Rings of Integers and Beyond
(Meeting Notes)

Felix Gotti

May 22, 2026

Contents

Introduction

Number Fields and their Rings of Integers

A subfield K of $\mathbb{C}$ is called an *algebraic number field* or, simply, a *number field* if K is a finite-dimensional vector space over $\mathbb{Q}$, in which case, one can write K as $\mathbb{Q}(\alpha)$ for some algebraic number α. Historically, these fields arose from the desire to solve higher-degree polynomial equations and understand the symmetries of their roots, a pursuit that transitioned from Galois's revolutionary group-theoretic work to Dedekind's formalization of field theory. The relevance of number fields lies in their ability to act as a "lens" for arithmetic as, by moving from $\mathbb{Q}$ to a larger field K, we can decompose numbers into new, algebraic factors that reveal the underlying structure of equations.

The *ring of integers* $\mathcal{O}_K$ of a number field K is the set of all elements in K that are roots of monic polynomials with coefficients in $\mathbb{Z}$. The study of these algebraic structures emerged in the 19th century when prominent mathematicians, including Carl Gauss, Gotthold Eisenstein, and Ernst Kummer, sought to extend the known laws of arithmetic beyond the set $\mathbb{Z}$ of rational or ordinary integers. From a more philosophical perspective, rings of integers represent the transition from the empirical observation of numbers to the structural understanding of mathematical reality, making tangible the tension between the concrete nature of specific numbers and the universal algebraic laws that govern them.

Rings of Integers and the Non-Unique Factorization Crisis

The study of rings of integers was significantly catalyzed by the "crisis of non-unique factorization," most notably when Gabriel Lamé incorrectly assumed that inside every cyclotomic ring extension $\mathbb{Z}[\zeta_p]$ of $\mathbb{Z}$ by a primitive p-th root of unity (with p prime), factorization into irreducibles was essentially unique, a claim debunked by Kummer's discovery that the unique factorization (UF) property fails in $\mathbb{Z}[\zeta_{23}]$. Today, rings of integers are the central objects of study in algebraic number theory, serving as the "local" playgrounds where we investigate the failure of the UF property and the behavior of prime ideals. Beyond their theoretical beauty, they are foundational to modern cryptography (specifically in lattice-based and isogeny-based systems), provide the framework for solving Diophantine equations, and offer deep insights into factorization theory through invariants like the divisor class group.

Cyclotomic Rings of Integers and Fermat's Last Theorem

At the heart of Fermat's Last Theorem (FLT) lies the fundamental tension between the arithmetic of the rational integers $\mathbb{Z}$ and the rings of integers $\mathcal{O}_K$ of cyclotomic fields. The equation $x^n + y^n = z^n$ can be elegantly factored as

$$z^n = \prod_{j=0}^{n-1} (x + \zeta_n^j y)$$

only by stepping into the ring $\mathbb{Z}[\zeta_n]$. The historical drama of FLT was driven by the discovery that these rings often lack unique factorization, a "failure" that initially thwarted Lamé but led Kummer to develop the theory of ideal numbers. By categorizing primes as "regular" based on whether they divide the class number of $\mathcal{O}_K$, Kummer was able to prove the theorem for regular prime exponents. Even in Wiles's final proof, the connection remains intrinsic: the modularity theorem bridges the gap between elliptic curves and the Galois representations associated with these rings of integers. Ultimately, FLT is not merely a statement about $\mathbb{Z}$, but a profound testament to how the structural properties of rings of integers govern the existence (or non-existence) of solutions to Diophantine equations.

Rings of Integers in Connections to Ideal Theory and Valuation Theory

The same crisis ignited the transition from classical number theory to modern abstract algebra. When Kummer introduced "ideal numbers" to rectify the non-unique factorization phenomenon in cyclotomic fields, he provided a computational workaround, but it was Richard Dedekind who transformed this into a robust structural theory. By defining an ideal as a set-theoretic object (an additive subgroup closed under multiplication by arbitrary elements of the ring), Dedekind shifted the focus from individual elements to collections of numbers, creating (or perhaps discovering) the modern concept of an ideal to restore unique factorization at the level of sets. This clever creation by Dedekind gave life to ideal theory. Ideals provided both the template for Noetherian rings and the axiomatic study of commutative algebra. Furthermore, the quest to understand the size and multiplicity of these ideals led directly to the development of valuation theory. By viewing the power of a prime ideal $\mathfrak{p}$ dividing an element as a valuation $v_{\mathfrak{p}}$, mathematicians like Kurt Hensel and József Kürschák were able to unify the arithmetic of rings of integers with the analytic properties of power series. Thus, the ring of integers served as the original laboratory for these theories, proving that the local behavior of valuations and the global structure of ideals are two sides of the same arithmetic coin.

Rings of Integers and Arithmetic Geometry

The earliest and most profound applications of factorization theory lie in algebraic number theory. Kummer's ideal numbers and Dedekind's subsequent formalization of ideals provided the conceptual foundation for the study of *ideal class groups*, whose structure measures

the failure of unique factorization in rings of integers. Class groups play a central role in understanding the arithmetic of number fields, influencing the solvability of Diophantine equations, the structure of algebraic curves, and the arithmetic of algebraic varieties (see [1]). The modern theory of global fields, divisor class groups, and Picard groups in algebraic geometry continues to depend fundamentally on these ideas (see [15]).

Foundations – Sets, Monoids, and Groups

In this preliminary chapter, we introduce the set theory notation and briefly recall some basics of commutative monoids and abelian groups we will be referring to later.

General Notation

As is customary, we let $\mathbb{Z}$ denote the ring of integers and $\mathbb{Q}$, $\mathbb{R}$, and $\mathbb{C}$ the fields of rational, real, and complex numbers, respectively. In addition, we let $\mathbb{P}$ denote the set of rational (standard) primes, while we let $\mathbb{N}$ denote the multiplicative monoid of positive integers. Finally, we set

$$\mathbb{N}_0 := \{0\} \cup \mathbb{N}.$$

For each prime $p \in \mathbb{P}$ and positive integer $n \in \mathbb{N}$, we let $\mathbb{F}_{p^n}$ denote the field with p^n elements (it is well known that the cardinality of every finite field is a prime power). For any real number r and a subset S of the real line, we set $S_{\geq r} := \{s \in S : s \geq r\}$. For any pair $(m, n) \in \mathbb{Z}^2$ with $m \leq n$, we set

$$[\![m, n]\!] := \{k \in \mathbb{Z} : m \leq k \leq n\}.$$

For any positive rational q, call the unique relatively prime positive integers $\mathsf{n}(q)$ and $\mathsf{d}(q)$ such that $q = \mathsf{n}(q)/\mathsf{d}(q)$ the *numerator* and the *denominator* of q, respectively. For a prime p, the *p-adic valuation* on $\mathbb{Q}$ is the map $v_p \colon \mathbb{Q} \to \mathbb{Z} \cup \{\infty\}$ defined as follows: $v_p(0) = \infty$ and $v_p(q) = v_p(\mathsf{n}(q)) - v_p(\mathsf{d}(q))$ for any $q \neq 0$, where for $n \in \mathbb{N}$ the value $v_p(n)$ is the exponent of the maximal power of p dividing n. One can readily verify that for $q_1, \ldots, q_n \in \mathbb{Q}_{>0}$:

$$v_p(q_1 + \cdots + q_n) \geq \min\{v_p(q_1), \ldots, v_p(q_n)\}$$

Commutative Semigroups and Monoids

A *binary operation* on a set S is a function $* \colon S \times S \to S$. When $*$ is a binary operation on a set S, it is customary to write $s * t$ instead of $*(s, t)$ for any $s, t \in S$. A pair $(S, *)$, where S is

a set and $*$ is a binary operation on S, is called a semigroup provided that the operation $*$ is associative: $r*(s*t)=(r*s)*t$ for all $r,s,t\in S$.

Let $(S,*)$ be a semigroup. An element $e\in S$ is called an *identity element* of S if $e*s=s*e=s$ for all $s\in S$. Every semigroup has at most one identity element: indeed, if $e_1,e_2\in S$ are both identity elements, then $e_1=e_1*e_2=e_2$. The semigroup $(S,*)$ is said to be *commutative* if $s*t=t*s$ for all $s,t\in S$. A semigroup having an identity element is called a *monoid*.

Let $(M,*)$ be a monoid with identity element denoted by e, and let us denote $(M,*)$ simply by M. An element $u\in M$ is called *invertible* or a *unit* if $u*v=v*u=e$ for some $v\in M$, in which case such an element v is called an *inverse* of u. As the identity element $e\in M$ satisfies $e*e=e$, it is its own inverse and, therefore, a unit. In a monoid, every unit has a unique inverse: indeed, if $v_1,v_2\in M$ are two inverses of a unit u, then $v_1=v_1*(u*v_2)=(v_1*u)*v_2=v_2$.

A subset S of M is called a *submonoid* of M if S contains the identity element of M and is *closed* under the operation of M, which means that $b*c\in S$ for all $b,c\in S$. If S is a submonoid of M such that $S\neq M$, then S is called a *proper* submonoid of M. It is routine to prove that the property of being submonoids of a given monoid is preserved under taking arbitrary intersections.

Let N denote a monoid $(N,*')$ with identity element e_N. A function $\varphi\colon M\to N$ is called a *monoid homomorphism* if $\varphi(e)=e_N$ and $\varphi(b*c)=\varphi(b)*'\varphi(c)$ for all $b,c\in M$. If $\varphi\colon M\to N$ is a bijective homomorphism, then φ is called a *monoid isomorphism* and, in this case, we say that the monoids M and N are *isomorphic*.

Abelian Groups

We recall the basic language of abelian groups, and briefly discuss the quotient of abelian groups.

Definition 0.1. A *group* is a monoid where every element is invertible. A group is said to be *abelian* if it is commutative as a monoid.

Unless we explicitly state otherwise, every abelian group we deal with in this note is written additively. For the rest of this section, let A be an abelian group. A submonoid S of A is said to be a *subgroup* provided that S is a group with the operation it inherits from A, in which case, we write $S\leq A$. If S is a subgroup of A such that $S\neq A$, then S is called a *proper* subgroup of A. Given abelian groups A and B, a map $\varphi\colon A\to B$ is called a *group homomorphism* provided that $\varphi(a+a')=\varphi(a)+\varphi(a')$ for all $a,a'\in A$. We say that a group homomorphism is an *isomorphism* if it is a bijection. Given a group homomorphism $\varphi\colon A\to B$, one can check that $\varphi(A)$ is a subgroup of B, while the subset $\ker\varphi$ of A consisting of all the elements mapped to 0 by φ is a subgroup of A called the *kernel* of φ:

$$\ker\varphi:=\{a\in A:\varphi(a)=0\}.$$

Observe that a group homomorphism is injective if and only if its kernel is the trivial group. Thus, images and kernels of group homomorphisms are groups.

Every group can be somehow divided by any given subgroup (at least those groups that are abelian). To show how this is done, let S be a subgroup of A. For each $a \in A$, we define the *coset* of a with respect to S as follows: $a + S := \{a + s : s \in S\}$. Now set

$$A/S := \{a + S : a \in A\}.$$

Let us define now a binary operation on A/S based on the operation of A: for any cosets $a + S$ and $a' + S$ of A/S,

$$(a + S) + (a' + S) := (a + a') + S. \tag{1}$$

It is routine to verify that this binary operation is well defined and also that A/S is an abelian group under such operation: the group A/S is called the *quotient group* of A by S. Then we can project A onto its quotient group A/S via the map $\pi\colon A \to A/S$ defined by $\pi(a) = a + S$ for all $a \in A$, which is clearly a surjective group homomorphism such that $\ker \pi = S$. In light of this, we see that every subgroup of the abelian group A is the kernel of a group homomorphism with domain A.

Proposition 0.2 (First Isomorphism Theorem)**.** *Let $\varphi\colon A \to A'$ be a group homomorphism. Then the quotient group $A/\ker\varphi$ is isomorphic to the subgroup $\varphi(A)$ of A' via the group homomorphism determined by the assignments $a + \ker\varphi \mapsto \varphi(a)$ for all $a \in A$.*

Proof. Define the map $\bar{\varphi}\colon A/\ker\varphi \to \varphi(A)$ by $\bar{\varphi}(a + \ker\varphi) = \varphi(a)$. First, we show $\bar{\varphi}$ is well-defined. If $a + \ker\varphi = b + \ker\varphi$, then $a - b \in \ker\varphi$ and so $\varphi(a - b) = 0$, which implies $\varphi(a) = \varphi(b)$. To verify that $\bar{\phi}$ is a homomorphism, observe that, for any $a, b \in A$,

$$\begin{aligned}\bar{\varphi}((a + \ker\varphi) + (b + \ker\varphi)) = \bar{\varphi}((a + b) + \ker\varphi) = \varphi(a + b) = \varphi(a) + \varphi(b)\\ = \bar{\varphi}(a + \ker\varphi) + \bar{\varphi}(b + \ker\varphi).\end{aligned}$$

Finally, we check bijectivity. Every element in $\varphi(A)$ is of the form $\varphi(a)$ for some $a \in A$, and $\bar{\varphi}(a + \ker\varphi) = \varphi(a)$. If $\bar{\varphi}(a + \ker\varphi) = 0$, then $\varphi(a) = 0$, so $a \in \ker\varphi$, meaning $a + \ker\varphi$ is the identity in $A/\ker\varphi$. Thus, $\bar{\varphi}$ is an isomorphism. □

The following result, known as the Second Isomorphism Theorem, is a consequence of the First Isomorphism Theorem. We leave the proof as an exercise.

Proposition 0.3 (Second Isomorphism Theorem)**.** *Let A be an abelian group, and let S and T be subgroups of A. Then $(S + T)/T \cong S/(S \cap T)$.*

Chapter 1

Preliminaries on Commutative Rings

1.1 Commutative Rings – Ideals, Quotients, and Homomorphisms

We now recall the notion of a commutative ring (with identity).

Definition 1.1. A triple $(R, +, \cdot)$, where R is a set and $+$ and $\cdot$ are two binary operations on R, is called a *ring* if the following conditions hold:

- $(R, +)$ is an abelian group,
- $(R, \cdot)$ is a monoid, and
- $r \cdot (s + t) = r \cdot s + r \cdot t$ and $(s + t) \cdot r = s \cdot r + t \cdot r$ for all $r, s, t \in R$.

