Algebraic Number Theory

Sergey Shpectorov

January–March, 2010

This course in on algebraic number theory. This means studying problems from number theory with methods from abstract algebra. For a long time the main motivation behind the development of algebraic number theory was the Fermat Last Theorem. Proven in 1995 by Wiles with the help of Taylor, this theorem states that there are no positive integers x, y and z satisfying the equation

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

where $n \geq 3$ is an integer. The proof of this statement for the particular case $n = 4$ goes back to Fibonacci, who lived four hundred years before Fermat. Modulo Fibonacci's result, Fermat Last Theorem needs to be proven only for the cases where $n = p$ is an odd prime. By the end of the course we will hopefully see, as an application of our theory, how to prove the Fermat Last Theorem for the so-called *regular* primes. The idea of this belongs to Kummer, although we will, of course, use more modern notation and methods.

Another accepted definition of algebraic number theory is that it studies the so-called *number fields*, which are the finite extensions of the field of rational numbers $\mathbb{Q}$. We mention right away, however, that most of this theory applies also in the second important case, known as the case of *function fields*. For example, finite extensions of the field of complex rational functions $\mathbb{C}(x)$ are function fields. We will stress the similarities and differences between the two types of fields, as appropriate.

Finite extensions of $\mathbb{Q}$ are algebraic, and this ties algebraic number theory with Galois theory, which is an important prerequisite for us. Other prerequisites include basic ring theory (homomorphisms, ideals, factor rings; also domains and field of fractions) and elementary number theory (primes and prime factorization). We will very briefly review those topics, as they become necessary.

In our exposition of algebraic number theory we follow the book "A Brief Guide to Algebraic Number Theory" by Swinnerton-Dyer. We will cover Chapters 1 and 2, as well as as large part of Chapter 3 as we can manage. We will also need the first half of the Appendix.

Chapter 1

Algebraic integers

We first cover the necessary topics from the Appendix of the book. This includes finitely generated abelian groups, the language of modules for rings, and norms and traces on finite field extensions. These topics are not usually covered in our courses. We will however skip some of the proofs to save time, or leave them as exercises.

After that we introduce the algebraic integers and develop the fundamental theory of the ring of integers. We note that below the word "integer" is often used to mean "algebraic integer", rather than to refer to just the elements of $\mathbb{Z}$, which we will often call rational integers.

1.1 Finitely generated abelian groups

In this section all groups are abelian. Accordingly, we will use additive notation for groups.

A set X of elements in a group G is said to *generate* G if X is not contained in any proper subgroup of G. We will refer to the individual elements of X as to *generators*; note, however, that this property makes no sense without the entire set X. We say that G is *finitely generated* if it admits a finite set of generators. It is clear that every factor group of a finitely generated group is finitely generated. Indeed, take a finite set of generators X in G and consider its image $\bar{X}$ in the factor group $\bar{G}$. Then $\bar{X}$ is a finite set of generators for $\bar{G}$.

We will see that a similar statement is true for subgroups, that is, every subgroup of a finitely generated (abelian!) group is finitely generated, although the proof of that is not as easy.

An element $g \in G$ is called a *torsion* element if it has a finite order. (The zero element has order one and so it's a torsion element according to this

definition.) We say that G is *torsion-free* if zero is the only torsion element in G.

Proposition 1.1.1 *All torsion elements of an abelian group G form a subgroup G_T. Furthermore, G/G_T is torsion-free.*

Proof: Both statements are left as exercises. □

The subgroup G_T is called the *torsion subgroup* of G. If G is finitely generated then G/G_T is finitely generated and torsion-free, so let us take a look at such groups.

Proposition 1.1.2 *Suppose G is a finitely generated torsion-free abelian group. Let $\{g_1, g_2, \ldots, g_n\}$ be a set of generators that is minimal with respect to inclusion. Then these generators satisfy no non-trivial relation*

$$a_1 g_1 + a_2 g_2 + \ldots + a_n g_n = 0,$$

with $a_1, a_2, \ldots, a_n \in \mathbb{Z}$.

Proof: By contradiction, suppose non-trivial relations exist for some minimal generating sets. Select a minimal generating set $\{g_1, g_2, \ldots, g_n\}$ and a non-trivial relation $a_1 g_1 + a_2 g_2 + \ldots + a_n g_n = 0$, so that $|a_1| + |a_2| + \ldots + |a_n|$ is minimal possible. Substituting $-g_i$ for g_i, as needed, we may assume that all a_i are nonnegative.

We note that at least two of the a_i must be non-zero. Indeed, if exactly one a_i is non-zero then the corresponding g_i is a torsion element; a contradiction, since $g_i \neq 0$ and G is torsion-free.

Without loss of generality assume that a_1 and a_2 are nonzero and, furthermore, that $a_1 \leq a_2$. The above relation can be rewritten as $a_1(g_1 + g_2) + (a_2 - a_1)g_2 + a_3 g_3 \ldots + a_n g_n = 0$, which is a nontrivial (as $a_1 \neq 0$) relation for the minimal generating set $g_1 + g_2, g_2, g_3, \ldots, g_n$. This relation has a smaller sum of coefficients, which contradicts our choice. This is the final contradiction, proving the claim. □

Note the absence of non-trivial relations for the generators $\{g_1, g_2, \ldots, g_n\}$ means that $G \cong \mathbb{Z}^n$, namely, $G = \langle g_1 \rangle \times \langle g_2 \rangle \times \ldots \times \langle g_n \rangle$. Indeed, the isomorphism from $\mathbb{Z}^n$ onto G can be defined simply as $(a_1, a_2, \ldots, a_n) \mapsto a_1 g_1 + a_2 g_2 + \ldots + a_n g_n$. The group $\mathbb{Z}^n$ (and hence also our group G) is called the *free abelian group* of *rank* n.

Any minimal set of generators for G as above will be called a *base* of G. All bases of G have the same size n, the rank of G. This can be seen as follows: n is an invariant of G because for any prime number p we have that $G/pG \cong \mathbb{Z}^n/p\mathbb{Z}^n \cong \mathbb{Z}_p^n$ is a group of order p^n. Here for an abelian group G,

we denote by pG the subgroup $\{pg \mid g \in G\}$. Thus we see that $\mathbb{Z}^n \cong \mathbb{Z}^m$ if and only if $n = m$.

Proposition 1.1.3 *Suppose G is an abelian group and $H \leq G$ such that G/H is a free abelian group of some rank n. Then $G = H \times K$ for some $K \leq G$ with $K \cong \mathbb{Z}^n$.*

Proof: Choose a base $\{k_1 + H, k_2 + H, \ldots, k_n + H\}$ in G/H and define $K = \langle k_1, k_2, \ldots, k_n \rangle$. Then, as no integral linear combination of $k_1, k_2, \ldots, k_n$ is contained in H, this set is a base for K and, furthermore, $K \cap H = 0$. Since also $G = H + K$, we get that $G = H \times K$. □

As a consequence of this we determine the structure of an arbitrary finitely generated abelian group.

Corollary 1.1.4 *If G is a finitely generated abelian group then $G = G_T \times F$ for a subgroup $F \leq G$ that is free abelian of some rank n.*

Proof: By Proposition 1.1.1, G/G_T is torsion-free. Hence by Proposition 1.1.2, G/G_T is free abelian of some rank n. Now an application of Proposition 1.1.3 completes the proof. □

Corollary 1.1.5 *If G is a finitely generated abelian group then G_T is a finite group.*

Proof: Indeed, by Corollary 1.1.4, $G_T \cong G/F$ for some subgroup $F \leq G$. Hence G_T is finitely generated. Now an abelian group generated by finitely many elements of finite order is finite. The details of this last step are left as an exercise. □

These two corollaries mean in short that every finitely generated abelian group is a direct product of cyclic groups (finite or infinite). Indeed, G_T, being a finite group, is the direct product of finite cyclic groups, while the complementary factor F is isomorphic to $\mathbb{Z}^n$. We note that this n (the rank of G/G_T) is an invariant of G and will be called the *free rank* of G.

Lastly, we will show that the subgroups of finitely generated groups are finitely generated and also relate the free rank of the subgroup with the free rank of the group.

We first deal with the torsion-free case. We will need the following lemma.

Lemma 1.1.6 *Suppose G is free abelian of rank n. Suppose further that $H \leq G$ and it is known that H is also free abelian of some rank m. Then $m \leq n$.*

Proof: We note that G/H is a finitely generated group. Hence its torsion subgroup $(G/H)_T$ is finite. Let p be a prime that does not divide the order of $(G/H)_T$. We claim that $pG \cap H = pH$. Indeed, clearly, $pH \subseteq pG$. Let $x \in pG \cap H$. Then $x = pg$ for some $g \in G$. Furthermore, $p(g+H) = pg+H = H$. Hence the coset $g + H$ is a torsion element in G/H and its order divides p. Since p was chosen to be coprime to $(G/H)_T$, we conclude that $g + H$ is the zero element of G/H, that is, $g + H = H$ and $g \in H$. Hence $x = pg \in pH$. We have shown that $pG \cap H = pH$.

Now by the Second Isomorphism Theorem,

$$H/pH = H/(pG \cap H) \cong (H + pG)/pG \leq G/pG.$$

Since $|H/pH| = p^m$ and $|G/pG| = p^n$, we conclude that $m \leq n$. □

Proposition 1.1.7 *If G is free abelian of rank n and $H \leq G$ then H is also free abelian of some rank $r \leq n$.*

Proof: We just need to show that H is finitely generated. Indeed, H is torsion-free, since so is G, which means that H is free abelian, and the above lemma completes the proof.

To show that H is finitely generated, consider a subgroup $K \leq H$, that is free abelian of the largest possible rank. (This is well-defined, since the lemma above limits the possible rank of free abelian subgroups by n.) We claim that H/K is entirely torsion, that is, $H/K = (H/K)_T$. Indeed, if not, $\bar{H} = H/K$ contains a subgroup $\bar{F} \cong \mathbb{Z}$. Let F be the full preimage of $\bar{F}$ in H (that is, $F = \{x \in H \mid \bar{x} = x + H \in \bar{F}\}$). Then $K \leq F$ and $F/K = \bar{F} \cong \mathbb{Z}$. By Proposition 1.1.3, F is free abelian of the rank one higher than the rank of K; a contradiction with the choice of K. Hence indeed, H/K is entirely torsion.

Since $H/K \leq G/K$, which is finitely generated and hence its torsion subgroup is finite by Corollary 1.1.5, we conclude that H/K is a finite group. Pick a base $k_1, k_2, \ldots, k_s$ in K and a set of generators $h_1+K, h_2+K, \ldots, h_r+K$ in H/K. Clearly, $k_1, \ldots, k_s, h_1, \ldots, h_r$ generate H. □

We also note the following fact. Its proof is a modification of the proof of the lemma above. It is left as an exercise.

Proposition 1.1.8 *If G is free abelian and $H \leq G$ then G and H have the same rank if and only if G/H is finite.*

Finally, the statement about the general finitely generated abelian groups.

Corollary 1.1.9 *If G is a finitely generated abelian group and $H \leq G$ then H is also finitely generated. Furthermore, the free rank of H is at most the free rank of G.*

Proof: We observe that $H_T \leq G_T$. Hence, H_T is a finite group, since G_T is so. Moreover, $H_T = H \cap G_T$, which means that $H/H_T = H/(H \cap G_T) \cong (H + G_T)/G_T$. The latter is a subgroup of the free abelian group G/G_T. By Proposition 1.1.7, H/H_T is free abelian and its rank is bounded by the rank of G/G_T. This yields all statements. □

1.2 Modules

In this course we will be using the language of modules. A *module* over a ring R (or an R-module) is an abelian group M together with a product operation $R \times M \to M$ that satisfy the following properties:

(M1) (Associativity) $r(sm) = (rs)m$ for all $r, s \in R$ and $m \in M$;

(M2) (Distributivity I) $(r + s)m = rm + sm$ for all $r, s \in R$ and $m \in M$;

(M3) (Distributivity II) $r(m + n) = rm + rn$ for all $r \in R$ and $m, n \in M$.

We will be exclusively dealing with the case where R is a domain (also called an integral domain), that is, a commutative ring with one and with no zero divisors. Whenever the ring has one, we will additionally require

(M4) (Identity) $1m = m$ for all $m \in M$.

There are at least two (and possibly three) kinds of modules that you have already met. If $R = F$ is a field then an F-module is simply a vector space with coefficients from F. Secondly, in the Representation Theory course you may have met the group modules. Note that a module for a group G over a field F is nothing but an FG-module where FG is the group algebra of G over F.

The last example is more closely related to the present course. A $\mathbb{Z}$-module is nothing but an abelian group. First of all, every $\mathbb{Z}$-module M is an abelian group by definition. Furthermore, the product operation is uniquely defined. Indeed, as follows from (M1)-(M4), we have, for $n \in \mathbb{Z}$ and $m \in M$:

$$nm = \begin{cases} 0, & \text{if } n = 0; \\ m + m + \ldots + m \ (n \text{ times}), & \text{if } n > 0; \\ -m - m - \ldots - m \ (|n| \text{ times}), & \text{if } n < 0. \end{cases} \tag{1.1}$$

This means that the structure of the $\mathbb{Z}$-module M is entirely specified by its group structure. Furthermore, the formulas in 1.1 produce a $\mathbb{Z}$-module structure on an arbitrary abelian group M. Hence $\mathbb{Z}$-modules and abelian groups are one and the same.

This last example can also be used to illustrate the big difference between the vector spaces (*i.e.*, modules over fields) and the general modules. For example, a $\mathbb{Q}$-vector space, as an additive group, is infinite and has no torsion. In fact, it is always a direct product of several copies of $\mathbb{Q}$ (viewed as an additive group). At the same time, a $\mathbb{Z}$-module can have torsion and can be finite, even though $\mathbb{Z}$ is infinite.

For a set $X \subseteq M$, where M is an R-module, we will denote by $\langle X \rangle$ the submodule of M *generated* by X, that is, the smallest submodule of M containing X. We say that M is *finitely generated* if $M = \langle X \rangle$ for a finite set X. If $R = \mathbb{Z}$ then $\langle X \rangle$ is the same as the subgroup of M generated by X. (This is not true for general modules over rings.) Furthermore, M is finitely generated as a $\mathbb{Z}$-module if and only if it is finitely generated as a group.

Therefore, the following is directly implied by Corollary 1.1.9.

