Algebraic Number Theory

Université du Luxembourg

Sara Arias-de-Reyna, Gabor Wiese

Contents

Preface

These are notes of a one-term course (12-14 lectures of 90 min each) taught at the University of Luxembourg for students in the second semester of the Master Programme. The lecture builds on the lecture *Commutative Algebra* from the first semester, the lecture notes of which are available on `http://maths.pratum.net`.
The lecture provides an introduction to the most basic classical topics of (global) algebraic number theory:

- first cases of Fermat's Last Theorem,
- norms, traces and discriminants of field extensions,
- rings of integers,
- ideal arithemtic and ideal class groups,
- Dedekind rings,
- fundamentals of the geometry of numbers,
- finiteness of the class number,
- Dirichlet's Unit Theorem.

In preparing these lectures we used several sources:

- Neukirch: *Algebraische Zahlentheorie*, Springer-Verlag.
- Washington: *Introduction to Cyclotomic Fields*, Springer-Verlag.
- Samuel: *Algebraic Theory of Numbers*.
- Bas Edixhoven: *Théorie algébrique des nombres (2002)*, Lecture notes available on Edixhoven's webpage.
- Peter Stevenhagen: *Number Rings*, Lecture notes available on Stevenhagen's webpage.
- Lecture notes of B.H. Matzat: *Algebra 1,2* (Universität Heidelberg, 1997/1998).
- Lecture notes of lectures on *Algebraische Zahlentheorie* taught at Universität Duisburg-Essen in Winter Term 2009/2010.

1 Fermat's Last Theorem

Nowadays, algebraic number theory has been very far developed and is even applied in real life applications due to its predominant use in cryptography and coding theory. A very important motivation for the development of algebraic number theory was the challenge posed by Pierre de Fermat who claimed (in the 17th century) that for all $n \geq 3$, there are no $x, y, z \in \mathbb{N}_{>0}$ such that

$$x^n + y^n = z^n.$$

However, he did not write a proof, and nowadays we are certain that he did not possess any.
The aim of this motivational part is to prove the following special case (called the *first case* for regular primes) of Fermat's Last Theorem. We follow the presentation in Washington's book *Introduction to Cyclotomic Fields*.

Theorem 1.1. *Let p be an odd prime.*
Assume

$$(H) \qquad p \text{ does not divide the class number of } \mathbb{Q}(\zeta_p) \text{ with } \zeta_p = e^{2\pi i/p}.$$

Then the equation

$$x^p + y^p = z^p$$

does not admit any solution with $x, y, z \in \mathbb{Z}$ such that $p \nmid xyz$.

Only in 1995 Fermat's Last Theorem could be settled in all cases:

Theorem 1.2 (Wiles, Fermat's Last Theorem)**.** *Let $n \geq 3$ be an integer.*
Then the equation

$$x^n + y^n = z^n$$

does not admit any solution with $x, y, z \in \mathbb{Z}$ such that $0 \neq xyz$.

Note that it suffices to prove Fermat's Last Theorem with $n = p$ a prime at least 3; so this is not a restriction. There are two restrictions: $p \nmid xyz$ instead of $0 \neq xyz$; this can be taken care of by more advanced Algebraic Number Theory: the theory of cyclotomic fields. However, it seems that Hypothesis (H) cannot be removed by Algebraic Number Theory only; Wiles had to develop totally new techniques.
Let us explain the Hypothesis (H). This, however, takes some time. We have to recall definitions from Commutative Algebra, and we have to introduce some new ones. Along the way we will state some of the main theorems of this lecture (which will, of course, be proved in the weeks to come).

Definition 1.3. *A* number field *is a finite field extension of* $\mathbb{Q}$.

The field $\mathbb{Q}(\zeta_p)$ is a number field. It is generated by the element ζ_p. In fact ζ_p is integral over $\mathbb{Z}$, i.e. it's the zero of a monic polynomial with coefficients in $\mathbb{Z}$, namely $X^{p-1} + X^{p-2} + \cdots + X + 1$. In order to see this, we multiply this polynomial by $X - 1$ and get $X^p - 1$, which clearly admits ζ_p as zero. As $\zeta_p \neq 1$, we find indeed that ζ_p is a zero of $X^{p-1} + X^{p-2} + \cdots + X + 1$. In fact, this polynomial is irreducible. Thus the field extension $\mathbb{Q}(\zeta_p)/\mathbb{Q}$ is of degree $p - 1$.

Definition 1.4. *Let K be a number field. The* ring of integers *of K is the integral closure of $\mathbb{Z}$ in K, i.e.*

$$\mathbb{Z}_K = \{z \in K \mid z \text{ is integral over } \mathbb{Z}\}.$$

For abbreviation, let us now only write ζ instead of ζ_p.

Proposition 1.5. *(a) The ring of integers of $\mathbb{Q}(\zeta)$ is $\mathbb{Z}[\zeta]$.*

(b) Any subset of $p-1$ elements of $1, \zeta, \zeta^2, \ldots, \zeta^{p-1}$ forms a $\mathbb{Z}$-basis of the free $\mathbb{Z}$-module $\mathbb{Z}[\zeta]$.

(c) The principal ideal $(1-\zeta)$ of $\mathbb{Z}[\zeta]$ is a prime ideal whose $(p-1)$-st power equals (p).

The proof will be given later in this course.
For the sequel, we need an important fact about rings of integers, already announced in the lecture on Commutative Algebra.

Theorem 1.6. *The ring of integers $\mathbb{Z}_K$ of any number field K is a Dedekind ring.*
Moreover, $\mathbb{Z}_K$ is free as a $\mathbb{Z}$-module of rank $[K : \mathbb{Q}]$.

The first part of this theorem has already almost been proved in Commutative Algebra. The only thing we are still lacking is that it is Noetherian. This will be established in the next section, where we introduce linear algebra tools. For that purpose, we will introduce the discriminant of ring/field extensions that generalises the discriminant of polynomials (recall that the discriminant of the polynomial $X^2 + aX + b$ is $a^2 - 4b$, telling us the number of roots).
Dedekind rings have actually been introduced because of their main feature: unique ideal factorisation. Before we explain what that means, we recall the notion of UFD: unique factorisation domain. Those are integral domains such that any non-zero element can be written as a finite product of prime elements. Examples are $\mathbb{Z}$, $K[X_1, \ldots, X_n]$ with K a field, any PID (principal ideal domain), hence also any Euclidean ring. However, $\mathbb{Z}[\zeta]$ is not a UFD for all $p \geq 19$.
We also know simpler examples of rings, even rings of integers of number fields, which are not UFDs.

Example 1.7. *(a) $\mathbb{Z}[\sqrt{-5}]$ is not a UFD because*

$$6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5})$$

are two factorisations into non-associate irreducible elements (that's an easy check). This is the ring of integers of $\mathbb{Q}(\sqrt{-5})$.

(b) In fact, one knows:
The ring of integers of the imaginary quadratic field $\mathbb{Q}(\sqrt{-d})$ with squarefree $d \in \mathbb{N}_{\geq 2}$ is a UFD if and only if $d \in \{1, 2, 3, 7, 11, 19, 43, 67, 163\}$.
This is a celebrated and difficult theorem (proved, among others, by Heilbronn and Baker (fields medal, 1970)), which was only proved at the end of the 1960s. The traditional statement of this theorem is for PIDs, but we use that Dedekind rings which are UFDs are PIDs (the proof is not so hard, but uses things we have not yet established).

For a ring of integers it is thus exceptional if it is a UFD. Most are not so nice. This means:
In general number fields, one cannot make use of arguments involving unique factorisation!. It was Eduard Kummer's idea to **consider *factorisation of ideals* instead of *factorisation of numbers***.
We will prove the following theorem in the lecture:

Theorem 1.8. *Let K be a number field and $\mathbb{Z}_K$ its ring of integers. Then every nonzero ideal $I \lhd \mathbb{Z}_K$ can be written in a unique (up to permutation) way as a product of prime ideals*

$$I = \mathfrak{p}_1 \cdot \mathfrak{p}_2 \cdot \ldots \cdot \mathfrak{p}_r.$$

As in the lecture Commutative Algebra the proof will then follow from a local-global analysis, i.e. we'll study the ideal theory in the localisations of the ring of integers at all maximal ideals, and derive the 'global' result from the local data.
Let us now for a moment dwell on the relation between unique factorisation of numbers and unique factorisations of ideals. Start with $\mathbb{Z}$. In $\mathbb{Z}$ we have unique factorisation of numbers, i.e. any $n \in \mathbb{Z}$ (say positive) can be written in a unique (up to permutation) way as

$$n = p_1 \cdot p_2 \cdot \ldots \cdot p_r$$

with $p_1, p_2, \ldots, p_r$ primes. Taking ideals (all principal, of course) on both sides gives

$$(n) = (p_1) \cdot (p_2) \cdot \ldots \cdot (p_r).$$

This is the unique ideal factorisation of (n) into prime ideals (recall that prime elements generate prime ideals, so that indeed all (p_i) are prime ideals).
Let's now start from the other side. Suppose that we have a number field K with integer ring $\mathbb{Z}_K$. Two nonzero elements $x, y \in \mathbb{Z}_K$ generate the same ideal $(x) = (y)$ if and only if xy^{-1} is a unit in $\mathbb{Z}_K$. Recall that a principal ideal (x) is prime if and only if x is a prime element (that is, for all $a, b \in \mathbb{Z}_K$ such that $x|ab$, one has $x|a$ or $x|b$). Hence, we have the bijection

$$\{ \text{ principal prime ideals of } \mathbb{Z}_K \} \times \mathbb{Z}_K^\times \leftrightarrow \{ \text{ prime elements of } \mathbb{Z}_K \}.$$

This leads to the study of the unit group $\mathbb{Z}_K^\times$. In the lecture, we will prove *Dirichlet's unit theorem* which describes the structure of the unit group completely. It will, however, not be needed to finish the special case of Fermat's Last Theorem.
As we said, $\mathbb{Z}_K$ is in general not a PID. The 'deviation' from being a PID is measured in a very elegant way by the *class group* (or *Picard group*), which we describe now. Consider the set of nonzero ideals of $\mathbb{Z}_K$. Note that one can multiply any pair of its elements to get a third one, and $(1) = \mathbb{Z}_K$ is the neutral element for this multiplication: it is a monoid. The monoid of ideals contains the submonoid of all principal ideals.
By introducing the natural notion of *fractional ideals* in order to define inverses to ideals, one actually obtains the group $\mathcal{I}_K$: the group of all fractional ideals of $\mathbb{Z}_K$; it is abelian and contains the subgroup of principal fractional ideals $\mathcal{P}_K$. The *class group* is the quotient group $\mathrm{CL}_K = \mathcal{I}_K / \mathcal{P}_K$.
Towards the end of the lecture, we will prove the following important result about class groups.

Theorem 1.9. *The class group of any number field is finite.*

Definition 1.10. *The cardinality of the class group of a number field is called the* class number.

Let's now state two simple consequences: the first one tells us how to find back the class of UFDs among all Dedekind rings; the second one will be used in the proof of the special case of Fermat's Last Theorem.

Proposition 1.11. *Let K be a number field.*

(a) $\mathbb{Z}_K$ is a UFD $\Leftrightarrow$ the class number of K is 1.

(b) Let $I \lhd \mathbb{Z}_K$ be a non-zero ideal, and let p be a prime number such that I^p is principal.

If p does not divide the class number of K, then I is a principal ideal.

For the sequel of this section, we need the following characterisation of divisibility of ideals in Dedekind rings.

Lemma 1.12. *Let I, J be non-zero ideals in a Dedekind ring. Then*

$$I \subseteq J \Leftrightarrow J \mid I.$$

Proof of Theorem 1.1. Let us start with a potential solution of the Fermat equation: $x^p + y^p = z^p$. Without loss of generality, we may assume that x, y are coprime, i.e. $\gcd(x, y) = 1$.
By two exercises, we may (and do) also assume

- $p \geq 5$ and
- $x \not\equiv y \mod p$.

We factor the Fermat equation over the number field $\mathbb{Q}(\zeta)$ as follows:

$$z^p = x^p + y^p = \prod_{j=0}^{p-1} (x + \zeta^j y). \tag{1.1}$$

If you have never seen this factorisation, just consider x as a variable and observe that $-\zeta^j y$ are n distinct roots of the polynomial $x^p + y^p$ and recall that a polynomial of degree p over an integral domain has at most p zeros.
If $\mathbb{Z}[\zeta]$ were a UFD, we could prove that the elements $x + \zeta^j y$ are coprime for distinct j and conclude that each $x + \zeta^j y$ is a p-th power. Since $\mathbb{Z}[\zeta]$ is not a UFD in general, we have to proceed differently: we will consider the corresponding equality of principal ideals:

$$(z)^p = \prod_{j=0}^{p-1} (x + \zeta^j y). \tag{1.2}$$

Lemma 1.13. *The principal ideals $(x + \zeta^j y)$ of $\mathbb{Z}[\zeta]$ are pairwise coprime for $j = 0, \ldots, p-1$.*

Proof. Let $i \neq j$ in $\{0, 1, \ldots, p-1\}$ and consider a prime ideal $\mathfrak{p}$ dividing both $(x + \zeta^i y)$ and $(x + \zeta^j y)$, i.e. $x + \zeta^i y \in \mathfrak{p}$ and $x + \zeta^j y \in \mathfrak{p}$, whence

$$\zeta^i y - \zeta^j y = \zeta^i \frac{1 - \zeta^{j-i}}{1 - \zeta}(1 - \zeta)y = \epsilon(1 - \zeta)y \in \mathfrak{p},$$

where $\epsilon = \zeta^i \frac{1-\zeta^{j-i}}{1-\zeta}$ is a unit by an exercise. Hence $\mathfrak{p}$ divides the product of ideals $(1 - \zeta) \cdot (y)$. It follows that either $\mathfrak{p} = (1 - \zeta)$ (because $(1 - \zeta)$ is a prime ideal) or $\mathfrak{p} \mid (y)$, i.e. $y \in \mathfrak{p}$.
Similarly we have

$$\zeta^j(x + \zeta^i y) - \zeta^i(x + \zeta^j y) = \zeta^j(1 - \zeta^{j-i})x = \zeta^j \frac{1 - \zeta^{j-i}}{1 - \zeta}(1 - \zeta)x = \delta(1 - \zeta)x \in \mathfrak{p},$$

where $\delta = \zeta^j \frac{1-\zeta^{j-i}}{1-\zeta}$ is again a unit. Thus we obtain that $\mathfrak{p}$ divides the product of ideals $(1 - \zeta) \cdot (x)$. It follows again that either $\mathfrak{p} = (1 - \zeta)$ or $\mathfrak{p} \mid (x)$.
If $\mathfrak{p} \neq (1-\zeta)$, then we get that $\mathfrak{p}$ divides both (x) and (y). This is excluded because x, y are coprime. We hence find $\mathfrak{p} = (1 - \zeta)$.
Now consider

$$x + y \equiv x + \zeta^i y \equiv 0 \mod \mathfrak{p},$$

where the first congruence is because we work modulo $(1 - \zeta)$, and the second one because we work modulo $\mathfrak{p}$. Because of $(x + y)^{p-1} \equiv 0 \mod \mathfrak{p}^{e-1} = (p)$, it follows that p divides $(x + y)^{p-1}$ and hence p divides $x + y$. Finally we see

$$z^p = x^p + y^p \equiv x + y \equiv 0 \mod p,$$

contradicting the assumption $p \nmid z$. □

We return to the main proof. The coprimeness from the previous lemma allows us to conclude from equation (1.2) that each of the principal ideals $(x + \zeta^j y)$ is a p-th power of some ideal I_j. Now we make use of the assumption on the class number and conclude from Proposition 1.11 that I_j is actually principal, say $I_j = (\alpha_j)$. We thus have

$$(x + \zeta^j y) = (\alpha_j)^p \text{ and thus } x + \zeta^j y = \epsilon_j \alpha_j^p$$

with a unit $\epsilon_j \in \mathbb{Z}[\zeta]$.
In order to continue, we need the following two results:

Proposition 1.14. *Let $\epsilon \in \mathbb{Z}[\zeta]$ be a unit. Then there are $\epsilon_1 \in \mathbb{Q}(\zeta + \zeta^{-1})$ and $r \in \mathbb{Z}$ such that $\epsilon = \zeta^r \epsilon_1$.*

Proof. Omitted. □

Lemma 1.15. *For all $\alpha \in \mathbb{Z}[\zeta]$, there is $a \in \mathbb{Z}$ such that*

$$\alpha^p \equiv a \mod (p).$$

Proof. Write $\alpha = b_0 + b_1\zeta + \cdots + b_{p-2}\zeta^{p-2}$. Then we have

$$\alpha^p \equiv b_0^p + b_1^p\zeta^p + \cdots + b_{p-2}^p\zeta^{p(p-2)} = b_0^p + b_1^p + \cdots + b_{p-2}^p = a \mod (p)$$

with $a = b_0^p + b_1^p + \cdots + b_{p-2}^p \in \mathbb{Z}$. □

We return to the main proof and consider the index $j = 1$ and drop it from the notation. We thus have

$$x + \zeta y = \epsilon\alpha^p.$$

Now by Proposition 1.14, we write $\epsilon = \zeta^r\epsilon_1$ with $\epsilon_1 = \overline{\epsilon_1}$ (complex conjugation). Furthermore, by Lemma 1.15, there is $a \in \mathbb{Z}$ such that $\alpha^p \equiv a \mod (p)$. We summarise

$$x + \zeta y = \zeta^r\epsilon_1\alpha^p \equiv \zeta^r\epsilon_1 a \mod (p).$$

Now we take complex conjugation on both sides

$$x + \zeta^{-1}y = \zeta^{-r}\epsilon_1\overline{\alpha}^p \equiv \zeta^{-r}\epsilon_1 a \mod (p).$$

Combining these two equations, we obtain

$$\zeta^{-r}(x + \zeta y) \equiv \zeta^r(x + \zeta^{-1}y) \mod (p),$$

which we rewrite as

$$x + \zeta y - \zeta^{2r}x - \zeta^{2r-1}y \equiv 0a \mod (p). \tag{1.3}$$

Now we use that any subset of $p-1$ elements of $1, \zeta, \zeta^2, \ldots, \zeta^{p-2}, \zeta^{p-1}$ forms a $\mathbb{Z}$-basis of $\mathbb{Z}[\zeta]$. It is thus natural to distinguish two cases:

(I) The elements $1, \zeta, \zeta^{2r-1}, \zeta^{2r}$ are distinct.

In this case, equation (1.3) implies that both x, y are divisible by p since all coordinates of any multiple of p are multiples of p, when we consider $1, \zeta, \zeta^{2r-1}, \zeta^{2r}$ as part of a $\mathbb{Z}$-basis of $\mathbb{Z}[\zeta]$.

(II) The elements $1, \zeta, \zeta^{2r-1}, \zeta^{2r}$ are not distinct.

We further distinguish cases as follows.

(a) $1 = \zeta^{2r}$

Now equation (1.3) becomes

$$\zeta y - \zeta^{-1}y = (\zeta - \zeta^{-1})y \equiv 0 \mod (p).$$

Since ζ and ζ^{-1} are part of a $\mathbb{Z}$-basis of $\mathbb{Z}[\zeta]$, the coordinates x, y are both divisible by p, contrary to our assumptions.

(b) $1 = \zeta^{2r-1}$ ($\Leftrightarrow \zeta = \zeta^{2r}$)

Now equation (1.3) becomes

$$x + \zeta y - \zeta x - y = (x - y) - \zeta(x - y) \equiv 0 \mod (p).$$

As before, we obtain $x \equiv y \mod p$ contrary to the assumptions at the beginning of the proof.

(c) $\zeta = \zeta^{2r-1}$

Now equation (1.3) becomes

$$x + \zeta y - \zeta^2 x - \zeta y = (1 - \zeta^2)x \equiv 0 \mod (p).$$

As before, we obtain $x \equiv 0 \mod p$ contrary to our assumptions.

This finishes the proof of Theorem 1.1. □

Appendix: The solutions of the Fermat equation for $n = 1, 2, 4$

Let $n \in \mathbb{N}$. The n-th Fermat equation is

$$F_n(a, b, c) = a^n + b^n - c^n.$$

What are the zeros of this equation in the (positive) integers?
$\underline{n = 1:}$ For any ring R, there is the bijection

$$\{(a, b, c) \in R^3 \mid F_1(a, b, c) = 0\} \leftrightarrow R^2,$$

given by sending (a, b, c) with $F_1(a, b, c) = a + b - c = 0$ to (a, b). Its inverse clearly is the map that sends (a, b) to $(a, b, a + b)$. This clearly describes all solutions.
$\underline{n = 2:}$ A triple $(a, b, c) \in \mathbb{N}^3$ such that $F_2(a, b, c) = a^2 + b^2 - c^2 = 0$ is called a *Pythagorean triple*. It is called *primitive* if $\gcd(a, b, c) = 1$ and a is odd (whence b is even). It is an exercise to prove that there is the bijection

$$\{(u, v) \in \mathbb{N}^2 \mid u > v,\ \gcd(u, v) = 1,\ 2 \mid uv\} \leftrightarrow \{(a, b, c) \in \mathbb{N}^3 \mid (a, b, c) \text{ primitive Pythagorean triple }\},$$

sending (u, v) to $(u^2 - v^2, 2uv, u^2 + v^2)$.
$\underline{n = 4:}$

Theorem 1.16. *There is no $(a, b, c) \in \mathbb{N}^3_{>0}$ such that $a^4 + b^4 = c^4$, i.e. F_4 has no solution in positive integers [recall that positive means strictly bigger than 0].*

This will immediately follow from the following Proposition.

Proposition 1.17. *Let $(a, b, c) \in \mathbb{Z}^3$ be such that $a^4 + b^4 = c^2$. Then $abc = 0$.*

Proof. Since the exponents are all even, we can without loss of generality assume that all a, b, c are non-negative. We assume that the assertion of the proposition is wrong and want to get a contradiction. For that we let c be minimal such that there are $a, b > 0$ satisfying $a^4 + b^4 = c^2$.
As c is minimal, we have that $\gcd(a, b, c) = 1$; for, if d is the greatest common divisior, then we have

$$\left(\frac{a}{d}\right)^4 + \left(\frac{b}{d}\right)^4 = \frac{a^4 + b^4}{d^4} = \frac{c^2}{d^4} = \left(\frac{c}{d^2}\right)^2,$$

because d^2 has to divide c.

Now we can reinterpret the equation as (a^2, b^2, c) being a primitive Pythagorean triple (after possibly exchanging a and b so that a^2 is odd). Hence, we may apply the case $n = 2$. This means that there are $u, v \in \mathbb{N}$ such that $u > v$, $\gcd(u, v) = 1$ and

$$a^2 = u^2 - v^2, \quad b^2 = 2uv, \quad c^2 = u^2 + v^2.$$

Hence, $a^2 + v^2 = u^2$, which gives yet another primitive Pythagorean triple, namely (a, v, u) (note that since a is odd, v is even). So, we can again apply $n = 2$ to obtain $r > s$ such that $\gcd(r, s) = 1$ and

$$a = r^2 - s^2, \quad v = 2rs, \quad u = r^2 + s^2.$$

Plugging in we get:

$$b^2 = 2uv = 4urs, \text{ and hence } \left(\frac{b}{2}\right)^2 = urs. \tag{1.4}$$

As $\gcd(u, v) = 1$, we also have that $\gcd(u, rs) = 1$ (note: u is odd). As, furthermore, $\gcd(r, s) = 1$, it follows from Equation (1.4) that u, r and s are squares:

$$u = x^2, \quad r = y^2, \quad s = z^2.$$

They satisfy:

$$x^2 = u = r^2 + s^2 = y^4 + z^4.$$

So, we have found a further solution of our equation. But:

$$c = u^2 + v^2 = x^4 + v^2 > x^4 \geq x,$$

contradicting the minimality of c. □

In this proof, the gcd played an important role and we used at several places that $\mathbb{Z}$ is a unique factorisation domain (UFD), that is, that every non-zero integer is uniquely the product of prime numbers (and -1).

Appendix: Analog of Fermat's Last Theorem over $\mathbb{C}[X]$

In order to illustrate that the above approach (factorising the Fermat equation) actually works IF one happens to be in a UFD, we now work for a moment over $\mathbb{C}[X]$, where this strategy actually succeeds. Recall that $\mathbb{C}[X]$ is a Euclidean ring, just like $\mathbb{Z}$. Below we will show that this strategy also works for the Fermat equation F_3 over $\mathbb{Z}$ because the ring $\mathbb{Z}[\zeta_3]$ with $\zeta_3 = e^{2\pi i/3}$ is a unique factorisation domain and has 'few' roots of unity.