Let $(R, +, \cdot)$ be a ring and, from now on, let us denote this triple simply by R (this is customary in the literature). The identity of the monoid $(R, +)$, is denoted by 0 and called the *zero element* of R or simply *zero*. For all $r \in R$, the equality $0 \cdot r = 0$ holds: it can be deduced from $0 \cdot r = (0 + 0) \cdot r = 0 \cdot r + 0 \cdot r$, as $0 \cdot r$ has an additive inverse. Similarly, $r \cdot 0 = 0$ for all $r \in R$. For $r, s \in R$, we write rs instead of $r \cdot s$ if we see no risk of confusion. We say that R is *commutative* if the semigroup $(R, \cdot)$ is commutative. In addition, we say that an element of R is an *identity* if it is an identity of the semigroup $(S, \cdot)$. Thus, if R contains an identity, then it must be unique and we denote it by either 1_R or 1 and refer to it as *the* identity element. In the scope of this exposition, we are only interested in commutative rings with identity, and we tacitly assume that the identity is not the zero element (otherwise, R is a singleton, which is not an interesting case to consider).

For a commutative ring R with identity, we let $R^\times$ denote its group of units (i.e., invertible elements) of R. For $r, s \in R$, we say that s *divides* r and write $s \mid_R r$ if $r = st$ for some $t \in R$. Elements $r, s \in R$ are *associates* if $s = ur$ for some $u \in R^\times$.

An additive subgroup S of R is called a *subring* if S is closed under multiplication and contains 1. Clearly, a subring of R is a commutative ring with identity under the binary operations it inherits from R.

Let R be a commutative ring with identity 1. An additive subgroup I of R is called an *ideal* if $ra \in I$ for all $r \in R$ and $a \in I$. It is clear that $\{0\}$ and R are ideals of R, and we call $\{0\}$ the *zero ideal* of R. An ideal I of R is called *proper* if $I \subsetneq R$. An ideal I of R is proper if and only if $I \cap R^\times$ is empty: for the less trivial direction, observe that if $u \in I \cap R^\times$ then $R = u(u^{-1}R) \subseteq IR = I$. Hence the only ideals of a field are the zero ideal and the whole field.

Let R and S be commutative rings with identities 1_R and 1_S, respectively. A map $\phi\colon R \to S$ is called a *ring homomorphism* if ϕ is a group homomorphism between the underlying additive groups of R and S and the following two conditions hold:

- $\phi(1_R) = 1_S$ and
- $\phi(r_1 r_2) = \phi(r_1)\phi(r_2)$ for all $r_1, r_2 \in R$.

If $\varphi\colon R \to S$ is a ring homomorphism, one can readily check that the subgroup $\ker\varphi$ of the underlying abelian group of R is indeed an ideal and that the subgroup $\varphi(R)$ of S is indeed a subring. An *isomorphism* of rings is a bijective ring homomorphism. If there exists an isomorphism between R and S, we say that R and S are *isomorphic* and write $R \cong S$.

The main relevance of ideals in ring theory is that we can quotient by them. For an ideal I of R, we can define a multiplicative operation on the quotient group R/I as follows:

$$(r + I)(s + I) := rs + I$$

for all $r, s \in R$. It is routine to verify that, under this multiplication, the quotient group R/I is a commutative ring with identity $1 + I$ (the absorbing property of the ideal I is needed for the multiplication to be well defined). We call R/I the *quotient ring* of R by I. Observe that the group homomorphism $\pi\colon R \to R/I$ is now a ring homomorphism. There is a version of the First Isomorphism Theorem in the setting of commutative rings, and this result describes the structural relationship among homomorphisms, ideals, and quotients.

Proposition 1.2. *Let $\varphi\colon R \to S$ be a ring homomorphism. Then the map $R/\ker\varphi \to S$ defined via the assignment $r + \ker\varphi \mapsto \varphi(r)$ (for all $r \in R$) is an injective ring homomorphism with image $\varphi(R)$, whence $R/\ker\varphi \cong \varphi(R)$.*

With notation as in Proposition 1.2, if $I \subseteq \ker\varphi$, then φ factors through π, that is, there exists a unique ring homomorphism $\overline{\varphi}\colon R/I \to S$ such that $\varphi = \overline{\varphi} \circ \pi$. As for the case of groups, there is also a Second Isomorphism Theorem for commutative rings.

Proposition 1.3. *Let R be a commutative ring with identity, and let S and I be a subring and an ideal of R, respectively. Then $S \cap I$ is an ideal of S and $(S + I)/I \cong S/(S \cap I)$.*

1.2 Integral Domains – UFDs, PIDs, and Euclidean Domains

In this section, we introduce three nested classes of integral domains, which are relevant in the study of rings of integers. A commutative ring R with identity is called an *integral domain* if, for all $r, s \in R$, the equality $rs = 0$ implies that $0 \in \{r, s\}$. For the rest of this section, we assume that R is an integral domain.

Definition 1.4. A *field* is an integral domain where every nonzero element is a unit.

A nonzero nonunit $r \in R$ is *irreducible* if whenever $r = uv$ for some $u, v \in R$ the set $\{u, v\} \cap R^\times$ is nonempty. We can now cast a relevant class of integral domains based on the statement of the Fundamental Theorem of Arithmetic (FTA).

Definition 1.5. An integral domain is a *unique factorization domain (UFD)* if for every nonzero $r \in R \setminus R^\times$, the following statements hold:

1. $r = p_1 \cdots p_m$ for some irreducibles $p_1, \ldots, p_m \in R$, and

2. if $r = q_1 \cdots q_n$ for irreducibles $q_1, \ldots, q_n \in R$, then $n = m$ and there is a bijection $\varphi \colon [\![1, m]\!] \to [\![1, m]\!]$ such that $q_{\varphi(j)}$ and p_j are associates for every $j \in [\![1, m]\!]$.

Every field is trivially a UFD, and $\mathbb{Z}$ is a UFD by the We will prove in the next subsection that the rings of polynomials $\mathbb{Z}[x]$ and $\mathbb{Z}[x, y]$ are UFDs.

We can now generalize the standard notion of a prime to elements in any commutative ring with identity. A nonzero element $r \in R \setminus R^\times$ is *prime* if whenever $r \mid_R st$ for some $s, t \in R$ either $r \mid_R s$ or $r \mid_R t$. It is not hard to verify that every prime is irreducible (prove this!).

Proposition 1.6. *Let R be a UFD. An element of R is prime if and only if it is irreducible.*

Proof. In every integral domain, primes are irreducibles, and we leave the verification of this fact to the reader. Now suppose that $p \in R$ is an irreducible. To check that p is prime, take $r, s \in R$ such that $p \mid_R rs$, and then write $pt = rs$ for some $t \in R$. As R is a UFD, we can factor t, r, and s into irreducibles to obtain factorizations of the same element in both sides of the equality $pt = rs$. Since p is irreducible and R is a UFD, p is associate with one of the irreducibles in the factorization of rs, and so either $p \mid_R r$ or $p \mid_R s$. Hence p is prime. □

For any $a \in R$, we can verify that $aR := \{ar : r \in R\}$ is the smallest ideal of R containing a: ideals of the form aR are called *principal ideals*. We often write (a) instead of aR. The zero ideal and the whole ideal R are both principal ideals as $\{0\} = 0R$ and $R = 1R$. Integral domains whose ideals are principal play an important role in commutative ring theory.

Definition 1.7. An integral domain R is called a *principal ideal domain (PID)* if every ideal of R is principal.

Every field is clearly a PID. Let us verify that $\mathbb{Z}$ is a PID.

Example 1.8. We verify that every ideal of $\mathbb{Z}$ is principal. Let I be a nonzero proper ideal, and take $m \in I \setminus \{0\}$ such that $|m| := \min\{|a| : a \in I \setminus \{0\}\}$. Then $m\mathbb{Z} \subseteq I\mathbb{Z} = I$. Conversely, for any $a \in I$ we can take $q, r \in \mathbb{Z}$ with $|r| < |m|$ such that $a = qm + r$ and, as $r = a - qm \in I - m\mathbb{Z} \subseteq I$, and $r = 0$ must hold by the minimality of $|m|$, whence $a = mq \in m\mathbb{Z}$. Hence $I = m\mathbb{Z}$ is a principal ideal. ■

We will prove in the next theorem that every PID is a UFD. First, we need to collect the following temporary result (once we prove Theorem 1.10, this lemma will become a special case of Proposition 1.6).

Lemma 1.9. *If R is a PID, then every irreducible in R must be prime.*

Proof. Let p be an irreducible in R, and let I be an ideal containing Rp. Since R is a PID, $I = Ra$ for some $a \in R$. After writing $p = ab$ for some $b \in R$, we see that either $a \in R^\times$ or $b \in R^\times$. Accordingly, we find that $I = R$ or $I = Rp$. Hence the only ideal properly containing Rp is R, which means that Rp is a maximal ideal and, therefore, a prime ideal. Hence p is prime. □

Theorem 1.10. *Every PID is a UFD.*

Proof. Let R be a PID. Suppose, by way of contradiction, that there is a nonzero element $r_0 \in R \setminus R^\times$ that does not factor into irreducibles. So $r_0 = r_1 s_1$ for some $r_1, s_1 \in R \setminus R^\times$ such that r_1 does not factor into irreducibles. As before, we can write $r_1 = r_2 s_2$ for some $r_2, s_2 \in R \setminus R^\times$ such that r_2 does not factor into irreducibles. Going on in a similar fashion, we can construct sequences $(r_n)_{n\geq 0}$ and $(s_n)_{n\geq 1}$ with $r_n, s_n \in R \setminus R^\times$ such that $r_n = r_{n+1}s_{n+1}$. Thus, the sequence $(Rr_n)_{n\geq 0}$ of ideals satisfies that $Rr_n \subsetneq Rr_{n+1}$ and, therefore, $I = \bigcup_{n\geq 0} Rr_n$ is an ideal. Since R is a PID, there is an $a \in R$ such that $I = Ra$. Take an $m \in \mathbb{N}$ such that $a \in Rr_m$. This implies that $I = R_m$, and so $Rr_{m+1} = Rr_m$. In this case, r_m and r_{m+1} are associates, which contradicts that Rr_{n+1} strictly contains Rr_n. Hence every nonzero element of $R \setminus R^\times$ is a product of irreducibles. The proof of uniqueness is left to the reader as an exercise. □

As the following example indicates, the converse of Theorem 1.10 does not hold.

Example 1.11. Consider the ring $\mathbb{Z}[x]$. We will show in the next section that $R[x]$ is a UFD provided that R is a UFD. Therefore $\mathbb{Z}[x]$ is a UFD. On the other hand, one can easily verify that the ideal $(2, x)$ is not principal. Hence $\mathbb{Z}[x]$ is not a PID.

The Euclidean division algorithm is an important tool we have at our disposal in $\mathbb{Z}$. We can consider generalizations of the ring $\mathbb{Z}$ where still we can perform the Euclidean division algorithm. Such rings are called Euclidean domains.

Definition 1.12. An integral domain R is called a *Euclidean domain* if there is a map $N\colon R \to \mathbb{N}_0$ with $\mathrm{N}(0) = 0$, called a *norm*, such that for any elements $a, b \in R$ with $b \neq 0$, there are elements $q, r \in R$ such that $a = qb + r$ and either $r = 0$ or $\mathrm{N}(r) < \mathrm{N}(b)$.

We proceed to show that every Euclidean domain is a PID.

Theorem 1.13. *Every Euclidean domain is a PID.*

Proof. Let R be a Euclidean domain with norm $N\colon R \to \mathbb{N}_0$. Take a nonzero ideal I of R. Let b be a nonzero element of I having minimum norm. We claim that $I = Rb$. Clearly, $Rb \subseteq I$. For the reverse inclusion, consider $a \in I$. Since R is a Euclidean domain, $a = qb + r$ for some $q, r \in R$, where either $r = 0$ or $\mathrm{N}(r) < \mathrm{N}(b)$. Since $r = a - qb \in I$, the minimality of $\mathrm{N}(b)$ ensures that $r = 0$, and so $a = qb \in I$. As a result, the inclusion $I \subseteq Rb$ holds and, therefore, I is principal. Hence R is a PID. □

We conclude this subsection emphasizing that not every PID is a Euclidean domain. However, examples witnessing this are not that easy to construct. One of the most tractable examples is $\mathbb{Z}[\omega]$, where $\omega := (1 + i\sqrt{19})/2$. To see why $\mathbb{Z}[\omega]$ is a PID but not a Euclidean domain, [5, Subsections 8.1 and 8.2].

1.3 Localization

TO BE INCLUDED...

1.4 Polynomial Rings – Irreducibility and Factorizations

TO BE INCLUDED...

Exercises – Preliminaries on Commutative Rings

Exercise 1.1. Prove Proposition 1.2, the First Isomorphism Theorem for commutative rings.

Exercise 1.2. Construct an integral domain having an irreducible element that is not a prime.

Exercise 1.3. Let R be a PID. Prove that any two factorizations of the same nonzero element must be the same up to order and associates.

Chapter 2

Algebraic Field Extensions and Number Fields

Given two fields K and L, the notation L/K means that K is a subfield of L, in which case we say that either L is an *extension field* of K or that L/K is a *field extension*. For the rest of this section, we let L/K be a field extension.

2.1 Algebraic Extensions

If S is a subset of L then $K(S)$ denotes the smallest subfield of L that contains both K and S, which is the intersection of all the subfields of L containing K and S. For a finite subset $\{\sigma_1, \sigma_2, \ldots, \sigma_n\}$ of L, we write $K(\sigma_1, \sigma_2, \ldots, \sigma_n)$ instead of $K(\{\sigma_1, \sigma_2, \ldots, \sigma_n\})$.

One can show that the action $K \times L \to L$ of K on L naturally induced by the multiplication inside L (i.e., $(\alpha, \beta) \mapsto \alpha\beta$ for all $(\alpha, \beta) \in K \times L$) turns L into a vector space over K. The *degree* of a field extension L/K, denoted by $[L : K]$, is the dimension of L as a K-vector space:

$$[L : K] := \dim_K L.$$

The extension L/K is called *finite* if L is a finite-dimensional vector space over K or, equivalently, $[L : K] < \infty$.

We are interested in whether $\alpha \in L$ satisfies a polynomial equation with coefficients in K. An element $\alpha \in L$ is *algebraic* over K if there exists a nonzero polynomial $p(x) \in K[x]$ such that $p(\alpha) = 0$. An element of L is *transcendental* over K if it is not algebraic over K. If $\alpha \in L$ is algebraic over K, there is a unique monic polynomial $m_\alpha(x) \in K[x]$ that vanishes at α and divides any other polynomial in $K[x]$ vanishing at α (exercise).

