PartII Number Fields

zc231

Contents

1 Algebraic number fields

1.1 Algebraic numbers

Definition 1.1. *An algebraic number α is a root of polynomial $P(x)$ with rational coefficients. Equivalently, $\mathbb{Q}(\alpha)$ is finite over $\mathbb{Q}$.*

Lemma 1.2. *Let α be an algebraic number. Then there exists a unique polynomial $P(x) \in \mathbb{Q}[x]$ such that (i) $P(x)$ is irreducible (ii) $P(x)$ is monic (i.e. the leading coefficient is 1) (iii) $P(\alpha) = 0$. Such $P(x)$ is called the minimal polynomial of α. The degree of α is defined as the degree of the minimal polynomial of α. Moreover, if $Q(x) \in \mathbb{Q}[x]$ is another polynomial such that $Q(\alpha) = 0$ then $P|Q$.*

Proof. By assumption there exists $Q(x) \in \mathbb{Q}[x]$ such that $Q(\alpha) = 0$. Let $P(x)$ a the monic polynomial and $P(\alpha) = 0$ with minimal degree. Then $P(x)$ is irreducible otherwise we have a polynomial which has α as a root of smaller degree.

If $R(x)$ is also a polynomial with the same property, then by assumption $\deg R \geq \deg P$. We apply division algorithm so that

$$R(x) = P(x)q(x) + r(x), \quad r(x) = 0 \text{ or } \deg r < \deg R.$$

But $0 = R(\alpha) = P(\alpha)q(\alpha) + r(\alpha)$ and so $r(\alpha) = 0$. By assumption $r(x) = 0$ and so $P(x)|R(x)$. Since $\deg R = \deg P$ and P, R are both monic we conclude that $P = R$. □

Definition 1.3. *Let α be an algebraic number with minimal polynomial P. The conjugates of α are defined as roots of P.*

Remark 1.4. *P is also the minimal polynomial of every conjugate of α because P is irreducible and monic.*

Since $\mathbb{Q}$ is a field of characteristic zero, P is separable and so conjugates of α are distinct.

Lemma 1.5. *The set of algebraic numbers form a field.*

Proof. If α has minimal polynomial

$$x^n + a_{n-1}x^{n-1} + \cdots + a_0, a_i \in \mathbb{Q}$$

then $a_0 \neq 0$ because the polynomial is irreducible and so

$$x^n + \frac{a_1}{a_0}x^{n-1} + \cdots + \frac{a_{n-1}}{a_0}x + \frac{1}{a_0}$$

is the minimal polynomial for α^{-1}.

Suppose α, β are algebraic numbers, so are $\alpha + \beta, \alpha\beta$ because

$$\mathbb{Q}(\alpha + \beta), \mathbb{Q}(\alpha\beta) \subset \mathbb{Q}(\alpha, \beta)$$

is finite over $\mathbb{Q}$. □

1.2 Algebraic number fields

Definition 1.6. *An algebraic number field is a field is a field K that is a finite extension of $\mathbb{Q}$. Equivalently, $K = \mathbb{Q}(\alpha)$ for some algebraic number α by primitive element theorem.*

Definition 1.7. *Let $K = \mathbb{Q}(\alpha)$ be an algebraic number field. Let $\alpha = \alpha_1, \alpha_2, \ldots, \alpha_n$ be the conjugates of α. The conjugate fields $K_1, \ldots, K_n$ are defined as the embeddings of K into $\mathbb{C}$ given by field homomorphism induced by $\sigma_j(\alpha) = \alpha_j$, i.e. $K_j = \mathbb{Q}(\alpha_j)$.*

Remark 1.8. *The conjugate fields are not necessarily distinct. For example, if $K/\mathbb{Q}$ is Galois the $K_j = K$ for each K.*

Definition 1.9. *Let $K = \mathbb{Q}(\alpha)$ be an algebraic number field and $\beta \in K$. The field polynomial of β is defined as*

$$f(x) = \prod_j (x - \sigma_j(\beta)).$$

Lemma 1.10. *If g is the minimal polynomial of β, and f is the field polynomial of β, then*

$$f(x) = (g(x))^m$$

for some $m \geq 1$.

Proof. Since $f(\beta) = 0$, so $g|f$ and let m be the largest integer such that $g^m|f$. Then $f(x) = (g(x))^m h(x)$ for some $h(x) \neq 0$. Suppose h is not constant, then h has at least one root. Each root of h is a root of f so we conclude that $h(\sigma_j(\beta)) = 0$ for some j. But σ_j is a homomorphism so

$$\sigma_j(h(\beta)) = h(\sigma_j(\beta)) = 0$$

and so $h(\beta) = 0$. This implies $g|h$ which contradicts the maximality of m. Therefore h is constant and so $h = 1$ because f, g are both monic. □

Definition 1.11. *Let $K = \mathbb{Q}(\alpha_1)$ be a number field and $K_j = \mathbb{Q}(\alpha_j), j = 1, \ldots, n$ be the conjugate fields. Then we have field isomorphisms*

$$\sigma_j : \mathbb{Q}[x]/\langle P(x)\rangle \cong K_j \subset \mathbb{C}$$

where $P(x)$ is the minimal polynomial of α. σ_j is called a real embedding if $K_j \subset \mathbb{R}$ and is called a complex embedding if $K_j \not\subset \mathbb{R}$. Since complex roots of $P(x)$ appear in pairs, so the number of complex embeddings is even.

We check that the above is well-defined in the following sense

Theorem 1.12. *Let $\mathbb{Q}(\alpha_1) = \mathbb{Q}(\beta_1)$ and $\beta_j, j = 1, 2, \ldots, n$ are the conjugates of β_1. Let $L_j = \mathbb{Q}(\beta_j)$ and*

$$\tau_j : \mathbb{Q}[x]/\langle Q(x)\rangle \cong L_j \subset \mathbb{C}$$

where $Q(x)$ is the minimal polynomial of β_1. If r', s' are the number of real and complex embeddings respectively for β_1, then $r' = r$ and $s' = s$. In other word, the number of real and complex embeddings is independent of the generator of the number field.

Proof. Since P and Q have the same degree so

$$r' + 2s' = r + 2s = n.$$

As $\mathbb{Q}(\alpha_1) = \mathbb{Q}(\beta_1)$, we have a field isomorphism

$$\phi : \mathbb{Q}[x]/\langle P(x)\rangle \cong \mathbb{Q}[x]/\langle Q(x)\rangle.$$

Since $\phi(\lambda) = \lambda$ for each $\lambda \in \mathbb{Q}$ and each real number is a limit of a sequence of rational numbers, we conclude that ϕ extends to an isomorphism

$$\phi : \mathbb{R}[x]/\langle P(x)\rangle \cong \mathbb{R}[x]/\langle Q(x)\rangle.$$

Each irreducible polynomial in $\mathbb{R}[x]$ has degree 1 or 2 because $\mathbb{C} = \mathbb{R}[i]$. Therefore, writing

$$P(x) = \prod_{i=1}^{m} P_i(x), \quad Q(x) = \prod_{j=1}^{k} Q_j(x)$$

where P_i, Q_j have degree 1 or 2 and using Chinese remainder theorem we have

$$\mathbb{R}[x]/\langle P_1\rangle \times \cdots \mathbb{R}[x]/\langle P_m\rangle \cong \mathbb{R}[x]/\langle Q_1\rangle \times \cdots \mathbb{R}[x]/\langle Q_k\rangle.$$

For each i, $\mathbb{R}[x]/\langle P_i\rangle \cong \mathbb{R}$ if P_i has degree 1 and $\mathbb{R}[x]/\langle P_i\rangle \cong \mathbb{C}$ if P_i has degree 2. The number of solutions for $x(x^2+1)=0$ in $\mathbb{R}[x]/\langle P_i\rangle$ is 1 if P_i has degree 1 and 3 if P_i has degree 2. Therefore, the number of solutions for $x(x^2+1)=0$ in the ring

$$\mathbb{R}[x]/\langle P_1\rangle \times \cdots \mathbb{R}[x]/\langle P_m\rangle$$

is $1^r 3^s = 3^s$. Similarly the number of solutions for $x(x^2+1)=0$ in the ring

$$\mathbb{R}[x]/\langle Q_1\rangle \times \cdots \mathbb{R}[x]/\langle Q_k\rangle$$

is $1^{r'} 3^{s'} = 3^{s'}$. Therefore $s = s'$ and so $r = r'$. □

Remark 1.13. *The above proof also shows that the embeddings σ_j are independent of the generator.*

1.3 Norm and Trace

Definition 1.14. *Let L/K be a finite field extension. Define for any $x \in L$ the K-linear map*

$$\phi_x : L \to L, \quad \phi_x(y) = xy.$$

Then
(i) The trace of x, written $T_{L/K}(x)$ is defined as the trace of ϕ_x.
(ii) The norm of x, written $N_{L/K}(x)$ is defined as the norm (determinant) of ϕ_x.

We establish some general field theory (which you probably have met in Galois Theory) and then obtain some useful and simpler expression for trace and norm.

Theorem 1.15 (**Dedekind**). *Let F, E be fields and $\sigma_1, \dots, \sigma_n$ be n distinct field homomorphisms from F to E. Then they are linearly independent over E in the E-vector space of all additive group homomorphisms from F to E. In other words, if $c_1, \dots, c_n \in E$ and $\sum_{i=1}^n c_i\sigma_i(x) = 0$ for all $x \in F$, then $c_i = 0$ for all i.*

Proof. Suppose not and let k be the minimal integer for which $\{\sigma_1, \dots, \sigma_k\}$ is linearly dependent. So there exist $c_j \in E$, such that $\sum_{j=1}^k c_j\sigma_j(x) = 0$ for all $x \in F$ and $c_k \neq 0$. Since $\sigma_k \neq 0$, there is some $t \leq k$ such that $c_t \neq 0$ and so we can choose $x \in F$ such that $\sigma_t(x) \neq \sigma_k(x)$. For all $y \in F$, we have

$$\sum_{j=1}^k c_j\sigma_j(x)\sigma_j(y) = \sum_{j=1}^k c_j\sigma_j(xy) = 0$$

and hence

$$\sum_{j=1}^k c_j\sigma_j(x)\sigma_j = 0$$

Therefore,

$$\sum_{j=1}^{k-1} c_j(\sigma_j(x) - \sigma_k(x))\sigma_j = \sum_{j=1}^{k} c_j(\sigma_j(x) - \sigma_k(x))\sigma_j = \sum_{j=1}^{k} c_j\sigma_j(x)\sigma_j - \sigma_k(x)\sum_{j=1}^{k} c_j\sigma_j = 0$$

As $\sigma_t(x) \neq \sigma_k(x)$, and $c_t \neq 0$, we conclude that $\{\sigma_1, \dots, \sigma_{k-1}\}$ is linearly dependent, which is a contradiction. □

Lemma 1.16. *Let F/K be a finite separable extension with $[F:K]=n$, and $\{\sigma_1,\dots,\sigma_n\}$ be the set of K-homomorphisms from F to E for an extension E/K. Then a subset $X=\{x_1,\dots,x_n\}\subset F$ is a K-basis of F if and only A is an invertible matrix where $A_{ij}=\sigma_i(x_j)$.*

Proof. If X is a basis. Let $X^*=\{x_1^*,\dots,x_1^*\}$ be the dual basis. Then X^* forms an E-basis for the set of K-linear maps from F to E. By Dedekind's theorem, the set $\{\sigma_1,\dots,\sigma_n\}$ also gives an E-basis for the set of K-linear maps from F to E. Since

$$\sigma_i=\sum_{j=1}^{n}\sigma_i(x_j)x_j^*$$

and so the matrix A must be invertible.

Conversely, suppose A is invertible. If $\sum_{j=1}^{n}c_jx_j=0$ for some $c_j\in K$, then

$$\sum_{j=1}^{n}c_j\sigma_i(x_j)=0$$

for all i. Therefore $c_j=0$ for all j. □

Theorem 1.17. *Let F/K be a finite separable extension and $[F:K]=n$. Then*

$$N_{F/K}(x)=\prod_{j=1}^{n}\sigma_j(x),\quad T_{F/K}(x)=\sum_{j=1}^{n}\sigma_j(x)$$

where $\{\sigma_1,\dots,\sigma_n\}$ is the set of K-homomorphism from F to E for some extension E/K.

Proof. The trace and norm is independent of the choice of the basis so we fix a K-basis $X=\{x_1,\dots,x_n\}$ for F. Let $X^*=\{x_1^*,\dots,x_n^*\}$ be the dual basis. If ϕ_x^* is the dual linear map to ϕ_x then it is a fact in linear algebra that ϕ_x^* has the same trace and determinant as ϕ_x. So we compute the trace and determinant of ϕ_x^*. We have

$$\phi_x^*(\sigma_j)(x_i)=\sigma_j\phi_x(x_i)=\sigma_j(xx_i)=\sigma_j(x)\sigma_j(x_i)$$

for all i,j and so

$$\phi_x^*(\sigma_j)=\sigma_j(x)\sigma_j$$

for all j. Therefore, with respect to the basis $\{\sigma_1,\dots,\sigma_n\}$, the linear map ϕ_x^* is diagonal with entries $\sigma_j(x)$. Hence the result follows. □

Corollary 1.18. *Let K be an algebraic number field with embeddings $\sigma_1,\dots,\sigma_n$ and $\alpha\in K$, then*

$$T_{K/\mathbb{Q}}(\alpha)=\sum_{j=1}^{n}\sigma_j(\alpha),\quad N_{K/\mathbb{Q}}(\alpha)=\prod_{j=1}^{n}\sigma_j(\alpha).$$

In particular, if $\alpha_1,\dots,\alpha_k$ are the conjugates of α, and

$$N\alpha=\prod_{i=1}^{k}\alpha_i,\quad T\alpha=\sum_{i=1}^{k}\alpha_i$$

then

$$T_{K/\mathbb{Q}}(\alpha)=mT\alpha,\quad N_{K/\mathbb{Q}}(\alpha)=(N\alpha)^m$$

for some $m\geq 1$.

Proof. Take $E = \mathbb{C}$ in the above theorem gives the first statement. The second statement follows from Lemma 1.10. □

Corollary 1.19. *Let $L/F/K$ be a tower of number fields and $x \in L$. Then*

$$N_{F/K}(N_{L/F}(x)) = N_{L/K}(x).$$

Proof. Let $L = F(\alpha)$ and $F = K(\beta)$. Let $\alpha_1, \dots, \alpha_n$ be the conjugates of α over F, i.e. if $P(x)$ is the minimal polynomial of α over F, then these are the roots of $P(x)$. Let

$$\tau_j : L \mapsto F(\alpha_j) \subset \mathbb{C}$$

be the F-algebra isomorphisms from L to $F(\alpha_j)$. Let σ_i be the embeddings from F to $K(\beta_i)$. By tower law, $\tau_j\sigma_i$ are the K-embeddings from L to its conjugate fields over K. Therefore,

$$N_{L/K}(x) = \prod_{i,j} \tau_j\sigma_i(x) = \prod_i \sigma_i \prod_j \tau_j(x) = N_{F/K}(N_{L/F}(x)).$$

□

1.4 Algebraic integers

Definition 1.20. *Let K be an algebraic number field. A element $\alpha \in K$ is called an algebraic integer if α is a root of $P(x)$ with integer coefficients where $P(x)$ is monic. It is clear that each algebraic integer is an algebraic number.*

More generally, if $A \subset B$ is a tower of rings, then $\alpha \in B$ is called integral over A if α is a root of $P(x)$ with coefficients in A where $P(x)$ is monic and irreducible. We say B is integral over A if α is integral over A for all $\alpha \in B$.

Lemma 1.21. *Let α be an algebraic number with minimal polynomial $P(x)$. Then α is an algebraic integer if and only if $P(x) \in \mathbb{Z}[x]$.*

Proof. If $P(x) \in \mathbb{Z}[x]$ then α is an algebraic integer by definition. Conversely, if α is an algebraic integer then there exists a monic polynomial $Q(x) \in \mathbb{Z}[x]$ such that $Q(\alpha) = 0$. Take $Q(x)$ with minimal degree. By Lemma 1.2, $P|Q$ in $\mathbb{Q}[x]$ and if $\deg P < \deg Q$ then $Q(x)$ is reducible. By Gauss's lemma, $Q(x)$ is reducible in $\mathbb{Z}[x]$, which contradicts the minimality of the degree of Q. So $\deg P = \deg Q$ and so $P = Q$ because P and Q are both monic. □

1.5 Ring of integers

We aim to show that the set of algebraic integers in an algebraic number field K is a ring.

Theorem 1.22 (Cayley-Hamilton theorem). *Let A be a ring and I be an ideal of A. Let M be an A-module generated by $m_1, \dots, m_n$ and $\phi : M \longmapsto M$ is an A-endomorphism such that $\phi(M) \subseteq IM$. Then ϕ satisfies an equation*

$$\phi^n + a_{n-1}\phi^{n-1} + \ldots + a_0 = 0$$

for some $a_i \in I$.

Proof. Let $\phi(m_i) = \sum_{j=1}^n a_{ij}m_j$ for some $a_{ij} \in I$ because $\phi(M) \subseteq IM$. So

$$\sum_{j=1}^{n} (\delta_{ij}\phi - a_{ij})m_j = 0 \text{ for all } i$$

Let $\mathrm{End}_A(M)$ be the set of A-endomorphism from M to M, then $A[\phi] \subseteq \mathrm{End}_A(M)$. Since $\mathrm{End}_A(M)$ is a commutative ring, so M is an $A[\phi]$-module. Thus we can write the above equation as

$$P \begin{pmatrix} m_1 \\ \vdots \\ m_n \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix}$$

Where $P_{ij} = \delta_{ij}\phi - a_{ij}$ which is an $n \times n$ matrix. Let P^{adj} be the adjoint matrix of P and so

$$P^{adj}P = (\det P)I_n$$

Therefore, we have

$$(\det P)I_n \begin{pmatrix} m_1 \\ \vdots \\ m_n \end{pmatrix} = P^{adj}P \begin{pmatrix} m_1 \\ \vdots \\ m_n \end{pmatrix} = P^{adj} \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix}$$

This implies $\det P = 0$, because $m_i \neq 0$. But

$$0 = \det P = \phi^n + a_{n-1}\phi^{n-1} + \ldots + a_0$$

for some a_i with each a_i a polynomial in a_{ij} and since $a_{ij} \in I$ for all i, j, so $a_i \in I$ for all i. □

Corollary 1.23. **[Nakayama's Lemma]** *Let A be a ring, I be an ideal of A and M be an A-module generated by $m_1, \ldots, m_n$. If $IM = M$, then there exists $x \in A$ such that $x \equiv 1$ (mod) I and $xM = 0$.*

Proof. Take ϕ to be the identity map and so every condition in the theorem 12.6 is satisfied. Then we have some $a_i \in I$ such that

$$\phi^n + a_{n-1}\phi^{n-1} + \ldots + a_0 = 0$$

Take $x = 1 + a_{n-1} + \ldots + a_0$. So $x \equiv 1$ (mod) I, and for each $m \in M$, we have

$$xm = (1 + a_{n-1} + \ldots + a_0)m = (\phi^n + a_{n-1}\phi^{n-1} + \ldots + a_0)m = 0.$$

□

Definition 1.24. *An A-module M is called faithful if for all $a \in A$ with $a \neq 0$, there exists $m \in M$ such that $am \neq 0$. Equivalently, for all $a \neq b \in A$, there exists $m \in M$ such that $am \neq bm$.*

Lemma 1.25. *Let A, B be two rings such that $A \subseteq B$. Let $x \in B$. Then the following are equivalent:*

(i) x is integral over A.