Theorem 1.18. *Let $n \geq 3$ and let $a, b, c \in \mathbb{C}[X]$ be such that $a^n + b^n = c^n$. Then a, b and c form a trivial solution: they are scalar multiples of one polynomial ($a(X) = \alpha f(X)$, $b(X) = \beta f(X)$, $c(X) = \gamma f(X)$ for some $f(X) \in \mathbb{C}[X]$ and $\alpha, \beta, \gamma \in \mathbb{C}$).*

Proof. We prove this by obtaining a contradiction. Let us, hence, assume that there are $a, b, c \in \mathbb{C}[X]$ satisfying $a^n + b^n = c^n$ such that

$$\max\{\deg(a), \deg(b), \deg(c)\} > 0 \text{ and is minimal among all solutions.}$$

As $\mathbb{C}[X]$ is factorial (because it is Euclidean), we can always divide out common divisors. Thus, by the minimality assumption the polynomials a, b, c are pairwise coprime. Also note that at most one of the polynomials can be constant, unless we have a trivial solution.
Recall once more that $\mathbb{C}[X]$ is a factorial ring. We are going to use this now, starting from the factorisation

$$c^n = a^n + b^n = \prod_{j=0}^{n-1} (c + \zeta^j b).$$

As $\mathbb{C}[X]$ is a UFD, it makes sense and is natural to ask whether the above factorisation is into pairwise coprime factors. We claim that this is indeed the case. In order to verify this, let $j, k \in \{0, \dots, n-1\}$ be distinct. We have:

$$b = \frac{1}{\zeta^k - \zeta^j}\big((c - \zeta^j b) - (c - \zeta^k b)\big) \text{ and } c = \frac{1}{\zeta^{-j} - \zeta^{-k}}\big(\zeta^{-j}(c - \zeta^j b) - \zeta^{-k}(c - \zeta^k b)\big).$$

Thus, any common divisor of $(c - \zeta^j b)$ and $(c - \zeta^k b)$ necessarily divides both b and c. As these are coprime, the common divisor has to be a constant polynomial, which is the claim.
We now look again at the factorisation and use the coprimeness of the factors. It follows that each factor $c - \zeta^j b$ has to be an n-th power itself, i.e. there are $y_j \in \mathbb{C}[X]$ such that

$$y_j^n = c - \zeta^j b$$

for all $j \in \{0, \dots, n-1\}$. Of course, the coprimeness of the $c - \zeta^j b$ immediately implies that y_j and y_k for $j \neq k$ have no common non-constant divisor. If the degrees of c and b are different, then the degree of y_j is equal to the maximum of the degrees of c and b divided by n for all j. If the degrees are equal, then at most one of the y_j can have degree strictly smaller than the degree of b divided by n because this can only happen if the leading coefficient of c equals ζ^j times the leading coefficient of b. As $n \geq 3$, we can pick three distinct $j, k, \ell \in \{0, \dots, n-1\}$. We do it in such a way that y_j is non-constant. Now consider the equation

$$\alpha y_j^n + \beta y_k^n = \alpha(c + \zeta^j b) + \beta(c + \zeta^k b) = c + \zeta^\ell b = y_\ell^n,$$

which we want to solve for $0 \neq \alpha, \beta \in \mathbb{C}$. Thus, we have to solve

$$\alpha + \beta = 1 \text{ and } \alpha\zeta^j + \beta\zeta^k = \zeta^\ell.$$

A solution obviously is

$$\alpha = \frac{\zeta^\ell - \zeta^k}{\zeta^j - \zeta^k} \text{ and } \beta = 1 - \alpha.$$

In $\mathbb{C}$ we can draw n-th roots: $\alpha = \gamma^n$ and $\beta = \delta^n$. Setting $r = \gamma y_j$, $s = \delta y_k$ and $t = y_\ell$, we obtain

$$r^n + s^n = t^n,$$

with polynomials $r, s, t \in \mathbb{C}[X]$. Let us first remark that r is non-constant. The degrees of r, s, t are less than or equal to the maximum of the degrees of b and c divided by n, hence, the degrees of r, s, t are strictly smaller than the degrees of b and c. As the degree of a has to be at most the maximum of the degrees of b and c, the degrees of r, s, t are strictly smaller than the maximum of the degrees of a, b, c. So, we found another solution with smaller maximum degree. This contradiction proves the proposition. □

2 Linear algebra in field extensions

Let L/K be a field extension, i.e. K is a subfield of L. Recall that multiplication in L makes L into a K-vector space. We speak of a *finite field extension* if $[L : K] := \dim_K(L) < \infty$. Recall, moreover, that an element $a \in L$ is called *algebraic over* K if there is a non-zero polynomial $m_a(X) \in K[X]$ such that $m_a(a) = 0$. If m_a is monic (leading coefficient equal to 1) and irreducible, then m_a is called the *minimal polynomial of* a *over* K. It can be characterised as the unique monic generator of the kernel of the *evaluation map*

$$K[X] \xrightarrow{f(X)\mapsto f(a)} L,$$

which is trivially checked to be a K-algebra homomorphism (i.e. a homomorphism of rings and of K-vector spaces).
We now assume that L/K is a finite extension of degree $[L : K] = n$. Later we will ask it to be separable, too (which is automatic if the characteristic of K (and hence L) is 0). Let $a \in L$. Note that multiplication by a:

$$T_a : L \to L, \quad x \mapsto ax$$

is L-linear and, thus, in particular, K-linear. Once we choose a K-basis of L, we can represent T_a by an $n \times n$-matrix with coefficients in K, also denoted T_a.
Here is the most simple, non-trivial example. The complex numbers $\mathbb{C}$ have the $\mathbb{R}$-basis $\{1, i\}$ and with respect to this basis, any $z \in \mathbb{C}$ is represented as $\left(\begin{smallmatrix} x \\ y \end{smallmatrix}\right) = x + yi$. Now, take $a = \left(\begin{smallmatrix} b \\ c \end{smallmatrix}\right) = b + ci \in \mathbb{C}$. We obtain: $T_a = \left(\begin{smallmatrix} b & -c \\ c & b \end{smallmatrix}\right)$, as we can easily check:

$$T_a(z) = az = (b + ci)(x + yi) = (bx - cy) + (cx + by)i \text{ and } T_a(z) = \left(\begin{smallmatrix} b & -c \\ c & b \end{smallmatrix}\right)\left(\begin{smallmatrix} x \\ y \end{smallmatrix}\right) = \left(\begin{smallmatrix} bx-cy \\ cx+by \end{smallmatrix}\right).$$

As an aside: You may have seen this matrix before; namely, writing $z = r(\cos(\varphi) + i\sin(\varphi))$, it looks like $r\left(\begin{smallmatrix} \cos(\varphi) & -\sin(\varphi) \\ \sin(\varphi) & \cos(\varphi) \end{smallmatrix}\right)$, i.e. it is a rotation matrix times a homothety (stretching) factor.
We can now do linear algebra with the matrix $T_a \in \mathrm{Mat}_n(K)$.

Definition 2.1. *Let L/K be a finite field extension of degree $[L : K] = n$. Let $a \in L$. The* trace of a in L/K *is defined as the trace of the matrix $T_a \in \mathrm{Mat}_n(K)$ and the* norm of a in L/K *is defined as the determinant of the matrix $T_a \in \mathrm{Mat}_n(K)$:*

$$\mathrm{Tr}_{L/K}(a) := \mathrm{Tr}(T_a) \text{ and } \mathrm{Norm}_{L/K}(a) := \det(T_a).$$

Note that trace and norm do not depend on the choice of basis by a standard result from linear algebra.

Let $L/K = \mathbb{C}/\mathbb{R}$ and $z = x + yi \in \mathbb{C}$. Then $\mathrm{Tr}_{\mathbb{C}/\mathbb{R}}(z) = 2x = 2\Re(z)$ and $\mathrm{Norm}_{\mathbb{C}/\mathbb{R}}(z) = x^2 + y^2 = |z|^2$.

Lemma 2.2. *Let L/K be a finite field extension.*

(a) $\mathrm{Tr}_{L/K}$ *defines a group homomorphism $(L, +) \to (K, +)$, i.e.*

$$\mathrm{Tr}_{L/K}(a + b) = \mathrm{Tr}_{L/K}(a) + \mathrm{Tr}_{L/K}(b) \text{ for all } a, b \in L.$$

(b) $\mathrm{Norm}_{L/K}$ *defines a group homomorphism* $(L^\times,\cdot)\to(K^\times,\cdot)$*, i.e.*

$$\mathrm{Norm}_{L/K}(a\cdot b)=\mathrm{Norm}_{L/K}(a)\cdot\mathrm{Norm}_{L/K}(b)\text{ for all }a,b\in L.$$

Proof. (a) The trace of a matrix is additive and $T_{a+b}=T_a+T_b$ because $T_{a+b}(x)=(a+b)x=ax+bx=T_a(x)+T_b(x)$ for all $x\in L$.
(b) The determinant of a matrix is multiplicative and $T_{a\cdot b}=T_a\circ T_b$ because $T_{a\cdot b}(x)=abx=T_a\big(T_b(x)\big)$ for all $x\in L$. □

Lemma 2.3. *Let L/K be a finite field extension of degree $[L:K]=n$. Let $a\in L$.*

(a) Let $f_a=X^n+b_{n-1}X^{n-1}+\cdots+b_1X+b_0\in K[X]$ be the characteristic polynomial of $T_a\in\mathrm{Mat}_n(K)$. Then $\mathrm{Tr}_{L/K}(a)=-b_{n-1}$ and $\mathrm{Norm}_{L/K}(a)=(-1)^nb_0$.

(b) Let $m_a=X^d+c_{d-1}X^{d-1}+\cdots+c_1X+c_0\in K[X]$ be the minimal polynomial of a over K. Then $d=[K(a):K]$ and with $e=[L:K(a)]$ one has $m_a(X)^e=f_a(X)$.

Proof. (a) is a general fact from linear algebra that can, for example, be checked on the Jordan normal form of T_a over an algebraic closure of K, using the fact that trace and determinant are conjugation invariants, that is, do not depend on the choice of basis.
(b) It is obvious that the evaluation map $K[X]\xrightarrow{f(X)\mapsto f(a)}L$ defines a field isomorphism

$$K[X]/(m_a(X))\cong K(a),$$

whence the degree of $[K(a):K]$ equals the degree of $m_a(X)$ and, moreover, $\{1,a,a^2,\dots,a^{d-1}\}$ forms a K-basis of $K(a)$.
We now compute the matrix T_a' for the map $K(a)\xrightarrow{x\mapsto ax}K(a)$ with respect to the chosen K-basis. Very simple checking shows that it is the following matrix:

$$T_a'=\begin{pmatrix}0&0&\cdots&0&-c_0\\1&0&\cdots&0&-c_1\\0&1&\cdots&0&-c_2\\\vdots&\vdots&\ddots&&\vdots\\0&0&\cdots&1&-c_{d-1}\end{pmatrix}.$$

Note that its characteristic polynomial is precisely $m_a(X)$.
Now let $\{s_1,\dots,s_e\}$ be a $K(a)$-basis of L. Then a K-basis of L is given by

$$\{s_1,s_1a,s_1a^2,\dots,s_1a^{d-1},\quad s_2,s_2a,s_2a^2,\dots,s_2a^{d-1},\quad\dots\quad s_e,s_ea,s_ea^2,\dots,s_ea^{d-1}\}.$$

K-linear independence is immediately checked and the number of basis elements is OK; this is the way one proves that the field degree is multiplicative in towers: $[L:K]=[L:K(a)][K(a):K]$.
With respect to this basis, the matrix T_a is a block matrix consisting of e blocks on the diagonal, each of them equal to T_a'. This proves (b). □

We need to use some results from field theory. They are gathered in the appendix to this section.

Proposition 2.4. *Let L/K be a finite separable field extension, $\overline{K}$ an algebraic closure of K containing L. Let, furthermore, $a\in L$ and f_a the characteristic polynomial of T_a. Then the following statements hold:*

(a) $f_a(X) = \prod_{\sigma\in \mathrm{Hom}_K(L,\overline{K})}(X-\sigma(a))$,

(b) $\mathrm{Tr}_{L/K}(a) = \sum_{\sigma\in \mathrm{Hom}_K(L,\overline{K})}\sigma(a)$, *and*

(c) $\mathrm{Norm}_{L/K}(a) = \prod_{\sigma\in \mathrm{Hom}_K(L,\overline{K})}\sigma(a)$.

Proof. Let $M = K(a)$. We use Lemma 2.10 from the appendix and its notation. By Proposition 2.12 in the appendix, the minimal polynomial of a over K is

$$m_a(X) := \prod_{i\in I}(X-\sigma_i(a)).$$

Let $e = \#J$. We obtain from Lemma 2.3:

$$\begin{aligned} f_a(X) = m_a(X)^e = \prod_{i\in I}(X-\sigma_i(a))^e = \prod_{i\in I}(X-\overline{\sigma}_i(a))^e \\ = \prod_{i\in I}\prod_{j\in J}(X-\overline{\sigma}_i\circ\tau_j(a)) = \prod_{\sigma\in \mathrm{Hom}_K(L,\overline{K})}(X-\sigma(a)). \end{aligned}$$

This shows (a). Multiplying out, (b) and (c) are an immediate consequence of the preceding lemma. □

Corollary 2.5. *Let $L/M/K$ be finite separable field extensions. Then*

$$\mathrm{Tr}_{L/K} = \mathrm{Tr}_{M/K}\circ\mathrm{Tr}_{L/M} \text{ and } \mathrm{Norm}_{L/K} = \mathrm{Norm}_{M/K}\circ\mathrm{Norm}_{L/M}.$$

Proof. We use Lemma 2.10 from the appendix and its notation. Then

$$\begin{aligned} \mathrm{Tr}_{M/K}\big(\mathrm{Tr}_{L/M}(a)\big) = \sum_{i\in I}\sigma_i\big(\mathrm{Tr}_{L/M}(a)\big) = \sum_{i\in I}\sigma_i\big(\sum_{j\in J}\tau_j(a)\big) \\ = \sum_{i\in I}\overline{\sigma}_i\big(\sum_{j\in J}\tau_j(a)\big) = \sum_{i\in I}\sum_{j\in J}\overline{\sigma}_i\circ\tau_j(a) = \mathrm{Tr}_{L/K}(a). \end{aligned}$$

In the same way, we have

$$\begin{aligned} \mathrm{Norm}_{M/K}\big(\mathrm{Norm}_{L/M}(a)\big) = \prod_{i\in I}\sigma_i\big(\mathrm{Norm}_{L/M}(a)\big) = \prod_{i\in I}\sigma_i\big(\prod_{j\in J}\tau_j(a)\big) \\ = \prod_{i\in I}\overline{\sigma}_i\big(\prod_{j\in J}\tau_j(a)\big) = \prod_{i\in I}\prod_{j\in J}\overline{\sigma}_i\circ\tau_j(a) = \mathrm{Norm}_{L/K}(a), \end{aligned}$$

showing the statement for the norm. □

Definition 2.6. *Let L/K be a finite separable field extension of degree $n = [L:K]$. Further, let $\mathrm{Hom}_K(L,\overline{K}) = \{\sigma_1,\dots,\sigma_n\}$ and let $\alpha_1,\dots,\alpha_n \in L$ be a K-basis of L. Form the matrix*

$$D(\alpha_1,\dots,\alpha_n) := (\sigma_i(\alpha_j))_{1\le i,j\le n} = \begin{pmatrix} \sigma_1(\alpha_1) & \sigma_1(\alpha_2) & \cdots & \sigma_1(\alpha_n) \\ \sigma_2(\alpha_1) & \sigma_2(\alpha_2) & \cdots & \sigma_2(\alpha_n) \\ \vdots & \vdots & \ddots & \vdots \\ \sigma_n(\alpha_1) & \sigma_n(\alpha_2) & \cdots & \sigma_n(\alpha_n) \end{pmatrix}.$$

The discriminant of $(\alpha_1, \ldots, \alpha_n)$ *is defined as*

$$\operatorname{disc}(\alpha_1, \ldots, \alpha_n) := \big(\det D(\alpha_1, \ldots, \alpha_n)\big)^2.$$

The trace pairing on L/K *is the bilinear pairing*

$$L \times L \to K, \quad (x, y) \mapsto \operatorname{Tr}_{L/K}(xy).$$

Example 2.7. *(a) Let $0, 1 \neq d \in \mathbb{Z}$ be a squarefree integer and consider $K = \mathbb{Q}(\sqrt{d})$. Computations (exercise) show:*

$$\operatorname{disc}(1, \sqrt{d}) = 4d \text{ and } \operatorname{disc}(1, \frac{1+\sqrt{d}}{2}) = d.$$

(b) Let $f(X) = X^3 + aX + b \in \mathbb{Z}[X]$ be an irreducible polynomial and consider $K = \mathbb{Q}[X]/(f)$. Let $\alpha \in \mathbb{C}$ be any root of f, so that we can identify $K = \mathbb{Q}(\alpha)$ and $1, \alpha, \alpha^2$ is a $\mathbb{Q}$-basis of K.

Computations also show $\operatorname{disc}(1, \alpha, \alpha^2) = -4a^3 - 27b^2$.

(One can make a brute force computation yielding this result. However, it is easier to identify this discriminant with the discriminant of the polynomial $f(X)$, which is defined by the resultant of f and its formal derivative f'. This, however, was not treated in last term's lecture and we do not have time for it here either.)

Proposition 2.8. *Let L/K be a finite separable field extension of degree $n = [L : K]$. Then the following statements hold:*

(a) Let $D := D(\alpha_1, \ldots, \alpha_n)$. Then $D^{\mathrm{tr}}D$ is the Gram matrix of the trace pairing with respect to any K-basis $\alpha_1, \ldots, \alpha_n$. That is, $D^{\mathrm{tr}}D = \big(\operatorname{Tr}_{L/K}(\alpha_i\alpha_j)\big)_{1\leq i,j\leq n}$.

(b) Let $\alpha_1, \ldots, \alpha_n$ be a K-basis of L. Then

$$\operatorname{disc}(\alpha_1, \ldots, \alpha_n) = \det(D)^2 = \det(D^{\mathrm{tr}}D) = \det\big(\operatorname{Tr}_{L/K}(\alpha_i\alpha_j)\big)_{1\leq i,j\leq n}.$$

(c) Let $\alpha_1, \ldots, \alpha_n$ be a K-basis of L and $C = (c_{i,j})_{1\leq i,j\leq n}$ be an $n \times n$-matrix with coefficients in K with $\det C \neq 0$ and put $\beta_i := C\alpha_i$ for $i = 1, \ldots, n$. Then

$$\operatorname{disc}(\beta_1, \ldots, \beta_n) = \det(C)^2 \operatorname{disc}(\alpha_1, \ldots, \alpha_n).$$

(d) If $L = K(a)$, then

$$\operatorname{disc}(1, a, \ldots, a^{n-1}) = \prod_{1\leq i<j\leq n} \big(\sigma_j(a) - \sigma_i(a)\big)^2,$$

where $\sigma_1, \ldots, \sigma_n$ are the K-homomorphisms $L \to \overline{K}$.

(e) The discriminant $\operatorname{disc}(\alpha_1, \ldots, \alpha_n)$ is non-zero and the trace pairing on L/K is non-degenerate.

Proof. (a) Let $\sigma_1, \dots, \sigma_n$ be the K-homomorphisms $L \to \overline{K}$. Then we have

$$\begin{aligned} D^{\mathrm{tr}}D &= \begin{pmatrix} \sigma_1(\alpha_1) & \sigma_2(\alpha_1) & \cdots & \sigma_n(\alpha_1) \\ \sigma_1(\alpha_2) & \sigma_2(\alpha_2) & \cdots & \sigma_n(\alpha_2) \\ \vdots & \vdots & \ddots & \vdots \\ \sigma_1(\alpha_n) & \sigma_2(\alpha_n) & \cdots & \sigma_n(\alpha_n) \end{pmatrix} \begin{pmatrix} \sigma_1(\alpha_1) & \sigma_1(\alpha_2) & \cdots & \sigma_1(\alpha_n) \\ \sigma_2(\alpha_1) & \sigma_2(\alpha_2) & \cdots & \sigma_2(\alpha_n) \\ \vdots & \vdots & \ddots & \vdots \\ \sigma_n(\alpha_1) & \sigma_n(\alpha_2) & \cdots & \sigma_n(\alpha_n) \end{pmatrix} \\ &= \begin{pmatrix} \sum_{k=1}^n \sigma_k(\alpha_1\alpha_1) & \sum_{k=1}^n \sigma_k(\alpha_1\alpha_2) & \cdots & \sum_{k=1}^n \sigma_k(\alpha_1\alpha_n) \\ \sum_{k=1}^n \sigma_k(\alpha_2\alpha_1) & \sum_{k=1}^n \sigma_k(\alpha_2\alpha_2) & \cdots & \sum_{k=1}^n \sigma_k(\alpha_2\alpha_n) \\ \vdots & \vdots & \ddots & \vdots \\ \sum_{k=1}^n \sigma_k(\alpha_n\alpha_1) & \sum_{k=1}^n \sigma_k(\alpha_n\alpha_2) & \cdots & \sum_{k=1}^n \sigma_k(\alpha_n\alpha_n) \end{pmatrix} \\ &= \begin{pmatrix} \mathrm{Tr}_{L/K}(\alpha_1\alpha_1) & \mathrm{Tr}_{L/K}(\alpha_1\alpha_2) & \cdots & \mathrm{Tr}_{L/K}(\alpha_1\alpha_n) \\ \mathrm{Tr}_{L/K}(\alpha_2\alpha_1) & \mathrm{Tr}_{L/K}(\alpha_2\alpha_2) & \cdots & \mathrm{Tr}_{L/K}(\alpha_2\alpha_n) \\ \vdots & \vdots & \ddots & \vdots \\ \mathrm{Tr}_{L/K}(\alpha_n\alpha_1) & \mathrm{Tr}_{L/K}(\alpha_n\alpha_2) & \cdots & \mathrm{Tr}_{L/K}(\alpha_n\alpha_n) \end{pmatrix}. \end{aligned}$$

So, the (i,j)-entry of the matrix $D^{\mathrm{tr}}D$ equals $\mathrm{Tr}(\alpha_i\alpha_j)$. Hence, $D^{\mathrm{tr}}D$ is the Gram matrix of the trace pairing with respect to the chosen K-basis.
(b) is clear.
(c) Exercise.
(d) Exercise.
(e) We may always choose some $a \in L$ such that $L = K(a)$ (this is shown in any standard course on Galois theory). From (d) it is obvious that the discriminant $\mathrm{disc}(1, a, \dots, a^{n-1})$ is non-zero and, hence, by (c) $\mathrm{disc}(\alpha_1, \dots, \alpha_n) \neq 0$. Consequently, the trace pairing on L/K is non-degenerate (because by a standard result from linear algebra a bilinear pairing is non-degenerate if and only if its Gram matrix with respect to any basis is invertible). □

Appendix: Some Galois theory

Let L/K be an algebraic extension of fields (not necessarily finite for the next definition) and $\overline{K}$ an algebraic closure of K containing L. We pre-suppose here the existence of an algebraic closure, which is not quite easy to prove. However, in the number field case we have $\mathbb{C}$, which we know to be algebraically closed, and in $\mathbb{C}$ we can take $\overline{\mathbb{Q}} = \{z \in \mathbb{C} \mid z \text{ algebraic over } \mathbb{Q}\}$, which is an algebraic closure of $\mathbb{Q}$ and also of all number fields.
Let $f \in K[X]$ be a polynomial of degree n. It is called *separable* if it has n distinct roots in $\overline{K}$. It is very easy to see that

$$f \text{ is separable } \Leftrightarrow 1 = \gcd(f', f),$$

where f' is the formal derivative of f. Otherwise, we say that f is *inseparable*.
If $\mathrm{char}(K) = 0$, then every irreducible polynomial f is separable because $\gcd(f', f) = 1$, as the only monic divisor of f of degree $< n$ is 1 and $\deg(f') = n - 1$. Moreover, if K is a finite field of characteristic p, then every irreducible polynomial $f \in K[X]$ is also separable. The reason is that the finite field $L := K[X]/(f(X))$ is a splitting field of the polynomial $X^{p^n} - X \in \mathbb{F}_p[X]$, where $\#L = p^n$. This implies that $f(X)$ divides $X^{p^n} - X$. As the latter polynomial is separable (because

$\gcd((X^{p^n}-X)', X^{p^n}-X) = \gcd(-1, X^{p^n}-X) = 1$), also f is separable. A field over which every irreducible polynomial is separable is called *perfect*. We have just seen that fields of characteristic 0 and finite fields are perfect. However, not every field is perfect. Consider $K = \mathbb{F}_p(T) = \mathrm{Frac}(\mathbb{F}_p[T])$ and $f(X) = X^p - T \in K[X]$. The Eisenstein criterion shows that f is irreducible, but, $\gcd(f', f) = \gcd(pX^{p-1}, X^p - T) = \gcd(0, X^p - T) = X^p - T \neq 1$, whence f is not separable. In this lecture, we shall almost entirely be working with number fields, and hence in characteristic 0, so that the phenomenon of inseparability will not occur.

Next we explain how irreducible separable polynomials are related to properties of field extensions. We let $\mathrm{Hom}_K(L, \overline{K})$ be the set of field homomorphisms (automatically injective!) $\tau : L \to \overline{K}$ such that $\tau|_K = \mathrm{id}_K$, i.e. $\tau(x) = x$ for all $x \in K$. Such a homomorphism is referred to as a *K-homomorphism*. We write $[L : K]_{\mathrm{sep}} := \#\mathrm{Hom}_K(L, \overline{K})$ and call it the *separable degree of L/K*, for reasons to become clear in a moment.

Let now $f \in K[X]$ be an irreducible polynomial and suppose $L = K[X]/(f)$. We have the bijection

$$\{\alpha \in \overline{K} \mid f(\alpha) = 0\} \longrightarrow \mathrm{Hom}_K(L, \overline{K}),$$

given by sending α to the K-homomorphism

$$\sigma_\alpha : K[X]/(f) \to \overline{K}, \quad g(X) + (f) \mapsto g(\alpha).$$

Note that it is well-defined because $f(\alpha) = 0$. The injectivity of the map is clear: $\alpha = \sigma_\alpha(X+(f)) = \sigma_\beta(X + (f)) = \beta$. For the surjectivity consider any $\sigma : K[X]/(f) \to \overline{K}$ and put $\gamma = \sigma(X)$. As $\sigma(f) = 0$, we have $f(\gamma) = 0$ and it follows that $\sigma = \sigma_\gamma$ because the $X^r + (f)$ form a K-generating system of $K[X]/(f)$ on which σ and σ_γ agree. We have shown for $L = K[X]/(f)$:

$$[L : K]_{\mathrm{sep}} = \#\{\alpha \in \overline{K} \mid f(\alpha) = 0\} \leq \deg(f) = [L : K].$$

Now we consider a general algebraic field extension L/K again. An element $a \in L$ is called *separable over K* if its minimal polynomial $f_a \in K[X]$ is separable. The algebraic field extension L/K is called *separable* if every element $a \in L$ is separable over K. As an immediate consequence every subextension of a separable extension is separable.

The most important technical tool in Galois theory is the following proposition.

Proposition 2.9. *Let L/K be an algebraic field extension and $\overline{K}$ an algebraic closure of K containing L. Then any K-homomorphism $\sigma : L \to \overline{K}$ can be extended to a K-homomorphism $\overline{\sigma} : \overline{K} \to \overline{K}$.*

In order to explain the idea behind this proposition, let us take $M = L(a)$ for some $a \in \overline{K}$, whence $M = L[X]/(f)$ with f the minimal polynomial of a over L, and let us extend σ to M, call it σ_M. The polynomial f factors into linear factors over $\overline{K}$, whence we may choose some $\alpha \in \overline{K}$ such that $f(\alpha) = 0$. Any element of M is of the form $\sum_{i=0}^d a_i X^i + (f)$ and we send it via σ_M to $\sum_{i=0}^d \sigma(a_i)\alpha^i$ in $\overline{K}$. Using a Zorn's lemma argument, one obtains that σ can indeed be extended to $\overline{K}$.

Lemma 2.10. *Let $L/M/K$ be algebraic field extensions contained inside $\overline{K}$ and let*

$$\mathrm{Hom}_K(M, \overline{K}) = \{\sigma_i \mid i \in I\} \overset{\text{bij.}}{\leftrightarrow} I \text{ and } \mathrm{Hom}_M(L, \overline{K}) = \{\tau_j \mid j \in J\} \overset{\text{bij.}}{\leftrightarrow} J.$$

By Proposition 2.9 we may choose $\overline{\sigma}_i : \overline{K} \to \overline{K}$ extending σ_i for $i \in I$.
Then the following statements hold.