Definition 2.1. Let L/K be a field extension. For any $\alpha \in L$ that is algebraic over K, the unique monic irreducible polynomial in $K[x]$ that divides any other polynomial in $K[x]$ having α as a root is called the *minimal polynomial* of α over K.

Let us take a quick at a couple of examples.

Example 2.2. The field extension $\mathbb{C}/\mathbb{R}$ is an algebraic extension because the field $\mathbb{C}$ is a simple extension of $\mathbb{R}$ by an algebraic element, namely, $\mathbb{C} = \mathbb{R}(\sqrt{-1})$. Since $x^2 + 1 \in \mathbb{R}[x]$ is the minimal polynomial of $\sqrt{-1}$, the extension $\mathbb{C}/\mathbb{R}$ has degree 2.

Example 2.3. The field extension $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ is also an algebraic extension because $\sqrt[3]{2}$ because $x^3 + 2 \in \mathbb{Q}[x]$ is the minimal polynomial of $\sqrt[3]{2}$ and so $\sqrt[3]{2}$ is an algebraic element over $\mathbb{Q}$.

Throughout these notes, we often denote the minimal polynomial of an algebraic number α by either $m_\alpha(x)$ or $m_{\alpha,K}(x)$. The extension field L of K is called *simple* if there exists $\alpha \in L$ such that $L = K(\alpha)$. As we proceed to prove, a simple extension $K(\alpha)/K$ is finite if and only if α is algebraic over K, in which case the dimension of the K-vector space $K(\alpha)$ equals the degree of the minimal polynomial of α.

Theorem 2.4. *For a field extension L/K, let $\alpha \in L$ be an algebraic element over K whose minimal polynomial $m(x) \in K[x]$ has degree d. Then the following statements hold.*

1. $K(\alpha) \cong K[x]/(m(x))$.
2. *The set $\{1, \alpha, \ldots, \alpha^{d-1}\}$ is a basis for $K(\alpha)$ over K.*
3. $[K(\alpha) : K] = \deg m(x)$.

Proof. (1) Now consider the map $\phi\colon K[x] \to K[\alpha]$ defined as $\phi(p(x)) = p(\alpha)$ for all $p(x) \in K[x]$. One can readily check that ϕ is a surjective ring homomorphism. In addition, note that a polynomial in $K[x]$ has α as a root if and only if it is divisible by $m_{\alpha,K}(x)$ in $K[x]$, whence

$$\ker \varphi = \{p(x) \in K[x] : p(\alpha) = 0\} = (m(x)).$$

Therefore in light of the First Isomorphism Theorem, $K[x]/(m(x)) \cong K[\alpha]$. It suffices to argue the equality $K[\alpha] = K(\alpha)$ or, equivalently, that $K[\alpha]$ is a field. As the polynomial $m(x)$ is irreducible in the UFD $K[x]$ (which is actually a PID), it must be a prime in $K[x]$, whence the ideal $(m(x))$ of $K[x]$ generated by $m(x)$ is prime. As $K[x]$ is a PID and so a one-dimensional domain, $(m(x))$ must be a maximal ideal. Thus, the quotient $K[x]/(m(x))$ is a field and, in light of the isomorphism $K[\alpha] \cong K[x]/(m(x))$ we have already established $K(\alpha) = K[\alpha] \cong K[x]/(m(x))$.

(2) Since every element of $K[\alpha]$ has the form $f(\alpha)$ for some polynomial $f(x) \in K[x]$, after writing $f(x) = m(x)g(x) + r(x)$ for some $g(x), r(x) \in K[x]$ such that the inequality $\deg r(x) < \deg m(x)$ holds, we see that $f(\alpha) = r(\alpha) \in \sum_{i=0}^{d-1} K\alpha_i$. Thus, $K(\alpha) = K[\alpha]$ is spanned by $\{1, \alpha, \ldots, \alpha^{d-1}\}$ as a vector space over K. Now suppose that $\sum_{i=0}^{d-1} c_i\alpha^i = 0$ for some $c_0, c_1, \ldots, c_{d-1} \in K$. Then α is a root of the polynomial $p(x) = \sum_{i=0}^{d-1} c_i x^i$, and so we can write $p(x) = m(x)q(x)$ for some polynomial $q(x) \in K[x]$. As $\deg m(x) = d > \deg p(x)$, we see that $q(x)$ is the zero polynomial and, as a consequence, so is $p(x)$. Thus, $c_0 = c_1 = \cdots = c_{d-1} = 0$, and so $\{1, \alpha, \ldots, \alpha^{d-1}\}$ is a linearly independent set of vectors in $K(\alpha)$. Hence $\{1, \alpha, \ldots, \alpha^{d-1}\}$ is a basis for $K(\alpha)$ as a vector space over K.

(3) We have just identified a basis for the K-vector space $K(\alpha)$ consisting of d vectors. Thus, $[K(\alpha) : K] = \dim_K K(\alpha) = d = \deg m(x)$, and this completes our proof. □

Corollary 2.5. *Let L/K be a field extension. For any $\alpha \in L$, the extension $K(\alpha)/K$ is algebraic if and only if it is finite.*

This theorem allows us to represent elements of a number field as linear combinations of powers of a single algebraic element.

Example 2.6. Consider the extension field $\mathbb{Q}(\zeta)$ of $\mathbb{Q}$, where ζ is the primitive third root of unity $e^{2\pi i/3}$. From $x^3 - 1 = (x-1)(x^2 + x + 1)$, we can deduce that ζ is a root of the irreducible polynomial $x^2 + x + 1 \in \mathbb{Q}[x]$, and so it is the minimal polynomial of ζ. Thus, it follows from Theorem 2.4 that $[\mathbb{Q}(\zeta) : \mathbb{Q}] = \deg m(x) = 2$ and also that $\{1, \zeta\}$ is a basis for $\mathbb{Q}(\zeta)$ as a vector space over $\mathbb{Q}$. It turns out that we can write $\mathbb{Q}(\zeta)$ as a simple extension of the field $\mathbb{Q}$ by an element different from ζ. For instance, let us verify that

$$\mathbb{Q}(\zeta) = \mathbb{Q}(\sqrt{-3}).$$

To argue the inclusion, $\mathbb{Q}(\zeta) \subseteq \mathbb{Q}(\sqrt{-3})$, it suffices to write ζ as a rational expression of $\sqrt{-3}$:

$$\zeta = e^{2\pi i/3} = -\frac{1}{2} + \frac{\sqrt{3}}{2}i = -\frac{1}{2} + \frac{\sqrt{-3}}{2} \in \mathbb{Q}(\sqrt{-3}). \tag{2.1}$$

On the other hand, we can deduce from (2.1) that $\sqrt{-3} = 2\zeta + 1$, which implies the other desired inclusion: $\mathbb{Q}(\sqrt{-3}) \subseteq \mathbb{Q}(\zeta)$. ■

Given a proper field extension L/K, the minimal polynomial $m(x)$ of any element in $L \setminus K$ that is algebraic over K cannot have any root $\alpha \in K$ as otherwise the linear polynomial $x - \alpha \in K[x]$ would be a proper irreducible factor of $m(x)$ in $K[x]$. However, there is always an extension field L of K such that $m(x)$ has a root in L. Let us provide a proof of this result, which is known as Kronecker's Theorem.

Theorem 2.7 (Kronecker's Theorem)**.** *Let K be a field, and let $f(x) \in K[x]$ be a nonconstant polynomial. Then there exists an extension field L of K such that $f(x)$ has a root in L.*

Proof. Let $f(x) \in K[x]$ be a nonconstant polynomial. Since $K[x]$ is a UFD, $f(x)$ has an irreducible factor $p(x) \in K[x]$. It suffices to show that there exists an extension field L in which $p(x)$ has a root. To argue this, note that because $K[x]$ is a UFD, $p(x)$ is prime and so $P := p(x)K[x]$ is a prime ideal. Indeed, P is a maximal ideal because $R[x]$ is a PID. Therefore the quotient ring

$$L := K[x]/P$$

is a field. Consider the map $\psi\colon K \to L$ defined by $\psi(\beta) = \beta + P$ for all $\beta \in K$. It is routine to verify that ψ is a ring homomorphism. In addition, observe that if $\sigma + P = \tau + P$ then $p(x) \mid_{K[x]} \tau - \sigma$, and so $\tau = \sigma$. Hence ψ is injective and, after identifying K with $\psi(K)$, we can assume that K is a subfield of L. Finally, observe that as P is the zero element of the field L, the element $\alpha := x + P \in L$ is a root of $p(x)$: indeed, $p(\alpha) = p(x + P) = p(x) + P = P$. □

Let us illustrate Kronecker's Theorem with a simple example.

Example 2.8. Observe that the quadratic polynomial $m(x) := x^2 - 2 \in \mathbb{Q}[x]$ does not have any roots in $\mathbb{Q}$ and, therefore, it is irreducible in $\mathbb{Q}[x]$. However, $m(x)$ has a root α in the extension field $\mathbb{Q}(\sqrt{2})$, namely, $\alpha := \sqrt{2}$.

For a nonconstant polynomial $f(x) \in F[x]$, an extension field E of F is a called a *splitting field* for $f(x)$ over F if the following conditions hold:

- $f(x)$ factors into linear factors in $E[x]$, and
- $E = F(\alpha_1, \alpha_2, \ldots, \alpha_n)$, meaning E is generated by the roots of $f(x)$ over F.

Let us argue the existence and uniqueness of the splitting field of a given polynomial.

Proposition 2.9. *For a field F and any non-constant polynomial $f(x) \in F[x]$, there exists a splitting field E for $f(x)$ over F. Furthermore, this splitting field is unique up to isomorphism.*

Proof of Existence. We proceed by induction on the degree $n = \deg f(x)$. For the base case ($n = 1$), it suffices to observe that if $f(x)$ is linear, the root is in F, which means that $E = F$. For the inductive step, fix $n \in \mathbb{N}$ and assume the statement of the proposition holds when the degree of the polynomial is less than n. By Kronecker's Theorem, there exists an extension K containing a root α_1. Therefore we can write $f(x) = (x - \alpha_1)g(x)$ for some $g(x) \in K[x]$ with $\deg g(x) = n - 1$. By the inductive hypothesis, there exists a splitting field E for $g(x)$. The field $F(\alpha_1, \ldots, \alpha_n) \subseteq E$ is the splitting field for $f(x)$. The uniqueness is left to the reader as an exercise.

□

An *intermediate field* of the extension L/K is a subfield F of L that contains K. The degree of extensions is multiplicative in the sense that it satisfies the following tower law.

Proposition 2.10. *Let $K \subseteq F \subseteq L$ be a tower of fields. Then L/K is finite if and only if L/F and F/K are finite, in which case*

$$[L : K] = [L : F][F : K].$$

Proof. Exercise. □

This is the primary tool for proving that certain geometric constructions (like doubling the cube) are impossible.

Proposition 2.11. *Let F, K, and L be fields such that $F \subseteq K \subseteq L$. Then the extension L/F is algebraic if and only if both extensions L/K and K/F are algebraic.*

Proof. For the direct implication, assume that L/F is algebraic. In this case, K/F is also an algebraic extension because every element of K is also an element of L and so a root of a polynomial in $F[x]$. In addition, L/K is algebraic because L/F is algebraic and $F[x] \subseteq K[x]$.

For the reverse implication, assume that both extensions L/K and K/F are algebraic, fix $\alpha \in L$, and let us prove that α is algebraic over F. Since L/K is algebraic, α is a root of a nonzero polynomial $p_0(x) := x^n + \sum_{i=0}^{n-1} a_i x^i$ for some $a_0, \ldots, a_{n-1} \in K$. Set $K_j := F(a_0, \ldots, a_{j-1})$ for every $j \in [\![1, n]\!]$. By the direction already proved, for each $j \in [\![1, n]\!]$, the extension $K_j(a_j)/K_j$ is algebraic and so $[K_j(a_j) : K_j] < \infty$ by Corollary 2.5 and, by the same corollary, $[K_0(\alpha) : K_0] < \infty$. Thus,

$$[K_0(\alpha) : F] = [K_0(\alpha) : K_0][K_0 : F] = [K_0(\alpha) : K_0] \cdot \sum_{j=1}^{k} [K_j(a_j) : K_j] < \infty.$$

Since the field extension $K_0(\alpha)/F$ is finite, it must be algebraic. In particular, α is algebraic over F. Hence K/F is an algebraic extension. □

It turns out that the algebraic extensions are precisely those generated by finitely many algebraic elements.

Proposition 2.12. *Let L/K be a field extension. Then L/K is finite if and only if there exist elements $\alpha_1, \ldots, \alpha_n \in L$ that are algebraic over K and $L = K(\alpha_1, \ldots, \alpha_n)$.*

Proof. For the direct implication, assume that L/K is a finite extension of degree $d = [L : K]$ and let $\{\alpha_1, \ldots, \alpha_d\}$ be a basis for L as a K-vector space. Since this set generates L as a vector space, it certainly follows that $L = K(\alpha_1, \ldots, \alpha_d)$. Now fix $i \in [\![1, n]\!]$, and let us check that $\alpha_i \in L$ is algebraic over K: indeed, $\{1, \alpha_i, \alpha_i^2, \ldots, \alpha_i^d\}$ is linearly dependent over K as it contains $d+1$ vectors and $\dim_K L = d$, so there exist $c_0, c_1, \ldots, c_d \in K$, not all zero, such that $\sum_{j=0}^{d} c_j \alpha_i^j = 0$, implying that α_i is a root of the non-constant polynomial $\sum_{j=0}^{d} c_j x^j \in K[x]$.

For the reverse implication, that $L = K(\alpha_1, \ldots, \alpha_n)$, where $\alpha_1, \ldots, \alpha_n$ are algebraic over K. We proceed by induction on n. For the base case $n = 1$, the extension $K(\alpha_1)/K$ is simple. Since α_1 is algebraic, let $p(x)$ be its minimal polynomial of degree d_1. Then $K(\alpha_1) \cong K[x]/(p(x))$, which has a K-basis $\{1, \alpha_1, \ldots, \alpha_1^{d_1 - 1}\}$. Thus, $[K(\alpha_1) : K] = d_1 < \infty$. Now assume the result holds for $n-1$ elements. Let $F = K(\alpha_1, \ldots, \alpha_{n-1})$. By the inductive hypothesis, $[F : K] < \infty$. Since α_n is algebraic over K, it is necessarily algebraic over the larger field F. By the base case, $[F(\alpha_n) : F] < \infty$. By Proposition 2.10,

$$[L : K] = [F(\alpha_n) : F][F : K].$$

As both terms on the right-hand side are finite, their product is finite. Since $L = F(\alpha_n)$, we conclude that $[L : K] < \infty$. □

2.2 Separable Extensions and Primitive Element Theorem

In this section, we introduce separable extension fields and prove the Primitive Element Theorem, which will allows us to conclude that every finite field extension of $\mathbb{Q}$ is a simple extension.