(ii) $A[x]$ is a finitely generated A-module.

(iii) $A[x]$ is contained in a subring C of B such that C is finitely generated A-module.

(iv) There exists a faithful $A[x]$-module M that is finitely generated as an A-module.

Proof. (i) ⇒ (ii): As x is integral over A, then there exists $a_i \in A$ such that

$$x^n + a_{n-1}x^{n-1} + \ldots + a_0 = 0$$

So $A[x]$ is finitely generated by $\{1, x, x^2, \ldots, x^{n-1}\}$ as an A-module.

(ii) ⇒ (iii): Take $C = A[x]$.

(iii) ⇒ (iv): Take $M = C$ and clearly the subring C is faithful.

(iv) ⇒ (i): Define the map

$$\phi : M \longmapsto M, \quad \phi(m) = xm.$$

Let $I = A$. Then $\phi(M) \subset IM$ because M is a finitely generated A-module. So by Cayley-Hamilton Theorem, there exist $a_i \in I = A$ such that

$$\phi^n + a_{n-1}\phi^{n-1} + \ldots + a_0 = 0$$

So for each $m \in M$, we have

$$(\phi^n + a_{n-1}\phi^{n-1} + \ldots + a_0)m = (x^n + a_{n-1}x^{n-1} + \ldots + a_0)m = 0$$

Suppose $x^n + a_{n-1}x^{n-1} + \ldots + a_0 \neq 0$. As M is a faithful $A[x]$-module, so there exists $m \in M$ such that

$$(x^n + a_{n-1}x^{n-1} + \ldots + a_0)m \neq 0.$$

which gives a contradiction. Therefore $x^n + a_{n-1}x^{n-1} + \ldots + a_0 = 0$ and so x is an algebraic integer over A. □

Corollary 1.26. *Let $x_1, \ldots, x_n \in B$ which are algebraic integers over A. Then $A[x_1, \ldots, x_n]$ is a finitely generated A-module.*

Proof. Use induction on n. When $n = 1$, use (i) ⇒ (ii) in the previous lemma. Suppose this is true for $n - 1$. Write $A[x_1, \ldots, x_n] = A[x_1, \ldots, x_{n-1}][x_n]$, and use the case $n = 1$, we conclude that $A[x_1, \ldots, x_n]$ is a finitely generated $A[x_1, \ldots, x_n]$-module. By inductive hypothesis, $A[x_1, \ldots, x_{n-1}]$ is a finitely generated A-module, and so $A[x_1, \ldots, x_n]$ is a finitely generated A-module by tower law. □

Corollary 1.27. *$O = \{x \in B : x$ is integral over $A\}$ is a subring of B. In particular, taking $A = \mathbb{Q}$ and $B = K$ an algebraic number field, we conclude the set of algebraic integers in K is a ring.*

Proof. For all $y, z \in O$, $C = A[y, z]$ is a finitely generated A-module by the previous corollary. Since $A[y + z], A[yz] \subseteq A[y, z]$, by (iii) ⇒ (i) in Lemma 1.25, we conclude that $y + z, yz$ are integral over A. Therefore, $y + z, yz \in O$. □

Definition 1.28. *Let K be an algebraic number field. The ring of integers of K, denoted by $\mathcal{O}_K$, is the set of algebraic integers in K. We have shown that $\mathcal{O}_K$ is indeed a ring.*

1.6 Exercises

1. Find the minimal polynomial of the following numbers (i) $(1+i)\sqrt{3}$ (ii) $i+\sqrt{3}$ (iii) $2\cos(2\pi/7)$ (iv) $(1 + \sqrt[3]{10} + \sqrt[3]{100})/3$ and determine which ones are algebraic integers.

2. Let K be a field with $\text{char}(K) \neq 2$. Show that every quadratic extension L/K is of the form $L = K(\sqrt{a})$ for some $a \in K$. Show further that $K(\sqrt{a}) = K(\sqrt{b})$ if and only if $a/b \in (K^*)^2$.

3. Let $\mathbb{Q} \subset K \subset L$ be finite extensions of fields. (i) Show that if $\alpha \in L$ is integral over $\mathcal{O}_K$ then it is an algebraic integer.

   (ii) Show that if $f \in K[x]$ is monic and $f^n \in \mathcal{O}_K[x]$ for some n then $f \in \mathcal{O}_K[x]$.

4. Let $A \subset B$ be integral domains and B is integral over A. Show that if I is a non-zero ideal of B, then $I \cap A$ is a non-zero ideal in A.

5. Let x, y be algebraic integers. Show that the conjugates of $x+y, xy$ are of the form $x'+y', x'y'$ where x', y' are conjugates of x, y respectively.

6. Let $K = \mathbb{Q}(\theta)$ where θ is a root of $X^3 - 2X + 6$. Show that $[K : \mathbb{Q}] = 3$ and compute $N_{K/\mathbb{Q}}(\alpha)$ and $T_{K/\mathbb{Q}}(\alpha)$ for $\alpha = n - \theta, n \in \mathbb{Z}$, $\alpha = 1 - \theta^2, 1 - \theta^3$.

2 Integral basis

We shall study $\mathcal{O}_K$ as a $\mathbb{Z}$-module in this chapter.

2.1 Integral closure

We are going to study some basis properties of integral elements over the base ring.

Lemma 2.1. *Let $A \subset B \subset C$ be a tower of rings.*
(i) If $x \in C$ is integral over A then it is also integral over B.
(ii) If B is integral over A and $x \in C$ is integral over B, then x is integral over A.

Proof. (i) This follows immediately from the fact $A \subset B$.
(ii) There exist $b_i \in B$ such that

$$x^n + b_{n-1}x^{n-1} + \cdots + b_0 = 0.$$

Let $R = A[b_0, \ldots, b_{n-1}]$. Since B is integral over A, so R is a finitely generated A-module by Corollary 1.26. But $R[x]$ is a finitely generated R-module since x is integral over R. So by tower law, $R[x]$ is a finitely generated A-module. By (iii) $\Rightarrow$ (i) in Lemma 1.25 we conclude that x is integral over A. □

Definition 2.2. *Let $A \subset B$ be rings. The integral closure of A in B, written A^B, is the set of elements in B which are integral over A.*

Corollary 2.3. *Let $A \subset B \subset C$ be a tower of rings. If B is integral over A, then the integral closure of A in C and the integral closure of B in C are the same.*

Proof. Use Lemma 2.1. □

Theorem 2.4. *Let A be a UFD (unique factorisation domain) and F be the field of quotients (fractions) of D. Then an element $c \in F$ is integral over A if and only if $c \in A$.*

Proof. If $c \in A$ then c is a root of $x - c$ and so it is integral over A. Conversely, if $c \in F$ is integral over A, then we have $a_i \in A$ such that

$$c^n + a_{n-1}c^{n-1} + \cdots + a_0 = 0.$$

Since $c \in F$, we can write $c = \frac{r}{s}$ for some $r, s \in A$. Therefore,

$$r^n + a_{n-1}r^{n-1}s + \cdots + a_0 s^n = 0.$$

A is a UFD and so we can assume r, s are coprime. But $s|r$ by the above equation and so $s = 1$ and so $c \in A$. □

Corollary 2.5. *Let $q \in \mathbb{Q}$, then q is an algebraic integer if and only if $q \in \mathbb{Z}$.*

Proof. $\mathbb{Q}$ is the field of quotients of $\mathbb{Z}$ and $\mathbb{Z}$ is a UFD. Use the above theorem. □

Definition 2.6. *An integral A is said to be integrally closed or normal if whenever $x \in F$ is integral over A, $x \in A$ where F is the field of quotients of A.*

Theorem 2.7. *Every algebraic number is of the form $\frac{a}{b}$ where a is an algebraic integer and b is a non-zero integer.*

Proof. Let x be an algebraic number. Then there exist $a_i \in \mathbb{Q}$ such that

$$x^n + a_{n-1}x^{n-1} + \cdots + a_0 = 0, \text{ where } a_0 \neq 0.$$

Let b be the least common multiple of $a_0, \ldots, a_{n-1}$ and so

$$(bx)^n + ba_{n-1}(bx)^{n-1} + \cdots + b^{n-1}a_1(bx) + a_0b^n = 0.$$

This shows that bx is an algebraic integer. □

Corollary 2.8. *Let K be a number field. Then the field of fractions of $\mathcal{O}_K$ is K.*

Proof. By the above theorem, each $\alpha \in K$ is of the form $\frac{x}{b}$ where x is an algebraic integer and $b \in \mathbb{Z} \subset K$. Then $x \in \mathcal{O}_K$. □

Corollary 2.9. *Let K be a number field. Then $\mathcal{O}_K$ is integrally closed.*

Proof. The field of fraction of $\mathcal{O}_K$ is K and by definition $\mathcal{O}_K$ contains all algebraic integers in K. □

2.2 $\mathcal{O}_K$ as finitely generated $\mathbb{Z}$-module

Lemma 2.10. *Let L/K be a finite separable extension and*

$$\phi_x : L \to L, \quad \phi_x(y) = xy.$$

Define the bilinear form

$$T : L \times L \to K, \quad T(x, y) = T_{L/K}(xy).$$

Then L/K is non-degenerate.

Proof. Let $[L : K] = n$ and $L = K(x)$ for some $x \in F$. Then $X = \{1, x, \ldots, x^{n-1}\}$ is a K-basis for L. Let $x_1 = x, \ldots, x_n$ be the conjugates of x over K. Then by Exercise 5 in the previous chapter, the conjugates of x^r are $x_1^r, \ldots, x_n^r$. Let T_{ij} be thei, jth entry of the matrix of T with respect to the basis X. Then

$$T_{ij} = T_{L/K}(x^{i-1}x^{j-1}) = T_{L/K}(x^{i+j-2}).$$

Let V be the Vandermonde matrix

$$\begin{pmatrix} 1 & 1 & \ldots & 1 \\ x_1 & x_2 & \ldots & x_n \\ \vdots & \vdots & \ldots & \vdots \\ x_1^{n-1} & x_2^{n-1} & \ldots & x_n^{n-1}. \end{pmatrix}$$

Then $T = V^tV$ and so we have $\det T = (\det V)^2$. But $x_i \neq x_j$ for all i, j as L/K is separable and so $\det T = (\det V)^2 \neq 0$. Therefore T is non-degenerate. □

Lemma 2.11. *Suppose $A \subset B$ be integral domain and A is integrally closed. Let F be the field of quotients of A and $z \in B$ be integral over A. Let $P(x)$ be the minimal polynomial of Z over F. Then $P(x) \in A[x]$.*

Proof. Each conjugate z_i of z is integral over A because z is integral over A. Then the sums and products of z_i is again integral over A. So if

$$P(x) = x^n + b_{n-1}x^{n-1} + \cdots + b_0, b_i \in F$$

then b_i is integral over A and so $b_i \in A$ because A is integrally closed. □

Theorem 2.12. *Let A be a Noetherian domain which is integrally closed. Let F be the field of quotients of A and K/F a finite separable extension. Then the integral closure A^K of A in K is a finitely generated A-module. In particular, by taking $A = \mathbb{Z}, F = \mathbb{Q}$ and K be any number field, $\mathcal{O}_K$ is a finitely generated $\mathbb{Z}$-module.*

Proof. K/F is finite and so it is algebraic. Let $u \in K$ and so there exists $q_i \in F$ such that

$$u^n + q_{n-1}u^{n-1} + \cdots + q_0 = 0.$$

Clearing the denominators we have $a_i \in A$ such that

$$a_n u^n + a_{n-1}u^{n-1} + \cdots + a_0 = 0.$$

Multiply both sides by a_n^{n-1} and so

$$(a_n u)^n + (a_n u)^{n-1}a_{n-1} + \cdots + a_n^{n-1}a_0 = 0.$$

Therefore $a_n u$ is integral over A and so $a_n u \in A^K$.

Since K/F is separable so the bilinear form T in Lemma 2.10 is non-degenerate. So we can pick a basis $U = \{u_1, \ldots, u_n\} \subset K$ such that

$$T(u_i, u_j) = \delta_{ij}.$$

By above we can take some suitable a_i and $v_i = a_i u_i$ such that $v_i \in A^K$. Also

$$T(v_i, v_j) = a_i a_j \delta_{ij}.$$

For each $x \in A^K$ we have $x = \sum_{j=1}^n x_j v_j$ for some $x_j \in F$. Since $v_i \in A^K$ for each i and so $xv_i \in A^K$ for each i. The previous lemma shows that the minimal polynomial P_i of xv_i has coefficients in A. In particular, $T_{K/F}(xv_i) \in A$ because it is the coefficient of the subleading term of P_i. On the other hand,

$$T_{K/F}(xv_i) = T_{K/F}(\sum_{j=1}^n x_j v_j v_i) = \sum_{j=1}^n x_j T(v_i, v_j) = a_i^2 x_i.$$

So $a_i^2 x_i \in A$. Since $a_i \in A \subset F$ so $x_i \in F$. Since A is integrally closed so $x_i \in A$. Therefore, A^K is contained in an A-module generated by $v_1, \ldots, v_n$. But A is Noetherian, so A^K is finitely generated. □

Corollary 2.13. *Let K be a number field. Then $\mathcal{O}_K$ is Noetherian.*

Proof. The previous theorem shows that $\mathcal{O}_K$ is a finitely generated $\mathbb{Z}$-module and since $\mathbb{Z}$ is Noetherian we conclude that $\mathcal{O}_K$ is Noetherian. □

2.3 Integral basis and discriminant

We have seen that $\mathcal{O}_K$ is a finitely generated $\mathbb{Z}$-module.

Definition 2.14. *A basis for $\mathcal{O}_K$ over $\mathbb{Z}$ is called an integral basis for K.*

Lemma 2.15. *Let K be an algebraic number field and $[K : \mathbb{Q}] = n$, with embeddings $\sigma_1, \ldots, \sigma_n$. Let $\{u_1, \ldots, u_n\}$ and $\{v_1, \ldots, v_n\}$ be integral bases and U, V be matrices such that*

$$U_{ij} = \sigma_j(u_i), \quad V_{ij} = \sigma_j(v_i).$$

Then $(\det U)^2 = (\det V)^2$.

Proof. Since $v_i \in \mathcal{O}_K$ for all i so there exist $a_{ij} \in \mathbb{Z}$ such that

$$v_i = \sum_{j=1}^{n} a_{ij} u_j.$$

But $\{v_1, \dots, v_n\}$ is also a basis so the matrix $A = (a_{ij})_{i,j=1}^{n}$ is invertible and so $\det A = \pm 1$. Since

$$V_{ik} = \theta_k(v_i) = \theta_k(\sum_{j=1}^{n} a_{ij} u_j) = \sum_{j=1}^{n} \theta_k(u_j) a_{ij} = \sum_{j=1}^{n} U_{jk} a_{ij}$$

so $V = UA$. Therefore

$$(\det V)^2 = (\det U)^2 (\det A)^2 = (\det U)^2.$$

□

The above lemma allows us to make the following definition.

Definition 2.16. *Let $[K : \mathbb{Q}] = n$. The discriminant of K, written $\mathcal{D}_K$, is defined as $\det S$ where S is the matrix with entries*

$$S_{ij} = \sigma_j(\theta_i)$$

and $\{\theta_1, \dots, \theta_n\}$ is an integral basis for K.

More generally, the discriminant of a (finitely generated) submodule in $\mathcal{O}_K$ generated by $u_1, \dots, u_n$ is defined as $(\det U)^2$ where $U_{ij} = \theta_j(u_i)$. Usually this is written as $\Delta(u_1, \dots, u_n)$.

Lemma 2.17. *Let M be a submodule in $\mathcal{O}_K$, generated by $u_1, \dots, u_n$ and $U_{ij} = \theta_j(u_i)$ and let $r = [\mathcal{O}_K : M]$ be the index. Then*

$$\Delta(u_1, \dots, u_n) = (\det U)^2 = r^2 \mathcal{D}_K.$$

Proof. By structure theorem of finitely generated module over principal ideal domain, if $\{\theta_1, \dots, \theta_n\}$ is an integral basis, then there exist $r_1, \dots, r_n$ with $r_1 \cdots r_n = r$ such that $\{\theta_1 r_1, \dots, \theta_n r_n\}$ is a basis for M. But we have seen that the square of the discriminant of a $\mathbb{Z}$-module is independent of the choice of the basis, so we have $(\det U)^2 = (\det R)^2$ where

$$R_{ij} = \sigma_j(\theta_i r_i) = r_i \sigma_j(\theta_i)$$

and so

$$(\det U)^2 = (\det R)^2 = r^2 \mathcal{D}_K.$$

□

Corollary 2.18. *Let K be an algebraic number field and $\alpha \in \mathcal{O}_K$ such that $K = \mathbb{Q}(\alpha)$. Let $[K : \mathbb{Q}] = n$ and f be the minimal polynomial of α. Then*

$$disc(f) = \Delta(1, \alpha, \cdots, \alpha^{n-1}) = r^2 \mathcal{D}_K$$

where $r = [\mathcal{O}_K : M]$ and M is the submodule in $\mathcal{O}_K$ generated by $1, \alpha, \dots, \alpha^{n-1}$. In particular, if disc$(f)$ is square free, then $\{1, \alpha, \dots, \alpha^{n-1}\}$ is an integral basis of K.

Proof. Let $\alpha_1 = \alpha, \alpha_2, \dots, \alpha_n$ be the conjugates of α such that $\sigma_j(\alpha_1) = \alpha_j$. Then $\sigma_j(\alpha^i) = \alpha_j^i$. So

$$\Delta(1, \alpha, \dots, \alpha^{n-1}) = \det \begin{pmatrix} 1 & 1 & \dots & 1 \\ \alpha_1 & \alpha_2 & \dots & \alpha_n \\ \vdots & \vdots & \vdots & \vdots \\ \alpha_1^{n-1} & \alpha_2^{n-1} & \dots & \alpha_n^{n-1} \end{pmatrix} = \prod_{i \neq j} (\alpha_i - \alpha_j) = \text{disc}(f).$$

The second equality follows from the previous lemma.