(a) $\mathrm{Hom}_K(L, \overline{K}) = \{\overline{\sigma}_i \circ \tau_j \mid i \in I, j \in J\}$.

(b) The map

$$I \times J \to \mathrm{Hom}_K(L, \overline{K}), \quad (i, j) \mapsto \overline{\sigma}_i \circ \tau_j$$

is a bijection.

(c) The separable degree is multiplicative in towers of algebraic field extensions:

$$[L : K]_{\mathrm{sep}} = [L : M]_{\mathrm{sep}} \cdot [M : K]_{\mathrm{sep}}.$$

Proof. (a) is easy to see: '$\supseteq$' is clear. '$\subseteq$': Let $\tau \in \mathrm{Hom}_K(L, \overline{K})$, then $\tau|_M \in \mathrm{Hom}_K(M, \overline{K})$, whence $\tau|_M = \sigma_i$ for some $i \in I$. Now consider $\overline{\sigma}_i^{-1} \circ \tau \in \mathrm{Hom}_M(L, \overline{K})$, whence there is $j \in J$ such that $\tau = \overline{\sigma}_i \circ \tau_j$.
(b) The surjectivity is precisely the inclusion '$\subseteq$' shown above. For the injectivity suppose $\overline{\sigma_i} \circ \tau_j = \overline{\sigma_k} \circ \tau_\ell$. Restrict this equality to M and get $\sigma_i = \sigma_k$, whence $i = k$. Having this, multiply from the left by $\overline{\sigma}_i^{-1}$ and obtain $\tau_j = \tau_\ell$, whence $j = \ell$.
(c) This is a consequence of the preceding statements. □

The multiplicativity of the separable degree combined with our calculations for $L = K[X]/(f)$ immediately give for a finite extension L/K:

$$L/K \text{ is separable } \Leftrightarrow [L : K] = [L : K]_{\mathrm{sep}},$$

and the inequality $[L : K] \geq [L : K]_{\mathrm{sep}}$ always holds.
One more definition: the set $K^{\mathrm{sep}} := \{x \in \overline{K} \mid x \text{ is separable over } K\}$ is called *the separable closure of K in $\overline{K}$*. It can be seen as the compositum of all finite separable subextensions L/K inside $\overline{K}$, whence it clearly is a field. Note that for a perfect field K one has $\overline{K} = K^{\mathrm{sep}}$.

Proposition 2.11. *Let $a \in K^{\mathrm{sep}}$ such that $\sigma(a) = a$ for all $\sigma \in \mathrm{Hom}_K(\overline{K}, \overline{K})$, then $a \in K$.*

Proof. Suppose a is not in K. We let $f \in K[X]$ be its minimal polynomial and we let $\alpha \in \overline{K}$ be a different root of f. Then we have $\sigma_\alpha : K(a) \to \overline{K}$ (defined as above, sending a to α) a non-trivial K-homomorphism, which we may extend to $\overline{\sigma}_\alpha : \overline{K} \to \overline{K}$, which does not fix a, contradiction. □

This allows us to write down the minimal polynomial of a separable element $x \in K^{\mathrm{sep}}$ as follows.

Proposition 2.12. *Let $a \in K^{\mathrm{sep}}$ and consider the set*

$$\{\sigma_1, \sigma_2, \ldots, \sigma_n\} = \mathrm{Hom}_K(K(a), \overline{K})$$

with $n = [K(a) : K] = [K(a) : K]_{\mathrm{sep}}$. Then the minimal polynomial of a over K is

$$f_a(X) := \prod_{i=1}^{n} (X - \sigma_i(a)).$$

Proof. We extend σ_i to $\overline{\sigma}_i : \overline{K} \to \overline{K}$ and observe $\overline{\sigma}(f_a) = f_a$ (where $\overline{\sigma}$ is applied to the coefficients of f_a) for all K-homomorphisms $\overline{\sigma} : \overline{K} \to \overline{K}$, whence $f_a \in K[X]$. Here we have used that every $\overline{\sigma}$ restricted to $K(a)$ is one of the σ_i, and, hence, application of $\overline{\sigma}$ just permutes the σ_i in the product. Proposition 2.11 now implies that the coefficients of f_a are indeed in K.
It remains to see that the polynomial is irreducible. But that is clear for degree reasons. Of course, a is a zero of f_a (one of the σ_i is the identity on a), f_a is monic and its degree is that of $[K(a) : K]$. □

3 Rings of integers

We recall central definitions and propositions from last term's course on commutative algebra.

Definition 3.1. *Let R be a ring and S an extension ring of R (i.e. a ring containing R as a subring). An element $a \in S$ is called* integral over R *if there exists a monic polynomial $f \in R[X]$ such that $f(a) = 0$.*

Note that integrality is also a relative notion; an element is integral *over* some ring. Also note the similarity with algebraic elements; we just added the requirement that the polynomial be monic.

Example 3.2. *(a) The elements of $\mathbb{Q}$ that are integral over $\mathbb{Z}$ are precisely the integers of $\mathbb{Z}$.*

(b) $\sqrt{2} \in \mathbb{R}$ is integral over $\mathbb{Z}$ because $X^2 - 2$ annihilates it.

(c) $\frac{1+\sqrt{5}}{2} \in \mathbb{R}$ is integral over $\mathbb{Z}$ because $X^2 - X - 1$ annihilates it.

(d) $a := \frac{1+\sqrt{-5}}{2} \in \mathbb{C}$ is not integral over $\mathbb{Z}$ because $f = X^2 - X + \frac{3}{2}$ annihilates it. If there were a monic polynomial $h \in \mathbb{Z}[X]$ annihilating a, then we would have $h = fg$ with some monic polynomial $g \in \mathbb{Q}[X]$. But, now it would follow that both f and g are in $\mathbb{Z}[X]$ (see Sheet 4 of last term's lecture on Commutative Algebra), which is a contradiction.

(e) Let K be a field and S a ring containing K (e.g. $L = S$ a field) and $a \in S$. Then a is integral over K if and only if a is algebraic over K.

Indeed, as K is a field any polynomial with coefficients in K can be made monic by dividing by the leading coefficient. So, if we work over a field, then the new notion of integrality is just the notion of algebraicity from the previous section.

Definition 3.3. *Let S be a ring and $R \subseteq S$ a subring.*

(a) The set $R_S = \{a \in S \mid a$ is integral over $R\}$ is called the integral closure of R in S *(compare with the algebraic closure of R in S – the two notions coincide if R is a field).*

An alternative name is: normalisation of R in S.

(b) S is called an integral ring extension of R *if $R_S = S$, i.e. if every element of S is integral over R (compare with algebraic field extension – the two notions coincide if R and S are fields).*

(c) R is called integrally closed in S *if $R_S = R$.*

(d) An integral domain R is called integrally closed *(i.e. without mentioning the ring in which the closure is taken) if R is integrally closed in its fraction field.*

(e) Let $a_i \in S$ for $i \in I$ (some indexing set). We let $R[a_i \mid i \in I]$ (note the square brackets!) be the smallest subring of S containing R and all the a_i, $i \in I$.

Note that we can see $R[a]$ inside S as the image of the ring homomorphism

$$\Phi_a : R[X] \to S, \quad \sum_{i=0}^{d} c_i X^i \mapsto \sum_{i=0}^{d} c_i a^i.$$

Proposition 3.4. *Let $R \subseteq S \subseteq T$ be rings.*

(a) For $a \in S$, the following statements are equivalent:

(i) a is integral over R.

(ii) $R[a] \subseteq S$ is a finitely generated R-module.

(b) Let $a_1, \ldots, a_n \in S$ be elements that are integral over R. Then $R[a_1, \ldots, a_n] \subseteq S$ is integral over R and it is finitely generated as an R-module.

(c) Let $R \subseteq S \subseteq T$ be rings. Then 'transitivity of integrality' holds:

$$T/R \text{ is integral} \;\Leftrightarrow\; T/S \text{ is integral and } S/R \text{ is integral.}$$

(d) R_S is a subring of S.

(e) Any $t \in S$ that is integral over R_S lies in R_S. In other words, R_S is integrally closed in S (justifying the name).

Definition 3.5. *Recall that a* number field *K is a finite field extension of $\mathbb{Q}$. The* ring of integers of *K is the integral closure of $\mathbb{Z}$ in K, i.e. $\mathbb{Z}_K$. An alternative notation is $\mathcal{O}_K$.*

Example 3.6. *Let $d \neq 0, 1$ be a squarefree integer. The ring of integers of $\mathbb{Q}(\sqrt{d})$ is*

(1) $\mathbb{Z}[\sqrt{d}]$, if $d \equiv 2, 3 \pmod 4$,

(2) $\mathbb{Z}[\frac{1+\sqrt{d}}{2}]$, if $d \equiv 1 \pmod 4$.

Proposition 3.7. *Every factorial ring (unique factoriation domain) is integrally closed.*

Proposition 3.8. *Let R be an integral domain, $K = \mathrm{Frac}(R)$, L/K a finite field extension and $S := R_L$ the integral closure of R in L. Then the following statements hold:*

(a) Every $a \in L$ can be written as $a = \frac{s}{r}$ with $s \in S$ and $0 \neq r \in R$.

(b) $L = \mathrm{Frac}(S)$ and S is integrally closed.

(c) If R is integrally closed, then $S \cap K = R$.

The following proposition was stated but not proved in last term's lecture.

Proposition 3.9. *Let R be an integral domain which is integrally closed (recall: that means integrally closed in $K = \mathrm{Frac}(R)$). Let $\overline{K}$ be an algebraic closure of K and let $a \in \overline{K}$ be separable over K. Then the following statements are equivalent:*

(i) a is integral over R.

(ii) The minimal polynomial $m_a \in K[X]$ of a over K has coefficients in R.

Proof. '(ii) $\Rightarrow$ (i)': Since by assumption $m_a \in R[X]$ is a monic polynomial annihilating a, by definition a is integral over R.
'(i) $\Rightarrow$ (ii)': From Proposition 2.12 we know that the minimal polynomial of a over K is

$$m_a(X) = \prod_{i=1}^{n}(X - \sigma_i(a)),$$

where $\{\sigma_1 = \mathrm{id}, \sigma_2, \ldots, \sigma_n\} = \mathrm{Hom}_K(K(a), \overline{K})$.
We assume that a is integral over R, so there is some monic polynomial $g_a \in R[X]$ annihilating a. It follows that m_a divides g_a. Consequently, $g_a(\sigma_i(a)) = \sigma_i(g_a(a)) = \sigma_i(0) = 0$ for all $i = 1, \ldots, n$, proving that also $\sigma_2(a), \sigma_3(a), \ldots, \sigma_n(a)$ are integral over R. Hence, m_a has integral coefficients over R (they are products and sums of the $\sigma_i(a)$). As R is integrally closed in K, the coefficients lie in R. □

We now apply norm and trace to integral elements.

Lemma 3.10. *Let R be an integrally closed integral domain, K its field of fractions, L/K a separable finite field extension and S the integral closure of R in L. Let $s \in S$. Then the following statements hold:*

(a) $\mathrm{Tr}_{L/K}(s) \in R$ *and* $\mathrm{Norm}_{L/K}(s) \in R$.

(b) $s \in S^\times \Leftrightarrow \mathrm{Norm}_{L/K}(s) \in R^\times$.

Proof. (a) directly follows from $S \cap K = R$.
(b) '$\Rightarrow$': Let $s, t \in S^\times$ such that $ts = 1$. Then

$$1 = \mathrm{Norm}_{L/K}(1) = \mathrm{Norm}_{L/K}(st) = \mathrm{Norm}_{L/K}(s)\mathrm{Norm}_{L/K}(t),$$

exhibiting an inverse of $\mathrm{Norm}_{L/K}(s)$ in R.
'$\Leftarrow$': Assume $\mathrm{Norm}_{L/K}(s) \in R^\times$. Then

$$1 = r\mathrm{Norm}_{L/K}(s) = r \prod_{\sigma \in \mathrm{Hom}_K(L,\overline{K})} \sigma(s) = \big(r \prod_{\mathrm{id} \neq \sigma \in \mathrm{Hom}_K(L,\overline{K})} \sigma(s)\big)s = ts,$$

exhibiting an inverse to s in S. □

Next we use the discriminant to show the existence of an integral basis. The discriminant will also be important in the proof of the Noetherian-ness of the ring of integers of a number field.

Lemma 3.11. *Let R be an integrally closed integral domain, K its field of fractions, L/K a separable finite field extension and S the integral closure of R in L.*

(a) For any K-basis $\alpha_1, \ldots, \alpha_n$ of L, there is an element $r \in R \setminus \{0\}$ such that $r\alpha_i \in S$ for all $i = 1, \ldots, n$.

(b) Let $\alpha_1, \ldots, \alpha_n \in S$ be a K-basis of L and let $d = \mathrm{disc}(\alpha_1, \ldots, \alpha_n)$ be the discriminant of this basis. Then $dS \subseteq R\alpha_1 + \cdots + R\alpha_n$.

Proof. (a) By Proposition 3.8 (a), we can write $\alpha_i = \frac{s_i}{r_i}$ with $r_i \in R$ and $s_i \in S$ for all $i = 1, \ldots, n$. Hence, we may take $r = r_1 \cdot \ldots \cdot r_n$.
(b) Let $s = \sum_{j=1}^{n} x_j \alpha_j$ be an element of S with $x_j \in K$ for $j = 1, \ldots, n$. We show $ds \in R\alpha_1 + \cdots + R\alpha_n$. Note that the elementary properties of the trace yield

$$\mathrm{Tr}_{L/K}(\alpha_i s) = \sum_{j=1}^{n} \mathrm{Tr}(\alpha_i \alpha_j) x_j \in R.$$

We can rewrite this in matrix form using $M = D^{\mathrm{tr}} D = \begin{pmatrix} \mathrm{Tr}_{L/K}(\alpha_1\alpha_1) & \cdots & \mathrm{Tr}_{L/K}(\alpha_1\alpha_n) \\ \vdots & \ddots & \vdots \\ \mathrm{Tr}_{L/K}(\alpha_n\alpha_1) & \cdots & \mathrm{Tr}_{L/K}(\alpha_n\alpha_n) \end{pmatrix}$. Now:

$$M \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = \begin{pmatrix} \sum_{j=1}^{n} \mathrm{Tr}(\alpha_1\alpha_j) x_j \\ \vdots \\ \sum_{j=1}^{n} \mathrm{Tr}(\alpha_n\alpha_j) x_j \end{pmatrix} \in R^n.$$

Multiplying through with the adjoint matrix $M^{\#}$ yields

$$M^{\#} M \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = \det(M) \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = d \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \in R^n.$$

Thus, $dx_i \in R$ for all $i = 1, \ldots, n$ and, consequently, $ds \in R\alpha_1 + \cdots + R\alpha_n$. □

We now need a statement that is very simple and could have been proved in last term's course on commutative algebra (but, it wasn't). We give a quick proof.

Theorem 3.12. *Let R be a principal ideal domain and M a finitely generated R-module. Then the following statements hold:*

(a) Assume that M is a free R-module of rank m. Then any submodule N of M is finitely generated and free of rank $\leq m$.

(b) An element $m \in M$ is called a torsion element *if there is $0 \neq r \in R$ such that $rm = 0$. The set $M_{\mathrm{torsion}} = \{m \in M \mid m \text{ is a torsion element }\}$ is an R-submodule of M.*

(c) M is a free R-module $\Leftrightarrow M_{\mathrm{torsion}} = \{0\}$.

(d) There is an integer m such that

$$M \cong M_{\mathrm{torsion}} \oplus \underbrace{R \oplus \ldots \oplus R}_{m \text{ times}}.$$

*The integer m is called the R-*rank *of M.*

(e) Let $0 \to N \to M \to Q \to 0$ be a short exact sequence of finitely generated R-modules. Then $\mathrm{rk}_R(M) = \mathrm{rk}_R(N) + \mathrm{rk}_R(Q)$.

Proof. (a) We give a proof by induction on m. The case $m = 0$ is clear (the only submodule of the zero-module is the zero-module).
Now let $m = 1$. Then $M \cong R$ and the submodules of M are the ideals of R under the isomorphism. As R is a principal ideal domain, the rank of the submodules of M is thus equal to 1, unless it is the zero-ideal.
Now, suppose we already know the statement for all ranks up to $m-1$ and we want to prove it for M of rank m. After an isomorphism, we may suppose $M = \underbrace{R \oplus \ldots \oplus R}_{m \text{ times}}$. Let $\pi : M = R \oplus \ldots \oplus R \to R$ be the m-th projection. It sits in the (trivial) exact sequence

$$0 \to \underbrace{R \oplus \ldots \oplus R}_{m-1 \text{ times}} \to M \xrightarrow{\pi} R \to 0.$$

Let now $N \leq M$ be a submodule and set

$$N_1 := N \cap \ker \pi = N \cap \underbrace{R \oplus \ldots \oplus R}_{m-1 \text{ times}}.$$

By the induction assumption, N_1 is a free R-module of rank at most $n - 1$. Moreover, $\pi(N)$ is a submodule of R, hence, by the case $m = 1$, it is free of rank 0 or 1. We have the exact sequence:

$$0 \to N_1 \to N \xrightarrow{\pi} \pi(N) \to 0.$$

As $\pi(N)$ is free, it is projective and this sequence splits, yielding

$$N \cong N_1 \oplus \pi(N),$$

showing that N is free of rank at most $(m - 1) + 1 = m$.
(b) is trivial.
(c) '$\Rightarrow$': Let $x_1, \ldots, x_n$ be a free system of generators of M. Let $x = \sum_{i=1}^{n} r_i x_i \in M$. If $rx = 0$ with $R \ni r \neq 0$, then $rr_i = 0$ for all i, thus $r_i = 0$ for all i, whence $x = 0$.
'$\Leftarrow$': Let $x_1, \ldots, x_n$ be any system of generators of M and let $x_1, \ldots, x_m$ with $m \leq n$ be a maximal free subset (possibly after renumbering). If $m = n$, then M is free, which we want to show. Assume, hence, that $m < n$. Then for all $m + 1 \leq i \leq n$, there is $0 \neq r_i \in R$ such that $r_i x_i = \sum_{j=1}^{m} r_{i,j} x_j$. Setting $r := r_{i+1} \cdot \ldots \cdot r_n$, we obtain for all $i = 1, \ldots, n$:

$$rx_i \in Rx_1 \oplus Rx_2 \oplus \ldots \oplus Rx_m$$

and, consequently, for all $x \in M$:

$$rx \in Rx_1 \oplus Rx_2 \oplus \ldots \oplus Rx_m.$$

As $M_{\text{torsion}} = \{0\}$, it follows that the map

$$M \to Rx_1 \oplus Rx_2 \oplus \ldots \oplus Rx_m, \quad x \mapsto rx,$$

gives an isomorphism between M and an R-submodule of the free R-module $Rx_1 \oplus Rx_2 \oplus \ldots \oplus Rx_m$, whence by (a) M is free.

(d) We consider the trivial exact sequence

$$0 \to M_{\text{torsion}} \to M \to M/M_{\text{torsion}} \to 0,$$

and claim that M/M_{torsion} is a free R-module. By (c) it suffices to show that the only torsion element in M/M_{torsion} is 0, which works like this: Let $x + M_{\text{torsion}} \in M/M_{\text{torsion}}$ and $0 \neq r \in R$ such that $r(x+M_{\text{torsion}}) = rx+M_{\text{torsion}} = 0+M_{\text{torsion}} \in M/M_{\text{torsion}}$. Then, clearly, $rx \in M_{\text{torsion}}$, whence there is $0 \neq s \in R$ such that $s(rx) = (sr)x = 0$, yielding $x \in M_{\text{torsion}}$, as desired.
As M/M_{torsion} is R-free, it is projective and, hence, the above exact sequence splits (see Commutative Algebra), yielding the desired assertion.
(e) First assume that Q is R-free of rank q. Then the exact sequence splits and one gets $M \cong N \oplus Q$, making the assertion obvious. If $Q = R^q \oplus Q_{\text{torsion}}$, then consider the composite map $\pi : M \twoheadrightarrow R^q \oplus Q_{\text{torsion}} \twoheadrightarrow R^q$. We get $\operatorname{rk}_R(M) = q + \operatorname{rk}_R(\widetilde{N})$ with $\widetilde{N} = \ker(\pi)$. From the snake lemma (see exercise) applied to the diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & N & \longrightarrow & M & \longrightarrow & Q & \longrightarrow & 0 \\ & & \downarrow & & \| & & \downarrow & & \\ 0 & \longrightarrow & \widetilde{N} & \longrightarrow & M & \longrightarrow & R^q & \longrightarrow & 0 \end{array}$$

it is obvious that $\widetilde{N}/N \cong Q_{\text{torsion}}$. From this we want to conclude that $\operatorname{rk}(N) = \operatorname{rk}(\widetilde{N})$, then we are done. Let $y_1 + N, \ldots, y_s + N$ be generators of $\widetilde{N}/N$. Since $\widetilde{N}/N$ is torsion, there are $r_1, \ldots, r_s \in R \setminus \{0\}$ such that $r_i y_i \in N$ for all $i \in \{1, \ldots, s\}$. Hence, with $r := r_1 \cdot r_2 \cdots r_s$ we have $r\widetilde{N} \leq N$, showing $\operatorname{rk}(\widetilde{N}) \leq \operatorname{rk}(N)$. Since $N \leq \widetilde{N}$, we have equality, as needed. □

Definition 3.13. *Let $R \subseteq S$ be an integral ring extension. If S is free as an R-module, then an R-basis of S (i.e. a free generating system) exists and is called an* integral basis of S over R.

We point out that, if S is an integral domain (as it always will be in this lecture), then an R-basis of S is also a K-basis of $L = \operatorname{Frac}(S)$ with $K = \operatorname{Frac}(R)$.
Note that, in general, there is no reason why an integral ring extension S should be free as an R-module. This is, however, the case for the rings of integers, as the following proposition shows.

Proposition 3.14. *Let R be a principal ideal domain, K its field of fractions, L/K a finite separable field extension and S the integral closure of R in L.*
Then every finitely generated S-submodule $0 \neq M$ of L is a free R-module of rank $[L : K]$. In particular, S possesses an integral basis over R.

Proof. As principal ideal domains are unique factorisation domains and, hence, integrally closed, we may apply Lemma 3.11 to obtain a K-basis $\alpha_1, \ldots, \alpha_n \in S$ of L and we also have $dS \subseteq R\alpha_1 + \cdots + R\alpha_n =: N$ with $d = \operatorname{disc}(\alpha_1, \ldots, \alpha_n)$. Note that N is a free R-module of rank $n = [L : K]$.
Let $m_1, \ldots, m_k \in M$ be a generating system of $M \subseteq L$ as S-module. As the m_i are elements of L, by Proposition 3.8 (a) there is $r \in R$ such that $rm_i \in S$ for all $i = 1, \ldots, k$, whence $rM \subseteq S$. Hence, $rdM \subseteq dS \subseteq N$. Consequently, Theorem 3.12 yields that rdM is a free R-module of rank at most n. Of course, the R-rank of rdM is equal to the R-rank of M. Let $0 \neq m \in M$. Then $Nm \leq Sm \leq M$, showing that n, the R-rank of N (which is equal to the R-rank of Nm) is at most the R-rank of M, finishing the proof. □

For the rest of this section we specialise to the case of number fields.

Definition 3.15. *Let K be a number field. A subring $\mathcal{O}$ of $\mathbb{Z}_K$ is called an* order of K *if $\mathcal{O}$ has an integral basis of length $[K:\mathbb{Q}]$.*

Corollary 3.16. *Any order in a number field K is a Noetherian integral domain of Krull dimension* 1.

Proof. Being a subring of a field, $\mathcal{O}$ is an integral domain. As the ring extension $\mathbb{Z} \subseteq \mathcal{O}$ is integral (being contained in the integral extension $\mathbb{Z} \subseteq \mathbb{Z}_K$), the Krull dimension of $\mathcal{O}$ equals the Krull dimension of $\mathbb{Z}$, which is 1 (see Commutative Algebra). As $\mathcal{O}$ has an integral basis, we have $\mathcal{O} \cong \underbrace{\mathbb{Z} \oplus \ldots \oplus \mathbb{Z}}_{[K:\mathbb{Q}] \text{ times}}$. That $\mathcal{O}$ is Noetherian now follows because $\mathbb{Z}$ is Noetherian and finite direct sums of Noetherian modules are Noetherian (see Commutative Algebra). □

Corollary 3.17. *Let K be a number field and $\mathbb{Z}_K$ the ring of integers of K. Then the following statements hold:*

(a) $\mathbb{Z}_K$ is an order of K, also called the maximal order of K.

(b) $\mathbb{Z}_K$ is a Dedekind ring.

(c) Let $0 \subsetneq I \trianglelefteq \mathbb{Z}_K$ be an ideal. Then I is a free $\mathbb{Z}$-module of rank $[K:\mathbb{Q}]$ and the quotient $\mathbb{Z}_K/I$ is finite (i.e. has finitely many elements; equivalently, the index $(\mathbb{Z}_K : I)$ is finite).

Proof. (a) It is a trivial consequence of Proposition 3.14 that $\mathbb{Z}_K$ is a free $\mathbb{Z}$-module of rank $[K:\mathbb{Q}]$ because $\mathbb{Z}_K$ is a $\mathbb{Z}_K$-module generated by a single element, namely 1. In particular, $\mathbb{Z}_K$ has an integral basis and, hence, is an order of K.
(b) From Corollary 3.16 we know that $\mathbb{Z}_K$ is a Noetherian integral domain of Krull dimension 1. It is also integrally closed (being defined as the integral closure of $\mathbb{Z}$ in K), hence, by definition, a Dedekind ring.
(c) As $\mathbb{Z}_K$ is Noetherian, the ideal I is finitely generated. Hence, Proposition 3.14 again gives that I is a free $\mathbb{Z}$-module of rank $[K:\mathbb{Q}]$. The quotient of any two free $\mathbb{Z}$-modules of the same rank is $\mathbb{Z}$-torsion by Theorem 3.12. Hence, $\mathbb{Z}_K/I$ is an abelian group generated by finitely many elements of finite order, hence, it is a finite group. □

Definition 3.18. *Let K be a number field with ring of integers $\mathbb{Z}_K$ and $0 \neq \mathfrak{a} \subset K$ be a finitely generated $\mathbb{Z}_K$-module. The* discriminant of $\mathfrak{a}$ *is defined as $\operatorname{disc}(\alpha_1, \ldots, \alpha_n)$ for any $\mathbb{Z}$-basis of the free $\mathbb{Z}$-module $\mathfrak{a}$ (see Proposition 3.14). (By Proposition 2.8 (c), this definition does not depend on the choice of $\mathbb{Z}$-basis because the basis transformation matrix is invertible with integral entries and thus has determinant ± 1.)*
The discriminant of K *is defined as $\operatorname{disc}(\mathbb{Z}_K)$.*

Proposition 3.19. *Let K be a number field and $\mathbb{Z}_K$ its ring of integers. Let $0 \neq \mathfrak{a} \subseteq \mathfrak{b} \subset K$ be two finitely generated $\mathbb{Z}_K$-modules. Then the index $(\mathfrak{b} : \mathfrak{a})$ is finite and satisfies*

$$\operatorname{disc}(\mathfrak{a}) = (\mathfrak{b} : \mathfrak{a})^2 \operatorname{disc}(\mathfrak{b}).$$

Proof. Exercise on Sheet 4. □

4 Ideal arithmetic

It is useful, in order to make the set of non-zero ideals of a Dedekind ring into a group with respect to multiplication of ideals, to introduce fractional ideals, which will be needed for the inverses.

