Algebraic number theory

Narmada Varadarajan

The broad theme of algebraic number theory is, well, to study the theory of algebraic numbers. There are many problems of elementary number theory that turn out to have deeper meaning when studied from an algebraic point of view. Fermat's last theorem is a classical example of this, but well beyond the scope of this note. Gauss's quadratic reciprocity law is another that turns out to follow from properties of field extensions of $\mathbb{Q}$, or *number fields*. In fact, the fact that the primes $p \equiv 1 \pmod 4$ can be written as a sum of two squares follows very quickly from factorising them in the ring $\mathbb{Z}[i]$.

In general, algebraic number theory studies extensions of the integers to understand the structure of prime numbers. Unique prime factorisation of integers, however, fails in general extensions, which is why Minkowski theory considers *ideals* instead of elements. Of course, here we run into another problem. Rings of integers of number fields need not be principal ideal domains, so there will be "more" ideals than just the principal ones. This is where the *ideal class group* and *Dirichlet's unit theorem* come in: the first tells us how far the ring of integers is from being a UFD, and the second classifies the units upto which unique factorisation can hold.

Contents

1 Preliminaries

A comprehensive and better introduction to commutative algebra and Galois theory can be found in other books. This is only intended to be a brief review of some fundamental concepts.

1.1 Commutative algebra

Unless stated otherwise, the rings we deal with will be commutative integral domains. If R is a ring, we say $I \subset R$ is an *ideal* of R if I is an additive subgroup of R, and for all $r \in R$, $rI \subset I$. We denote this by $I \lhd R$. We say a proper ideal $I \lhd R$ is *prime* if whenever a product $ab \in I$, then either $a \in I$ or $b \in I$. We say a proper ideal $I \lhd R$ is *maximal* if it is not contained in any other proper ideal of R.

Exercise 1. Show that a prime ideal is maximal.

Ideals are the analogues of normal subgroups: they are exactly the kernels of ring homomorphisms. Given an ideal $I \lhd R$, we can define a quotient ring R/I in the natural way.

Exercise 2. $P \lhd R$ is a prime ideal if and only if R/P is an integral domain. $P \lhd R$ is a maximal ideal if and only if R/P is a field.

We say two ideals $I, J \lhd R$ are *coprime* if $I + J = R$.

Theorem 1.1 (Chinese Remainder Theorem)**.** *If $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ are pairwise coprime ideals in R, then*

$$R\big/\textstyle\bigcap_{i=1}^{r}\mathfrak{p}_i \cong R\big/\mathfrak{p}_1 \times \cdots \times R\big/\mathfrak{p}_r.$$

Each element $r \in R$ generates an ideal $\langle r \rangle$. We call such an ideal *principal*. A *principal ideal domain* (PID) is a commutative integral domain in which every ideal is principal.

Exercise 3. Give an example of a commutative integral domain that is not a PID.[1]

We say r is a *unit* in R if it is invertible in R.

Exercise 4. $\langle r \rangle$ is a proper ideal if and only if r is not a unit.

We say r is *prime* if whenever r divides a product ab ($rs = ab$ for some $s \in R$) then r divides a or r divides b. We say r is *irreducible* if whenever $r = ab$ then either a or b is a unit.

Exercise 5. Show that the ideal generated by a prime element is a prime ideal.

Exercise 6. Show that every prime element is irreducible. Give an example of a prime element that is not irreducible.[2]

Exercise 7. Show that 2 is irreducible in $\mathbb{Z}[X]$, but the ideal $\langle 2 \rangle$ is not maximal.

A ring R is a *unique factorisation domain* (UFD) if every $r \in R$ can be written as a product of irreducibles $r = p_1 \ldots p_n$, unique upto multiplication by units. The elements of a UFD mimic many properties of the integers: for example, we can define a greatest common divisor (gcd) in a UFD. The first fundamental theorem of commutative algebra is the following. Its proof is a worthwhile exercise in definition-chasing.

Theorem 1.2. *Every principal ideal domain is a unique factorisation domain.*

The converse is not true in general. For example, $\mathbb{Z}[X]$ is not a PID (as an earlier exercise showed), but it is a UFD: every polynomial factors as a product of irreducible polynomials.

[1] Hint: look at rings of polynomials.

[2] Hint: Look at $\mathbb{Z}[\sqrt{5}]$.

1.1.1 Modules

Given a ring R, we say M is an R-module if M is an abelian group and we have a ring homomorphism $R \longrightarrow \operatorname{End}(M)$. Informally, R "acts" on M; for each $r \in R$, the map $m \longrightarrow rm$ is a group homomorphism, and the composition of maps corresponds to multiplication of the ring elements. A subgroup $N \leq M$ is called an R-*submodule* of M if $rN \subset N$ for all $r \in R$.

Exercise 8. Consider R as an R-module with left multiplication. What are its R-submodules?

We say $S \subset M$ is a generating set for M as an R-module if M is generated by R-linear combinations of S. For example, $\mathbb{Z}[\sqrt{2}]$ is generated by $\{1, \sqrt{2}\}$ as a $\mathbb{Z}$-module. Every ring is generated by $\{1\}$ as a module over itself. An R-module M is *free* if $M \cong \bigoplus_{i \in I} Ra_i$ as an R-module for some $\{a_i : i \in I\} \subset M$.

Exercise 9. Give an example of a $\mathbb{Z}$-module that is not free.

A result we will need for later manipulations is the following.

Theorem 1.3. *If M is a free module over a PID R, and $N \leq M$, then N is also a free R-module. If M and N have the same finite rank, and A is a transition matrix from a basis of M to a basis of N, then*

$$|\det(A)| = |M : N|.$$

An R-module M is *Noetherian* if every ascending chain of submodules has a maximal element. Equivalently, if every submodule is finitely generated over R. A ring R is *Noetherian* if it is Noetherian as an R-module; equivalently, if every ideal is finitely generated.

Exercise 10. Give an example of a ring that is not Noetherian.

Proposition 1.4. *If R is a Noetherian ring, every finitely generated R-module is Noetherian.*

Exercise 11. Give an example of a ring R, an R-module M, and a submodule $N \leq M$ such that M is finitely generated over R but N is not.[3]

1.1.2 Polynomial rings

Our first goal is to determine which properties of R extend to $R[X]$, any by extension to any polynomial ring over R.

Theorem 1.5 (Hilbert's basis theorem)**.** *If R is a Noetherian ring, then $R[X]$ is a Noetherian ring.*

Note that "$R[X]$ is Noetherian as a ring" is different from "$R[X]$ is Noetherian as an R-module". The first statement is what we will prove, and the second statement is false.

Exercise 12. Show that $R[X]$ is not Noetherian as an R-module.

Proof. Suppose $I \lhd R[X]$ is not finitely generated. By induction, we can construct a sequence of polynomials $p_0, p_1, \ldots, p_n, \cdots$, where $p_n \in I \setminus \langle p_0, \ldots, p_{n-1} \rangle$ is chosen to be a polynomial of least degree. By construction, $\deg(p_n)$ is nondecreasing. Let $a_n \in R$ be the leading coefficient of p_n. The chain of ideals $\langle a_0 \rangle \subset \langle a_0, a_1 \rangle \subset \ldots$ terminates at some step, say at $\langle a_0, \ldots, a_{N-1} \rangle$. Write $a_N = \sum_{i=0}^{N-1} r_i a_i$. Define

$$g(X) = \sum_{i=0}^{N-1} r_i X^{\deg(p_N) - \deg(p_i)} p_i(X) \in R[X].$$

Then, $g(X) \in I$, $\deg(g) = \deg(p_N)$, and $g - p_N \in I \setminus \langle p_0, \ldots, p_{N-1} \rangle$ is a polynomial of smaller degree than p_N, a contradiction. □

Proposition 1.6. *If K is a field, then $K[X]$ is a PID.*

[3] *Hint:* every ring is a module over itself.

Proof. Given two polynomials $a(X), b(X) \in K[X]$, there exist unique polynomials $q(X), r(X) \in K[X]$ such that $a(X) = q(X)b(X) + r(X)$, with $r(X) = 0$ or $0 \leq \deg\big(r(X)\big) < \deg\big(a(X)\big)$. Using this, now show that any nonzero ideal $I \lhd R[X]$ is generated by the polynomial of least degree. □

Proposition 1.7. *If R is a UFD, then $R[X]$ is a UFD.*

The crux of the proof is Gauss's lemma.

Definition 1.8. A polynomial $p(X) = a_0 + a_1X + \cdots + a_nX^n \in R[X]$ is *primitive* if the ideal $\langle a_0, a_1, \cdots, a_n\rangle = R$. When R is a UFD, this is equivalent to saying that the GCD of the coefficients of p is equal to 1.

Theorem 1.9 (Gauss's lemma)**.** *If $p(X), q(X) \in R[X]$ are primitive polynomials, so is their product $p(X)q(X)$.*

Proof. NOTE: improve the proof from here https://math.stackexchange.com/questions/2974813/is-content-multiplicative-if-the-ring-is-only-integrally-closed

Let C_p, C_q, and $C_{pq} \lhd R$ be the ideals generated by by $p(X), q(X)$, and $pq(X)$ respectively. By definition, $C_{pq} \subset C(p)$ and $C_{pq} \subset C_q$, so if pq is primitive, then p and q are primitive.

Conversely, suppose p and q are primitive but pq is not. Then, C_{pq} is contained in some proper maximal ideal $M \lhd R$. Since p and q are primitive, they are nonzero in R/M, but their product $pq + R/M = 0$. R/M is a field, so it is not possible for the product of two nonzero elements to be zero, giving us the desired contradiction. □

Now that we have studied some properties of the ring $R[X]$, we will look at properties of its polynomials. Suppose $A \leq B$ are rings, and $b \in B$ is the root of a monic polynomial in A. There is a unique monic polynomial $m_b(X) \in A[X]$ such that $m_b(b) = 0$. Further, if $p(b) = 0$ for some polynomial $p(X) \in A[X]$, then $m_b(X)|p(X)$. We call this the *minimal polynomial* of b over A.

Exercise 13. $m_b(X)$ is irreducible in $A[X]$.

Example 1.10. The minimal polynomial depends on the ring A. For example, the minimal polynomial of $\sqrt{2}$ in $\mathbb{Z}[X]$ is $X^2 - 2$, but in $\mathbb{R}[X]$ it is $X - \sqrt{2}$.

Let $\omega \in \mathbb{C}$ be a primitive third root of unity. The minimal polynomial of ω is *not* $X^3 - 1$. We have the factorisation $X^3 - 1 = (X - 1)(X^2 + X + 1)$, so $X^3 - 1$ is irreducible in $\mathbb{Z}[X]$. The minimal polynomial of ω is in fact $X^2 + X + 1$. In general, if ζ is a primitive nth root of unity, its minimal polynomial in $\mathbb{Z}[X]$ has degree $\phi(n)$, where ϕ is the Euler totient function. The minimal polynomials of the roots of unity are called *cyclotomic polynomials*.

Exercise 14. If $a \in \mathbb{Q}$ is the root of a monic polynomial in $\mathbb{Z}[X]$, then $a \in \mathbb{Z}$.

Exercise 15. Let R be a UFD and K its field of fractions. If $a \in K$ is the root of a monic polynomial in $R[X]$, then $a \in R$.

We conclude this subsection with an important criterion for a polynomial to be irreducible.

Theorem 1.11 (Eisenstein's criterion)**.** *Let R be a commutative integral domain, and $p(X) = a_0 + a_1X + \cdots + a_nX^n \in R[X]$. Suppose there exists a prime ideal $\mathfrak{p} \lhd R$ such that*

(i) $a_i \in \mathfrak{p}$ for $i = 0, \ldots, n-1$,

(ii) $a_n \notin \mathfrak{p}$, and

(iii) $a_0 \notin \mathfrak{p}^2$.

Then $p(X)$ cannot be written as the product of two non-constant polynomials in $R[X]$. If $p(X)$ is primitive, then it is irreducible in $R[X]$.

A polynomial that satisfies these conditions is called an *Eisenstein polynomial*. This is a necessary but not sufficient condition for irreducibility. For example, the polynomial $X^2 + 1 \in \mathbb{Z}[X]$ is not Eisenstein for any prime in $\mathbb{Z}$, but it is irreducible.

1.2 Extensions

Suppose A is a ring, and α is an element of B, another ring. Define the ring of formal sums

$$A[\alpha] = \Big\{ \sum_{i=0}^{n} a_i \alpha^i : a_i \in A, n \in \mathbb{N} \Big\}$$

with addition and multiplication defined as one would expect. For example, when $\alpha = X$, $A[X]$ is the ring of polynomials with coefficients in A. Of course, we can extend this definition to a finite set $\{\alpha_1, \dots, \alpha_k\} \subset B$, or even an arbitrary (possibly infinite) subset $S \subset B$. We are typically interested in the case when A is a subring of B, and the formal sums satisfy some sort of recursion. For example, if $A = \mathbb{Z}$, $B = \mathbb{R}$, and $\alpha = \sqrt{2}$, then $\sqrt{2}^2 = 2 \in \mathbb{Z}$. We would like to differentiate between the "dimension" of $\mathbb{Z}[X]$ and $\mathbb{Z}[\sqrt{2}]$ over $\mathbb{Z}$. In the first case, no monomial X^n can be expressed as a $\mathbb{Z}$-linear combination of $1, X, \dots, X^{n-1}$, and the formal sums $\sum_{i=0}^{n} a_i X^i$ can have arbitrarily many terms. In $\mathbb{Z}[\sqrt{2}]$, however, each term can be expressed uniquely as $a + b\sqrt{2}$. This corresponds exactly to the structure of $\mathbb{Z}[X]$ and $\mathbb{Z}[\sqrt{2}]$ as $\mathbb{Z}$-modules.

If $A \leq B$, we call the dimension of B as an A-module the *degree* of the extension B/A. Note that even though the ring $\mathbb{Z}[X]$ is obtained by adjoining one element to $\mathbb{Z}$, its degree is infinite.

Now suppose K and L are fields, and L is an *extension* of K, i.e. K is a subfield L. K and L are also rings, so we extend the same definitions to the extension L/K. In particular, the degree of the extension, denoted $|L : K|$, is the dimension of L as a K-vector space.

Proposition 1.12. *Given three fields $K \leq L \leq M$,*

$$|M : K| = |M : L| \cdot |L : K|.$$

Unfortuntately, composite fields do not satisfy such a nice identity in general. If K_1 and K_2 are subfields of a field K, let K_1K_2 denote the field generated by K_1 and K_2, or the smallest subfield of K containing K_1 and K_2. The field K_1K_2 is referred to as the *composite* field.

Proposition 1.13. *If K_1 and K_2 are finite extensions of F, then*

$$|K_1K_2 : F| \leq |K_1 : F| \cdot |K_2 : F|.$$

Exercise 16. If $|K_1 : F|$ and $|K_2 : F|$ are coprime, then we have equality in the above proposition.

Remark. If $A[S]$ is the ring obtained by adjoining the elements of S to A, we denote by $A(S)$ its field of fractions. The field of fractions of $A[X]$, $A(X)$, is called the field of *rational functions* over A: these are the quotients of polynomials. An important result that we will need is that if K is a field, and $K[S]$ is finitely generated[4], then $K[S] = K(S)$. In particular, any finitely generated *ring* extension of a field is itself a field.

1.2.1 Integrality

Definition 1.14. If $A \leq B$ are rings, we say $b \in B$ is *integral* over A if it is the root of a monic polynomial with coefficients in A. We say B is integral over A if every element of it is integral over A.