If disc(f) is square free, then $r = 1$ and so $\mathcal{O}_K$ is generated by $1, \alpha, \dots, \alpha^{n-1}$. □

2.4 Calculation of bases

Proposition 2.19. *Let $d \neq 0, 1$ be a square free integer and $K = \mathbb{Q}(\sqrt{d})$. If $d \not\equiv 1$ mod 4 then $\mathcal{O}_K = \mathbb{Z}[\sqrt{d}]$. If $d \equiv 1$ mod 4 then $\mathcal{O}_K = \mathbb{Z}[(1+\sqrt{d})/2]$.*

Proof. It is clear that for each d, $\mathbb{Z}[\sqrt{d}] \subset \mathcal{O}_K$ because $\sqrt{d}$ is a root of $x^2 - d$.

Let $\alpha = a + b\sqrt{d}, a, b \in \mathbb{Q}$. $\alpha \in \mathcal{O}_K$ if and only if $T_{K/\mathbb{Q}}(\alpha), N_{K/\mathbb{Q}}(\alpha) \in \mathbb{Z}$ because the minimal polynomial of α is

$$x^2 - T_{K/\mathbb{Q}}(\alpha) + N_{K/\mathbb{Q}}(\alpha).$$

We have

$$T_{K/\mathbb{Q}}(\alpha) = 2a, \quad N_{K/\mathbb{Q}} = a^2 - b^2 d$$

and so $a \in \frac{1}{2}\mathbb{Z}$ and $a^2 - b^2 d \in \mathbb{Z}$. If $a \in \mathbb{Z}$ then $b \in \mathbb{Z}$ because d is square free.

If $a \notin \mathbb{Z}$ then $a = \frac{1}{2} + a'$ for some $a' \in \mathbb{Z}$. So

$$a^2 - b^2 d = a'^2 + a' + \frac{1}{4} - b^2 d \in \mathbb{Z}$$

and so $\frac{1}{4} - b^2 d \in \mathbb{Z}$. So $4|1 - (4b^2)d$ and so $2b \in \mathbb{Z}$ because d is square free and $4|1-(4b^2)d$ can only happen when $2b$ is odd and $d \equiv 1$ mod 4. Therefore, we conclude that if $d \not\equiv 1$ mod 4, $\mathcal{O}_K = \mathbb{Z}[\sqrt{d}]$ and when $d \equiv 1$ mod 4, $\mathcal{O}_K = \mathbb{Z}[(1+\sqrt{d})/2]$. □

Corollary 2.20. *Let $d \neq 0, 1$ be a square free integer and $K = \mathbb{Q}(\sqrt{d})$. Then $\mathcal{D}_K = d$ if $d \equiv 1$ mod 4 and $\mathcal{D}_K = 4d$ if $d \not\equiv 1$ mod 4.*

Proof. $\{1, (1+\sqrt{d})/2\}$ is an integral basis if $d \equiv 1$ mod 4 and so

$$\mathcal{D}_K = \begin{vmatrix} 1 & (1+\sqrt{d})/2 \\ 1 & (1-\sqrt{d})/2 \end{vmatrix}^2 = d.$$

If $d \not\equiv 1$ mod 4 then

$$\mathcal{D}_K = \begin{vmatrix} 1 & \sqrt{d} \\ 1 & -\sqrt{d} \end{vmatrix} = 4d.$$

□

The following proposition is useful to compte the integral basis of a number field with intermediate extensions.

Proposition 2.21. *Let $K/F/\mathbb{Q}$ be finite extensions of fields. If $\alpha \in \mathcal{O}_K$, then $T_{K/F}(\alpha)$, $N_{K/F}(\alpha) \in \mathcal{O}_F$.*

Proof. α is integral over $\mathbb{Z}$ and so integral over $\mathcal{O}_F$. Let f be the minimal polynomial of α over F then each coefficient of f is contained in $\mathcal{O}_F$. But $T_{K/F}(\alpha), N_{K/F}(\alpha)$ are (up to ±1) the coefficients of the subleading term and the constant term of f so they are both contained in $\mathcal{O}_F$. □

2.5 Exercises

1. Let $K = \mathbb{Q}(\delta)$ where $\delta = \sqrt[3]{d}$ and $d \neq 0, \pm 1$ is a square free integer. Show that $\Delta(1, \delta, \delta^2) = -27d^2$. By calculating the traces of $\theta, \delta\theta, \delta^2\theta$ and the norm of θ, where $\theta = u + v\delta + w\delta^2$ with $u, v, w \in \mathbb{Q}$, show that the ring of integers $\mathcal{O}_K$ of K satisfies

$$\mathbb{Z}[\delta] \subset \mathcal{O}_K \subset \frac{1}{3}\mathbb{Z}[\delta].$$

Verify that the field polynomial of θ is

$$x^3 - 3ux^2 + 3(u^2 - vwd)x - (u^3 + v^3 d + w^3 d^2 - 3uvwd).$$

By considering the cases when $3u, 3v, 3w$ are $0, \pm 1$, prove that an integral basis for K is given by $1, \delta, \delta^2$ when $d \not\equiv \pm 1 \bmod 9$ and by $1, \delta, \gamma$ otherwise, where $\gamma = \frac{1}{1 \pm \delta + \delta^2}$ with corresponding $\pm$ signs.

2. Let $K = \mathbb{Q}(i, \sqrt{2})$. By computing the relative traces $T_{K/k}(\theta)$ where k runs through the three quadratic subfields of K, show that the algebraic integers θ of K have the form $\frac{1}{2}(\alpha + \beta\sqrt{2})$ where $\alpha = a + ib$ and $\beta = c + id$ are Gaussian integers. By considering $N_{K/k}(\theta)$ where $k = \mathbb{Q}(i)$ show that

$$\begin{aligned} a^2 - b^2 - 2c^2 + 2d^2 &\equiv 0 \bmod 4 \\ ab - 2cd &\equiv 0 \bmod 2. \end{aligned}$$

Hence prove that an integral basis for K is $1, i, \sqrt{2}, \frac{1}{2}(1+i)\sqrt{2}$ and calculate the discriminant $\mathcal{D}_K$. The method illustrated here can be used to compute integral bases for many biquadratic extensions.

3. Suppose that K is a number field of degree $n = r + 2s$ where r is the number of real embeddings and s is the number of complex embeddings. Show that the sign of the discriminant $\mathcal{D}_K$ is $(-1)^s$.

4. Let $f(X) \in \mathbb{Q}[X]$ be an irreducible polynomial of degree n, and $\theta \in \mathbb{C}$ a root of f.

   (i) Show that $\operatorname{disc}(f) = (-1)^{\binom{n}{2}} N_{K/\mathbb{Q}}(f'(\theta))$ where $K = \mathbb{Q}(\theta)$.

   (ii) Let $f(X) = X^n + aX + b$. Write own the matrix representing multiplication by $f'(\theta)$ with respect to the basis $1, \theta, \ldots, \theta^{n-1}$ for K. Hence show that

   $$\operatorname{disc}(f) = (-1)^{\binom{n}{2}}((1-n)^{n-1}a^n + n^n b^{n-1}).$$

5. Let K be an algebraic number field and define the bilinear form

$$T : \mathcal{O}_K \times \mathcal{O}_K \to \mathbb{Z}, \quad T(x, y) = T_{K/\mathbb{Q}}(xy).$$

Show that $\mathcal{D}_K = \det A$ where $A_{ij} = T(e_i, e_j)$ and $\{e_1, \ldots, e_n\}$ is an integral basis of K.

6. Let K be an algebraic number field of degree n with an integral basis $\{x_1, \ldots, x_n\}$ and embeddings $\sigma_1, \ldots, \sigma_n$. Write $\mathcal{D}_K = d^2$ where $d = \det(\sigma_j(x_i))$. By considering $d = P - N$ where P is the sum in the determinant corresponding to even permutations in S_n and N is the sum corresponding to odd permutations, show that $\mathcal{D}_K \equiv 0, 1 \bmod 4$. Hence compute the ring of integers of $K(\theta)$ where θ is a root of $X^3 - X + 2$.

3 Unique factorisation

We know that every positive integer n can be written uniquely as a product of primes. Can we establish a similar statement for ideals? This question leads to the study of a special integral domain called Dedekind domain.

3.1 Dedekind domain

We have seen in the previous chapters that the ring of integers $\mathcal{O}_K$ is (i) integrally closed (ii) Noetherian. We now establish more properties of $\mathcal{O}_K$.

Lemma 3.1. *Let K be a number field and $I \subset \mathcal{O}_K$ an ideal. Then $I \cap \mathbb{Z} \neq \varnothing$ and $\mathcal{O}_K/I$ is finite.*

Proof. Take a non-zero element $x \in I$ and there exist $a_i \in \mathbb{Z}$ such that

$$x^n + a_{n-1}x^{n-1} + \cdots + a_0 = 0, \text{ where } a_0 \neq 0.$$

Then

$$a_0 = (-x^{n-1} - a_{n-1}x^{n-2} - \cdots - a_1)x \in I$$

and so $a_0 \in I \cap \mathbb{Z}$.

Let $\{e_1, \ldots, e_n\}$ be an integral basis of K. Write $\bar{e}_i = e_i \bmod I$ and so $\{\bar{e}_1, \ldots, \bar{e}_n\}$ is a $\mathbb{Z}/I \cap \mathbb{Z}$-basis for $\mathcal{O}_K/I$. Since $\mathbb{Z}$ is a principal ideal domain and so we write $I \cap \mathbb{Z} = \langle \alpha \rangle$. Therefore,

$$\mathbb{Z}/I \cap \mathbb{Z} \cong \{0, 1, \ldots, \alpha - 1\}$$

is finite and so $\mathcal{O}_K/I$ is a finitely generated module over a finite ring, which must be finite. □

Corollary 3.2. *Every non-zero prime ideal $\mathfrak{p} \subset \mathcal{O}_K$ is maximal.*

Proof. Since $\mathfrak{p}$ is prime, so $\mathcal{O}_K/\mathfrak{p}$ is an integral domain. The previous lemma shows that this is a finite integral domain, which is a field by standard ring theory. Therefore $\mathfrak{p}$ is maximal. □

Theorem 3.3. *For all primes $p \in \mathbb{Z}$, there exists a prime ideal $\mathfrak{p} \subset \mathcal{O}_K$ such that $\mathfrak{p} \cap \mathbb{Z} = p$. Moreover, there exist only finitely many such $\mathfrak{p}$.*

Proof. $\langle p \rangle \mathcal{O}_K \neq \mathcal{O}_K$ because otherwise $\frac{1}{p} \in \mathcal{O}_K$ because $1 \in \mathcal{O}_K$, which is impossible. Take any maximal ideal $\mathfrak{p} \subset \mathcal{O}_K$ which contains $\langle p \rangle \mathcal{O}_K$ (because $\mathcal{O}_K$ is Noetherian). So $\mathfrak{p}$ is prime and $\mathfrak{p} \cap \mathbb{Z}$ is an ideal in $\mathbb{Z}$ which contains p. If the intersection contains any integer which is not a multiple of p, then $1 \in \mathfrak{p}$ which is a contradiction. Therefore,

$$\mathfrak{p} \cap \mathbb{Z} = p.$$

By Lemma 3.1, $\mathcal{O}_K/\langle p \rangle \mathcal{O}_K$ is finite. But there is a one-to-one correspondence between prime ideals $\mathfrak{p} \subset \mathcal{O}_K$ containing $\langle p \rangle \mathcal{O}_K$ and prime ideals in $\mathcal{O}_K/\langle p \rangle \mathcal{O}_K$ and so there are only finitely many of them. □

Definition 3.4. *An integral domain D is a Dedekind domain if (i) D is Noetherian (ii) D is integrally closed (iii) each non-zero prime ideal of D is a maximal ideal.*

So we have shown that $\mathcal{O}_K$ is a Dedekind domain.

Proposition 3.5. *Every principal ideal domain is a Dedekind domain.*

Proof. It is clear that any principal ideal domain satisfies (i) and (iii) in the above definition. But it is also a unique factorisation domain and so it satisfies (ii) by Theorem 2.4. □

3.2 Fractional ideals

Definition 3.6. *Let D be an integral domain and K be the field of quotients of D. A fractional ideal I of D is a set of elements in K satisfying the following properties: (i) If $\alpha, \beta \in I$, then $\alpha + \beta \in I$. (ii) If $\alpha \in I$ and $r \in D$, then $r\alpha \in I$. (iii) There exists $\gamma \in D$ with $\gamma \neq 0$ such that $\gamma I \subset D$. Equivalently, it is a D-module of K such that there exists $0 \neq \gamma$ with $\gamma I \subset D$. The element γ can be considered as the common factor of these elements in I.*

For example, $I = \left\{\frac{n}{25} : n \in \mathbb{Z}\right\}$ is a fractional ideal and $I = \left\{\frac{n}{3^m} : n \in \mathbb{Z}, m \in \mathbb{Z}_{\geq 0}\right\}$ is not a fractional ideal. It is clear that every ideal is in fact a fractional ideal (by taking $\gamma = 1$).

Lemma 3.7. *Let I be a fractional ideal. Then there exists γ such that $\gamma I \subset D$.*

Proof. Use (iii) in the definition. □

Lemma 3.8. *Let I, J be fractional ideals. Then $I + J, IJ$ are also fractional ideals.*

Proof. Let γ, δ be elements such that $\gamma I, \delta J \in D$. Then

$$\gamma\delta(I + J), \gamma\delta IJ \subset D.$$

□

Definition 3.9. *The inverse of an fractional ideal I is defined as*

$$I^{-1} = \{x \in K : xI \subset D\}.$$

Lemma 3.10. *I^{-1} is a fractional ideal.*

Proof. Suppose $\alpha, \beta \in I^{-1}$, then

$$(\alpha + \beta)I = \alpha I + \beta I \subset D + D = D.$$

If $\alpha \in I^{-1}$ and $r \in D$, then

$$r\alpha I \subset rD \subset D.$$

Finally take any $\gamma \in I$, then for each $\alpha \in I^{-1}$, we have $\alpha\gamma \in D$ and so $\gamma I^{-1} \subset D$. □

We now focus on Dedekind domain.

Lemma 3.11. *Let D be a Dedekind domain and $I \subset D$ a non-zero ideal. Then I contains a product of prime ideals.*

Proof. Suppose not, let S be the set of non-zero ideals which do not contain a product of prime ideals and so S is non-empty. Since D is Noetherian, there exist an ideal $A \in S$ which is maximal with this property. In other words, $A \not\subset B$ for any $B \in S$. By assumption A itself is not prime and there exist ideals B, C such that

$$BC \subset A, \quad B \not\subset A, \quad C \not\subset A.$$

Define B_1 and C_1 by $B_1 = A+B$ and $C_1 = A+C$. Then $A \subset B_1, C_1$. By maximality of A, $B_1, C_1 \notin S$ and so there are prime ideals $P_1, \ldots, P_m$ and $Q_1, \ldots, Q_n$ such that

$$P_1 \cdots P_m \subset B_1, \quad Q_1 \cdots Q_n \subset C_1.$$

But $B_1C_1 = (A + B)(A + C) \subset A$ and so

$$P_1 \cdots P_m Q_1 \cdots Q_n \subset A$$

which is a contradiction. □

Lemma 3.12. *Let D be a Dedekind domain and $\mathfrak{p}$ a non-zero prime ideal of D. Then D is strictly contained in $\mathfrak{p}^{-1}$.*

Proof. It is clear that $D \subset P^{-1}$. Take a non-zero element $x \in \mathfrak{p}$ then the previous lemma shows that we have prime ideals $P_1, \ldots, P_m$ such that

$$P_1 \cdots P_m \subset \langle x \rangle \subset \mathfrak{p}.$$

Let k be the least integer m such that the inclusion holds. Since $\mathfrak{p}$ is prime so $P_i \subset \mathfrak{p}$ for some i. We may assume $i = 1$ by relabeling. But P_1 is prime and so it is maximal. So $P_1 = \mathfrak{p}$.

If $k \geq 2$ by minimality of k we have

$$P_2 \cdots P_k \not\subset \langle x \rangle$$

and so there exists $y \in P_2 \cdots P_k$ such that $y \notin \langle x \rangle$. Let $\gamma = \frac{y}{x}$ and so $\gamma \notin D$. But

$$\mathfrak{p}\langle y \rangle = P_1 \langle y \rangle \subset P_1 \cdots P_k \subset \langle x \rangle$$

and so $\gamma \mathfrak{p} \subset D$. This shows that $\gamma \in \mathfrak{p}^{-1}$ which is an element in $\mathfrak{p}^{-1} \backslash D$.

If $k = 1$, we must have $\mathfrak{p} = P_1 = \langle x \rangle$ and so x is not a unit. Let $\gamma = \frac{1}{x}$ and so

$$\gamma \mathfrak{p} = \frac{1}{x} \langle x \rangle = \langle 1 \rangle = D.$$

This shows that $\gamma \in \mathfrak{p}^{-1}$ which is an element in $\mathfrak{p}^{-1} \backslash D$. □

Corollary 3.13. *Let D be a Dedekind domain and $\mathfrak{p}$ a non-zero prime ideal. Then $\mathfrak{p}\mathfrak{p}^{-1} = D$.*

Proof. Let $P = \mathfrak{p}\mathfrak{p}^{-1}$. Since $1 \in \mathfrak{p}^{-1}$ and so $\mathfrak{p} \subset P$. But each non-zero prime ideal in D is maximal and so $P = \mathfrak{p}$ or D.

Suppose $P = \mathfrak{p}$. For each $x \in \mathfrak{p}^{-1}$, we have

$$x\mathfrak{p} \subset P = \mathfrak{p}.$$

So for all $x, y \in \mathfrak{p}^{-1}$ we have

$$xy\mathfrak{p} \subset x\mathfrak{p} \subset \mathfrak{p} \subset D$$

and so $xy \in \mathfrak{p}^{-1}$. This shows that $\mathfrak{p}^{-1}$ is a subring of D. Since D is Noetherian so $\mathfrak{p}^{-1}$ is a finitely generated D-module. Therefore x is integral over D for any $x \in \mathfrak{p}^{-1}$ by Lemma 1.25 (iii) ⇒ (i). But D is integrally closed and so $x \in D$. This shows that $\mathfrak{P}^{-1} \subset D$ which is a contradiction to the previous lemma. Therefore, $P = D$. □

3.3 Unique factorisation

Theorem 3.14. *Let D be a Dedekind domain. Then every ideal $I \subset D$, $I \neq D$ can be written uniquely as a product of prime ideals:*

$$I = \prod_{i=1}^{n} \mathfrak{p}_i^{a_i}.$$

Proof. Existence: Suppose not, let S be the set which contains ideals which are not product of prime ideals. Since D is Noetherian, there exists a maximal element A in S, i.e. for any $J \in S$, $A \not\subset J$. Since $A \neq D$, there exists a maximal ideal $B \subset D$ which contains A and B is prime. Let $C = B^{-1}$. Then $AC \subset BC \subset D$ is an ideal in D.