Proposition 1.2.1 *If V is a finitely generated $\mathbb{Z}$-module and U is a submodule of V then U is also finitely generated.* □

Lastly, in the book and in our notes we will use the tensor product notation, such as, say, $M \otimes_{\mathbb{Z}} \mathbb{Q}$. We won't go into what this really means. For our purposes, it will suffice to know that $M \otimes_{\mathbb{Z}} \mathbb{Q}$ is a vector space over $\mathbb{Q}$, which contains M and which is spanned (over $\mathbb{Q}$) by any generating set of M.

1.3 Algebraic integers

Here we start Algebraic Number Theory proper!

Recall from the Galois Theory course that a field element $\alpha \in \mathbb{C}$ is algebraic (over $\mathbb{Q}$) if it is a root of a polynomial from $\mathbb{Q}[x]$. All algebraic elements form a subfield $\bar{\mathbb{Q}}$ of $\mathbb{C}$ known as the *algebraic closure* of $\mathbb{Q}$. This field $\bar{\mathbb{Q}}$ will be our universe because every *number field*, *i.e.*, a finite extension of $\mathbb{Q}$, embeds into $\bar{\mathbb{Q}}$. So we will just think of number fields as subfields of $\bar{\mathbb{Q}}$.

The main difference between Galois Theory and Algebraic Number Theory is that Galois Theory deals exclusively with fields. Algebraic Number Theory deals, on the other hand, with rings. To define these rings we need now to introduce special algebraic elements. An element $\alpha \in \bar{\mathbb{Q}}$ is an *algebraic integer* if it is a root of a monic polynomial from $\mathbb{Z}[x]$. Recall that a

monic polynomial is a nonzero polynomial with the leading coefficient equal to one.

We will first prove two different ways to check that α is an algebraic integer. For a set of elements $A \subseteq \bar{\mathbb{Q}}$, let $\mathbb{Z}[A]$ be the smallest subring of $\bar{\mathbb{Q}}$ containing A (and $\mathbb{Z}$, of course). When $A = \{\alpha_1, \ldots, \alpha_n\}$ is finite, we write $\mathbb{Z}[\alpha_1, \ldots, \alpha_n]$ instead of $\mathbb{Z}[\{\alpha_1, \ldots, \alpha_n\}]$. We will need the following description of $\mathbb{Z}[\alpha_1, \ldots, \alpha_n]$.

Proposition 1.3.1 *The subring $\mathbb{Z}[\alpha_1, \ldots, \alpha_n]$ consists of all $\beta \in \bar{\mathbb{Q}}$, which can be expressed as $\beta = f(\alpha_1, \ldots, \alpha_n)$ for some $f \in \mathbb{Z}[x_1, \ldots, x_n]$. In other words, $\mathbb{Z}[\alpha_1, \ldots, \alpha_n]$ is the image of the evaluation homomorphism $\mathbb{Z}[x_1, \ldots, x_n] \to \bar{\mathbb{Q}}$ sending $f \in \mathbb{Z}[x_1, \ldots, x_n]$ to $f(\alpha_1, \ldots, \alpha_n)$.* □

In particular, $\mathbb{Z}[\alpha]$ consists of all $\beta = f(\alpha)$, where $f \in \mathbb{Z}[x]$. We can now state and prove the following result.

Proposition 1.3.2 *The following conditions are equivalent:*

(1) α is a root of a monic polynomial from $\mathbb{Z}[x]$;

(2) the minimal polynomial of α over $\mathbb{Q}$ is in $\mathbb{Z}[x]$; and

(3) $\mathbb{Z}[\alpha]$ is a finitely generated $\mathbb{Z}$-module.

Proof: We will first show that (1) and (2) are equivalent. Clearly, (2) implies (1), since the minimal polynomial is monic by definition. Suppose α is a root of a monic polynomial $f \in \mathbb{Z}[x]$. Then $f = mg$, where $m \in \mathbb{Q}[x]$ is the minimal polynomial of α and $g \in \mathbb{Q}[x]$ is just some polynomial. If $m \in \mathbb{Z}[x]$ then there is nothing to prove. Otherwise, at least one of the coefficients in m is not integer and so we can take a prime p that divides the denominator of that coefficient. Let p^a be the highest power of p that divides any of the denominators in m and, similarly, let p^b be the highest power of p that divides any of the denominators in g. We note that b can be zero, but $a \geq 1$ by our choice of p.

We now reduce the equation $p^{a+b} f = (p^a m)(p^b g)$ modulo p. Namely, we notice that all coefficients of $m' = p^a m$ and $g' = p^b g$ are contained in the subring $R = \{\frac{a}{b} \in \mathbb{Q} \mid \mathrm{hcf}(b, p) = 1\}$ of $\mathbb{Q}$. Furthermore, the mapping $\phi : R \to \mathbb{Z}_p$ defined by $\frac{a}{b} \mapsto \bar{a}\bar{b}^{-1}$ (where the bar means taking the integer modulo p) is a surjective homomorphism of rings. We leave this last statement as an exercise, but just note that since $\mathrm{hcf}(b, p) = 1$, the congruence class $\hat{b}$ is nonzero, and so $\hat{b}^{-1}$ is defined.

The homomorphism ϕ also leads to a homomorphism $\hat{\phi} : R[x] \to \mathbb{Z}_p[x]$. By the choice of p^a and p^b, both $\hat{\phi}(p^a m)$ and $\hat{\phi}(p^b g)$ are nonzero, while

$\hat{\phi}(p^{a+b}f)$ is zero, since all coefficients are integer multiples of p. This is a contradiction, proving that m has integral coefficients.

Now we prove the equivalence of (1) and (3). First suppose that (1) holds. Then $f(\alpha) = 0$ for some monic polynomial $f \in \mathbb{Z}[x]$. Let $f = x^n + g$, where $g \in \mathbb{Z}[x]$ is, clearly, a polynomial of degree less or equal $n-1$. Consider the $\mathbb{Z}$-submodule V generated by $1, \alpha, \alpha^2, \ldots, \alpha^{n-1}$. Since $f(\alpha) = 0$, we have that $\alpha^n = -g(\alpha) \in V$. By induction, using $\alpha^{n+m} = \alpha^m g(\alpha)$, we have that all powers of α are in V, which means that $\mathbb{Z}[\alpha]$ is a submodule of V. By Proposition 1.2.1, $\mathbb{Z}[\alpha]$ is finitely generated as a $\mathbb{Z}$-module. Hence (3) holds.

Now assume that (3) holds. Pick a finite generating set $\beta_1, \beta_2, \ldots, \beta_m$ for the module $\mathbb{Z}[\alpha]$. By Proposition 1.3.1, every β_i is equal to $f_i(\alpha)$ for some $f_i \in \mathbb{Z}[x]$. Let n be greater than the maximal degree of the f_i's. Since $\beta_1, \ldots, \beta_m$ generate $\mathbb{Z}[\alpha]$, we have $\alpha^n = a_1\beta_1 + a_2\beta_2 + \ldots + a_m\beta_m$ for some $a_1, \ldots, a_m \in \mathbb{Z}$. Set $f = x^n - a_1 f_1 - \ldots - a_m f_m \in \mathbb{Z}[x]$. Clearly, x^n is the highest term of f, and so f is a monic polynomial. Finally, $f(\alpha) = \alpha^n - a_1 f_1(\alpha) - \ldots - a_m f_m(\alpha) = \alpha^n - a_1\beta_1 - \ldots - a_m\beta_m = 0$. So (1) holds.□

This proposition shows that (2) and (3) are also necessary and sufficient conditions for α to be an algebraic integer. It follows from (3) and Proposition 1.2.1 that if a subring in $\bar{\mathbb{Q}}$ is finitely generated as a $\mathbb{Z}$ module then it consists entirely of algebraic integers. Clearly, this subring is also finitely generated as a subring. We will now prove the converse of this statement.

Proposition 1.3.3 *Suppose a subring $R \subseteq \bar{\mathbb{Q}}$ is generated by a finite number of algebraic integer elements. Then R is also finitely generated as a $\mathbb{Z}$-module.*

Proof: Suppose the algebraic integers $\alpha_1, \ldots, \alpha_m$ are the generators of R. Let n_i be the order of the minimal polynomial of α_i. As above, this means that every power of α_i is an integral linear combination of $1, \alpha_i, \ldots, \alpha_i^{n_i-1}$. Combining this with Proposition 1.3.1, we see that the products $\alpha_1^{j_1}\alpha_2^{j_2}\cdots\alpha_m^{j_m}$, where for each i we have $0 \le j_i \le n_i - 1$, generate R as a $\mathbb{Z}$-module. □

One of the consequences of this proposition is that all algebraic integers form a subring $\mathfrak{O}$ of $\bar{\mathbb{Q}}$.

Proposition 1.3.4 *The set $\mathfrak{O}$ of consisting of all algebraic integers is a subring of $\bar{\mathbb{Q}}$.*

Proof: Let $\alpha, \beta \in \mathfrak{O}$. We need to show that $\mathfrak{O}$ also contains $\alpha\beta$ and $\alpha - \beta$. By Proposition 1.3.3, $\mathbb{Z}[\alpha, \beta]$ is finitely generated as a $\mathbb{Z}$-module. Since it contains both $\mathbb{Z}[\alpha\beta]$ and $\mathbb{Z}[\alpha - \beta]$ as subrings, these subrings are also finitely generated as $\mathbb{Z}$-modules. Therefore $\alpha\beta$ and $\alpha - \beta$ are algebraic integers. □

For a subfield k of $\bar{\mathbb{Q}}$ (in particular, for a number field k), we let $\mathfrak{o}_k = \mathfrak{O} \cap k$ be the set of all algebraic integers contained in k. It follows from Proposition 1.3.4 that $\mathfrak{o}_k$ is a subring in k. We will call $\mathfrak{o}_k$ the *ring of integers* of k. The ring of integers is in the focus of this course. Let us establish some basic properties of $\mathfrak{o}_k$.

Proposition 1.3.5 *We have* $\mathfrak{o}_{\mathbb{Q}} = \mathbb{Z}$.

Proof: If $\alpha \in \mathbb{Q}$ then the minimal polynomial of α is simply the degree one polynomial $f = x - \alpha \in \mathbb{Q}[x]$. Thus, by Proposition 1.3.2, part (2), α is an algebraic integer if and only if f has integral coefficients, that is, if $\alpha \in \mathbb{Z}$. □

Since $\mathfrak{o}_k$ is a subring in a field and since $1 \in \mathfrak{o}_k$, the ring $\mathfrak{o}_k$ is a domain. We next show that k can be recovered from its ring of integers $\mathfrak{o}_k$ just like $\mathbb{Q}$ can be recovered from $\mathbb{Z}$.

Proposition 1.3.6 *Every algebraic number $\beta \in \bar{\mathbb{Q}}$ can be written as $\frac{\alpha}{a}$, where $\alpha \in \mathfrak{O}$ is an algebraic integer and $a \in \mathbb{Z}$. In particular, every subfield k of $\bar{\mathbb{Q}}$ is the field of fractions of $\mathfrak{o}_k$.*

Proof: Suppose $f = x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0 \in \mathbb{Q}[x]$ is the minimal polynomial of β. Then for $\alpha = a\beta$, where $a \in \mathbb{Z}$, the minimal polynomial is $a^n f(\frac{x}{a}) = x^n + aa_{n-1}x^{n-1} + \ldots + a^{n-1}a_1 x + a^n a_0$. In particular, if we choose a to be a common multiple of all denominators of all coefficients in f then the resulting minimal polynomial has integral coefficients, and hence this α is an algebraic integer.

The last claim is now clear. □

Note that the last claim is rather weak compared to the first statement of the proposition. We can express it more adequately by writing $k = \mathfrak{o}_k \otimes_{\mathbb{Z}} \mathbb{Q}$.

Before we switch to a new topic, we prove a further property of $\mathfrak{o}_k$. For commutative rings $R_1 \subseteq R_2$, we say that R_1 is *integrally closed* in R_2 is every $r \in R_2$ that is a root of a monic polynomial from $R_1[x]$ is, in fact, contained in R_1.

Proposition 1.3.7 *The ring $\mathfrak{O}$ is integrally closed in $\bar{\mathbb{Q}}$. In particular, for every subfield k of $\bar{\mathbb{Q}}$, we have that $\mathfrak{o}_k$ is integrally closed in k.*

Proof: Suppose $\beta \in \bar{\mathbb{Q}}$ is a root of a polynomial $f = x^n + \alpha_{n-1}x^{n-1} + \ldots + \alpha_1 x + \alpha_0$, where the coefficients α_i are all in $\mathfrak{O}$. By Proposition 1.3.3, $R = \mathbb{Z}[\alpha_{n-1}, \ldots, \alpha_0]$ is finitely generated as a $\mathbb{Z}$-module. Let $S = \{\sigma_1, \ldots, \sigma_m\}$ be a finite set of generators for it. Using essentially the same idea as in Proposition 1.3.3, we note that the products $\sigma_i \beta^j$, where $0 \leq j \leq n-1$, generate $R[\beta] = \mathbb{Z}[\alpha_{n-1}, \ldots, \alpha_0, \beta]$ as a $\mathbb{Z}$-module. Again, this implies that

the subring $\mathbb{Z}[\beta]$ is finitely generated as a $\mathbb{Z}$-module, and hence β is an algebraic integer. □

1.4 Norms and traces

We will need the concepts of the norm and trace of an element in a finite field extension. This topic really belongs in a Galois Theory course, but we usually don't cover this, so here we will have to provide some details.

Suppose K is a finite extension of a field k, say, of degree n. Consider K as a vector space over k. For $\alpha \in K$, the mapping $ad_\alpha : K \to K$ defined by $ad_\alpha : \beta \mapsto \alpha\beta$ is called the *adjoint* action of α. This is a k-linear mapping and it is invertible whenever $\alpha \neq 0$. The *norm* of α with respect to this extension is defined by $\mathrm{norm}_{K/k}(\alpha) := \det \mathrm{ad}_\alpha$. Similarly, the trace of α with respect to the extension K/k is $\mathrm{Tr}_{K/k}(\alpha) = \mathrm{Tr}\,\mathrm{ad}_\alpha$, the trace of the adjoint action. Note that the determinant and trace of a linear mapping are independent of the choice of the basis, so any basis can be used for the computation.

We first record some immediate properties of the norm and trace.