Definition 4.1. *Let R be an integral domain and $K = \mathrm{Frac}(R)$.*

- *An R-submodule $I \leq K$ is called a* fractional ideal of R *(or:* fractional R-ideal*) if*
  - *$I \neq (0)$ and*
  - *there is $x \in K^\times$ such that $xI \subseteq R$.*

  Note that x can always be chosen in $R \setminus \{0\}$. Note also that xI is an ideal of R (in the usual sense).
- *A fractional R-ideal I is called an* integral ideal *if $I \subseteq R$.*

  Note that for a subset $(0) \neq I \subset K$, one trivially has:

  $$I \trianglelefteq R \text{ is an ideal of } R \text{ in the usual sense} \Leftrightarrow I \text{ is an integral fractional } R\text{-ideal.}$$
- *A fractional R-ideal I is called* principal *if there is $x \in K^\times$ such that $I = Rx$.*
- *Let I, J be fractional R-ideals. The* ideal quotient *of I by J is defined as*

  $$I : J = (I : J) = \{x \in K \mid xJ \subseteq I\}.$$
- *The* inverse ideal *of the fractional R-ideal I is defined as*

  $$I^{-1} := (R : I) = \{x \in K \mid xI \subseteq R\}.$$
- *The* multiplier ring *of the fractional R-ideal I is defined as*

  $$r(I) := (I : I) = \{x \in K \mid xI \subseteq I\}.$$

Example 4.2. *The fractional ideals of $\mathbb{Z}$ are all of the form $I = \frac{a}{b}\mathbb{Z}$ with $a, b \in \mathbb{Z} \setminus \{0\}$. Hence, all fractional $\mathbb{Z}$-ideals are principal.*
It is clear that $\frac{a}{b}\mathbb{Z}$ is a fractional ideal. Conversely, let I be a fractional ideal such that bI is an ideal of $\mathbb{Z}$, whence $bI = (a) = a\mathbb{Z}$, so that $I = \frac{a}{b}\mathbb{Z}$.
Let $I = \frac{a}{b}\mathbb{Z}$ and $J = \frac{c}{d}\mathbb{Z}$, then

$$(I : J) = \{x \in \mathbb{Q} \mid x\frac{c}{d}\mathbb{Z} \in \frac{a}{b}\mathbb{Z}\} = \{x \in \mathbb{Q} \mid x \in \frac{ad}{bc}\mathbb{Z}\} = \frac{ad}{bc}\mathbb{Z}.$$

In particular, $I^{-1} = \frac{b}{a}\mathbb{Z}$ and $II^{-1} = \mathbb{Z}$ (because, clearly $\subseteq$ and $1 \in II^{-1}$).

Lemma 4.3. *Let R be an integral domain and $K = \mathrm{Frac}(R)$. Let $I, J \subset K$ be fractional R-ideals. Then the following sets are fractional R-ideals.*

- $I + J = \{x + y \mid x \in I, y \in J\}$,
- $IJ = \{\sum_{i=1}^{n} x_i y_j \mid n \in \mathbb{N}, x_1, \ldots, x_n \in I, y_1, \ldots, y_n \in J\}$,
- $I^n = \underbrace{I \cdot I \cdot \ldots \cdot I}_{n \text{ times}}$,
- $I \cap J$,
- $(I : J)$.

Proof. Exercise. □

Lemma 4.4. *Let R be an integral domain and $H, I, J \subset K$ fractional R-ideals. Then the following properties hold:*

(a) $IJ \subseteq I \cap J$ *(assume here that I and J are integral ideals),*

(b) $H + (I + J) = (H + I) + J = H + I + J$,

(c) $H(IJ) = (HI)J$,

(d) $H(I + J) = HI + HJ$.

Proof. Exercise. □

Lemma 4.5. *Let R be an integral domain and $I, J \trianglelefteq R$ be ideals (in the usual sense). If $I + J = R$, then we call I and J* coprime ideals.
Suppose now that I and J are coprime. Then the following statements hold:

(a) I^n *and* J^m *are coprime for all* $n, m \in \mathbb{N}$.

(b) $I \cap J = IJ$.

(c) $R/(IJ) \cong R/I \times R/J$ *(Chinese Remainder Theorem).*

(d) If $IJ = H^n$ *for some* $n \in \mathbb{N}$, *then* $I = (I + H)^n$, $J = (J + H)^n$ *and* $(I + H)(J + H) = H$.

In words: If an ideal is an n-th power, then so is each of its coprime factors.

Proof. (a) By assumption $1 = i + j$ for some $i \in I$ and some $j \in J$. Now $1 = 1^{n+m} = (i + j)^{n+m} \in I^n + J^m$.
(b) The inclusion '$\supseteq$' is clear. We now show '$\subseteq$'. Let $x \in I \cap J$. Again by assumption $1 = i + j$ for some $i \in I$ and some $j \in J$. Hence, $x = x \cdot 1 = xi + xj$, whence $x \in IJ$ because $xi \in IJ$ and $xj \in IJ$.
(c) That's just a reminder. It was proved in some of your Algebra lectures.
(d) We start with the following computation:

$$\begin{aligned}(I + H)^n &= I^n + I^{n-1}H + I^{n-2}H^2 + \cdots + IH^{n-1} + H^n \\ &= I(I^{n-1} + I^{n-2}H + \cdots + H^{n-1} + J) \\ &= IR = I\end{aligned}$$

because $H^n = IJ$ and J and I^{n-1} are coprime by (a). Define $A = I + H$ and $B = J + H$. Then

$$AB = (I+H)(J+H) = IJ + IH + JH + H^2 = H^n + IH + JH + H^2 \\ = H(H^{n-1} + I + J + H) = HR = H,$$

as required. □

Example 4.6. *Let us consider the ring $R = \mathbb{Z}[\sqrt{-19}]$. In this ring, we have the following factorisations:*

$$18^2 + 19 = (18 + \sqrt{-19})(18 - \sqrt{-19}) = 343 = 7^3.$$

Let us take the principal ideals $I = (18 + \sqrt{-19})$ and $J = (18 - \sqrt{-19})$, then

$$IJ = (7)^3.$$

The previous lemma now gives:

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

But, one can check, by hand, that the elements $18 + \sqrt{-19}$ and $18 - \sqrt{-19}$ are not third powers in R (just take $(a + b\sqrt{-19})^3 = 18 - \sqrt{-19}$ and work out that no such $a, b \in \mathbb{Z}$ exist).
In this example we see that ideals behave better than elements. We will extend the phenomenon that we just saw to the unique factorisation of any ideal in a Dedekind ring into a product of prime ideals.

Proposition 4.7. *Let R be a Noetherian integral domain, $K = \mathrm{Frac}(R)$ and $(0) \neq I \subset K$ a subset. Then the following two statements are equivalent:*

(i) I is a fractional R-ideal.

(ii) I is a finitely generated R-submodule of K (this is the definition in Neukirch's book).

Proof. '(i)⇒(ii)': By definition, there is $r \in R \setminus \{0\}$ such that $rI \subseteq R$, hence, rI is an ideal of R in the usual sense. As R is Noetherian, rI is finitely generated, say by $a_1, \ldots, a_n$. Then I is finitely generated as R-submodule of K by $\frac{a_1}{r}, \ldots, \frac{a_n}{r}$.
'(ii)⇒(i)': Suppose I is generated as R-submodule of K by $\frac{a_1}{r_1}, \ldots, \frac{a_n}{r_n}$. Then $r = r_1 \cdot \ldots \cdot r_n$ is such that $rI \subseteq R$. □

This proposition also shows us how we must think about fractional R-ideals, namely, just as R-linear combinations of a given set of fractions $\frac{a_1}{r_1}, \ldots, \frac{a_n}{r_n}$ (where we may choose a common denominator).

Definition 4.8. *Let R be an integral domain and $K = \mathrm{Frac}(R)$. A fractional R-ideal I is called an* invertible R-ideal *if there is a fractional R-ideal J such that $IJ = R$.*

Note that the term 'invertible R-ideal' applies only to fractional R-ideals (which may, of course, be integral).

Lemma 4.9. *Let R be an integral domain, $K = \mathrm{Frac}(R)$ and I a fractional R-ideal. Then the following statements hold:*

(a) $II^{-1} \subseteq R$.

(b) I *is invertible* $\Leftrightarrow II^{-1} = R$.

(c) Let J *be an invertible* R*-ideal. Then* $(I : J) = IJ^{-1}$.

(d) If $0 \neq i \in I$ *such that* $i^{-1} \in I^{-1}$*, then* $I = (i)$.

Proof. (a) holds by definition.
(b) '$\Rightarrow$': Let J be a fractional R-ideal such that $IJ = R$ (exists by definition of I being invertible). Then, on the one hand, by the definition of I^{-1} we have $J \subseteq I^{-1}$. On the other hand, $I^{-1} = I^{-1}IJ \subseteq RJ = J$, showing $J = I^{-1}$.
'$\Leftarrow$': is trivial.
(c) We show both inclusions of $\{x \in K \mid xJ \subseteq I\} = IJ^{-1}$.
'$\subseteq$': Let $x \in K$ such that $xJ \subseteq I$. This implies $x \in xR = xJJ^{-1} \subseteq IJ^{-1}$.
'$\supseteq$': We have $(IJ^{-1})J = I(JJ^{-1}) = I \subseteq I$, whence $IJ^{-1} \subseteq (I : J)$.
(d) We have $I = i(i^{-1}I) \subseteq iI^{-1}I \subseteq iR = (i) \subseteq I$. □

We include the next lemma to avoid writing down the Noetherian hypothesis in the next corollary and the subsequent definition.

Lemma 4.10. *Let* R *be an integral domain with* $K = \mathrm{Frac}(R)$*. Then any invertible* R*-ideal is finitely generated.*

Proof. Let $IJ = R$. In particular, 1 is in IJ, whence there are $i_k \in I$ and $j_k \in J$ for $k = 1, \ldots, n$ (some $n \in \mathbb{N}$) such that $1 = \sum_{k=1}^{n} i_k j_k$. Let $x \in I$. Then

$$x = x \cdot 1 = \sum_{k=1}^{n} (xj_k) i_k \in \sum_{k=1}^{n} R i_k,$$

hence, $I = \sum_{k=1}^{n} R i_k$. □

Corollary 4.11. *Let* R *be an integral domain. The set* $\mathcal{I}(R)$ *of invertible fractional* R*-ideals forms an abelian group with respect to multiplication of ideals, with* R *being the neutral element, and the inverse of* $I \in \mathcal{I}(R)$ *being* I^{-1}.
The set $\mathcal{P}(R) := \{xR \mid x \in K^\times\}$ *of principal fractional* R*-ideals forms a subgroup of* $\mathcal{I}(R)$.

Proof. This just summarises what we have seen. That $\mathcal{P}(R)$ is a subgroup is clear. □

Definition 4.12. *Let* R *be an integral domain. One calls* $\mathcal{I}(R)$ *the* group of invertible R-ideals *and* $\mathcal{P}(R)$ *the* subgroup of principal invertible R-ideals.
The quotient group $\mathrm{Pic}(R) := \mathcal{I}(R)/\mathcal{P}(R)$ *is called the* Picard group of R.
If K *is a number field and* $\mathbb{Z}_K$ *its ring of integers, one also writes* $\mathrm{CL}(K) := \mathrm{Pic}(\mathbb{Z}_K)$*, and calls it the* ideal class group of K.

Corollary 4.13. *Let* R *be an integral domain and* $K = \mathrm{Frac}(R)$*. Then we have the exact sequence of abelian groups*

$$1 \to R^\times \to K^\times \xrightarrow{f} \mathcal{I}(R) \xrightarrow{\mathrm{proj}} \mathrm{Pic}(R) \to 1,$$

where $f(x)$ *is the principal fractional* R*-ideal* xR.

Proof. The exactness is trivially checked. Note, in particular, that $xR = R$ (the neutral element in the group) if and only if $x \in R^\times$. □

Corollary 4.14. *Let R be a principal ideal domain. Then $\mathrm{Pic}(R) = \{R\}$ (the group with one element).*

Proof. This is the case by definition: that every ideal is principal implies that every fractional ideal is principal, i.e. $\mathcal{I}(R) = \mathcal{P}(R)$, whence their quotient is the group with one element. □

Example 4.15. *The groups $\mathrm{CL}(\mathbb{Q}) = \mathrm{Pic}(\mathbb{Z})$ and $\mathrm{Pic}(K[X])$ (for K a field) are trivial.*

5 Ideals in Dedekind rings

We will now give a 'local characterisation' of invertible ideals. Recall that, if R is a ring and $\mathfrak{p}$ is a prime ideal, we defined the localisation of R at $\mathfrak{p}$ as $R_\mathfrak{p} := S^{-1}R$, where the multiplicatively closed subset $S \subseteq R$ is given as $S = R \setminus \mathfrak{p}$ (the multiplicative closedness being precisely the property of $\mathfrak{p}$ being a prime ideal). For any R-module, we defined its localisation at $\mathfrak{p}$ as $M_\mathfrak{p} = S^{-1}M$. Consequently, if I is a fractional R-ideal, then $I_\mathfrak{p} \subseteq K$ (note that $S^{-1}K = K$ and thus the embedding $I \hookrightarrow K$ gives rise to an embedding $I_\mathfrak{p} \hookrightarrow K$). If $I \trianglelefteq R$ is an ideal in the usual sense, then $I_\mathfrak{p} = S^{-1}I \subseteq S^{-1}R = R_\mathfrak{p} \subseteq K$. See the lecture on Commutative Algebra for more details on localisation. Very concretely, we have $R_\mathfrak{p} = \{\frac{r}{s} \in K \mid r \in R, s \in S\}$ and $I_\mathfrak{p} = \{\frac{i}{s} \in K \mid i \in I, s \in S\}$. Moreover, we have $(I_\mathfrak{p})^{-1} = (I^{-1})_\mathfrak{p}$.
We first prove that the invertibility of an ideal is a local property.

Theorem 5.1. *Let R be an integral domain and I a fractional R-ideal. Then the following statements are equivalent:*

(i) I is invertible.

(ii)
- *I is finitely generated as R-submodule of $K := \mathrm{Frac}(R)$ (this assumption is unnecessary if R is Noetherian by Proposition 4.7) and*
- *$I_\mathfrak{m}$ is a principal fractional $R_\mathfrak{m}$-ideal for all maximal ideals $\mathfrak{m} \lhd R$.*

Proof. '$\Rightarrow$': Let I be invertible. Then Lemma 4.10 implies that I is finitely generated. Since $II^{-1} = R$, there are $i_k \in I$ and $j_k \in I^{-1}$ for $k = 1, \dots, n$ and for some $n \in \mathbb{N}$ such that $1 = \sum_{k=1}^n i_k j_k$. Let $\mathfrak{m}$ be any maximal ideal. There is some index k such that $i_k j_k \notin \mathfrak{m}$, as otherwise $1 \in \mathfrak{m}$. Hence, $i_k j_k =: s \in R \setminus \mathfrak{m}$, so that $i_k^{-1} = \frac{j_k}{s} \in I_\mathfrak{m}^{-1}$. Lemma 4.9 (d) implies $I_\mathfrak{m} = i_k R_\mathfrak{m}$.
'$\Leftarrow$': Let us assume the contrary, i.e. $II^{-1} \subsetneq R$. Then there is a maximal ideal $\mathfrak{m} \lhd R$ such that $II^{-1} \subseteq \mathfrak{m}$. By assumption we have $I_\mathfrak{m} = xR_\mathfrak{m}$ with some $x \in I$ (after clearing denominators). The finite generation of I implies $I = (i_1, \dots, i_n)$ for some $n \in \mathbb{N}$. For each $k = 1, \dots, n$ we find $r_k \in R$ and we find $s \in R \setminus \mathfrak{m}$ such that

$$i_k = x\frac{r_k}{s} \quad \text{(same denominator without loss of generality).}$$

Hence, we have $R \ni r_k = s i_k x^{-1}$ for all $k = 1, \dots, n$. Thus, we have $sx^{-1}I \subseteq R$, whence $sx^{-1} \in I^{-1}$. We conclude $s \in xI^{-1} \subseteq II^{-1} \subseteq \mathfrak{m}$, which is a contradiction because s is not in $\mathfrak{m}$. □

The property (ii) is called: 'I is locally free of rank 1'. In Algebraic Geometry one usually takes this property as the defining property of invertibility: one defines invertible sheaves as those sheaves that are locally free of rank 1.

Example 5.2. *We continue Example 4.6. Hence, $R = \mathbb{Z}[\sqrt{-19}]$ and we consider the ideal $I := (18+\sqrt{-19}, 7) = (7, 3-\sqrt{-19})$ (to see the equality, just substract 21 from the first generated in the first ideal).*
We first show that I is maximal. That we do as follows. Consider the ring homomorphism

$$\alpha : \mathbb{Z}[X] \xrightarrow{X\mapsto 3} \mathbb{F}_7.$$

Its kernel clearly is $(7, X-3)$. Moreover, consider the natural projection

$$\pi : \mathbb{Z}[X] \twoheadrightarrow \mathbb{Z}[X]/(X^2+19) \xrightarrow{\sim\, X\mapsto\sqrt{-19}} \mathbb{Z}[\sqrt{-19}].$$

Also consider the surjection

$$\phi : \mathbb{Z}[\sqrt{-19}] \to \mathbb{F}_7, \quad a + b\sqrt{-19} \mapsto \overline{a} + \overline{b}\overline{3}.$$

We note that $\alpha = \phi \circ \pi$, from which we conclude that the kernel of ϕ is the image under π of $(7, X-3)$, hence, is equal to $(7, \sqrt{-19}-3) = I$ as claimed. Hence, I is maximal because the quotient $R/I = \mathbb{F}_7$ is a field.
Next, we compute the localisation of I at a maximal ideal $\mathfrak{m} \lhd \mathbb{Z}[\sqrt{-19}]$.
First case: $\mathfrak{m} \neq I$. *Then there is $x \in I \setminus \mathfrak{m}$, so that $I_\mathfrak{m} = R_\mathfrak{m}$ because $I_\mathfrak{m}$ contains a unit of $R_\mathfrak{m}$.*
Second case: $\mathfrak{m} = I$. *Then we claim that $I_\mathfrak{m} = 7R_\mathfrak{m}$. For this, we have to show that $3-\sqrt{-19} \in 7R_\mathfrak{m}$. We have:*

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

Note that $4 \notin I$ and $3+\sqrt{-19} \notin I$ (to see the former, observe that in the contrary case $2 \cdot 4 - 7 = 1 \in I$; to see the latter observe that in the contrary case $7 - (3+\sqrt{-19}) - (3-\sqrt{-19}) = 1 \in I$). Hence, $\frac{3+\sqrt{-19}}{4}$ is a unit in $R_\mathfrak{m}$, proving the claim.

Lemma 5.3. *Let R be a Noetherian integral domain with field of fractions K. For every ideal $0 \neq I \trianglelefteq R$, there is $n \in \mathbb{N}$ and there are non-zero prime ideals $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$ such that*

$$\mathfrak{p}_1 \cdot \mathfrak{p}_2 \cdot \ldots \cdot \mathfrak{p}_n \subseteq I.$$

Proof. Consider the set

$$\mathcal{M} := \{0 \neq I \trianglelefteq R \mid \text{ the assertion is wrong for } I\}.$$

We want to show $\mathcal{M} = \emptyset$. So, let us assume $\mathcal{M} \neq \emptyset$. We want to apply Zorn's lemma to obtain a maximal element J in $\mathcal{M}$, i.e. an element $J \in \mathcal{M}$ such that for all ideals $J \subsetneq I$ we have $I \notin \mathcal{M}$.
Note that $\mathcal{M}$ has a partial ordering given by $\subseteq$. For Zorn's Lemma we have to check that every ascending chain

$$I_1 \subseteq I_2 \subseteq \ldots$$

with $I_i \in \mathcal{M}$ for $i = 1, 2, \ldots$ has an upper bound, that is, an element $I \in \mathcal{M}$ containing all the I_i. That is the case since R is Noetherian and, thus, the ideal chain becomes stationary. So, let $J \in \mathcal{M}$ be such a maximal element. We distinguish two cases.
First case: J is a prime ideal. Then $J \subseteq J$ implies $J \notin \mathcal{M}$, contradiction. Hence, we are in the
Second case: J is not a prime ideal. Consequently, there are two elements $x, y \in R$ such that $xy \in J$ but $x, y \notin J$. This allows us to consider the ideals

$$J_1 := (J, x) \supsetneq J \text{ and } J_2 := (J, y) \supsetneq J.$$

Due to the maximality of $J \in \mathcal{M}$, we have that J_1 and J_2 are not in $\mathcal{M}$. Consequently, there are $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$ and $\mathfrak{q}_1, \ldots, \mathfrak{q}_m$ non-zero prime ideals of R such that

$$\mathfrak{p}_1 \cdot \ldots \cdot \mathfrak{p}_n \subseteq J_1 \text{ and } \mathfrak{q}_1 \cdot \ldots \cdot \mathfrak{q}_m \subseteq J_2.$$

This implies

$$\mathfrak{p}_1 \cdot \ldots \cdot \mathfrak{p}_n \cdot \mathfrak{q}_1 \cdot \ldots \cdot \mathfrak{q}_m \subseteq J_1 J_2 = (J, x)(J, y) \subseteq J,$$

which is also a contradiction. Hence, $\mathcal{M} = \emptyset$. □

Corollary 5.4. *Let R be a local Noetherian integral domain of Krull dimension 1. Then every non-zero ideal $I \trianglelefteq R$ contains a power of the maximal ideal $\mathfrak{p}$.*

Proof. Since R is a local Noetherian integral domain of Krull dimension 1, its only non-zero prime ideal is $\mathfrak{p}$. Hence, the assertion follows directly from Lemma 5.3. □

Corollary 5.5. *Let R be a Noetherian integral domain of Krull dimension 1. Then every non-zero ideal $I \triangleleft R$ with $I \neq R$ is contained in only finitely many maximal ideals of R. More precisely, if $\mathfrak{p}_1 \cdot \ldots \cdot \mathfrak{p}_n \subseteq I$, then I is not contained in any maximal ideal different from $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$.*

Proof. By Lemma 5.3 there are non-zero prime ideals $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$ such that $\mathfrak{p}_1 \cdot \ldots \cdot \mathfrak{p}_n \subseteq I$. Let now $\mathfrak{m}$ be a maximal ideal of R containing I. We want to show that $\mathfrak{m}$ is equal to one of the $\mathfrak{p}_i$, which proves the assertions. Assume, hence, that $\mathfrak{m}$ is none of the $\mathfrak{p}_i$. As the Krull dimension is 1, none of the $\mathfrak{p}_i$ can be contained in $\mathfrak{m}$. Consequently, for each $i = 1, \ldots, n$ the ideal $\mathfrak{p}_i$ is coprime to $\mathfrak{m}$. There are thus $x_i \in \mathfrak{p}_i$ and $y_i \in \mathfrak{m}$ such that $1 = x_i + y_i$. We conclude

$$\mathfrak{m} \supseteq \mathfrak{p}_1 \cdot \ldots \cdot \mathfrak{p}_n \ni x_1 \cdot \ldots \cdot x_n = (1 - y_1) \cdot \ldots \cdot (1 - y_n) \in 1 + \mathfrak{m},$$

which is the desired contradiction. □

Lemma 5.6. *Let R be an integral domain and I a fractional R-ideal. Then $I = \bigcap_{\mathfrak{m} \triangleleft R \text{ maximal}} I_{\mathfrak{m}} \subset K$. In particular, $R = \bigcap_{\mathfrak{m} \triangleleft R \text{ maximal}} R_{\mathfrak{m}} \subset K$ (see also the lecture on Commutative Algebra).*

Proof. We show both inclusions.
'$\subseteq$': is trivial because $I \subseteq I_{\mathfrak{m}}$ for all prime ideals (and, hence, in particular, all maximal ideals) $\mathfrak{m}$, as K is an integral domain.
'$\supseteq$': Let $x \in \bigcap_{\mathfrak{m} \triangleleft R \text{ maximal}} I_{\mathfrak{m}}$ and consider the ideal $J := \{r \in R \mid rx \in I\} \trianglelefteq R$. We want to show $J = R$ because then $x \in I$. If $J \neq R$, then J is contained in some maximal ideal $\mathfrak{m} \triangleleft R$. Write $x = \frac{a}{s}$ with $a \in I$ and $s \in R \setminus \mathfrak{m}$. Because $sx = a \in I$, it follows $s \in J \subseteq \mathfrak{m}$, which is a contradiction. □

Recall that for a prime ideal $\mathfrak{p} \lhd R$, the equality $\mathfrak{p}R_\mathfrak{p} \cap R = \mathfrak{p}$ was shown in the lecture on Commutative Algebra. This equality can also be checked directly, like this: if $\frac{x}{s} = \frac{r}{1}$ with $x \in \mathfrak{p}$, $r \in R$ and $s \in R \setminus \mathfrak{p}$, then $x = rs \in \mathfrak{p}$, whence $r \in \mathfrak{p}$ by the prime ideal property of $\mathfrak{p}$.

Lemma 5.7. *Let R be a Noetherian integral domain of Krull dimension* 1.

(a) Let $\mathfrak{p} \lhd R$ be a maximal ideal and $\mathfrak{a} \lhd R_\mathfrak{p}$ any nonzero ideal. Let $J := R \cap \mathfrak{a}$. Then $J_\mathfrak{p} = \mathfrak{a}$ and $J_\mathfrak{m} = R_\mathfrak{m}$ for all maximal ideals $\mathfrak{m} \neq \mathfrak{p}$.