Proposition 1.15. *The elements $b_1, \dots, b_n$ are integral over A if and only if $A[b_1, \dots, b_n]$ is a finitely generated A-module.*

Proof. Consider the case when we have just one element, b. If b is integral over A, let $f(X) = X^n + a_{n-1}X^{n-1} + \cdots + a_0$ be its minimal polynomial over A. By induction, for any $m \geq n$, $b^m \in A[1, b, \dots, b^{n-1}]$, so $A[b]$ is generated by $\{1, b, \dots, b^{n-1}\}$.

[4] This is an important condition! For example, $K[X] \neq K(X)$.

For the converse, suppose $A[b]$ is a finitely generated A-module. At most finitely many of the elements $\{b^n : n \in \mathbb{N}\}$ can be algebraically independent over A. There is an integer n so that $b^n \in A[1, b, \ldots, b^{n-1}]$. If $b^n = a_{n-1}b^{n-1} + \cdots + a_1 b + a_0$, then b is the root of $X^n - a_{n-1}X^{n-1} + \cdots + a_1 X + a_0 \in A[X]$.

For larger n, the proof follows easily by induction considering the chain $A \leq A[b_1] \leq \cdots \leq A[b_1, \ldots, b_{n-1}] \leq A[b_1, \ldots, b_{n-1}, b_n]$. □

An easy application of the previous proposition also shows that if $A \leq B \leq C$, B is integral over A, and C is integral over B, then C is integral over A.

Corollary 1.16. *The integral elements in B over A form a subring.*

Define the *integral closure* of A in B as the subring of integral elements. We say an integral domain is *integrally closed* if it is equal to its integral closure in its field of fractions. For example, an earlier exercise showed that every UFD is integrally closed.

For fields, we say an element is *algebraic* over a field K if it is the root of a monic polynomial over K. We say L is *algebraic* over K if every element of it is algebraic over K. As an important corollary of the work we have done for rings,

Corollary 1.17. *Every finite extension of fields L/K is algebraic.*

If α is *not* algebraic over K, we say it is transcendental.

Corollary 1.18. *If α is transcendental over K, $K[\alpha]$ is infinite-dimensional over K.*

Suppose A is an integrally closed domain, K its field of fractions, L a finite extension of K, and B the integral closure of A in L. We refer to this setup as $AKLB$.

Claim 1.19. *The following hold:*

(i) B is integrally closed.

(ii) Any $\beta \in L$ can be expressed as b/a for $b \in B$ and $a \in A$.

(iii) $\beta \in L$ is integral over A if and only if its minimal polynomial over K has coefficients in A.

Proof. (i) follows from the definition. For (ii), multiplying the minimal polynomial of β in $K[X]$ by a "common denominator", we obtain a polynomial $a_n X^n + a_{n-1}X^{n-1} + \cdots + a_1 X + a_0 \in A[X]$ of which β is a root. Multiply this polynomial by a_n^{n-1}, and set $b = a_n \beta$. Then $b \in L$ is the root of a monic polynomial over A, so $b \in B$ and $\beta = b/a_n$. For (iii), the implication $\Longleftarrow$ is clear. For the converse, let $m_A(X) \in A[X]$ and $m_K(X) \in K[X]$ are the minimal polynomials of β over A and K respectively. Then, $m_K(X)$ divides $m_A(X)$ in $K[X]$, so the roots of $m_K(X)$ are integral over A. The coefficients of $m_K(X)$ are linear combinations of the roots, so they are integral over A as well. Since A is integrally closed, $m_K(X) \in A[X]$. □

In particular, when $A = \mathbb{Z}$ and $K = \mathbb{Q}$, we say L is a *number field* and B is the *ring of integers* in L.

1.3 Galois theory

Let K be a field. The *algebraic closure* of K, denoted usually by $\bar{K}$, is the unique algebraic extension of K such that every polynomial in $K[X]$ splits into linear factors over $\bar{K}$. Equivalently, we obtain it by adjoining all roots of monic polynomials over K to K.

Exercise 17. Suppose α is algebraic over K and $p(X) \in K[X]$ is its minimal polynomial. Show that

$$K[\alpha] \cong K[X] \big/ (p(X)).$$

Exercise 18. Show that every field has an algebraic closure.[5]

[5] *Hint:* use Zorn's lemma.

We say a polynomial $f(X) \in K[X]$ is *separable* if it has no repeated roots. That is, if α is a root of $f(X)$, then $(X-\alpha)^2$ does not divide $f(X)$. Let L be an extension of K.[6] We say an element $\alpha \in L$ is separable over K if its minimal polynomial over K is separable. We say L is *separable* if every element of L is separable over K. Equivalently, if for any $\alpha \in L$, its minimal polynomial over K splits into distinct linear factors over the algebraic closure of K.

Exercise 19. A polynomial $f(X) \in K[X]$ is separable if and only if it is coprime to its formal derivative $Df(X) \in K[X]$. As a consequence, $f(X)$ is inseparable if and only if Df is identically 0.

Exercise 20. Let K be a field of prime characteristic p. A polynomial $f(X) \in K[X]$ is *inseparable* if and only if $f(X) = g(X^p)$ for some $g(X) \in K[X]$.

Exercise 21. If $\mathrm{char} K = 0$ or if K is a finite field, then every irreducible polynomial is separable.[7]

Most of the fields we deal with will be extensions of $\mathbb{Q}$, so separability will not be a concern.

Example 1.20. Let $L = \mathbb{F}_p(t)$ be the field of rational functions over $\mathbb{F}_p$ in the indeterminate t. This is an infinite field with characteristic p. Consider the subfield $K = \mathbb{F}_p(t^p)$ of L. The minimal polynomial of $t \in L$ over K is $X^p - t^p = (X-t)^p$, which is inseparable.

We say the extension L/K is *normal* if for any $\alpha \in L$, its minimal polynomial over K splits in L. Equivalently, if an irreducible polynomial $f(X) \in K[X]$ has one root in L, it has all its roots in L.

Example 1.21. Consider the field $\mathbb{Q}[\sqrt{2}]$. This is both separable and normal; the roots of the minimal polynomial of an element $a + b\sqrt{2}$ are $a \pm b\sqrt{2}$. On the other hand, $\mathbb{Q}[\sqrt[3]{2}]$ is not a normal extension of $\mathbb{Q}$. If ω is a primitive 3rd root of unity, the roots of the polynomial $X^3 - 2$ are $\sqrt[3]{2}, \omega\sqrt[3]{2}$, and $\omega^2\sqrt[3]{2}$. The polynomial $X^3 - 2$ has one root in $\mathbb{Q}[\sqrt[3]{2}]$, but not all. Nevertheless, $|\mathbb{Q}[\sqrt[3]{2}] : \mathbb{Q}| = 3$, generated by $\{1, \sqrt[3]{2}, \sqrt[3]{4}\}$.

We say an extension L/K is *Galois* if it is both separable and normal. An important example of a Galois extension of K is the *splitting field* of a separable polynomial $f(X) \in K[X]$. This is the smallest extension of K in which $f(X)$ splits, or the extension obtained from K by adjoining all roots of $f(X)$.

Exercise 22. Technically, *a* splitting field of $f(X) \in K[X]$ is a minimal field extension of K in which $f(X)$ splits into linear factors. Prove that if L_1 and L_2 are two splitting fields of $f(X)$, then $L_1 \cong L_2$, justifying the phrase "*the* splitting field".[8]

Example 1.22. We know the extension $Q[\sqrt[3]{2}]/\mathbb{Q}$ is not Galois. The splitting field of $X^3 - 2$ is in fact $\mathbb{Q}[\omega, \sqrt[3]{2}]$. The degree of this extension $|Q[\omega, \sqrt[3]{2}] : \mathbb{Q}| = 6$, as it is generated by $\{1, \sqrt[3]{2}, \sqrt[3]{4}, \omega, \omega\sqrt[3]{2}, \omega\sqrt[3]{4}\}$. This is worrisome because we would like the splitting field of $f(X)$ to have the same degree as the degree of $f(X)$. The trükk here is that we are looking at this as the splitting field of the wrong polynomial. In an ideal world, a splitting field of $f(X)$ would be obtained from K by adjoining exactly one root of it, and letting the others follow. In this case, we need to write $\mathbb{Q}[\omega, \sqrt[3]{2}] = \mathbb{Q}[\omega + \sqrt[3]{2}]$. The minimal polynomial of $\omega + \sqrt[3]{2}$ has degree 6, and this is its splitting field.

Exercise 23. If $f(X) \in K[X]$ has degree n, its splitting field has degree at most $n!$.

Proposition 1.23. *If $L = K[\theta]$ is separable and L is the splitting field for $f(X) \in K[X]$, the minimal polynomial of θ, then L/K is Galois and $|L : K| = \deg(f)$.*

We say L is *simple* if $L = K[\theta]$ for some $\theta \in L$. θ is called a *primitive element*. We will use the following highly nontrivial fact.

Theorem 1.24. *Any finite separable extension is simple.*

Definition 1.25. The *Galois group* of L/K, $\mathrm{Gal}(L/K)$, is the group of field automorphisms of L that fix K.

$$\mathrm{Gal}(L/K) = \{\sigma : \sigma \text{ is a field automorphism of } L, \sigma|_K = id|_K\}.$$

If $\alpha \in L$ and $\sigma \in \mathrm{Gal}(L/K)$, we call $\sigma(\alpha)$ a *Galois conjugate* of α.

[6] The letters L and K will almost surely almost always denote fields.

[7] *Hint:* If K is a finite field of characteristic p, then $a^p + b^p = (a+b)^p$.

[8] *Hint:* if α and β have the same minimal polynomial in $K[X]$, then $K[\alpha] \cong K[\beta]$.

Exercise 24. If $\alpha \in L$ is a root of $f(X) \in K[X]$, so are its Galois conjugates.

Example 1.26. Let us return to $\mathbb{Q}[\sqrt[3]{2}]$. Any automorphism in $\mathrm{Gal}(\mathbb{Q}[\sqrt[3]{2}]/\mathbb{Q})$ must map $\sqrt[3]{2}$ to a root of $X^3 - 2$, so it must fix $\sqrt[3]{2}$. So $\mathrm{Gal}(\mathbb{Q}[\sqrt[3]{2}]/\mathbb{Q})$ is the trivial group; $1 = |\mathrm{Gal}(\mathbb{Q}[\sqrt[3]{2}]/\mathbb{Q}) : \mathbb{Q}| < |\mathbb{Q}[\sqrt[3]{2}] : \mathbb{Q}| = 3$.

Proposition 1.27. *For any field extension L/K, $|\mathrm{Gal}(L/K)| \leq |L : K|$.*

We call a field extension L/K *Galois* if it is both normal and separable. The *normal closure* of a separable extension is the smallest Galois extension containing it.

Proposition 1.28. *A finite extension L/K is Galois if and only if $|\mathrm{Gal}(L/K)| = |L : K|$.*

Proposition 1.29. *Let $\bar{K}$ denote the algebraic closure of K and L be a finite separable extension of K. Any embedding of K into $\bar{K}$ extends to exactly $|L : K|$ embeddings of L into $\bar{K}$.*

Corollary 1.30. *Let L/K be a finite separable extension and $\mathrm{Hom}_K(L, \bar{K})$ denote the embeddings of L into $\bar{K}$ that fix K. Then $|\mathrm{Hom}_K(L, \bar{K})| = |L : K|$.*

Proof of proposition 1.29. We proceed by induction on n. When $n > 1$, let $\alpha \in L \setminus K$. Let $|L : K[\alpha]| = l$ and $|K[\alpha] : K| = k$, so that $n = kl$. There are exactly k embeddings of $K[\alpha]$ into $\bar{K}$ that extend the embedding of K into $\bar{K}$, corresponding to the roots of the minimal polynomial of α. By induction, each of these embeddings extends to exactly l embeddings of $L/K[\alpha]$ into $\bar{K}$, completing the proof. □

Exercise 25. If L is a splitting field for $f(X) \in K[X]$, then $|\mathrm{Gal}(L/K)| \leq |L : K|$, with equality if $f(X)$ is separable.[9]

The relationship between subgroups of $\mathrm{Gal}(L/K)$ and subfields of L is inclusion reversing. If $K \leq L \leq M$, then $\mathrm{Gal}(M/L) \leq \mathrm{Gal}(M/K)$. Given a finite extension L of K, we can define a correspondence between intermediate fields $K \leq F \leq L$ and subgroups of $\mathrm{Gal}(L/K)$. Namely, for any subgroup $H \leq \mathrm{Gal}(L/K)$, the corresponding *fixed field K^H* is the subfield of L fixed by H. Conversely, given an intermediate field F, the corresponding subgroup is the set of elements of $\mathrm{Gal}(L/K)$ fixing F.

Exercise 26. Convince yourself that if $H \leq \mathrm{Gal}(L/K)$, then the set of elements of L fixed by H is a field. Conversely, that if $K \leq F \leq L$, the set of elements of $\mathrm{Gal}(L/K)$ fixing F is a group.

Example 1.31. There are no nontrivial intermediate fields for $\mathbb{Q}[\sqrt{2}]$ or $\mathbb{Q}[\sqrt[3]{2}]$. (Why?) A straightforward but tedious calculation shows that

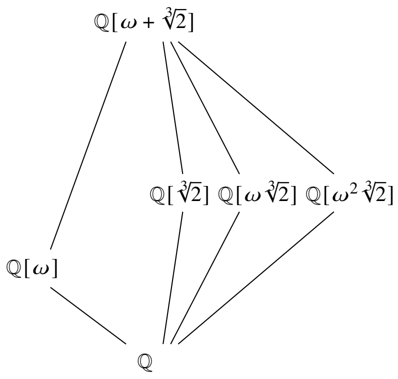
$$\mathrm{Gal}(\mathbb{Q}[\omega + \sqrt[3]{2}]/\mathbb{Q}) = S_3$$

(Our first example of a nonabelian Galois group!) The following theorem tells us how to look for its intermediate fields.

Theorem 1.32 (Fundamental theorem of Galois theory)**.** *The correspondence between intermediate fields of L/K and subgroups of $\mathrm{Gal}(L/K)$ is one-to-one if and only if L is a Galois extension of K. Further, an intermediate field K^H is Galois if and only if the corresponding subgroup H is normal, in which case $\mathrm{Gal}(K^H/K) = \mathrm{Gal}(L/K)/H$.*

Example 1.33. S_3 has a unique subgroup of order 3 and index 2, and this corresponds to the field $\mathbb{Q}[\omega]$ which is a degree 2 extension of $\mathbb{Q}$. This subgroup is normal, so $\mathbb{Q}[\omega]$ is a Galois extension of $\mathbb{Q}$. However, S_3 has three subgroups of order 2, corresponding to the intermediate fields $\mathbb{Q}[\sqrt[3]{2}]$, $\mathbb{Q}[\omega\sqrt[3]{2}]$, and $\mathbb{Q}[\omega^2\sqrt[3]{2}]$. None of these fields is Galois. Because $\mathbb{Q}[\omega + \sqrt[3]{2}]$ is Galois, these determine all its intermediate fields.

[9] *Hint:* Take an irreducible factor $p(X)$ of $f(X)$ and let $\alpha \in L$ be a root of $p(X)$. For fixed $\sigma \in \mathrm{Gal}(L/K)$, how many possibilities exist for $\sigma|_{K[\alpha]}$? Now proceed by induction with the extension $L/K[\alpha]$.