2.2.1 Separable Extensions

In the context of abstract algebra, the derivative is a purely algebraic map that does not require the notion of limits. It serves as a diagnostic tool for the multiplicity of roots.

Definition 2.13. Let K be a field and let $f(x) = \sum_{i=0}^{n} c_i x^i \in K[x]$. The *formal derivative* of $f(x)$, denoted by $f'(x)$ or $Df(x)$, is the polynomial

$$f'(x) = \sum_{i=1}^{n} i c_i x^{i-1} \in K[x].$$

The main utility of the formal derivative lies in the following property regarding root multiplicity.

Proposition 2.14. *Let K be a field. A nonconstant polynomial $f(x) \in K[x]$ has a multiple root in some extension field if and only if $\gcd(f(x), f'(x)) \neq 1$ in $K[x]$.*

Proof. Suppose α is a multiple root of $f(x)$ in its splitting field. Then $f(x) = (x-\alpha)^2 g(x)$ for some polynomial $g(x)$. Taking the formal derivative using the product rule (which holds algebraically), we have

$$f'(x) = 2(x-\alpha)g(x) + (x-\alpha)^2 g'(x) = (x-\alpha)\big(2g(x) + (x-\alpha)g'(x)\big).$$

Thus, $x - \alpha$ is a common factor of $f(x)$ and $f'(x)$ in the splitting field, implying their greatest common divisor in $K[x]$ is nonconstant.

Conversely, if $d(x) = \gcd(f(x), f'(x))$ is nonconstant, then any root α of $d(x)$ is a root of both $f(x)$ and $f'(x)$. Writing $f(x) = (x-\alpha)h(x)$, we find $f'(x) = h(x) + (x-\alpha)h'(x)$. Since $f'(\alpha) = 0$, it follows that $h(\alpha) = 0$, which means $(x-\alpha)$ divides $h(x)$. Therefore $(x-\alpha)^2$ divides $f(x)$. □

Our next goal is to introduce separable extensions. First, we introduce separable polynomials and discuss how we can use formal derivatives as a tool to determine whether a polynomial is separable. An irreducible polynomial $p(x) \in K[x]$ is said to be *separable* if it has no multiple roots in its splitting field.

By the previous proposition, an irreducible polynomial $p(x)$ is separable if and only if $p'(x) \neq 0$.

Definition 2.15. A field extension L/K is called *separable* if every element of L is separable over K.

For a field F of characteristic zero and a nonconstant polynomial $p(x) \in F[x]$, the condition $p'(x) = 0$ is impossible, as the leading coefficient nc_n cannot be zero for $c_n \neq 0$ and $n \in [\![1, \deg(p)]\!]$. Thus, for fields of characteristic zero, such as $\mathbb{Q}$ and its extensions, we never encounter the pathological behavior of multiple roots for irreducible polynomials.

Proposition 2.16. *Let K be a field of characteristic zero. Every finite extension L/K of a field K is separable.*

Proof. Let L/K be a finite extension and let $\alpha \in L$. We must show that α is separable over K. Let $p(x) \in K[x]$ be the minimal polynomial of α over K. Recall that a polynomial has a multiple root in its splitting field if and only if it shares a common factor with its formal derivative $p'(x)$.

Suppose $p(x)$ is not separable. Then there exists a root β in the splitting field such that $p(\beta) = 0$ and $p'(\beta) = 0$. This implies that the greatest common divisor $\gcd(p(x), p'(x))$ is a nonconstant polynomial in $K[x]$. However, since $p(x)$ is irreducible, its only factors in $K[x]$ are 1 and itself (up to units). Thus, we must have $p(x) \mid p'(x)$.In any field, the degree of the derivative satisfies $\deg(p') \leq \deg(p) - 1$. The only way for an irreducible polynomial to divide its derivative is if $p'(x)$ is the zero polynomial. Let $p(x) = \sum_{i=0}^{n} a_i x^i$. Then

$$p'(x) = \sum_{i=1}^{n} i a_i x^{i-1}.$$

For $p'(x) = 0$, each coefficient ia_i must be zero. Since we are in a field of characteristic zero, $i \cdot 1 \neq 0$ for all $i \in [\![1, n]\!]$. Therefore, we must have $a_i = 0$ for all $i \geq 1$. This would imply that $p(x) = a_0$ is a constant polynomial, which contradicts the fact that it is the minimal polynomial of α.Thus, $p'(x)$ cannot be zero, $p(x)$ cannot divide $p'(x)$, and $p(x)$ must have no multiple roots. We conclude that α is separable over K, and consequently, L/K is a separable extension. □

Proposition 2.17. *Let L/K be an algebraic field extension. If K has characteristic 0, then the extension L/K is separable.*

Proof. Suppose first that $K/\mathbb{Q}$ is normal, and let $\sigma\colon K \to \mathbb{C}$ be a $\mathbb{Q}$-embedding. Take $\alpha \in K$, and let $m_\alpha(x) \in \mathbb{Q}[x]$ be the minimal polynomial of α over $\mathbb{Q}$. By the previous lemma, $\sigma(\alpha)$ is also a root of $m_\alpha(x)$. Since $K/\mathbb{Q}$ is normal and $m_\alpha(x)$ has the root α in K, the polynomial $m_\alpha(x)$ splits completely in $K[x]$. In particular, every root of $m_\alpha(x)$ belongs to K, and so $\sigma(\alpha) \in K$. As this holds for every $\alpha \in K$, we obtain $\sigma(K) \subseteq K$.

Conversely, suppose that $\sigma(K) \subseteq K$ for every $\mathbb{Q}$-embedding $\sigma\colon K \to \mathbb{C}$. Let $f(x) \in \mathbb{Q}[x]$ be an irreducible polynomial having a root $\alpha \in K$. We show that $f(x)$ splits completely in $K[x]$. Let $\beta \in \mathbb{C}$ be any root of $f(x)$. Since $f(x)$ is irreducible over $\mathbb{Q}$, the assignment $\alpha \mapsto \beta$ determines a $\mathbb{Q}$-isomorphism $\mathbb{Q}(\alpha) \to \mathbb{Q}(\beta)$. As we are working in characteristic zero, this isomorphism extends to a $\mathbb{Q}$-embedding $\sigma\colon K \to \mathbb{C}$. By hypothesis, $\sigma(K) \subseteq K$, and therefore $\beta = \sigma(\alpha) \in K$. Thus every root of $f(x)$ belongs to K, which means that $f(x)$ splits completely in $K[x]$. Hence $K/\mathbb{Q}$ is normal. □

It turns out that every finite separable extension is simple, and this result is known as the Primitive Element Theorem.

Theorem 2.18 (Primitive Element Theorem)**.** *If L/K is a finite separable field extension, then there exists $\theta \in L$ such that $L = K(\theta)$.*

Proof. If K is a finite field, then so is L and so the multiplicative group $L^\times$ is cyclic. If θ is a generator of the group $L^\times$ then $L = K(\theta)$. Therefore we assume K is infinite.

As the extension L/K is finite, L is the extension field of K by finitely many algebraic elements. Thus, it suffices to assume that

$$L = K(\alpha, \beta)$$

for some $\alpha, \beta \in L$ and prove that we can pick $\kappa \in K$ such that $L = K(\alpha + \kappa\beta)$. To do so, let $A(x), B(x) \in K[x]$ be the minimal polynomials of α and β, respectively. Set $m := \deg A(x)$ and $n := \deg B(x)$, and let $\alpha = \alpha_1, \alpha_2, \ldots, \alpha_m$ and $\beta = \beta_1, \beta_2, \ldots \beta_n$ be the roots of $A(x)$ and $B(x)$, respectively. Now pick $\kappa \in K$ such that $\kappa \neq \frac{\alpha_i - \alpha}{\beta - \beta_j}$ for any pair $(i, j) \in [\![1, m]\!] \times [\![1, n]\!]$ with $j \neq 1$, and then set $\gamma := \alpha + \kappa\beta \in L$. Let us show that $L = K(\gamma)$. As $\gamma \in L$, the inclusion $K(\gamma) \subseteq L$ holds. For the reverse inclusion, set $F(x) := A(\gamma - \kappa x) \in K(\gamma)[x]$ and observe that $F(\beta_1) = F(\beta) = A(\alpha) = 0$, while $F(\beta_j) = A(\gamma - \kappa\beta_j) \neq 0$ when $j \geq 2$ because the intersection

$$\{\alpha_i : i \in [\![1, m]\!]\} \cap \{\alpha + q(\beta - \beta_j) : j \in [\![1, n]\!]\}$$

is empty by our choice of κ. Then the only common root of $F(x)$ and $B(x)$ in L is β_1 and, as the extension L/K is separable, $\gcd(F(x), B(x)) = x - \beta$. Thus, from the fact that $F(x), B(x) \in K(\gamma)[x]$, we deduce that $x - \beta \in \gcd(F(x), B(x)) \in K(\gamma)[x]$, which implies that $\beta \in K(\gamma)$. In addition, $\alpha = (\alpha + \kappa\beta) - \kappa\beta \in K(\gamma)$. Hence $L = K(\alpha, \beta) \subseteq K(\gamma)$, which completes the proof. □

As $\mathbb{Q}$ is a field of characteristic zero, any algebraic extension of $\mathbb{Q}$ is separable. Then, in light of the Primitive Theorem, every finite extension field of $\mathbb{Q}$ has the form $\mathbb{Q}(\alpha)$ for some algebraic number α,

Corollary 2.19. *Every finite field extension $L/\mathbb{Q}$ is simple.*

2.3 Number Fields and Rings of Integers

In this section, we formally introduced the most relevant arithmetic objects we are interested in here: algebraic number fields and their corresponding rings of integers.

Definition 2.20. A subfield K of $\mathbb{C}$ is called an *algebraic number field* or, simply, a *number field* provided that K is a finite dimensional vector space over $\mathbb{Q}$. If K is a number field, then $[K : \mathbb{Q}]$ denotes the dimension of K as a $\mathbb{Q}$-vector space.

The main algebraic objects we will discuss throughout this course are the subrings of $\mathbb{C}$ we obtain by taking the integral closure of $\mathbb{Z}$ in K.

Definition 2.21. The integral closure of $\mathbb{Z}$ with respect to an algebraic number field K is called the *ring of integers* of K and is denoted by $\mathscr{O}_K$.

Let us take a look at some examples.

Example 2.22. The simplest ring of integers is $\mathbb{Z}$, which is the ring of integers of the number field $\mathbb{Q}$ (as $\mathbb{Z}$ is a UFD, it is integrally closed in its field of fractions $\mathbb{Q}$). ■

The next example concerns the ring of integers of the number field $\mathbb{Q}(i)$, which is known as the *ring of Gaussian integers*.

Example 2.23 (The Gaussian Integers)**.** As i is a root of the irreducible polynomial x^2+1, the field $K := \mathbb{Q}(i)$ is a number field with $[K:\mathbb{Q}] = 2$. It follows from Theorem 2.4 that $\{1, i\}$ is a $\mathbb{Q}$-basis for K as a vector space over $\mathbb{Q}$, so

$$K = \mathbb{Q} + \mathbb{Q}i = \{q + ri : q, r \in \mathbb{Q}\}.$$

Let us prove now that $\mathscr{O}_K = \mathbb{Z}[i]$. To verify that $\mathbb{Z}[i] \subseteq \mathscr{O}_K$, it suffices to observe that if $\alpha := a + bi \in \mathbb{Z}[i]$ for some $a, b \in \mathbb{Z}$, then α is a root of the monic polynomial

$$m(x) = (x-\alpha)(x-\bar{\alpha}) = x^2 - 2ax + (a^2+b^2) \in \mathbb{Z}[x]$$

and so $\alpha \in \mathscr{O}_K$. For the reverse inclusion, take $\alpha \in \mathscr{O}_K \subseteq \mathbb{Q}(i)$ and write $\alpha = q + ri$ for some $q, r \in \mathbb{Q}$. If $r = 0$, then $\alpha = q$ and so the minimal polynomial of α is $p(x) := x - q \in \mathbb{Z}[x]$ and so $\alpha = q \in \mathbb{Z} \subseteq \mathbb{Z}[x]$. Thus, we assume that $r \neq 0$. The fact that $\alpha \in \mathbb{Q}(i)$ ensures that $[\mathbb{Q}(\alpha):\mathbb{Q}]$ divides $[\mathbb{Q}(i):\mathbb{Q}] = 2$. As $\alpha \notin \mathbb{Z}$, its minimal polynomial $m(x)$ has degree 2, and so

$$m_\alpha(x) = (x-\alpha)(x-\bar{\alpha}) = x^2 + 2qx + (q^2+r^2).$$

As $\alpha \in \mathscr{O}_K$, we see that $2q, q^2+r^2 \in \mathbb{Z}$. Therefore $(2q)^2 + 4r^2 \in 4\mathbb{Z}$, and so $4r^2 \in \mathbb{Z}$ or, equivalently, $2r \in \mathbb{Z}$. Now the fact that $4 \mid (2q)^2 + (2r)^2$ ensures that $2q$ and $2r$ have the same parity, but they cannot be odd because 2 is not a quadratic residue modulo 4. Hence $q, r \in \mathbb{Z}$, and so $\alpha = q + ri \in \mathbb{Z}[i]$. Thus, the inclusion $\mathscr{O}_K \subseteq \mathbb{Z}[i]$ also holds, whence

$$\mathscr{O}_K = \mathbb{Z}[i].$$

Example 2.24. Now that we have the norm at our disposal, let us use it to better understand the arithmetic structure of the Gaussian ring of integers. First, let us find its group of units.

Claim 1. $\mathbb{Z}[i]^\times = \{\pm 1, \pm i\} \cong \mathbb{Z}/4\mathbb{Z}$.