Proposition 1.4.1 *Let $\alpha, \beta \in K$ and $a \in k$. As above, $n = [K : k]$. Then the following hold:*

(1) $\mathrm{norm}_{K/k}(\alpha\beta) = \mathrm{norm}_{K/k}(\alpha)\mathrm{norm}_{K/k}(\beta)$, *that is, norm is multiplicative; also,* $\mathrm{norm}_{K/k}(a\alpha) = a^n\mathrm{norm}_{K/k}(\alpha)$;

(2) $\mathrm{Tr}_{K/k}(\alpha + \beta) = \mathrm{Tr}_{K/k}(\alpha) + \mathrm{Tr}_{K/k}(\beta)$ *and* $\mathrm{Tr}_{K/k}(a\alpha) = a\mathrm{Tr}_{K/k}(\alpha)$, *that is, trace is a k-linear mapping from K to k.*

Proof: This follows from the properties of the determinant and trace of an $n \times n$ matrix. □

Our next goal is to find a practical way to compute the norm and the trace. We first reduce the computation to the case where $K = k(\alpha)$.

Proposition 1.4.2 *Let $L = k(\alpha)$ and $m = [K : L]$. Then* $\mathrm{norm}_{K/k}(\alpha) = \mathrm{norm}_{L/k}(\alpha)^m$ *and* $\mathrm{Tr}_{K/k}(\alpha) = m\mathrm{Tr}_{L/k}(\alpha)$.

Proof: Note that L is a subspace of the k-vector space K and that L is invariant under ad_α, since $\alpha \in L$. Pick a basis $\mathcal{B}$ in L and let the matrix A represents the action of ad_α on L with respect to the basis $\mathcal{B}$.

If $0 \neq \beta \in K$ then the action of β on K commutes with the action of α, since K is commutative. This means that $L' = \beta L$ is also an ad_α-invariant subspace of the same dimension as L and, furthermore, if we take $\mathcal{B}' = \beta\mathcal{B}$

as basis in L' then the action of ad_α on L' is represented with respect to $\mathcal{B}'$ by the same matrix A.

Let $\beta_1 = 1, \beta_2, \ldots, \beta_m$ be a basis for K as a vector space over L. Then $L_1 = L, L_2 = \beta_2 L, \ldots, L_m = \beta_m L$ decompose K as a k-vector space, that is, $K = L_1 \oplus L_2 \oplus \ldots \oplus L_m$. Moreover, if we take as our basis in K the union of $\mathcal{B}_i = \beta_i \mathcal{B}$ then the action of ad_α is represented by the block-diagonal matrix with m identical blocks equal to A. This immediately yields the claim. □

Because of this proposition, to calculate the norm and trace we can first consider the case where $K = L = k(\alpha)$. Let $f = x^s + a_{s-1}x^{s-1} + \ldots + a_1 x + a_0 \in k[x]$ be the minimal polynomial of α. We know from Galois Theory that $s = [K : k]$ and, moreover, $\mathcal{B} = \{1, \alpha, \alpha^2, \ldots, \alpha^{s-1}\}$ is a basis in K. When we write the action of ad_α with respect to this action, we will get the following matrix M:

$$\begin{pmatrix} 0 & 0 & 0 & \cdots & 0 & -a_0 \\ 1 & 0 & 0 & \cdots & 0 & -a_1 \\ 0 & 1 & 0 & \cdots & 0 & -a_2 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 0 & -a_{s-2} \\ 0 & 0 & 0 & \cdots & 1 & -a_{s-1} \end{pmatrix}.$$

Manifestly, $\mathrm{Tr}_{K/k}(\alpha) = \mathrm{Tr}\, M = -a_{s-1}$ and $\mathrm{norm}_{K,k}(\alpha) = \det M = (-1)^s a_0$. Next, recall that these same numbers, $-a_{s-1}$ and $(-1)^s a_0$, coincide with the sum and product of all roots of f, as a found in a suitable (splitting for f) extension of K. (Say, in $\bar{\mathbb{Q}}$!)

We could arrive at the same conclusion from a different angle. Namely, f coincides with the characteristic polynomial of ad_α, the roots of the characteristic polynomial are the eigenvalues of ad_α on K and the trace and determinant are equal to the sum and product of the eigenvalues, respectively. Anyway, if $\alpha_1 = \alpha, \alpha_2, \ldots, \alpha_s$ are the roots of f then $\mathrm{Tr}_{K/k}(\alpha) = \sum_{i=1}^s \alpha_i$ and $\mathrm{norm}_{K/k}(\alpha) = \prod_{i=1}^s \alpha_i$.

In this course we are dealing exclusively with number fields, which have characteristic zero. In characteristic zero all polynomials are separable, which means that the roots α_i of f are pairwise distinct.

We will now transform the above formulas into statements that can be generalized to the arbitrary case (where $K \neq L = k(\alpha)$). We will need the following fact, which is a particular case (for number fields only) of a more general result from Galois Theory.

Proposition 1.4.3 *Let K/k be an extension of number fields. Every injective homomorphism of k into $\bar{\mathbb{Q}}$ extends to exactly $n = [K : k]$ different (injective) homomorphisms of K into $\bar{\mathbb{Q}}$.* □

Now continuing the discussion of the case $K = L = k(\alpha)$, let $\Sigma = \{\sigma_1 = \mathrm{id}_K, \sigma_2, \ldots, \sigma_s\}$ be the full set of homomorphisms $\sigma : K \to \bar{\mathbb{Q}}$ such that $\sigma|_k = \mathrm{id}_k$. Every such σ is uniquely identified by α^σ (we will use the exponential notation for σ's), which must coincide with one of the roots α_i, because α and α^σ have the same minimal polynomial. Without loss of generality we can assume that the order of σ_i's and α_i's match, that is, $\alpha^{\sigma_i} = \alpha_i$. (This agrees with our choice above that $\alpha_1 = \alpha$ and $\sigma_1 = \mathrm{id}_K$.) Now we can rewrite our formulas for trace and norm as follows:

$$\mathrm{Tr}_{K/k}(\alpha) = \sum_{\sigma \in \Sigma} \alpha^\sigma$$

and

$$\mathrm{norm}_{K/k}(\alpha) = \prod_{\sigma \in \Sigma} \alpha^s g.$$

So far we only have this in the case where $K = L = k(\alpha)$. However, the same statements remain true for arbitrary extensions K/k, as the following theorem shows.

Theorem 1.4.4 *Let K/k be an extension of number fields and let Σ be the full set of homomorphisms $\sigma : K \to \bar{\mathbb{Q}}$ such that $\sigma|_k = \mathrm{id}_k$. Then, for every $\alpha \in K$, we have $\mathrm{Tr}_{K/k}(\alpha) = \sum_{\sigma \in \Sigma} \alpha^\sigma$ and $\mathrm{norm}_{K/k}(\alpha) = \prod_{\sigma \in \Sigma} \alpha^\sigma$.*

Proof: The set Σ consists of $n = [K : k]$ homomorphisms. Let $L = k(\alpha)$, $s = [K : k]$ and $m = [K : L]$ (so that $n = sm$). By Proposition 1.4.3 there exists exactly s homomorphsims $\tau_i : L \to \bar{\mathbb{Q}}$ with $\tau_i|_k = \mathrm{id}_k$. Each τ_i sends α to a different root α_i of f, the minimal polynomial of α. By the same Proposition 1.4.3, each τ_i has exactly m elements of Σ, and so this accounts for all $\sigma \in \Sigma$. Each extension of τ_i sends α to the same α_i, hence each root α_i appears as summand in $T = \sum_{\sigma \in \Sigma} \alpha^\sigma$ exactly m times. This means that $T = m \sum_{i=1}^s \alpha_i = m\mathrm{Tr}_{L/k}(\alpha)$. In view of Proposition 1.4.2, the latter equals $\mathrm{Tr}_{K/k}(\alpha)$, as claimed. Similarly, $\prod_{\sigma \in \Sigma} \alpha^\sigma = (\prod_{i=1}^s \alpha_i)^m = \mathrm{norm}_{L/k}(\alpha)^m = \mathrm{norm}_{K/k}(\alpha)$. □

The last result in this section is useful when K is constructed as a sequence of (simple) extensions.

Proposition 1.4.5 *Suppose $k \subseteq L \subseteq K$ is a tower of extensions. Then, for each $\alpha \in K$ we have*

$$\mathrm{Tr}_{K/k}(\alpha) = \mathrm{Tr}_{L/k}(\mathrm{Tr}_{K/L}(\alpha))$$

and, similarly,

$$\mathrm{norm}_{K/k}(\alpha) = \mathrm{norm}_{L/k}(\mathrm{norm}_{K/L}(\alpha)).$$

Proof: Let $s = [L : k]$, $m = [K : L]$, and $n = sm = [K : k]$. Let $T = \{\tau_1 = \mathrm{id}_L, \tau_2, \ldots, \tau_s\}$ be the complete set of all homomorphisms of $\tau : L \to \bar{\mathbb{Q}}$ such that $\tau|_k = \mathrm{id}_k$. Similarly, let Σ be the set of all $\sigma : K \to \bar{\mathbb{Q}}$ such that $\sigma|_k = \mathrm{id}_k$. Also, for each i, let Σ_i be the set of all homomorphisms $\sigma : K \to \bar{\mathbb{Q}}$ such that $\sigma|_L = \tau_i$. Then by Proposition 1.4.3, each Σ_i consists of exactly m elements and the sets Σ_i partition Σ. For notational convenience let us extend each τ_i to the entire $\bar{\mathbb{Q}}$ (in any possible way). We will use the same notation τ_i for the resulting automorphism of $\bar{\mathbb{Q}}$.

Now notice that $\Sigma_i = \Sigma_1 \tau_i$. Therefore, we have

$$\mathrm{Tr}_{K/k}(\alpha) = \sum_{\sigma \in \Sigma} \alpha^\sigma = \sum_{i=1}^{s} (\sum_{\sigma \in \Sigma_i} \alpha^\sigma) = \sum_{i=1}^{s} (\sum_{\sigma \in \Sigma_1} \alpha^{\sigma \tau_i}) =$$

$$= \sum_{i=1}^{s} (\sum_{\sigma \in \Sigma_1} \alpha^\sigma)^{\tau_i} = \sum_{i=1}^{s} (\mathrm{Tr}_{K/L}(\alpha))^{\tau_i} = \mathrm{Tr}_{L/k}(\mathrm{Tr}_{K/L}(\alpha)).$$

The argument for the norm is quite similar. □

1.5 Lattices

A *lattice* in a finite-dimensional vector space V over $\mathbb{Q}$ (or $\mathbb{R}$, or $\mathbb{C}$) is a subgroup $\Lambda \leq V$ that is generated by a basis in V. In this section we establish that the ring $\mathfrak{o}_k$ (and all its nonzero ideals) are lattices in the number field k, which we view as a vector space over $\mathbb{Q}$.

We first need a criterion for a subgroup of V to be a lattice.

Proposition 1.5.1 *Suppose V is an n-dimensional vector space over $\mathbb{Q}$ and suppose Λ is a subgroup of V. Then Λ is a lattice if and only if the following three conditions are satisfied:*

(1) *Λ spans V;*

(2) *$\Lambda \cong \mathbb{Z}^n$; and*

(3) *Λ is discrete in V.*

Furthermore, any two of these conditions imply the third.

Proof: If Λ is a lattice then it is generated by a basis $\mathcal{B}$ of V. In particular, Λ spans V, and so (1) holds. Also, the vectors from $\mathcal{B}$ are linearly independent, hence they form a base in Λ, yielding (2). Conversely, suppose (1) and (2) are satisfied. Take a base in Λ. The base generates Λ and by (1) it also

spans V. Since by (2) the number of vectors in the base coincides with the dimension of V, they must be linearly independent in V and so they form a basis in V, that is, Λ is generated by a basis, hence it is a lattice.

We next show that (1) and (2) together imply (3). It suffices to see that the zero has an open neighbourhood U such that $\Lambda \cap U = \{0\}$. Indeed, if such a neighbourhood U exists then, for every $v \in \Lambda$, $U_v = v + U$ is an open neighbourhood of v, such that $U_v \cap \Lambda = \{v\}$, and so Λ is discrete. Consider again a base $\mathcal{B} = \{v_1, \ldots, v_n\}$ in Λ. By (1), $\mathcal{B}$ spans V, since it generates Λ. Also, by (2), $\mathcal{B}$ consists of exactly $n = \dim V$ vectors, and so it is a basis in V. Hence every vector $v \in V$ can be uniquely written as $v = a_1v_1 + \ldots + a_nv_n$ for some coordinates $a_1, \ldots, a_n \in \mathbb{Q}$ (or $\mathbb{R}$). Note that the elements of Λ have integral coordinates. This means that the open cube $U = \{v = a_1v_1 + \ldots + a_nv_n \mid -1 < a_i < 1 \text{ for all } i\}$ contains only one element of Λ, the zero. So (3) holds.

Assume now that (1) and (3) hold. Since Λ spans V, it contains a basis $\mathcal{B} = \{v_1, \ldots, v_n\}$ of V. Let Λ_0 be the subgroup of Λ generated by $\mathcal{B}$. Then clearly Λ_0 is a lattice in V and, in particular, $\Lambda_0 \cong \mathbb{Z}^n$. We claim that Λ_0 has finite index in Λ, that is, Λ/Λ_0 is finite. Using coordinates with respect to $\mathcal{B}$, introduce a distance function on V via the usual formula. Since Λ is discrete, $d_0 = \inf\{d(u, v) \mid u, v \in \Lambda, u \neq v\} > 0$. Pick $r = \frac{d_0}{2}$. Then for any $u, v \in \Lambda$, $u \neq v$, we have that the open balls $B_r(u)$ and $B_r(v)$ are disjoint. Now notice that in every coset of Λ_0 in Λ we can pick a representative $v = a_1v_1 + \ldots + a_nv_n$, where $0 \leq a_i < 1$. Thus the number of cosets of Λ_0 in Λ does not exceed the number of elements of Λ in the above unit n-dimensional cube. Clearly, this number can be estimated from above by the volume of the cube divided by the volume of the ball $B_r(v)$. Hence the number of cosets is finite, say m.