$\mathbb{Q}[\omega + \sqrt[3]{2}]$
$\mathbb{Q}[\sqrt[3]{2}]$
$\mathbb{Q}[\omega\sqrt[3]{2}]$
$\mathbb{Q}[\omega^2\sqrt[3]{2}]$
$\mathbb{Q}[\omega]$
$\mathbb{Q}$

Exercise 27. Let $f(X) \in \mathbb{Z}[X]$ be an irreducible monic polynomial such that the Galois group of its splitting field is abelian. If it has one root $\alpha \in C$ such that $|\alpha| = 1$, show that all of its roots have absolute value 1.

Exercise 28. Let α be an algebraic integer whose Galois conjugates all have absolute value 1. Show that α is a root of unity.

Finally, let us look at the Galois theory of finite fields $\mathbb{F}_p$. For proofs and more see [1].

Exercise 29. Show that:

(i) A finite integral domain is a field.

(ii) Every finite field has prime power order, and for every prime power there is a unique finite field of that order.

(iii) The multiplicative group G of a finite field is cyclic.[10]

The following classification is extremely important, and we will revisit the Frobenius automorphism later. The proof of the theorem is left as an exercise. (It follows easily from the results in this section.)

Theorem 1.34. *Any finite extension of $\mathbb{F}_q$ is of the form $\mathbb{F}_{q^n}$, and $|\mathbb{F}_{q^n} : \mathbb{F}_q| = n$. The field $\mathbb{F}_{q^n}$ is the splitting field of $X^{q^n} - X$ over $\mathbb{F}_q$. Its Galois group is cyclic and generated by the Frobenius automorphism*

$$\sigma : x \longrightarrow x^q.$$

2 Rings of integers

The ring of integers $\mathbb{Z}$ is a Euclidean domain (hence a PID, and hence a UFD), and it is *integrally closed* in $\mathbb{Q}$: any rational number that is the root of a polynomial in $\mathbb{Z}[X]$ is an integer. We say K is a *number field* if K is a finite extension of $\mathbb{Q}$. What is the analog of the integers in K? Intuitively, we would like this to be the set of elements of K that are the corresponding "extension" of $\mathbb{Z}$; this is not far from the truth. In this section, we will show that the ring of integers of a number field is finitely generated, and then see how these generators correspond to the generators of $K/\mathbb{Q}$.

2.1 Trace, norm, and discriminant

For the rest of this section, we assume L is a finite extension of K.

[10] *Hint:* let G_d be the set of elements of G that have order d. Show that $|G_d| \leq \phi(d)$.

2.1.1 The trace and norm

Definition 2.1. The *trace* and *norm* of $a \in L$ are the trace and determinant respectively of the K-linear map $T_a : L \longrightarrow L$, $T_a(x) = ax$.

It follows immediately that these induce homomorphisms

$$\mathrm{Tr}_{L/K} : L \to K,$$

$$\mathrm{Nm}_{L/K} : L^\times \to K^\times.$$

Sometimes we will drop the subscript and simply write $\mathrm{Tr}(a)$ or $\mathrm{Nm}(a)$, when the extension L/K is clear from context.

Example 2.2. Consider the extension $\mathbb{Q}[i]/\mathbb{Q}$, and choose the basis $\{1, i\}$. For an element $a + bi \in \mathbb{Q}[i]$, the matrix of the corresponding linear map in this basis is given by

$$T_{a+bi} = \begin{bmatrix} a & -b \\ b & a \end{bmatrix}.$$

Thus, $\mathrm{Tr}(a + bi) = 2a$, and $\mathrm{Nm}(a + bi) = a^2 + b^2$.

Exercise 30. Let $D \in \mathbb{Z}$ be a squarefree integer and $K = \mathbb{Q}[\sqrt{D}]$. For $a, b \in \mathbb{Z}$, show that $\mathrm{Tr}_{K/Q}(a + b\sqrt{D}) = 2a$ and $\mathrm{Nm}_{K/Q}(a + b\sqrt{D}) = a^2 - Db^2$.

The following theorem gives an extremely useful characterisation of the trace and norm with the Galois group.

Theorem 2.3. *Let L/K be a separable extension and $\sigma : L \longrightarrow \bar{K}$ vary over* $\mathrm{Hom}_K(L, \bar{K})$. *For any $a \in L$, if $f_a(X) \in K[X]$ is the characteristic polynomial of the linear map $T_a : L \longrightarrow L$ as above, then,*

(1) $f_a(X) = \prod_\sigma (X - \sigma a)$,

(2) $\mathrm{Tr}_{L/K}(a) = \sum_\sigma \sigma a$, *and*

(3) $\mathrm{Nm}_{L/K}(a) = \prod_\sigma \sigma a$.

Proof. It suffices to prove (1), as (2) and (3) follow by examining the coefficients of the characteristic polynomial. Fix $a \in L$, and consider the tower of field extensions $K \leq K[a] \leq L$. Let $|L : K[a]| = l$ and $|K[a] : K| = k$. The minimal polynomial $m_a(X) = X^k + a_{k-1}X^{k-1} + \cdots + a_1X + a_0 \in K[X]$ of a over K has degree k (why?), and $\{1, a, \ldots, a^{k-1}\}$ is a basis of $K[a]/K$. Choose a basis $b_1, \ldots, b_l$ of $L/K[a]$ so that $\{b_1a^i, \ldots, b_la^i : 0 \leq i \leq k-1\}$ is a basis of L/K. The matrix of T_a in this basis is block diagonal, with each block equal to

$$\begin{bmatrix} 0 & \ldots & 0 & -a_0 \\ 1 & \ldots & 0 & -a_1 \\ & & \ldots & \\ 0 & \ldots & 1 & -a_{k-1} \end{bmatrix}.$$

It now follows that the characteristic polynomial satisfies $f_a(X) = \left(m_a(X)\right)^l$.

Define an equivalence relation $\sim$ on $\mathrm{Hom}_K(L, \bar{K})$ by $\sigma \sim \tau$ if and only if $\sigma(a) = \tau(a)$. This defines exactly k equivalence classes with l elements each. (Why?) Choose a system of representatives $\sigma_1, \ldots, \sigma_k$. It follows that

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

$$f_a(X) = \prod_{i=1}^{k} (X - \sigma_i(a))^l = \prod_\sigma (X - \sigma(a)).$$

□

Exercise 31. If L/K is Galois, then $\mathrm{Hom}_K(L, \bar{K}) = \mathrm{Gal}(L/K)$.

Exercise 32. Show that if $|K : \mathbb{Q}| = 2$, then $K = \mathbb{Q}[\sqrt{D}]$ for a squarefree integer $D \in \mathbb{Z}$.[11]

Example 2.4. For $z \in \mathbb{Q}[i]$, its Galois conjugates over $\mathbb{Q}$ are z and $\bar{z}$, its complex conjugate. The minimal polynomial of z is $X^2 - (z + \bar{z}) + z\bar{z}$.

Consider the extension $\mathbb{Q}[\sqrt[3]{2}]/\mathbb{Q}$, which is not Galois. $\mathrm{Hom}_{\mathbb{Q}}(\mathbb{Q}[\sqrt[3]{2}], \mathbb{Q}) = \{\sigma_1, \sigma_2, \sigma_3\}$, where $\sigma_1(\sqrt[3]{2}) = \sqrt[3]{2}$, $\sigma_2(\sqrt[3]{2}) = \omega\sqrt[3]{2}$, and $\sigma_3(\sqrt[3]{2}) = \omega^2\sqrt[3]{2}$. The "conjugates" of an element $a + b\sqrt[3]{2} + c\sqrt[3]{4}$ are given by $a + b\sqrt[3]{2} + c\sqrt[3]{4}$, $a + b\omega\sqrt[3]{2} + c\omega\sqrt[3]{4}$, and $a + b\omega^2\sqrt[3]{2} + c\omega^2\sqrt[3]{4}$. Let $K = \mathbb{Q}[\sqrt[3]{2}]$. The theorem tells us that $\mathrm{Tr}_{K/\mathbb{Q}}(\sqrt[3]{2}) = 0$ and $\mathrm{Nm}_{K/\mathbb{Q}}(\sqrt[3]{2}) = 2$.

Now take the normal closure of K, the field $L = \mathbb{Q}[\omega + \sqrt[3]{2}]$. Recall that $|\mathrm{Gal}(L/\mathbb{Q})| = 6$, determined by the images of $\sqrt[3]{2}$ and ω. With the same notation as the theorem, $m_{\sqrt[3]{2}}(X) = X^3 - 2$, but the characteristic polynomial $f_{\sqrt[3]{2}}(X) = \left(X^3 - 2\right)^2$. In this extension, $\mathrm{Nm}_{L/\mathbb{Q}}(\sqrt[3]{2}) = 4$. The trace and norm are not intrinsic properties of an element, but depend on the extension (as the next corollary will show).

Corollary 2.5. *If $K \leq L \leq M$ are finite extensions,* $\mathrm{Tr}_{L/K} \circ \mathrm{Tr}_{M/L} = \mathrm{Tr}_{M/K}$ *and* $\mathrm{Nm}_{L/K} \circ \mathrm{Nm}_{M/L} = \mathrm{Nm}_{M/K}$.

Proof. Let us only concern ourselves with the case when both extensions are separable so we can apply the previous theorem. The statement is also true for inseparable extensions, but the proof is more complicated.

Since L is algebraic over K, $\bar{L} = \bar{K}$. Define an equivalence relation $\sim$ on $\mathrm{Hom}_K(M, \bar{K})$ by $\sigma \sim \tau$ if $\sigma(L) = \tau(L)$. $\mathrm{Hom}_L(M, \bar{K})$ forms one equivalence class, and there are $l = |L : K|$ equivalence classes of $m = |M : L|$ elements each. Choose representatives $\sigma_1, \ldots, \sigma_l$. The equivalence class of σ_i is $\mathrm{Hom}_{\sigma_i(L)}(\sigma_i(M), \bar{K})$, and $\mathrm{Hom}_K(L, \bar{K}) = \{\sigma_1|_L, \ldots, \sigma_l|_L\}$.

$$\mathrm{Tr}_{M/K}(a) = \sum_{\sigma} \sigma(a) = \sum_{i=1}^{l} \sum_{\sigma \sim \sigma_i} \sigma(a) = \sum_{i=1}^{l} \mathrm{Tr}_{\sigma_i(M)/\sigma_i(L)}(\sigma_i a) = \sum_{i=1}^{m} \sigma_i \mathrm{Tr}_{M/L}(a) = \mathrm{Tr}_{L/K} \circ \mathrm{Tr}_{M/L}(a)$$

The equality for the norm is analogous. □

Exercise 33. Where did we use separability?

Corollary 2.6. *Given $AKLB$[12], if $b \in B$, then* $\mathrm{Tr}_{L/K}(b)$ *and* $\mathrm{Nm}_{L/K}(b)$ *are in A.*

Exercise 34. Show that $a + bi \in \mathbb{Z}[i]$ if and only if $\mathrm{Tr}_{\mathbb{Q}[i]/\mathbb{Q}}(a + bi) \in \mathbb{Z}$ and $\mathrm{Nm}_{\mathbb{Q}[i]/\mathbb{Q}}(a + bi) \in \mathbb{Z}$.

Exercise 35. Let $K = \mathbb{Q}[\sqrt{5}]$. Show that $\mathrm{Tr}_{K/\mathbb{Q}}(\frac{1+\sqrt{5}}{2}) \in \mathbb{Z}$ and $\mathrm{Nm}_{K/\mathbb{Q}}(\frac{1+\sqrt{5}}{2}) \in \mathbb{Z}$.

Exercise 36. Show that if K is a number field and B its ring of integers, then the units of B are the elements of norm ± 1, i.e.

$$\{b \in B : b^{-1} \in B\} = \{b \in B : \mathrm{Nm}_{K/\mathbb{Q}}(b) = \pm 1\}.$$

2.1.2 The discriminant

Now suppose $\{\alpha_1, \ldots, \alpha_n\}$ is a basis of L/K.

Definition 2.7. The *discriminant* of the basis is defined as the determinant of the matrix $\left(\mathrm{Tr}_{L/K} \alpha_i \alpha_j\right)_{i,j=1}^{n}$.

Exercise 37. Find the discriminant of the basis $\{1, \sqrt{D}\}$ of $\mathbb{Q}[\sqrt{D}]$, where $D \in \mathbb{Z}$ is a squarefree integer.

Let $\mathrm{Hom}_K(L, \bar{K}) = \{\sigma_1, \ldots, \sigma_n\}$. Then

$$\mathrm{Tr}_{L/K}(\alpha_i \alpha_j) = \sum_{k=1}^{n} (\sigma_k \alpha_i)(\sigma_k \alpha_j),$$

[11] *Hint:* find an element $a \in K$ such that $\mathrm{Tr}(a) = 0$ and $\mathrm{Nm}(a)$ is a squarefree integer.

[12] A is an integrally closed domain, K its field of fractions, L a finite extension of K, and B the integral closure of A in L.

so the matrix $\left(\mathrm{Tr}_{L/K}\alpha_i\alpha_j\right)_{i,j=1}^n$ is the product of the matrices $\left(\sigma_i\alpha_j\right)^T\left(\sigma_i\alpha_j\right)$, and

$$d(\alpha_1,\dots,\alpha_n)=\det\left(\sigma_i\alpha_j\right)^2$$

The following lemma is elementary linear algebra:

Lemma 2.8. *If $\{\beta_1,\dots,\beta_n\}$ is a basis for L/K and $\alpha_1,\dots,\alpha_n\in L$, write*

$$\alpha_j=\sum_{i=1}^n a_{ji}\beta_i$$

for each $j=1,\dots,n$. $\{\alpha_1,\dots,\alpha_n\}$ is a basis for L/K if and only if $\det\left(a_{ij}\right)$ *is invertible. In this case,*

$$d(\alpha_1,\dots,\alpha_n)=\det\left(a_{ij}\right)^2\cdot d(\beta_1,\dots,\beta_n).$$

Proposition 2.9. *If L/K is finite and separable, then $d(\alpha_1,\dots,\alpha_n)\neq 0$ and $\langle x,y\rangle=\mathrm{Tr}(xy)$ is a nondegenerate bilinear form.*

Proof. By the lemma, it suffices to show this for a fixed basis of L/K. Every finite separable extension is simple, so write $L=K[\theta]$, and let $|L:K|=n$. The matrix $\left(\sigma_i\theta^j\right)$ is a Vandermonde matrix with nonzero determinant (why?), so $d(1,\theta,\dots,\theta^{n-1})\neq 0$. Further, the matrix $\left(\mathrm{Tr}(\theta^{i+j})\right)$ is the matrix associated to the bilinear form, and as it has nonzero determinant, the form is nondegenerate. □

Lemma 2.10 (Dedekind's lemma)**.** *If L/K is finite and separable, the elements of* $\mathrm{Hom}_K(L,\bar{K})$ *are linearly independent over K.*

Proof. Let $\mathrm{Hom}_K(L,\bar{K})=\{\sigma_1,\dots,\sigma_n\}$. Suppose there exist $a_1,\dots,a_n\in K$ such that

$$\sum_{i=1}^n a_i\sigma_i\equiv 0.$$

Choose a basis $\{\alpha_1,\dots,\alpha_n\}$ for L/K. Then,

$$\left(\sigma_j\alpha_i\right)_{i,j=1}^n\cdot\begin{bmatrix}a_1\\ \vdots\\ a_n\end{bmatrix}=\begin{bmatrix}\sum_{j=1}^n a_j\sigma_j(\alpha_1)\\ \vdots\\ \sum_{j=1}^n a_j\sigma_j(\alpha_n)\end{bmatrix}=\begin{bmatrix}0\\ \vdots\\ 0\end{bmatrix}.$$