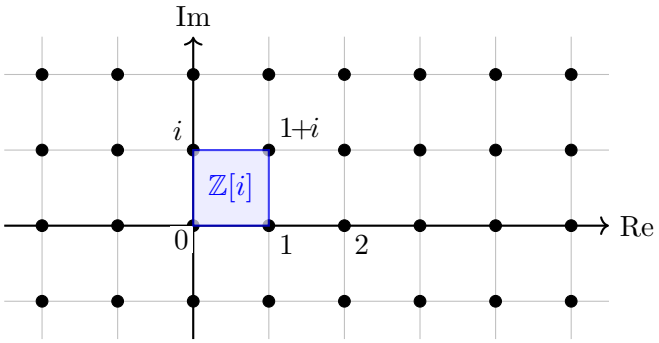

Figure 2.1: Geometric representation of the ring of Gaussian integers $\mathbb{Z}[i]$.

Proof of Claim 1. It is clear that ± 1 and $\pm i$ are all units of $\mathscr{O}_K$. Before we argue that these are the only units, it is convenient to define $N\colon \mathscr{O}_K \to \mathbb{N}_0$ as

$$\mathrm{N}(\alpha) = \alpha\bar{\alpha} = |\alpha|^2$$

for all $\alpha \in \mathscr{O}_K$. nd observe that

$$\mathrm{N}(\alpha\beta) = (\alpha\beta)(\overline{\alpha\beta}) = (\alpha\bar{\alpha})(\beta\bar{\beta}) = \mathrm{N}(\alpha)N(\beta)$$

for all $\alpha, \beta \in \mathscr{O}_K$. Now take $u = a + bi \in \mathscr{O}_K^\times$ for some $a, b \in \mathbb{Z}$ and then write $uv = 1$ for some $v \in \mathscr{O}_K$. Then $1 = \mathrm{N}(uv) = \mathrm{N}(u)\,\mathrm{N}(v)$, and so the fact that $\mathrm{N}(u), \mathrm{N}(v) \in \mathbb{N}_0$ ensures that $a^2 + b^2 = \mathrm{N}(u) = 1$. From this, we deduce that $u \in \{\pm 1, \pm i\}$. Hence we conclude that

$$\mathscr{O}_K^\times = \{\pm 1, \pm i\} \cong \mathbb{Z}/4\mathbb{Z}.$$

As a result, Claim 1 is already established.

It turns out that $\mathbb{Z}[i]$ is a UFD. Indeed, let us argue the following stronger claim.

Claim 2. $\mathbb{Z}[i]$ is a Euclidean domain.

Proof of Claim 2. We need to argue that, for any elements $\alpha, \beta \in \mathscr{O}_K$ with $\beta \neq 0$, we can write $\alpha = q\beta + r$ for some $q, r \in \mathscr{O}_K$ such that either $r = 0$ or $\mathrm{N}(r) < \mathrm{N}(\beta)$. To do so, fix $\alpha, \beta \in \mathscr{O}_K$ with $\beta \neq 0$, and write $\alpha/\beta = q_1 + iq_2$, where $q_1, q_2 \in \mathbb{Q}$. Now take $m, n \in \mathbb{Z}$ such that $|q_1 - m| \leq 1/2$ and $|q_2 - n| \leq 1/2$, and then set $q = m + in \in \mathscr{O}_K$ and $r = \alpha - q\beta \in \mathbb{Z}[i]$. Observe that

$$\mathrm{N}(r) = \mathrm{N}(\beta)\,\mathrm{N}\left(\frac{\alpha}{\beta} - q\right) = \mathrm{N}(\beta)\left(|q_1 - m|^2 + |q_2 - n|^2\right) \leq \frac{\mathrm{N}(\beta)}{2} < \mathrm{N}(\beta).$$

As a consequence, we conclude that $\mathscr{O}_K$ is a Euclidean domain with respect to the norm N.

In particular, $\mathscr{O}_K$ is a UFD. Thus, the irreducibles of $\mathbb{Z}[i]$ are precisely its prime elements. The Gaussian primes can be classified based on how the standard "rational" primes $p \in \mathbb{Z}$ behave in the complex plane. ■

We conclude this section discussing the pure cubic field $\mathbb{Q}(\sqrt[3]{2})$, the simplest and most illuminating example of a cubic number field.

Example 2.25. Consider the number field $K := \mathbb{Q}(\theta)$, where $\theta := \sqrt[3]{2}$. Observe that the minimal polynomial of θ is

$$m(x) = x^3 - 2,$$

which is irreducible by Eisenstein's Criterion with $p = 2$. This immediately confirms that $[K : \mathbb{Q}] = 3$. The most natural basis for K as a vector space over $\mathbb{Q}$ is the power basis $\mathscr{B} = \{1, \theta, \theta^2\}$, which is indeed a basis by Theorem 1.13. As a consequence, we can write

$$K = \mathbb{Q} + \mathbb{Q}\theta + \mathbb{Q}\theta^2.$$

Next, we turn our attention to determine the ring of integers $\mathscr{O}_K$. Let $\alpha = a + b\theta + c\theta^2 \in K$ with $a, b, c \in \mathbb{Q}$. Observe that if $\theta := \theta^{(1)}, \theta^{(2)}$, and $\theta^{(3)}$ are the roots of $m(x)$, then for any index $i \in [\![1, 3]\!]$ there is a unique field isomorphism $\eta_i \colon \mathbb{Q}(\theta) \to \mathbb{Q}(\theta^{(i)})$ such that $\eta_i(\theta) = \theta^{(i)}$. Define a map $N \colon K \to \mathbb{Q}$ as follows:

$$\mathrm{N}(\alpha) := \eta_1(\alpha)\eta_2(\alpha)\eta_3(\alpha)$$

for all $\alpha \in K$ (cf. the norm N we define in Example 2.23). As an exercise, one can verify the following two facts:

(i) $\mathrm{N}(a + b\theta + c\theta^2) = a^3 + 2b^3 + 4c^3 - 6abc$ for all $a, b, c \in \mathbb{Q}$,

(ii) $\mathrm{N}(\mathscr{O}_K) \subseteq \mathbb{Z}$.

Claim 1. $\mathscr{O}_K = \mathbb{Z}[\sqrt[3]{2}]$.

Claim 2. It is clear that $\mathbb{Z}[\sqrt[3]{2}] \subseteq \mathscr{O}_K$. For the reverse inclusion, take $\alpha = a + b\theta + c\theta^2 \in \mathscr{O}_K$, where $a, b, c \in \mathbb{Q}$. Write $a = A/d$, $b = B/d$, and $c = C/d$ for some $A, B, C, d \in \mathbb{Z}$ with $d \neq 0$. After subsituting (a, b, c) by $(A/d, B/d, C/d)$ in condition (i), condition (ii) ensures that

$$A^3 + 2B^3 + 4C^3 - 6ABC \equiv 0 \pmod{d^3}.$$

For $d = 2$, we obtain that $A^3 \equiv 0 \pmod 2$ and so A is even. Write $A = 2A'$ for some $A' \in \mathbb{Z}$. Substituting back leads to $2B^3 \equiv 0 \pmod 4$, so B is also even. This recursion shows $a, b, c \in \mathbb{Z}$. Thus,

$$\mathscr{O}_K = \mathbb{Z}[\sqrt[3]{2}].$$

Claim 2. $\mathscr{O}_K^\times = \{\pm(1 + \sqrt[3]{2} + \sqrt[3]{4})^n : n \in \mathbb{Z}\}$.

Proof of Claim 2. An element $\alpha \in \mathscr{O}_K$ is a unit if $|N_{K/\mathbb{Q}}(\alpha)| = 1$. By the identity $x^3 - y^3 = (x - y)(x^2 + xy + y^2)$, we substitute $x = \sqrt[3]{2}$ and $y = 1$:

$$1 = (\sqrt[3]{2})^3 - 1^3 = (\sqrt[3]{2} - 1)(\sqrt[3]{4} + \sqrt[3]{2} + 1).$$

This identifies $\varepsilon = 1 + \sqrt[3]{2} + \sqrt[3]{4}$ as a unit. Since $K \cap \mathbb{R} = K$ and the only roots of unity in $\mathbb{R}$ are ± 1, and since $\varepsilon > 1$ is the smallest unit obtained by small integer search in the norm equation,

$$\mathscr{O}_K^\times = \{\pm(1 + \sqrt[3]{2} + \sqrt[3]{4})^n : n \in \mathbb{Z}\}.$$

2.4 Quadratic Number Fields

In the following example we show that a number field K is a 2-dimensional vector space over $\mathbb{Q}$ if and only if $K = \mathbb{Q}(\sqrt{d})$ for some square-free $d \in \mathbb{Z}$ with $d \neq 1$.

Example 2.26. First, assume that K is a number field with $[K : \mathbb{Q}] = 2$. In light of the Primitive Element Theorem, we can take $\alpha \in K$ such that $K = \mathbb{Q}(\alpha)$. Because $[K : \mathbb{Q}] = 2$, the minimal polynomial of α over $\mathbb{Q}$ must have the form $m(x) := x^2 + bx + c$ for some $b, c \in \mathbb{Q}$. The roots of $m(x)$ are the following:

$$\alpha = \frac{-b \pm \sqrt{b^2 - 4c}}{2}.$$

Let $D = b^2 - 4c$. Since $\alpha \notin \mathbb{Q}$ (otherwise the degree would be 1), the rational D cannot be a square in $\mathbb{Q}$. From the expression for α, it is clear that $\alpha \in \mathbb{Q}(\sqrt{D})$. Conversely, $\sqrt{D} = \pm(2\alpha + b)$, so $\sqrt{D} \in \mathbb{Q}(\alpha)$. Thus,

$$K = \mathbb{Q}(\alpha) = \mathbb{Q}(\sqrt{D}).$$

Now write $D = \frac{p}{q}$ for $p, q \in \mathbb{Z}$ and $q \neq 0$. Then

$$\sqrt{D} = \sqrt{\frac{pq}{q^2}} = \frac{1}{|q|}\sqrt{pq}.$$

Thus, $\mathbb{Q}(\sqrt{D}) = \mathbb{Q}(\sqrt{pq})$. Let $N = pq$ and write $N = s^2 d$ for some $s, d \in \mathbb{Z}$ such that d is square-free. Then $\sqrt{N} = \sqrt{s^2 d} = s\sqrt{d}$. Since $s \in \mathbb{Z}$, it follows that

$$K = \mathbb{Q}(\sqrt{D}) = \mathbb{Q}(\sqrt{N}) = \mathbb{Q}(\sqrt{d}).$$

We just need to observe now that $s \neq 1$ as otherwise $K = \sqrt{1} = \mathbb{Q}$.

Conversely, let d be a (nonzero) square-free integer with $d \neq 1$, and let us argue that $K := \mathbb{Q}(\sqrt{d})$ is a number field such that $\{1, \sqrt{d}\}$ is a basis for K as a vector space over $\mathbb{Q}$. To determine the minimal polynomial of $\sqrt{d}$, we consider the following two cases.

- $d = -1$. In this case, $\sqrt{d} = i$, which is a root of the monic irreducible polynomial $x^2 + 1 \in \mathbb{Z}[x]$. Hence $x^2 + 1$ is the minimal polynomial of $\sqrt{d}$.

- $d \neq -1$. In this case, $|d| \geq 2$. Then we can take $p \in \mathbb{P}$ such that $p \mid d$ but $p^2 \nmid d$, whence the polynomial $x^2 - d \in \mathbb{Z}[x]$ is irreducible by Eisenstein's criterion at the prime ideal (p). Therefore $x^2 - d$ must be the minimal polynomial of $\sqrt{d}$.

Theorem 2.4 ensures that K is a number field such that $\{1, \sqrt{d}\}$ is a basis for K as a vector space over $\mathbb{Q}$. Hence we can write

$$K = \mathbb{Q} + \mathbb{Q}\sqrt{d} = \{q + r\sqrt{d} : q, r \in \mathbb{Q}\}.$$

■

2.5 Exercises – Algebraic Field Extensions and Number Fields

Throughout the list of exercises, assume that L/K is a field extension.

Exercise 2.1. Prove that, for any $\alpha \in L$ is algebraic over K, there is a unique monic polynomial $m_\alpha(x) \in K[x]$ that vanishes at α and divides any other polynomial in $K[x]$ vanishing at α.

Exercise 2.2. For distinct primes p and q, find $\alpha \in \mathbf{A}$ such that $\mathbb{Q}(\sqrt{p}, \sqrt{q}) = \mathbb{Q}(\alpha)$.

Exercise 2.3. Let $K \subseteq F \subseteq L$ be a tower of fields. Prove that L/K is finite if and only if L/F and F/K are finite, in which case $[L : K] = [L : F][F : K]$.

Exercise 2.4. Let L/K be a field extension. Prove that L/K is finite if and only if there exist elements $\alpha_1, \ldots, \alpha_n \in L$ that are algebraic over K and $L = K(\alpha_1, \ldots, \alpha_n)$.

Exercise 2.5. Determine the group of units of $\mathbb{Z}[\sqrt{-3}]$, the Eisenstein ring of integers.

Exercise 2.6.

1. Prove that $\mathbb{Z}[\sqrt{2}]$ is a Euclidean domain.
2. Prove that $\mathbb{Z}[\sqrt[3]{2}]$ is a Euclidean domain.

Exercise 2.7. Prove that $\mathbb{Z}[\sqrt{-5}]$ is not a UFD.

Chapter 3

The Additive Structure of Rings of Integers

In this section, we study the additive structure of rings of integers. First, we introduce the norm and trace of a number field, which will be crucial tools in what follows. Then we prove that the ring of integers $\mathscr{O}_K$ is a free $\mathbb{Z}$-module of rank $[K : \mathbb{Q}]$.

3.1 $\mathbb{Q}$-Embeddings, Conjugates, and Normality

Let K be a number field of degree $n = [K : \mathbb{Q}]$. A $\mathbb{Q}$-*embedding* of K is an injective field homomorphism $\sigma\colon K \to \mathbb{C}$ such that $\sigma|_{\mathbb{Q}} = \mathrm{id}_{\mathbb{Q}}$. Let us take a look at some examples.