Consider the homomorphism $\phi : \Lambda \to \Lambda$ defined via $v \mapsto mv$. Then, as the ground field has characteristic zero, Λ has no torsion and hence ϕ is injective. Also, the image of ϕ is contained in Λ_0. Therefore, Λ is isomorphic to a subgroup of Λ_0. This means that Λ is finitely generated. Now Proposition 1.1.8 gives us that Λ has rank n. Since it has no torsion, we conclude that $\Lambda \cong \mathbb{Z}^n$, and so (2) holds.

Finally, suppose (2) and (3) hold. Let V_0 be the subspace of V spanned by Λ. Now, with respect to V_0, Λ satisfies (1) and (3) and hence Λ is a lattice in V_0. Since $\Lambda \cong \mathbb{Z}^n$, we conclude that V_0 has dimension n, that is, $V_0 = V$.□

We now turn to the case where $V = k$, a number field, and $\Lambda = \mathfrak{o}_k$.

Proposition 1.5.2 *Let k be a number field. Then $\mathfrak{o}_k$ is a lattice in k viewed as a vector space over $\mathbb{Q}$.*

Proof: Clearly $\Lambda = \mathfrak{o}_k$ is a subgroup in $V = k$. We will apply the criteria from

Proposition 1.5.1. By Proposition 1.3.6, every element of k can be written as $\frac{1}{m}\alpha$, where $\alpha \in \mathfrak{o}_k$ and $m \in \mathbb{Z}$, $m \neq 0$. In particular, $\mathfrak{o}_k$ spans k, that is, (1) holds. Next, since the norm, $\mathrm{norm}_{k/\mathbb{Q}}$, is given by a homogeneous polynomial in terms of the coordinates (for an arbitrary basis of k), it is a continuous function, and so there exists an open neighbourhood U of zero, such that for all $\alpha \in U$ we have $|\mathrm{norm}_{k/\mathbb{Q}}(\alpha)| = |\mathrm{norm}_{k/\mathbb{Q}}(\alpha) - \mathrm{norm}_{k/\mathbb{Q}}(0)| < 1$. If $\alpha \in \mathfrak{o}_k$ then $\mathrm{norm}_{k/\mathbb{Q}}(\alpha) \in \mathbb{Z}$. Since 0 is the only element of k with norm zero, $U \cap \mathfrak{o}_k = \{0\}$, which means that $\mathfrak{o}_k$ is discrete, and (3) holds. By Proposition 1.5.1, $\mathfrak{o}_k$ is a lattice. □

In fact, more can be said.

Proposition 1.5.3 *Let k be a number field. Then every nonzero ideal in $\mathfrak{o}_k$ is a lattice in k.*

Proof: Let $\mathfrak{a} \neq 0$ be an ideal in $\mathfrak{o}_k$. Then $\mathfrak{a}$ is a subgroup of $\mathfrak{o}_k$ and hence also a subgroup of k. Pick $0 \neq \alpha \in \mathfrak{a}$ and consider the mapping $\phi : \mathfrak{o}_k \to \mathfrak{o}_k$ defined by $\beta \mapsto \alpha\beta$. Then this mapping is $\mathfrak{o}_k$-linear, in particular, it is a group homomorphism. Furthermore, since $\mathfrak{o}_k$ is a domain, it has no zero divisors, which means that $\ker \phi = 0$. Also, since $\mathfrak{a}$ is an ideal and since $\alpha \in \mathfrak{a}$, we have that $\mathrm{im}\, \phi \subseteq \mathfrak{a}$. This means that $\mathfrak{a}$ contains a subgroup isomorphic to $\mathfrak{o}_k \cong \mathbb{Z}^n$, where $n = [k : \mathbb{Q}]$. It follows that the rank of $\mathfrak{a}$ is at least n, and hence exactly n. Thus, $\mathfrak{a} \cong \mathbb{Z}^n$. Also, $\mathfrak{a}$ is discrete in k, since $\mathfrak{a}$ is contained in the lattice $\mathfrak{o}_k$. So (2) and (3) of Proposition 1.5.1 are satisfied for $\mathfrak{a}$, which means that $\mathfrak{a}$ is a lattice. □

We also have the following interesting corollary.

Corollary 1.5.4 *Every nonzero ideal $\mathfrak{a}$ in $\mathfrak{o}_k$ has finite index, that is, $\mathfrak{o}_k/\mathfrak{a}$ is a finite ring.*

Proof: Indeed, $\mathfrak{a}$ has the same rank as $\mathfrak{o}_k$, and so the claim follows from Proposition 1.1.8. □

1.6 Absolute discriminant

The absolute discriminant is a convenient measure of how dense the lattice $\mathfrak{o}_k$ is within the number field k. To define it, we first need the *symmetric embedding* of k into $\mathbb{C}^n$. This is obtained as follows. Let Σ be again (as in the section about norms and traces) the full set of injective homomorphisms of k into $\bar{\mathbb{Q}} \subset \mathbb{C}$. Then $\Sigma = \{\sigma_1, \ldots, \sigma_n\}$, where $n = [k : \mathbb{Q}]$. Define $\tau : k \to \mathbb{C}^n$ as follows:

$$\tau(\alpha) = (\alpha^{\sigma_1}, \alpha^{\sigma_2}, \ldots, \alpha^{\sigma_n}).$$

Since every homomorphism $\sigma \in \Sigma$ acts as identity on $\mathbb{Q}$, it is $\mathbb{Q}$-linear, which implies that τ is also $\mathbb{Q}$-linear. This mapping is symmetric in the sense that every automorphism of $\mathbb{C}$ (or $\bar{\mathbb{Q}}$) permutes the σ_i and thus leads to a simple permutation of coordinates, which does not influence the length function, if the latter is defined so that the standard basis of $\mathbb{C}^n$ is orthonormal.

We also note that the linear mapping τ is, clearly, injective, and this is why we refer to it as an embedding. Next, we show that τ takes bases to bases.

Proposition 1.6.1 *If $\mathcal{B}$ is a basis of k as a $\mathbb{Q}$-vector space then $\tau(\mathcal{B})$ is a basis of $\mathbb{C}^n$.*

Proof: We will use the statement from Galois Theory known as the Primitive Element Theorem. It claims that every finite field extension is simple. In our case this means that $k = \mathbb{Q}(\alpha)$ for some $\alpha \in k$. Recall also that in a simple extension $\mathbb{Q}(\alpha)$ of degree n, one can take as $\mathbb{Q}$-basis the powers of α: $\mathcal{B} = \{1, \alpha, \alpha^2, \ldots, \alpha^{n-1}\}$.

Let $\alpha_i = \alpha^{\sigma_i}$ for $i = 1, 2, \ldots, n$. Note that if $\alpha_i = \alpha_j$ then $\alpha^{\sigma_i} = \alpha^{\sigma_j}$. Since $k = \mathbb{Q}(\alpha)$, we conclude that $\sigma_i = \sigma_j$, that is, $i = j$. This means that the α_i are pairwise distinct.

We now turn to the main claim of the proposition. It suffices to show that the image in $\mathbb{C}^n$ of one basis of k is linear independent, hence a basis. Naturally, we will do so for the basis $\mathcal{B}$ chosen above. To check the linear independence, we need to show that the matrix formed by the rows $\tau(\alpha^j) = ((\alpha^j)^{\sigma_1}, (\alpha^j)^{\sigma_2}, \ldots, (\alpha^j)^{\sigma_n})$, where $j = 0, 1, \ldots, n-1$, has non-zero determinant. We note that $(\alpha^j)^{\sigma_i} = (\alpha^{\sigma_i})^j = \alpha_i^j$. Therefore, the resulting matrix is as follows:

$$\begin{pmatrix} 1 & 1 & 1 & \cdots & 1 \\ \alpha_1 & \alpha_2 & \alpha^2 & \cdots & \alpha_n \\ \alpha_1^2 & \alpha_2^2 & \alpha_3^2 & \cdots & \alpha_n^2 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ \alpha_1^{n-1} & \alpha_2^{n-1} & \alpha_3^{n-1} & \cdots & \alpha_n^{n-1} \end{pmatrix}$$

This is a Vandermonde matrix and its determinant, equal to

$$\prod_{1 \le i < j \le n} (\alpha_j - \alpha_i),$$

is non-zero, because the α_i are pairwise distinct.

We showed that the image of $\mathcal{B}$ under τ is linearly independent. Since both k and $\mathbb{C}^n$ have dimension n (over $\mathbb{Q}$ and $\mathbb{C}$, respectively) we conclude that $\tau(\mathcal{B})$ is a basis of $\mathbb{C}^n$. Hence the same is also true for any basis of k. $\square$

This proposition means that $V = k^\tau \otimes_{\mathbb{Q}} \mathbb{R} \subseteq \mathbb{C}^n$ is an n-dimensional real vector space endowed with a positive definite inner product inherited from $\mathbb{C}^n$. This inner product allows us to define in V in the usual way lengths, areas, volumes. Skipping some computations, we will just claim that the volume of the n-dimensional parallelepiped, having some vectors $\alpha_1, \alpha_2, \ldots, \alpha_n$ as the edges adjacent to the vertex 0, is given by the absolute value of the determinant of the $n \times n$ matrix M formed by these vectors. In particular, if we take $\alpha_1, \alpha_2, \ldots, \alpha_n$ to be a base of $\mathfrak{o}_k$ then it correspond to a basis $\tau(\alpha_1), \tau(\alpha_2), \ldots, \tau(\alpha_n)$ of V and so the corresponding parallelepiped P is the fundamental domain for the action of $\tau(\mathfrak{o}_k)$ on V by shifts, and hence it is equal to the volume of the quotient $V/\tau(\mathfrak{o}_k)$.

We note that $\det M$ is in general a complex number. It can be shown that $\det M = |\det M| i^{r_2}$, where r_2 is the number of complex conjugate pairs of non-real embeddings σ_i. We call $(\det M)^2$ the *absolute discriminant* of the field k and denote it by d_k. From what was said above it follows that d_k is a real number and its sign depends on the parity of r_2.

We conclude this section with two results showing that d_k is indeed an invariant of the field k and that d_k is integer.

Proposition 1.6.2 *The value of d_k does not depend on the choice of the base $\alpha_1, \alpha_2, \ldots, \alpha_n$ of $\mathfrak{o}_k$.*

Proof: If $\alpha'_1, \alpha'_2, \ldots, \alpha'_m$ is another base in $\mathfrak{o}_k$ and M' is the corresponding matrix then $M' = MA$ where A is the change-of-basis matrix. In particular, A is an invertible matrix with integral entries. This means that $\det A = \pm 1$. Hence $\det M' = \pm \det M$ and hence $(\det M')^2 = (\det M)^2$. □

Proposition 1.6.3 *Let, as above, $\alpha_1, \alpha_2, \ldots, \alpha_n$ be a base of $\mathfrak{o}_k$ and let M be the matrix made out of the vectors $\tau(\alpha_i)$. Then $d_k = \det MM^t$ and MM^t is a symmetric integral matrix with ij-entry equal to $\mathrm{Tr}(\alpha_i\alpha_j)$.*

Proof: Clearly, $d_k = (\det M)^2 = \det M \det M^t = \det MM^t$. Also, the ij-entry in MM^t is equal to $\tau(\alpha_i)\tau(\alpha_j)^t = \alpha_i^{\sigma_1}\alpha_j^(\sigma_1) + \alpha_i^{\sigma_2}\alpha_j^{\sigma_2} + \ldots + \alpha_i^{\sigma_n}\alpha_j^{\sigma_n} = (\alpha_i\alpha_j)^{\sigma_1} + (\alpha_i\alpha_j)^{\sigma_2} + \ldots + (\alpha_i\alpha_j)^{\sigma_n} = \mathrm{Tr}(\alpha_i\alpha_j)$, as claimed. Clearly, the ij-entry and the ji-entry are equal, hence the matrix is symmetric. Since both α_i and α_j are algebraic integers, $\mathrm{Tr}(\alpha_i\alpha_j)$ is an integer. □

Note that this lemma provides a convenient way of computing d_k for concrete fields k.

1.7 Noetherian rings and modules

In this short section we provide the necessary information about Noetherian rings. We will just deal with the commutative case. Suppose R is a commutative ring and M is an R-module. We say that the module M is Noetherian if it satisfies the *ascending chain condition*, namely, every chain of submodule $M_1 \subseteq M_2 \subseteq \ldots \subseteq M_i \subseteq \ldots$ stabilizes. That is, there exists $n \geq 1$ such that for every $i \geq n$ we have $M_i = M_n$.

The following is immediate from the definitions and is left as an exercise.

Proposition 1.7.1 *If M is an R-module and $U \subseteq M$ is a submodule then M is Noetherian if and only if U and M/U are Noetherian.* □

In particular, submodules and factor modules of Noetherian modules are Noetherian. The next result gives two conditions equivalent to M being Noetherian.

Proposition 1.7.2 *Suppose M is an R-module. Then the following are equivalent:*

(1) *M is Noetherian;*

(2) *every submodule in M is finitely generated; and*

(3) *every nonempty collection of submodules in M has a maximal element.*

Proof: We first show that (2) implies (1). Suppose $M_1 \subseteq M_2 \subseteq \ldots \subseteq M_i \subseteq \ldots$ is an ascending chain of submodules in M. Let $U = \cup_{i=1}^{\infty} M_i$. Note that U is a submodule. Indeed, if $u, v \in U$ then $u \in M_i$ and $v \in M_j$ for some i and j. Hence $u, v \in M_k$, where $k = \max\{i, j\}$. We know have that $u - v \in M_k \subseteq U$ and also $au \in M_k \subseteq U$ for all $a \in R$. So indeed U is a submodule. By (2), U must be finite-dimensional, that is, $U = \langle u_1, \ldots, u_s \rangle_R$ for some $u_1, \ldots, u_s \in U$. Let, say, $u_i \in M_{j_i}$ for each i. Set $n = \max\{j_1, \ldots, j_s\}$. Since the chain is ascending, $u_i \in M_n$ for all i. However, this means that $M_n = U$ and so the chain stabilizes.

Next assume (3). We shall show (2), that is, that every submodule U of M is finitely generated. Consider the collection of all finitely generated submodules of U. Clearly, this collection is nonempty. Let W be a maximal element in this collection. we claim that $W = U$. Indeed, suppose not. Then pick $u \in U \setminus W$ and set $W' = \langle W, u \rangle_R$. Since W is finitely generated and W' needs just one extra generator, W' is also finitely generated. However, $W' \subseteq U$ and also $W' \supset W$, which contradicts maximality of W. This shows that (3) implies (2).