(b) Let $\mathfrak{p}$ be a maximal ideal of R. Then $\mathfrak{p}^n = \mathfrak{p}^n R_\mathfrak{p} \cap R = (\mathfrak{p}R_\mathfrak{p})^n \cap R$ for all $n \in \mathbb{N}$.

Proof. (a) We first prove $J_\mathfrak{p} = \mathfrak{a}$:
'$\subseteq$': Let $r \in R \cap \mathfrak{a} = J$, that means $\frac{r}{1} \in \mathfrak{a}$, whence $\frac{r}{s} \in \mathfrak{a}$ for all $s \in S = R \setminus \mathfrak{p}$.
'$\supseteq$': Let $\frac{a}{s} \in \mathfrak{a}$ with $a \in R$ and $s \in S = R \setminus \mathfrak{p}$. Then $s\frac{a}{s} = \frac{a}{1} \in \mathfrak{a} \cap R = J$, whence $\frac{a}{s} \in J_\mathfrak{p}$.
That $J_\mathfrak{m} = R_\mathfrak{m}$ for all maximal ideals $\mathfrak{m} \neq \mathfrak{p}$ follows like this: By Corollary 5.4 there is $n \in \mathbb{N}$ such that $(\mathfrak{p}R_\mathfrak{p})^n \subseteq \mathfrak{a}$. We have $\mathfrak{p}^n \subseteq (\mathfrak{p}R_\mathfrak{p})^n \cap R$. Consequently, $\mathfrak{p}^n \subseteq (\mathfrak{p}R_\mathfrak{p})^n \cap R \subseteq \mathfrak{a} \cap R = J$. By Corollary 5.5 we have that $J \not\subseteq \mathfrak{m}$ for all maximal ideals $\mathfrak{m} \neq \mathfrak{p}$, whence $J_\mathfrak{m} = R_\mathfrak{m}$.
(b) Put $I = \mathfrak{p}^n$ for some $n \in \mathbb{N}$. Then by Corollary 5.5 $I_\mathfrak{m} = R_\mathfrak{m}$ if $\mathfrak{m} \neq \mathfrak{p}$ and $I_\mathfrak{p} = \mathfrak{p}^n R_\mathfrak{p}$. The equality $\mathfrak{p}^n R_\mathfrak{p} = (\mathfrak{p}R_\mathfrak{p})^n$ is clear. Now we obtain from Lemma 5.6

$$\mathfrak{p}^n = I = \bigcap_{\mathfrak{m} \lhd R \text{ maximal}} I_\mathfrak{m} = \Big(\bigcap_{\mathfrak{m} \lhd R \text{ maximal, } \mathfrak{m} \neq \mathfrak{p}} R_\mathfrak{m} \Big) \cap \mathfrak{p}^n R_\mathfrak{p}$$
$$= \Big(\bigcap_{\mathfrak{m} \lhd R \text{ maximal}} R_\mathfrak{m} \Big) \cap \mathfrak{p}^n R_\mathfrak{p} = R \cap \mathfrak{p}^n R_\mathfrak{p},$$

as claimed. □

Theorem 5.8. *Let R be a Noetherian integral domain of Krull dimension* 1. *Then the map*

$$\Phi : \mathcal{I}(R) \to \bigoplus_{0 \neq \mathfrak{p} \lhd R \text{ prime ideal}} \mathcal{P}(R_\mathfrak{p}), \quad I \mapsto (\ldots, I_\mathfrak{p}, \ldots),$$

is an isomorphism of abelian groups.

The meaning of this theorem is that any non-zero invertible ideal $I \lhd R$ is uniquely determined by all its localisations $I_\mathfrak{p}$ (at the non-zero prime ideals of R).

Proof. There are four things to show.

- Φ is well-defined. First recall that Theorem 5.1 shows that $I_\mathfrak{p}$ is a principal ideal. Second, recall that an element of a direct sum only has finitely many components different from the identity; the identity of $\mathcal{P}(R_\mathfrak{p})$ is $(1) = R_\mathfrak{p}$.

  We first show that the statement is correct for any integral ideal $0 \neq I \trianglelefteq R$. By Corollary 5.5, I is contained in only finitely many maximal ideals $\mathfrak{p}$. For all others, we have $I \not\subseteq \mathfrak{p}$, hence $I_\mathfrak{p} = R_\mathfrak{p} = (1)$. Now let us suppose that I is a fractional R-ideal. Then there is some $r \in R \setminus \{0\}$ such that $0 \neq rI \trianglelefteq R$ is an integral ideal. Thus, we may (and do) apply the previous reasoning to the integral ideals rI and $(r) = rR$, and we obtain that for all prime ideals but possibly finitely many $(rI)_\mathfrak{p} = R_\mathfrak{p}$ and $(r)_\mathfrak{p} = rR_\mathfrak{p} = R_\mathfrak{p}$. For any such $\mathfrak{p}$ we hence have $R_\mathfrak{p} = (rI)_\mathfrak{p} = (rR_\mathfrak{p}) \cdot I_\mathfrak{p} = R_\mathfrak{p} \cdot I_\mathfrak{p} = I_\mathfrak{p}$, proving the assertion.

- Φ is a group homomorphism. This is a property of localisations (already used in the previous item): Let $S = R \setminus \mathfrak{p}$. Then $(S^{-1}I_1)(S^{-1}I_2) = S^{-1}(I_1I_2)$, i.e. $\Phi(I_1I_2) = \Phi(I_1)\Phi(I_2)$.
- Φ is injective. Suppose $I_\mathfrak{p} = R_\mathfrak{p}$ for all non-zero prime ideals $\mathfrak{p}$ of R. Then we have

$$I = \bigcap_{0 \neq \mathfrak{p} \lhd R \text{ prime ideal}} I_\mathfrak{p} = \bigcap_{0 \neq \mathfrak{p} \lhd R \text{ prime ideal}} R_\mathfrak{p} = R$$

  by Lemma 5.6.
- Φ is surjective. As Φ is a group homomorphism, it suffices to construct an invertible ideal $J \in \mathcal{I}(R)$ such that, for given maximal ideal $\mathfrak{p} \lhd R$ and given principal ideal $\mathfrak{a} \lhd R_\mathfrak{p}$, we have $J_\mathfrak{m} = R_\mathfrak{m}$ for all nonzero prime ideals $\mathfrak{p} \neq \mathfrak{m}$ and $J_\mathfrak{p} = \mathfrak{a}$. Lemma 5.7 (a) shows that $J := R \cap \mathfrak{a}$ does precisely this.

This concludes the proof. □

We are now going to apply the above to Dedekind rings. For this, we recall the following characterisation from the lecture on Commutative Algebra.

Proposition 5.9. *Let R be a Noetherian integral domain of Krull dimension 1. Then the following assertions are equivalent:*

(i) *R is a Dedekind ring.*

(ii) *R is integrally closed.*

(iii) *$R_\mathfrak{m}$ is integrally closed for all maximal ideals $\mathfrak{m} \lhd R$.*

(iv) *$R_\mathfrak{m}$ is regular for all maximal ideals $\mathfrak{m} \lhd R$.*

(v) *$R_\mathfrak{m}$ is a principal ideal domain for all maximal ideals $\mathfrak{m} \lhd R$.*

Corollary 5.10. *Let R be a Dedekind ring. Then any fractional R-ideal is invertible.*

Proof. By Proposition 5.9 we know that $R_\mathfrak{m}$ is a principal ideal domain for all maximal ideals $\mathfrak{m} \lhd R$. Hence, given any fractional R-ideal I, we have that $I_\mathfrak{m}$ is principal for all $\mathfrak{m}$, which by Theorem 5.1 implies that I is invertible. □

We will mostly be interested in (iv) of Proposition 5.9. Hence, it is useful to quickly recall the definition of a regular local ring and the main property of such rings in our case of Krull dimension 1.

Definition 5.11. *A Noetherian local ring with maximal ideal $\mathfrak{m}$ is called* regular *if $\dim_{R/\mathfrak{m}}(\mathfrak{m}/\mathfrak{m}^2)$ equals the Krull dimension of R.*

Proposition 5.12. *Let R be a regular local ring of Krull dimension 1. Then there is $x \in R$ such that all non-zero ideals are of the form (x^n) for some $n \in \mathbb{N}$.*
Such a ring is called a discrete valuation ring.

Corollary 5.13. *Let R be a regular local ring of Krull dimension 1 and let $\mathfrak{p}$ be its maximal ideal. Then there is $x \in R$ such that all fractional ideals of R are of the form $(x)^n = \mathfrak{p}^n$ for some $n \in \mathbb{Z}$. Moreover, the map*

$$\mathbb{Z} \to \mathcal{I}(R), \quad n \mapsto \mathfrak{p}^n$$

is an isomorphism of abelian groups.

Proof. By Proposition 5.12, the unique maximal ideal $\mathfrak{p}$ is equal to (x), and, hence, all nonzero integral ideals of R are of the form $\mathfrak{p}^n$ for some $n \in \mathbb{N}$. It is clear that $(x^n) = \mathfrak{p}^n$ is invertible with inverse $((\frac{1}{x})^n) = (x)^{-n}$. The final statement is an immediate consequence. □

Definition 5.14. *Let R be a Dedekind ring and I be an invertible R-ideal. For a maximal ideal $\mathfrak{p} \lhd R$, by Proposition 5.12, there is a unique integer $n \geq 0$ such that $I_\mathfrak{p} = (\mathfrak{p}R_\mathfrak{p})^n$. We write $\operatorname{ord}_\mathfrak{p}(I) := n$.*

Now we can prove unique ideal factorisation.

Theorem 5.15. *Let R be a Dedekind ring. The map*

$$\Phi : \mathcal{I}(R) \to \bigoplus_{0 \neq \mathfrak{p} \lhd R \text{ prime ideal}} \mathbb{Z}, \quad I \mapsto (\ldots, \operatorname{ord}_\mathfrak{p}(I), \ldots)$$

is an isomorphism of abelian groups. Every $I \in \mathcal{I}(R)$ can be uniquely written as

$$I = \prod_{0 \neq \mathfrak{p} \lhd R \text{ prime ideal}} \mathfrak{p}^{\operatorname{ord}_\mathfrak{p}(I)}$$

(note that the product is finite).

Proof. The first statement follows from composing the isomorphism of Theorem 5.8 (which also implies the finiteness of the product) with the isomorphism $\mathcal{P}(R_\mathfrak{p}) \to \mathbb{Z}$, given by $\operatorname{ord}_\mathfrak{p}$ (the inverse to the isomorphism from Corollary 5.13).
It suffices to show the final claim for invertible integral ideals because we can write any fractional R-ideal as a quotient of two integral ones: $rI \trianglelefteq R$ for some $r \in R \setminus \{0\}$, whence $I = (rI) \cdot (r)^{-1}$. To see the final claim, for $I \trianglelefteq R$ we compute

$$\begin{aligned} I &= \bigcap_{0 \neq \mathfrak{p} \lhd R \text{ prime ideal}} I_\mathfrak{p} = \Big(\bigcap_{0 \neq \mathfrak{p} \lhd R \text{ prime ideal}} I_\mathfrak{p} \Big) \cap R = \bigcap_{0 \neq \mathfrak{p} \lhd R \text{ prime ideal}} (I_\mathfrak{p} \cap R) \\ &= \bigcap_{0 \neq \mathfrak{p} \lhd R \text{ prime ideal}} ((\mathfrak{p}R_\mathfrak{p})^{\operatorname{ord}_\mathfrak{p}(I)} \cap R) = \bigcap_{0 \neq \mathfrak{p} \lhd R \text{ prime ideal}} \mathfrak{p}^{\operatorname{ord}_\mathfrak{p}(I)} = \prod_{0 \neq \mathfrak{p} \lhd R \text{ prime ideal}} \mathfrak{p}^{\operatorname{ord}_\mathfrak{p}(I)}, \end{aligned}$$

where we used Lemmas 5.6 and 5.7 and the pairwise coprimeness of the maximal ideals, so that the intersection becomes a product. □

Remark 5.16. *Theorem 5.15 is a generalisation of unique factorisation in a principal ideal domain.*

Remark 5.17. *Let I be an invertible integral R-ideal of a Noetherian integral domain of Krull dimension 1. For a maximal ideal $\mathfrak{p} \lhd R$ we define* the $\mathfrak{p}$-primary component of I *as $I_{(\mathfrak{p})} := I_\mathfrak{p} \cap R$. Lemma 5.7 (a) shows that the localisation at a maximal ideal $\mathfrak{m}$ is the following one:*

$$(I_{(\mathfrak{p})})_\mathfrak{m} = \begin{cases} I_\mathfrak{p} & \text{if } \mathfrak{p} = \mathfrak{m}, \\ R_\mathfrak{m} & \text{if } \mathfrak{p} \neq \mathfrak{m}. \end{cases}$$

Moreover, the primary components behave 'multiplicatively':

$$(IJ)_{(\mathfrak{p})} = I_{(\mathfrak{p})}J_{(\mathfrak{p})}$$

for any invertible integral R-ideals I and J. This is easy to see by working locally at all maximal ideals $\mathfrak{p}$ (which suffices by Theorem 5.8): the ideals on both sides have the same local components at all maximal ideals $\mathfrak{m}$.

6 Geometry of Numbers

6.1 Introduction

Up to this point, we have been studying Dedekind domains in quite some generality. In this last part of the series of lectures, we will focus on the case of rings of integers of number fields.
Recall (cf. Corollary 4.13) that, for any integral domain R, we have the following exact sequence

$$1 \longrightarrow R^\times \longrightarrow K^\times \xrightarrow{f} \mathcal{I}(R) \xrightarrow{\text{proj}} \text{Pic}(R) \longrightarrow 1$$

where:

- K is the field of fractions of R.
- $\mathcal{I}(R)$ is the group of invertible ideals of R.
- $\text{Pic}(R)$ is the Picard group of R, that is to say, the quotient of $\mathcal{I}(R)$ modulo the group $\mathcal{P}(R)$ of principal fractionals ideals of R.
- $f : K^\times \to \mathcal{I}(R)$ maps an element $x \in K$ to the principal fractional ideal xR.
- $\text{proj} : \mathcal{I}(R) \to \mathcal{I}(R)/\mathcal{P}(R) = \text{Pic}(R)$ is the projection.

We want to study this exact sequence in the particular case where $R = \mathbb{Z}_K$ is the ring of integers of a number field K. Since $\mathbb{Z}_K$ is a Dedekind domain, all fractional ideals are invertible (see Corollary 5.10). Hence $\mathcal{I}(\mathbb{Z}_K)$ is the set of all fractional ideals. Recall also that we denote $\text{Pic}(\mathbb{Z}_K) = \text{CL}(K)$ and call it the *class group* of K. The exact sequence boils down to:

$$1 \longrightarrow \mathbb{Z}_K^\times \longrightarrow K^\times \xrightarrow{f} \mathcal{I}(\mathbb{Z}_K) \xrightarrow{\text{proj}} \text{CL}(K) \longrightarrow 1 \tag{6.5}$$

The group $\text{CL}(K)$ measures the failure of $\mathbb{Z}_K$ to be a principal ideal domain. More precisely, if $\text{CL}(K)$ has just one element, then the map $f : K^\times \to \mathcal{I}(R)$ is surjective, so that each fractional ideal can be expressed as xR for some $x \in K^\times$. In other words, every fractional ideal is principal. On the other hand, the greater $\text{CL}(K)$ is, the further is f from being surjective, meaning there will be "many" fractional ideals which are not principal.
One of the fundamental results that we will prove is that $\text{CL}(K)$ is finite (hence, although $\mathbb{Z}_K$ is not a principal ideal domain, it is also "not too far" from it). Another important result will be that $\mathbb{Z}_K^\times$ is finitely generated. As a motivation to study $\mathbb{Z}_K^\times$, consider the following example.

Example 6.1. *Let d be a rational integer which is not a square. Consider the equation $x^2 = dy^2 + 1$.*

Question: Find all the solutions $(x, y) \in \mathbb{Z} \times \mathbb{Z}$ of $x^2 = dy^2 + 1$.

This equation is called Pell's equation*, and was already considered by Archimedes (287? BC–212?BC). Actually, Exercise Sheet 8 is devoted to the Problem of the Cattle of the Sun, that Archimedes proposes in a letter to Eratóstenes of Cirene.*
If $d \leq 0$, then we can rewrite the equation as $x^2 + (-d)y^2 = 1$, and it only has the trivial solutions $(\pm 1, 0)$ for $d \neq -1$ and $(\pm 1, 0), (0, \pm 1)$ for $d = -1$. But if $d > 0$, it is not obvious whether this equation has a solution (different from $(\pm 1, 0)$) or not, much less to find all solutions of the equation.

Actually, without making use of any machinery at all, we can prove that for $d > 0$ Pell's equation always admits a nontrivial solution. We need the following auxiliary lemma.

Lemma 6.2. *Let d be a positive rational integer which is not a square. There exist infinitely many pairs of integers (x, y) such that $0 < |x^2 - dy^2| < 1 + 2\sqrt{d}$.*

Proof. First let us see that there exists a pair of positive integers (x, y) with $0 < |x^2 - dy^2| < 1 + 2\sqrt{d}$, later we will see there are infinitely many. Let $m > 1$ be a positive integer. For each $j \in \{1, \ldots, m\}$, let $x_j \in \mathbb{Z}$ be such that $0 \leq x_j - j\sqrt{d} < 1$; namely, take $x_j := \lceil j\sqrt{d} \rceil$, that is, the smallest integer which is greater than or equal to $j\sqrt{d}$.
Now divide the interval

$$[0, 1) = \left[0, \frac{1}{m-1}\right) \cup \left[\frac{1}{m-1}, \frac{2}{m-1}\right) \cup \cdots \cup \left[\frac{m-2}{m-1}, 1\right).$$

There are $m - 1$ intervals, but m pairs (x_j, j). Hence (by *Dirichlet's Pidgeonhole Principle*), there is one interval which contains both $x_j - j\sqrt{d}$ and $x_k - k\sqrt{d}$ for some j, k with $j \neq k$. Assume $x_j - j\sqrt{d} \geq x_k - k\sqrt{d}$ (otherwise swap j and k). Call $x = x_j - x_k$, $y = j - k$. We will see that $x^2 - dy^2$ satisfies the desired inequalities.
First note that

$$x - y\sqrt{d} = (x_j - x_k) - (j - k)\sqrt{d} = (x_j - j\sqrt{d}) - (x_k - k\sqrt{d}) \leq \frac{1}{m-1},$$

thus

$$0 \leq x - y\sqrt{d} \leq \frac{1}{m-1}.$$

Since $1 \leq j, k \leq m$, we have $0 < |y| < m$, hence $x - y\sqrt{d} \leq \frac{1}{m-1} \leq \frac{1}{|y|}$. Now we can bound

$$\begin{aligned} 0 \leq |x^2 - dy^2| &= |(x + y\sqrt{d})(x - y\sqrt{d})| = |(x - y\sqrt{d} + 2y\sqrt{d})|(x - y\sqrt{d}) \\ &= (x - y\sqrt{d})^2 + 2|y|\sqrt{d}(x - y\sqrt{d}) \leq 1 + 2\frac{|y|}{m-1}\sqrt{d} \leq 1 + 2\frac{|y|}{|y|}\sqrt{d} = 1 + 2\sqrt{d}. \end{aligned}$$

Moreover we know that, since d is not a square, $x^2 - dy^2 \neq 0$, and $|x^2 - y^2 d| \neq 1 + 2\sqrt{d}$.
Suppose now that the set $A = \{(x, y) \in \mathbb{Z} \times \mathbb{Z} \text{ such that } 0 < |x^2 - dy^2| < 1 + 2\sqrt{d}\}$ is finite. Then choosing an $m \in \mathbb{N}$ such that $\frac{1}{m-1}$ is smaller than $x - y\sqrt{d}$ for all $(x, y) \in A$, the previous construction provides us with a pair $(x', y') \in A$ satisfying $x' - y'\sqrt{d} < \frac{1}{m-1}$, which is a contradiction. □

Proposition 6.3. *Let d be a positive rational integer which is not a square. There exists a pair of rational integers (x, y) with $y \neq 0$ such that $x^2 - dy^2 = 1$.*

Proof. Since the number of integers in $(-1 - 2\sqrt{d}, 1 + 2\sqrt{d}) \setminus \{0\}$ is finite, by Lemma 6.2 there exists one k in this set such that there are infinitely many pairs (x, y) with $x^2 - dy^2 = k$. Note that $k \neq 0$ because d is not a rational square. Moreover, since there are only finitely many residue classes in $\mathbb{Z}/k\mathbb{Z}$, we can assume that there are $\alpha, \beta \in \mathbb{Z}/k\mathbb{Z}$ such that there are infinitely many pairs (x, y) with $x^2 - dy^2 = k$ and $x \equiv \alpha \pmod{k}$, $y \equiv \beta \pmod{k}$. Take two such pairs, (x_1, y_1) and (x_2, y_2). Consider the product

$$(x_1 - y_1\sqrt{d})(x_2 + y_2\sqrt{d}) = (x_1x_2 - y_1y_2d) + (x_1y_2 - x_2y_1)\sqrt{d}.$$

Note that k divides both $x_1(x_2-x_1)+k+dy_1(y_1-y_2) = x_1(x_2-x_1)+(x_1^2-dy_1^2)+dy_1(y_1-y_2) = x_1x_2 - dy_1y_2$ and $(x_1 - x_2)y_2 - (y_1 - y_2)x_2 = x_1y_2 - x_2y_1$. Hence we can write

$$(x_1 - y_1\sqrt{d})(x_2 + y_2\sqrt{d}) = k(t + u\sqrt{d})$$

for some integers t, u. Moreover note that

$$(x_1 + y_1\sqrt{d})(x_2 - y_2\sqrt{d}) = k(t - u\sqrt{d}),$$

thus

$$k^2 = (x_1^2 - y_1^2d)(x_2^2 - y_2^2d) = k^2(t^2 - u^2d),$$

so that dividing by k^2 (which is nonzero), we get $t^2 - u^2d = 1$.
This reasoning is valid for all (x_1, y_1) and (x_2, y_2) satisfying $y_i^2 - dx_i^2 = k$ and $x_i \equiv \alpha \pmod{k}$, $y_i \equiv \beta \pmod{k}$ for $i = 1, 2$. It remains to see that we can choose (x_1, y_1) and (x_2, y_2) so that the corresponding u is nonzero. Note that, if $u = 0$, then $t = \pm 1$, so

$$(x_1 - y_1\sqrt{d})(x_2 + y_2\sqrt{d}) = k(t + u\sqrt{d}) = \pm k$$

On the other hand we have

$$(x_1 - y_1\sqrt{d})(x_1 + y_1\sqrt{d}) = x_1^2 - y_1^2d = k.$$

Therefore we get $x_1 + y_1\sqrt{d} = \pm(x_2 + y_2\sqrt{d})$
Fix one pair (x_1, y_1). Since we can choose (x_2, y_2) from an infinity of pairs, we can assume, without loss of generality, that $x_2 + y_2\sqrt{d} \neq \pm(x_1 + y_1\sqrt{d})$ (just take $x_2 \neq \pm x_1$, $y_2 \neq \pm y_1$), and hence the solution (t, u) that we obtain satisfies $u \neq 0$. □

Remark 6.4. *Let d be a positive rational integer which is not a square. So there exists an integer x such that $d = d'x^2$ with d' a squarefree integer. Consider the ring of integers $\mathbb{Z}_K$ of $K = \mathbb{Q}(\sqrt{d})$. Recall that $\mathbb{Z}_K$ is $\mathbb{Z}[\sqrt{d'}]$ if $d' \equiv 2, 3 \pmod{4}$, $\mathbb{Z}[\frac{1+\sqrt{d'}}{2}]$ if $d' \equiv 1 \pmod{4}$ (see Example 3.6).*
In both cases we have that, for any $x, y \in \mathbb{Z}$, $z = x + y\sqrt{d} \in \mathbb{Z}_K$, and

$$x^2 - dy^2 = 1 \Leftrightarrow \mathrm{Norm}_{K/\mathbb{Q}}(z) = 1$$

$$\mathrm{Norm}_{K/\mathbb{Q}}(z) = 1 \Rightarrow z \in \mathbb{Z}_K^\times.$$

Note moreover that the set $\{x + y\sqrt{d}$ *such that* $x, y \in \mathbb{Z}$ *and* $\mathrm{Norm}_{N/\mathbb{Q}}(x + y\sqrt{d}) = 1\} \subseteq \mathbb{Z}_K^\times$ *is a subgroup.*
We will see that the knowledge of the structure group of unities of quadratic fields completely determines the set of solutions of the Pell equation.

The tool that we will use to study the exact sequence (6.5) is called Geometry of Numbers. This consists of viewing rings of integers as special subsets of $\mathbb{R}^n$ (namely lattices), and using some analytic tools (computing volumes) to obtain results concerning $\mathbb{Z}_K$.

6.2 Lattices

In this section we work with $(\mathbb{R}^n)$, endowed with the following structures:

- A $\mathbb{R}$-vector space structure $(\mathbb{R}^n, +, \cdot)$, where $+$ and $\cdot$ are defined componentwise.
- A $\mathbb{Z}$-module structure $(\mathbb{R}^n, +)$, obtained from the vector structure above by forgetting the scalar multiplication.
- A normed vector space structure $(\mathbb{R}^n, +, \cdot, \|\cdot\|_2)$, where the $\mathbb{R}$-vector space structure is the one above and the norm is defined as

$$\|\cdot\|_2 : \mathbb{R}^n \to \mathbb{R}$$
$$\|(a_1, \ldots, a_n)\|_2 = \sqrt{|a_1|^2 + \cdots + |a_n|^2}.$$

We will denote by $\{e_1, \ldots, e_n\}$ the canonical basis of $\mathbb{R}^n$ as $\mathbb{R}$-vector space, so that $\sum_{i+1}^n a_i e_i = (a_1, \ldots, a_n)$.
Given a vector $v \in \mathbb{R}^n$ and a positive real number r, we denote by $B(v; r) := \{w \in \mathbb{R}^n : \|w - v\|_2 < r\}$ the open ball of radius r centered at v and $\overline{B}(v; r) := \{w \in \mathbb{R}^n : \|w - v\|_2 \leq r\}$ the closed ball of radius r centered at v. The set of all balls $\{B(v; r) : v \in \mathbb{R}^n, r > 0\}$ is a basis for the topology in $\mathbb{R}^n$. We say that a set $A \subset \mathbb{R}^n$ is bounded if it is contained in some ball centered at $0 \in \mathbb{R}^n$. Recall that a set is compact if and only if it is closed and bounded (Theorem of Heine-Borel).
We will usually work with subgroups of $(\mathbb{R}, +)$ which are not subvector spaces. For instance, $\mathbb{Z}^n$ is one such subgroup. Given $v_1, \ldots, v_r \in \mathbb{R}^n$, we will denote by $\langle v_1, \ldots, v_r \rangle_\mathbb{Z}$ the $\mathbb{Z}$-module generated by $v_1, \ldots, v_r$ inside $\mathbb{R}^n$. Note that $\langle v_1, \ldots, v_r \rangle_\mathbb{Z}$ is a countable subset, while the vector space generated by $v_1, \ldots, v_r$ has cardinality $|\mathbb{R}|$. On the other hand, whenever we talk about linear dependence of elements of $\mathbb{R}^n$, we will always be considering $\mathbb{R}^n$ with the structure of $\mathbb{R}$-vector space.
For $x \in \mathbb{R}$, we denote by $\lfloor x \rfloor$ the integer part of x, that is, the maximum $m \in \mathbb{Z}$ such that $m \leq x$.