Since $\det\left(\sigma_j\alpha_i\right)\neq 0$, it follows that $a_i=0$ for all $i=1,\dots,n$. □

Theorem 2.11 (Hilbert 90)**.** *Let L/K be Galois with cyclic Galois group of order n generated by σ. For $\alpha\in L$,* $\mathrm{Nm}_{L/K}(\alpha)=1$ *if and only if $\alpha=\beta/\sigma(\beta)$ for some $\beta\in L$.*

Proof. The direction $\Longleftarrow$ follows from the multiplicativity of the norm. Conversely, given $\alpha\in L$ of norm 1, we want to find $\beta\in L$ such that $\beta=\alpha\sigma(\beta)$. In other words, we want a nonzero fixed point of the operator $\alpha\sigma$ defined by $\alpha\sigma(x)=\alpha\cdot\sigma(x)$. Choose any $\gamma\in L$ and suppose $\alpha\sigma(\gamma)\neq\gamma$. Set

$$\beta=\gamma+\alpha\sigma(\gamma)+(\alpha\sigma)^2(\gamma)+\cdots+(\alpha\sigma)^{n-1}(\gamma)$$

Then

$$(\alpha\sigma)^n=\alpha\sigma(\alpha)\dots\sigma^{n-1}(\alpha)=\mathrm{Nm}_{L/K}(\alpha)=1$$

is the identity map, so β is a fixed point of $\alpha\sigma$. Since $1,\sigma,\dots,\sigma^{n-1}$ are linearly independent by Dedekind's lemma, β is nonzero. □

One interpretation of Hilbert's theorem 90 is that an element α has norm 1 if and only if the linear map $\alpha\sigma$ has an eigenvector with eigenvalue 1. Here is an interesting application of the theorem to classification of Pythagorean triples. A Pythagorean triple is a triple $a, b, c \in \mathbb{Z}$ such that $a^2 + b^2 = c^2$, and the integers are pairwise coprime. Equivalently, setting $K = \mathbb{Q}[i]$, $\mathrm{Nm}_{K/\mathbb{Q}}(a + bi) = c^2$, or $\mathrm{Nm}_{K/\mathbb{Q}}(\frac{a}{c} + \frac{b}{c}i) = 1$. By Hilbert's theorem 90, there exist coprime integers $u, v \in \mathbb{Z}$ such that

$$\frac{a}{c} + \frac{b}{c}i = \frac{u + vi}{u - vi} = \frac{u^2 - v^2}{u^2 + v^2} + \frac{2uv}{u^2 + v^2}i.$$

This implies that $a = u^2 - v^2$, $b = 2uv$, and $c = u^2 + v^2$, so any Pythagorean triple has this form. Conversely, any integers satisfying these identities form a Pythagorean triple.

Exercise 38. Let K be a field containing a primitive nth root of unity, and L/K an extension such that $\mathrm{Gal}(L/K) = \mathbb{Z}_n$. Show that $L = K[\alpha^{1/n}]$ for some $\alpha \in K$.

Remark. We do not need B to be free as an A-module in order to make sense of the discriminant. Each element $b \in B$ defines a K-linear map, so its trace is well-defined. It follows from theorem 2.3 that if $\{b_1, \dots, b_n\}$ is a basis for B as an A-module, then its discriminant $d(b_1, \dots, b_n) \in A$. Further, if $\{b_1, \dots, b_n\}$ and $\{c_1, \dots, c_n\}$ are bases of B/A, then their respective discriminants differ only by a unit of A. We can refer to *the* discriminant of B/A as the ideal generated by the discriminant of some basis.

2.1.3 Integral bases

Definition 2.12. Suppose $AKLB$ and $|L : K| = n$. We say $\{w_1, \dots, w_n\} \subset B$ is an *integral basis* for L/K if it is a basis for L/K and $B = \bigoplus A \cdot w_i$ as a free A-module.

Example 2.13. $\{1, i\}$ is an integral basis for $\mathbb{Q}[i]$.

Exercise 39. $\{1, \sqrt{5}\}$ is *not* an integral basis for $\mathbb{Q}[\sqrt{5}]$.

Proposition 2.14. *If* $\{\alpha_1, \dots, \alpha_n\} \subset B$ *is a basis of* L/K *and* $d = d(\alpha_1, \dots, \alpha_n)$*, then*

$$d \cdot B \subset \bigoplus_{i=1}^{n} A \cdot \alpha_i \subset B.$$

Proof. The second inclusion is clear; for the first, we need to show that $d\beta \in \bigoplus_{i=1}^n A \cdot \alpha_i$ for each $\beta \in B$. Write

$$\beta = x_1\alpha_1 + \cdots + x_n\alpha_n : \quad x_1, \dots, x_n \in K.$$

By corollary 2.6, for $i, j = 1, \dots, n$, $\mathrm{Tr}(\alpha_i\beta)$ and $\mathrm{Tr}(\alpha_i\alpha_j)$ are in A. Define $M = \Big(\mathrm{Tr}(\alpha_i\alpha_j)\Big)_{i,j=1}^n \in A^{n\times n}$, and $x = (x_i)_{i=1}^n \in K^n$. Then,

$$Mx = (\mathrm{Tr}(\alpha_i\beta))_{i=1}^n \in A^n,$$

so if $M^* \in A^{n\times n}$ is the adjoint[13] of M,

$$M^*Mx = \det(M)x = dx \in A^n.$$

In particular, $dx_i \in A$ for each i, so $d\beta \in \bigoplus_{i=1}^n A \cdot \alpha_i$.

□

Theorem 2.15. *If A is a PID and L/K is separable, then B has an integral basis (B is a free A-module).*

[13] Recall that the adjoint M^* is defined by $M^*_{i,j} = (-1)^{i+j} \det M(i, j)$, where $M(i, j)$ is the submatrix of M obtained by deleting the i^{th} row and j^{th} column. If $M \in A^{n\times n}$, so is M^*, as taking adjoints is closed under the ring operations.

Proof. This is really a corollary: let $\{\alpha_1, \dots, \alpha_n\} \subset B$ be a basis for L/K and d its discriminant. Then,

$$\bigoplus_{i=1}^{n} A\alpha_i \subseteq B \subseteq \bigoplus_{i=1}^{n} A\frac{\alpha_i}{d}.$$

Every submodule of a free module over a PID is free, so B is a free A-module. The two inclusions imply that B has rank n as an A-module, so $B = \bigoplus_{i=1}^{n} Aw_i$ where $\{w_1, \dots, w_n\}$ is a basis of L/K. □

Corollary 2.16. *The ring of integers in a number field is finitely generated (and free) as a $\mathbb{Z}$-module.*

Exercise 40. Suppose $AKLB$ where A is a PID and L/K is separable. Any ideal $I \lhd B$ is a free A-module of the same rank as B.

Exercise 41. Suppose L is a number field. Show that the discriminant of an integral basis is independent of the choice of basis.

From now on, when we refer to *the* discriminant of a number field, we will mean the discriminant of an integral basis. For number fields, we can generalise the definition of discriminant to ideals $I \lhd B$, as they are also free $\mathbb{Z}$-modules.

Definition 2.17. Suppose L is a number field and B its ring of integers. For any ideal $I \lhd B$, if $I = \bigoplus_{i=1}^{n} \mathbb{Z}w_i$, define

$$d(I) = d(w_1, \dots, w_n).$$

Exercise 42. Show that when L is a number field, $d(I)$ is independent of the choice of basis.

Proposition 2.18. *Suppose L is a number field and B its ring of integers. If $I \leq I'$ are ideals in B, then*

$$d(I) = |I' : I|^2 \cdot d(I').$$

Proof. Fix bases for I and I', and let $M \in \mathbb{Z}^{n \times n}$ be the transition matrix from I' to I. On one hand,

$$d(I) = \det(M)^2 d(I')$$

and on the other hand by theorem 1.3, $\det(M) = |I' : I|$, completing the proof. □

The following sequence of exercises determine the discriminants of quadratic number fields. Let $D \in \mathbb{Z}$ be a squarefree integer, $L = \mathbb{Q}[\sqrt{D}]$, and B the ring of integers in L.

Exercise 43. Given $x \in L$, show that $x \in B$ if and only if $\mathrm{Tr}_{L/\mathbb{Q}}(x)$ and $\mathrm{Nm}_{L/\mathbb{Q}}(x) \in \mathbb{Z}$.

Exercise 44. Show that if $D \equiv 1 \pmod 4$, then $B = \mathbb{Z} \oplus \mathbb{Z}\left(\frac{1+\sqrt{D}}{2}\right)$. If $D \equiv 2$ or $3 \pmod 4$, then $B = \mathbb{Z} \oplus \mathbb{Z}\sqrt{D}$.

Exercise 45. Let d be the discriminant of L. Show that $d = D$ if $D \equiv 1 \pmod 4$, and $d = 4D$ if $D \equiv 2$ or $3 \pmod 4$.

Finally, a natural question to ask is whether the discriminant is multiplicative, and the answer is: almost.

Proposition 2.19. *Let L_m and L_n be Galois extensions of K of degree m and n respectively such that $L_1 \cap L_2 = K$. Let $\{\alpha_1, \dots, \alpha_m\}$ (resp. $\{\beta_1, \dots, \beta_n\}$) be an integral basis of L_m (resp. L_n) with discriminant c (resp. d). Suppose c and d are coprime, i.e. $xc + yd = 1$ for some $x, y \in A$. Then $\{\alpha_i\beta_j : i = 1, \dots, m; j = 1, \dots, n\}$ is an integral basis of L_mL_n with discriminant $c^n d^m$.*

Exercise 46 (Stickelberger's discriminant relation). Let d be the discriminant of a number field K. Show that $d \equiv 0$ or $1 \bmod 4$.[14]

[14] *Hint:* The determinant of the matrix $(\sigma_i w_j)$ can be written as the difference of positive terms P and negative terms N. Show that $d = (P - N)^2 = (P + N)^2 - 4PN$.

2.2 Dedekind domains

What structure of $\mathbb{Z}$ carries over to the ring of integers?

Definition 2.20. A domain $\mathcal{O}$ is a Dedekind domain if it is Noetherian, integrally closed, and has dimension 1 (i.e. every prime ideal is maximal).

Theorem 2.21. *The ring of integers $\mathcal{O}_K$ in a number field K is a Dedekind domain.*

Proof. $\mathcal{O}_K$ is a finitely generated $\mathbb{Z}$-module, so it is Noetherian, and integrally closed by definition. Any prime ideal $\mathfrak{p} \lhd \mathcal{O}_K$ is a free module of the same rank, and has finite index, so $\mathcal{O}_K/\mathfrak{p}$ is a finite integral domain. In other words, $\mathcal{O}_K/\mathfrak{p}$ is a finite field, so $\mathfrak{p}$ is maximal. □

Our goal for this section is to show that every ideal in a Dedekind domain factors uniquely as a product of prime ideals. This extends the unique factorisation in $\mathbb{Z}$, and is in fact a characterisation of a Dedekind domain. We will then prove another characterisation of Dedekind domains involving localisations.

2.2.1 Unique factorisation of ideals

Let K be the field of fractions of $\mathcal{O}$, a Dedekind domain.

Lemma 2.22. *Every nonzero ideal in $\mathcal{O}$ contains the product of some nonzero prime ideals.*

Proof. Let S be the set of nonzero ideals which do not contain a product of nonzero prime ideals. If S is nonempty, since $\mathcal{O}$ is Noetherian, S contains a maximal element I. The ideal I cannot be prime, so there is a product $ab \in I$ such that $a, b \notin I$. Then $\langle I, a\rangle$ and $\langle I, b\rangle$ both contain products of nonzero prime ideals by the maximality of I, but

$$\langle I, a\rangle\langle I, b\rangle = \langle I^2, aI, bI, ab\rangle \subseteq I,$$

so I contains a product of nonzero prime ideals. □

Definition 2.23. A *fractional ideal* of $\mathcal{O}$ is a nonzero finitely generated $\mathcal{O}$-submodule of K.

Exercise 47. An $\mathcal{O}$-submodule $J \leq K$ is a fractional ideal of $\mathcal{O}$ if and only if there exists $c \neq 0$, $c \in \mathcal{O}$ such that $cJ \subset \mathcal{O}$.

For a fractional ideal J, define $J^{-1} = \{\alpha \in K : \alpha J \subset \mathcal{O}\}$. It follows from the exercise that when $I \lhd \mathcal{O}$, I^{-1} is a fractional ideal of $\mathcal{O}$.

Lemma 2.24. *If $I \lhd \mathcal{O}$ is a nonzero ideal, and $\mathfrak{p} \lhd \mathcal{O}$ is a nonzero prime ideal, then $I\mathfrak{p}^{-1} \neq I$.*

Proof. Since $\mathcal{O} \subseteq \mathfrak{p}^{-1}$, $I \subseteq I\mathfrak{p}^{-1}$. We need to show that this inclusion is strict. We first prove the lemma when $I = \mathcal{O}$. Let $a \in \mathfrak{p}$ be nonzero, and n be the least integer such that there is a product of prime ideals $\mathfrak{p}_1 \dots \mathfrak{p}_n \subseteq \langle a\rangle$. Since $\mathfrak{p}_1 \dots \mathfrak{p}_n \subseteq \mathfrak{p}$ and $\mathcal{O}$ has dimension 1, one of them, say $\mathfrak{p}_1 = \mathfrak{p}$. By the minimality of n, $\mathfrak{p}_2 \dots \mathfrak{p}_n \not\subset \langle a\rangle$. Choose $b \in \mathfrak{p}_2 \dots \mathfrak{p}_n \setminus \langle a\rangle$. Then $ba^{-1} \notin \mathcal{O}$, but

$$b\mathfrak{p} \subseteq \langle a\rangle \implies ba^{-1}\mathfrak{p} \subseteq \mathcal{O} \implies ba^{-1} \in \mathfrak{p}^{-1} \setminus \mathcal{O}.$$

Now let I be an arbitrary nonzero ideal in $\mathcal{O}$, and suppose for contradiction that $I\mathfrak{p}^{-1} = I$. Let I be generated by $\{b_1, \dots, b_n\}$ and let $a \in \mathfrak{p}^{-1}$. For each $j = 1, \dots, n$, express

$$ab_j = \sum_{i=1}^{n} a_{ij}\beta_i; \quad a_{ij} \in \mathcal{O}.$$

Let A be the matrix $\left(a_{ij}\right)_{i,j=1}^{n}$, and $\beta = (b_i)_{i=1}^{n}$. Since β is nonzero and $A\beta = a \cdot \beta$, $\det(a\mathrm{Id} - A) = 0$. Then $a \in K$ is the root of a monic polynomial with coefficients in $\mathcal{O}$, so $a \in \mathcal{O}$ since $\mathcal{O}$ is integrally closed. But this implies $\mathfrak{p}^{-1} = \mathcal{O}$, contradicting the first part of this proof. □

Lemma 2.25. *If $\mathfrak{p} \lhd \mathcal{O}$ is prime, then $\mathfrak{p}\mathfrak{p}^{-1} = \mathcal{O}$.*

Proof. Since $\mathcal{O} \subsetneq \mathfrak{p}^{-1}$, $\mathfrak{p} \subsetneq \mathfrak{p}\mathfrak{p}^{-1} \subseteq O$. By the maximality of $\mathfrak{p}$, $\mathfrak{p}\mathfrak{p}^{-1} = \mathcal{O}$. □

We are finally ready to prove our main result.