Finally, we need to show that (1) implies (3). Assume M is Noetherian and at the same time, by contradiction, M contains a nonempty collection $\mathcal{C}$ of submodules with no maximal element. Let M_1 be any submodule from $\mathcal{C}$. Since $\mathcal{C}$ has no maximal elements, there is a submodule $M_2 \in \mathcal{C}$ that properly contains M_1. Similarly, there is $M_3 \in \mathcal{C}$ that properly contains M_2, and so on. This gives us an ascending chain of submodules that never stabilizes; a contradiction. □

A ring R is called Noetherian if it is Noetherian as a module over itself. Since the submodules for this module are the same as ideals of R, the condition can be restated as follows: every ascending chain of ideals in R must stabilize. The following is an immediate consequence of Proposition 1.7.1.

Proposition 1.7.3 *Suppose R is a (commutative) ring and I is an ideal of R. Then R is Noetherian if and only if I is Noetherian as an R-module and R/I is a Noetherian ring.* □

Similarly, as a consequence of Proposition 1.7.2, we get the following.

Proposition 1.7.4 *Suppose R is a (commutative) ring. Then the following are equivalent:*

(1) *R is Noetherian;*

(2) *every ideal in R is finitely generated; and*

(3) *every nonempty collection of ideals in R has a maximal element.* □

1.8 Dedekind rings

Recall that an ideal I in a commutative ring R is called *prime* if and only for all $a, b \in R$ if $ab \in I$ then either $a \in I$ or $b \in I$. Equivalently, I is prime if and only if R/I has no zero divisors. Every maximal ideal is prime, but in general there may be prime ideals that are not maximal.

A domain D (recall that a domain is a commutative ring with identity and with no zero divisors) with the field of fractions k is called a *Dedekind domain* if the following three conditions are satisfied:

(1) D is Noetherian;

(2) D is integrally closed in k; and

(3) every nonzero prime ideal in D is maximal; that is, if $I \neq 0$ is a prime ideal in D then D/I is a field.

The purpose of this short section is to prove the following key result.

Theorem 1.8.1 *If k is a number field then $\mathfrak{o}_k$ is Dedekind.*

Proof: Note first of all that $\mathfrak{o}_k$ is a domain and k is its field of fractions. We need to check the conditions (1)–(3). Condition (2) was proved in Proposition 1.3.7. We proved in Proposition 1.5.3 that every nonzero ideal $\mathfrak{o}_k$ is a lattice in k, in particular, as a group, it is isomorphic to $\mathbb{Z}^n$, where $n = [k : \mathbb{Q}]$. In particular, every ideal is finitely generated (even as a group!) this means that $\mathfrak{o}_k$ is Noetherian, and so (1) holds.

To prove (3), consider a prime ideal $\mathfrak{p} \neq 0$ in $\mathfrak{o}_k$. Clearly, $\mathfrak{o}_k/\mathfrak{p}$ is a domain. Furthermore, by Corollary 1.5.4, it is a finite domain. So we just need to see that every finite domain is a field. Apparently, this was in the "Rings and Polynomials" course, we will however provide the details.

Let D be a finite domain. We need to show that if $a \in D$ and $a \neq 0$ then a has a multiplicative inverse. Consider the mapping $\phi : D \to D$ given by $d \mapsto ad$. We claim that ϕ is injective. Indeed, if $ax = ay$ then $a(x - y) = 0$ and so $x - y = 0$, since D has no zero divisors and $a \neq 0$. Thus, $x = y$ and so ϕ is indeed injective. Next, every injective mapping between sets of equal size must be a bijection. In particular, ϕ is onto. This means that $1 = \phi(b) = ab$ for some $b \in D$. Clearly, this b is the multiplicative inverse of a. Thus D is a field. □

1.9 Fractional ideals

In this section we define fractional ideals for Dedekind domains and prove that the nonzero fractional ideals form a group for a suitably defined multiplication.

Let D be a Dedekind domain and k be its field of fractions. We can view k as a D-module. A *fractional ideal* in k is simply any finitely generated D-submodule in k. Note that since D is Noetherian, every ideal in D is finitely generated and so every ideal of D is a fractional ideal. We will also call the ideal of D the *integral ideals*. In the particular case, where a fractional ideal is generated by a single element, we call such a fractional ideal *principal*. This fits with the usual definition of the principal ideals of D.

Note that a fractional ideal F is generated by $\alpha_1, \ldots, \alpha_s \in k$ if and only if $F = \{a_1\alpha_1 + \ldots + a_s\alpha_s \mid a_1, \ldots, a_s \in D\}$. We can also write $F = \alpha_1 D + \ldots + \alpha_s D$ and even $F = (\alpha_1, \ldots, \alpha_s)$, extending the usual notation for ideals. If F is a principal fractional ideal generated by $\alpha \in k$ then $F = \{a\alpha \mid a \in D\} = \alpha D$ and we write $F = (\alpha)$.

We first prove the following characterization of fractional ideals.

Proposition 1.9.1 *A subset $F \subseteq k$ is a fractional ideal if and only if $F = cI$ for some $c \in k$ and some ideal I of D.*

Proof: It is easy to see that if I is an ideal of D generated by $\alpha_1, \ldots, \alpha_s \in D$ and if $c \in k$ then $F = cI$ is a D-submodule in k and F is generated by $c\alpha_1, \ldots, c\alpha_s$. So F is a fractional ideal.

Conversely, suppose F is a fractional ideal. Then it must be finitely generated as a D-module. Say, it is generated by $\alpha_1, \ldots, \alpha_s \in k$. Since k is the field of fractions of D, we can write each α_i as $\alpha_i = \frac{p_i}{q_i}$, where $p_i, q_i \in D$ and $q_i \neq 0$. Set $d = \prod_{i=1}^{s} q_i$ and $I = Fd$. Note that $d\alpha_i = p_i \prod_{j \neq i} q_j \in D$ for all i. Since I is generated by the elements $d\alpha_i$, we have $I \subseteq D$. Also, I is a D-submodule, hence an ideal of D. It remains to notice that $F = cI$, where $c = d^{-1}$. Note that $d \neq 0$, since $q_i \neq 0$ for all i. □

We next discuss the multiplication of fractional ideals. It is again the natural generalization of the operation that is well-known for the usual integral ideals. Suppose F_1 and F_2 are fractional ideals. We set F_1F_2 to be the set $\{u_1v_1 + \ldots + u_mv_m \mid u_1, \ldots, u_m \in F_1, v_1, \ldots, v_m \in F_2\}$. This is again a fractional ideal, as the following result shows. This is left as an exercise.

Proposition 1.9.2 *If $F = (\alpha_1, \ldots, \alpha_s)$ and $F_2 = (\beta_1, \ldots, \beta_t)$ then $F_1F_2 = (\alpha_1\beta_1, \alpha_1\beta_2, \ldots, \alpha_i\beta_j, \ldots, \alpha_s\beta_t)$.* □

In particular, if $F_1 = (\alpha)$ and $F_2 = (\beta)$ are both principal fractional ideals then $F_1F_2 = (\alpha\beta)$ is also principal.

Clearly, the above multiplication is commutative. Proposition 1.9.2 also yields the following.

Corollary 1.9.3 *The multiplication of fractional ideals is associative.*

Proof: If $F_1 = (\alpha_1, \ldots, \alpha_s)$, $F_2 = (\beta_1, \ldots, \beta_t)$, and $F_3 = (\gamma_1, \ldots, \gamma_m)$ then both $(F_1F_2)F_3$ and $F_1(F_2F_3)$ are generated by all products $\alpha_i\beta_j\gamma_l$. So these products are equal. □

If F_1 and F_2 are both nonzero then, clearly, F_1F_2 is also nonzero. Thus, the set of nonzero fractional ideals is closed with respect to the commutative and associative operation of multiplication. Furthermore, the principal ideal $(1) = D$ is the identity element, since $FD = F$ for any fractional ideal F. Indeed, since F is a D-submodule, we have that $FD \subseteq F$ and, since $1 \in D$, we also have $FD \supseteq F$, yielding $FD = F$.

This means that if we show that every fractional ideal is invertible then we will have the following.

Theorem 1.9.4 *All nonzero fractional ideals form a group.*

We will prove this theorem in a sequence of lemmas. The first result exploits condition (2) from the definition of Dedekind rings.

Lemma 1.9.5 *For every nonzero fractional ideal F we have $\{\alpha \in k \mid \alpha F \subseteq F\} = D$.*

Proof: Clearly, $D \subseteq \{\alpha \in k \mid \alpha F \subseteq H\}$. Suppose $\alpha \in k$ and $\alpha F \subseteq F$. We need to see that $\alpha \in D$. Suppose $F = (\beta_1, \ldots, \beta_s)$. Since $\alpha\beta_i \in F$, we can write, for each i,

$$\alpha\beta_i = \sum_{j=1}^{s} b_{ij}\beta_j$$

for some $b_{ij} \in D$. Consider the $s \times s$ matrix $B = (b_{ij})$ and let $A = \alpha I_s - B$ (where I_s is the identity matrix of size $s \times s$). The above equalities mean that the column vector with entries β_j is a (nonzero) eigenvector of A with eigenvalue zero. Hence $\det A = 0$. Hence α is the root of the characteristic polynomial $\det(xI_s - B)$ of the matrix D. This is a monic polynomial from $D[x]$ (since all entries of B are in D). Since D is Dedekind, we have by condition (2) that D is integrally closed in k, which means that $\alpha \in D$. □

The second lemma only relies on the property that D is Noetherian.

Lemma 1.9.6 *Every nonzero ideal of D contains a product of nonzero prime ideals.*

Proof: By contradiction, suppose there exist nonzero ideals not containing products of nonzero prime ideals. Since D is Noetherian, there must exist a maximal such ideal I. Note that I cannot itself be prime, otherwise it contains a one-factor product, itself. Hence there exist $\alpha_1, \alpha_2 \in D \setminus I$ such that $\alpha_1\alpha_2 \in I$. Set $I_1 = (I, \alpha_1)$ and $I_2 = (I, \alpha_2)$. Clearly, I_1 and I_2 strictly larger than I, so each of these ideals contains a product of nonzero prime ideals, say, $\mathfrak{p}_1\mathfrak{p}_2\cdots\mathfrak{p}_s \subseteq I_1$ and $\mathfrak{p}_{s+1}\mathfrak{p}_{s+2}\cdots\mathfrak{p}_{s+t} \subseteq I_2$. Finally, note that $I_1I_2 \subseteq I$ and so $\mathfrak{p}_1\mathfrak{p}_2 \cdot \mathfrak{p}_{s+t} \subseteq I$, a contradiction. □

For a fractional ideal $F \neq 0$, we set $F^- = \{\alpha \in k \mid \alpha F \subseteq D\}$. This F^- is our candidate for the multiplicative inverse of F. First of all, let us see that F^- is a fractional ideal.

Lemma 1.9.7 *F^- is a fractional ideal.*

Proof: By Proposition 1.9.1, $F^- \neq 0$. Indeed, if $F = cI$ for an ideal I of D and $c \in k$ then $c^{-1} \in F^-$. Next, we note that F^- is a D-submodule. Indeed, if $\alpha, \beta \in F^-$ then $(\alpha - \beta)F \subseteq \alpha F + \beta F \subseteq D + D = D$. So $\alpha - \beta \in F^-$. Also, if $a \in D$ then $a\alpha F \subseteq aD \subseteq D$. So indeed F^- is a D-submodule. Moreover,

for every $\alpha \in F$, we have that $\alpha F^- \subseteq D$ (and hence αF is an ideal), which means, according to Proposition 1.9.1, that F^- is a fractional ideal. □

Note that when F is an integral ideal, F^- contains D, since $DF = F \subseteq D$. Our next step is to show that at least in the case, where $F = \mathfrak{p}$ is a prime ideal of D, F^- is strictly larger than D.

Lemma 1.9.8 *If $\mathfrak{p}$ is a nonzero prime ideal of D then $\mathfrak{p}^- \neq D$. In particular, $\mathfrak{p}^-$ strictly contains D.*

Proof: Select an element $\beta \in \mathfrak{p}$, $\beta \neq 0$. By Lemma 1.9.6, the ideal $I = (\beta)$ contains a product $\mathfrak{p}_1 \cdots \mathfrak{p}_s$ of nonzero prime ideals. Without loss of generality, the number of factors, s, is the smallest possible for this I. Note that one of the factors of the product must be $\mathfrak{p}$. Otherwise, every $\mathfrak{p}_i$, being maximal, is not contained in $\mathfrak{p}$, and so we can choose $\alpha_i \in \mathfrak{p}_i \setminus \mathfrak{p}$. This leads to a contradiction, since $\alpha_1 \cdots \alpha_s \in \mathfrak{p}_1 \cdots \mathfrak{p}_s \subseteq I \subseteq \mathfrak{p}$. Thus, indeed, one of the factors $\mathfrak{p}_i$ must be equal to $\mathfrak{p}$, say, $\mathfrak{p}_1 = \mathfrak{p}$.

Now the product $\mathfrak{p}_2 \cdot \mathfrak{p}_s$ (possibly of length zero, in which case it is equal D) is shorter and so it is not contained in I. Pick $\gamma \in \mathfrak{p}_2 \cdot \mathfrak{p}_s \setminus I$ and set $\alpha = \frac{\gamma}{\beta}$. Note that since $\gamma \notin I = (\beta)$ we have that $\alpha \notin D$. Finally, $\alpha\mathfrak{p} = \frac{1}{\beta}\gamma\mathfrak{p} \subseteq \frac{1}{\beta}\mathfrak{p}\mathfrak{p}_2 \cdots \mathfrak{p}_s \subseteq \frac{1}{\beta}I = \frac{1}{\beta}(\beta) = (1) = D$. Thus, $\alpha \in \mathfrak{p}^-$ and so $\mathfrak{p}^-$ is strictly larger than D. □

Corollary 1.9.9 *Suppose $\mathfrak{p}$ is a nonzero prime ideal of D and F is a fractional ideal. Then $F\mathfrak{p}^-$ is strictly larger than F.*

Proof: Since $\mathfrak{p}^- \supset D$, we have $F\mathfrak{p}^- \supseteq F$. If $F\mathfrak{p}^- = F$ then Lemma 1.9.5 implies that $\mathfrak{p}^- \subseteq D$, which contradicts Lemma 1.9.8. Thus $F\mathfrak{p}^- \neq F$. □

We are finally ready to prove the existence of inverses for all nonzero fractional ideals, and thus establish Theorem 1.9.4.

