At $s = 0$ it has a zero of order r_1+r_2-1 with leading coefficient of the Taylor expansion at 0 equal to $-h_F R_F / w_F$. These are the so-called trivial zeroes. All other zeroes ρ satisfy $0 \leq \mathrm{Re}(\rho) \leq 1$.

Proof. We have proved *(i)* in section 6. For a proof of *(ii)* and *(iii)* we refer to Lang's book [32]. Part *(iv)* is a rather easy consequence of the properties of the Γ-function [2].

For the case $F = \mathbf{Q}$, i.e., for the Riemann ζ-function $\zeta(s) = \zeta_{\mathbf{Q}}(s)$, the results in Theorem 13.5 were all proved by Euler and Riemann. Riemann observed that many zeroes ρ of $\zeta(s)$ satisfy $\mathrm{Re}(\rho) = 1/2$ and conjectured that this is true for all non-trivial zeroes. This is the celebrated *Riemann Hypothesis* which is still unproven. Its truth is considered very likely and would have important consequences. A very weak version of it was proved by Hadamard and De la Vallée

Poussin in 1899. They showed that $\mathrm{Re}\,\rho \neq 1$ for every zero ρ of $\zeta(s)$. As an immediate consequence they deduced the famous *Prime Number Theorem [24]:*

$$\#\{p < X : \ p \text{ prime}\} \approx \frac{X}{\log X}.$$

The Riemann Hypothesis has been numerically tested [50]: The $3 \cdot 10^9$ zeroes ρ with $|\mathrm{Im}\,\rho| < 545439823.15\ldots$ all have their real parts equal to $1/2$.

The Generalized Riemann Hypothesis is the statement that for every number field F, all non-trivial zeroes of $\zeta_F(s)$ have their real parts equal to $1/2$. Needless to say, this important conjecture conjecture has not been proved either.

There are analogues of the Riemann ζ-function in algebraic geometry. For some of these functions the analogue of the Riemann Hypothesis has been proved e.g. for zeta functions of curves over finite fields by A. Weil [52] in 1948. This result was extended by P. Deligne [13] to smooth and proper varieties over finite fields in 1973.

In the introduction we mentioned the recent proof by A. Wiles of Fermat's Last Theorem. The most important step in this proof is the proof of an analogue of part *(iii)* of Theorem 13.5 for the ζ-functions associated to *elliptic curves* over $\mathbf{Q}$. See the article by Rubin and Silverberg [45].

(13.A) Show that the Dedekind ζ-function of $\mathbf{Q}(i)$ satisfies

$$\zeta_{\mathbf{Q}(i)}(s)/\zeta_{\mathbf{Q}}(s) = \sum_{\substack{n=1 \\ n \text{ odd}}}^{\infty} \frac{(-1)^{(n-1)/2}}{n^s}.$$

Verify, in a straightforward way, Theorem 13.1 for the Dedekind ζ-function of $\mathbf{Q}(i)$.

(13.B) Verify that the set Γ_1 occurring in the proof of Theorem 13.1, is bounded.

(13.C) The Γ-function $\Gamma(s)$ is for $s \in \mathbf{C}$, $\mathrm{Re}(s) > 0$ is defined by

$$\Gamma(s) = \int_0^\infty e^{-t} t^s \frac{dt}{t}.$$

Show

(i) for every $s \in \mathbf{C}$, $\mathrm{Re}(s) > 0$ one has that $\Gamma(s+1) = s\Gamma(s)$;

(ii) the Γ-function admits a meromorphic extension to $\mathbf{C}$ with poles at $0, -1, -2, \ldots$ of order 1. The residue at $-k$ is $(-1)^k/k!$;

(iii) $\Gamma(s)\Gamma(1-s) = \pi/\sin(\pi s)$ for $s \in \mathbf{C} - \mathbf{Z}$.