By Lemma 3.12, D is strictly contained in C. But $A = AD \subset AC$ and so A is strictly contained in an ideal AC of D. By maximality of A, $AC \notin S$ and so there exist $\mathfrak{p}_i, a_i$ such that

$$AC = \prod_{i=1}^{n} \mathfrak{p}_i^{a_i}.$$

Multiplying both sides by B gives

$$A = \prod_{i=1}^{n} \mathfrak{p}_i^{a_i} B$$

which gives a contradiction (as B is also prime).

Uniqueness: suppose we have prime ideals $P_1, \ldots, P_m, Q_1, \ldots, Q_n$ not necessarily distinct, such that

$$P_1 \cdots P_m = Q_1 \cdots Q_n.$$

Then $P_1 \cdots P_m \subset Q_1$ and so $P_i \subset Q_1$ for some i. We may assume $i = 1$ by relabeling $P_1, \ldots, P_m$. But P_1 is maximal and $Q_1 \neq D$ so $P_1 = Q_1$. Now multiply both sides by P_1^{-1} and we have

$$P_2 \cdots P_m = Q_2 \cdots Q_n.$$

Repeat the above and so we conclude that $m = n$ and $P_i = Q_i$ after relabeling. □

Corollary 3.15. *Let D be a Dedekind domain and $I \subset D$ a non-zero ideal. Then $II^{-1} = D$.*

Proof. Use unique factorisation of I and the fact $\mathfrak{p}\mathfrak{p}^{-1} = D$ for any prime ideal $\mathfrak{p}$. □

Example 3.16. *Let $D = \mathbb{Z}[\sqrt{-5}]$. Since $-5 \not\equiv 1$ mod 4, so $D = \mathcal{O}_K$ where $K = \mathbb{Q}(\sqrt{-5})$ and so it is a Dedekind domain. Note that D is not a UFD because*

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

Let

$$\mathfrak{p}_1 = \langle 2, 1 + \sqrt{-5} \rangle, \mathfrak{p}_2 = \langle 3, 1 + \sqrt{-5} \rangle, \mathfrak{p}_3 = \langle 3, 1 - \sqrt{-5} \rangle.$$

Then

$$\mathfrak{p}_2\mathfrak{p}_3 = \langle 9, 3(1 + \sqrt{-5}), 3(1 - \sqrt{-5}), 6 \rangle = \langle 3 \rangle \langle 3, 1 + \sqrt{-5}, 1 - \sqrt{-5}, 2 \rangle = \langle 3 \rangle$$

and

$$\mathfrak{p}_1^2 = \langle 4, 2(1 + \sqrt{-5}), -4 + 2\sqrt{-5} \rangle = \langle 2 \rangle \langle 2, 1 + \sqrt{-5}, -2 + \sqrt{-5} \rangle = \langle 2 \rangle.$$

Therefore, $\langle 6 \rangle = \langle 2 \rangle \langle 3 \rangle = \mathfrak{p}_1^2 \mathfrak{p}_2 \mathfrak{p}_3$.

We can similarly check that

$$\langle 1 + \sqrt{-5} \rangle = \langle 2, 1 + \sqrt{-5} \rangle \langle 3, 1 + \sqrt{-5} \rangle, \langle 1 - \sqrt{-5} \rangle = \langle 2, 1 + \sqrt{-5} \rangle \langle 3, 1 - \sqrt{-5} \rangle$$

and so the factorisation of $\langle 6 \rangle$ is unique.

3.4 Valuations

Definition 3.17. *Let D be a Dedekind domain and $A, B \subset D$ non-zero ideals. We say A divides B, written $A|B$, if there exists $C \subset D$ such that $B = AC$.*

Lemma 3.18. *$A|B$ if and only if $B \subset A$.*

Proof. $A|B$ if and only if $A^{-1}B \subset D$, if and only if $B \subset AD = A$. □

Corollary 3.19. *Let D be a Dedekind domain and $A, B \subset D$ be non-zero ideals and write*

$$A = \prod_i \mathfrak{p}_i^{a_i}, \quad B = \prod_i \mathfrak{p}_i^{b_i}, \text{ where } a_i, b_i \geq 0$$

and $\mathfrak{p}_i$ are distinct prime ideals. Then

$$A + B = \prod_i \mathfrak{p}_i^{c_i}, \quad A \cap B = \prod_i \mathfrak{p}_i^{d_i}$$

where $c_i = \min\{a_i, b_i\}$ and $d_i = \max\{a_i, b_i\}$. In other words, $A + B$ is the greatest common divisor of A, B and $A \cap B$ is the least common multiple of A, B.

Proof. $A, B \subset A+B$ and so $A+B|A, B$. For any $C|A, B$, we have $A, B \subset C$ and so $A+B \subset C$. So $C|A+B$ and $A+B$ is the greatest common divisor of A, B.

$A \cap B \subset A, B$ and so $A, B|A \cap B$. For any C with $A, B|C$, we have $C \subset A, B$ and so $C \subset A \cap B$. So $A \cap B|C$ and $A \cap B$ is the least common multiple of A, B. □

Definition 3.20. *Let D be a Dedekind domain and $A = \prod_i \mathfrak{p}_i^{a_i}$ a non-zero ideal in D. The valuation of A at a non-zero prime ideal P, written $v_P(A)$, is 0 if $P \nmid A$ and a_i if $P = \mathfrak{p}_i$.*

If $0 \neq a \in D$, then the valuation of a at P is defined as $v_P(A)$ where $A = \langle a \rangle$.

Proposition 3.21. *(i) For any non-zero ideals $A, B \in D$ and non-zero prime ideal P, we have*

$$v_P(AB) = v_P(A) + v_P(B)$$

and

$$v_P(A+B) = \min\{v_P(A), v_P(B)\}.$$

(ii) For any non-zero element $a \in D$ and non-zero ideal $A \subset D$, $a \in A$ if and only if $v_P(a) \geq v_P(A)$ for all non-zero prime ideals P.

(iii) If $0 \neq x, y \in D$ with $\alpha + \beta \neq 0$, then

$$v_P(x+y) \geq \min\{v_P(x), v_P(y)\}$$

for any non-zero prime ideal P, with equality holds if $v_P(x) \neq v_P(y)$.

Proof. (i) $v_P(AB) = v_P(A) + v_P(B)$ by using unique factorisation of A, B. Then use the fact $A+B$ is the greatest common divisor of A and B.

(ii) $a \in A$ if and only if $A|\langle a \rangle$, if and only if $v_P(a) \geq v_P(A)$ by unique factorisation.

(iii) Since $x+y \subset \langle x \rangle + \langle y \rangle$ and so the inequality follows from (i) and (ii). Suppose $v_P(x) \neq v_P(y)$, we assume $v_P(x) > v_P(y)$. It is clear that $v_P(-x) = v_P(x)$ and so

$$v_P(y) = v_P((x+y) - x) \geq \min\{v_P(x+y), v_P(x)\}.$$

But $v_P(x) > v_P(y)$ so $\min\{v_P(x+y), v_P(x)\} = v_P(x+y)$ and

$$v_P(y) \geq v_P(x+y).$$

But $v_P(x+y) \geq \min\{v_P(x), v_P(y)\} = v_P(y)$, so $v_P(x+y) = v_P(y)$. □

Theorem 3.22. *Let D be a Dedekind domain and $P_1, \ldots, P_k$ be non-zero prime ideals of D. For any $a_1, \ldots, a_k \geq 0$, there exists an element $x \in D$ such that $v_{P_i}(x) = a_i$ for each i.*

Proof. Let $J = \prod_j P_j^{a_j+1}$ and $I_i = P_i^{a_i} \prod_{j \neq i} P_j^{a_j+1}$ for each i. Since $I_i \neq J$ and $I_i|J$, there exists $x_i \in I_i, x_i \notin J$ because J is strictly contained in I_i for each i. Let $x = x_1 + \cdots + x_k$.

For each i, $I_i|x_i$ but $J \nmid x_i$, so $v_{P_i}(x_i) = a_i$ and $v_{P_j}(x_i) \geq a_{j+1}$ for $j \neq i$. Applying (iii) in the lemma above repeatedly, we conclude that $v_{P_i}(x) = a_i$. □

3.5 Exercises

Throughout, D is a Dedekind domain.

1. Let P, Q be non-zero ideals in D such that $P+Q = D$. Then

$$D/PQ \cong D/P \times D/Q.$$

This is usually called the Chinese remainder theorem for Dedekind domain.

2. Show that for every ideal $A \subset D$, there exists an ideal $B \subset D$ such that $AB = \langle c \rangle$ where $c \in D$.

3. Show that if D is a UFD, then it is a PID. Thus, a Dedekind domain is a PID if and only if it is a UFD.

4. Let $D = \mathbb{Z}[\sqrt{-5}]$ and $I = \langle 2, 1 + \sqrt{-5}\rangle$. Find I^{-1}.

5. Let $A \subset D$ be a non-zero ideal. Show that every ideal in D/A is principal. Hence show that every ideal in D is generated by at most two elements.

6. Let $\mathcal{O}_K$ be the ring of integers for an algebraic number field K. Show that there are infinitely many prime ideals in $\mathcal{O}_K$.

7. (i)Let $I \subset D$ be a non-zero ideal and K be the field of quotients of D. Show that if $x \in K$ and $xI \subset I$, then $x \in D$.

   (ii) A DVR (discrete valuation ring) is principal ideal domain with exactly one non-zero prime ideal. Show that a ring R is a DVR if and only if it is a Dedekind domain with exactly one prime ideal.

4 Ideals

We shall study the norm of ideals in $\mathcal{O}_K$ and the factorisation of $\langle p\rangle$ in $\mathcal{O}_K$ where $p \in \mathbb{Z}$ is a prime number.

4.1 Norm of ideals

We have seen in the previous chapter that $\mathcal{O}_K/I$ is finite for any non-zero ideal I.

Definition 4.1. *Let $I \subset \mathcal{O}_K$ be a non-zero ideal. The norm of I, written $N(I)$ is defined as the size of $\mathcal{O}_K/I$. For convention, $N(\langle 0\rangle) = 0$.*

Remark 4.2. *Recall that each ideal $I \subset \mathcal{O}_K$ is a finitely generated $\mathbb{Z}$-module. Recall that the discriminant of I (as a $\mathbb{Z}$-submodule in $\mathcal{O}_K$) is*

$$\Delta(x_1, \dots, x_n)$$

for a basis $\{x_1, \dots, x_n\}$ of I. Then it is easy to see that

$$N(I)^2 = \Delta(x_1, \dots, x_n)/\mathcal{D}_K$$

by Lemma 2.17.

We are going to show that the norm is multiplicative.

Lemma 4.3. *For any prime ideal $\mathfrak{p}$ and $n \geq 0$, we have*

$$\mathfrak{p}^n/\mathfrak{p}^{n+1} \cong \mathcal{O}_K/\mathfrak{p}$$

as $\mathcal{O}_K$-module.

Proof. $\mathfrak{p}^n \neq \mathfrak{p}^{n+1}$ by unique factorisation, and so there exists $\pi \in \mathfrak{p}^n \backslash \mathfrak{p}^{n+1}$. Therefore, $\mathfrak{p}^n | \langle\pi\rangle$ and $\mathfrak{p}^{n+1} \nmid \langle\pi\rangle$. Define the map

$$\psi : \mathcal{O}_K \to \mathcal{O}_K/\mathfrak{p}^{n+1}, \quad x \mapsto \pi x + \mathfrak{p}^{n+1}.$$

The kernel is $\mathfrak{p}$ and the image is $\langle\pi\rangle + \mathfrak{p}^{n+1}$. But in $\mathcal{O}_K$, the sum

$$\mathfrak{p}^{n+1} + \langle\pi\rangle = \mathfrak{p}^n$$

and so the image is $\mathfrak{p}^n + \mathfrak{p}^{n+1}$ in $\mathcal{O}_K/\mathfrak{p}^{n+1}$. So the result follows by isomorphism theorem. □

Lemma 4.4. *For any prime ideal P and $n \geq 0$,*

$$N(\mathfrak{p}^n) = N(\mathfrak{p})^n.$$

Proof. Apply isomorphism theorem repeatedly

$$\mathcal{O}_K/\mathfrak{p}^n \cong \mathcal{O}_K/\mathfrak{p} \times \mathfrak{p}/\mathfrak{p}^2 \times \cdots \times \mathfrak{p}^{n-1}/\mathfrak{p}^n$$

and use the previous lemma. □

Corollary 4.5. *$N(IJ) = N(I)N(J)$ for any ideals I, J in $\mathcal{O}_K$.*

Proof. If any of I, J is zero then the result is clear so we assume $I, J \neq 0$. If I, J are coprime, then the result follows by Chinese remainder theorem (exercise 1 in the previous chapter). Therefore, we only need to show that

$$N(P^{a+b}) = N(P^a)N(P^b)$$

for any prime ideal P and integers $a, b \geq 0$. This follows from the previous lemma. □

Proposition 4.6. *$N(I) \in I$ for any ideal I.*

Proof. By definition, $N(I)a \in I$ for any $a \in \mathcal{O}_K$ because $N(I) = |\mathcal{O}_K/I|$. Take $a = 1$. □

Theorem 4.7. *Let K be an algebraic number field and $x \in K$. Then*

$$N(\langle x\rangle) = |N_{K/\mathbb{Q}}(x)|.$$

Proof. Let $\{\theta_1, \dots, \theta_n\}$ be an integral basis of K and so $\{x\theta_1, \dots, x\theta_n\}$ is a $\mathbb{Z}$-basis for $\langle x\rangle$. The discriminant of the ideal $\langle x\rangle$ is $(\det X)^2$ where $X_{ij} = \sigma_j(x\theta_i) = \sigma_j(x)\sigma_j(\theta_i)$. Therefore,

$$\mathcal{D}(\langle x\rangle) = (\det X)^2 = \prod_{i=1}^{n}(\sigma_j(x))^2 \det \begin{pmatrix} \sigma_1(\theta_1) & \dots & \sigma_n(\theta_1) \\ \vdots & \vdots & \vdots \\ \sigma_1(\theta_n) & \dots & \sigma_n(\theta_n) \end{pmatrix} = N_{K/\mathbb{Q}}(x)^2\mathcal{D}_K.$$

So $N(\langle x\rangle) = \sqrt{\mathcal{D}(\langle x\rangle)/\mathcal{D}_K} = |N_{K/\mathbb{Q}}(x)|$. □

4.2 Prime ideals

Lemma 4.8. *Let K be an algebraic number field and $\mathfrak{p}$ be a non-zero prime ideal of $\mathcal{O}_K$. then there exists a unique prime number p such that $\mathfrak{p}|\langle p\rangle$. We say $\mathfrak{p}$ is a prime ideal above p.*

Proof. $\in \mathfrak{p} \cap \mathbb{Z}$ is a prime ideal in $\mathbb{Z}$ and so there exists p such that

$$\mathfrak{p} \cap \mathbb{Z} = \langle p\rangle.$$

Since $\langle p\rangle \subset \mathfrak{p}$ so $\mathfrak{p}|\langle p\rangle$.

Suppose there exists another prime q with $\mathfrak{p}|q$, then $p, q \in \mathfrak{p}$ and so $1 \in \mathfrak{p}$ which is a contradiction. □

Corollary 4.9. *Let K be an algebraic number field and $\mathfrak{p}$ a prime ideal above p. Let $a, b \in \mathbb{Z}$. Then*

$$a \equiv b \textit{ mod } p \textit{ if and only if } a \equiv b \textit{ mod } \mathfrak{p}.$$

Proof. By considering $a - b$ we may assume $b = 0$. Since $\mathfrak{p}|\langle p\rangle$ so $a \equiv 0 \bmod p$ implies $a \equiv 0 \bmod \mathfrak{p}$.

Conversely if $a \equiv 0 \bmod \mathfrak{p}$ then $a \in \mathfrak{p} \cap \mathbb{Z} = \langle p\rangle$ and so $a \equiv 0 \bmod p$. □

Lemma 4.10. *Let K be an algebraic number field of degree n and $\mathfrak{p}$ a prime ideal above p. Then*

$$N(\mathfrak{p}) = p^{f_\mathfrak{p}}$$

for some $f_\mathfrak{p} \le n$ which depends on $\mathfrak{p}$. $f_\mathfrak{p}$ is called the residue degree of $\mathfrak{p}$.

Proof. We have $N(\langle p\rangle) = |N_{K/\mathbb{Q}}(p)| = p^n$ and $N(\mathfrak{p})|N(\langle p\rangle)$. So $N(\mathfrak{p}) = p^f$ for some $f \le n$. □

Corollary 4.11. *Let K be an algebraic number field of degree n and p a prime number. Suppose*

$$\langle p\rangle = \prod_{i=1}^{k} \mathfrak{p}_i^{e_i}$$

where $\mathfrak{p}_1, \dots, \mathfrak{p}_k$ are distinct prime ideals in $\mathcal{O}_K$ and $e_i \ge 1$. Then

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

where $f_i = f_{\mathfrak{p}_i}$ is the residue degree of $\mathfrak{p}_i$. The number e_i here is called the ramification degree of $\mathfrak{p}_i$.

Proof. This follows by taking the norm of both sides. □

Definition 4.12. *Let K be an algebraic number field and p a prime number. Suppose*

$$\langle p\rangle = \prod_{i=1}^{k} \mathfrak{p}_i^{e_i}.$$

We say p is ramified if $e_i > 1$ for some i and p is unramified if $e_i = 1$ for all i.

We say p inerts if $k = 1$ and $e_1 = 1$, i.e. p is unramified and there is only one prime above p. We say p is totally ramified if $k = 1$ and $e_1 = n$, i.e. there is only one prime above p and p is ramified.

We say p splits if $k > 1$ and splits completely if $e_i, f_i = 1$ for all i (in which case $k = n$).

Theorem 4.13. *p is ramified in K if and only if $\mathcal{O}_K/\langle p\rangle$ has a nilpotent element.*

Proof. By Chinese remainder theorem, if $\langle r\rangle = \prod_i \mathfrak{p}_i^{e_i}$, then

$$\mathcal{O}_K/\langle p\rangle \cong \prod_i \mathcal{O}_K/\mathfrak{p}_i^{e_i}.$$

p is ramified if and only if $e_j \geq 2$ for some j.

For each j with $e_j \geq 2$, the element x with $x \in \mathfrak{p}_j$ and $x \notin \mathfrak{p}_j^2$ is a nilpotent element in $\mathcal{O}_K/\mathfrak{p}_j^{e_j}$. This shows that if p is ramified then $\mathcal{O}_K/\langle p\rangle$ contains a nilpotent element.