Theorem 2.26. *Every ideal of $\mathcal{O}$ factors uniquely as a product of prime ideals.*

Proof. Suppose not. Since $\mathcal{O}$ is Noetherian, by Zorn's lemma we can choose a maximal ideal I that does not factor into a product of prime ideals. There is a prime ideal $\mathfrak{p}$ properly containing I. Then $I \subsetneq I\mathfrak{p}^{-1} \subsetneq \mathcal{O}$, and by the maximality of I, $I\mathfrak{p}^{-1}$ admits a factorisation $I\mathfrak{p}^{-1} = \mathfrak{p}_1 \dots \mathfrak{p}_r$. However,

$$I\mathfrak{p}^{-1}\mathfrak{p} = I\mathcal{O} = I = \mathfrak{p}_1 \dots \mathfrak{p}_r \mathfrak{p}$$

is a factorisation of I. This concludes the proof of existence.

For uniqueness, suppose

$$\mathfrak{p}_1 \dots \mathfrak{p}_r = \mathfrak{q}_1 \dots \mathfrak{q}_s,$$

where $\mathfrak{p}_1, \dots, \mathfrak{p}_r, \mathfrak{q}_1, \dots, \mathfrak{q}_s$ are nonzero prime ideals in $\mathcal{O}$. Since $\mathfrak{q}_1 \dots \mathfrak{q}_s \subseteq \mathfrak{p}_1$, one of them, say $\mathfrak{q}_1 = \mathfrak{p}_1$. Just as in the proof of the fundamental theorem of arithmetic, we proceed recursively to show that $r = s$ and, after an appropriate permutation, $\mathfrak{q}_i = \mathfrak{p}_i$ for each $i = 1, \dots, r$. □

Corollary 2.27. *The set of fractional ideals of $\mathcal{O}$ is the free abelian group generated by the prime ideals of $\mathcal{O}$.*

Proof. The commutativity and associativity of fractional ideal multiplication are straightforward, and $\mathcal{O}$ is an identity for this operation. Suppose $I = \mathfrak{p}_1 \dots \mathfrak{p}_r$ is an ideal in $\mathcal{O}$. We claim that $I^{-1} = \mathfrak{p}_1^{-1} \dots \mathfrak{p}_r^{-1}$, where I^{-1} is as defined earlier. Set $B = \mathfrak{p}_1^{-1} \dots \mathfrak{p}_r^{-1}$. Clearly $IB = \mathcal{O}$, so $B \subseteq I^{-1}$. Conversely, if $x \in I^{-1}$, then $xI \subset \mathcal{O}$, and $x \in x\mathcal{O} = xIB \subseteq B$, so $x \in B$.

Finally, suppose J is an arbitrary fractional ideal of $\mathcal{O}$. Let $c \in \mathcal{O}$ be nonzero so that $cJ \lhd \mathcal{O}$. Then, $c(cJ)^{-1}$ is an inverse for J.

Finally, to show that this group is freely generated by the prime ideals, let $J \leq K$ and $c \in \mathcal{O}$ be as above. We can factor the ideals $cJ = \mathfrak{p}_1^{r_1} \dots p_m^{r_m}$ and $\langle c \rangle = \mathfrak{p}_1^{s_1} \dots \mathfrak{p}_m^{s_m}$, so $J = \mathfrak{p}_1^{r_1 - s_1} \dots p_m^{r_m - s_m}$. The freeness follows from unique factorisation. □

Exercise 48. Let $\mathcal{O}$ be a Dedekind domain. $\mathcal{O}$ is a PID if and only if $\mathcal{O}$ is a UFD.

Exercise 49. If $\mathcal{O}$ has only finitely many prime ideals, $\mathcal{O}$ is a PID.

Exercise 50. Each ideal in $\mathcal{O}$ is generated by at most two elements.

We will refer to ideals of $\mathcal{O}$ as *integral* ideals. Let J_K denote the set of fractional ideals of $\mathcal{O}$. Emmy Noether showed the converse: that if J_K forms a group under multiplication, then $\mathcal{O}$ is a Dedekind domain. Let $P_K \leq J_K$ denote the subgroup of principal fractional ideals.

Definition 2.28. Define the *ideal class group* $Cl_K = J_K / P_K$. $|Cl_K|$ is called the *class number* of K.

It is clear that the class group is trivial if and only if $\mathcal{O}$ is a PID. Because a Dedekind domain is a PID if and only if it is a UFD, in order to study unique factorisation in rings of integers we will instead study their class numbers.

In summary, we have the following exact sequence:

$$1 \to \mathcal{O}^\times \to K^\times \to J_K \to Cl_K \to 1.$$

Exercise 51. What are the maps that make this sequence exact?

2.2.2 Dedekind domains and localisation

Before we move on to the promised *number theory*, we will need another (equivalent) characterisation of Dedekind domains. Again, all rings are commutative integral domains.

Definition 2.29. Let $S \subset R$ be a multiplicatively closed set such that $1 \in S$ and $0 \notin S$. Define the *localisation* of R at S as

$$RS^{-1} = \{a/s : a \in R, s \in S\},$$

with multiplication and addition defined as expected.

In other words, RS^{-1} is the intermediate ring between R and its field of fractions in which all elements of S are invertible. The map $a \to a/1$ is a natural embedding of R into RS^{-1}. We are interested in the special case when $S = R \setminus P$ for a prime ideal P; we denote the localisation as R_P. We say a ring is a *local ring* if it has a unique maximal ideal.

Exercise 52. A ring is local if and only if the set of non-units forms an ideal.

Lemma 2.30. *If $P \lhd R$ is a prime ideal, then R_P is a local ring.*

Proof. Clearly PR_P is a prime ideal in R_P. It suffices to show that any element outside PR_P is invertible. If $a/s \in R_P \setminus PR_P$, then $a \in R \setminus P$, so $s/a \in R_P \setminus PR_P$. Then a/s is invertible, making PR_P the unique maximal ideal. □

Lemma 2.31. *If $P \lhd R$ is maximal, then*

$$R/_{P^n} \cong R_P/_{(PR_P)^n}.$$

Proof. Consider the map $\varphi : R \to R_P/_{(PR_P)^n}$ that sends $\varphi : a \to \frac{a}{1} + (PR_P)^n$.

$$\ker \varphi = \{a \in R : \frac{a}{1} \in (PR_P)^n\} = P^n$$

We only need to show that φ is surjective. Let $s \in R \setminus P$. By induction on n, we will show that $\langle P^n, s\rangle = R$. For $n = 1$, this is clear by the maximality of P. In general, if $\langle P^{n-1}, s\rangle = R$, then $P = P\langle P^{n-1}, s\rangle \subsetneq \langle P^n, s\rangle \leq R$. By the maximality of P, the last inclusion must be equality. So, $1 - s \cdot b \in P^n$ for some $b \in R$, and $\varphi(b) = \frac{1}{s} + (PR_P)^n$. It follows that φ is surjective. □

Lemma 2.32.

$$R = \bigcap_{P \text{ prime}} R_P$$

Proof. As R embeds in each R_P, clearly $R \subseteq \bigcap_P R_P$. Conversely, suppose $a \in \bigcap_P R_P$. Define

$$A = \{b \in R : ab \in R\}.$$

A is an ideal of R. If A is a proper ideal, then it is contained in a maximal ideal P. Since $a \in R_P$, for some $s \in R \setminus P$, $as \in R$. Then $s \in A \subseteq P$, which is not possible. This implies that $A = R$, so in particular $1 \cdot a \in R$. □

Definition 2.33. A domain R is a *discrete valuation ring* (DVR) if it is a local ring and a PID.

Corollary 2.34. *DVRs are integrally closed.*

Now we are ready to prove a second characterisation of Dedekind domains. In what follows, $\mathbb{O}$ once again denotes a Dedekind domain.

Proposition 2.35. *If $\mathbb{O}$ is Dedekind, so is $\mathbb{O}S^{-1}$.*

Proof. For any ideal $J \lhd \mathbb{O}S^{-1}$, $I = J \cap \mathbb{O}$ is finitely generated, so $J = IS^{-1}$ is finitely generated as well. Hence $\mathbb{O}$ is Noetherian. Similarly, if $\mathfrak{q} \lhd \mathbb{O}S^{-1}$ is a prime ideal, then $Q = \mathfrak{q} \cap \mathbb{O}$ is prime, therefore maximal, implying that $\mathfrak{q} = \mathfrak{q}S^{-1}$ is also maximal. Finally, we need to show that $\mathbb{O}S^{-1}$ is integrally closed in its field of fractions K. K is also the field of fractions of $\mathbb{O}$. Suppose $x \in K$ satisfies

$$x^n + (a_{n-1}/s_{n-1})x + \cdots + (a_0/s_0) = 0.$$

Multiplying by a common denominator s^n, we obtain a monic polynomial in sx over $\mathbb{O}$. Then $sx \in \mathbb{O}$, so $x \in \mathbb{O}S^{-1}$. □

Theorem 2.36. *Suppose $\mathcal{O}$ is Noetherian. $\mathcal{O}$ is Dedekind if and only if $\mathcal{O}_\mathfrak{p}$ is a DVR for every prime ideal $\mathfrak{p}$.*

Proof. If $\mathcal{O}$ is Dedekind, then $\mathcal{O}_\mathfrak{p}$ is a local ring. $\mathcal{O}_\mathfrak{p}$ is a Dedekind domain with only one prime ideal, so it is a PID (by an earlier exercise); by definition, it is a DVR.

Conversely, suppose $\mathcal{O}_\mathfrak{p}$ is a DVR for every prime ideal $\mathfrak{p}$, and that $\mathcal{O}$ is Noetherian. Suppose $\mathfrak{q} \leq \mathfrak{p}$ are prime ideals of $\mathcal{O}$. Then $\mathfrak{q}\mathcal{O}_\mathfrak{p}$ is a prime ideal in $\mathcal{O}_\mathfrak{p}$, so $\mathfrak{q} = \mathfrak{p}$, and $\mathcal{O}$ has dimension 1. Let K denote the field of fractions of $\mathcal{O}$ and suppose $a \in K$ is integral over $\mathcal{O}$. Then it is integral over $\mathcal{O}_\mathfrak{p}$ for every prime ideal $\mathfrak{p}$. Since each $\mathcal{O}_\mathfrak{p}$ is integrally closed, $a \in \bigcap_\mathfrak{p} \mathcal{O}_\mathfrak{p} = \mathcal{O}$, so $\mathcal{O}$ is integrally closed. □

Finally,

Proposition 2.37. *If L is a finite extension of K, and $\mathcal{O}_L$ the integral closure of $\mathcal{O}$ in L, then $\mathcal{O}_L$ is a Dedekind domain.*

Proof. $\mathcal{O}_L$ is integrally closed by definition. $\mathcal{O}_L$ is a finitely generated $\mathcal{O}$-module and $\mathcal{O} \leq \mathcal{O}_L$ is Noetherian, so $\mathcal{O}_L$ is Noetherian. Let $\mathfrak{P} \lhd \mathcal{O}_L$ be a prime ideal, and $\mathfrak{p} = \mathfrak{P} \cap \mathcal{O}$, so $\mathfrak{p}$ is a prime (hence maximal) ideal in $\mathcal{O}$. Let $\Bbbk = \mathcal{O}/\mathfrak{p}$. If $b \in \mathcal{O}_L/\mathfrak{P}$ is nonzero, we want to show that it is algebraic over $\Bbbk$, so that $b^{-1} \in \Bbbk[b] \leq \mathcal{O}_L/\mathfrak{P}$. Choose $\beta \in \mathcal{O}_L$ so that $\beta = b \pmod{\mathfrak{P}}$. β is the root of a monic polynomial in $\mathcal{O}_K[X]$, so b is the root of a monic polynomial in $\Bbbk[X]$. This shows that every nonzero element in $\mathcal{O}_L/\mathfrak{P}$ is invertible. □

Let $\mathcal{O}_K\mathcal{O}_L$ refer to the setup where $\mathcal{O}_K$ is a Dedekind domain, K its field of fractions, L a finite extension of K, and $\mathcal{O}_L$ the integral closure of $\mathcal{O}_K$ in L.

3 Factorisation in rings of integers

We have finally developed enough theory to study factorisation in rings of integers. We will make heavy use of key characterisations of Dedekind domains, namely that (1) every ideal factors uniquely as a product of primes, and (2) $\mathcal{O}_\mathfrak{p}$ is a DVR for every prime ideal $\mathfrak{p}$. In particular, rings of integers are Dedekind domains.

Given $\mathcal{O}_K\mathcal{O}_L$, why do we care about the ideal class group, or the structure of units in $\mathcal{O}_L$? Recall that the motivation for defining ideals is to replicate factorisation of *elements*. The ideal class group provides a partial answer to how much ideals in a ring of integers behave like elements. The other part of the answer is provided by the group of units in $\mathcal{O}_L$. Send each element of $\mathcal{O}_L^\times$ to the corresponding principal ideal; its kernel is the group of units, and its cokernel the ideal class group. The failure of this map to be an isomorphism is the failure of these groups to be trivial.

The next natural question to ask is to what extent the factorisation of ideals in $\mathcal{O}_K$ is preserved in $\mathcal{O}_L$. That is, any ideal $I \lhd \mathcal{O}_K$ factorises as a product of primes in $\mathcal{O}_K$, but the corresponding ideal $I\mathcal{O}_L \lhd \mathcal{O}_L$ also factorises as a product of primes in $\mathcal{O}_L$. Hilbert's ramification theory studies the factorisation of prime ideals of $\mathcal{O}_K$ in $\mathcal{O}_L$.

3.1 The Gaussian integers

Before we move on to more general theory, let us warm up with the ring of Gaussian integers $\mathbb{Z}[i]$. This is the ring of integers in the extension $\mathbb{Q}[i]$ of $\mathbb{Q}$. A classical result in elementary number theory says that

Theorem 3.1. *An odd prime $p \in \mathbb{Z}$ can be expressed as the sum of 2 squares if and only if $p \equiv 1 \pmod 4$.*

The implication $\implies$ is easy to see, as the only squares mod 4 are 0 and 1. The proof of the converse is less easy, because it is a statement about $\mathbb{Z}[i]$ in disguise. A prime $p = a^2 + b^2$ if and only if it factors as $p = (a + bi)(a - bi)$ in $\mathbb{Z}[i]$. So the question now becomes: which primes factor in $\mathbb{Z}[i]$?