Lemma 1.9.10 *If F is a nonzero fractional ideal then $FF^- = D$. Hence F^- is the multiplicative inverse of F.*

Proof: By definition $FF^- \subseteq D$, that is, $I = FF^-$ is an ideal of D. Suppose by contradiction that $I \neq D$. Then, since D is Noetherian, I is contained in a maximal ideal $\mathfrak{p}$. (Recall that every maximal ideal is prime.) By Lemma 1.9.9, we have that $F^-\mathfrak{p}^-$ is strictly larger than F^-. On the other hand, $F(F^-\mathfrak{p}^-) = (FF^-)\mathfrak{p}^- \subseteq \mathfrak{p}\mathfrak{p}^- \subseteq D$. This means that $F^-\mathfrak{p}^- \subseteq F^-$, which is a contradiction. □

1.10 Unique factorization of ideals

In this section again D is a Dedekind domain with the field of fractions k.

For nonzero fractional ideals F_1 and F_2 in k, we say that F_1 *divides* F_2 (and write $F_1|F_2$) if $F_2F_1^{-1} \subseteq D$ (that is, it is an integral ideal). The following is left as an exercise.

Proposition 1.10.1 *Suppose F_1 and F_2 are nonzero fractional ideals in k. The following are equivalent:*

(1) *F_1 divides F_2;*

(2) *F_2^{-1} divides F_1^{-1};*

(3) *F_1 contains F_2;*

(4) *F_1^{-1} is contained in F_2^{1-}; and*

(5) *$F_1F_2^{-1}$ contains D.* □

The following is the first main result of the section.

Theorem 1.10.2 *Suppose D is a Dedekind domain. Then every nonzero ideal I in D can be written as a product $\mathfrak{p}_1 \cdots \mathfrak{p}_s$ of (nonzero) prime ideals and this expression is unique up to the order of the factors.*

Proof: By contradiction, suppose there exist nonzero ideals that cannot be written as products of prime ideals. Since D is Noetherian, we can pick I to be maximal among all such ideals. Clearly, $I \neq D$. Let $\mathfrak{p}$ be a prime ideal that contains I. By Lemma 1.9.9, $I\mathfrak{p}^{-1}$ is strictly greater than I. Also, by Proposition 1.10.1, since $\mathfrak{p} \supseteq I$, we have that $I\mathfrak{p}^{-1} \subseteq D$, that is, it is an ideal of D. In particular, in view of maximality of I, $I\mathfrak{p}^{-1} = \mathfrak{p}_1 \cdots \mathfrak{p}_s$ for some prime ideals $\mathfrak{p}_i$. However, this means that $I = \mathfrak{p}_1 \cdots \mathfrak{p}_s\mathfrak{p}$, a contradiction. So the first claim is proven.

Suppose $\mathfrak{p}_1 \cdots \mathfrak{p}_s = \mathfrak{q}_1 \cdots \mathfrak{q}_t$, where all factors are nonzero prime. If the product is equal to D then $s = t = 0$ and there is nothing to prove. Otherwise, the product ideal lies in some prime ideal $\mathfrak{p}$. Since $\mathfrak{p}$ is prime, one of the factors $\mathfrak{p}_i$ must be equal to $\mathfrak{p}$. Without loss of generality we may assume that $\mathfrak{p}_1 = \mathfrak{p}$. Similarly, $\mathfrak{p}$ must be equal to one of the $\mathfrak{q}_j$ and so again without loss of generality we may assume that $\mathfrak{q}_1 = \mathfrak{p}$. Cancelling this factor, we get a similar equality with fewer factors, so the uniqueness follows by induction. □

Similarly, our second main result is a unique factorization statement for fractional ideals.

Theorem 1.10.3 *Suppose D is a Dedekind domain with the field of fractions k. Then every nonzero fractional ideal F can be written as $F = \mathfrak{p}_1 \cdots \mathfrak{p}_s / \mathfrak{q}_1 \cdots \mathfrak{q}_t$ (where $\mathfrak{p}_i \neq \mathfrak{q}_j$ for all i and j) and this expression is unique up to the order of the factors in both the numerator and denominator.*

Proof: We leave this as an exercise and just note that $\mathfrak{p}_1 \cdots \mathfrak{p}_s = F \cap D \neq 0$ and $\mathfrak{q}_1 \cdots \mathfrak{q}_t = (F \cap D)F^{-1}$. □

1.11 Ideal norm

In this section we return to number fields. Our goal is to introduce a norm on the ideals (Norm with a capital 'N') that generalizes our norm of the elements. The ideas for this come from the section on absolute discriminant. In particular, recall that k admits a special embedding τ into $V \subset \mathbb{C}^n$, $V \cong \mathbb{R}^n$.

We first make the following observation.

Proposition 1.11.1 *If F is a nonzero fractional ideal of k then F is a lattice in k, and hence $\tau(F)$ is a lattice in V.*

Proof: By the Proposition 1.9.1, $F = cI$ for an ideal I of $\mathfrak{o}_k$ and $c \in k$. By Proposition 1.5.3, I is a lattice in k. Now, the mapping $I \to F$ defined by $\alpha \mapsto c\alpha$ is an isomorphisms of abelian groups, hence $F \cong I \cong \mathbb{Z}^n$. Also, I spans k, and so also F spans k. So F is a lattice in k by Proposition 1.5.1.

Since τ is injective and takes bases of k to bases of V, we see that $\tau(F)$ is generated by a basis of V, hence $\tau(F)$ is a lattice in V. □

To define the norm of the fractional ideal we use the volume measure introduced in the section on absolute discriminant.

We set the ideal norm $\mathrm{Norm}_{k/\mathbb{Q}}(F)$ to be the ratio of the volume of $V/\tau(F)$ (which is well defined and finite exactly because $\tau(F)$ is a lattice in V) and the volume of $V/\tau(\mathfrak{o}_k)$. Thus, the ideal norm measures how dense F is in V compared with $\mathfrak{o}_k$.

Immediately from this definition we have that $\mathrm{Norm}_{k/\mathbb{Q}}(\mathfrak{o}_k) = 1$.

Proposition 1.11.2 *If for two fractional ideals F and F' we have inclusion $F' \subseteq F$ then $\mathrm{Norm}_{k/\mathbb{Q}}(F') = [F : F']\mathrm{Norm}_{k/\mathbb{Q}}(F)$.*

Proof: (This is merely a sketch.) It suffices to show that the volume of $V/\tau(F')$ equals to the volume of $V/tau(F)$ times the index $[F : F']$. If D is a fundamental domain for the action of $\tau(F)$ on V, it can be seen that $D' = \cup_{i=1}^{s}(D + \beta_i)$ is a fundamental domain for the action of $\tau(F')$ on V,

where $s = [F : F']$ and $\beta_1, \beta_2, \ldots, \beta_s$ is a complete set of representatives of $\tau(F')$-cosets in $\tau(F)$.

Note that the pieces $D + \beta_i$ are pairwise disjoint (with the possible exception of some boundary points). Hence the volume of D' equals to s times the volume of D.

Finally, for a lattice F, the volume of the fundamental domain is equal to the volume of $V/\tau(F)$. □

As a corollary we have the following.

Proposition 1.11.3 *Suppose F is a nonzero fractional ideal of k and let $c \in \mathbb{Z}$, $c \neq 0$, be such that $I = cF$ is an ideal of $\mathfrak{o}_k$. Then*

$$\mathrm{Norm}_{k/\mathbb{Q}}(F) = \frac{[\mathfrak{o}_k : I]}{[F : I]}.$$

In particular, if $F = I$ is an (integral) ideal then $\mathrm{Norm}_{k/\mathbb{Q}}(F) = [\mathfrak{o}_k : I]$.

Proof: This follows from Proposition 1.11.2 once we notice that $I \subseteq F$. □

In particular, this means that the norm of every nonzero ideal is a rational number and the norm of an integral ideal is an integer!

We will also record (without proofs) the following two important properties of the ideal norm. The first relates the ideal norm with the norm of elements.

Proposition 1.11.4 *If $F = (\alpha)$ is a principal fractional ideal of k with $\alpha \neq 0$ then* $\mathrm{Norm}_{k/\mathbb{Q}}(F) = |\mathrm{norm}_{k/\mathbb{Q}}(\alpha)|$. □

The second property expresses the multiplicativity of the ideal norm.

Proposition 1.11.5 *For two nonzero fractional ideals F and F' we have that* $\mathrm{Norm}_{k/\mathbb{Q}}(FF') = \mathrm{Norm}_{k/\mathbb{Q}}(F)\mathrm{Norm}_{k/\mathbb{Q}}(F')$. □

This means that the ideal norm is a homomorphism from the group of nonzero fractional ideals to the multiplicative group of positive rational numbers.

1.12 Class group

Let k be the field of fractions of a Dedekind domain D. If α and β are nonzero elements of k then $(\alpha)(\beta) = (\alpha\beta)$. This means that the nonzero principal fractional ideals of k form a subgroup $\mathcal{P}$ of the group $\mathcal{F}$ of all nonzero fractional ideals. Since $\mathcal{F}$ is abelian, every its subgroup is normal

and so we can consider the factor group $\mathcal{F}/\mathcal{P}$. This factor group is known as the *class group* of k. It measures how far is D from being a principal ideal domain (PID).

In general, the class group can be infinite. The goal of the present section is to show that the class group is always finite when k is a number field and $D = \mathfrak{o}_k$. The size of the (finite) class group is known as the *class number* of k. It is usually denoted by $h = h_k$.

We will start with an example of a non-principal ideal to stress that $h > 1$ is possible.

Let $k = \mathbb{Q}(\sqrt{-5})$. Then $D = \mathfrak{o}_k = \mathbb{Z}[\sqrt{-5}]$. We claim that $I = (2, 1 + \sqrt{-5})$ is non-principal. By contradiction suppose that $I = (\alpha)$ for some $\alpha = a + b\sqrt{-5} \in D$. Then α divides both 2 and $1 + \sqrt{-5}$ in D. As a consequence, also the norm of α, equal to $a^2 + 5b^2$, divides $\mathrm{norm}_{k/\mathbb{Q}}(2) = 4$ and $\mathrm{norm}_{k/\mathbb{Q}}(1 + \sqrt{-5}) = 6$. Since $a^2 + 5b^2$ is a positive integer, we conclude that $\mathrm{norm}_{k/\mathbb{Q}}(\alpha) = 1$ or 2. Furthermore, it is easy to see that the equation $a^2 + 5b^2 = 2$ has no solutions with $a, b \in \mathbb{Z}$. Hence $\mathrm{norm}_{k/\mathbb{Q}}(\alpha) = 2$ is impossible. We conclude that $\mathrm{norm}_{k/\mathbb{Q}}(\alpha) = 1$, which means (see next section) that α is a unit. Therefore, $I = (\alpha) = (1) = D$.

To get the final contradiction, consider $3I = 3(2, 1 + \sqrt{-5}) = (6, 3(1 + \sqrt{-5})$. Observe that $1 + \sqrt{-5}$ divides $6 = (1 + \sqrt{-5})(1 - \sqrt{-5})$ and, clearly, $1 + \sqrt{-5}$ also divides $3(1 + \sqrt{-5})$. This means that $1 + \sqrt{-5}$ divides every element of $3I$. In particular, $1 + \sqrt{-5}$ must divide 3. However, the norm of $1 + \sqrt{-5}$, equal to six does not divide the norm of 3, which equal to nine. This is the final contradiction proving that $I = (2, 1 + \sqrt{-5})$ is non-principal.

In particular, non-principal ideals in $k = \mathbb{Q}(\sqrt{-5})$ exist, which means that $\mathcal{P} \neq \mathcal{F}$. Hence the class group in this case is non-trivial, that is, $h > 1$.

If we want to determine the exact structure of the class group then the following result (which we give without a proof) is very useful. We will refer to the elements of the class group (cosets of $\mathcal{P}$) as to the *ideal classes*.

Proposition 1.12.1 *Every ideal class contains an integral ideal of norm at most $C\sqrt{|d_k|}$. Here the constant C depends only on n (more precisely, it depends on r_1 and r_2).* □

For practical computations we need a particular value for C. It can be shown that for all n the value of $C = 1$ will work. Furthermore, for $n = 2$ we can take $C = \frac{1}{\sqrt{2}}$.

Clearly, since the norm of of an integral ideal coincides with its index in $\mathfrak{o}_k$, there exist only finitely many integral ideals with norm under $C\sqrt{|d_k|}$. Hence the following is true.

Corollary 1.12.2 *The class group of every number field k is finite.* □

We will conclude this section with two examples of the class group computation. We first finish the example where $k = \mathbb{Q}(\sqrt{-5})$. We already know that $h > 1$. To apply Proposition 1.12.1, we need to compute d_k. Note that 1 and $\sqrt{-5}$ is a base of $\mathfrak{o}_k$. Since $\mathrm{Tr}(1 \cdot 1) = 2$, $\mathrm{Tr}(\sqrt{-5} \cdot 1) = \mathrm{Tr}(1 \cdot \sqrt{-5}) = 0$, and $\mathrm{Tr}(\sqrt{-5} \cdot \sqrt{-5}) = -10$, we have by Proposition 1.6.3 that $d_k = 2(-10) = -20$. Hence by Proposition 1.12.1 with $C = \frac{1}{\sqrt{2}}$ we get that every ideal class contains an integral ideal of norm at most $\frac{1}{\sqrt{2}}\sqrt{20} = \sqrt{10} < 4$.

Hence we need to find all ideals of norm 1, 2, and 3. Clearly, there is only one ideal of norm 1—$\mathfrak{o}_k$ itself. We next observe that due to multiplicativity of the ideal norm (Proposition 1.11.5) every ideal whose norm is a prime number is prime. So we are looking at prime ideals only.

We will need the following fact about prime ideals.