Lemma 3.1. *Let $\sigma\colon K \to \mathbb{C}$ be an embedding of a number field K, and let $m(x) \in \mathbb{Q}[x]$. If $\rho \in K$ is a root of $m(x)$, so is $\sigma(\rho)$.*

Proof. Write $m(x) = \sum_{i=0}^{d} c_i x^i \in \mathbb{Q}[x]$. Since σ is a $\mathbb{Q}$-embedding, $\sigma(c_i) = c_i$ for every $i \in [\![0, d]\!]$, whence

$$m(\sigma(\rho)) = \sum_{i=0}^{d} c_i \sigma(\rho)^i = \sum_{i=0}^{d} \sigma(c_i \rho^i) = \sigma\Big(\sum_{i=0}^{d} c_i \rho^i \Big) = \sigma(m(\rho)) = \sigma(0) = 0.$$

Thus, $\sigma(\rho)$ is also a root of $m(x)$. □

As a consequence of Lemma 3.1, every $\mathbb{Q}$-embedding of a number field $\mathbb{Q}(\alpha)$ permutes the roots of the minimal polynomial of α. Let us take a look at two examples.

Example 3.2. Consider the Gaussian number field $K = \mathbb{Q}(i)$. If $\sigma\colon K \to \mathbb{C}$ is a $\mathbb{Q}$-embedding of K, then $\sigma(i)$ must be a root of $x^2 + 1$, which means that $\sigma(i) = i$ or $\sigma(i) = -i$. If $\sigma(i) = i$, then $\sigma\colon \mathbb{Q}(i) \to \mathbb{Q}(i)$ is the identity field homomorphism. Otherwise, $\sigma(i) = -i$, in which case, σ is the conjugation field isomorphism, which means that $\sigma(q + ri) = q - ri$ for all $q, r \in \mathbb{Q}$.

Example 3.3. Consider the number field $K = \mathbb{Q}(\alpha)$, where $\alpha := \sqrt[3]{2}$. Now let $\zeta = e^{2\pi i/3}$. The minimal polynomial of α is $x^3 - 2$, whose roots are α, $\zeta\alpha$, and $\zeta^2\alpha$. Thus,if σ is a $\mathbb{Q}$-embedding, then $\sigma(\alpha) \in \{\alpha, \zeta\alpha, \zeta^2\alpha\}$. We can actually check that, for each $i \in [\![1, 3]\!]$, the map $\sigma_i \colon K \to \mathbb{C}$ fixing $\mathbb{Q}$ and satisfying $\sigma_i(\alpha) = \zeta^i\alpha$ is a $\mathbb{Q}$-embedding. Hence the $\mathbb{Q}$-embeddigns of K are σ_1, σ_2, and σ_3.

Let $K = \mathbb{Q}(\alpha)$ be a number field of degree n. Let $f(x) \in \mathbb{Q}[x]$ be the minimal polynomial of α, and let $\alpha_1, \alpha_2, \ldots, \alpha_n \in \mathbb{C}$ be the n distinct roots of $f(x)$. The elements $\alpha_1, \ldots, \alpha_n$ are called the *conjugates* of α.

Theorem 3.4. *For an algebraic $\alpha \in \mathbb{C}$, consider the number field $K := \mathbb{Q}(\alpha)$, and let $\alpha_1, \ldots, \alpha_n$ be the conjugates of α, where $n := [K : \mathbb{Q}]$. Then the following statements hold.*

1. *For every $i \in [\![1, n]\!]$, the map $\sigma_i \colon K \to \mathbb{Q}(\alpha_i) \subseteq \mathbb{C}$ defined by the assignment $\sigma_i(\alpha) = \alpha_i$ is a field isomorphism and so a $\mathbb{Q}$-embedding.*

2. *There are precisely n $\mathbb{Q}$-embeddings of K into $\mathbb{C}$, namely, $\sigma_1, \ldots, \sigma_n$.*

Proof. Exercise. □

Let us introduce another relevant type of field extensions.

Definition 3.5. An algebraic extension L/K is called a *normal extension* if every irreducible polynomial $f(x) \in K[x]$ that has at least one root in L actually splits completely in $L[x]$.

Normal extensions can be characterized using $\mathbb{Q}$-embedding as follows.

Proposition 3.6. *For a number field K, the following conditions are equivalent.*

(a) $K/\mathbb{Q}$ is a normal extension.

(b) $\sigma(K) \subseteq K$ for every $\mathbb{Q}$-embedding $\sigma \colon K \to \mathbb{C}$.

Proof. First, assume that $K/\mathbb{Q}$ is normal, and let $\sigma \colon K \to \mathbb{C}$ be a $\mathbb{Q}$-embedding. Take $\alpha \in K$, and let $m(x) \in \mathbb{Q}[x]$ be the minimal polynomial of α over $\mathbb{Q}$. By Lemma 3.1, $\sigma(\alpha)$ is also a root of $m(x)$. Since $K/\mathbb{Q}$ is normal and $m(x)$ has the root α in K, the polynomial $m(x)$ splits completely in $K[x]$. In particular, every root of $m_\alpha(x)$ belongs to K, and so $\sigma(\alpha) \in K$. As this holds for every $\alpha \in K$, we obtain $\sigma(K) \subseteq K$.

Now assume that $\sigma(K) \subseteq K$ for every $\mathbb{Q}$-embedding $\sigma \colon K \to \mathbb{C}$. Let $f(x) \in \mathbb{Q}[x]$ be an irreducible polynomial having a root $\alpha \in K$. We show that $f(x)$ splits completely in $K[x]$. Let $\beta \in \mathbb{C}$ be any root of $f(x)$. Since $f(x)$ is irreducible over $\mathbb{Q}$, the assignment $\alpha \mapsto \beta$ determines a $\mathbb{Q}$-isomorphism $\mathbb{Q}(\alpha) \to \mathbb{Q}(\beta)$. As we are working in characteristic zero, this isomorphism extends to a $\mathbb{Q}$-embedding $\sigma \colon K \to \mathbb{C}$. By hypothesis, $\sigma(K) \subseteq K$, and therefore $\beta = \sigma(\alpha) \in K$. Thus every root of $f(x)$ belongs to K, which means that $f(x)$ splits completely in $K[x]$. Hence $K/\mathbb{Q}$ is normal. □

We conclude this section with the following examples.

Example 3.7. Set $L = \mathbb{Q}(\sqrt{2}, \sqrt{3})$. The minimal polynomials for the generators are $x^2 - 2$ (roots $\pm\sqrt{2}$) and $x^2 - 3$ (roots $\pm\sqrt{3}$). Since all these roots are in L, any irreducible polynomial having a root in L will split completely in L. ■

Example 3.8. Set $L = \mathbb{Q}(\sqrt[3]{2})$.The minimal polynomial of $\sqrt[3]{2}$ is $f(x) = x^3 - 2$. While $\sqrt[3]{2} \in L$, the other two roots are complex: $\sqrt[3]{2}\omega$ and $\sqrt[3]{2}\omega^2$ (where ω is a primitive cube root of unity). Since these complex roots are not in $L \subset \mathbb{R}$, the extension is not normal. ■

Remark 3.9. In the context of normal extensions, every $\mathbb{Q}$-embedding is an element of the automorphism group $\mathrm{Aut}(K/\mathbb{Q})$. For such extensions, the study of embeddings is equivalent to the study of the Galois group.

Next we prove the Dedekind's lemma on the independence of characters as it is convenient to establish our next result.

Theorem 3.10 (Dedekind's Lemma)**.** *Let E and F be fields. Let $\sigma_1, \ldots, \sigma_n$ be distinct field homomorphisms from E to F. Then $\sigma_1, \ldots, \sigma_n$ are linearly independent over F.*

Proof. Exercise. □

For a number field K with $\mathbb{Q}$-basis $\omega_1, \ldots, \omega_n$ and $\mathbb{Q}$-embeddings $\sigma_1, \ldots, \sigma_n \colon K \to \mathbb{C}$, the matrix $(\sigma_j(\omega_i))_{i,j}$ will play a relevant role in coming sections. As an application of Dedekind's lemma, such a matrix is invertible.

Lemma 3.11. *Let K be a number field with $\mathbb{Q}$-basis $\omega_1, \ldots, \omega_n$, and let $\sigma_1, \ldots, \sigma_n \colon K \to \mathbb{C}$ be the $\mathbb{Q}$-embeddings of K. Then the matrix*

$$(\sigma_j(\omega_i))_{i,j}$$

is invertible.

Proof. Let K be a number field of degree n, and let $\mathscr{B} = \{\omega_1, \ldots, \omega_n\}$ be a $\mathbb{Q}$-basis for K. Let $\sigma_1, \ldots, \sigma_n \colon K \to \mathbb{C}$ be the distinct $\mathbb{Q}$-embeddings.

Suppose, for the sake of contradiction, that the matrix $\Omega = (\sigma_j(\omega_i))$ is not invertible. Then the columns of Ω must be linearly dependent over $\mathbb{C}$. Thus, there exist $c_1, \ldots, c_n \in \mathbb{C}$, not all zero, such that for every row $i \in [\![1, n]\!]$:

$$\sum_{j=1}^{n} c_j \sigma_j(\omega_i) = 0.$$

By the linearity of the embeddings σ_j, for any element $\alpha \in K$, we can write α in terms of the basis as $\alpha = \sum_{i=1}^{n} q_i \omega_i$ for some $q_i \in \mathbb{Q}$. Multiplying the above equation by q_i and summing over i, we obtain

$$\sum_{i=1}^{n} q_i \left(\sum_{j=1}^{n} c_j \sigma_j(\omega_i) \right) = \sum_{j=1}^{n} c_j \sigma_j \left(\sum_{i=1}^{n} q_i \omega_i \right) = \sum_{j=1}^{n} c_j \sigma_j(\alpha) = 0.$$

Since this holds for every $\alpha \in K$, we have obtained a nontrivial linear combination of the embeddings that vanishes identically on K:

$$\sum_{j=1}^{n} c_j \sigma_j = 0.$$

However, the Dedekind's lemma states that any set of distinct field homomorphisms from a field K into another field L is linearly independent over L. Because the $\mathbb{Q}$-embeddings $\sigma_1, \ldots, \sigma_n$ are distinct homomorphisms into $\mathbb{C}$, they must be linearly independent. This contradicts our assumption that a nontrivial linear combination vanishes.Therefore, the matrix Ω must be invertible, and its determinant $\det(\Omega)$ is nonzero. □

3.2 Norm and Trace

The main purpose of this section is to introduce the norm and the trace of a number field, and discuss the main properties.

For the rest of this section, we let K be a number field. For each $\alpha \in K$, we can consider the linear operator Φ_α on K given by multiplication by α: the determinant and the trace of Φ_alpha play a crucial role in the investigation of the ring of integers of K. Let us introduce them in a formal way.

Definition 3.12. Let K be an algebraic number field, and for each $\alpha \in K$, consider the linear operator on K given by multiplication by α:

$$\Phi_\alpha \colon K \to K, \quad \textit{where} \quad \Phi_\alpha(\beta) = \alpha\beta$$

for all $\beta \in K$. The *norm* and the *trace* of K are the maps $\mathrm{N}, \mathrm{Tr} \colon K \to \mathbb{Q}$ defined as follows: for all $\alpha \in K$,

$$\mathrm{N}_K(\alpha) = \det(\Phi_\alpha) \quad \text{and} \quad \mathrm{Tr}_K(\alpha) = \mathrm{Tr}_K(\Phi_\alpha).$$

It turns out that Tr_K is linear and N_K is multiplicative.

Proposition 3.13. *For a number field K, the following statements hold.*

1. *The trace of K is a $\mathbb{Q}$-linear map: for all $q, r \in \mathbb{Q}$ and $\alpha, \beta \in K$,*

$$\mathrm{Tr}_K(q\alpha + r\beta) = q\,\mathrm{Tr}_K(\alpha) + r\,\mathrm{Tr}_K(\beta).$$

2. *The norm of K is multiplicative: for all $\alpha, \beta \in K$,*

$$\mathrm{N}_K(\alpha\beta) = \mathrm{N}_K(\alpha)\,\mathrm{N}_K(\beta).$$

Proof. (1) Fix $q, r \in \mathbb{Q}$ and $\alpha, \beta \in K$. For each $\gamma \in K$,

$$\Phi_{q\alpha+r\beta}(\gamma) = (q\alpha + r\beta)\gamma = q(\alpha\gamma) + r(\beta\gamma) = q\Phi_\alpha(\gamma) + r\Phi_\beta(\gamma) = (q\Phi_\alpha + r\Phi_\beta)(\gamma).$$

This implies that $\Phi_{q\alpha+r\beta} = q\Phi_\alpha + r\Phi_\beta$. Using now the linearity of the trace operator in linear algebra,

$$\mathrm{Tr}_K(q\alpha + r\beta) = \mathrm{Tr}(\Phi_{q\alpha+r\beta}) = \mathrm{Tr}(q\Phi_\alpha + r\Phi_\beta) = q\,\mathrm{Tr}(\Phi_\alpha) + r\,\mathrm{Tr}(\Phi_\beta).$$

As a consequence, the trace Tr_K is a linear map.

(2) To argue that the norm N_K is a multiplicative map, fix $\alpha, \beta \in K$. We first observe that, for each $\gamma \in K$,

$$\Phi_{\alpha\beta}(\gamma) = (\alpha\beta)\gamma = \alpha(\beta\gamma) = \Phi_\alpha(\Phi_\beta(\gamma)) = (\Phi_\alpha \circ \Phi_\beta)(\gamma).$$

This shows that $\Phi_{\alpha\beta} = \Phi_\alpha \circ \Phi_\beta$. Using the multiplicative property of the determinant, we can proceed as follows:

$$\mathrm{N}_K(\alpha\beta) = \det(\Phi_{\alpha\beta}) = \det(\Phi_\alpha \circ \Phi_\beta) = \det(\Phi_\alpha)\det(\Phi_\beta) = \mathrm{N}_K(\alpha)\,\mathrm{N}_K(\beta).$$

Thus, the norm is multiplicative, as desired. □

It turns out that both $\mathrm{N}_K(\alpha)$ and $\mathrm{Tr}_K(\alpha)$ are integers when $\alpha \in \mathscr{O}_K$. In its proof we use the Kronecker delta function $\delta_{j,k}$, which is defined by $\delta_{j,k} = 1$ if $j = k$ and $\delta_{j,k} = 0$ otherwise.