Conversely, if p is unramified, then $e_i = 1$ for all i and so $\mathcal{O}_K/\langle p\rangle$ is a product of fields (recall that each non-zero prime ideal is maximal), and so it has no nilpotent elements. □

Theorem 4.14. *p is ramified in K if and only if $p|\mathcal{D}_K$.*

Proof. Recall that $\mathcal{D}_K$ is the discriminant of the bilinear trace form

$$T : \mathcal{O}_K \times \mathcal{O}_K \to \mathbb{Z}, T(x, y) = T_{K/\mathbb{Q}}(xy).$$

Let $\{\theta_1, \ldots, \theta_n\}$ be an integral basis and let $T_{ij} = T(\theta_i, \theta_j)$. Then $p|\mathcal{D}_K$ if and only if $\det T \equiv 0 \bmod p$.

Let $\bar{T}$ be the matrix T with entries reduced mod p. So it represents the bilinear form

$$\bar{T} : \mathcal{O}_K/\langle p\rangle \times \mathcal{O}_K/\langle p\rangle \to \mathbb{Z}/\langle p\rangle$$

and so $p|\mathcal{D}_K$ if and only if $\det \bar{T} = 0$ in $\mathbb{Z}/\langle p\rangle$, if and only if $\bar{T}$ is degenerate. Let

$$p = \prod_i \mathfrak{p}_i^{e_i}.$$

Suppose p is unramified, then $e_i = 1$ for all i and since $\mathcal{O}_K/\mathfrak{p}$ is a field and it is finite. Therefore it is separable. So the restriction of $\bar{T}$ on $\mathcal{O}_K/\mathfrak{p} \times \mathcal{O}_K/\mathfrak{p}$ is non-degenerate and so $\bar{T}$ is non-degenerate on $\mathcal{O}_K/\langle p\rangle \times \mathcal{O}_K/\langle p\rangle$.

Suppose p is ramified and $e_i \geq 2$ for some i. Then the previous theorem shows that $\mathcal{O}_K/\langle p\rangle$ has a nilpotent element x. Let $x^n = 0$ for some n. Therefore, $(xy)^n = 0$ for all $y \in \mathcal{O}_K/\langle p\rangle$. This shows that the map

$$\phi_{xy} : K \to K, \quad \phi_{xy}(z) = xyz$$

is nilpotent and so every eigenvalue of ϕ_{xy} is zero. Since the trace of ϕ_{xy} is the sum of the eigenvalues so the trace is zero. In other words,

$$\bar{T}(xy) = 0 \text{ for all } y \in \mathcal{O}_K/\langle p\rangle.$$

Therefore, $\bar{T}$ is degenerate. □

4.3 The different

Definition 4.15. *Let K be an algebraic number field. The inverse different (or codifferent) is defined as*

$$\mathcal{D}_{K/\mathbb{Q}}^{-1} = \{y \in K : T_{K/\mathbb{Q}}(xy) \in \mathbb{Z} \text{ for all } x \in \mathcal{O}_K\}.$$

Lemma 4.16. *$\mathcal{D}_{K/\mathbb{Q}}^{-1}$ is a fractional ideal.*

Proof. Since the trace is linear so if $y_1, y_2 \in \mathcal{D}_{K/\mathbb{Q}}^{-1}$ then so is $y_1 + y_2$. By definition it is clear that if $y \in \mathcal{D}_{K/\mathbb{Q}}^{-1}$ and $r \in \mathcal{O}_K$ then $ry \in \mathcal{D}_{K/\mathbb{Q}}^{-1}$.

Finally, let $\{x_1, \ldots, x_n\}$ be an integral basis of K. For each $y \in \mathcal{D}_{K/\mathbb{Q}}^{-1}$ we write $y = \sum_j \lambda_j x_j$ where $\lambda_j \in \mathbb{Q}$. Then for each i,

$$\sum_j \lambda_j T_{K/\mathbb{Q}}(x_i x_j) = T_{K/\mathbb{Q}}(yx_i) \in \mathbb{Z}.$$

Therefore, let T be the matrix with $T_{ij} = T(x_i, x_j)$ and λ be the vector with entries λ_j, then $T\lambda = z$ where z is a vector with integer entries.

We have seen that T is non-singular and so $\lambda = T^{-1}z$. Since $T^{-1} = \frac{1}{\mathcal{D}_K}T^{adj}$, and T^{adj} has entries in $\mathbb{Z}$, we conclude that $\lambda_j \in \frac{1}{\mathcal{D}_K}\mathbb{Z}$. Therefore,

$$y \in \frac{1}{\mathcal{D}_K}\mathcal{O}_K$$

and so $\mathcal{D}_K\mathcal{D}_{K/\mathbb{Q}}^{-1} \subset \mathcal{O}_K$. □

Definition 4.17. *The different of an algebraic number field K, written $\mathcal{D}_{K/\mathbb{Q}}$ is the inverse of the codifferent $\mathcal{D}_{K/\mathbb{Q}}^{-1}$. Since $\mathcal{D}_{L/K}^{-1}$ contains $\mathcal{O}_K$, it is clear that the different is an ideal in $\mathcal{O}_K$.*

Lemma 4.18. *Let $\{x_1, \ldots, x_n\}$ be an integral basis of K. Then $\mathcal{D}_{L/K}^{-1}$ has a $\mathbb{Z}$-basis $\{y_1, \ldots, y_n\}$ where*

$$T_{K/\mathbb{Q}}(x_i y_j) = \delta_{ij}.$$

Proof. It is clear that such $y_1, \ldots, y_n$ exist by taking dual basis. Suppose $\alpha = \sum_i r_i y_i$ for some $r_i \in \mathbb{Z}$, then

$$T_{K/\mathbb{Q}}(\alpha x_j) = r_j \in \mathbb{Z} \text{ for all } j$$

and so $\alpha \in \mathcal{D}_{K/\mathbb{Q}}^{-1}$.

Suppose $\alpha \in \mathcal{D}_{K/\mathbb{Q}}^{-1}$ then there exist $r_1, \ldots, r_n \in \mathbb{Q}$ such that $\alpha = \sum_i r_i y_i$. By assumption $T_{K/\mathbb{Q}}(\alpha x_j) \in \mathbb{Z}$ for all j and by construction

$$r_j = T_{K/\mathbb{Q}}(\alpha x_j) \in \mathbb{Z}.$$

□

Theorem 4.19. $N(\mathcal{D}_{K/\mathbb{Q}}) = |\mathcal{D}_K|$.

Proof. Let $\{x_1, \ldots, x_n\}$ be an integral basis of K and let $\{y_1, \ldots, y_n\}$ be a $\mathbb{Z}$-basis of $\mathcal{D}_{K/\mathbb{Q}}^{-1}$ in the previous lemma. Let $d = \mathcal{D}_K$ and so $d\mathcal{D}_{K/\mathbb{Q}}^{-1} \subset \mathcal{O}_K$. Therefore,

$$d^{2n}\Delta(y_1, \ldots, y_n) = \Delta(dy_1, \ldots, dy_n) = dr^2$$

where $r = [\mathcal{O}_K : d\mathcal{D}_{K/\mathbb{Q}}^{-1}] = N(d\mathcal{D}_{K/\mathbb{Q}}^{-1})$. But

$$d\mathcal{D}_{K/\mathbb{Q}}^{-1}\mathcal{D}_{K/\mathbb{Q}} = \langle d \rangle$$

and so by multiplicity of the norms, we conclude that

$$r = \frac{d^n}{N(\mathcal{D}_{K/\mathbb{Q}})}.$$

Therefore,

$$\Delta(y_1, \ldots, y_n) = \Delta(dy_1, \ldots, dy_n) = \frac{d}{N(\mathcal{D}_{K/\mathbb{Q}})^2}.$$

Let X, Y be matrices such that $X_{ij} = \sigma_j(x_i)$ and $Y_{ij} = \sigma_i(y_j)$. Then

$$(XY)_{ij} = \sum_k X_{ik}Y_{kj} = \sum_k \sigma_j(x_i)\sigma_k(y_j) = \sum_k \sigma_k(x_i y_j) = T_{K/\mathbb{Q}}(x_i y_j) = \delta_{ij}$$

and so XY is the identity matrix. So $Y = X^{-1}$ and so $(\det Y)^2 = (\det X)^{-2}$. We have shown that

$$(\det Y)^2 = \Delta(y_1, \ldots, y_n) = \frac{d}{N(\mathcal{D}_{K/\mathbb{Q}})^2}$$

and so

$$d = (\det X)^2 = (\det Y)^{-2} = \frac{N(\mathcal{D}_{K/\mathbb{Q}})^2}{d}.$$

Therefore $|d| = N(\mathcal{D}_{K/\mathbb{Q}})$.

□

4.4 Dedekind's criterion

We shall study a theorem of Dedekind which allows us to write down the factorisation of prime ideals in $\mathcal{O}_K$ in most cases.

Theorem 4.20 (Dedekind's criterion). *Let $K = \mathbb{Q}(\theta)$ be an algebraic number field with $\theta \in \mathcal{O}_K$. Let f be the minimal polynomial of θ. Let p be a prime number which does not divide $[\mathcal{O}_K : \mathbb{Z}[\theta]]$, and $\bar{f}$ be the reduction of f mod p. Write*

$$\bar{f}(x) = \prod_{i=1}^{r} g_i^{e_i}$$

for the factorisation of $\bar{f}$ over $\mathbb{Z}/p\mathbb{Z}$, where $g_1, \ldots, g_r$ are distinct monic irreducible polynomials.

For each i, if $f_i(x)$ is a monic polynomial with integer coefficients such that $\bar{f_i} = g_i$, then

$$\langle p \rangle = \prod_{i=1}^{r} \mathfrak{p}_i^{e_i}$$

where

$$\mathfrak{p}_i = \langle p, f_i(\theta) \rangle \text{ and } N(\mathfrak{p}_i) = p^{\deg f_i}.$$

Roughly speaking, the factorisation of $\langle p \rangle$ looks like the factorisation of f mod p.

Proof. Write $A = \mathbb{Z}[\theta]$ and $\mathbb{F}_p = \mathbb{Z}/\langle p \rangle$. Write $\mathfrak{p}_i = \langle p, f_i(\theta) \rangle$ and define

$$\psi : \mathbb{Z}[X]/\langle f(X), p, f_i(X) \rangle \to A/\mathfrak{p}_i A$$

induced by $\psi(X) = \theta$. It is clearly a ring homomorphism and surjective. If $\psi(h(X)) = 0$ in the image then $h(\theta) \in \mathfrak{p}_i A$. That means $h(\theta) = pu(\theta) + f_i(\theta)v(\theta)$ where $u, v \in \mathbb{Z}[\theta]$. So θ is a root of $h(X) - pu(X) - f_i(X)v(X)$ and since f is the minimal polynomial of θ we conclude that f divides $h(X) - pu(X) - f_i(X)v(X)$. This shows that $h(X) \in \langle f(X), p, f_i(X) \rangle$ and so ψ is an isomorphism.

We also have

$$\mathbb{Z}[X]/\langle f(X), p, f_i(X)\rangle \cong \mathbb{F}_p[X]/\langle \bar{f}(X), g_i(X)\rangle \cong \mathbb{F}_p[X]/\langle g_i(X)\rangle$$

and so

$$\mathbb{F}_p[X]/\langle g_i(X)\rangle \cong A/\mathfrak{p}_i A.$$

The natural map

$$\phi : A/\mathfrak{p}_i A \to \mathcal{O}_K/\mathfrak{p}_i, \quad x + \mathfrak{p}_i A \mapsto x + \mathfrak{p}_i$$

is well-defined because $\mathfrak{p}_i \mathcal{O}_K \supset \mathfrak{p}_i A$.

Let $N = [\mathcal{O}_K : A]$. Since $p \nmid N$ there exists M such that $NM \equiv 1 \bmod p$. If $x \in \mathcal{O}_K$, then $Nx \in A$ and so $MNx \in A$. But $MNx \equiv x \bmod p$ and since $\mathfrak{p}_i | \langle p\rangle$, so $MNx \equiv x \bmod \mathfrak{p}_i$. Therefore,

$$\phi(MNx + \mathfrak{p}_i A) = MNx + \mathfrak{p}_i = x + \mathfrak{p}_i$$

and so ϕ is surjective. Since $\mathfrak{p}_i \supset \mathfrak{p}_i A$ and so the map is injective. Therefore ϕ is an isomorphism and so we conclude

$$\mathbb{F}_p[X]\langle g_i(X)\rangle \cong A/\mathfrak{p}_i A \cong \mathcal{O}_K/\mathfrak{p}_i.$$

Since $g_i(X)$ is irreducible so $\mathbb{F}_p[X]/\langle g_i(X)\rangle$ is a field and so $\mathfrak{p}_i$ is maximal (prime).

For $i \neq j$, we know g_i, g_j are coprime and so we have $\lambda(X), \mu(X)$ such that

$$\lambda(X) f_i(X) + \mu(X) f_j(X) \equiv 1 \bmod p.$$

This shows that $1 \in \mathfrak{p}_i + \mathfrak{p}_j$ and so $\mathfrak{p}_i + \mathfrak{p}_j = \mathcal{O}_K$. In particular, $\mathfrak{p}_i \neq \mathfrak{p}_j$ for all $i \neq j$.

Finally,

$$\prod_i P_i^{e_i} = \prod_i \langle p, f_i(\theta)\rangle^{e_i} \subset \langle p\rangle + \langle \prod_i f_i(\theta)^{e_i}\rangle = \langle p\rangle$$

because $\prod_i f_i(\theta)^{e_i} = \bar{f}(\theta) \equiv 0 \bmod p$. Since $\mathbb{F}_p[X]/\langle g_i(X)\rangle \cong \mathcal{O}_K/\mathfrak{p}_i$, we conclude that $N(\mathfrak{p}_i) = p^{\deg g_i}$. Then

$$N(\prod_i P_i^{e_i}) = \prod_i (p^{\deg g_i})^{e_i} = p^{\sum_i \deg g_i e_i} = p^n = N(\langle p\rangle)$$

and so

$$\prod_i P_i^{e_i} = \langle p\rangle.$$

The residue degree of $\mathfrak{p}_i$ is $\deg g_i = \deg f_i$. □

Corollary 4.21. *Let $K = \mathbb{Q}(\theta)$ be an algebraic number field where $\theta \in \mathcal{O}_K$. Let f be the minimal polynomial of θ. If f mod p has distinct roots in $\mathbb{F}_p$ (i.e. $\bar{f}$ is separable) then $[\mathcal{O}_K : \mathbb{Z}[\theta]]$ is coprime to p and so Dedekind's criterion applies.*

Proof. Let $\theta = \theta_1, \dots, \theta_n$ be the roots of f and let $\bar{f}$ be f mod p. By assumption $\bar{\theta}_i$ are distinct in $\mathbb{F}_p$ and so

$$p \nmid \prod_{i<j} (\theta_i - \theta_j) = \operatorname{disc}(f).$$

Let $\{x_1, \dots, x_n\}$ be an integral basis of K and so there exist a_{ij} such that

$$\alpha^{i-1} = \sum_{j=1}^{n} a_{ij} x_j$$

for each $i = 1, 2, \dots, n$. Let A be the matrix with entries a_{ij} and so $\det A = [\mathcal{O}_K : \mathbb{Z}[\theta]]$. Let $\sigma_1, \dots, \sigma_n$ be the embeddings. Therefore,

$$\prod_{i<j} (\theta_i - \theta_j) = \det \begin{pmatrix} 1 & \theta_1 & \dots & \theta_1^{n-1} \\ 1 & \theta_2 & \dots & \theta_1^{n-1} \\ \vdots & \vdots & \vdots & \vdots \\ 1 & \theta_n & \dots & \theta_n^{n-1} \end{pmatrix} = \det M \det B = \det(MB)$$

where $B_{ij} = \sigma_j(x_i)$. So $p \nmid \det(MB)$ and so $p \nmid \det M$. □

Example 4.22. *Let $K = \mathbb{Q}(\sqrt{-5})$ and $\mathcal{O}_K = \mathbb{Z}[\sqrt{-5}]$. The minimal polynomial of $\sqrt{-5}$ is $f = x^2+5$ and so*

$$f \equiv (x+1)^2 \ mod\ 2, \quad f \equiv (x+1)(x-1) \ mod\ 3.$$

Therefore,

$$\langle 2 \rangle = \langle 2, \sqrt{-5}+1 \rangle^2, \quad \langle 3 \rangle = \langle 3, 1+\sqrt{-5} \rangle \langle 3, 1-\sqrt{-5} \rangle.$$

This recovers the example we have seen in Example 3.16.

4.5 Exercises

1. Let $I \subset \mathcal{O}_K$ be an ideal. Show that if $N(I)$ is a prime number then I is a prime ideal.

2. Let K be an algebraic number field. Let $a \in \mathcal{O}_K$ and $\mathfrak{p}$ a prime ideal such that $\mathfrak{p} \nmid \langle a \rangle$. Show that
$$a^{N(\mathfrak{p})-1} \equiv 1 \text{ mod } \mathfrak{p}.$$

3. Let $I \subset \mathcal{O}_K$ be an ideal and let
$$\phi(I) = |(\mathcal{O}_K/I)^\times|.$$
Show that
$$\phi(I) = N(I) \prod_{\mathfrak{p}|I} (1 - \frac{1}{N(\mathfrak{p})}).$$

4. Let $I \subset \mathcal{O}_K$ and m the smallest positive integer in I. Prove that m and $N(I)$ have the same prime divisors.

5. Let $L/K/\mathbb{Q}$ be extensions of number fields.

   (i) Show that if p is ramified in K, then p is ramified in L.

   (ii) If $\mathfrak{p} \subset \mathcal{O}_K$ is a prime ideal then $\mathfrak{p}\mathcal{O}_K \neq \mathcal{O}_L$. Hence show that if I, J are ideals in $\mathcal{O}_K$ with $I\mathcal{O}_L = J\mathcal{O}_L$, then $I = J$.

   (iii) Show that if p is totally ramified in L then it is totally ramified in K.

6. Let $K = \mathbb{Q}(\sqrt{d})$. Show that if $\mathcal{O}_K$ is an Euclidean domain, then it contains a principal ideal of norm 2 or 3.

7. Let $K/\mathbb{Q}$ be a finite Galois extension and p a prime number in $\mathbb{Q}$. Let
$$\langle p \rangle = \prod_{i=1}^{k} \mathfrak{p}_i^{e_i}.$$
Show that $e_1 = e_2 = \dots = e_k$. Let $f_1, \dots, f_k$ be the residue degrees of $\mathfrak{p}_1, \dots, \mathfrak{p}_k$ respectively. Show that $f_1 = \dots = f_k$.