Lemma 3.2. *$\mathbb{Z}[i]$ is a UFD.*

Proof. We will show that $\mathbb{Z}[i]$ is a Euclidean domain; for any $\alpha, \beta \in \mathbb{Z}[i]$, there exist unique elements $\rho, \gamma \in \mathbb{Z}[i]$ such that $\alpha = \gamma \cdot \beta + \rho$, and $0 \leq |\rho| < |\beta|$. Since $\mathbb{Z}[i]$ forms a *lattice* in $\mathbb{C}$, let γ be the nearest lattice point to $\frac{\alpha}{\beta}$. Then,

$$\left|\frac{\alpha}{\beta} - \gamma\right| \leq \frac{\sqrt{2}}{2} < 1.$$

Setting $\rho = \alpha - \gamma \cdot \beta$ concludes the proof. □

Lemma 3.3. *The only units in $\mathbb{Z}[i]$ are $\{\pm 1, \pm i\}$.*

Proof. Given $a + bi \in \mathbb{Z}[i]$, $\mathrm{Nm}(a + bi) = a^2 + b^2$. By an earlier exercise, $a + bi$ is a unit if and only if $a^2 + b^2 = 1$. □

Now, suppose a prime number p factors nontrivially in $\mathbb{Z}[i]$ $p = \alpha \cdot \beta$, where $\alpha, \beta \in \mathbb{Z}[i]$ are not units. Then, $p^2 = \mathrm{Nm}(p) = \mathrm{Nm}(\alpha)\mathrm{Nm}(\beta)$ in $\mathbb{Z}$. Since $\mathrm{Nm}(\alpha) \neq 1$ and $\mathrm{Nm}(\beta) \neq 1$, $p = \mathrm{Nm}(\alpha) = a^2 + b^2$ for some $a, b \in \mathbb{Z}$.

Proof of theorem 3.1. It suffices to show that if $p \equiv 1 \pmod 4$, then p is not a prime element of $\mathbb{Z}[i]$. Since -1 is a square mod p, choose $x \in \mathbb{Z}$ so that $x^2 \equiv -1 \pmod p$. Then, p divides the product $(x + i)(x - i)$ in $\mathbb{Z}[i]$, but $\frac{x}{p} \pm \frac{i}{p} \notin \mathbb{Z}[i]$, so p does not divide either of terms. This shows that p does not remain prime, and its factorisation yields an expression as a sum of two squares. □

We can in fact determine all the prime elements of $\mathbb{Z}[i]$. We say two elements a and b are *associated* if $a = ub$ for some unit u.

Theorem 3.4. *Suppose $\pi \in \mathbb{Z}[i]$ is prime. Then π is associated to an element of one of the following forms:*

i. $1 \pm i$, *or*

ii. $a + bi$, *where* $a^2 + b^2 = p$ *for some prime number* $p \equiv 1 \pmod 4$, *or*

iii. p *for some prime number* $p \equiv 3 \pmod 4$.

Proof. We have already seen that if π is of type ii or iii, then π is prime in $\mathbb{Z}[i]$. If π is of type i and $\pi = \alpha\beta$, then $2 = \mathrm{Nm}(\pi) = \mathrm{Nm}(\alpha)\mathrm{Nm}(\beta) \in \mathbb{Z}$ implies that either α or β is a unit.

Finally, it remains to see that all primes of $\mathbb{Z}[i]$ are of one of these types. Let $\pi = a + bi \in \mathbb{Z}[i]$ be prime, and let the factorisation of $\mathrm{Nm}(\pi) = \pi\bar{\pi} = p_1 \cdots p_r \in \mathbb{Z}$. This shows that π divides some prime, say p_1, so $\mathrm{Nm}(\pi)$ divides $\mathrm{Nm}(p_1) = p_1^2$. If $a^2 + b^2 = \mathrm{Nm}(\pi) = p_1$, then π is of type i or ii. If $\mathrm{Nm}(\pi) = p^2$, then π/p is a unit in $\mathbb{Z}[i]$ so π is of type iii. □

3.2 Lattices

The inclusion $\mathbb{Z}[i] \subset \mathbb{C}$, considering the Gaussian integers as lattice points in the complex plane, was useful in the proof of theorem 3.1. The extension of this perspective to arbitrary number fields is essential to algebraic number theory. For instance, it will enable us to prove that the class number of a number field is finite.

Definition 3.5. Let V be an n-dimensional vector space over $\mathbb{R}$. We say $\Gamma \subset V$ is a *lattice* if $\Gamma = \oplus_{i=1}^{m} \mathbb{Z} v_i$ as a $\mathbb{Z}$-module, where the set $\{v_i : i = 1, \ldots, m\}$ is linearly independent over K. If $m = \dim V$, we say Γ is a *full* lattice.

Example 3.6. $\mathbb{Z}$ is a lattice in $\mathbb{R}$, and more generally, $\mathbb{Z}x = \{zx : z \in \mathbb{Z}\}$ is a lattice in $\mathbb{R}$ for any $x \in \mathbb{R}$. However, $\mathbb{Z}[\sqrt{2}] = \mathbb{Z} + \mathbb{Z}\sqrt{2}$ is *not* a lattice in $\mathbb{R}$.

Definition 3.7. The *fundamental domain/mesh* of a lattice $\Gamma = \oplus_{i=1}^{m} \mathbb{Z} v_i$ is

$$\Phi = \left\{ \sum_{i=1}^{m} x_i v_i : 0 \leq x_i < 1 \right\}.$$

The *volume* of Γ is defined as the volume of its fundamental domain.

By construction, the translates $\gamma + \Phi$ are pairwise disjoint for each $\gamma \in \Gamma$.

Remark. Let A be a matrix whose column vectors form a basis for Γ. Then, $\mathrm{vol}(\Phi) = \sqrt{\det(A^T A)}$. If Γ is a full lattice, then $\mathrm{vol}(\Phi) = \det(A)$.

Proposition 3.8. *The following are equivalent for a lattice $\Gamma \subset V$.*

1. *Γ is full.*

2. *The translates $\gamma + \Phi$ for $\gamma \in \Gamma$ cover V.*

3. *There exists a bounded subset $M \subset V$ such that the translates $M + \gamma$ for $\gamma \in \Gamma$ cover V.*

Proof. The equivalence of 1 and 2 is left as an exercise, and the implication $2 \implies 3$ is immediate. Suppose $M \subset V$ is a bounded set whose translates $\gamma + M$ cover V. Let V_0 be the subspace of V spanned by Γ. We want to show that $V_0 = V$. Let $v \in V$ be arbitrary, and for each $n \in \mathbb{N}$, $nv = a_n + \gamma_n$ for some $a_n \in M$ and $\gamma_n \in \Gamma$. Since M is bounded, $n^{-1}a_n$ converges to 0, and since V_0 is closed,

$$v = \lim_{n\to\infty} n^{-1}a_n + \lim_{n\to\infty} n^{-1}\gamma_n = \lim_{n\to\infty} n^{-1}\gamma_n \in V_0.$$

□

Lemma 3.9. *An additive subgroup Γ of V is a lattice if and only if it is discrete, i.e. every $\gamma \in \Gamma$ has a neighbourhood $U \subset V$ such that $U \cap \Gamma = \{\gamma\}$.*

Proof. First, suppose Γ is a discrete subgroup of V. We will show that Γ is closed. Let U be a neighbourhood of 0 such that $U \cap \Gamma = \{0\}$, and $U' \subset U$ another neighbourhood of 0 such that $U' - U' \subset U$. Suppose $x \notin \Gamma$ is a limit point of Γ. Then, there exist distinct elements $\gamma_1, \gamma_2 \in \Gamma \cap (x + U')$. However, $0 \neq \gamma_1 - \gamma_2 \in U' - U' \subset U$, a contradiction.

INCOMPLETE □

Theorem 3.10 (Minkowski's lattice point theorem)**.** *Let V be an n-dimensional vector space over $\mathbb{R}$, Γ a full lattice, and X a centrally symmetric, convex subset of V. If* $\mathrm{vol}(X) > 2^n\mathrm{vol}(\Gamma)$*, then X contains a nonzero lattice point of* Γ.

Proof. Suppose that the sets $\left(\frac{1}{2}X + \gamma\right)$ are pairwise disjoint. We know that the translates of the fundamental mesh Φ by Γ are disjoint and cover the space, so

$$\mathrm{vol}(\Phi) \geq \sum_\gamma \mathrm{vol}\left(\Phi \cap \left(\frac{1}{2}X + \gamma\right)\right) = \sum_\gamma \mathrm{vol}\left((\Phi - \gamma) \cap \frac{1}{2}X\right) = \mathrm{vol}\left(\bigcup_\gamma (\Phi - \gamma) \cap \frac{1}{2}X\right) = \mathrm{vol}\left(\frac{1}{2}X\right) = 2^{-n}\mathrm{vol}(X) > \mathrm{vol}(\Phi),$$

a contradiction.

There exist distinct elements $\gamma_1, \gamma_2 \in \Gamma$ so that

$$\left(\frac{1}{2}X + \gamma_1\right) \cap \left(\frac{1}{2}X + \gamma_2\right) \neq \emptyset,$$

so that

$$\frac{x_1}{2} + \gamma_1 = \frac{x_2}{2} + \gamma_2 \implies \gamma_1 - \gamma_2 = \frac{x_2 - x_1}{2} \in X,$$

where the last inclusion follows as $\frac{x_2 - x_1}{2}$ is the midpoint of x_2 and $-x_1$. □

Exercise 53. With the same notation as above, give an example of a centrally symmetric convex set X such that $\mathrm{vol}(X) = 2^n\mathrm{vol}(\Gamma)$, but X does not contain a nonzero lattice point.

Exercise 54. Show that if we assume that X is also closed, then the lattice point theorem holds even if $\mathrm{vol}(X) = 2^n\mathrm{vol}(\Gamma)$.[15]

Minkowski's lattice point theorem, though not difficult to state or prove, is the foundation for a branch of number theory called the 'geometry of numbers'. Let's look at a cute application of the lattice point theorem.

Theorem 3.11. *Every positive integer can be written as the sum of four squares.*

First, convince yourself that it suffices to show that every odd prime can be written as the sum of four squares.

Exercise 55. If $n, m \in \mathbb{N}$ can be written as the sum of four squares, so can their product nm.

[15] *Hint:* if X is closed, then $X = \bigcap_{\epsilon\to 0}(1 + \epsilon)X$.

Proof of theorem 3.11. Consider the polynomial

$$X^2 + Y^2 + 1 \equiv 0 \pmod{p}.$$

X^2 and $(-1 - Y^2)$ take $(p+1)/2$ distinct values each as they run through the integers $\{0, \ldots, p-1\}$, so for some choice of $x, y \in \{0, \ldots, p-1\}$, we must have $x^2 + y^2 + 1 \equiv 0 \pmod{p}$. Let $\Gamma \subset \mathbb{Z}^4$ be the lattice defined by

$$\Gamma = \Big\{(a, b, c, d) : c \equiv ax + by \pmod{p}, d \equiv bx - ay \pmod{p}\Big\}.$$

Then, $p\mathbb{Z}^4 \subset \Gamma \subset \mathbb{Z}^4$, and $\Gamma/p\mathbb{Z}^4$ is 2-dimensional over $\mathbb{F}_p$, so $|\mathbb{Z}^4 : \Gamma| = p^2$. It follows that $\mathrm{vol}(\Gamma) = p^2$.

Let X be the closed ball of radius r centered at the origin, for some choice of $2p > r^2 > 1.9p$. Then,

$$\mathrm{vol}(T) = \frac{\pi^2 r^4}{2} > 16p^2 = 2^4 \mathrm{vol}(\Gamma).$$

So T contains a nonzero lattice point $(a, b, c, d) \in \Gamma$, and $0 < a^2 + b^2 + c^2 + d^2 \leq r^2 < 2p$ by construction. Further,

$$\begin{aligned} a^2 + b^2 + c^2 + d^2 &\equiv a^2 + b^2 + (ax + by)^2 + (bx - ay)^2 \pmod{p} \\ &\equiv a^2(x^2 + y^2 + 1) + b^2(x^2 + y^2 + 1) \equiv 0 \pmod{p}. \end{aligned}$$

Putting this together, $a^2 + b^2 + c^2 + d^2 = p$. □

3.3 The class number

Our goal is to prove that if $K/\mathbb{Q}$ is a finite extension, then $|Cl_K|$, the *class number* of K, is finite. We will embed K in a vector space V so that the image of any ideal $I \lhd \mathcal{O}_K$ is a full lattice. (This seems sensible, as every ideal is after all a free $\mathbb{Z}$-module with the same rank as $\mathcal{O}_K$, and this is the dimension of K.)

3.3.1 Additive Minkowski theory

Our vector space of choice will be $K_{\mathbb{C}} = \prod_\sigma \mathbb{C}$, where σ varies over $\mathrm{Hom}_{\mathbb{Q}}(K, \mathbb{C})$. $K_{\mathbb{C}}$ is not only a $\mathbb{C}$-vector space, but also a $\mathbb{C}$-algebra under pointwise multiplication, and it is equipped with the standard Hermitian inner product

$$\langle x, y \rangle = \sum_\sigma x_\sigma \overline{y_\sigma}.$$

We can define an involution $F : K_{\mathbb{C}} \to K_{\mathbb{C}}$ analogous to complex conjugation by

$$F : z \to Fz; \quad (Fz)_\sigma = \overline{(z)_{\overline{\sigma}}}.$$

The fixed points of this involution play the role of the real numbers.

$$K_{\mathbb{R}} = \big\{z \in K_{\mathbb{C}} : Fz = z\big\} = \big\{z \in K_{\mathbb{C}} : (z)_{\overline{\sigma}} = \overline{(z)_\sigma}\big\}.$$

The Hermitian inner product $\langle \cdot, \cdot \rangle$ restricts to a symmetric bilinear form on $K_{\mathbb{R}}$. We have a canonical embedding $\jmath : K \to K_{\mathbb{C}}$

$$\jmath : x \to \big(\sigma x\big)_\sigma$$

Of course, for $x \in K$, $\overline{\sigma}(x) = \overline{\sigma(x)}$, so $\jmath(K) \subset K_{\mathbb{R}}$.

We say an embedding $\rho \in \mathrm{Hom}_{\mathbb{Q}}(K, \mathbb{C})$ is *real* if $\tau(K) \subset \mathbb{R}$, and *complex* otherwise. The conjugate of a complex embedding is a different complex embedding, so the complex embeddings come in pairs. Let r be the number of real embeddings, $2s$ the number of complex embeddings, and $n = r + 2s$ the dimension of $K_{\mathbb{C}}$ as a $\mathbb{C}$-vector space. Fix a representative σ from each pair of complex embeddings. For ease of notation, ρ will denote a real embedding, σ a complex embedding from our representative family, and $\overline{\sigma}$ the corresponding conjugate embedding.

A standard basis of $K_{\mathbb{R}}$ is given by $\{e_\tau : \tau \in \mathrm{Hom}_{\mathbb{Q}}(K, \mathbb{C})\}$, where

$$\begin{aligned} \left(e_\rho\right)_\rho &= 1, \quad \rho \text{ is a real embedding,} \\ \left(e_\sigma\right)_\sigma = \left(e_\sigma\right)_{\overline{\sigma}} &= 1, \\ \left(e_{\overline{\sigma}}\right)_\sigma = i, \left(e_{\overline{\sigma}}\right)_{\overline{\sigma}} &= -i, \quad \sigma \text{ is a representative complex embedding.} \end{aligned}$$

Define a linear map $f : K_{\mathbb{R}} \to \mathbb{R}^n$ by

$$\begin{aligned} \left(fz\right)_\rho &= z_\rho && \text{for } \rho \text{ real, and} \\ \left(fz\right)_\sigma = Re(z_\sigma) \text{ and } \left(fz\right)_{\overline{\sigma}} &= Im(z_\sigma) && \text{for } \sigma \text{ complex.} \end{aligned}$$

Exercise 56. Show that:

i. f maps the standard basis of $K_{\mathbb{R}}$ to the standard basis of R^n.

ii. if T is the transition matrix from the standard basis of $K_{\mathbb{R}}$ to that of $\mathbb{R}^n$, then $|\det(T)| = 2^s$.[16]

Proposition 3.12. *f is a vector space isomorphism, and f transforms the Euclidean inner product $\langle \cdot, \cdot \rangle$ into the scalar product $(\cdot, \cdot)$ by*

$$\langle x, y \rangle = (fx, fy) = \sum_{\tau \in \mathrm{Hom}_{\mathbb{Q}}(K, \mathbb{C})} \epsilon_\tau (fx)_\tau (fy)_\tau : x, y \in K_{\mathbb{R}}$$

where $\epsilon_\rho = 1$ for ρ real, and $\epsilon_\sigma = \epsilon_{\overline{\sigma}} = 2$ for σ complex.