Proposition 3.14. *Let K be a number field with ring of integers $\mathscr{O}_K$. Then $\mathrm{Tr}_K(\mathscr{O}_K) \subseteq \mathbb{Z}$ and $\mathrm{N}_K(\mathscr{O}_K) \subseteq \mathbb{Z}$.*

Proof. Set $n := [K : \mathbb{Q}]$ and fix a $\mathbb{Q}$-basis $\{\omega_1, \ldots, \omega_n\}$ for K. Now take $\alpha \in \mathscr{O}_K$ and let $m(x) \in \mathbb{Z}[x]$ be the minimal polynomial of α. Then let $\alpha^{(1)}, \ldots, \alpha^{(n)}$ be the conjugates of α and assume that $\alpha^{(1)} := \alpha$. For each index $i \in [\![1, n]\!]$, write

$$\alpha\omega_i = \sum_{j=1}^{n} q_{i,j}\omega_j, \tag{3.1}$$

where $q_{i,j} \in \mathbb{Q}$ for every $j \in [\![1, n]\!]$. Observe that, for each index $k \in [\![1, n]\!]$, there is a unique field isomorphism $\phi_k \colon \mathbb{Q}(\alpha) \to \mathbb{Q}(\alpha^{(k)})$ fixing $\mathbb{Q}$ such that $\phi_k \colon \alpha \mapsto \alpha^{(k)}$: set $\beta^{(k)} := \phi_k(\beta)$ for all $\beta \in \mathbb{Q}(\alpha)$ and observe that

$$\sum_{j=1}^{n} \delta_{j,k}\alpha^{(j)}\omega_i^{(j)} = \alpha^{(k)}\omega_i^{(k)} = \sum_{j=1}^{n} q_{i,j}\omega_j^{(k)} \tag{3.2}$$

for all $i, k \in [\![1, n]\!]$, where the second equality results from applying ϕ_k to both sides of (3.1). Then we can write the equality (3.2) in compact form as follows:

$$\Omega D = Q\Omega,$$

where $D := (\alpha^{(i)}\delta_{i,j})$, $\Omega = (\omega_i^{(j)})$, and $Q = (q_{i,j})$. We can prove that the matrix Ω is an invertible matrix (see exercises). Thus, $Q = \Omega D \Omega^{-1}$. Because D is the diagonal matrix having $\alpha^{(i)}$ in its (i,i) position for every $i \in [\![1, n]\!]$, we see that

$$\mathrm{N}_K(\alpha) = \det(Q_0) = \prod_{i=1}^{n} \alpha^{(i)} \quad \text{and} \quad \mathrm{Tr}_K(\alpha) = \mathrm{Tr}_K(Q_0) = \sum_{i=1}^{n} \alpha^{(i)}.$$

As $|\sum_{i=1}^{n} \alpha^{(i)}|$ and $|\prod_{i=1}^{n} \alpha^{(i)}|$ are two coefficients of $m(x)$, we conclude that both $\mathrm{N}_K(\alpha)$ and $\mathrm{Tr}_K(\alpha)$ are integers. □

Example 3.15. TODO: Add a computational example about norm and trace...

We can compute the trace and the norm of a number field K in terms of the $\mathbb{Q}$-embeddings of K as follows.

Proposition 3.16. *Let K be a number field with $n := [K : \mathbb{Q}]$, and let $\sigma_1, \dots, \sigma_n \colon K \to \mathbb{C}$ be the n distinct $\mathbb{Q}$-embeddings of K into $\mathbb{C}$. If $\mathrm{Tr}_K, \mathrm{N}_k \colon K \to \mathbb{Q}$ are the trace and norm of K, then*

$$\mathrm{Tr}_K = \sum_{k=1}^{n} \sigma_k \quad \textit{and} \quad \mathrm{N}_K = \prod_{k=1}^{n} \sigma_k.$$

Proof. Take $\alpha \in K$, and let $m_\alpha(x) \in \mathbb{Q}[x]$ be the minimal polynomial of α. Set $d := \deg m_\alpha(x)$ and let $\alpha_1, \dots, \alpha_d$ be the conjugates of α. Let $\Phi_\alpha \colon K \to K$ be the operator that multiplies every element by α, that is, $\Phi_\alpha(\beta) = \alpha\beta$ for all $\beta \in K$, and let $\lambda_1, \dots, \lambda_n$ be the eigenvalues of Φ_α, which are the roots of the characteristic polynomial $\chi_\alpha(x)$ of Φ_α. Then

$$\mathrm{Tr}_K(\alpha) = \mathrm{Tr}(\Phi_\alpha) = \sum_{i=1}^{n} \lambda_i = \frac{n}{d} \sum_{i=1}^{d} \alpha_i \quad \text{and} \quad \mathrm{N}_K(\alpha) = \det(\Phi_\alpha) = \prod_{i=1}^{n} \lambda_i = \Big(\prod_{i=1}^{d} \alpha_i \Big)^{n/d},$$

where both last equalities hold because $\chi_\alpha(x) = m(x)^{n/d}$. Therefore if $\sigma_1, \dots, \sigma_n$ are the $\mathbb{Q}$-embeddings of K into $\mathbb{C}$, then the sequence $\sigma_1(\alpha), \dots, \sigma_n(\alpha)$ contains exactly n/d copies of α_i for every $i \in [\![1, d]\!]$: this is because each of the d $\mathbb{Q}$-embeddings of $\mathbb{Q}(\alpha)$ into $\mathbb{C}$ extends to a $\mathbb{Q}$-embedding $K \to \mathbb{C}$ exactly into n/d distinct manners. Hence

$$\mathrm{Tr}_K(\alpha) = \frac{n}{d} \sum_{i=1}^{d} \alpha_i = \sum_{i=1}^{n} \sigma_i(\alpha) \quad \text{and} \quad \mathrm{N}_K(\alpha) = \Big(\prod_{i=1}^{d} \alpha_i \Big)^{n/d} = \prod_{i=1}^{n} \sigma_i(\alpha).$$

□

3.3 Existence of Integral Basis

In this section, we prove that every ring of integers has an integral basis, which is a basis as a $\mathbb{Z}$-module. In order to do so, we need to understand the $\mathbb{Z}$-modules of a finite-rank free $\mathbb{Z}$-modules.

3.3.1 Submodules of a finite-rank free $\mathbb{Z}$-module

Before examining the structural properties of submodules over the ring of integers, we establish some basic notions and terminology of module theory, generalizing the familiar geometric intuition of vector spaces over fields to modules over a commutative ring with identity.

Let M be an R-module, where R is a commutative ring with identity, and let B be a subset of the R-module M.

- B is said to be *linearly independent* over R if, for any distinct elements $\beta_1, \ldots, \beta_n \in B$ and coefficients $c_1, \ldots, c_n \in R$, the relation $\sum_{i=1}^{n} c_i\beta_i = 0$.
- B is called a *generating set* for M if every element $m \in M$ can be written as $m = \sum_{i=1}^{n} c_i\beta_i$ for some $c_1, \ldots, c_n \in R$ and $\beta_1, \ldots, \beta_n \in B$.
- B is a *basis* for M if every element of M can be uniquely expressed as a finite R-linear combination of elements in B.

An R-module M is called a *free R-module* if it possesses a basis B. Because R is commutative, the cardinality of any basis for a given free R-module M is invariant, and this is defined as the *rank* of M, denoted $\text{rank}_R(M)$. If M is free R-module of finite rank k then $M \cong R^k$.

Example 3.17. For a commutative ring R with identity, the standard R-module $M = R^k$ is free of rank k over R with the canonical basis $\{e_1, e_2, \ldots, e_k\}$. In particular, $\mathbb{Z}^k$ is a free $\mathbb{Z}$-module of rank k.

Example 3.18. Let K be a number field of degree $d = [K : \mathbb{Q}]$, and let $\mathscr{O}_K$ denotes its ring of integers of K. It is clear that $\mathscr{O}_K$ is a $\mathbb{Z}$-module. Moreover, we will prove in this section that $\mathscr{O}_K$ is a free $\mathbb{Z}$-module of rank d. A $\mathbb{Z}$-basis for $\mathscr{O}_K$ as a $\mathbb{Z}$-module is called an integral basis for K, yielding an isomorphism of abelian groups $\mathscr{O}_K \cong \mathbb{Z}^d$.

As $\mathbb{Z}$ is a PID, every finitely generated $\mathbb{Z}$-module can be decomposed as the direct sum of a torsion submodule and a finite-rank free $\mathbb{Z}$-module, and the rank of the free part does not depend on the decomposition. The following result is central to the classification theorem of finitely generated abelian groups.

Proposition 3.19. *Every submodule of a free $\mathbb{Z}$-module of finite rank k is a free $\mathbb{Z}$-module of rank at most k.*

Proof. We proceed by mathematical induction on the rank k of the free $\mathbb{Z}$-module. For the base case $k = 1$, let M be a free $\mathbb{Z}$-module of rank 1, meaning $M \cong \mathbb{Z}$. An R-submodule $N \subseteq M$ corresponds directly to an ideal of $\mathbb{Z}$. Since every ideal of $\mathbb{Z}$ is principal, as an ideal of $\mathbb{Z}$, we see that $N = n\mathbb{Z}$. If $n = 0$, then $N = \{0\}$, which is a free $\mathbb{Z}$-module of rank 0. If $n \neq 0$, then $N = n\mathbb{Z}$. The map $\phi : \mathbb{Z} \to n\mathbb{Z}$ defined by $x \mapsto nx$ is an isomorphism because $\mathbb{Z}$ has no zero divisors. Thus, $N \cong \mathbb{Z}$, which is a free $\mathbb{Z}$-module of rank 1. In both scenarios, N is free and $\text{rank}(N) \leq 1$.

For the inductive step, assume that the hypothesis holds true for all free $\mathbb{Z}$-modules of rank less than k. Let M be a free $\mathbb{Z}$-module of rank $k \geq 2$, and let $\{x_1, x_2, \ldots, x_k\}$ be a basis for M. We define a projection homomorphism $\pi\colon M \to \mathbb{Z}$ that isolates the coefficient of the final basis element as follows:

$$\pi(c_1x_1 + c_2x_2 + \cdots + c_kx_k) = c_k$$

Let N be an arbitrary submodule of M. We restrict the projection mapping to N, denoting it as $\pi|_N : N \to \mathbb{Z}$. The image $\pi(N)$ constitutes a submodule (an ideal) of $\mathbb{Z}$. By our baseline analysis, $\pi(N)$ is principal, hence $\pi(N) = d\mathbb{Z}$ for some $d \in \mathbb{Z}$. The kernel of this restricted homomorphism is

$$\ker(\pi|_N) = N \cap \ker(\pi) = N \cap \operatorname{span}_{\mathbb{Z}}(x_1, \ldots, x_{k-1})$$

Notice that $\ker(\pi|_N)$ is a submodule of $\operatorname{span}_{\mathbb{Z}}(x_1, \ldots, x_{k-1})$, which is explicitly a free $\mathbb{Z}$-module of rank $k-1$. Applying our inductive hypothesis, $\ker(\pi|_N)$ must be a free $\mathbb{Z}$-module of rank $m \leq k-1$. Let $\{y_1, y_2, \ldots, y_m\}$ be a basis for $\ker(\pi|_N)$.

We now evaluate the structure of N based on the ideal $\pi(N)$.

Case 1: $\pi(N) = \{0\}$. If the image is trivial, it follows immediately that $N = \ker(\pi|_N)$. Therefore, N is a free $\mathbb{Z}$-module of rank $m \leq k-1 < k$, which satisfies the claim.

Case 2: $\pi(N) = d\mathbb{Z}$ with $d \neq 0$. Take an element $z \in N$ such that $\pi(z) = d$. This structure can be framed within the context of a short exact sequence:

$$0 \longrightarrow \ker(\pi|_N) \longrightarrow N \xrightarrow{\pi|_N} d\mathbb{Z} \longrightarrow 0$$

Because $d\mathbb{Z} \cong \mathbb{Z}$ is a free $\mathbb{Z}$-module, it is inherently projective. Consequently, the short exact sequence splits, which implies that:

$$N \cong \ker(\pi|_N) \oplus d\mathbb{Z}$$

Concretely, every element $n \in N$ can be uniquely expressed in the form $n = u + cz$, where $u \in \ker(\pi|_N)$ and $c \in \mathbb{Z}$. Thus, the set $\{y_1, y_2, \ldots, y_m, z\}$ forms a linearly independent generating set for N. The rank of N is precisely $m+1$. Given our inductive constraint $m \leq k-1$, we conclude that

$$\operatorname{rank}(N) = m + 1 \leq (k-1) + 1 = k$$

Hence N is a free $\mathbb{Z}$-module of rank at most k. By the principle of mathematical induction, the theorem holds universally for all finite ranks k. □

Before proving that $\mathcal{O}_K$ is a free $\mathbb{Z}$-module of rank $[K : \mathbb{Q}]$, we will argue the following lemma.

Lemma 3.20. *For any $\alpha \in \mathbf{A}$, there exists a nonzero $d \in \mathbb{Z}$ such that $d\alpha$ is an algebraic integer.*

Proof. Fix $\alpha \in \mathbf{A}$, and let $m(x) := x^n + \sum_{i=1}^{n-1} q_i x^i \in \mathbb{Q}[x]$ be the minimal polynomial of α. Then set $d := \prod_{i=0}^{n-1} \mathsf{d}(q_i)$ and observe that

$$p(d\alpha) = (d\alpha)^n + \sum_{i=0}^{n-1} d^{n-i} q_i (d\alpha)^i = d^n \left(\alpha^n + \sum_{i=0}^{n-1} q_i x^i \right) = d^n m(\alpha) = 0.$$

Therefore $d\alpha$ is a root of the monic polynomial $p(x) := x^n + \sum_{i=0}^{n-1} d^{n-i} q_i x^i$. In addition, $\mathsf{d}(q_i) \mid d$ for every $i \in [\![0, n-1]\!]$, and so $p(x) \in \mathbb{Z}[x]$. Hence $d\alpha$ is an algebraic integer. □

Let K be a number field and $\omega_1, \ldots, \omega_n$ be a basis for K over $\mathbb{Q}$. Now consider the correspondence $K \to M_n(\mathbb{Q})$ given by $\alpha \mapsto (q_{ij})$ given by $\alpha\omega_i = \sum_{i=1}^{n} q_{ij}\omega_j$.

Lemma 3.21. *Let K be a number field, and define $B \colon K \times K \to \mathbb{Q}$ by $B(x, y) := \mathrm{Tr}_K(xy)$. Then B is a nondegenerate bilinear form.*

Proof. Exercise. □

Let K be a number field and set $n := [K : \mathbb{Q}]$. Define $B \colon K \times K \to \mathbb{Q}$ as follows: $B(x, y) = \mathrm{Tr}_K(xy)$ for all $x, y \in K$. Observe that B is a bilinear form. Since K is an algebraic extension of $\mathbb{Q}$, it is separable. Thus, the bilinear form B is non-degenerate. One can use this to prove the following lemma.