8. We are going to compute the ring of integers of $\mathbb{Q}(\zeta_p)$. Compute $[K:\mathbb{Q}]$.

   (i) By considering the traces $T_{K/\mathbb{Q}}(\alpha\zeta_p^j)$, show that $\mathbb{Z}[\zeta_p] \subset \mathcal{O}_K \subset \frac{1}{p}\mathbb{Z}[\zeta_p]$.

   (ii) Show that $(1-\zeta_p^r)/(1-\zeta_p^s)$ is a unit for all $r, s \in \mathbb{Z}$ coprime to p. Let $\pi = 1 - \zeta_p$. Show that $\pi^{p-1} = up$ where u is a unit.

   (iii) Compute $N_{K/\mathbb{Q}}(\pi)$. Show that the natural map $\mathbb{Z} \to \mathcal{O}_K/\langle\pi\rangle$ is surjective. Hence deduce that for any $\alpha \in \mathcal{O}_K$ and $m \geq 1$ there exist $a_0, \ldots, a_{n-1} \in \mathbb{Z}$ such that

   $$\alpha \equiv a_0 + a_1\pi + \cdots + a_{m-1}\pi^{m-1} \bmod \pi^m\mathcal{O}_K.$$

   (iv) Show that $\mathcal{O}_K = \mathbb{Z}[\pi] = \mathbb{Z}[\zeta_p]$.

9. Let $K = \mathbb{Q}(\theta)$ such that $\mathcal{O}_K = \mathbb{Z}[\theta]$. Let f be the minimal polynomial of θ. Suppose $\theta_1 = \theta, \ldots, \theta_n$ are the conjugates of θ. Show that

   $$\frac{1}{f(X)} = \sum_{i=1}^{n} \frac{1}{f'(\theta_i)(X-\theta_i)}.$$

   Deduce that $T_{K/\mathbb{Q}}\left(\frac{\theta^r}{f'(\theta)}\right) = 0$ if $0 \leq r < n-1$ and 1 if $r = n-1$. Hence, show that

   $$\mathcal{D}_{K/\mathbb{Q}} = \langle f'(\theta)\rangle.$$

   This shows that when we have a power basis then there exists an element whose absolute norm is $\mathcal{D}_K$.

10. Let $\mathfrak{p}$ be a prime ideal in $\mathcal{O}_K$ with ramification index e. Show that if $x \in \langle p\rangle/\mathfrak{p}^{e-1}$, then $p|T_{K/\mathbb{Q}}(x)$. Hence show that $\mathfrak{p}^{e-1}|\mathcal{D}_{K/\mathbb{Q}}$. This shows that p is ramified if and only if $\mathfrak{p}|\mathcal{D}_{K/\mathbb{Q}}$ for some prime ideal $\mathfrak{p}$ above p.

11. We give an example of K such that $\mathcal{O}_K$ has no power basis. Let $K = \mathbb{Q}(\alpha)$ where α is a root of $X^3 + X^2 - 2X + 8$. This polynomial is irreducible and has discriminant -4×503.

    (i) Show that $\beta = 4/\alpha \in \mathcal{O}_K$ and $\beta \notin \mathbb{Z}[\alpha]$. Deduce that $\mathcal{O}_K = \mathbb{Z}[\alpha, \beta]$.

    (ii) Show that there is an isomorphism of rings $\mathcal{O}_K/\langle 2\rangle \cong \mathbb{F}_2 \times \mathbb{F}_2 \times \mathbb{F}_2$. Deduce that 2 splits completely in K.

    (iii) Use Dedekind's criterion to show that $\mathcal{O}_K \neq \mathbb{Z}[\theta]$ for any θ.

5 The ideal class group and Mordell's equation

It is clear that the set of non-zero fractional ideal $I(K)$ in an algebraic number field forms an abelian group under multiplication, with identity $\mathcal{O}_K$. The set of non-zero principal (fractional) ideal $P(K)$ is a subgroup of $I(K)$.

Definition 5.1. *The ideal class group of a number field K, written $C(K)$, is the quotient $I(K)/P(K)$. The size of $C(K)$ is called the class number, written $h(K)$. We will show that the class number is finite. Note that $h(K) = 1$ if and only if $\mathcal{O}_K$ is a PID. If I is a non-zero fractional ideal, then we write $[I]$ to be the ideal class in the class group.*

5.1 Minkowski's convex body theorem

Definition 5.2. *Let R be a ring and V be an R-module. A subset $H \subset V$ is discrete if for every compact subset $X \subset V$, $H \cap X$ is finite.*

Lemma 5.3. *Let $V \subset \mathbb{R}^n$ be a $\mathbb{Z}$-module and $H \subset V$ a submodule. The followings are equivalent:*

(i) H is discrete.

(ii) H is finitely generated as $\mathbb{Z}$-module and there exists a generating set which is linearly independent over $\mathbb{R}$

(iii) H is finitely generated as $\mathbb{Z}$-module and every generating set is linearly independent over $\mathbb{R}$.

Proof. (i) ⇒ (ii): Let r be the maximal number such that there exist $e_1, \ldots, e_r \in H$ which are linearly independent over $\mathbb{R}$. Clearly, $r \leq n$. Let

$$P = \{\sum_{i=1}^{r} a_i e_i : a_i \in [0, 1)\}.$$

Since the closure $\bar{P}$ is closed and bounded so it is compact and so $P \cap H$ is finite because H is discrete. For each $x \in H$, $x = \sum_{i=1}^{r} b_i e_i$ where $b_i \in \mathbb{R}$. Write $b_i = [b_i] + a_i e_i$ where $a_i \in [0, 1)$ and so we conclude that H is generated by $P \cap H$ and $e_1, \ldots, e_n$.

For each integer j, define

$$x_j = jx - \sum_{i=1}^{r} [jb_i] e_i = \sum_{i=1}^{r} (jb_i - [jb_i]) e_i \in P.$$

Since $jx, \sum_{i=1}^{r} [jb_i] e_i \in H$, so $x_j \in H \cap P$. But $P \cap H$ is finite, so we have $j \neq k$ such that $x_j = x_k$, and so

$$(j - k) b_i = [jb_i] - [kb_i]$$

because $e_1, \ldots, e_i$ are linearly independent. So

$$b_i = \frac{[jb_i] - [kb_i]}{j - k} \in \mathbb{Q}$$

and b_i does not depend on x. So we can write $b_i = \frac{B_i}{N}$ where $B_i \in \mathbb{Z}$ and so

$$x = \sum_{i=1}^{r} b_i e_i = \sum_{i=1}^{r} \frac{B_i e_i}{N}.$$

Therefore, H is a $\mathbb{Z}$-module generated by $\{\frac{e_1}{N}, \ldots, \frac{e_r}{N}\}$.

(ii) ⇒ (iii): Let $\{e_1, \ldots, e_r\}$ be a generating set of H which is linearly independent over $\mathbb{R}$. For any $\mathbb{Z}$-basis $\{f_1, \ldots, f_r\}$ of H, there exist $a_{ij} \in \mathbb{Z}$ such that

$$f_i = \sum_{j=1}^{r} a_{ij} e_j$$

The matrix A with entries $A_{ij} = a_{ij}$ is invertible. If $\sum_{i=1}^{r} b_i f_i = 0$, then

$$\sum_{i=1}^{r} b_i \sum_{j=1}^{r} a_{ij} e_j = 0.$$

Since $e_1, \ldots, e_r$ are linearly independent over $\mathbb{R}$, so $\sum_{j=1}^{r} b_i a_{ij} = 0$ for each i. Since A is invertible, $b_i = 0$ for each i and so $\{f_1, \ldots, f_r\}$ is also linearly independent over $\mathbb{R}$.

(iii) ⇒ (i): Take any $\mathbb{Z}$-basis $\{e_1, \ldots, e_r\}$ of H which is linearly independent over $\mathbb{R}$. Extend this to an $\mathbb{R}$-basis $\{e_1, \ldots, e_r, e_{r+1}, \ldots, e_n\}$ of $\mathbb{R}^n$. Let $\{f_1, \ldots, f_n\}$ be the standard orthogonal basis for $\mathbb{R}^n$. Then there exists an invertible linear map L which takes $\{e_1, \ldots, e_n\}$ to $\{f_1, \ldots, f_n\}$. It is clear that L and L^{-1} are both continuous.

So for any $X \subset V$ is a compact subset, $L(X)$ is also compact. So there exists a ball $B_R(0) \subset V$ with radius R centered at the origin such that

$$L(X) \subset B.$$

By linearity,

$$L(H) \subset \mathbb{Z}f_1 \oplus \mathbb{Z}f_2 \cdots \oplus \mathbb{Z}f_n.$$

Since there are only finitely many tuples $(m_1, \ldots, m_n)$ with $m_i \in \mathbb{Z}$ such that $\sum_{i=1}^{n} m_i^2 \leq R^2$, so $L(H) \cap B_R(0)$ is finite. Since L is invertible, we have

$$H \cap L^{-1}(B_R(0)) = L^{-1}(L(H) \cap B_R(0))$$

and so $H \cap L^{-1}(B_R(0))$ is finite. But $X \subset L^{-1}(B)$ and so $H \cap X$ is finite. This shows that H is discrete. □

Definition 5.4. *Let V be a $\mathbb{Z}$-module in $\mathbb{R}^n$. A lattice is an discrete additive subgroup H of V (i.e. by the previous lemma, it is a $\mathbb{Z}$-submodule) such that $\text{rank}_{\mathbb{R}} H = n$ (so it is generated by n $\mathbb{R}$-linearly independent elements).*

Lemma 5.5. *Let H be a lattice in $\mathbb{R}^n$ with a $\mathbb{Z}$-basis $\{e_1, \ldots, e_n\}$. Suppose $\{f_1, \ldots, f_n\}$ is another $\mathbb{Z}$-basis for H, and*

$$P_e = \{\sum_{i=1}^{n} a_i e_i : a_i \in [0, 1)\}, \quad P_f = \{\sum_{i=1}^{n} a_i f_i : a_i \in [0, 1)\},$$

then the volume of P_e is equal to the volume of P_f.

Proof. There exists an invertible matrix A with integer entries such that A sends $\{e_1, \ldots, e_n\}$ to $\{f_1, \ldots, f_n\}$. So $\det A = \pm 1$. Therefore,

$$V(P_f) = |\det A| V(P_e) = V(P_e).$$

□

This allows one to define the following.

Definition 5.6. *Let H be a lattice in $\mathbb{R}^n$. The covolume of H, written $cov(H)$, is defined as the volume of P where*

$$P = \{\sum_{i=1}^{n} a_i e_i : a_i \in [0, 1)]\}$$

and $\{e_1, \dots, e_n\}$ is a $\mathbb{Z}$-basis for H.

Definition 5.7. *A set $S \in \mathbb{R}^n$ is convex if for all $x, y \in S$, and $\lambda \in [0, 1]$, $\lambda x + (1 - \lambda)y \in S$. S is called a convex body if S is compact and convex. S is called symmetric if $-\alpha \in S$ for any $\alpha \in S$.*

Lemma 5.8. *Let H be a lattice in $\mathbb{R}^n$ with a $\mathbb{Z}$-basis $\{e_1, \dots, e_n\}$ and*

$$P = \{\sum_{i=1}^{n} a_i e_i : a_i \in [0, 1)\}.$$

Then $\mathbb{R}^n = \cup_{h \in H} P_h$ where for each h,

$$P_h = \{h + p : p \in P\}.$$

Moreover, the union is disjoint.

Proof. Since H is a lattice so $e_1, \dots, e_n$ are $\mathbb{R}$-linearly independent and so they form a basis for $\mathbb{R}^n$. Let $r \in \mathbb{R}^n$ then $r = \sum_i b_i e_i$ and let $a_i = b_i - [b_i]$. Since $\sum_i [b_i] e_i \in H$ we conclude that $r \in P_h$ for some $h \in H$. Therefore, $\mathbb{R}^n = \cap_{h \in H} P_h$.

Suppose $P_h \cap P_{h'} \neq$ then we have a_i, a'_i such that

$$\sum_i a_i e_i + h = \sum_i a'_i e_i + h'.$$

Writing $c_i = a'_i - a_i$, we have

$$h - h' = \sum_i (a'_i - a_i) e_i = \sum_i c_i e_i \in H.$$

This shows that c_i is an integer for each i but $c_i \in (-1, 1)$, so $c_i = 0$ for all i. So $a'_i = a_i$ for all i and so $h = h'$. This shows that $P_h = P_{h'}$ or $P_h \cap P_{h'} = \varnothing$. □

Theorem 5.9 (Minkowskis's convex body theorem). *Suppose $H \subset \mathbb{R}^n$ is a lattice and $S \subset V$ is measurable (S has a volume), and the volume of S is denoted by $m(S)$.*

(i) Suppose $m(s) > cov(H)$, then there exist $x, y \in S$ such that $0 \neq x - y \in H$.

(ii) If $m(S) > 2^n cov(H)$ and S is convex and symmetric, then there exists a non-zero element $x \in S \cap H$.

(iii) If $m(S) \geq 2^n cov(H)$ and S is a convex body and symmetric, then there exists a non-zero element $x \in S \cap H$.

Proof. (i) Let $\{e_1, \dots, e_n\}$ be a $\mathbb{Z}$-basis for H and

$$P = \{\sum_{i=1}^{n} a_i e_i : a_i \in [0, 1)\}.$$

For each $k \in H$, we have

$$m(S \cap P_k) = m(S_{-k} \cap P) \text{ where } S_k = \{k + s : s \in S\}$$

because translation fixes the volume. Since $\mathbb{R}^n = \cup_{k\in H} P_k$, so $S = \cup_{k\in H}(S \cap P_k)$, which is a disjoint union, and so

$$m(S) = \sum_{k\in H} m(S \cap P_k) = \sum_{k\in H} m(S_{-k} \cap P).$$

Suppose $(S_{-k} \cap P) \cap (S_{-h} \cap h) = \varnothing$ for all $h \neq k$ then

$$m(S) = \sum_{k\in H} m(S_{-k} \cap P) \leq m(P) = \mathrm{cov}(H)$$

which is a contradiction. Therefore, we have $h \neq k \in H$ such that

$$(S_{-k} \cap P) \cap (S_{-h} \cap P) \neq \varnothing.$$

In particular, $S_{-k} \cap S_{-h} \neq \varnothing$. Therefore, we have $x, y \in S$ such that $x - h = y - k$ and so $x - y = h - k \neq 0$.

(ii) Let $S' = \frac{1}{2}S = \{\frac{1}{2}s : s \in S\}$. Then $m(S') = \frac{1}{2^n}m(S)$ and so $m(S') > \mathrm{cov}(H)$. By (i) there exist $y \neq z \in S'$ such that $y - z \in H$. So $2y, 2z, -2z \in S$ because S is symmetric. Let $x = y - z$ and so

$$x = \frac{1}{2}2y + \frac{1}{2}(-2z) \in S$$

because S is convex. So $0 \neq x \in S \cap H$.

(iii) For any integer m, define

$$S_m = \left(1 + \frac{1}{m}\right) S.$$

It is clear that for all m, S_m is convex and symmetric, and

$$S \subset S_m \subset S_{m-1} \subset S_1.$$

So $m(S_m) > 2^n \mathrm{cov}(H)$ for all m. By (ii), we have a sequence of non-zero elements

$$x_m \in S_m \cap H \subset S_1 \cap H.$$

Since S_1 is compact and H is a lattice, so $S_1 \cap H$ is finite and so there exists $x \in S_1 \cap H$ such that $x_m = x$ for infinitely many m. Let m_j be the subsequence such that $x = x_{m_j} \in S_{m_j}$ and so

$$x \in \cap_j S_{m_j} = S$$

because S is compact. The fact $x \in H$ is clear from above. □

5.2 The ideal class group

We shall prove that the class number for any algebraic number field is finite.

Definition 5.10. *Let K be an algebraic number field and $[K : \mathbb{Q}] = n = r + 2s$. Define*

$$\sigma = (\sigma_1, \ldots, \sigma_{r+s}) : K \to \mathbb{C}$$

such that we only take one of the embeddings for each pair of complex embeddings. We can think of this map as

$$\sigma = (\sigma_1, \ldots, \sigma_r, \Re\sigma_{r+1}, \Im\sigma_{r+1}, \ldots) : K \to \mathbb{R}^{r+2s}.$$

Lemma 5.11. *With the same notation in the previous definition, we conclude that $\sigma(\mathcal{O}_K)$ is a lattice of $\mathbb{R}^n$ with covolume $2^{-s}\sqrt{|\mathcal{D}_K|}$. Moreover, if $I \subset \mathcal{O}_K$ is an ideal, then $\sigma(I)$ is a lattice of $\mathbb{R}^n$ with covolume $2^{-s}\sqrt{|\mathcal{D}_K|}N(I)$.*

Proof. Let $\{e_1, \ldots, e_n\}$ be an integral basis of K. Let X be the $n \times n$ matrix such that the k^{th} row is $\sigma(e_k)$. Let z^* be the complex conjugate of any complex number z. Then $\sigma_j(e_k) = a_{jk} + ib_{jk}$ and $\sigma_j(e_k) = \sigma_j(e_k) - 2ib_{jk}$ where $a_{jk} = \Re(\sigma_j(e_k))$ and $b_{jk} = \Im(\sigma_j(e_k))$. So by column operations, we conclude that

$$\det X = \frac{1}{(2i)^s} \det(\sigma_j(e_k))$$

and so

$$(\det X)^2 = \frac{1}{(2i)^{2s}} \mathcal{D}_K \neq 0.$$

So the vectors $\sigma(e_1), \ldots, \sigma(e_n)$ are linearly independent and so it is a $\mathbb{Z}$-basis for $\sigma(\mathcal{O}_K)$. Therefore, it is a lattice (of rank n) because $\mathcal{O}_K$ is a $\mathbb{Z}$-module. By definition of determinant in real space, we conclude that

$$\operatorname{cov}(\sigma(\mathcal{O}_K)) = |\det X| = 2^{-s}\sqrt{|\mathcal{D}_K|}.$$

Let $I \subset \mathcal{O}_K$ be an ideal. Then repeat the above argument with a $\mathbb{Z}$-basis for I we obtain the corresponding result for I. □

Definition 5.12. *Let K be an algebraic number field and $[K : \mathbb{Q}] = n = r + 2s$. The Minkowski's bound is defined as*

$$c_K = \left(\frac{4}{\pi}\right)^s \frac{n!}{n^n} \sqrt{|\mathcal{D}_K|}.$$

Theorem 5.13. *Let K be an algebraic number field and $I \subset \mathcal{O}_K$ an ideal. Then there exists a non-zero element $x \in I$ such that*

$$|N_{K/\mathbb{Q}}(x)| \leq N(I)c_K.$$

Proof. For any positive real number t, define the set

$$B(r,s)_t = B_t = \{(y_1, \ldots, y_r, z_1, \ldots, z_s) \in \mathbb{R}^r \times \mathbb{C}^s : \sum_{i=1}^r |y_i| + 2\sum_{j=1}^s |z_j| \leq t\}.$$

It is clear that $B(r,s)_t$ is symmetric, convex (by triangular inequality) and compact. The volume of $B(r,s)_t$ is

$$m(B(r,s)_t) = 2^r \left(\frac{\pi}{2}\right)^s \frac{t^n}{n!}.$$

You can check this by double induction on r, s and using polar coordinate.