Proof. That f is a vector space isomorphism is easily checked by taking a basis of $K_{\mathbb{R}}$. The transformation of the Euclidean inner product to what we will call the *canonical metric* is more interesting. Let $\left(x_\tau\right), \left(y_\tau\right) \in K_{\mathbb{R}}$. Consider the terms in the inner product $\langle x, y \rangle$. For a real embedding ρ, $x_\rho \overline{y_\rho} = x_\rho y_\rho = (fx)_\rho (fy)_\rho$. For a complex embedding σ, two terms appear in the inner product:

$$x_\sigma \overline{y_\sigma} + x_{\overline{\sigma}} \overline{y_{\overline{\sigma}}} = x_\sigma \overline{y_\sigma} + \overline{x_\sigma} y_\sigma = 2\mathrm{Re}(x_\sigma \overline{y_\sigma}) = 2\big((fx)_\sigma (fy)_\sigma + (fx)_{\overline{\sigma}} (fy)_{\overline{\sigma}}\big).$$

□

3.3.2 Ideal norms and the class group

Now that we know that $K_{\mathbb{R}}$ is an n-dimensional vector space over $\mathbb{R}$, we want the ideals of $\mathcal{O}_K$ to form lattices under this embedding.

Definition 3.13. The *absolute norm* of a nonzero ideal $I \lhd \mathcal{O}_K$ is $\mathrm{Nm} I = |\mathcal{O}_K : I|$.

Exercise 57. Show that if I is nonzero, then $\mathrm{Nm} I$ is finite.

Exercise 58. Show that if $0 \neq I \lhd \mathcal{O}_K$, then $\jmath(I)$ is a full lattice in $K_{\mathbb{R}}$.

The next proposition shows that the ideal norm agrees with $\mathrm{Nm}_{K/\mathbb{Q}}$ for elements of $\mathcal{O}_K$.

Proposition 3.14. *If $a \in \mathcal{O}_K$,*

$$\mathrm{Nm}\big(\langle a \rangle\big) = \left|\mathrm{Nm}_{K/\mathbb{Q}}(a)\right|.$$

Proof. Let $\{\omega_1, \ldots, \omega_n\}$ be an integral basis of $\mathcal{O}_K$, so that $\{a\omega_1, \ldots, a\omega_n\}$ is a basis of $\langle a \rangle$. The matrix T_a of multiplication by a is also the transition matrix from the basis $\{\omega_1, \ldots, \omega_n\}$ to $\{a\omega_1, \ldots, a\omega_n\}$. So,

$$\mathrm{Nm}_{K/\mathbb{Q}}(a) = \det(T_a) = |\mathcal{O}_K : \langle a \rangle|.$$

□

[16] *Hint:* what are the elementary row operations to obtain T^{-1} from the identity?

Lemma 3.15. *Let $I \lhd \mathcal{O}_K$ have prime factorisation $I = \mathfrak{p}_1^{a_1} \dots \mathfrak{p}_r^{a_r}$. Then,*

$$\mathrm{Nm}(I) = \mathrm{Nm}(\mathfrak{p}_1)^{a_1} \dots \mathrm{Nm}(\mathfrak{p}_r)^{a_r}.$$

Proof. By the Chinese Remainder theorem, we can reduce this to showing that $\mathrm{Nm}(\mathfrak{p}^a) = \mathrm{Nm}(p)^a$ for prime ideals. By unique prime factorisation, $\mathfrak{p}^i \neq \mathfrak{p}^{i+1}$. Let $b \in \mathfrak{p}^i \setminus \mathfrak{p}^{i+1}$. If $\langle \mathfrak{p}^{i+1}, b\rangle$ is a proper ideal in $\mathfrak{p}^i$, then $\mathfrak{p}^{-i}\langle \mathfrak{p}^{i+1}, b\rangle$ is a proper ideal in $\mathcal{O}_K$ containing $\mathfrak{p} = \mathfrak{p}^{i+1}\mathfrak{p}^{-i}$, a contradiction. So, $\mathfrak{p}^{i+1}/\mathfrak{p}^i$ is a 1-dimensional vector space over $\mathcal{O}_K/\mathfrak{p}$: $\mathfrak{p}^{i+1}/\mathfrak{p}^i \cong \mathcal{O}_K/\mathfrak{p}$. Finally,

$$\mathrm{Nm}(\mathfrak{p}^a) = |\mathcal{O}_K : \mathfrak{p}^a| = |\mathcal{O}_K : \mathfrak{p}| \cdot |\mathfrak{p} : \mathfrak{p}^2| \cdots |\mathfrak{p}^{a-1} : \mathfrak{p}^a| = |\mathcal{O}_K : \mathfrak{p}|^a = \mathrm{Nm}(\mathfrak{p})^a.$$

□

It follows that $\mathrm{Nm}(I)\mathrm{Nm}(J) = \mathrm{Nm}(IJ)$ for integral ideals. By defining $\mathrm{Nm}(I^{-1}) = \mathrm{Nm}(I)$ for integral ideals I, we can extend this multiplicatively to all fractional ideals.

Corollary 3.16. *There are at most finitely many integral ideals of $\mathcal{O}_K$ with a given norm.*

Proof. If $\mathfrak{p}$ is a nonzero prime ideal of $\mathcal{O}_K$, then $\mathfrak{p} \cap \mathbb{Z} = \langle p \rangle$ for some prime $p \in \mathbb{Z}$, and $|\mathcal{O}_K : \mathfrak{p}| = p^f$ for some positive integer f. If $\mathfrak{p} \cap \mathbb{Z} = \langle p \rangle$, then $\mathfrak{p}$ divides $p\mathcal{O}_K$. So there are at most finitely many ideals $\mathfrak{p}$ such that $\mathfrak{p} \cap \mathbb{Z} = \langle p \rangle$ for a given prime $p \in \mathbb{Z}$. By the multiplicativity of the ideal norm and unique factorisation in $\mathbb{Z}$, it follows that for any $M > 0$, there are at most finitely many ideals $I \lhd \mathcal{O}_K$ with $\mathrm{Nm}(I) \leq M$. □

Proposition 3.17. *If $0 \neq I \lhd \mathcal{O}_K$, then $\jmath(I)$ is a full lattice in $K_\mathbb{R}$ with volume $\sqrt{|d_K|}\mathrm{Nm}(I)$.*

Proof. Let $\{\alpha_1, \dots, \alpha_n\}$ be a $\mathbb{Z}$-basis for I in $\mathcal{O}_K$. Let $\mathrm{Hom}_\mathbb{Q}(K, \mathbb{C}) = \{\tau_1, \dots, \tau_n\}$ and $A = \left(\tau_i \alpha_j\right)$. By proposition 2.18,

$$d(I) = \det(A)^2 = |\mathcal{O}_K : I|^2 d_K = \mathrm{Nm}(I)^2 d_K.$$

So,

$$\mathrm{vol}(\Gamma) = \det\left(\langle \jmath\alpha_i, \jmath\alpha_j\rangle\right)^{1/2} = \det\left(\sum_{l=1}^n \tau_l\alpha_i \cdot \overline{\tau_l}\alpha_j\right)^{1/2} = \det\left(A\bar{A}^T\right)^{1/2} = \left|\det(A)\right| = \sqrt{|d_K|}\mathrm{Nm}(I).$$

□

Theorem 3.18. *Let $0 \neq I \lhd \mathcal{O}_K$. Choose real numbers $c_\tau > 0$ for each $\tau \in \mathrm{Hom}_\mathbb{Q}(K, \mathbb{C})$ such that $c_\tau = c_{\bar{\tau}}$, and*

$$\prod_\tau c_\tau > \left(\frac{2}{\pi}\right)^s |d_K|^{1/2}\mathrm{Nm}(I).$$

Then, there is a nonzero $a \in I$ with $|\tau(a)| < c_\tau$ for each τ.

Proof. Define the centrally symmetric and convex set

$$X = \{z \in K_\mathbb{R} : |z_\tau| < c_\tau, \forall \tau\}.$$

Then,

$$f(X) = \{x \in \mathbb{R}^n : |x_\rho| < c_\rho, x_\sigma^2 + x_{\bar{\sigma}}^2 < c_\sigma^2\}.$$

By proposition 3.12 and the exercise preceding it, if vol_n denotes the Lebesgue measure on $\mathbb{R}^n$,

$$\mathrm{vol}(X) = 2^s \mathrm{vol}_n(f(X)) = 2^s \cdot \prod_\rho 2c_\rho \prod_\sigma (\pi c_\sigma)^2 = 2^{r+s}\pi^s \prod_\tau c_\tau.$$

The hypothesis then implies that $\mathrm{vol}(X) > 2^n \mathrm{vol}(\jmath(I))$, so by Minkowski's lattice point theorem, X contains a nonzero element $\jmath(a)$ for $a \in I$. By construction, $|\tau(a)| < c_\tau$ for each τ. □

Corollary 3.19. *For any nonzero $I \lhd \mathcal{O}_K$, $\exists$ a nonzero $a \in I$ with* $\mathrm{Nm}_{K/\mathbb{Q}}(a) \leq (2/\pi)^s |d_K|^{1/2}\mathrm{Nm}(I)$.

Proof. For any $\epsilon > 0$, we can choose real numbers $c_\tau > 0$ such that $c_\tau = c_{\overline{\tau}}$ and

$$\prod_\tau c_\tau = \left(\frac{2}{\pi}\right)^s |d_K|^{1/2}\mathrm{Nm}(I) + \epsilon.$$

There exists a corresponding element $a_\epsilon \in I$ such that $|\mathrm{Nm}_{K/\mathbb{Q}}(a_\epsilon)| < (2/\pi)^s|d_K|^{1/2}\mathrm{Nm}(I) + \epsilon$. Since $|\mathrm{Nm}_{K/\mathbb{Q}}(a_\epsilon)|$ is a positive integer, there exists $a \in I$ such that $|\mathrm{Nm}_{K/\mathbb{Q}}(a)| \leq (2/\pi)^s|d_K|^{1/2}\mathrm{Nm}(I)$. □

Theorem 3.20. $|Cl_K| < \infty$.

Proof. We claim that if $M = (2/\pi)^s\sqrt{|d_K|}$, then every class in the ideal class group has a representative with norm $\leq M$. It follows from the corollary that there are finitely many classes in the class group.

Choose a representative I for some class in Cl_K. There exists $c \in \mathcal{O}_K$ such that $J = cI^{-1} \lhd \mathcal{O}_K$. By corollary 3.19, there is a nonzero element $a \in J$ such that

$$|\mathrm{Nm}_{K/\mathbb{Q}}(a)| \cdot \mathrm{Nm}(J)^{-1} = \mathrm{Nm}(aJ^{-1}) = \mathrm{Nm}(ac^{-1}I) \leq \left(\frac{2}{\pi}\right)^s |d_K|^{1/2}.$$

$ac^{-1}I$ is a fractional ideal in the same class as I with norm at most M, concluding the proof. □

The behaviour of the ideal class groups is mostly unpredictable; it is not even known if there are infinitely many number fields with class number 1. We do know that the only imaginary quadratic fields ($\mathbb{Q}[\sqrt{D}]$ with $D < 0$ and squarefree) with class number 1 occur for $D = -1, -2, -3, -7, -11, -19, -43, -67, -163$.

The role of the class number in $\mathbb{Q}[\zeta_p]$, where ζ_p is a primitive pth root of unity, is closely linked to Fermat's Last Theorem. Just as we studied $x^2 + y^2 = p$ as a factorisation in $\mathbb{Z}[i]$, we study $x^p + y^p = z^p$ as a factorisation in $\mathbb{Z}[\zeta_p]$:

$$y \cdot y \cdots y = (z - x)(z - \zeta_p x) \cdots (z - \zeta_p^{p-1}x).$$

If $\mathbb{Z}[\zeta_p]$ is a UFD, this gives two nontrivial factorisations of the same element, which is a contradiction. Unfortunately, the class number $\mathbb{Q}[\zeta_p]$ need not always be equal to 1. The least counterexample to this is $\mathbb{Q}[\zeta_{23}]$ which has class number 3.

Exercise 59.

i. Suppose the class $I \lhd \mathcal{O}_K$ in Cl_K has order m, i.e. $I^m = \langle\alpha\rangle$ for some $\alpha \in \mathcal{O}_K$. Set $\beta = \alpha^{1/m}$ and $L = K[\beta]$. Show that $I\mathcal{O}_L = \langle\beta\rangle$ in $\mathcal{O}_L$.

ii. Show that for any finite extension $K/\mathbb{Q}$, there is a finite extension L/K in which every ideal of K becomes principal.

iii. Show that the ring Ω of all algebraic integers in $\mathbb{C}$ is a *Bézout domain*: every finitely generated ideal is principal.

3.3.3 An application to the discriminant

Theorem 3.21. *If K is an extension of $\mathbb{Q}$ of degree n, then*

$$|d_K|^{1/2} \geq \frac{n^n}{n!}\left(\frac{\pi}{4}\right)^{n/2}.$$

As a consequence, if K is a nontrivial extension of $\mathbb{Q}$, then $|d_K| > 1$.