Lemma 3.22. *For any basis $\{\beta_1, \ldots, \beta_n\}$ of K over $\mathbb{Q}$, there exists a dual basis $\{\beta_1^*, \ldots, \beta_n^*\}$ such that*

$$\mathrm{Tr}_K(\beta_i^* \beta_j) = \delta_{ij}$$

for all $i, j \in [\![1, n]\!]$.

At this point we have all the tools we need to prove that the $\mathbb{Z}$-module $\mathscr{O}_K$ is a free $\mathbb{Z}$-module of rank $[K : \mathbb{Q}]$.

Theorem 3.23 (Existence of Integral Bases)**.** *Let K be an algebraic number field such that $[K : \mathbb{Q}] = n$. Then $\mathscr{O}_K$ is a free $\mathbb{Z}$-module of finite rank n.*

Proof. Let us argue first that $\mathscr{O}_K$ contains a free $\mathbb{Z}$-module of rank n. To do so, take $v_1, \ldots, v_n \in K$ such that $\{v_1, \ldots, v_n\}$ is a $\mathbb{Q}$-basis for K. In light of Lemma 3.20, after replacing $\{v_1, \ldots, v_n\}$ by $\{cv_1, \ldots, cv_n\}$ for some $c \in \mathbb{N}$, we can assume the existence of a basis $\{\beta_1, \ldots, \beta_n\}$ of K over $\mathbb{Q}$ such that $\bigoplus_{i=1}^{n} \mathbb{Z}\beta_i \subseteq \mathscr{O}_K$. As $\bigoplus_{i=1}^{n} \mathbb{Z}\beta_i$ is a free $\mathbb{Z}$-module of rank n, we obtain that the rank of $\mathscr{O}_K$ as a $\mathbb{Z}$-module is at least n.

We now prove that the rank of $\mathscr{O}_K$ as a $\mathbb{Z}$-module is at most n. For each $\alpha \in K$, consider the linear map $\alpha^* \colon K \to K$ defined as $\alpha^*(\beta) = \alpha\beta$ for all $\beta \in K$. Now set $\mathscr{O}_K^* := \{\alpha^* : \alpha \in \mathscr{O}_K\}$. It is clear that $\mathscr{O}_K$ and $\mathscr{O}_K^*$ are isomorphic as $\mathbb{Z}$-modules. Let us argue that there exist a basis $\beta_1^*, \ldots, \beta_n^*$ of K^* such that $\mathscr{O}_K^* \subseteq \bigoplus_{i=1}^{n} \mathbb{Z}\beta_i^*$.

For this, choose a basis $\{\beta_1, \ldots, \beta_n\}$ for K such that $\{\beta_1, \ldots, \beta_n\} \subseteq \mathscr{O}_K$. Because the function $K \times K \to \mathbb{Q}$ defined as $(x, y) \mapsto \mathrm{Tr}_K(xy)$ for all $x, y \in K$ is a non-degenerated bilinear form, there exists a dual basis $\{\beta_1^*, \ldots, \beta_n^*\}$ of K^* such that

$$\mathrm{Tr}_K(\beta_j^* \beta_i) = \delta_{ij}$$

for all $i, j \in [\![1, n]\!]$. Now take $\alpha^* \in \mathscr{O}_K^*$ and write α^* as a $\mathbb{Q}$-linear combination of the dual basis:

$$\alpha^* = \sum_{j=1}^{n} c_j \beta_j^* \tag{3.3}$$

for some $c_1, \ldots, c_n \in \mathbb{Q}$. To argue that the coefficients $c_1, \ldots, c_n$ are integers, we use the trace form: for each $i \in [\![1, n]\!]$,

$$\mathrm{Tr}_K(\alpha^* \beta_i) = \mathrm{Tr}_K\left(\sum_{j=1}^{n} c_j \beta_j^* \beta_i\right) = \sum_{j=1}^{n} c_j \,\mathrm{Tr}_K(\beta_j^* \beta_i) = c_i.$$

As $\alpha \in \mathscr{O}_K$ and $\{\beta_1, \ldots, \beta_n\} \subset \mathscr{O}_K$, we obtain that $c_i = \mathrm{Tr}_K(\alpha^* \beta_i) = \mathrm{Tr}_K(\alpha \beta_i) \in \mathbb{Z}$ for every $i \in [\![1, n]\!]$. Hence it follows from (3.3) that $\alpha^* \in \sum_{j=1}^n \mathbb{Z}\beta_j^*$. Thus, $\mathscr{O}_K^* \subseteq \sum_{j=1}^n \mathbb{Z}\beta_j^*$, and so we have proved that

$$\sum_{j=1}^{n} \mathbb{Z}\beta_j \subseteq \mathscr{O}_K \cong \mathscr{O}_K^* \subseteq \sum_{j=1}^{n} \mathbb{Z}\beta_j^*.$$

Thus, as both $\sum_{j=1}^n \mathbb{Z}\beta_j$ and $\sum_{j=1}^n \mathbb{Z}\beta_j^*$ are free $\mathbb{Z}$-modules of rank n, we conclude that $\mathscr{O}_K$ is a free $\mathbb{Z}$-module of rank n. □

Let us compute the integral basis for quadratic rings of integers.

Example 3.24. The standard module $M = R^k$ is free of rank k over R, with the canonical basis $\{e_1, e_2, \ldots, e_k\}$. In particular, $\mathbb{Z}^k$ is a free $\mathbb{Z}$-module of rank k.

Example 3.25. Let K be a quadratic number field, and let $d \in \mathbb{Z}$ be a square-free integer such that $K = \mathbb{Q}(\sqrt{d})$. Now take $\alpha \in \mathscr{O}_K$. Write $\alpha = a + b\sqrt{d}$ for some $a, b \in \mathbb{Q}$. If $b = 0$ then $\alpha = a \in \mathbb{Q}$, which is integrally closed if and only if $a \in \mathbb{Z}$.

Now assume $b \neq 0$. The minimal polynomial of α over $\mathbb{Q}$ is $x^2 - 2ax + (a^2 - b^2 d) = 0$. For α to be an algebraic integer, the coefficients must be in $\mathbb{Z}$, and so we can write $a = \frac{m}{2}$ for some $m \in \mathbb{Z}$ and $a^2 - b^2 d \in \mathbb{Z}$. Let $b = \frac{u}{v}$ in lowest terms, where $\gcd(u, v) = 1$. Substituting $a = \frac{m}{2}$ into $a^2 - b^2 d \in \mathbb{Z}$, one sees that $\frac{m^2}{4} - \frac{u^2}{v^2} d \in \mathbb{Z}$, which in turn implies that

$$m^2 v^2 \equiv 4u^2 d \pmod{4v^2}.$$

If an odd prime p divides v, then $p^2 \mid v^2$, implying $p^2 \mid 4u^2 d$. Since $\gcd(u, v) = 1$, we must have $p^2 \mid d$, which contradicts that d is square-free. If $4 \mid v$, then $16 \mid 4v^2$, forcing an impossible power of 2 to divide $4d$. Thus, the only allowable denominators are $v = 1$ or $v = 2$.

- If $v = 1$, then $b \in \mathbb{Z}$, which forces $a \in \mathbb{Z}$, whence $\mathscr{O}_K = \mathbb{Z}[\sqrt{d}]$.
- If $v = 2$, then $b = \frac{u}{2}$ for an odd integer u. The congruence simplifies to $m^2 - u^2 d \equiv m^2 - d \equiv 0 \pmod 4$. If $d \equiv 2, 3 \pmod 4$, no solution for m exists. If $d \equiv 1 \pmod 4$, then m must be odd, meaning that a and b are strict half-integers with matching parity.

Thus, the free $\mathbb{Z}$-module $\mathscr{O}_K$ has the following integral basis:

$$\mathscr{O}_K = \begin{cases} \mathbb{Z} + \mathbb{Z}\left[\frac{\sqrt{d}+1}{2}\right] & \text{if } d \equiv 1 \pmod 4, \\ \mathbb{Z} + \mathbb{Z}\sqrt{d} & \text{if } d \equiv 2, 3 \pmod 4. \end{cases}$$

Example 3.26. Let $K = \mathbb{Q}(\alpha)$ where $\alpha = \sqrt[3]{2}$. Let $\omega = c_0 + c_1\alpha + c_2\alpha^2 \in \mathscr{O}_K$ for $c_0, c_1, c_2 \in \mathbb{Q}$. We determine the denominators of c_i locally at each prime p. To do so, we consider the following cases.

- For $p \neq 2, 3$: The field traces are $\mathrm{Tr}(1) = 3$, $\mathrm{Tr}(\alpha) = 0$, and $\mathrm{Tr}(\alpha^2) = 0$. Thus $\mathrm{Tr}(\omega) = 3c_0 \in \mathbb{Z}$. Since $p \neq 3$, c_0 is p-integral. Iterating this trace map on $(\omega - c_0)\alpha = 2c_2 + c_1\alpha^2$ yields $\mathrm{Tr}((\omega - c_0)\alpha) = 6c_2 \in \mathbb{Z}$, ensuring c_2 (and consequently c_1) are p-integral.
- For $p = 2$: The minimal polynomial $x^3 - 2$ is Eisenstein at 2. Let ν be the unique valuation extending the 2-adic valuation. Since $\alpha^3 = 2$, $\nu(\alpha) = \frac{1}{3}$. The valuations of the components of ω satisfy:

  $$\nu(c_0) \in \mathbb{Z}, \quad \nu(c_1\alpha) \in \mathbb{Z} + \frac{1}{3}, \quad \nu(c_2\alpha^2) \in \mathbb{Z} + \frac{2}{3}$$

  Because these values lie in distinct cosets of $\mathbb{Z}$, no cancellation occurs. Thus, $\nu(\omega) = \min\left(\nu(c_0), \nu(c_1) + \frac{1}{3}, \nu(c_2) + \frac{2}{3}\right) \geq 0$, which forces $\nu(c_i) \geq 0$ for all i.
- For $p = 3$: Shift the generator by setting $\beta = \alpha - 2$. Its minimal polynomial is $g(x) = x^3 + 6x^2 + 12x + 6$, which is Eisenstein at 3. Let μ be the valuation extending the 3-adic valuation, yielding $\mu(\beta) = \frac{1}{3}$. Rewriting $\omega = b_0 + b_1\beta + b_2\beta^2$, the identical distinct coset argument requires $\mu(b_i) \geq 0$.

Since no primes divide any denominators, $c_0, c_1, c_2 \in \mathbb{Z}$. Thus, $\mathscr{O}_K = \mathbb{Z}[\alpha]$, and a $\mathbb{Z}$-basis is given by $\{1, \sqrt[3]{2}, \sqrt[3]{4}\}$.

3.3.2 Exercises – The Additive Structure of Rings of Integers

Exercise 3.1. Prove that the matrix $(\sigma_j(\omega_i))$ is invertible.

Exercise 3.2. Prove Dedekind's lemma.

Exercise 3.3. Run the example $\mathbb{Q}(\sqrt[3]{2}, \sqrt[3]{4})$.

Exercise 3.4. Let $\mathbb{Q}(\alpha)$ be an algebraic number field with $n := [\mathbb{Q}(\alpha) : \mathbb{Q}] \geq 2$, and let α' be a complex conjugate of α. Prove that there exists a unique isomorphism $\mathbb{Q}(\alpha) \to \mathbb{Q}(\alpha')$ fixing $\mathbb{Q}$ and sending α to α'.

Bibliography

[1] E. Artin and J. Tate, *Class Field Theory*, Addison-Wesley, Reading, MA, 1967.

[2] L. Carlitz, *A characterization of algebraic number fields with class number two*, Proc. Amer. Math. Soc. **11** (1960), 391–392.

[3] P. Cohn, *Bezout rings and their subrings*, Proc. Camb. Phil. Soc. **64** (1968) 251–264.

[4] R. Dedekind, *Über die Theorie der ganzen algebraischen Zahlen*, Supplement X to P. G. Lejeune Dirichlet, Vorlesungen über Zahlentheorie, 1st ed., Vieweg, Braunschweig, 1871, pp. 265–290.

[5] D. S. Dummit and R. M. Foote, *Abstract Algebra* (Third Edition), John Wiley & Sons, 2004.

[6] A. Geroldinger and F. Halter-Koch, *Non-unique factorizations: a survey*. In: Multiplicative Ideal Theory in Commutative Algebra (Eds. J. W. Brewer, S. Glaz, W. J. Heinzer, and B. M. Olberding), Springer, Boston, 2006.

[7] A. Geroldinger and F. Halter-Koch, *Non-Unique Factorizations: Algebraic, Combinatorial and Analytic Theory*, Pure and Applied Mathematics Vol. 278, Chapman & Hall/CRC, Boca Raton, 2006.

[8] R. Gilmer, *Multiplicative Ideal Theory*, Queen's Papers in Pure and Applied Mathematics, No. 12, Queen's Univ. Press, Kingston, Ontario, 1968.

[9] A. Grams, *Atomic domains and ascending chain conditions on principal ideals*, Math. Proc. Cambridge Philos. Soc. **75** (1974) 321–329.

[10] F. Halter-Koch, *Finiteness theorems for factorizations*, Semigroup Forum **44** (1992) 112–117.

[11] A. Heinle and V. Levandovskyy, *A factorization algorithm for G-algebras and applications*. Preprint on arXiv: https://arxiv.org/abs/1602.00296

[12] D. Hilbert, *Über die Theorie der algebraischen Formen*, Math. Ann. **36** (1890) 473–534.

[13] E. E. Kummer, *Über die Zerlegung der aus Wurzeln der Einheit gebildeten complexen Zahlen in ihre Primfactoren*, Journal für die reine und angewandte Mathematik **35** (1847) 327–367.

[14] J.-P. G. Lamé, *Sur le dernier théoréme de Fermat*, Comptes Rendus Hebdomadaires des Séances de l'Académie des Sciences **24** (1847) 410–416 (session of March 1, 1847).

[15] S. Lang, *Algebraic Number Theory*, 2nd ed., Springer-Verlag, New York, 1994.

[16] D. Mumford, J. Fogarty, and F. Kirwan, *Geometric Invariant Theory*, 3rd ed., Springer-Verlag, Berlin, 1994.

[17] E. Noether, *Idealtheorie in Ringbereichen*, Math. Ann. **83** (1921) 24–66.