Now I is a fixed ideal and so we take some t such that

$$m(B(r,s)_t) = 2^n \operatorname{cov}(I)$$

which gives

$$t^n = \left(\frac{4}{\pi}\right)^s n! \sqrt{|\mathcal{D}_K|} N(I)$$

by the previous lemma. By Minkowski's convex body theorem there is a non-zero element $y \in B(r,s)_t \cap \sigma(I)$. Let $\sigma(x) = y = (y_1, \ldots, y_r, z_1, \ldots, z_s) \in B(r,s)_t$. Then

$$|N_{K/\mathbb{Q}}(x)| = \left|\prod_{i=1}^r y_i\right| \left|\prod_{j=1}^s z_j z_j^*\right| = \prod_{i=1}^r |y_i| \prod_{j=1}^s |z_j|^2.$$

By AM-GM inequality, we have

$$|N_{K/\mathbb{Q}}(x)|^{\frac{1}{n}} \leq \frac{1}{n}\left(\sum_{i=1}^r |y_i| + 2\sum_{j=1}^s |z_j|\right) \leq \frac{t}{n}$$

and so

$$|N_{K/\mathbb{Q}}(x)| \leq \left(\frac{t}{n}\right)^n = \left(\frac{4}{\pi}\right)^s \frac{n!}{n^n}\sqrt{|\mathcal{D}_K|}N(I).$$

□

Corollary 5.14. *Every ideal class in $\mathcal{O}_K$ has a representative I such that $N(I) \leq c_K$.*

Proof. Let M be any ideal in the given class. Take $\alpha \in K$ such that αM contains $\mathcal{O}_K$. For example, $\alpha = y^{-1}$ for some $y \in M$. So we can assume that $M \supset \mathcal{O}_K$ because $[\alpha M] = [M]$, and so $M^{-1} \subset \mathcal{O}_K$. The previous theorem shows there is a non-zero element $x \in M^{-1}$ such that

$$|N_{K/\mathbb{Q}}(x)| < N(M^{-1})c_K$$

and so $N(xM) \leq c_K$ where $[xM] = [M]$. □

Lemma 5.15. *Let K be an algebraic number field and n a positive integer. Then there exist only finitely many ideals I such that $N(I) = n$.*

Proof. Since $N(I) \in I$ for any ideal I, we have $I|\langle N(I)\rangle$ and so if $N(I) = n$, then $I|\langle n\rangle$. Write $\langle n\rangle = \prod_i \mathfrak{p}_i^{a_i}$ and so

$$I = \prod_i \mathfrak{p}_i^{b_i}$$

for some $0 \leq b_i \leq a_i$. Therefore, we have finitely many possible choices for I. □

Corollary 5.16. *The class number of any algebraic number field is finite.*

Proof. By Corollary 5.14, each ideal class contains a representative with norm less than c_K. The previous lemma shows that for each integer $n \leq c_K$, there are only finitely many ideals with norm equal to n, say $I_{n_1}, \dots, I_{n_m}$. So the class group, as a set, is contained in the finite set

$$\{[I_{n_j}] : n \leq c_K, j \leq n_m\}.$$

□

Remark 5.17. *By unique factorisation of ideals and the corollary above, we only need to compute the factorisation of $\langle p\rangle$ in $\mathcal{O}_K$ for p prime numbers $\leq c_K$. We will give some examples later.*

5.3 Application of Minkowski's theorem

We give some applications of Minkowski's theorem.

Lemma 5.18. *Let $n = [K : \mathbb{Q}]$. If $n \geq 2$, then $|\mathcal{D}_K| \geq \frac{\pi}{3}\left(\frac{3\pi}{4}\right)^{n-1} > 1$. In particular, a number field K has discriminant 1 if and only if $K = \mathbb{Q}$.*

Proof. By Corollary 5.14, take an ideal I with $N(I) \leq c_K$. Since $N(I), c_K \geq 1$, we have

$$\sqrt{|\mathcal{D}_K|} \geq \left(\frac{\pi}{4}\right)^s \frac{n^n}{n!}.$$

Since $2s \leq n$ and $\frac{\pi}{4} \leq 1$, so

$$|\mathcal{D}_K| \geq \left(\frac{\pi}{4}\right)^n \frac{n^{2n}}{(n!)^2}.$$

For each $n \geq 2$, define $a_n = \left(\frac{\pi}{4}\right)^n \frac{n^{2n}}{(n!)^2}$. It is clear that $a_2 = \frac{\pi^2}{4} > 1$. For $n > 2$, we have

$$\frac{a_{n+1}}{a_n} = \frac{\pi}{4}\left(1 + \frac{1}{n}\right)^{2n} > \frac{\pi}{4}\left(1 + 2n\frac{1}{n}\right) = \frac{3\pi}{4}.$$

This gives the result.

□

Corollary 5.19. *Let $n = [K : \mathbb{Q}] \geq 2$. Then there exists a prime which is ramified in K.*

Proof. The previous lemma shows $|\mathcal{D}_K|$ is an integer > 2 and so it is divisible by some prime. Recall that a prime p is ramified if and only if $p|\mathcal{D}_K$. □

Theorem 5.20 (Hermite). *For each $C > 0$, there are only finitely many algebraic number fields K such that $|\mathcal{D}_K| < C$.*

Proof. We will show that the number of K with $|\mathcal{D}_K| = M$ is finite for each integer $M < C$. By Lemma 5.18,

$$M = |\mathcal{D}_K| > \frac{\pi}{3}\left(\frac{3\pi}{4}\right)^{n-1}$$

and so n is bounded. Write $n = r+2s$ and for each fixed n there are only finitely many pairs (r, s) such that $n = r + 2s$. So it suffices to show that there are only finitely many K with $[K : \mathbb{Q}] = n = r + 2s$ and $|\mathcal{D}_K| = M$ where r, s are fixed.

Fix r and s. If $r \geq 1$, let

$$B_r = \{(y_1, \dots, y_r, z_1, \dots, z_s) \in \mathbb{R}^r \times \mathbb{C}^s : |y_1| \leq 2^{n-1}\left(\frac{\pi}{2}\right)^{-s}\sqrt{|\mathcal{D}_K|}, |y_i|, |z_j| \leq \frac{1}{2} \text{ for all } i \neq 1, j\}.$$

Also let

$$B_0 = \{(z_1, \dots, z_s) : \Re|z_1| \leq 2^{n-2}, \Im|z_1| \leq \frac{\pi}{4}\left(\frac{\pi}{2}\right)^{-s}\sqrt{|\mathcal{D}_K|}, |z_j| \leq \frac{1}{2} \text{ for all } j \neq 1\}.$$

It is clear that B_r and B_0 are convex bodies. It is easy to find the volumes

$$m(B_r) = m(B_0) = 2^n 2^{-s}\sqrt{|\mathcal{D}_K|} = 2^n \mathrm{cov}(\sigma(\mathcal{O}_K)).$$

So by Minkowski's convex body theorem, there exists a non-zero element $x \in \mathcal{O}_K$ such that

$$\sigma(x) \in \sigma(\mathcal{O}_K) \cap B_r, r \geq 0.$$

We will show that $K = \mathbb{Q}(x)$.

If $r > 0$ then $|\sigma_j(x)| \leq \frac{1}{2}$ for all $j \neq 1$ and since $|N_{K/\mathbb{Q}}(x)|$ is a non-zero integer, we conclude that $|\sigma_1(x)| > 1$. So it is distinct from any other $\sigma_j(x)$ and so the minimal polynomial of x has degree n. So $K = \mathbb{Q}(x)$. If $r = 0$, then $|\sigma_1(x)| > 1$ whence $|\sigma_j(x)| \leq \frac{1}{2}$, and so again we have $K = \mathbb{Q}(x)$.

Each $|\sigma_i(x)|$ is bounded because $\sigma(x) \in B_r$. The coefficients of the minimal polynomial of x are elementary symmetric functions in $|\sigma_i(x)|$ and so the coefficients are bounded. So there are only finitely many such x, and hence finitely many $K = \mathbb{Q}(x)$. □

5.4 Computation of the ideal class group

We now give illustrate an algorithm and give some examples for the computation of class groups.

(i) Determine $r + 2s = n = [K : \mathbb{Q}]$.

(ii) Compute the Minkowski's bound c_K.

(iii) For each prime number $p \leq c_K$, find the factorisation of $\langle p \rangle$. List the prime ideals above these prime numbers.

(iv) The class group is generated by the prime ideals in (iii). Find the relations between these ideals in the class group and hence determine the group structure.

Example 5.21. *$K = \mathbb{Q}(\sqrt{-19})$. We have $n = 2, r = 0, s = 1$ and $\mathcal{D}_K = -19$. Then*

$$c_K = \left(\frac{4}{\pi}\right)\frac{2!}{2^2}\sqrt{19} = \frac{2}{\pi}\sqrt{19} < 4.$$

To apply Dedekind criterion, we rewrite $K = \mathbb{Q}(\alpha)$ where $\alpha = \frac{1}{2}(1 + \sqrt{-19})$ and so $\mathcal{O}_K = \mathbb{Z}[\alpha]$. The minimal polynomial of α is $x^2 - x + 5$. Then $\langle 2\rangle, \langle 3\rangle$ are both principal ideals and so the class group is trivial.

Example 5.22. *$K = \mathbb{Q}(\sqrt{-14})$. We have $n = 2, r = 0, s = 1$ and $\mathcal{D}_K = -56$. Then*

$$c_K = \left(\frac{4}{\pi}\right)\frac{2!}{2^2}\sqrt{56} < 5.$$

By Dedekind's criterion, we have

$$\langle 2\rangle = \mathfrak{p}^2 = \langle 2, \sqrt{-14}\rangle^2, \quad \langle 3\rangle = \mathfrak{q}\bar{\mathfrak{q}} = \langle 3, \sqrt{-14} - 1\rangle\langle 3, \sqrt{-14} + 1\rangle.$$

The prime ideal $\langle 2, \sqrt{-14}\rangle$ is NOT principal because otherwise there exists an element of norm 2. So we have integers a, b such that $a^2 + 14b^2 = 2$. Then $b = 0$ otherwise $a^2 + 14b^2 \geq 14$ and so $a^2 = 2$ which is a contradiction. Similarly, both prime ideals above 3 are NOT principal.

To find the relations between these ideals, we consider a principal ideal of norm 2^a3^b for some integers a, b. The ideal $\langle 2 + \sqrt{-14}\rangle$ has norm 18 and so it must be one of the following

$$\mathfrak{p}\mathfrak{q}^2, \quad \mathfrak{p}\mathfrak{q}\bar{\mathfrak{q}}, \quad \mathfrak{p}\bar{\mathfrak{q}}^2.$$

But if it is the second case then $\langle 3\rangle\mathfrak{q}\bar{\mathfrak{q}}$ divides $\langle 2 + \sqrt{-14}\rangle$ and so $\frac{2+\sqrt{-14}}{3}$ is an element in $\mathcal{O}_K$. This is impossible. Also, $\langle 2 + \sqrt{-14}\rangle$ is contained in $\mathfrak{q}$ and so $\mathfrak{q}|\langle 2 + \sqrt{-14}\rangle$. So it must be $\mathfrak{p}\mathfrak{q}^2$. So in the class group, we now have

$$1 = [\mathfrak{p}]^2 = [\mathfrak{p}][\mathfrak{q}]^2$$

and so $[\mathfrak{p}] = [\mathfrak{q}]^2$. Also $[\bar{\mathfrak{q}}] = [\mathfrak{q}]^{-1}$ so the ideal class group is generated by $[\mathfrak{q}]$, which has order 4. So the class group is C_4.

Remark 5.23. *After we obtain the prime ideals above p where $p \leq c_K$, we usually try to find some principal ideals of norm of the form $p_1^{a_1}p_2^{a_2}\cdots$ to determine the relations between these ideals in the class group. The norm can usually be used to determine the factorisation of this principal ideals, together with the fact that $\mathfrak{p}|\langle\alpha\rangle$ if and only if $\alpha \in \mathfrak{p}$.*

We give a table (table 1) of some class groups of $\mathbb{Q}(\sqrt{d})$ for small values of d.

One can check these by using the method illustrated above. For the real quadratic fields, it probably takes some more effort to determine whether an ideal is principal. We will see some examples in the exercise.

5.5 Mordell's equation

One of the main reasons we study the ideal class group is to find integer solutions to Mordell's equation

$$y^2 = x^3 - d.$$

Lemma 5.24. *Let d be a square free integer and $d \neq 0, d \neq -1$. For any integer y, if $\langle y + \sqrt{-d}\rangle$ and $\langle y - \sqrt{-d}\rangle$ are NOT coprime, then the only common factors are the ideals $\mathfrak{p}|\langle 2\rangle$. In this case, we have $\frac{y+\sqrt{-d}}{2} \in \mathcal{O}_K$ where $K = \mathbb{Q}(\sqrt{-d})$.*

Table 1: $K = \mathbb{Q}(\sqrt{d})$,$|d| < 30$ square free.

d	$C(K)$	generators
10	C_2	$I = [\langle 2, \sqrt{10}\rangle]$
15	C_2	$I = [\langle 2, 1+\sqrt{15}\rangle]$
26	C_2	$I = [\langle 2, \sqrt{26}\rangle]$
30	C_2	$I = [\langle 2, \sqrt{30}\rangle]$
-5	C_2	$I = [\langle 2, 1+\sqrt{-15}\rangle]$
-6	C_2	$I = [\langle 2, \sqrt{-6}\rangle]$
-13	C_2	$I = [\langle 2, \sqrt{-10}\rangle]$
-14	C_4	$I = [\langle 3, 1+\sqrt{-14}\rangle]$
-15	C_2	$I = [\langle 2, \frac{1}{2}(3+\sqrt{-15})\rangle]$
-17	C_4	$I = [\langle 3, 1+\sqrt{-17}\rangle]$
-21	$C_2 \times C_2$	$I = [\langle 2, 1+\sqrt{-21}\rangle]$,$J = [\langle 3, \sqrt{-21}\rangle]$, $Cl(K) = \{I, J, IJ, 1\}$
-22	C_2	$I = \langle [2, \sqrt{-22}\rangle]$
-23	C_3	$I = [\langle 2, \frac{1}{2}(1+\sqrt{-23})\rangle]$
-26	C_6	$I = [\langle 5, 2+\sqrt{-26}\rangle]$
-29	C_6	$I = [\langle 3, 1+\sqrt{-29}\rangle]$
-30	$C_2 \times C_2$	$I = [\langle 2, \sqrt{-30}\rangle]$,$J = [\langle 3, \sqrt{-30}\rangle]$, $Cl(K) = \{I, J, IJ, 1\}$

Proof. Suppose $\mathfrak{p}$ is a prime ideal which divides both $\langle y + \sqrt{-d}\rangle$ and $\langle y - \sqrt{-d}\rangle$. Let $\bar{\mathfrak{p}}$ be the conjugate of $\mathfrak{p}$. Since $\mathfrak{p}$ is a prime ideal, so we have three possible cases for $\mathfrak{p}$: (i) $\mathfrak{p} = \langle p\rangle$ where p is a prime number which inerts (ii) $\mathfrak{p}^2 = \langle p\rangle$ where p is a prime number which is ramified (iii) $\mathfrak{p}\bar{\mathfrak{p}} = \langle p\rangle$ where p is a prime number which splits.

Since $\mathfrak{p}|\langle y + \sqrt{-d}\rangle$ and $\mathfrak{p}|\langle y - \sqrt{-d}\rangle$, so $\bar{\mathfrak{p}}|\langle y + \sqrt{-d}\rangle$. In case (i) $\mathfrak{p} = \langle p\rangle$ and so $p|y + \sqrt{-d}$ in $\mathcal{O}_K$ which is only possible if $p = 2$. In cases (ii) and (iii) $\langle p\rangle|\langle y + \sqrt{-d}\rangle$ which is again only possible when $p = 2$. Therefore, $p = 2$ and $\mathfrak{p}$ is a prime above 2. In particular, $\frac{y+\sqrt{-d}}{2} \in \mathcal{O}_K$. □

Corollary 5.25. *Let $d \neq 0, -1$ be a square free integer and $-d \not\equiv 1 \mod 4$, then $\langle y+\sqrt{-d}\rangle$, $\langle y-\sqrt{-d}\rangle$ are coprime.*

Proof. If $-d \not\equiv 1 \bmod 4$ then $\mathcal{O}_K = \mathbb{Z}[\sqrt{-d}]$ where $K = \mathbb{Q}(\sqrt{-d})$. □

Example 5.26. *We have seen that the class number of $K = \mathbb{Q}(\sqrt{-14})$ is 4. We consider the equation*

$$y^2 = x^3 - 14$$

which can be factorised

$$\langle y + \sqrt{-14}\rangle\langle y - \sqrt{-14}\rangle = \langle x\rangle^3.$$

The previous corollary shows that $\langle y+\sqrt{-14}\rangle$, $\langle y-\sqrt{-14}\rangle$ are coprime. The product of them is $\langle x\rangle^3$ and so by unique factorisation each of them must be I^3 for some ideal I. But

$$[I]^3 = [\langle y + \sqrt{-14}\rangle] = 1$$

and so $[I] = 1$ because the class number is coprime to 3. So

$$\langle y + \sqrt{-14}\rangle = \langle a + b\sqrt{-14}\rangle^3$$

for some integers a, b. We can assume $y + \sqrt{-14} = (a + b\sqrt{-14})^3$ because the only units are ± 1 and both of ± 1 are cubic powers. So

$$y + \sqrt{-14} = a^3 + 3a^2b\sqrt{-14} - 42ab^2 - 14b^3\sqrt{-14}.$$

Compare the coefficients of $\sqrt{-14}$ and we conclude that

$$1 = b(3a^2 - 14b^2).$$

So $b = \pm 1$. If $b = 1$ then $3a^2 = 5$ which is impossible. If $b = -1$ then $13 = 3a^2$ which is also impossible. So the equation has no integer solutions.

5.6 Exercises

1. Let $K = \mathbb{Q}(\sqrt{-d})$ where d is a positive square free integer. Show that

   (i) If d is composite and p is an odd prime divisor of d then $\langle p \rangle = \mathfrak{p}^2$ where $\mathfrak{p}$ is not principal.

   (ii) If $d \equiv 1, 2 \bmod 4$ then $\langle 2 \rangle = \mathfrak{p}^2$ where $\mathfrak{p}$ is not principal unless $d = 1$ or 2.