Definition 6.5. *A* lattice *in* $\mathbb{R}^n$ *is a* $\mathbb{Z}$*-module generated by* n *linearly independent vectors. A* basis *of a lattice* $H \subset \mathbb{R}^n$ *is a basis of* H *as a* $\mathbb{Z}$*-module.*

Note that a basis of a lattice H consists of n linearly independent vectors of $\mathbb{R}^n$, so in particular is a basis of $\mathbb{R}^n$ as $\mathbb{R}$-vector space.

Definition 6.6. *A* half-open parallelotope *(resp.* closed parallelotope*) is a subset of $\mathbb{R}^n$ of the form*

$$P := \{v \in \mathbb{R}^n : v = \sum_{i=1}^{m} a_i v_i \text{ with } 0 \le a_i < 1 \text{ for all } i\},$$
$$\left(\text{resp. } P := \{v \in \mathbb{R}^n : v = \sum_{i=1}^{m} a_i v_i \text{ with } 0 \le a_i \le 1 \text{ for all } i\}\right)$$

where $v_1, \dots, v_m \in \mathbb{R}^n$ are linearly independent. We say that P is the half-open parallelotope determined by $v_1, \dots, v_m$ *(resp.* closed parallelotope determined by $v_1, \dots, v_m$*)*

Definition 6.7. *Let $H \subset \mathbb{R}^n$ be a lattice, and $\mathcal{U} = \{u_1, \dots, u_n\}$ a basis of H. We will say that the (half-open) parallelotope P determined by $\mathcal{U}$ is a* fundamental domain for H.

Remark 6.8. *One lattice has different fundamental domains; in other words, fundamental domains are not unique.*

In this section we need to compute volumes of parallelotopes in $\mathbb{R}^n$. We mean by this the *Lebesgue measure* of the parallelotope.
We will denote by μ the Lebesgue measure on $\mathbb{R}^n$. We will not recall here its definition, but just one very important property: it is invariant under translation; that is, for all measurable sets A and all vectors $v \in \mathbb{R}^n$, the set $A + v := \{w + v : w \in A\}$ is measurable and we have

$$\mu(A) = \mu(A + v).$$

Moreover the measure is normalized so that the measure of the standard cube $\{\sum_{i=1}^n \lambda_i e_i : 0 \le \lambda_i \le 1\}$ is equal to 1.
The following lemma can be proven in an elementary calculus course.

Lemma 6.9. *Let P be the parallelotope defined by n linearly independent vectors $v_1, \dots, v_n \in \mathbb{R}^n$, where each $v_i = \sum_{j=1}^n a_{ij} e_j$. Then $\mu(P) = |\det((a_{ij})_{1 \le i,j \le n})|$.*

Lemma 6.10. *Let $H \subset \mathbb{R}^n$ be a lattice, P, P' fundamental domains for H. Then $\mu(P) = \mu(P')$.*

Proof. Let $\mathcal{B} = \{u_1, \dots, u_n\}$ (resp. $\mathcal{B}' = \{u'_1, \dots, u'_n\}$) be a basis of H defining P (resp. P') and let $\{e_1, \dots, e_n\}$ the canonical basis of $\mathbb{R}^n$. Write $u'_i = \sum_{j=1}^n a_{ij} u_j$ with $a_{ij} \in \mathbb{Z}$, $u_i = \sum_{j=1}^n b_{ij} e_j$, $u'_i = \sum_{j=1}^n c_{ij} e_j$ with $b_{ij}, c_{ij} \in \mathbb{R}$ and set $A = (a_{ij})_{1 \le i,j \le n}$, $B = (b_{ij})_{1 \le i,j \le n}$, $C = (c_{ij})_{1 \le i,j \le n}$. We have $C = AB$. Since both $\mathcal{B}$ and $\mathcal{B}'$ are $\mathbb{Z}$-bases of H, we have $\det((a_{ij})_{1 \le i,j \le n}) = \pm 1$. And by Lemma 6.9

$$\mu(P) = |\det(B)| = |\det(B)| \cdot |\det(A)| = |\det(C)| = \mu(P').$$

□

Definition 6.11. *Let $H \subset \mathbb{R}^n$ be a lattice. We define the* volume *of H as*

$$v(H) := \mu(P),$$

for some fundamental domain P of H.

Lemma 6.12. *Let $H \subset \mathbb{R}^n$ be a lattice and P be a fundamental domain.*

- *For each $v \in \mathbb{R}^n$ there exists a unique $w \in P$ such that $v - w \in H$.*
- *$\mathbb{R}^n$ is the disjoint union of the family $\{P + u\}_{u \in H}$.*

Proof. See Sheet 9. □

Definition 6.13. *A subgroup $H \subset \mathbb{R}^n$ is called* discrete *if, for any compact subset $K \subset \mathbb{R}^n$, $H \cap K$ is a finite set.*

Remark 6.14. *Since a subset of $\mathbb{R}^n$ is compact if and only if it is closed and bounded, then a subgroup $H \subset \mathbb{R}^n$ is discrete if and only if for every $r > 0$, $H \cap \overline{B}(0; r)$ is finite.*

Example 6.15. • *Let $v_1, \dots, v_m \in \mathbb{R}^n$ be m linearly independent vectors. Then $\langle v_1, \dots, v_m \rangle_{\mathbb{Z}}$ is a discrete subgroup. Indeed, given any $r > 0$, we can show that $\langle v_1, \dots, v_m \rangle_{\mathbb{Z}} \cap \overline{B}(0; r)$ is finite as follows:*

First of all, complete $v_1, \dots, v_m$ to a basis $v_1, \dots, v_n$ of $\mathbb{R}^n$. It suffices to show that the intersection $\langle v_1, \dots, v_n \rangle_{\mathbb{Z}} \cap \overline{B}(0; r)$ is finite.

Consider the linear map

$$f : \mathbb{R}^n \to \mathbb{R}^n$$
$$v_i \mapsto e_i \text{ for all } i = 1, \dots n.$$

Thus $f(\sum_{i=1}^n \lambda_i v_i) = \sum_{i=1}^n \lambda_i e_i$.

Linear maps between finite dimensional finite-dimensional $\mathbb{R}$-vector spaces are bounded operators; that is to say there exists a constant C such that, for all $v \in \mathbb{R}^n$,

$$\|f(v)\|_2 \leq C \cdot \|v\|_2$$

Indeed, we have that

$$\|f(\sum_{i=1}^n a_i e_i)\|_2 \leq \sum_{i=1}^n |a_i| \cdot \|f(e_i)\|_2 \leq \max\{|a_i| : 1 \leq i \leq n\} \cdot \sum_{i=1}^n \|f(e_i)\|_2$$

Taking $C = \sum_{i=1}^n \|f(e_i)\|_2$, it suffices to observe that

$$\max\{|a_i| : 1 \leq i \leq n\} \leq \sqrt{\sum_{i=1}^n |a_i|^2} = \|\sum_{i=1}^n a_i e_i\|_2.$$

Therefore, we have that

$$\|\sum_{i=1}^n \lambda_i e_i\|_2 \leq C \cdot \|\sum_{i=1}^n \lambda_i v_i\|_2. \tag{6.6}$$

Assume now that $v = \sum_{i=1}^n \lambda_i v_i$ with some $\lambda_{i_0} > rC$. Then Equation 6.6 implies that

$$\|v\|_2 \geq \frac{1}{C} \|\sum_{i=1}^n \lambda_i e_i\|_2 \geq \frac{1}{C} |\lambda_{i_0}| > r,$$

hence $v \notin \overline{B}(0;r)$. Thus

$$\langle v_1, \dots, v_n \rangle_{\mathbb{Z}} \cap \overline{B}(0;r) \subset \left\{ \sum_{i=1}^{n} \lambda_i v_i : \lambda_i \leq \frac{r}{C} \text{ for all } i \right\},$$

which is a finite set.

- *Let $v \in \mathbb{R}^n$ be a nonzero vector. Then $\langle v, \sqrt{2}v \rangle_{\mathbb{Z}}$ is not a discrete subgroup of $\mathbb{R}^n$ (see Sheet 9).*

We have the following characterisation of discrete subgroups of $\mathbb{R}^n$.

Proposition 6.16. *Let H be a discrete subgroup of $\mathbb{R}^n$. Then H is generated as a $\mathbb{Z}$-module by m linearly independent vectors for some $m \leq n$.*

Proof. We can assume without loss of generality that $H \neq \{0\}$. Let

$$m := \max\{r : \text{ there exist } v_1, \dots, v_r \in H \text{ linearly independent in } \mathbb{R}^n\}. \tag{6.7}$$

Since the numbers r appearing in (6.7) are bounded by n, we have that m is a finite number between 0 and n. Since $H \neq \{0\}$, we have that $m \geq 1$. Now let $u_1, \dots, u_m \in H$ be m vectors which are linearly independent in $\mathbb{R}^n$. Fix any $v \in H$ nonzero. Then the set $\{u_1, \dots, u_m, v\}$ is linearly dependent by the maximality of m, so there exist $\lambda_1, \dots, \lambda_m \in \mathbb{R}$ such that $v = \sum_{i=1}^m \lambda_i u_i$. For each $j \in \mathbb{N}$, we consider

$$v_j := \sum_{i=1}^{m} (j\lambda_i - \lfloor j\lambda_i \rfloor) u_i = jv - \sum \lfloor j\lambda_i \rfloor u_i \in H.$$

On the other hand, $v_j \in \{w \in \mathbb{R}^n : w = \sum_{i=1}^m a_i u_i \text{ with } 0 \leq a_i \leq 1\} =: P$, and the set P is compact (because it is closed and bounded) so v_j belongs to the finite set $H \cap P$. This implies already that H is a $\mathbb{Z}$-module of finite type (more precisely, we have proven that every v in H can be written as $v_1 + \sum_{i=1}^m \lfloor \lambda_i \rfloor u_i$, so H is generated as a $\mathbb{Z}$-module by the finite set $\mathcal{G} = (H \cap P) \cup \{u_1, \dots, u_m\}$). Since the set $\{v_j : j \in \mathbb{N}\}$ is finite, there must exist j, k different natural numbers such that $v_j = v_k$, that is $\sum_{i=1}^m (j\lambda_i - \lfloor j\lambda_i \rfloor) u_i = \sum_{i=1}^m (k\lambda_i - \lfloor k\lambda_i \rfloor) u_i$. Since the u_i's are linearly independent, we get that for all i, $(j-k)\lambda_i = \lfloor j\lambda_i \rfloor - \lfloor k\lambda_i \rfloor$. In particular, for all i, $\lambda_i \in \mathbb{Q}$. Since this is valid for all $v \in H$, we get that H is a finitely generated $\mathbb{Z}$-module contained in the $\mathbb{Q}$-vector space generated by $u_1, \dots, u_m$. Pick a finite number of generators of H as $\mathbb{Z}$-module (for example $\mathcal{G}$), write each of them as $\sum_{i=1}^r \lambda_i u_i$ for $\lambda_i \in \mathbb{Q}$ and pick a common denominator d for all the coefficients λ_i's of all the generators. Then we have $dH \subset \langle u_1, \dots, u_m \rangle_{\mathbb{Z}}$. We now apply Theorem 3.12 to conclude that dH is a free $\mathbb{Z}$-module of rank smaller than or equal to m. Since we know that dH contains the free $\mathbb{Z}$-module generated by $du_1, \dots, du_m$, the rank must be precisely m. Let $u_1', \dots, u_m' \in dH$ be such that $\langle u_1', \dots, u_m' \rangle_{\mathbb{Z}} = dH$. Since dH contains the m linearly independent vectors $du_1, \dots, du_m$, it follows that $u_1', \dots, u_m'$ must span a $\mathbb{R}$-space of dimension m, hence they are linearly independent over $\mathbb{R}$. Finally, $\frac{1}{d}u_1', \dots, \frac{1}{d}u_m' \in H$ are linearly independent vectors such that $\langle \frac{1}{d}u_1', \dots, \frac{1}{d}u_m' \rangle_{\mathbb{Z}} = H$. □

Corollary 6.17. *Let $H \subset \mathbb{R}^n$ be a discrete subgroup of $\mathbb{R}^n$. The H is a lattice if and only if H is generated by n linearly independent vectors.*

Now we will state the fundamental result of this section. The idea is the following: given a lattice H, if a measurable set $S \subset \mathbb{R}^n$ is big enough (with respecto to μ), no matter what it looks like, it must contain two elements which are "equivalent modulo H", that is to say, two different elements $v_1, v_2 \in S$ with $v_1 - v_2 \in H$.

Theorem 6.18 (Minkowsky)**.** *Let $H \subset \mathbb{R}^n$ be a lattice and $S \subset \mathbb{R}^n$ be a measurable subset of $\mathbb{R}^n$ satisfying $\mu(S) > v(H)$. Then there exist $v_1, v_2 \in S$ different elements with $v_1 - v_2 \in H$.*

Proof. Sine P is a fundamental domain for H, Lemma 6.12 implies that $\mathbb{R}^n = \bigsqcup_{u\in H}(P + u)$. Intersecting both sides with S yields

$$S = \bigsqcup_{u\in H} (S \cap (P + u)).$$

Recall that H is countable. Therefore by the countable additivity of μ, we get

$$\mu(S) = \sum_{u\in H} \mu(S \cap (P + u)).$$

Since μ is invariant by translation, we get that, for all $u \in H$, $\mu(S\cap(P+u)) = \mu((S-u)\cap P)$. Now if the family of sets $\{(S - u) \cap P\}_{u\in H}$ was disjoint, we would get, using the countable additivity of μ again, that $\sum_{u\in H} \mu((S - u) \cap P) = \mu(\bigsqcup_{u\in H}(S - u) \cap P)) \leq \mu(P)$. Hence

$$\mu(S) = \sum_{u\in H} \mu(S \cap (P + u)) = \sum_{u\in H} \mu((S - u) \cap P) = \mu(\bigsqcup_{u\in H} ((S - u) \cap P))) \leq \mu(P)$$

contradicting that $\mu(S) > v(H)$. Thus the family $\{(S - u) \cap P\}_{u\in H}$ is not disjoint, that is to say, there exist $u_1, u_2 \in H$, $u_1 \neq u_2$, with $((S - u_1) \cap P) \cap ((S - u_2) \cap P) \neq \emptyset$. Let $w \in (S - u_1) \cap P) \cap ((S - u_2) \cap P)$. Then $w = v_1 - u_1 = v_2 - u_2$ for some $v_1, v_2 \in S$. And $v_1 - v_2 = u_1 - u_2 \in H$ is nonzero. □

We will use a particular case of this theorem, when S has some special properties.

Definition 6.19. *Let $S \subset \mathbb{R}^n$.*

- *S is* centrally symmetric *if, for all $v \in S$, $-v \in S$.*
- *S is* convex *if, for all $v_1, v_2 \in S$, for all $\lambda \in [0, 1]$, $\lambda v_1 + (1 - \lambda)v_2 \in S$.*

Corollary 6.20. *Let $H \subset \mathbb{R}^n$ be a lattice and $S \subset \mathbb{R}^n$ be a centrally symmetric, convex, measurable set such that $\mu(S) > 2^n v(H)$. Then $S \cap (H \setminus \{0\}) \neq \emptyset$.*

Proof. Let $S' = \frac{1}{2}S := \{\frac{1}{2}v : v \in S\}$. Note that $\mu(S') = \frac{1}{2^n}\mu(S) > v(H)$. Hence we can apply Theorem 6.18 to S' and conclude that there are elements $v_1, v_2 \in S'$ with $v_1 - v_2 \in H \setminus \{0\}$. Note furthermore that $v_1, v_2 \in S'$ implies that $2v_1, 2v_2 \in S$, and since S is centrally symmetric, also $-2v_2 \in S$. The convexity of S now implies that $v_1 - v_2 = \frac{1}{2}(2v_1) + \left(1 - \frac{1}{2}\right)(-2v_2) \in S$. Hence $v_1 - v_2 \in S \cap (H \setminus \{0\})$. □

6.3 Number rings as lattices

In this section we want to study number fields of degree n by embedding them into $\mathbb{R}^n$, in such a way that the ring of integers corresponds to a lattice.
Let $\mathbb{C}$ be the field of complex numbers. Inside $\mathbb{C}$ we have the subfield of rational numbers $\mathbb{Q}$, which can be characterised as the smallest subfield of $\mathbb{C}$ (or, in other words, the *prime field* of $\mathbb{C}$, that is to say, the intersection of all subfields of $\mathbb{C}$). We also have the subfield of $\mathbb{C}$ defined as $\overline{\mathbb{Q}} := \{z \in \mathbb{C} : z \text{ is algebraic over } \mathbb{Q}\}$. $\overline{\mathbb{Q}}$ is an algebraically closed field, and clearly it is the smallest subfield of $\mathbb{C}$ containing $\mathbb{Q}$ which is algebraically closed, hence an algebraic closure of $\mathbb{Q}$.
Let $K/\mathbb{Q}$ be a number field of degree n and let $\overline{K}$ be an algebraic closure. Since K is algebraic over $\mathbb{Q}$, $\overline{K}$ is also an algebraic closure of $\mathbb{Q}$ and hence isomorphic to $\overline{\mathbb{Q}}$. Fixing one such isomorphism, we can identify $\overline{K}$ with $\overline{\mathbb{Q}}$ and K with a subfield of $\overline{\mathbb{Q}} \subset \mathbb{C}$.
Since $\mathrm{char}(K) = 0$, K is separable, and therefore (see the Appendix to section 2) there exist n different ring homomorphism (necessarily injective) from K to $\overline{\mathbb{Q}}$ fixing $\mathbb{Q}$. Since the image of any ring homomorphism $\sigma : K \to \mathbb{C}$ must be contained in $\overline{\mathbb{Q}}$, we have that there are exactly n different ring homomorphisms $\sigma : K \hookrightarrow \mathbb{C}$ fixing $\mathbb{Q}$. We can consider the ring homomorphism

$$\begin{aligned} \Phi_0 : K &\to \mathbb{C}^n \\ x &\mapsto (\sigma_1(x), \dots, \sigma_n(x)) \end{aligned}$$

Let $\alpha : \mathbb{C} \to \mathbb{C}$ be the complex conjugation. Then, for all $\sigma \in \mathrm{Hom}_{\mathbb{Q}}(K, \mathbb{C})$, we have that $\alpha \circ \sigma \in \mathrm{Hom}_{\mathbb{Q}}(K, \mathbb{C})$, and $\alpha \circ \sigma = \sigma$ if and only if $\sigma(K) \subset \mathbb{R}$. Call r_1 the number of ring homomorphisms $\sigma : K \to \mathbb{C}$ such that $\alpha \circ \sigma = \sigma$. The remaining homomorphisms can be collected in pairs $\{\sigma, \alpha \circ \sigma\}$, so there is an even number of them. Let us call $2r_2$ this number, so that $n = r_1 + 2r_2$.
Let us enumerate the n homomorphisms in $\mathrm{Hom}(K, \mathbb{C})$ in the following way:

- Let $\sigma_1, \dots, \sigma_{r_1}$ be the r_1 homomorphisms with image contained in $\mathbb{R}$.
- Let us enumerate the r_2 pairs $\{\sigma, \alpha \circ \sigma\}$ and, for each pair, choose one of the two homomorphisms. The chosen homomorphism of the i-th pair ($1 \leq i \leq r_2$) will be σ_{r_1+i}, the other one will be $\sigma_{r_1+r_2+i}$.

Now we can define a ring homomorphism

$$\begin{aligned} \Phi_1 : K &\to \mathbb{R}^{r_1} \times \mathbb{C}^{r_2} \\ x &\mapsto (\sigma_1(x), \dots, \sigma_{r_1}(x), \sigma_{r_1+1}(x), \dots, \sigma_{r_1+r_2}(x)) \end{aligned}$$

Definition 6.21. *For $z = x + iy \in \mathbb{C}$, denote by $\mathrm{Re}z := x$ the real part of z and $\mathrm{Im}z := y$ the imaginary part of z. The map $\mathbb{C} \to \mathbb{R} \times \mathbb{R}$ defined as $z \mapsto (\mathrm{Re}z, \mathrm{Im}z)$ is an isomorphism of $\mathbb{R}$-vector spaces. Define the map*

$$\begin{aligned} \Phi : K &\to \mathbb{R}^{r_1} \times \mathbb{R}^{2r_2} \\ x &\mapsto (\sigma_1(x), \dots, \sigma_{r_1}(x), \mathrm{Re}\sigma_{r_1+1}(x), \mathrm{Im}\sigma_{r_1+1}(x) \dots, \mathrm{Re}\sigma_{r_1+r_2}(x), \mathrm{Im}\sigma_{r_1+r_2}(x)). \end{aligned}$$

Remark 6.22. • *The map Φ above is injective (because each σ_i is injective), and a group homomorphism (of the additive groups $(K, +)$ and $(\mathbb{R}^n, +)$). Moreover, both K and $\mathbb{R}^n$ have a $\mathbb{Q}$-vector space structure, and Φ preserves it.*

- Φ *provides us with a way to see number fields inside* n*-dimensional* $\mathbb{R}$*-vector spaces. We are interested in subgroups of* K *that give rise to lattices in* $\mathbb{R}^n$.

Proposition 6.23. *Let* $M \subset K$ *be a free* $\mathbb{Z}$*-module of rank* n*, say with basis* $\{x_1, \dots, x_n\}$*. Then*

- $\Phi(M)$ *is a lattice in* $\mathbb{R}^n$.
- *Let* $A = (\sigma_i(x_j))_{1 \le i,j \le n}$*. Then* $v(\Phi(M)) = 2^{-r_2} |\det A|$.

Remark 6.24. *With the notations above, the discriminant of the tuple* $(x_1, \dots, x_n) \in K^n$ *is defined as the square of* $\det A$*. Moreover (see Proposition 2.8-(e)) the discriminant of* $(x_1, \dots, x_n)$ *is nonzero.*

Proof. $\Phi : K \to \mathbb{R}^n$ is an injective morphism from $(K, +)$ to $(\mathbb{R}^n, +)$, hence it carries free $\mathbb{Z}$-modules into free $\mathbb{Z}$-modules, and transforms $\mathbb{Z}$-bases into $\mathbb{Z}$-bases. Therefore $\Phi(M)$ is a $\mathbb{Z}$-module of rank n in $\mathbb{R}^n$ with basis $\Phi(x_1), \dots, \Phi(x_n)$. To prove that it is a lattice, we need to see that the n vectors $\Phi(x_1), \dots, \Phi(x_n)$ are linearly independent over $\mathbb{R}$. The coordinates of $\Phi(x_i)$ are

$$(\sigma_1(x_i), \dots, \sigma_{r_1+1}(x_i), \mathrm{Re}\sigma_{r_1+1}(x_i), \mathrm{Im}\sigma_{r_1+1}(x_i) \dots, \mathrm{Re}\sigma_{r_1+r_2}(x_i), \mathrm{Im}\sigma_{r_1+r_2}(x))$$

Let B be the matrix with i-th row as above, for all $i \in \{1, \dots, n\}$. We will prove that $\det B \neq 0$, thus showing that the vectors $\Phi(x_1), \dots, \Phi(x_n)$ are linearly independent over $\mathbb{R}$.
For $j = 1, \dots, r_2$, call $\mathbf{z}_j$ the column vector with entries $(\sigma_{r_1+j}(x_i))_{i=1,\dots,n}$, and denote the column vector whose entries are the complex conjugates of the entries of $\mathbf{z}_j$ by $\overline{\mathbf{z}}_j$. Then we have that

$$B = \left(\vdots \,\middle|\, \mathrm{Re}\mathbf{z}_j \,\middle|\, \mathrm{Im}\mathbf{z}_j \,\middle|\, \vdots \right) = \left(\vdots \,\middle|\, \tfrac{\mathbf{z}_j + \overline{\mathbf{z}}_j}{2} \,\middle|\, \tfrac{\mathbf{z}_j - \overline{\mathbf{z}}_j}{2i} \,\middle|\, \vdots \right)$$

Hence

$$\begin{aligned} \det B = \det \left(\vdots \,\middle|\, \tfrac{\mathbf{z}_j}{2} \,\middle|\, \tfrac{\mathbf{z}_j}{2i} \,\middle|\, \vdots \right) + \det \left(\vdots \,\middle|\, \tfrac{\mathbf{z}_j}{2} \,\middle|\, \tfrac{-\overline{\mathbf{z}}_j}{2i} \,\middle|\, \vdots \right) \\ + \det \left(\vdots \,\middle|\, \tfrac{\overline{\mathbf{z}}_j}{2} \,\middle|\, \tfrac{\mathbf{z}_j}{2i} \,\middle|\, \vdots \right) + \det \left(\vdots \,\middle|\, \tfrac{\overline{\mathbf{z}}_j}{2} \,\middle|\, \tfrac{-\overline{\mathbf{z}}_j}{2i} \,\middle|\, \vdots \right) \end{aligned}$$

$$= \frac{-1}{4i} \det \left(\vdots \,\middle|\, \mathbf{z}_j \,\middle|\, \overline{\mathbf{z}}_j \,\middle|\, \vdots \right) + \frac{1}{4i} \det \left(\vdots \,\middle|\, \overline{\mathbf{z}}_j \,\middle|\, \mathbf{z}_j \,\middle|\, \vdots \right) = \frac{-1}{2i} \det \left(\vdots \,\middle|\, \mathbf{z}_j \,\middle|\, \overline{\mathbf{z}}_j \,\middle|\, \vdots \right).$$

Repeating this process for all $i = 1, \dots, r_2$, we get

$$\det B = \left(\frac{-1}{2i} \right)^{r_2} \det A',$$

where A' is the matrix with i-th row given by

$$(\sigma_1(x_i), \dots, \sigma_{r_1+1}(x_i), \sigma_{r_1+1}(x_i), \alpha \circ \sigma_{r_1+1}(x_i) \dots, \sigma_{r_1+r_2}(x_i), \alpha \circ \sigma_{r_1+r_2}(x_i)).$$

Since the columns of A and A' coincide up to a permutation, we have $|\det A'| = |\det A| \neq 0$. This proves that $\Phi(M)$ is a lattice. Moreover $v(\Phi(M)) = |\det B| = 2^{-r_2} |\det A|$. □

Definition 6.25. *Let* K *be a number field.*

Let $\mathfrak{a} \subset \mathbb{Z}_K$ be a nonzero integral ideal. We define the norm *of $\mathfrak{a}$ as $N(\mathfrak{a}) = [\mathbb{Z}_K : \mathfrak{a}]$.*

Let $I \subset K$ be a fractional ideal. We define the norm *of I as $N(I) = N(xI)/|N_{K/\mathbb{Q}}(x)|$, where $x \in \mathbb{Z}_K$ is some element different from zero such that xI is an integral ideal.*

Remark 6.26. *Let K be a number field. Then $N : \mathcal{I}(\mathbb{Z}_K) \to \mathbb{Q}^\times$ is a group homomorphism (See Sheet 9).*

Corollary 6.27. *Let $K/\mathbb{Q}$ be a number field of degre $n = r_1 + 2r_2$ and $\mathfrak{a}$ an integral ideal of $\mathbb{Z}_K$. Then we have that $\Phi(\mathbb{Z}_K)$, $\Phi(\mathfrak{a})$ are lattices of $\mathbb{R}^n$ and*

$$v(\Phi(\mathbb{Z}_K)) = 2^{-r_2}\sqrt{|\mathrm{disc}(\mathbb{Z}_K)|}, \quad v(\Phi(\mathfrak{a})) = 2^{-r_2}\sqrt{|\mathrm{disc}(\mathbb{Z}_K)|}N(\mathfrak{a}).$$

Proof. Since $\mathbb{Z}_K$ is an order of K (see Corollary 3.17-(a)), it is a free $\mathbb{Z}$-modules of rank n. By Corollary 3.17-(c), $\mathfrak{a}$ is also a free $\mathbb{Z}$-module of rank n. The formula for the volume of $\Phi(\mathbb{Z}_K)$ follows directly from the definition of $\mathrm{disc}(\mathbb{Z}_K)$; the formula for the volume of $\Phi(\mathfrak{a})$ follows from Proposition 3.19. □

6.4 Finiteness of the class number

Let K be a number field of degree n. As in the previous section, we denote by r_1 the number of embeddings of $K \hookrightarrow \mathbb{R}$ and $r_2 = (n - r_1)/2$.