Proof. For $t > 0$, define

$$X_t = \{z \in K_\mathbb{R} : \sum_\tau |z_\tau| \leq t\}.$$

We will compute the Lebesgue volume $f(X_t)$ in $\mathbb{R}^n$, as $\mathrm{vol}(X_t) = 2^s\mathrm{vol}(f(X_t))$. Since $f(X_t)$ is symmetric about the r real axes, $\mathrm{vol}(f(X_t)) = 2^r\mathrm{vol}(Y_t)$, where

$$Y_t = \{z \in \mathbb{R}^n : \sum_\tau |z_\tau| \leq t, z_\rho \geq 0\}.$$

If $\sigma_1, \dots, \sigma_s$ are the representative complex embeddings, we change variables to polar coordinates so that $z_{\sigma_i} = \frac{r_i}{2} e^{i\theta_i}$. The Jacobian for this change is $r_i/4$. Integrating over the variables θ_i for $0 \leq \theta_i \leq 2\pi$,

$$\mathrm{vol}(X_t) = 2^{r+s}4^{-s}(2\pi)^s \int_Z r_1 \dots r_s dx_1 \dots dx_r dr_1 \dots dr_s,$$

where

$$Z = \{(x_1, \dots, x_r, r_1, \dots, r_s) \in \mathbb{R}^{r+s} : x_i, r_i \geq 0, \sum_{i=1}^r x_i + \sum_{i=1}^s r_i \leq t\}.$$

Denote the integral as $W_{r,s}(t)$. Since $W_{r,s}(t) = t^n W_{r,s}(1)$, we estimate $W_{r,s}(1)$ first. The condition $\sum_{i=1}^r x_i + \sum_{i=1}^s r_i \leq 1$ is equivalent to $\sum_{i=2}^r x_i + \sum_{i=1}^s r_i \leq 1 - x_1$. So,

$$\begin{aligned} W_{r,s}(1) &= \int_0^1 W_{r-1,s}(1-x_1)dx_1 \\ &= \int_0^1 (1-x_1)^n W_{r-1,s}(1)dx_1 \\ &= \frac{1}{n} W_{r-1,s}(1). \end{aligned}$$

By induction,

$$W_{r,s}(1) = \frac{1}{n(n-1)\cdots(n-r+1)} W_{0,s}(1)$$

and now we attack the second set of variables in the same way.

$$\begin{aligned} W_{0,s}(1) &= W_{0,s-1}(1) \int_0^1 r_1(1-r_1)^{2s-2} dr_1 \\ &= \frac{1}{(2s)!} W_{0,0}(1) = \frac{1}{(2s)!}. \end{aligned}$$

So, $W_{r,s}(t) = t^n/n!$, yielding

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

Choose $t > 0$ so that $\mathrm{vol}(X_t) > 2^n \mathrm{vol}(\jmath(\mathcal{O}_K)) = 2^n |d_K|^{1/2}$. Then, there exists $\alpha \in \mathcal{O}_K$ such that $|\tau(\alpha)| \leq t$ for all τ. Then $|\mathrm{Nm}_{K/\mathbb{Q}}(\alpha)| \leq t^n/n^n$ by the inequality between arithmetic and geometric means. Further,

$$\begin{aligned} \mathrm{vol}(X_t) = 2^r \pi^s \frac{t^n}{n!} &\geq 2^n |d_K|^{1/2} \\ t^n &\geq n! \frac{2^{2s}}{\pi^s} |d_K|^{1/2}. \end{aligned}$$

Choose t so that equality is achieved, and

$$\begin{aligned} 1 \leq |\mathrm{Nm}(a)| &\leq \frac{t^n}{n^n} = \frac{n!}{n^n} \frac{4^s}{\pi^2} |d_K|^{1/2} \\ \implies |d_K|^{1/2} &\geq \frac{n^n}{n!} \left(\frac{\pi}{4}\right)^s \geq \frac{n^n}{n!} \left(\frac{\pi}{4}\right)^{n/2}. \end{aligned}$$

If K is a nontrivial extension of $\mathbb{Q}$, then $n \geq 2$, so $|d_K| > 1$. □

3.4 Dirichlet's Unit theorem

Given a number field K, we want to determine the structure of $U_K = \mathcal{O}_K^\times$, referred to as *the group of units* of K. Recall that $U_K = \{a \in \mathcal{O}_K : \mathrm{Nm}_{K/\mathbb{Q}}(a) = \pm 1\}$. It is clear that U_K contains the finite group $\mu(K)$ of the roots of unity in K. In general though, U_K is not finite.

Recall we had r real embeddings of K into $\mathbb{C}$ and s pairs $(\sigma, \overline{\sigma})$ of complex embeddings. We want to first show that U_K is a finitely generated abelian group, and use the fundamental theorem of finitely generated abelian groups to prove

Theorem 3.22 (Dirichlet's unit theorem)**.**

$$U_K \cong \mu(K) \oplus \mathbb{Z}^{r+s-1}.$$

3.4.1 Multiplicative Minkowski theory

Under the map $\jmath : K \to K_{\mathbb{C}}$, $K^\times$ is embedded in $K_{\mathbb{C}}^\times$, where

$$K_{\mathbb{C}}^\times = \Big\{ \big(z_\tau\big) : z_\tau \neq 0, \forall \tau \Big\}.$$

It is clear that $K_{\mathbb{C}}^\times$ is a group under coordinate-wise multiplication, and the restriction $\jmath : K^\times \to K_{\mathbb{C}}^\times$ is a homomorphism of multiplicative groups. Define a homomorphism $\mathrm{Nm} : K_{\mathbb{C}}^\times \to \mathbb{C}^\times$ by

$$\mathrm{Nm}\big(z_\tau\big) = \prod_\tau z_\tau.$$

The composition $\mathrm{Nm} \circ \jmath$ on $K^\times$ is just $\mathrm{Nm}_{K/\mathbb{Q}}$.

We pass from multiplicative groups to additive groups with a logarithm. Define a homomorphism $\mathbb{C}^\times \to \mathbb{R}$ by

$$z \to \log |z|,$$

inducing a surjective homomorphism

$$\ell : K_{\mathbb{C}}^\times \to \prod_\tau \mathbb{R}$$

Its restriction to $K_{\mathbb{R}}^\times$ yields

$$\ell(K_{\mathbb{R}}^\times) = \Big\{ z \in \prod_\tau \mathbb{R} : z_\tau = z_{\overline{\tau}}, \forall \tau \Big\}.$$

$\ell(K_{\mathbb{R}}^\times)$ to $\mathbb{R}^{r+s}$ as an $\mathbb{R}$-vector space. Define a 'trace' map, $\mathrm{Tr} : \ell(K_{\mathbb{R}}^\times) \to \mathbb{R}$, as the sum of the coordinates. This is all a convoluted way of setting up the following commutative diagram.

$$\begin{tikzcd}
K^\times \arrow[r, "\jmath"] \arrow[d, "\mathrm{Nm}_{K/\mathbb{Q}}"'] & K_{\mathbb{R}}^\times \arrow[r, "\ell"] \arrow[d, "\mathrm{Nm}"'] & \ell(K_{\mathbb{R}}^\times) \arrow[d, "\mathrm{Tr}"] \\
\mathbb{Q}^\times \arrow[r] & \mathbb{R}^\times \arrow[r, "\log|\cdot|"] & \mathbb{R}
\end{tikzcd}$$

3.4.2 The group of units

What happens to U_K in this commutative diagram? Looking at the "kernels" of the vertical arrows, we have

$$\begin{aligned}
U_K &= \{a \in \mathcal{O}_K : \mathrm{Nm}_{K/\mathbb{Q}}(a) = \pm 1\}, \\
S &= \{z \in K_{\mathbb{R}}^\times : \mathrm{Nm} z = \pm 1\}, \\
H &= \{x \in \ell(K_{\mathbb{R}}^\times) : \mathrm{Tr} x = 0\}.
\end{aligned}$$

We have the homomorphisms

$$U_K \xrightarrow{\jmath} S \xrightarrow{l} H$$

and the composition $\lambda : U_K \to H$. Let $\Gamma = \lambda(U_K) \subset \ell(K_{\mathbb{R}}^\times)$.

Proposition 3.23. *The sequence*

$$1 \to \mu(K) \to U_K \xrightarrow{\lambda} \Gamma \to 0$$

is exact.

Proof. The only thing we need to show is that $\ker(\lambda) = \mu(K)$. If $\zeta \in \mu(K)$ and $\tau \in \mathrm{Hom}_{\mathbb{Q}}(K, \mathbb{C})$, then $\log |\tau\zeta| = \log 1 = 0$. So $\lambda(\mu(K)) = 0$.

Conversely, suppose $u \in U_K$ and $\lambda(u) = 0$. Equivalently, $|\tau(u)| = 1$ for all $\tau \in \mathrm{Hom}_{\mathbb{Q}}(K, \mathbb{C})$. By an earlier exercise, since u is an algebraic integer all of whose Galois conjugates have absolute value 1, u is a root of unity. □

Vigyázz!. We have shown that ${}^{U_K}\!/_{\mu(K)} \cong \Gamma$. This does not yet imply that $U_K \cong \mu(K) \times \Gamma$.

Lemma 3.24. *Up to multiplication by units, there are only finitely many $\alpha \in \mathcal{O}_K$ of a given norm* $\mathrm{Nm}_{K/\mathbb{Q}}(\alpha) = a$.

Proof. $\mathrm{Nm}_{K/\mathbb{Q}}(\alpha) = \mathrm{Nm}\langle\alpha\rangle$, and there are only finitely many ideals of a given norm. □

Theorem 3.25. *H is an $(r+s-1)$-dimensional real vector space, and Γ is a complete lattice in it. As a consequence,* $\Gamma \cong \mathbb{Z}^{r+s-1}$.

Proof. H is the trace-zero hyperplane in $\ell(K_{\mathbb{R}}^{\times})$, which is an $(r+s)$-dimensional real vector space, so the first part of the theorem is true.

We will first show that Γ is a discrete subgroup of H. $\lambda : U_K \longrightarrow H$ is the restriction of the mapping $K^{\times} \xrightarrow{j} K_{\mathbb{C}}^{\times} \xrightarrow{\ell} \prod_{\tau} \mathbb{R}$. It suffices to show that for any $c > 0$, the ball

$$B_c = \left\{x \in \prod_{\tau} \mathbb{R} : |x_\tau| < c, \forall \tau\right\}$$

contains at most finitely many points of Γ. The preimage of this under ℓ is

$$\ell^{-1}(B_c) = \left\{z \in K_{\mathbb{C}}^{\times} : e^{-t} < |z_\tau| < e^{t}, \forall\tau\right\}.$$

Since $j\mathcal{O}_K$ is a lattice in $K_{\mathbb{R}}$, $\ell^{-1}(B_c)$ contains at most finitely many points of $j(U_K)$, thus B_c contains at most finitely many points of Γ.

The crux of the proof is to show that Γ is a *full* lattice in H, which we will do by constructing a bounded set $M \subset H$ such that the translates $M + \gamma$ cover H (see proposition 3.8). We will do this by constructing a bounded set $T \subset S$ so that the *multiplicative* translates $j(u)T$ for $u \in U_K$ cover S. If $x = (x_\tau) \in T$, since the absolute values $|x_\tau|$ are bounded above, they must be bounded below away from 0. So the image $M = \ell(T)$ is the set we want.

Choose real numbers $c_\tau > 0$ with $c_\tau = c_{\overline{\tau}}$ so that

$$C = \prod_{\tau} c_\tau > \left(\frac{2}{\pi}\right)^{s} \sqrt{|d_K|},$$

and define

$$X = \left\{z \in K_{\mathbb{R}} : |z_\tau| < c_\tau, \forall\tau\right\}.$$

For any $y \in S$, the multiplicative translate is

$$Xy = \left\{z \in K_{\mathbb{R}} : |z_\tau| < c'_\tau, \forall\tau\right\},$$

where $c'_\tau = c_\tau |y_\tau|$, and $\prod c'_\tau = \prod c_\tau \prod |y_\tau| = C$. So, there exists a nonzero $a \in \mathcal{O}_K$ such that $j(a) \in Xy$. Since $0 < |\mathrm{Nm}_{K/\mathbb{Q}}(a)| \leq C$, we can choose a finite set of representatives $\{a_1, \ldots, a_N\}$ so that each element of $\{a \in \mathcal{O}_K : j(a) \in Xy, y \in S\}$ is associate to one of the a_i (by lemma 3.24). Finally, set

$$T = S \cap \bigcup_{i=1}^{N} (j a_i)^{-1} X.$$

Since X is bounded, so is T, and it remains to show that

$$S = \bigcup_{u \in U_K} j(u)T.$$

If $y \in S$, then there exists $u \in U_K$ and a_i so that $j(ua_i) \in Xy^{-1}$. Equivalently,for some $x \in X$,

$$\begin{aligned} &j(ua_i) = xy^{-1} \\ \implies\ & y = xj(u^{-1})j(a_i^{-1}) \in j(u^{-1})T. \end{aligned}$$

□

Finally,

Proof of theorem 3.22. What remains is an elementary exercise in group theory: to show that ${}^{U_K}\!\big/_{\mu(K)} \cong \mathbb{Z}^{r+s-1} \implies U_K \cong \mu(K) \times \mathbb{Z}^{r+s-1}$. Let $m = r+s-1$, write $\mathbb{Z}^m$ multiplicatively, and let $\{\beta_1, \ldots, \beta_m\} \subset U_K$ be a set of free generators of ${}^{U_K}\!\big/_{\mu(K)}$. Let $B \leq U_K$ be the group generated by $\{\beta_1, \ldots, \beta_m\}$. Since $\mu(K)B = U_K$, we only need to show that $\mu(K) \cap B = \{1\}$. Suppose $\beta_1^{a_1} \cdots \beta_m^{a_m} \in \mu(K)$. Then, $\beta_1^{a_1} \cdots \beta_m^{a_m} \mu(K) = \mu(K)$ in the quotient group ${}^{U_K}\!\big/_{\mu(K)}$. Since the quotient group is a free group, this is only possible when $a_1 = \cdots a_m = 0$. This shows that $B = \mathbb{Z}^m = \mathbb{Z}^{r+s-1}$ so $U_K = \mu(K) \times B = \mu(K) \times \mathbb{Z}^{r+s-1}$. □

We will call generators of $\mathbb{Z}^{r+s-1}$ in U_K *fundamental units* of K.

Example 3.26. Let $D > 1$ be a squarefree integer and $K = \mathbb{Q}[\sqrt{D}]$. Then $\mathrm{Hom}_{\mathbb{Q}}(K, \mathbb{C}) = \mathrm{Hom}_{\mathbb{Q}}(K, \mathbb{R})$, $r = 2$ and $s = 0$. By the unit theorem, $U_K = \mu(K) \times \mathbb{Z}$. Since $D > 1$, $\mu(K) = \{\pm 1\} \cong \mathbb{Z}_2$. Which unit generates an infinite cyclic group?

Let $d = d_K$. Let $a, b > 0$ be the unique minimal integer solution of $X^2 - dY^2 = -4$—or if this has no solution, of $X^2 - dY^2 = 4$. Then,

$$\epsilon = \frac{a + b\sqrt{d}}{2}$$

is the fundamental unit of K. Check that it actually generates an infinite cyclic group.

Exercise 60. Let $D < -1$ be a squarefree integer. What are the units in $\mathbb{Q}[\sqrt{D}]$?

4 Closing remarks

Minkowski theory sets up the language we need to study number fields. There are (at least) two types of questions we can ask about them. The first, perhaps most natural one, is: can we classify/characterise all "nice" number fields? The second: what do we learn about the structure of the field itself?

The first fundamental theorem of algebraic number theory, the Kronecker–Weber theorem, answers a question of the first type. It is not too complicated to prove that any finite *cyclotomic* extension of $\mathbb{Q}$ (obtained by adjoining a root of unity), has abelian Galois group. The Kronecker–Weber theorem is a sort of converse: every finite extension of $\mathbb{Q}$ with abelian Galois group is contained in a cyclotomic extension.

To answer the second question, it turns out that the prime ideals of a number field play an integral role. This will be evident in the proof of the Kronecker–Weber theorem, as the *global* case follows from the *local* case for finite extensions of p-adic numbers.

While the Kronecker–Weber theorem characterises the maximal abelian extension in terms of its subextensions, class field theory characterises this extension in terms of the structure of the base field. It is a surprising result that if K^{ab} is the maximal abelian extension of a *nonarchimedean local field*, then $\mathrm{Gal}(K^{\mathrm{ab}}/K)$ is isomorphic to $K^\times$, and this isomorphism can be constructed. It is perhaps even more surprising that this statement has a cohomological formulation. Perhaps someday I will update these notes to include a complete presentation of Kronecker–Weber.

References

[1] Keith Conrad. *Finite Fields*. https://kconrad.math.uconn.edu/blurbs/galoistheory/finitefields.pdf

[2] Milne. *Algebraic Number Theory*.

[3] Milne. *Class Field Theory*.

[4] Neukirch. *Algebraic Number Theory*.