(13.D)*Let $\mathbf{F}_q$ be a finite field with q elements. Let $\zeta(s)$ denote the ζ-function of the ring $\mathbf{F}_q[T]$:

$$\zeta_{\mathbf{F}_q(T)}(s) = \sum_{I \neq 0} \frac{1}{\mathrm{N}(I)^s}.$$

(Here the product runs over the non-zero ideals I and $\mathrm{N}(I) = [\mathbf{F}_q[T] : I]$.) Show that

$$\zeta_{\mathbf{F}_q(T)}(s) = \frac{1}{1 - q^{1-s}}.$$

What is the ζ-function of the ring $\mathbf{F}_q[X,Y]/(X^2+Y^2+1)$? (Hint: show that the conic $X^2+Y^2+1=0$ is isomorphic to the projective line over $\mathbf{F}_q$.)

Bibliography

[1] Abrahamowitz and Stegun, *Handbook of Mathematical Functions*, Dover Publ. New York 1965.
[2] Artin, E.: *The Gamma function*, Holt, Rinehart& Winston 1964.
[3] Artin, E. and Tate J.T.: *Class Field Theory*, Benjamin, New York 1967.
[4] Bianchi, L.: *Lezioni sulla teoria dei numeri algebrici*, Zanichelli, Bologna 1923.
[5] Borevič, Z. and Shafarevič, I.: *Number Theory*, Academic Press, London 1966.
[6] Bourbaki, N.: *Algèbre*, Hermann, Paris 1970. Masson, Paris 1981.
[7] Bourbaki, N.: *Eléments d'histoire des mathématiques*, Coll. Histoire de la pensée **4**, Hermann, Paris 1969.
[8] Buhler, J., Crandall, R., Ernvall, R. and Metsänkylä, T.: Irregular primes and cyclotomic invariants to four million, *Math. Comp.* **61**, (1993), 151–154.
[9] Cassels, J.W.S and Fröhlich, A.: *Algebraic Number Theory*, Academic Press, London 1967.
[10] Chatland and Davenport, H.: Euclids algorithm in real quadratic fields, *Canadian J. of Math.*, **2** (1950), 289–296. In: Davenport, H.: *Collected works I*, Academic Press, London 1977, 366–373.
[11] Claborn, L.: Every abelian group is a class group, *Pacific J. of Math.*, **18** (1966), 219–222.
[12] Dedekind, R.: *Gesammelte mathematische Werke*, Vieweg, Braunschweig 1932.
[13] Deligne, P.: La conjecture de Weil I, *Institut des Hautes Etudes Sci. Publ. Math.* **43** (1974), 273–307.
[14] Diaz y Diaz, F.: Tables minorant la racine n-ième du discriminant d'un corps de degré n. *Publ. Math.*, Orsay 1980.
[15] *Diophanti Alexandrini Opera Omnia ...*, éd. P. Tannery, Teubner, Lipsiae 1893–1895.
[16] Edwards, H.M.: *Riemann's zeta function*, Academic Press, New York 1974.
[17] Edwards, H.: *Fermat's last theorem, a genetic introduction to algebraic number theory*, Grad. Texts in Math. **50**, Springer-Verlag, New York 1977.
[18] Fermat, P. de: *Œuvres*, Gauthier-Villars, Paris 1891–1922.
[20] Gelbart, S.: An elementary introduction to the Langlands program, *Bulletin of the Amer. Math. Soc.*, **10** (1984), 177–219.
[19] Gauß, C.F.: *Disquisitiones Arithmeticae*, Leipzig 1801.
[21] Gras, M.-N.: Non monogénité de l'anneau des entiers des extensions cycliques de $\mathbf{Q}$ de degré premier $l \geq 5$. *J. of Number Theory*, **23** (1986), 347–353.
[22] Grothendieck, A. et Dieudonné, J.: *Élements de Géométrie Algébrique* EGA I–V, Publ. Math. IHES **4, 8, 11, 17, 20, 24, 28, 32**, (1961–1967)
[23] Grothendieck, A. et Dieudonné, J.: *Séminaire de Géométrie Algébrique*, SGA 1–7, Lecture Notes in Math. **151, 152, 153, 224, 225, 269, 270, 288, 305, 340, 569, 589**, Springer Verlag 1970–1978. (SGA 2: North Holland, Amsterdam 1968)
[24] Hardy, G.H. and Wright, E.M.: *An Introduction to the Theory of numbers*, (4th ed.), Oxford Univ. Press, Oxford 1960.
[25] Hecke, E.: *Vorlesungen über die Theorie der algebraischen Zahlen*, Leipzig 1923. Chelsea, New York 1970.
[26] Hecke, E.: Mathematicshe Werke, Vandenhoeck and Ruprecht, Göttingen 1959.
[27] Hilbert, D.: Die Theorie der algebraischen Zahlkörper, *Jahresbericht Deutsche. Math.-Verein*, **4** (1897), 175–546. (*Gesammelte Abhandlungen I*, Springer-Verlag, Berlin Heidelberg New York 63–363).
[28] Janusz, G.J.: *Algebraic Number Fields*, Academic Press, New York London 1973.
[29] Kolyvagin, V.B.: Euler systems, in *The Grothendieck Festschrift* II, 435–483. Eds. P. Cartier et al., Birkhäuser, Boston 1990.
[30] Kummer, E.E.: *Collected Papers* (ed. by A. Weil), Springer-Verlag, New York 1975.
[31] Lang, S.: *Algebra* (2nd edition), Addison-Wesley, Menlo Park (Ca) 1984.
[32] Lang S.: *Algebraic Number Theory*, Addison-Wesley, Reading MA 1970.
[33] Lejeune-Dirichlet, P.G.: *Werke*, Reimer, Berlin 1889–1897.
[34] Lekkerkerker, C.G. and Gruber, P.: *Geometry of Numbers*, North Holland, Amsterdam 1987.
[35] Lenstra, H.W.: Euclidean number fields. *Math. Intelligencer*, **2** (1979), 6–15 and (1980) 73–77, 99–103.
[36] Lenstra, H.W.: Euclid's algorithm in cyclotomic fields. *J. London Math. Soc*, **10**,(1975), 457–465.
[37] Lenstra, H.W.: *Elementaire Algebraïsche getaltheorie*, Syllabus, Univ. van Amsterdam 1982.