Proposition 6.28. *Let $\mathfrak{a} \subset \mathbb{Z}_K$ be a nonzero integral ideal. There exists $a \in \mathfrak{a}$ different from zero such that*

$$|N_{K/\mathbb{Q}}(a)| \leq \left(\frac{2}{\pi}\right)^{r_2} \sqrt{|\mathrm{disc}(\mathbb{Z}_K)|}N(\mathfrak{a}).$$

Proof. We will apply Corollary 6.20 in $\mathbb{R}^n$. First we define the measurable set S as follows: Let $A_1, \dots, A_{r_1}$ and $B_1, \dots, B_{r_2}$ be some positive real numbers. Consider the set $S \subset \mathbb{R}^n$ defined by

$$S = \{(x_1, \dots, x_{r_1}, y_1, {y'}_1, \dots, y_{r_2}, {y'}_{r_2}) : \\ |x_i| \leq A_i \text{ for all } i = 1, \dots, r_1, \sqrt{y_j^2 + {y'_j}^2} \leq B_j \text{ for all } j = 1, \dots, r_2\}. \quad (6.8)$$

The set S is centrally symmetric (clear) and convex: if we have $(x_1, \dots, x_{r_1}, y_1, {y'}_1, \dots, y_{r_2}, {y'}_{r_2})$ and $(\tilde{x}_1, \dots, \tilde{x}_{r_1}, \tilde{y}_1, \tilde{y}'_1, \dots, \tilde{y}_{r_2}, \tilde{y}'_{r_2})$ in S, then for any $\lambda \in (0, 1)$,

$$|\lambda x_i + (1 - \lambda)\tilde{x}_i| \leq |\lambda| \cdot |x_i| + |1 - \lambda| \cdot |\tilde{x}_i| \leq A_i,$$

and

$$\sqrt{(\lambda y_j + (1 - \lambda)\tilde{y}_j)^2 + (\lambda y'_j + (1 - \lambda)\tilde{y}'_j)^2} \leq \\ \sqrt{(\lambda y_j)^2 + (\lambda y'_j)^2} + \sqrt{((1 - \lambda)\tilde{y}_j)^2 + ((1 - \lambda)\tilde{y}'_j)^2} \leq \\ |\lambda| \cdot \sqrt{y_j^2 + {y'_j}^2} + |1 - \lambda| \cdot \sqrt{\tilde{y}_j^2 + (\tilde{y}'_j)^2} \leq B_j.$$

Its Lebesgue measure can be computed as

$$\mu(S) = \prod_{i=1}^{r_1}(2A_i) \cdot \prod_{j=1}^{r_2}(\pi B_j^2) = 2^{r_1}\pi^{r_2}\prod_{i=1}^{r_1}A_i \prod_{j=1}^{r_2}B_j^2.$$

On the other hand, we can embed $K \hookrightarrow \mathbb{R}^n$ via the map Φ from Definition 6.21. $H = \Phi(\mathfrak{a})$ is a lattice of volume $v(H) = 2^{-r_2}\sqrt{|\mathrm{disc}(\mathbb{Z}_K)|}N(\mathfrak{a})$ (Corollary 6.27).
Let $\varepsilon > 0$. Choose $A_1, \dots, A_{r_1}, B_1, \dots, B_{r_2}$ (depending on ε) positive integers such that

$$\prod_{i=1}^{r_1}A_i \prod_{j=1}^{r_2}B_j^2 = \left(\frac{2}{\pi}\right)^{r_2}\sqrt{|\mathrm{disc}(\mathbb{Z}_K)|}N(\mathfrak{a}) + \varepsilon,$$

and call S_ε the set defined by (6.8).
Then it holds that $2^n v(H) < \mu(S_\varepsilon)$, so we can apply Corollary 6.20 and conclude that there exists some nonzero $v_\varepsilon \in S_\varepsilon \cap H$. Let $a_\varepsilon \in \mathfrak{a}$ such that $\Phi(a_\varepsilon) = v_\varepsilon$. The fact that $\Phi(a_\varepsilon) \in S_\varepsilon$ means that, for all $i = 1, \dots, r_1$, $|\sigma_i(a_\varepsilon)| \leq A_i$, and for all $j = 1, \dots, r_2$, $\sqrt{(\mathrm{Re}\sigma_{r_1+j}(a_\varepsilon))^2 + (\mathrm{Im}\sigma_{r_1+j}(a_\varepsilon))^2} \leq B_j$. Therefore

$$|N_{K/\mathbb{Q}}(a_\varepsilon)| = \prod_{i=1}^{r_1}|\sigma_i(a_\varepsilon)| \cdot \prod_{j=1}^{r_2}|\sigma_j(a_\varepsilon)|^2 \leq \prod_{i=1}^{r_1}A_i \prod_{j=1}^{r_2}B_j^2 = \left(\frac{2}{\pi}\right)^{r_2}\sqrt{|\mathrm{disc}(\mathbb{Z}_K)|}N(\mathfrak{a}) + \varepsilon$$

Let $C = \left(\frac{2}{\pi}\right)^{r_2}\sqrt{|\mathrm{disc}(\mathbb{Z}_K)|}N(\mathfrak{a}) \in \mathbb{R}$, $\lfloor C \rfloor$ the integer part of C, and choose ε such that $C + \varepsilon < \lfloor C \rfloor + 1$. Then the greatest integer A satisfying that $A \leq C + \varepsilon$ is $\lfloor C \rfloor$. But $|N_{K/\mathbb{Q}}(a_\varepsilon)|$ is an integer which is smaller than or equal to $C + \varepsilon$. Thus $|N_{K/\mathbb{Q}}(a_\varepsilon)| \leq \lfloor C \rfloor \leq C$.

□

Proposition 6.29. *Let $\mathfrak{a} \subset \mathbb{Z}_K$ a nonzero integral ideal. There exists $a \in \mathfrak{a}$ different from zero such that*

$$|N_{K/\mathbb{Q}}(a)| \leq \left(\frac{4}{\pi}\right)^{r_2}\frac{n!}{n^n}\sqrt{|\mathrm{disc}(\mathbb{Z}_K)|}N(\mathfrak{a}).$$

Proof. See Sheet 10. □

Proposition 6.28 (or Proposition 6.29) will be a key ingredient in the proof of the following result.

Theorem 6.30 (Dirichlet)**.** *Let K be a number field. The class group $\mathrm{CL}(K) = \mathcal{I}(\mathbb{Z}_K)/\mathcal{P}(\mathbb{Z}_K)$ is finite.*

Before proceeding to the proof, let us establish a technical lemma.

Lemma 6.31. *Let K be a number field, and $C \in \mathrm{CL}(K)$ be a class of ideals. Then there exists a nonzero integral ideal $\mathfrak{a}$ of $\mathbb{Z}_K$ which belongs to C and satisfies*

$$N(\mathfrak{a}) \leq \left(\frac{2}{\pi}\right)^{r_2}\sqrt{|\mathrm{disc}(\mathbb{Z}_K)|}.$$

Proof. Let I be a fractional ideal in C. Then $I^{-1} = \{a \in \mathbb{Z}_K : aI \subset \mathbb{Z}_K\}$ is also a fractional ideal. Therefore there exists a nonzero $x \in K$ such that $\mathfrak{b} = xI^{-1}$ is a nonzero integral ideal. We can apply Proposition 6.28 to the ideal $\mathfrak{b}$; there exists $b \in \mathfrak{b}$ nonzero such that

$$|N_{K/\mathbb{Q}}(b)| \leq \left(\frac{2}{\pi}\right)^{r_2} \sqrt{|\mathrm{disc}(\mathbb{Z}_K)|} N(\mathfrak{b}) = \left(\frac{2}{\pi}\right)^{r_2} \sqrt{|\mathrm{disc}(\mathbb{Z}_K)|} |N_{K/\mathbb{Q}}(x)| N(I)^{-1}.$$

The ideal $\mathfrak{a} = \frac{b}{x} I$ belongs to the class C, is contained in $\mathbb{Z}_K$ and furthermore

$$N(\mathfrak{a}) = \frac{|N_{K/\mathbb{Q}}(b)|}{|N_{K/\mathbb{Q}}(x)|} N(I) \leq \left(\frac{2}{\pi}\right)^{r_2} \sqrt{|\mathrm{disc}(\mathbb{Z}_K)|}.$$

□

Proof of Theorem 6.30. Since every class $C \in \mathrm{CL}(K)$ contains a nonzero integral ideal of norm smaller than $\left(\frac{2}{\pi}\right)^{r_2} \sqrt{|\mathrm{disc}(\mathbb{Z}_K)|}$ (because of Lemma 6.31), it suffices to prove that, for any $M \in \mathbb{N}$, there are only finitely many integral ideals of norm smaller than M. First of all, note that it suffices to see that there are only finitely many prime integral ideals of norm smaller than M; indeed if $\mathfrak{a} = \prod_{i=1}^{r} \mathfrak{p}_i^{e_i}$ is a factorisation of $\mathfrak{a}$ into a product of prime ideals, then $N(\mathfrak{a}) = \prod_{i=1}^{r} N(\mathfrak{p}_i)^{e_i}$, so if $N(\mathfrak{a})$ is smaller than M, the only prime ideals that can occur in the factorisation of $\mathfrak{a}$ are those with norm smaller than M, and the exponents e_i that can occur must also be smaller than M.
Assume now that $\mathfrak{p}$ is a prime integral ideal of norm smaller than M, say m. Then $\overline{1} \in \mathbb{Z}_K/\mathfrak{p}$ satisfies that $m \cdot \overline{1} = 0 \in \mathbb{Z}_K/\mathfrak{p}$, thus $m \in \mathfrak{p}$. But we know that that there are only a finite number of maximal ideals of $\mathbb{Z}_K$ containing a given ideal I (Corollary 5.5). In particular, for $I = (m)$, we get that there are only finitely many prime ideals $\mathfrak{p}$ of $\mathbb{Z}_K$ of norm m. □

Remark 6.32.
- *Let K be a number field. Then $\mathrm{CL}(K)$ is generated by the classes of the prime ideals $\mathfrak{p} \in \mathcal{I}(\mathbb{Z}_K)$ such that $N(\mathfrak{p}) \leq \left(\frac{2}{\pi}\right)^{r_2} \sqrt{|\mathrm{disc}(\mathbb{Z}_K)|}$. This allows one to compute explicitly the class group of a given number field, provided one knows how to compute the prime ideals of given norm.*
- *The same proof, but using the better bound of Proposition 6.29, shows that $\mathrm{CL}(K)$ is generated by the classes of the prime ideals $\mathfrak{p} \in \mathcal{I}(\mathbb{Z}_K)$ such that $N(\mathfrak{p}) \leq \left(\frac{4}{\pi}\right)^{r_2} \frac{n!}{n^n} \sqrt{|\mathrm{disc}(\mathbb{Z}_K)|}$.*

Remark 6.33. *Let E/K be an extension of number fields, and let $\mathfrak{p} \subset \mathbb{Z}_K$ be a nonzero prime ideal. The ideal $\mathfrak{p}\mathbb{Z}_E$ generated by the elements of $\mathfrak{p}$ inside $\mathbb{Z}_E$ need not be prime anymore, but, since $\mathbb{Z}_E$ is a Dedekind domain, it will factor in a unique way as a product of primes*

$$\mathfrak{p}\mathbb{Z}_E = \prod_{i=1}^{r} \mathfrak{P}_i^{e_i}.$$

The ideals $\mathfrak{P}_i$ are the prime ideals of $\mathbb{Z}_E$ containing $\mathfrak{p}\mathbb{Z}_K$ (Corollary 5.5). We will say that $\mathfrak{P}_1, \ldots, \mathfrak{P}_r$ are the prime ideals of $\mathbb{Z}_E$ lying above $\mathfrak{p}$.

Remark 6.34. *Let K be a number field, $p \in \mathbb{Z}$ a nonzero prime. Then the prime ideals of $\mathbb{Z}_K$ above (p) are those whose norm is a power of p.*

Proposition 6.35. *Let K be a number field, and assume that there exists $\alpha \in \mathbb{Z}_K$ such that $\mathbb{Z}[\alpha] = \mathbb{Z}_K$. Call $f(X) \in \mathbb{Z}[X]$ be the minimal polynomial of α over $\mathbb{Q}$. Let p be a prime, let $\overline{f}(X) \in \mathbb{F}_p[X]$ be the reduction of $f(X)$ mod p, and let*

$$\overline{f}(X) = \prod_{i=1}^{r} \overline{q}_i(X)$$

be a factorisation of $\overline{f}(X)$ into monic irreducible polynomials in $\mathbb{F}_p[X]$. For each $i = 1, \ldots, r$, choose $q_i(X) \in \mathbb{Z}[X]$ reducing to $\overline{q}_i(x)$ mod p. Then the prime ideals of $\mathbb{Z}_K$ of norm equal to a power of p are given by

$$\mathfrak{p}_i := (p, q_i(\alpha))_{\mathbb{Z}_K}, \qquad i = 1, \ldots, r.$$

Example 6.36. • *Let $K = \mathbb{Q}(\sqrt{7})$. Then $\mathbb{Z}_K = \mathbb{Z}[\sqrt{7}]$, and $\operatorname{disc}(\mathbb{Z}_K) = 4 \cdot 7$. Since $K \subset \mathbb{R}$, $r_2 = 0$ and $n = r_1 = 2$. The quantity $C = \left(\frac{2}{\pi}\right)^{r_2} \sqrt{|\operatorname{disc}(\mathbb{Z}_K)|}$ satisfies $C < 6$. Therefore $\mathrm{CL}(K)$ is generated by the classes of the nonzero prime ideals of $\mathbb{Z}_K$ of norm less than or equal to 6. In particular, $\mathrm{CL}(K)$ is generated by the primes above 2, 3 and 5. Below we apply Corollary 6.35 to $\mathbb{Z}_K = \mathbb{Z}[\sqrt{7}]$ with $\alpha = \sqrt{7}$. The minimal polynomial of α over $\mathbb{Q}$ is $f(x) = x^2 - 7$.*

  – ***Prime ideals of norm a power of** 2: $f(x) \equiv x^2 - 7 \equiv x^2 + 1 = (x+1)^2 \pmod 2$, hence the only prime ideal of $\mathbb{Z}_K$ above (2) is $\mathfrak{p} = (2, 1 + \sqrt{7}) = (3 + \sqrt{7})$.*
  – ***Prime ideals of norm a power of** 3: $f(x) \equiv x^2 - 1 \equiv (x+1)(x-1) \pmod 3$, hence the only prime ideals of $\mathbb{Z}_K$ above (3) are $\mathfrak{p}_1 = (3, 1 + \sqrt{7}) = (5 + 2\sqrt{7})$ and $\mathfrak{p}_2 = (3, \sqrt{7} - 1) = (5 - 2\sqrt{7})$.*
  – ***Prime ideals of norm a power of** 5: $f(x) \equiv x^2 - 2 \pmod 5$, which is irreducible. Hence the only prime ideal of $\mathbb{Z}_K$ above (5) is $\mathfrak{p} = (5, (\sqrt{7})^2 - 2) = (5, 5) = (5)$.*

  Therefore $\mathrm{CL}(K)$ is generated by the classes of principal ideals. Thus $\mathrm{CL}(K) = \{1\}$.

Proof of Proposition 6.35. Let $i \in \{1, \ldots, r\}$, and fix a root $\overline{\beta}_i \in \overline{\mathbb{F}}_p$ of $\overline{q}_i(X)$. Consider the ring homomorphism

$$\begin{aligned} \Phi_i : \mathbb{Z}[X] &\to \mathbb{F}_p[\overline{\beta}_i] \\ X &\mapsto \overline{\beta}_i \\ a \in \mathbb{Z} &\mapsto \overline{a} \in \mathbb{F}_p = (\mathbb{Z}/p\mathbb{Z}). \end{aligned}$$

Since $\Phi_i(f(X)) = 0$, we obtain the following commutative diagram for some morphism ϕ_i:

$$\begin{array}{ccc} \mathbb{Z}[X] & \xrightarrow{\Phi_i} & \mathbb{F}_p[\overline{\beta}_i] \\ \downarrow & \nearrow_{\phi_i} & \\ \mathbb{Z}[\alpha] & & \end{array}$$

Let $\mathfrak{p}_i = \ker \phi_i$. Since $\mathbb{F}_p[\overline{\beta}_i] \subset \overline{\mathbb{F}}_p$ is an integral domain, we obtain that $\mathbb{Z}[\alpha]/\mathfrak{p}_i \hookrightarrow \mathbb{F}_p[\overline{\beta}_i]$ is an integral domain, and $\mathfrak{p}_i$ is thus a prime ideal. We will now show that $\mathfrak{p}_i = (p, q_i(\alpha))_{\mathbb{Z}[\alpha]}$.

- $\supseteq$ Clearly $\phi_i(a) = 0$ for all $a \in p\mathbb{Z}$ and $\phi_i(q_i(\alpha)) = \overline{q}_i(\overline{\beta}_i) = 0$, hence we have the inclusion.
- $\subseteq$ Let $b \in \mathfrak{p}$, say $b = g(\alpha)$ for some $g(X) \in \mathbb{Z}[X]$. Then $0 = \phi_i(b) = \phi_i(g(\alpha)) = \overline{g}(\phi_i(\alpha)) = \overline{g}(\overline{\beta}_i)$, where $\overline{g}(X) \in \mathbb{F}_p[X]$ is the reduction of $g(X)$ modulo p. Thus $\overline{g}(X)$ is divisible by the minimal polynomial of $\overline{\beta}_i$ over $\mathbb{F}_p$, that is $\overline{q}_i(X)$, say $\overline{g}(X) = \overline{q}_i(X)\overline{h}(X)$. Taking $h(X) \in \mathbb{Z}[X]$ reducing to $\overline{h}(X)$, we have that $g(X) - q_i(X)h(X) \in \mathbb{Z}[X]$ has coefficients in $p\mathbb{Z}$, and therefore $g(\alpha) \in (q_i(\alpha), p)_{\mathbb{Z}[\alpha]}$. This proves the other inclusion.

This proves that the r primes $\mathfrak{p}_i$ are primes of $\mathbb{Z}_K$ above $p\mathbb{Z}$. Reciprocally, let $\mathfrak{p}$ be a prime over $p\mathbb{Z}$, and consider the projection $\phi : \mathbb{Z}[\alpha] \to \mathbb{Z}[\alpha]/\mathfrak{p}$. Since $\mathfrak{p}$ is a proper ideal which contains p, it follows that the composition ψ of the natural inclusion $\mathbb{Z} \hookrightarrow \mathbb{Z}[\alpha]$ with ϕ,

$$\mathbb{Z} \longrightarrow \mathbb{Z}[\alpha] \xrightarrow{\phi} \mathbb{Z}[\alpha]/\mathfrak{p} \ , \qquad \mathbb{Z} \xrightarrow{\psi} \mathbb{Z}[\alpha]/\mathfrak{p}$$

has kernel $\ker(\psi) = p\mathbb{Z}$.
Thus we know that $\mathbb{Z}[\alpha]/\mathfrak{p}$ is a field (all nonzero prime ideals in $\mathbb{Z}_K$ are maximal), and we have a natural inclusion $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z} \hookrightarrow \mathbb{Z}[\alpha]/\mathfrak{p}$. The element $\overline{\alpha} := \phi(\alpha)$ is algebraic over $\mathbb{F}_p$ (it satisfies $\overline{f}(\overline{\alpha}) = \phi(f(\alpha)) = 0$). Thus we have the inclusions $\mathbb{F}_p \subset \mathbb{F}_p[\overline{\alpha}] \subset \overline{\mathbb{F}}_p$, together with an isomorphism $\mathbb{F}_p[\overline{\alpha}] \simeq \mathbb{Z}[\alpha]/\mathfrak{p}$ (obtained by extending the inclusion $\mathbb{F}_p \hookrightarrow \mathbb{Z}[\alpha]/\mathfrak{p}$ to $\mathbb{F}_p[X] \hookrightarrow \mathbb{Z}[\alpha]/\mathfrak{p} \subset \overline{\mathbb{F}}_p$ by sending X to $\overline{\alpha}$, and observing that the kernel is the minimal polynomial of α over $\mathbb{F}_p$).
Moreover, from the equation $\overline{f}(\overline{\alpha}) = 0$ we obtain that $\overline{\alpha}$ is a root of some of the $\overline{q}_i(X)$. Since $\overline{q}_i(X) \in \mathbb{F}_p[X]$ is monic and irreducible, it is the minimal polynomial of $\overline{\alpha}$ over $\mathbb{F}_p$. This implies that we have isomorphisms

$$\mathbb{F}_p[\overline{\beta}_i] \simeq \mathbb{F}_p[X]/(\overline{q}_i(X)) \simeq \mathbb{F}_p[\overline{\alpha}].$$

Hence, the map ϕ is the composition of one of the projections ϕ_i considered above with an isomorphism $\tau : \mathbb{Z}[\alpha]/\mathfrak{p}_i \simeq \mathbb{Z}[\alpha]/\mathfrak{p}$. Therefore $\mathfrak{p} = \ker(\tau \circ \phi_i) = \ker \phi_i = \mathfrak{p}_i$. □

6.5 Dirichlet Unit Theorem

The aim of this section is to prove the following result:

Theorem 6.37 (Dirichlet)**.** *Let K be a number field of degree $n = r_1 + 2r_2$. Then there is a group isomorphism*

$$\Psi : \mathbb{Z}_K^\times \simeq \mu_K \times \mathbb{Z}^{r_1+r_2-1},$$

between the (multiplicative) group of units of $\mathbb{Z}_K$ and the direct product of the finite (multiplicative) subgroup μ_K of $\mathbb{Z}_K^\times$, consisting of all roots of unity contained in K, and the (additive) group $\mathbb{Z}^{r_1+r_2-1}$.

Remark 6.38. *Note that, in both $\mathbb{Z}_K^\times$ and μ_K the group structure is written multiplicatively, whereas in $\mathbb{Z}^{r_1+r_2-1}$ the group structure is written additively.*

Remark 6.39. *More precisely, we will prove that there exist $\xi_1, \dots, \xi_{r_1+r_2-1} \in \mathbb{Z}_K^\times$ such that every element $u \in \mathbb{Z}_K^\times$ can be written in a unique way as*

$$u = \mu \cdot \xi_1^{n_1} \cdot \dots \cdot \xi_{r_1+r_2-1}^{n_{r_1+r_2-1}}$$

for some root of unity $\mu \in K$ and some tuple $(n_1, \dots, n_{r_1+r_2-1}) \in \mathbb{Z}^{r_1+r_2-1}$.

The remark above motivates the following definition.

Definition 6.40. *Let K be a number field of degree $n = r_1 + 2r_2$.*
We will say that a tuple $(\xi_1, \dots, \xi_{r_1+r_2-1}) \in (\mathbb{Z}_K^\times)^{r_1+r_2-1}$ is a fundamental system of units *if, for all $u \in \mathbb{Z}_K^\times$ there exist a root of unity $\mu \in \mathbb{Z}_K$ and $n_1, \dots, n_{r_1+r_2-1} \in \mathbb{Z}$ such that*

$$u = \mu \cdot \xi_1^{n_1} \cdot \dots \cdot \xi_{r_1+r_2-1}^{n_{r_1+r_2-1}}.$$

The proof of this theorem will be given gradually through a series of steps (Lemmas 6.42 6.43, 6.46, 6.47, 6.48 and Corollaries 6.44, 6.45).
Consider the following map

$$K \longrightarrow \mathbb{R}^{r_1} \times \mathbb{C}^{r_2} \longrightarrow \mathbb{R}^{r_1+r_2}$$

$$a \longmapsto \Phi_0(a) = (\sigma_1(a), \dots, \sigma_{r_1+r_2}(a)) \longmapsto (|\sigma_1(a)|, \dots, |\sigma_{r_1+r_2}(a)|),$$

where Φ_0 is the map considered before Definition 6.21 and, in the second map, $|\cdot| : \mathbb{R} \to \mathbb{R}$ is the usual absolute value, and $|\cdot| : \mathbb{C} \to \mathbb{R}$ is the norm given by $|x + iy| = \sqrt{x^2 + y^2}$ for all $x, y \in \mathbb{R}$.