Lemma 1.12.3 *If I is a nonzero prime ideal of $\mathfrak{o}_k$ then $I \cap \mathbb{Z}$ is a nonzero prime ideal of $\mathbb{Z}$.*

Proof: Let $J = I \cap \mathbb{Z}$. If $a, b \in \mathbb{Z} \setminus J$ then $a, b \in \mathfrak{o}_k \setminus I$ and hence, since I is prime, we have that $ab \notin I$. Consequently also $ab \notin J$, proving that J is a prime ideal of $\mathbb{Z}$. If $a \in I$ and $a \neq 0$ then $\mathrm{norm}_{k/\mathbb{Q}}(a) \in J$ and $\mathrm{norm}_{k/\mathbb{Q}}(a) \neq 0$. □

We now continue with our example $k = \mathbb{Q}(\sqrt{-5})$. The above lemma means that, say, an ideal I of $\mathfrak{o}_k$ of norm 2 would have to contain $p\mathbb{Z}$ for a prime $p \in \mathbb{Z}$. Consequently, $p \in I$ and so $(p) \subseteq I$. By Proposition 1.11.4, we compute $\mathrm{Norm}_{k/\mathbb{Q}}((p)) = |\mathrm{norm}_{k/\mathbb{Q}}(p)| = p^2$. By multiplicativity, we must have that 2 divides p^2. Hence $p = 2$. So I contains (2). Similarly, if I is an ideal of I of norm 3 then it contains (3).

Thus we simply need to determine all ideals of $\mathfrak{o}_k$ above (that is, properly containing) (2) and all ideals above (3).

We start with (2). By the correspondence theorem for rings, we have that all ideals above (2) bijectively correspond to the nonzero ideals in $\mathfrak{o}_k/(2)$. We have that $\mathfrak{o}_k = \mathbb{Z}[\sqrt{-5}] \cong \mathbb{Z}[x]/(x^2 + 5)$ and so $\mathfrak{o}_k/(2)$ is isomorphic to $\mathbb{Z}_2[x]/(x^2 + 1)$. Since $\mathbb{Z}_2[x]$ is a principal ideal domain, by the same correspondence theorem we have that the non-zero proper ideals of $\mathbb{Z}_2[x]$ bijectively correspond to the irreducible factors of $x^2 + 1 \in \mathbb{Z}_2[x]$. Since $x^2+1 = (x+1)^2$ (remember: we work modulo 2), there is only one irreducible factor, $x + 1$, and so there is only one ideal in $\mathfrak{o}_k$ above (2). We have seen that $I = (2, 1 + \sqrt{-5})$ is non-principal. Since $2 \in I$, it is above (2). Thus, I is the only ideal of $\mathfrak{o}_k$ of norm 2.

We remark that $I^2 = (2)$. Indeed, $I \supset (2)$, which means that I divides (2). Suppose $(2) = IJ$ for some integral ideal J. Since $\mathrm{Norm}_{k/\mathbb{Q}}((2)) = 4$

and $\mathrm{Norm}_{k/\mathbb{Q}}(I) = 2$, we compute that $\mathrm{Norm}_{k/\mathbb{Q}}(J) = 2$, which means that $J = I$. Therefore, $I^2 = (2)$.

Now we turn to the ideals above (3). Similarly to the above, $\mathfrak{o}_k/(3) \cong \mathbb{Z}_3[x]/(x^2-1)$. Since $x^2 - 1 = (x-1)(x+1)$, there exist exactly two proper ideals in $\mathfrak{o}_k$ above (3). Since $\sqrt{-5}$ maps to the coset $x + (x_1^2)$, we see that the two ideals above (3) are the ideals $J_1 = (3, 1+\sqrt{-5})$ and $J_2 = (3, 1-\sqrt{-5})$. We claim that both these ideals are contained in the same ideal class as $I = (2, 1+\sqrt{-5})$. Indeed, if we multiply I with $\frac{1-\sqrt{-5}}{2}$ then we get $(1-\sqrt{-5}, \frac{(1+\sqrt{-5})(1-\sqrt{-5})}{2}) = (1-\sqrt{-5}, \frac{6}{2}) = J_2$. Also, noticing that $I = (2, 1+\sqrt{-5}) = (2, 1-\sqrt{-5})$, we obtain that I multiplied with $\frac{1+\sqrt{-5}}{2}$ equals $(1+\sqrt{-5}, \frac{(1-\sqrt{-5})(1+\sqrt{-5})}{2}) = (1+\sqrt{-5}, \frac{6}{2}) = J_1$. So all three ideals, I, J_1, and J_2 belong to the same ideal class. This just means that the estimate $C = \frac{1}{\sqrt{2}}$ that we used here is not very precise.

We conclude that $k = \mathbb{Q}(\sqrt{-5})$ contains only one non-principal ideal class, that is, $h_k = 2$.

Our second example will be $k = \mathbb{Q}(\sqrt{-13})$. Above we saw two possibilities: we can have one prime ideal above (p) or we can have two prime ideals above (p). Here we will see a third option: it may happen that (p) is itself prime in $\mathfrak{o}_k$, and so there are no prime ideals above it.

If $k = \mathbb{Q}(\sqrt{-13})$ then $\mathfrak{o}_k = \mathbb{Z}[\sqrt{-13}]$ with a base 1 and $\sqrt{-13}$. Since $\mathrm{Tr}_{k/\mathbb{Q}}(1 \cdot 1) = 2$, $\mathrm{Tr}_{k/\mathbb{Q}}(1 \cdot \sqrt{-13}) = 0$ and $\mathrm{Tr}_{k/\mathbb{Q}}(\sqrt{-13} \cdot \sqrt{-13}) = -26$, we get that $d_k = 2(-26) = 52$. Hence by using the estimate from Proposition 1.12.1, we get that every ideal class contains an integral ideal of norm at most $\frac{1}{\sqrt{2}}\sqrt{52} = \sqrt{26} < 6$. So we need to look at ideals of norm 2, 3, 4, and 5.

As before, the ideals of norm $p = 2$, 3, or 5 must be prime and they must be above the corresponding principal ideals (p). For $p = 2$, we get again that $\mathfrak{o}_k/(2) \cong \mathbb{Z}_2[x]/((x+1)^2)$ and so there is exactly one prime ideal above (2), namely the ideal $I = (2, 1+\sqrt{-13})$. This ideal in non-principal; we skip the details as they are quite similar to the case of $k = \mathbb{Q}(\sqrt{-5})$. The situation is quite different for $p = 3$. Namely, $\mathfrak{o}_k/(3) \cong \mathbb{Z}_3[x]/(x^2+1)$ (since 13 is the same as 1 modulo 3). Since $x^2 + 1$ is irreducible in $\mathbb{Z}_3[x]$, the factor ring $\mathbb{Z}_3[x]/(x^2+1)$ is a field (the unique field of size $3^2 = 9$). In particular, it has no proper nonzero ideals, which means that there no ideals of norm 3 in $\mathfrak{o}_k$. Hence (3) is prime. For $p = 5$ we have a similar situation: $\mathfrak{o}_k/(5) \cong \mathbb{Z}_5[x]/(x^2+3)$, which is a field. Thus $\mathfrak{o}_k$ contains no ideals of norm 5 and (5) is prime. We now turn to the last possibility: ideals of norm 4. We claim that there is only one such ideal, namely, (2), and it is clearly principal. Indeed, suppose J is an ideal of $\mathfrak{o}_k$ of norm 4. If J is prime then $J \cap \mathbb{Z} = (p)$ and, clearly, we must have $p = 2$. So J contains (2) and then we must have $J = (2)$, as they both have the same norm 4. However, (2) is not prime, as

it is properly contained in $I = (2, 1 + \sqrt{-13})$. Thus J cannot be prime. This means that it must be a product of at least prime ideals. Since the norm of J is $4 = 2^2$, we conclude that J is a product of two prime ideals, and each of the factors has norm 2. However, we have already seen that I is the only ideal of norm 2, so $J = I^2$. Also, (2) has norm 4. Hence we must also have that $(2) = I^2 = J$.

We conclude that there exists only one non-principal ideal of norm less than 6, namely, $I = (2, 1 + \sqrt{-13})$ of norm 2. It follows that there exists a unique non-principal ideal class and so $h_k = 2$.

1.13 Units in $\mathfrak{o}_k$

In this short section we discuss the group of units of $\mathfrak{o}_k$. Recall that $\alpha \in \mathfrak{o}_k$ is a unit if and only if $\mathrm{norm}_{k/\mathbb{Q}}(\alpha) = \pm 1$.

The main result is as follows.

Theorem 1.13.1 *The group G of units of $\mathfrak{o}_k$ is finitely generated. The torsion subgroup G_T of this group is cyclic and it consists of all (complex) roots of unity contained in $\mathfrak{o}_k$. The free rank of G equals to $r_1 + r_2 - 1$.*

Proof: We will only prove the claim concerning the torsion. First of all, we note that every torsion element α is a root of unity since $\alpha^t = 1$, where t is the order of α. Next, all roots of unity are lying on the unit circle in the complex plane. The unit circle is compact, hence the torsion group G_T is finite, as $\mathfrak{o}_k$ is discrete, and so it cannot have limit points. Let t be the order of G_T. Then $\alpha^t = 1$ for all $\alpha \in G_T$, hence G_T consists of all tth roots of unity from $\mathbb{C}$. The group of all tth roots of unity is cyclic generated by the primitive tth root of unity. Therefore, G_T is cyclic. □

As an example, let consider the group of units in $\mathfrak{o}_k$, where $k = \mathbb{Q}(\sqrt{m})$, where m is a negative square-free integer. if m is nor equal to 1 modulo 4 then $\mathfrak{o}_k = \mathbb{Z}[\sqrt{m}]$. Since $\mathrm{norm}_{k/\mathbb{Q}}(a + b\sqrt{m}) = a^2 - mb^2$, we see that the norm is nonnegative. Furthermore, unless $m = -1$, there is only two units, 1 and -1. If $m = -1$ then there are four units, ± 1 and $\pm i$.

Let us now turn to the case where m is congruent to 1 modulo 4. In this case $\mathfrak{o}_k$ is larger than $\mathbb{Z}[\sqrt{m}]$, namely, $\mathfrak{o}_k$ consists of all complex numbers $\frac{a+b\sqrt{m}}{2}$, where the integers a and b are either both even or both odd. The norm is now $\frac{a^2-mb^2}{4}$ so the units correspond to the solutions of $a^2 - mb^2 = 4$, where a and b are as above. If $m < -3$ then we must have $b = 0$ and then $a = \pm_2$, giving only the obvious units ± 1. If $m = -3$ then in addition to the solutions $(a, b) = (2, 0)$ and $(-2, 0)$ we also find the solutions $(1, 1)$, $(1, -1)$,

$(-1,1)$, and $(-1,-1)$, giving the units $\frac{\pm 1 \pm \sqrt{-3}}{2}$. Thus, the unit group G is of order 6.

To summarize, the unit group of $\mathfrak{o}_k$, where $k = \mathbb{Q}(\sqrt{m})$ for a square-free negative integer m, is of order two unless $m = -1$ or $m = -3$. In the first exceptional case the group of units is of order four, and in the second case it is of order six.

1.14 Valuations

For a field k, a *valuation* on k is a map $k \to \mathbb{R}$, denoted $\alpha \mapsto ||\alpha||$, such that for all $\alpha, \beta \in k$ we have:

1. $||\alpha|| > 0$ if $\alpha \neq 0_k$, and $||0_k|| = 0$;
2. $||\alpha\beta|| = ||\alpha|| \cdot ||\beta||$; and
3. $||\alpha + \beta|| \leq ||\alpha + ||\beta||$.

The mapping sending 0_k to $0 \in \mathbb{R}$ and all other elements of k to $1 \in \mathbb{R}$ is a valuation. It is known as the *trivial valuation*. We will refer to the property 2 above as to multiplicativity of the valuation. Note that this property means that the valuation induces a homomorphism from the multiplicative group $k^{\#}$ into $\mathbb{R}_+ = \{a \in \mathbb{R} \mid r > 0\}$. In particular, $||1_k|| = 1$ and if $\alpha \neq 0_k$ then $||\alpha^{-1}|| = ||\alpha||^{-1}$. In general, $||\alpha^n|| = ||\alpha||^n$ for all $n \in \mathbb{Z}$.

Each valuation defines a metric on k, via $d(\alpha, \beta) = ||\alpha - \beta||$, and the metric defines a topology. For example, the trivial valuation defines the discrete metric: $d(\alpha, \beta) = 1$ if and only if $\alpha \neq \beta$ and the discrete topology on k, whereby every one-point subset of k is open. (Which means that every subset is open!)

We say that two valuations, $||\cdot||_1$ and $||\cdot||_2$, are *equivalent* if and only if $||\alpha||_2 = ||\alpha||_1^c$ for a fixed $c \in \mathbb{R}_+$ and all $\alpha \in K$.

Lemma 1.14.1 *Suppose $||\cdot||$ is a valuation on k. Then the set $\{\alpha \in k \mid ||\alpha|| < 1\}$ coincides with the set of all $\alpha \in k$ for which the sequence α^n converges (with respect to the topology induced by $||\cdot||$) to 0_k.*

Proof: Note that a sequence α_n converges to 0_k if and only if $d(\alpha_n, 0_k) = ||\alpha_n - 0_k|| = ||\alpha_n||$ tends to zero. If $\alpha_n = \alpha^n$ for some fixed $\alpha \in k$ then, using that the valuation is multiplicative we now get that $||\alpha_n|| = ||\alpha^n|| = ||\alpha||^n$, so it tends to zero if and only if $||\alpha|| < 1$. □

Proposition 1.14.2 *Two valuations are equivalent if and only if they induce the same topology on k.*

Proof: Suppose the two valuations induce the same topology on k. By Lemma 1.14.1, $||\alpha||_1 < 1$ if and only if α^n converges to 0_k with respect to the induced topology. By symmetry the same is also true for $||\cdot||_2$. Since the two valuations induce the same topology, we conclude that $||\alpha||_1 < 1$ if and only if $||\alpha||_2 < 1$. That is, the set $B = \{\alpha \in k\# \mid ||\alpha||_i < 1\}$ is independent of whether $i = 1$ or $i = 2$.

If $B = \emptyset$ then also $B^{-1} = \{\alpha \in k \mid ||\alpha||_i > 1\}$ is empty. This means that both valuations are trivial (hence equivalent). So we can assume that $B \neq \emptyset$. Select $\alpha_0 \in B$ and define $c \in \mathbb{R}_+$ via: $||\alpha_0||_2 = ||\alpha_0||\_1^c$. Note that $c > 0$, since $||\alpha_0||_2 < 1$.