[38] Martinet, J.: Tours de corps de classes et estimations de discriminants, *Invent. Math.* **44**, (1978), 65–73.
[39] Mazur, B.: Modular curves and the Eisenstein ideal, *Publ. Math. IHES*, **47** (1977), 33–186.
[40] Minkowski, H.: *Geometrie der Zahlen.*, Chelsea, New York 1953.
[41] Minkowski, H.: *Gesammelte Abhandlungen*, Chelsea, New York 1967.
[42] Ono, T.: *An introduction to algebraic number theory*, Plenum Press, New York 1990.
[43] Poitou, G.: Minorations de discriminants (d'après Odlyzko). Sém. Bourbaki 1975/1976, Exp. 479, In: Springer Lecture Notes in Math. **567**,(1977), 136–153.
[44] Ribet, K.: ..., *Notices of the Amer. Math.Soc.* **40**, (1993),
[45] Rubin, K. and Silverberg, A.: Wiles' proof of Fermat's Last Theorem, preprint, november 1993.
[46] Samuel, P.: *Théorie algébrique des nombres*, Hermann, Paris 1971.
[47] Serre, J.-P.: Cours d'Arithmétique, Grad. Texts in Math. **7**, Springer-Verlag, Berlin Heidelberg New York 1973.
[48] Stewart, I.N.: *Galois theory*, 2nd edition, Chapman and Hall, London New York 1989.
[49] Stewart, I.N. and Tall, D.O.: *Algebraic number theory*, Chapman and Hall, London 1987.
[50] Van der Lune, J., te Riele, H.J.J. and Winter, D.T.: On the zeroes of the Riemann ζ-function in the critical strip IV, *Math. Comp.* **46** (1986), 667–681.
[51] Washington, L.: *Introduction to cyclotomic fields*, Grad. Texts in Math. **83**, Springer-verlag, New York 1982.
[52] Weil, A.:*Les courbes algébriques et les variétés qui s'en déduissent*, Paris 1948.
[53] Weil, A.: *Number Theory, An approach through history*, Birkhäuser, Boston 1984.