Definition 6.41. *Let K be a number field of degree $n = r_1+2r_2$. We define the* logarithmic embedding *as the group morphism*

$$\begin{aligned} \Phi_{\log} : K^\times &\to \mathbb{R}^{r_1+r_2} \\ a &\mapsto (\log|\sigma_1(a)|, \dots, \log|\sigma_{r_1+r_2}(a)|). \end{aligned}$$

Recall that, if K is a number field and $a \in \mathbb{Z}_K$, then $a \in \mathbb{Z}_K^\times$ if and only if $N_{K/\mathbb{Q}}(a) = \pm 1$ (cf. Lemma 3.10).

Lemma 6.42. *Let K be a number field of degree $n = r_1 + 2r_2$ and $B \subset \mathbb{R}^{r_1+r_2}$ a compact set. Consider the set*

$$B' := \{a \in \mathbb{Z}_K^\times : \Phi_{\log}(a) \in B\}.$$

Then there exists an $M > 1$ such that, for all $a \in B'$ and all $i = 1, \dots, r_1 + r_2$,

$$\frac{1}{M} < |\sigma_i(a)| < M.$$

Proof. Since B is bounded, there exists an N such that, for all $y = (y_1, \dots, y_{r_1+r_2}) \in B$, $|y_i| < N$ for all $i = 1, \dots, r_1 + r_2$. If $a \in B'$, then $\Phi_{\log}(a) \in B$, and therefore $|\log|\sigma_i(a)|| \leq N$ for all $i = 1, \dots, r_1 + r_2$. Hence

$$e^{-N} < |\sigma_i(a)| < e^N \text{ for all } i = 1, \dots, r_1 + r_2.$$

Take $M = e^N$. □

Lemma 6.43. *Let K be a number field of degree $n = r_1 + 2r_2$ and B, B' as in Lemma 6.42. Then B' is finite.*

Proof. By Lemma 6.42, there exists $M > 1$ such that, for all $i = 1, \dots, r_1 + r_2$, $|\sigma_i(a)| < M$ for all $a \in B'$. Since $\sigma_{i+r_1+r_2}(x)$ is the complex conjugate of $\sigma_{i+r_1}(x)$ for all $i = 1, \dots, r_2$, the inequality $|\sigma_i(a)| < M$ actually holds for all $i = 1, \dots, r_1 + 2r_2 = n$.
For any $x \in K$, the minimal polynomial of x over $\mathbb{Q}$ is given by

$$f(X) = \prod_{i=1}^{n} (X - \sigma_i(x))$$

(cf. Proposition 2.4). Therefore the coefficients of $f(X)$ are given by the *elementary symmetric polynomials* $S_j(X_1, \dots, X_n) \in \mathbb{Z}[X_1, \dots, X_n]$, $j = 1, \dots, n$, evaluated at $\sigma_1(x), \dots, \sigma_n(x)$. These polynomials are homogeneous polynomials of degree j, and they do not depend on $x \in K$. Therefore, for all $a \in B'$, we have that the coefficients of the minimal polynomial of a over $\mathbb{Q}$ are of the form $S_j(\sigma_1(a), \dots, \sigma_n(a))$, and therefore can be bounded in terms of n and M. But these coefficients must belong to $\mathbb{Z}$. Hence there are only a finite number of possible minimal polynomials over $\mathbb{Q}$ for the elements of B', thus B' is finite. □

Corollary 6.44. *$\Phi_{\log}(\mathbb{Z}_K^\times)$ is a discrete subgroup, hence a free $\mathbb{Z}$-module of rank less than or equal to $r_1 + r_2$.*

Proof. This follows from Proposition 6.16. □

Corollary 6.45. *The kernel of $\Phi_{\log}|_{\mathbb{Z}_K^\times}$ is a finite group, consisting of the roots of unity contained in $\mathbb{Z}_K$.*

Proof. Take any compact B of $\mathbb{R}^{r_1+r_2}$ containing 0. Then $\ker(\Phi_{\log}|_{\mathbb{Z}_K^\times}) \subset B'$, hence it is finite. If $a \in \mathbb{Z}_K^\times$ belongs to a finite subgroup, it must have finite order, so there exists $s \in \mathbb{N}$ with $a^s = 1$. In other words, a is a root of unity.
Reciprocally, if $a \in \mathbb{Z}_K$ is a root of unity, then it satisfies that, for some $s \in \mathbb{N}$, $a^s = 1$. Therefore, for all $i = 1, \dots, r_1 + r_2$, $\sigma_i(a)^s = 1$, thus $\log|\sigma_i(a)| = \log 1 = 0$, and $\Phi_{\log}(a) = 0$. □

Lemma 6.46. *Let K be a number field. Then*

$$\mathbb{Z}_K^\times \simeq \mu_K \times \Phi_{\log}(\mathbb{Z}_K^\times)$$

Proof. We have the exact sequence of groups

$$1 \to \ker(\Phi_{\log}|_{\mathbb{Z}_K^\times}) \to \mathbb{Z}_K^\times \to \Phi_{\log}(\mathbb{Z}_K^\times) \to 0.$$

By Corollary 6.45 we know that $\ker(\Phi_{\log}|_{\mathbb{Z}_K^\times}) = \mu_K$, and by Corollary 6.44 we know that $\Phi_{\log}(\mathbb{Z}_K^\times)$ is a free $\mathbb{Z}$-module, hence the exact sequence splits. □

Lemma 6.47. *Let K be a number field of degree $n = r_1 + 2r_2$. The rank of $\Phi_{\log}(\mathbb{Z}_K^\times)$ is less than or equal to $r_1 + r_2 - 1$.*

Proof. Let $a \in \mathbb{Z}_K^\times$. Then the norm of a is ± 1, thus

$$\pm 1 = N_{K/\mathbb{Q}}(a) = \prod_{i=1}^{r_1} \sigma_i(a) \cdot \prod_{i=r_1+1}^{r_1+r_2} \sigma_i(a)(\alpha \circ \sigma_i)(a)$$

where $\alpha : \mathbb{C} \to \mathbb{C}$ denotes the complex conjugation. Applying $\log|\cdot|$ to both sides, we get

$$0 = \sum_{i=1}^{r_1} \log|\sigma_i(a)| + 2\sum_{i=r_1+1}^{r_1+r_2} \log|\sigma_i(a)|.$$

Therefore $\Phi_{\log}(a)$ belongs to the subspace

$$W := \{(y_1, \dots, y_{r_1+r_2}) \in \mathbb{R}^{r_1+r_2} : \sum_{i=1}^{r_1} y_i + 2\sum_{i=r_1+1}^{r_1+r_2} y_i = 0\}.$$

Therefore $\Phi_{\log}(\mathbb{Z}_K^\times)$ must have rank smaller than or equal to $\dim_{\mathbb{R}} W = r_1 + r_2 - 1$. □

Up to this point, we have proven that $\mathbb{Z}_K^\times$ is not very big, that is, it is finitely generated, and we even have a bound for the number of generators of the free part. That was the easy part. Note that, up to now, we have not used Minkowsky's Theorem 6.18 or its corollary. The hard part is to show that, indeed, the torsion-free part of the group $\mathbb{Z}_K^\times$ has $r_1 + r_2 - 1$ free generators; and for this we will need Corollary 6.20.

Lemma 6.48. *Let K be a number field of degree $n = r_1 + 2r_2$. The rank of $\Phi_{\log}(\mathbb{Z}_K^\times)$ is equal to $r_1 + r_2 - 1$.*

Proof. We already know one inequality by Lemma 6.47. To show the other inequality, we will prove that $\Phi_{\log}(\mathbb{Z}_K^\times)$ cannot be contained in any proper vector subspace of $W := \{(y_1, \dots, y_{r_1+r_2}) \in \mathbb{R}^{r_1+r_2} : \sum_{i=1}^{r_1} y + 2\sum_{i=r_1+1}^{r_1+r_2} y_i = 0\}$.
Assume then that there exists $W_0 \subset \mathbb{R}^{r_1+r_2}$ a proper subvector space of W containing $\Phi_{\log}(\mathbb{Z}_K^\times)$. The projection $W \to \mathbb{R}^{r_1+r_2-1}$ given by $(y_1, \dots, y_{r_1+r_2}) \mapsto (y_1, \dots, y_{r_1+r_2-1})$ is an isomorphism of $\mathbb{R}$-vector spaces. Via this projection, W_0 corresponds to a subvector space of $\mathbb{R}^{r_1+r_2-1}$. In particular, there exists a vector $(c_1, \dots, c_{r_1+r_2-1}) \in \mathbb{R}^{r_1+r_2-1}$ such that, for all $w \in W_0$, $\sum_{i=1}^{r_1+r_2-1} c_i w_i = 0$. We will find an $u \in \mathbb{Z}_K^\times$ such that

$$\sum_{i=1}^{r_1+r_2-1} c_i \log|\sigma_i(u)| \neq 0.$$

Let us fix some constant

$$M > \left(\frac{2}{\pi}\right)^{r_2} \sqrt{|\mathrm{disc}(\mathbb{Z}_K)|}.$$

The main step in the proof of this lemma is to show that, for any tuple $\mathbf{A} = (A_1, \dots, A_{r_1+r_2-1}) \in \mathbb{R}_{>0}^{r_1+r_2-1}$ of positive real numbers, there exists an $a \in \mathbb{Z}_K$ such that $|N_{K/\mathbb{Q}}(a)| \leq M$ and

$$\left| \sum_{i=1}^{r_1+r_2-1} c_i \log|\sigma_i(a)| - \sum_{i=1}^{r_1+r_2-1} c_i \log A_i \right| \leq \sum_{i=1}^{r_1+r_2-1} |c_i| \log M. \tag{6.9}$$

We proceed as follows: given $\mathbf{A} = (A_1, \dots, A_{r_1+r_2-1})$, set

$$A_{r_1+r_2} := \sqrt{\frac{M}{\prod_{i=1}^{r_1} 2A_i \prod_{j=r_1+1}^{r_2-1} A_j^2}}.$$

Then, like in the proof of Proposition 6.28, we consider the set $S \subset \mathbb{R}^{r_1+2r_2}$ defined by

$$S = \{(x_1, \dots, x_{r_1}, y_1, {y'}_1, \dots, y_{r_2}, {y'}_{r_2}) : \\ |x_i| \leq A_i \text{ for all } i = 1, \dots, r_1, \sqrt{y_j^2 + {y'_j}^2} \leq A_j \text{ for all } j = r_1 + 1, \dots, r_1 + r_2\}.$$

We already saw in the proof of Proposition 6.28 that S is a centrally symmetric and convex set of Lebesgue measure

$$\mu(S) = \prod_{i=1}^{r_1}(2A_i) \cdot \prod_{j=1}^{r_2}(\pi B_j^2) = 2^{r_1}\pi^{r_2} \prod_{i=1}^{r_1} A_i \prod_{j=r_1+1}^{r_1+r_2} A_j^2 = 2^{r_1}\pi^{r_2} M > 2^{r_1+r_2} v(\Phi(\mathbb{Z}_K)).$$

Therefore by Corollary 6.20 there exists $a_{\mathbf{A}} \in \mathbb{Z}_K$ such that $\Phi(a_{\mathbf{A}}) \in S$. That means that

$$|\sigma_i(a_{\mathbf{A}})| \leq A_i \text{ for all } i = 1, \dots, r_1 + r_2$$

Now we will play around with these inequalities. First note that

$$|N_{K/\mathbb{Q}}(a_{\mathbf{A}})| = \prod_{i=1}^{n} |\sigma_i(a_{\mathbf{A}})| = \prod_{i=1}^{r_1} |\sigma_i(a_{\mathbf{A}})| \prod_{i=r_1+1}^{r_1+r_2} |\sigma_i(a_{\mathbf{A}})|^2 \leq \prod_{i=1}^{r_1} A_i \prod_{i=r_1+1}^{r_1+r_2} A_i^2 = M. \tag{6.10}$$

To complete the main step, we need to check that Equation (6.9) holds for $a = a_{\mathbf{A}}$.
On the one hand, since $a_{\mathbf{A}} \in \mathbb{Z}_K$, its norm satisfies $|N_{K/\mathbb{Q}}(a_{\mathbf{A}})| \geq 1$, and on the other hand, since $a_{\mathbf{A}} \in S$, we have that

$$|\sigma_i(a_{\mathbf{A}})| = |N_{K/\mathbb{Q}}(a_{\mathbf{A}})| \cdot \left(\prod_{j \neq i} |\sigma_j(a_{\mathbf{A}})|\right)^{-1} \geq 1 \cdot \left(\prod_{j \neq i} |\sigma_j(a_{\mathbf{A}})|\right)^{-1} \geq A_i M^{-1}$$

Therefore we have, for all $i = 1, \dots, n$,

$$A_i M^{-1} \leq |\sigma_i(a_{\mathbf{A}})| \leq A_i$$

We now take logarithms in this equation (recall that all A_i are positive numbers)

$$\log A_i - \log M \leq \log |\sigma_i(a_{\mathbf{A}})| \leq \log A_i$$

Multiplying by -1 and summing $\log A_i$ we obtain that, for all $i = 1, \dots, n$,

$$0 \leq \log A_i - \log |\sigma_i(a_{\mathbf{A}})| \leq \log M.$$

Now we can estimate the difference between $\sum_{i=1}^{r_1+r_2-1} c_i \log |\sigma_i(a_{\mathbf{A}})|$ and $\sum_{i=1}^{r_1+r_2-1} c_i \log A_i$ as follows:

$$\left| \sum_{i=1}^{r_1+r_2-1} c_i \log |\sigma_i(a_{\mathbf{A}})| - \sum_{i=1}^{r_1+r_2-1} c_i \log A_i \right| \\ = \left| \sum_{i=1}^{r_1+r_2-1} c_i (\log |\sigma_i(a_{\mathbf{A}})| - \log A_i) \right| \leq \sum_{i=1}^{r_1+r_2-1} |c_i| \log M.$$

This completes the main step.
Let $M_1 > \sum_{i=1}^{r_1+r_2-1} |c_i| \log M$. Now we will apply the main step to the following tuples $\mathbf{A}$: For each $m \in \mathbb{N}$, choose $A_1^{(m)}, \dots, A_{r_1+r_2-1}^{(m)} > 0$ such that $\sum_{i=1}^{r_1+r_2-1} c_i \log A_i^{(m)} = 2mM_1$, and set $\mathbf{A}^{(m)} := (A_1^{(m)}, \dots, A_{r_1+r_2-1}^{(m)})$. Then (by the main step) there exists $a_m \in \mathbb{Z}_K$ satisfying that $|N_{K/\mathbb{Q}}(a_m)| \leq M$ and Equation (6.9), that is to say,

$$\left| \sum_{i=1}^{r_1+r_2-1} c_i \log |\sigma_i(a_m)| - 2M_1 m \right| \leq M_1.$$

Therefore we have that

$$\sum_{i=1}^{r_1+r_2-1} c_i \log |\sigma_i(a_m)| \in ((2m-1)M_1, (2m+1)M_1).$$

This implies that the sequence of numbers $\{\sum_{i=1}^{r_1+r_2-1} c_i \log |\sigma_i(a_m)|\}_{m\in\mathbb{N}}$ is strictly increasing.
But, on the other hand, the principal ideals $a_m\mathbb{Z}_K$ have all norm bounded by M, and we know that there are only a finite number of integral ideals with bounded norm (see the proof of Theorem 6.30). Therefore there exist $m_1 \neq m_2$ such that $a_{m_1}\mathbb{Z}_K = a_{m_2}\mathbb{Z}_K$. Hence there is a unit $u \in \mathbb{Z}_K^\times$ such that $a_{m_1} = ua_{m_2}$, and

$$\sum_{i=1}^{r_1+r_2-1} c_i \log |\sigma_i(a_{m_1})| = \sum_{i=1}^{r_1+r_2-1} c_i \log |\sigma_i(ua_{m_2})| = \sum_{i=1}^{r_1+r_2-1} c_i \log |\sigma_i(u)| + \sum_{i=1}^{r_1+r_2-1} c_i \log |\sigma_i(a_{m_2})|,$$

thus

$$\sum_{i=1}^{r_1+r_2-1} c_i \log |\sigma_i(u)| = \sum_{i=1}^{r_1+r_2-1} c_i \log |\sigma_i(a_{m_1})| - \sum_{i=1}^{r_1+r_2-1} c_i \log |\sigma_i(a_{m_2})| \neq 0.$$

This shows that $u \notin W_0$, and concludes the proof of Theorem 6.37.

□

To finish this section we will see how Dirichlet Unit Theorem applies to the case of real quadratic fields, allowing a complete description of the solutions of the Pell equation considered in Example 6.1.
Let $d \in \mathbb{Z}$ be a squarefree, positive number, and let $K = \mathbb{Q}(\sqrt{d})$. For the rest of the section, fix an embedding $K \hookrightarrow \mathbb{R}$. We have that $n := [K : \mathbb{Q}] = 2$, and, since $K \subset \mathbb{R}$, $r_2 = 0$ and $r_1 = 2$. Therefore $r_1 + r_2 - 1 = 1$, and from Dirichlet Unit Theorem we obtain:

Corollary 6.49. *Let K be a real quadratic field. Then $\mathbb{Z}_K^\times \simeq \mu_K \times \mathbb{Z}$.*

Note that the only roots of unity in $\mathbb{R}$ are ± 1 (since the m-th roots of unity in $\mathbb{C}$ are $e^{\frac{2\pi i r}{m}}$, $r = 1, \dots, m$, and of these only ± 1 are real). In particular, since $K \subset \mathbb{R}$, the only roots of unity of K are ± 1. Hence

$$\mathbb{Z}_K^\times \simeq \{\pm 1\} \times \mathbb{Z}.$$

For each $z \in \mathbb{Z}_K^\times$, we have that $-z, z^{-1}, -z^{-1}$ also belong to $\mathbb{Z}_K^\times$. Assume that $z > 0$ (otherwise, interchange z and $-z$). Then $z^{-1} > 0$, $-z, -z^{-1} < 0$. Moreover, if $z \neq 1$, one of the two numbers z, z^{-1} must be greater than 1, the other smaller than 1. Interchanging z and z^{-1} if necessary, we can assume $z > 1$. Then

$$z > 1 > z^{-1} > 0 > -z^{-1} > -1 > -z.$$

If we consider only the units which are ≥ 0 , then these form a group isomorphic to $\mathbb{Z}$, say $\mathbb{Z}_{K,>0}^\times$. There are two elements $z, z^{-1} \in \mathbb{Z}_{K,>0}^\times$ that generate the group (those corresponding to $\pm 1 \in \mathbb{Z}$). The neutral element in $\mathbb{Z}$, which is 0, corresponds to the neutral element of $\mathbb{Z}_{K,>0}^\times$, which is 1, so $z \neq 1$, and therefore one of the two numbers $z, z^{-1} \in \mathbb{R}$ is greater than 1, and the other smaller than 1. Denote by $\mathbb{Z}_{K,>1}$ the units that are > 1. We call the *fundamental unit of* $\mathbb{Z}_K$ the generator of $\mathbb{Z}_{K,>0}^\times$ that belongs to $\mathbb{Z}_{K,>1}$ (note that this terminology differs slightly from Definition 6.40, and note also that it depends on our choice of embedding $K \subset \mathbb{R}$). Thus in order to find all units of $\mathbb{Z}_K$, it is enough to find the fundamental unit $z_1 = a_1 + b_1\sqrt{d} \in \mathbb{Z}_{K,>1}^\times$; then

$$\begin{aligned}
\mathbb{Z}_K^\times &= \{\pm(a_1 + b_1\sqrt{d})^m : m \in \mathbb{Z}\} \\
\mathbb{Z}_{K,>0}^\times &= \{(a_1 + b_1\sqrt{d})^m : m \in \mathbb{Z}\} \\
\mathbb{Z}_{K,>1}^\times &= \{(a_1 + b_1\sqrt{d})^m : m \in \mathbb{N}\}
\end{aligned}$$

Note that, since

$$N_{K/\mathbb{Q}}(z_1) = (a_1 + b_1\sqrt{d})(a_1 - b_1\sqrt{d}) = \pm 1,$$

either $z_1^{-1} = a_1 - b_1\sqrt{d}$ (and $-z_1^{-1} = -a_1 + b_1\sqrt{d}$), or $z_1^{-1} = -a_1 + b_1\sqrt{d}$ (and $-z_1^{-1} = a_1 - b_1\sqrt{d}$). We have

$$\{z_1, z_1^{-1}, -z_1, -z_1^{-1}\} = \{a_1 + b_1\sqrt{d}, a_1 - b_1\sqrt{d}, -a_1 + b_1\sqrt{d}, -a_1 - b_1\sqrt{d}\}.$$

Of these four numbers the biggest is $|a_1| + |b_1|\sqrt{d}$. Therefore we conclude that $a_1, b_1 \geq 0$, and the equation $\pm 1 = a_1^2 - b_1^2 d$, together with the fact that $z_1 \neq 0$, implies that $b_1 > 0$.
Call $z_m = a_m + b_m\sqrt{d}$, then

$$\begin{cases} a_{m+1} := a_m a_1 + d b_m b_1 \\ b_{m+1} := a_m b_1 + a_1 b_m \end{cases}$$

Note that the sequence $\{b_m\}_{m\in\mathbb{N}}$ is increasing. Hence $b_1 := \min\{b \in \mathbb{N} : \exists a \in \mathbb{N} \text{ such that } a^2 - db^2 = \pm 1\}$. In this way one can explicitly find the fundamental unit z_1.

We now focus on the solution to Pell's equation. We distinguish two cases:

- $d \equiv 2, 3 \pmod 4$. Then $\mathbb{Z}_K = \mathbb{Z}[\sqrt{d}]$. For any $m \in \mathbb{Z}$, define $z_m = a_m + b_m\sqrt{d} := z_1^m$.

  There are two possibilities:

  - If $N_{K/\mathbb{Q}}(z_1) = 1$, then for all $m \in \mathbb{Z}$ we have $a_m^2 - db_m^2 = N_{K/\mathbb{Q}}(z_1)^m = 1$. The solutions of the equation $x^2 - dy^2$ correspond to the elements in $\mathbb{Z}_K^\times$.
  - If $N_{K/\mathbb{Q}}(z_1) = -1$, then for all $m \in \mathbb{Z}$ we have $a_m^2 - db_m^2 = N_{K/\mathbb{Q}}(z_1)^m = (-1)^m$. The solutions of the equation $x^2 - dy^2$ correspond to the elements in $\langle -1, z_1^2\rangle \subset \mathbb{Z}_K^\times$.

- $d \equiv 1 \pmod 4$. Then $\mathbb{Z}_K = \mathbb{Z}[\frac{1+\sqrt{d}}{2}]$.

  Write
  $$z_1 = a \cdot 1 + b \cdot \left(\frac{1+\sqrt{d}}{2}\right) = \frac{x_1}{2} + \frac{y_1}{2}\sqrt{d}.$$
  For each $m \in \mathbb{N}$, define $z_m = (x_m/2) + (y_m/2)\sqrt{d} := z_1^m$. Now we have to distinguish cases, according to the parity of b:

  – Assume b is even. Then for all $m \in \mathbb{Z}$, $a_m := x_m/2$ and $b_m := y_m/2$ are integers, and they satisfy $a_m^2 + db_m^2 = N_{K/\mathbb{Q}}(z_1)^m = (\pm 1)^m$.

    ∗ Assume $N_{K/\mathbb{Q}}(z_1) = 1$. Then all units correspond to solutions of $x^2 - dy^2 = 1$.

    ∗ Assume $N_{K/\mathbb{Q}}(z_1) = -1$. The solutions of $x^2 - dy^2 = 1$ correspond to the units in $\langle -1, z_1^2 \rangle \subset \mathbb{Z}_K^\times$.

  – Assume that b_1 is odd. Then
  $$z_2 = \frac{1}{2^2}(x_1 + y_1\sqrt{d})^2 = \frac{1}{2}(\frac{x_1^2 + y_1^2 d}{2} + \frac{2x_1y_1}{2}\sqrt{d}) = \frac{1}{2}\left(\frac{x_1^2 + y_1^2 d}{2} + x_1y_1\sqrt{d}\right)$$
  Note that, since $d \equiv 1 \pmod 4$, $x_1^2 + y_1^2 d$ is divisible once and only once by 2, hence $x_2 = \frac{x_1^2+y_1^2 d}{2}$ and $y_2 = x_1y_1$ are both odd.

  $$z_3 = \frac{1}{2^3}(x_1 + y_1\sqrt{d})^3 = \frac{1}{8}(x_1^3 + 3x_1y_1^2 d + (3x_1^2y_1 + y_1^3 d)\sqrt{d}) = \frac{1}{8}(x_1(x_1^2 + 3y_1^2 d) + y_1(3x_1^2 + y_1^2 d)\sqrt{d})$$
  Now both $x_1^2 + 3y_1^2 d = (\pm 4 + y_1^2 d) + 3y_1^2 d = 4(\pm 1 + y_1 d)$ and $3x_1^2 + y_1^2 d = 3x_1^2 + (\pm 4 + x_1^2) = 4(x_1^2 \pm 1)$ are divisible by 8, hence x_3, y_3 are both even, and $a_3 = \frac{x_3}{2}$ and $b_3 = \frac{y_3}{2}$ is a solution of $x^2 - dy^2 = \pm 1$.

  In other words, we have shown that $a_m := x_m/2$ and $b_m := y_m/2$ are integers if and only if $3|m$, and they satisfy $a_m^2 + db_m^2 = N_{K/\mathbb{Q}}(z_1)^m = (-1)^m$.

  ∗ Assume $N_{K/\mathbb{Q}}(z_1) = 1$. The solutions of $x^2 - dy^2 = 1$ correspond to the units in $\langle -1, z_1^3 \rangle \subset \mathbb{Z}_K^\times$.

  ∗ Assume $N_{K/\mathbb{Q}}(z_1) = -1$. The solutions of $x^2 - dy^2 = 1$ correspond to the units in $\langle -1, z_1^6 \rangle \subset \mathbb{Z}_K^\times$.

Remark 6.50. *The smallest solution to the Problem of the Cattle of the Sun (see Example 6.1 and Sheet 8) has 206545 digits (in base ten).*