Now consider an arbitrary $\alpha \in B$. Let λ_i, $i = 1, 2$, be defined by: $||\alpha||_i = ||\alpha_0||_i^{\lambda_i}$. Clearly, both λ_1 and λ_2 are positive. Suppose $\lambda_1 < \frac{m}{n} \in \mathbb{Q}$, where both m and n are positive integers. Then $||\frac{\alpha_0^m}{\alpha^n}||_1 = \frac{||\alpha_0||_1^m}{||\alpha||_1^n} = \frac{||\alpha_0||_1^m}{||\alpha_0||_1^{n\lambda_1}} = ||\alpha_0||_1^{m-n\lambda_1}$. Since $\lambda_1 < \frac{m}{n}$, we have that $a = m - n\lambda_1 > 0$, and so $||\frac{\alpha_0^m}{\alpha^n}||_1 = ||\alpha_0||\_1^a < 1$. That is, $\frac{\alpha_0^m}{\alpha^n} \in B$. By the above, we also must have that $||\frac{\alpha_0^m}{\alpha^n}||_2 < 1$. Since we again have that $||\frac{\alpha_0^m}{\alpha^n}||_2 = \frac{||\alpha_0||_2^m}{||\alpha||_2^n} = \frac{||\alpha_0||_2^m}{||\alpha_0||_2^{n\lambda_2}} = ||\alpha_0||_1^{m-n\lambda_2}$, we conclude that $m - n\lambda_2 > 0$, which means that $\lambda_2 < \frac{m}{n}$.

Symmetrically, if $\lambda_2 < \frac{m}{n}$ then also $\lambda_1 < \frac{m}{n}$. So $\lambda_1 < \frac{m}{n}$ if and only if $\lambda_2 < \frac{m}{n}$. Since this is true for all positive rational numbers $\frac{m}{n}$, we conclude that $\lambda_1 = \lambda_2$.

Finally, $||\alpha||_2 = ||\alpha_0||_2^{\lambda_2} = ||\alpha_0||_1^{c\lambda_2} = ||\alpha_0||_1^{c\lambda_1} = ||\alpha||_1^c$. So we have $||\alpha||_2 = ||\alpha||_1^c$ for all $\alpha \in B$. Also, if $\alpha \in B^{-1}$ then $\alpha^{-1} \in B$ and so $||\alpha||_2 = ||\alpha^{-1}||_2^{-1} = (||\alpha^{-1}||_1^c)^{-1} = (||\alpha^{-1}||_1^{-1})^c = ||\alpha||_1^c$. If $\alpha \notin B \cup B^{-1}$ then either $\alpha = 0_k$, in which case $||\alpha||_1 = ||\alpha||_2 = 0$, or $\alpha \neq 0_k$ and then $||\alpha||_1 = ||\alpha||_2 = 1$. In all cases we have $||\alpha||_2 = ||\alpha||_1^c$. Thus the two valuations are equivalent.

Conversely, assuming that $||\cdot||_1$ and $||\cdot||_2$ arre equivalent, we have that $||\alpha||_2 = ||\alpha||_1^c$ for a fixed positive $c \in \mathbb{R}$ and all $\alpha \in \mathbb{R}$. From this it follows that the open ball of radius r with center α computed with respect to $||\cdot||_1$ coincides with the open ball of radius r^c and center α computed with respect to $||\cdot||_2$. Thus, the two valuations produces exactly the same collection of open balls in k, hence they define the same topology. □

In view of this proposition the different topologies on k induced by valuations are in a bijection with equivalence classes of valuations. These equivalence classes are called *places*.

A valuation $||\cdot||$ on k is called *Archimedean* if k has characteristic zero and $||m|| > 1$ for some $m \in \mathbb{Z}$.

Lemma 1.14.3 *If $||\cdot||$ is Archimedean then $||m|| > 1$ for all $m \in \mathbb{Z}$ with $|m| > 1$.*

Proof: Clearly, $||0|| = 0$ and $||\pm 1|| = 1$. Take $m \in \mathbb{Z}$ with $|m| > 1$. Note that $||-m|| = ||-1|| \cdot ||m|| = ||m||$, so it suffices to consider the case where $m > 1$. Suppose $||m|| \leq 1$. Let A be the maximum of $||a||$, where $0 \leq a < m$. Take $n \in \mathbb{Z}$, $n > 0$ and for an arbitrary power n^t, write it as

$$n^t = \sum_{i=0}^{k} a_i m^i,$$

where $0 \leq a_i < m$ for all i. Note that $k \leq t\frac{\log n}{\log m}$. By the multiplicativity of the valuation and by the triangle inequality (property 3 in the definition) we have that $||n||^t = ||n^t|| \leq \sum_{i=1}^{k} ||a_i m^i|| = \sum_{i=1}^{k} ||a_i|| \cdot ||m||^i \leq (k+1)A$ (since $||m|| \leq 1$). So we get that $||n||^t \leq (1 + t\frac{\log n}{\log m})A$. Taking the tth roots of both sides and letting $t \to \infty$, we see that $||n|| \leq 1$. Since this is true for all positive integers n (and hence also for all integers), we conclude that $||\cdot||$ is not Archimedean, a contradiction. □

Next we show that the field $k = \mathbb{Q}$ has up to equivalence only one Archimedean valuation.

Proposition 1.14.4 *Every Archimedean valuation on $k = \mathbb{Q}$ is equivalent to the absolute value mapping.*

Proof: We first show that $||m|| = |m|^c$ for a fixed positive $c \in \mathbb{R}$ and all $m \in \mathbb{Z}$. The proof uses the same idea as the proof of Lemma 1.14.3.

Clearly, we only need to consider integers m with $|m| > 1$. Without loss of generality we can restrict ourselves to just the positive integers, so let us take $m, n \in \mathbb{Z}$ with $m, m > 1$. As in the proof of Lemma 1.14.3, pick a positive power t and write $n^t = \sum_{i=0}^{k} a_i m^i$, for a suitable a_i with $0 \leq a_i < m$ and $k \leq t\frac{\log n}{\log m}$. Using multiplicativity and the triangle inequality we get:

$$||n||^t \leq \sum_{i=0}^{k} ||a_i|| \cdot ||m||^i \leq (1 + t\frac{\log n}{\log m})A \cdot ||m||^k \leq (1 + t\frac{\log n}{\log m})A \cdot ||m||^{t\frac{\log n}{\log m}},$$

where A is the maximum of $||a||$ for $0 \leq a < m$. We also used that $||m|| > 1$ and so $||m||^i \leq ||m||^k \leq ||m||^{t\frac{\log n}{\log m}}$ for $0 \leq i \leq k$.

Thus, $||n||^t \leq (1 + t\frac{\log n}{\log m})A \cdot ||m||^{t\frac{\log n}{\log m}}$. Taking the tth roots of both sides and letting t tend to ∞, we obtain that $||n|| \leq ||m||^{\frac{\log n}{\log m}}$, or equivalently, $||n||^{\frac{1}{\log n}} \leq ||m||^{\frac{1}{\log m}}$. In view of the symmetry between m and n we must

also have $||m||^{\frac{1}{\log m}} \leq ||n||^{\frac{1}{\log n}}$, that is, in fact we have the equality $||n||^{\frac{1}{\log n}} = ||m||^{\frac{1}{\log m}}$ for all $m, n > 1$. So $C = ||n||^{\frac{1}{\log n}}$ is independent of the value of $n > 1$.

Finally, we can set $c = \log C$ and note that $||n||^{\frac{1}{\log n}} = e^c$ implies $||n|| = (e^c)^{\log n} = (e^{\log n})^c = n^c$ for all $n > 1$. Now for an arbitrary integer n we clearly have $||n|| = |n|^c$, as claimed.

If $\frac{a}{b} \in \mathbb{Q}$ with $a, b \in \mathbb{Z}$ then $||\frac{a}{b}|| = \frac{||a||}{||b||} = \frac{|a|^c}{|b|^c} = |\frac{a}{b}|^c$. So the claim holds.□

The following more general statement (currently without proof) shows that up to equivalence all Archimedean valuations of a number field k come from the embeddings of k into $\mathbb{C}$.

Theorem 1.14.5 *If k is a number field then every Archimedean valuation of k is equivalent to $||\alpha|| = |\alpha^\sigma|$, where σ is an injective homomorphisms from k into $\mathbb{C}$ and $|\cdot|$ is the usual complex norm.* □

Clearly, $|\alpha^\sigma| = |\alpha^{\bar{\sigma}}|$, which means that conjugate embeddings into $\mathbb{C}$ define equal Archimedean valuations. It can be shown that non-conjugate embeddings define nonequivalent valuations. This means that the number of different Archimedean places is equal to $r_1 + r_2$. Here, as always, r_1 is the number of real embeddings (i.e. the embeddings into $\mathbb{R}$), while r_2 is the number of conjugate pairs of non-real embeddings.

We now turn to the non-Archimedean valuations. First of all, in the non-Archimedean case the triangle inequality can be significantly strengthened.

Proposition 1.14.6 *For a non-Archimedean valuation $||\cdot||$ on a field k, we have $||\alpha + \beta|| \leq \max(||\alpha||, ||\beta||)$ for all $\alpha, \beta \in k$.*

Proof: Consider a large integer t and write $||\alpha + \beta||^t = ||(\alpha + \beta)^t|| = ||\sum_{i=0}^t \binom{t}{i} \alpha^i \beta^{t-i}|| \leq \sum_{i=0}^t ||\binom{t}{i}|| \cdot ||\alpha||^i \cdot ||\beta||^{t-i}$. Here we used multiplicativity, then the triangular inequality and then again multiplicativity. Since the valuation is non-Archimedean, $||\binom{t}{i}|| \leq 1$. Also, clearly, $||\alpha||, ||\beta|| \leq \max(||\alpha||, ||\beta||)$. Hence every summand is at most $\max(||\alpha||, ||\beta||)^t$. We conclude that $||\alpha + \beta||^t \leq (t+1) \max(||\alpha||, ||\beta||)^t$. Taking the tth root of both sides and letting t go to infinity yields the desired inequality. □

The non-Archimedean valuations on k can also be completely classified. However, the classification looks very different from the Archimedean case.

First we note the following property.

Proposition 1.14.7 *If $||\cdot||$ is a non-Archimedean valuation on a number field k then $||\alpha|| \leq 1$ for all $\alpha \in \mathfrak{o}_k$.*

Proof: Since α is an algebraic integer, it is a root of a monic polynomial $f = x^m + a_{m-1}x^{m-1} + \ldots + a_1 x + a_0 \in \mathbb{Z}[x]$. Hence $\alpha^m = -a_{m-1}x^{m-1} - \ldots - a_1 x - a_0$. If $||\alpha||$ were more than one then the valuation of left side of this equality would have been greater than the valuation of any of the summands on the right. This contradicts to Proposition 1.14.6. □

Next we note that the valuation leads to a prime ideal in $\mathfrak{o}_k$.

Proposition 1.14.8 *Suppose $||\cdot||$ is a non-Archimedean valuation on a number field k. Let $\mathfrak{p}$ consists of all algebraic integers $\alpha \in \mathfrak{o}_k$ such that $||\alpha|| < 1$. Then $\mathfrak{p}$ is a prime ideal of $\mathfrak{o}_k$.*

Proof: If $\alpha, \beta \in \mathfrak{p}$ then $||\alpha \pm \beta|| \leq \max(||\alpha||, ||\beta||) < 1$. Hence $\mathfrak{p}$ is an additive subgroup of $\mathfrak{o}_k$. Similarly, if $\alpha \in \mathfrak{p}$ and $\beta \in \mathfrak{o}_k$ then $||\beta|| \leq 1$ by Proposition 1.14.7 and so $||\alpha\beta|| = ||\alpha|| \cdot ||\beta|| \leq ||\alpha|| < 1$, implying that $\alpha\beta \in \mathfrak{p}$. This means that $\mathfrak{p}$ is an ideal in $\mathfrak{o}_k$. Finally, if $\alpha, \beta \in \mathfrak{o}_k \setminus \mathfrak{p}$ then $||\alpha|| = 1 = ||\beta||$ and hence $||\alpha\beta|| = 1$, yielding that $\alpha\beta \notin \mathfrak{p}$. Hence $\mathfrak{p}$ is prime. □

Clearly, the trivial valuation is non-Archimedean and the ideal $\mathfrak{p}$ in this case is the zero ideal. More interestingly, we have the following.

Proposition 1.14.9 *If $||\cdot||$ is a nontrivial non-Archimedean valuation then the corresponding prime ideal $\mathfrak{p}$ is nonzero.*

Proof: We need to show that $\mathfrak{p}$ contains a nonzero element. If $||t|| < 1$ for some nonzero integer t then the claim is clearly true. So suppose that $||t|| = 1$ for all nonzero integers t. Since $||\cdot||$ is nontrivial, there exists $0 \neq \alpha \in k$ such that $||\alpha|| \neq 1$. Substituting, if necessary, α with α^{-1}, we can assume that $||\alpha|| < 1$. By Proposition 1.3.6 we know that for some nonzero $a \in \mathbb{Z}$ we have that $\beta = a\alpha$ is an algebraic integer, that is, $\beta \in \mathfrak{o}_k$. Since $||a|| = 1$, we must now have that $||\beta|| = ||a|| \cdot ||\alpha|| = ||\alpha|| < 1$. Thus, $\beta \in \mathfrak{p}$, and so $\mathfrak{p}$ is nonzero. □

We conclude this section with a statement classifying non-Archimedean valuations, which is given without a proof. We need some notation. For a nontrivial non-Archimedean valuation $||\cdot||$, let $\mathfrak{p}$ be the corresponding prime ideal in $\mathfrak{o}_k$ and for a nonzero fractional ideal F let $v_\mathfrak{p}(F)$ be the exponent of $\mathfrak{p}$ in the unique factorization of F. Note that the integer $v_\mathfrak{p}(F)$ can be positive, negative, or zero, but it is nonnegative if F is an (integral) ideal.

Theorem 1.14.10 *Suppose $||\cdot||$ is a nontrivial non-Archimedean valuation of a number filed k and let $\mathfrak{p}$ and $v_\mathfrak{p}$ be as above. Then for some real number $C > 1$ and all $0 \neq \alpha \in k$ we have $||\alpha|| = C^{-v_\mathfrak{p}((\alpha))}$, where, as usual, (α) denotes the principal fractional ideal generated by α.* □

Because the non-Archimedean valuations correspond to the nonzero prime ideals of $\mathfrak{o}_k$, the non-Archimedean places are usually called *finite* places, whereas the Archimedean places are called *infinite* places.