   (iii) If $d \equiv 7 \bmod 8$ then $\langle 2 \rangle = \mathfrak{p}\bar{\mathfrak{p}}$ where $\mathfrak{p}$ is not principal unless $d = 7$.

   Deduce that if K has class number 1 then either $d = 1, 2$ or 7 or d is a prime and $d \equiv 3 \bmod 8$.

2. Let m be a square free even integer and K be an algebraic number field such that the class number $h(K)$ is coprime to 3. Show that $y^2 + m = x^3$ has at most two integer solutions.

3. Compute the class number of $K = \mathbb{Q}(\sqrt{14})$.

4. Let $d_n = \min\{|\mathcal{D}_K| : [K : \mathbb{Q}] = n\}$. Show that $d_n \to \infty$ as $n \to \infty$. You may use stirling's formula
$$n! = \sqrt{2\pi n}\left(\frac{n}{e}\right)^n \exp\left(\frac{\theta}{12n}\right), \text{ for some } 0 < \theta < 1.$$

5. Compute the class group of $\mathbb{Q}(\sqrt{-31})$. Show that if $y^2 + 31 = x^3$ has a solution (x, y) then y must be odd. Hence show that it has no integer solution.

6. Find all integer solutions of
$$y^2 + 1175 = 4x^3.$$

7. Let K be an algebraic number field. Show that there is a number field L containing K such that for every ideal $I \subset \mathcal{O}_K$, the ideal in $\mathcal{O}_L$ generated by I (denoted $I\mathcal{O}_L$) is principal.

8. Let $K = \mathbb{Q}(\sqrt{-m})$ where $m \not\equiv 3 \bmod 4$ and $m = p_1 \cdots p_k$ a product of distinct primes. Show that $\langle p_i \rangle = \mathfrak{p}_i^2$ where $\mathfrak{p}_i = \langle p_i, \sqrt{-m} \rangle$. When are the ideals $\prod_i \mathfrak{p}_i^{r_i}$ and $\prod_i \mathfrak{p}_i^{s_i}$ in the same ideal class? Deduce that the class group $C(K)$ contains a subgroup isomorphic to $(\mathbb{Z}/2\mathbb{Z})^{k-1}$.

9. Let p and q be distinct odd primes such that p is a square mod q and q is a square mod p.

   (i) Show that at least one of p and q is congruent to 1 mod 4. Assume $p \equiv 1 \bmod 4$, show that there are integers u, v such that
$$u^2 \equiv p \bmod 4q, \quad p|u, \quad v^2 \equiv q \bmod p, \text{ and } q|v.$$

   (ii) Define
$$\Lambda = \{(x, y, z) \in \mathbb{Z}^3 : \mathbb{Z} \equiv 0 \bmod 2, x \equiv uy + vz \bmod 2pq\}.$$
   Show that Λ is a lattice in $\mathbb{R}^3$ and if $(x, y, z) \in \Lambda$ then
$$x^2 - py^2 - qz^2 \equiv 0 \bmod 4pq.$$

(iii) By considering the ellipsoid

$$X = \{(x, y, z) \in \mathbb{R}^3 : x^2 + py^2 + qz^2 < 4pq\}$$

show that

$$x^2 - py^2 - qz^2 = 0$$

has a non-trivial solution.

10. Let $K = \mathbb{Q}(\alpha)$ where α is a root of $f(x) = x^3 - 3x + 1$.

(i) Show that f is irreducible over $\mathbb{Q}$ and compute its discriminant.

(ii) Show that $3\mathcal{O}_K = \mathfrak{p}^3$ where $\mathfrak{p} = \langle \alpha + 1 \rangle$ is a prime ideal in $\mathcal{O}_K$ with residue field $\mathbb{F}_3$. Deduce that $\mathcal{O}_K = \mathbb{Z}[\alpha] + 3\mathcal{O}_K$.

(iii) Show that $\mathcal{O}_K = \mathbb{Z}[\alpha]$. Compute the class group of K.

6 Units

The units in $\mathcal{O}_K$, denoted $U(K)$ (or $\mathcal{O}_K^\times$) is just the set of invertible elements in $\mathcal{O}_K$. We will study the structure of the units.

6.1 The norm condition

Lemma 6.1. *Let K be an algebraic number field. Then $u \in \mathcal{O}_K$ is a unit if and only if $N_{K/\mathbb{Q}}(u) = \pm 1$.*

Proof. u is a unit if and only if $|\mathcal{O}_K/u\mathcal{O}_K| = 1$, if and only if $|N_{K/\mathbb{Q}}(u)| = 1$. □

If one has read theorems in continued fraction, then it is immediate that any real quadratic number field has a non-trivial unit (unit not equal to ±1). We give an alternative proof.

Theorem 6.2. *Let $K = \mathbb{Q}(\sqrt{m})$ then K has a non-trivial unit. In particular,*

$$U(K) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}.$$

Proof. Let $H = \sigma(\mathcal{O}_K)$ which is a lattice in $\mathbb{R}^2$. Note that if $\sigma(\alpha) = (\alpha_x, \alpha_y) \in H$ then the norm of α is $\alpha_x\alpha_y$. Let C be the covolume of H. For each $\lambda \in \mathbb{R}$ let $\mu = \frac{C}{\lambda}$. Then consider the rectangle

$$S_\lambda = x \in [-\lambda, \lambda], y \in [-\mu, \mu]$$

centered at the origin. The volume of S_λ is $4\lambda\mu = 4C \geq 4C$. So by Minkowski convex body theorem we have $(0,0) \neq (x_\lambda, y_\lambda) \in S_\lambda \cap H$. By choice of S_λ, we have $|x_\lambda| \leq \lambda, |y_\lambda| \leq \mu = \frac{C}{\lambda}$. Further

$$|x_\lambda||y_\lambda| \leq \lambda\mu = C$$

and since $(x_\lambda, y_\lambda) \neq 0$ so the norm is non-zero and as the norm must be an integer. We have

$$|x_\lambda||y_\lambda| \geq 1$$

and so

$$|x_\lambda| \geq \frac{1}{|y_\lambda|} \geq \frac{1}{\mu} = \frac{\lambda}{C}.$$

Since the covolume $C > 1$ then for each n let $\lambda_n = C^{2n}$. Then from the above we must have

$$C^{2n-1} \leq |x_{\lambda_n}| \leq C^{2n} \Rightarrow |x_{\lambda_n}| \leq |x_{\lambda_{n+1}}|$$

and so $|x_{\lambda_n}| \neq |x_{\lambda_m}|$ for $m \neq n$.

Finally, as the norm of x_{λ_n} is $x_{\lambda_n}y_{\lambda_n}$ which has modulus less than C and there are only finitely many ideals with norm less than C so we conclude that for some $n \neq m$, we have

$$\langle x_{\lambda_n} \rangle = \langle x_{\lambda_m} \rangle$$

and so $x_{\lambda_n} = ux_{\lambda_m}$ for some unit u. But $|x_{\lambda_n}| \neq |x_{\lambda_m}|$ so $u \neq \pm 1$. We can also assume $u > 1$ by considering $-u$ and $1/u$.

u is a unit if and only if $-u$ is a unit. So we consider the positive units. Let u be the smallest positive unit > 1. It is possible to pick the smallest one because $\sigma(\mathcal{O}_K)$ is a lattice. If v is another unit > 1 then take n with

$$u^n \leq v < u^{n+1}$$

and so

$$1 \leq vu^{-n} < u.$$

By our choice of u we conclude that $vu^{-n} = 1$ and so $v = u^n$. Since every unit w with $0 < w < 1$ is $1/v$ for some $v > 1$, we conclude that every positive unit is a power of u. So $U(K)_{>0} \cong \mathbb{Z}$ and so the result follows. □

Definition 6.3. *Let K be a real quadratic number field. The fundamental unit u in $\mathcal{O}_K$ is the smallest unit > 1, which is also the generator for the free part of $U(K)$.*

Proposition 6.4. *Let $d > 1$ be a square free integer. Suppose d has a factor which is 3 mod 4, then the fundamental unit of $\mathbb{Q}(\sqrt{d})$ has norm 1.*

Proof. The assumption shows that d has a prime factor p which is 3 mod 4. We show there is no unit of norm -1. If $d \equiv 2, 3 \bmod 4$, then there is no integer solution of

$$x^2 - dy^2 = -1$$

by considering reduction mod p. If $d \equiv 1 \bmod 4$, then the norm of elements take the form

$$x^2 + xy + y^2 \frac{1-d}{4},$$

If this is -1 then

$$(2x+y)^2 - dy^2 = -4$$

and so -4 is a square mod p, which again is a contradiction. □

6.2 Dirichlet's unit theorem

Lemma 6.5. *Rewrite $\sigma_1, \ldots, \sigma_n$ in the way that $\sigma_1, \ldots, \sigma_r$ are the real embeddings, and that $\sigma_{r+1}, \overline{\sigma_{r+1}}, \ldots, \sigma_{r+s}, \overline{\sigma_{r+s}}$ are the complex embeddings.*

Define the map

$$L : \mathcal{O}_K \backslash \{0\} \to \mathbb{R}^{r+s}, x \mapsto (\log |\sigma_1(x)|, \ldots, \log |\sigma_r(x)|, 2 \log |\sigma_{r+1}(x)|, \ldots, 2 \log |\sigma_{r+s}(x)|) = (x_1, \ldots, x_{r+s}).$$

Then for each non-zero $\alpha \in \mathcal{O}_K$ and each fixed k with $1 \leq k \leq r+s$, there exists a non-zero $\beta \in \mathcal{O}_K$ such that $|N_{K/\mathbb{Q}}(\beta)| \leq \frac{4}{\pi}\sqrt{|\mathcal{D}_K|}$ and $\beta_i < \alpha_i$ for all $i \neq k$.

Proof. For each $i \neq k$ pick c_i such that

$$0 < c_i < \exp(\alpha_i).$$

and define c_k such that

$$\prod_{i=1}^{r+s} c_i = \left(\frac{4}{\pi}\right)^s \sqrt{|\mathcal{D}_K|}.$$

Let

$$E = \{(y_1, \ldots, y_r, z_1, \ldots, z_s) \in \mathbb{R}^r \times \mathbb{C}^s : |y_i| \leq c_i, |z_j|^2 < c_{r+j}\}.$$

It is clear that E is a convex body and the volume

$$m(E) = 2^r \pi^s \prod_{i=1}^{r} c_i \prod_{j=1}^{s} c_{r+j} = 2^{r+2s}\sqrt{|\mathcal{D}_K|} = 2^n \mathrm{cov}(\sigma(\mathcal{O}_K)).$$

By Minkowski's convex body theorem, there exists a non-zero $\beta \in \mathcal{O}_K$ such that

$$\sigma(\beta) \in E \cap \sigma(\mathcal{O}_K).$$

Since $\sigma(\beta) \in E$, so

$$|N_{K/\mathbb{Q}}(\beta)| \leq \prod_{i=1}^{r+s} c_i \leq \frac{4}{\pi}\sqrt{|\mathcal{D}_K|}.$$

For each $i \neq k, i \leq r$, we have

$$\beta_i = \log |\sigma_i(\beta)| \leq \log c_i \leq \alpha_i$$

and for $i \neq k, i > r$ we have

$$\beta_i = 2 \log |\sigma_i(\beta)| \leq 2 \log \sqrt{c_i} < \alpha_i.$$

□

Lemma 6.6. *Define L as in the previous lemma and $L(\theta) = (\theta_1, \dots, \theta_n)$ for any non-zero $\theta \in \mathcal{O}_K$. For each fixed k with $1 \leq k \leq r+s$, there exists a unit $\theta \in \mathcal{O}_K$, such that $\theta_i < 0$ for all $i \neq k$.*

Proof. Fix k. Let x_1 be any non-zero element in $\mathcal{O}_K$. Define a sequence x_n inductively as in the previous lemma such that x_{n+1} is a non-zero element in $\mathcal{O}_K$ such that

$$N_{K/\mathbb{Q}}(x_{n+1})| \leq \frac{4}{\pi}\sqrt{|\mathcal{D}_K|}$$

and the i^{th} coordinate of $L(x_{n+1}$ is less than the i^{th} coordinate of $L(x_n)$ for all $i \neq k$. So we have a sequence of elements of bounded norm and since there are only finitely many ideals of bounded norms we conclude that

$$\langle x_n \rangle = \langle x_{n+r} \rangle$$

for some $n, r > 0$. So $\theta = \frac{x_{n+r}}{x_n}$ is a unit. By construction, if $L(\theta) = (\theta_1, \dots, \theta_r, \theta_{r+1}, \dots, \theta_s)$ then $\theta_i < 0$ for all $i \neq k$. □

Lemma 6.7. *For each $k \leq r+s$, let u_k be the unit in the previous lemma. Let A be the square matrix whose i^{th} row is $L(u_i)$. Then A is a real matrix such that $A_{ij} < 0$ for all $i \neq j$ and $A_{ii} > 0$ for each i. Moreover, the sum of each row is 0 and the rank of A is $r+s-1$.*

Proof. It is clear that A is real and the sum of k^{th} row is

$$\log \prod_{i=1}^{r+s} |\sigma_i(u_k)| = \log |N_{K/\mathbb{Q}}(u_k)| = 0.$$

By the previous lemma, we have $A_{ij} < 0$ for each $i \neq j$. Since the sum of each row is 0 so $A_{ii} > 0$ for each i, and the vector $(1, 1, \dots, 1)^t$ is in the kernel of A. So the rank of A is at most $r+s-1$.

Let V_i be the i^{th} column. Suppose $\sum_{i=1}^{r+s-1} t_i V_i = 0$, t_i not all zero, then pick $k \in \{1, \dots, r+s-1\}$ with $t_k \neq 0$ and t_k maximal. Divide both sides by t_k and rewrite the equation as

$$t_1 V_1 + \cdots + t_{r+s-1} V_{r+s-1} = 0, \quad t_i \leq 1 \text{ for all } i \neq k, t_k = 1.$$

Consider the k^{th} coordinate of the above vector where $k < r+s$. Since $A_{ki} < 0$ for each $i \neq k$ and so

$$0 = \sum_{i=1}^{r+s-1} t_i A_{ki} \geq \sum_{i=1}^{r+s-1} A_{ki} > \sum_{i=1}^{r+s} A_{ki} = 0$$

which is a contradiction. Therefore $V_1, \dots, V_{r+s-1}$ are linearly independent and so the rank is precisely $r+s-1$. □

Theorem 6.8 (Dirichlet's unit theorem). *For each algebraic number field K,*

$$U_K \cong \mu_K \times \mathbb{Z}^{r+s-1}$$

where μ_K is the set of roots of unity in K.

Proof. Let L be the map as the previous lemmas. Then $L(U_K)$ is contained in the hyperplane W where

$$W = \{(y_1, \dots, y_r, z_1, \dots, z_s) \in \mathbb{R}^{r+s} : \sum_{i=1}^{r} y_i + \sum_{j=1}^{s} z_j = 0\}.$$

Let B be a compact subset in W then there exists $a \in \mathbb{R}$ such that

$$\frac{1}{a} \leq |\sigma_i(x)| \leq a$$

for all i and for all $x \in L^{-1}(B)$. Since $|\sigma_i(x)|$ is bounded, so there are only finitely many such x because the coefficients of the minimal polynomial of x are symmetric polynomials in $\sigma_i(x)$. So $L^{-1}(B)$ is finite and so $B \cap L(U_K)$ is finite. Therefore, $L(U_K)$ is a discrete additive subgroup of W. Since $\{0\}$ is also a compact subset in W, so $L^{-1}(\{0\})$ is finite, and so the kernel of L is finite. Restricting L on U_K, we conclude that

$$U_K/(\ker L \cap U_K) \cong V \subset W$$

where V is a discrete additive subgroup. By Lemma 5.3, V is finitely generated over $\mathbb{Z}$ and every $\mathbb{Z}$-basis is linearly independent over $\mathbb{R}$. So the rank of V is less than or equal to the rank of W, which is $r+s-1$ and we can write

$$U_K/(\ker L \cap U_K) \cong V \cong \mathbb{Z}^m, \text{ for some } m \leq r+s-1.$$

The previous lemma shows that we can find $r+s-1$ units whose image under L are linearly independent over $\mathbb{R}$. So $m = r+s-1$. Finally, $\ker L \cap U_K$ is a subgroup of $K^\times$ and so it is cyclic. Therefore, $\ker L \cap U_K = \mu_K$. □

Definition 6.9. *The units $e_1, \ldots, e_k \in U_K$ are said to be independent if*

$$e_1^{a_1} \cdots e_k^{a_k} = 1$$

implies $a_1, \ldots, a_k = 0$.

We say $\{e_1, \ldots, e_{r+s-1}\}$ is a fundamental system of units if $e_1, \ldots, e_{r+s-1}$ are independent and any unit $u \in U_K$ can be uniquely written as

$$u = \zeta e_1^{a_1} \cdots e_{r+s-1}^{a_{r+s-1}}$$

where $\zeta \in \mu_K$.

6.3 Regulator

Let $r, s, \sigma_1, \ldots, \sigma_{r+s}$ be the same notation as before.

Definition 6.10. *Let $\{e_1, \ldots, e_{r+s-1}\}$ be a fundamental system of units in U_K and E be the $(r+s-1) \times (r+s)$ matrix with*

$$E_{ij} = \log|\sigma_j(e_i)|, i = 1, \ldots, r+s-1, j = 1, \ldots, r+s.$$

Let A be any $r+s-1 \times r+s-1$ minors of E, then the non-negative number

$$R(K) = |\det A|$$

is called the regulator of K.

We shall check $R(K)$ is well-defined.

Lemma 6.11. *$R(K)$ is independent of the choice of A. In other words, let A_i be the matrices formed by E with the i^{th} column deleted, then for any $i \neq j$,*

$$|\det A_i| = |\det A_j|.$$

Proof. Let $V_1, \ldots, V_{r+s}$ be the columns of the matrix E. Since the sum of each row of the matrix E is 0, we have

$$V_{r+s} = -V_1 - V_2 - \cdots - V_{r+s-1}$$

and so $V_i = -V_1 - V_2 - \cdots - V_{i-1} - V_{i+1} - \cdots - V_{r+s}$. By column operation we conclude that

$$|\det A_i| = |\det A_{r+s}|$$

for any i. □

Lemma 6.12. *The regulator is independent of the choice of the fundamental system of units.*

Proof. Let $\{e_1, \ldots, e_{r+s-1}\}$ and $\{f_1, \ldots, f_{r+s-1}\}$ be fundamental systems of units. Then there exist $b_i, a_{ij} \in \mathbb{Z}$ such that

$$f_i = \zeta^{b_i} \prod_{j=1}^{r+s-1} e_j^{a_{ij}}$$

and c_i, d_{ij} such that

$$e_i = \zeta^{c_i} \prod_{j=1}^{r+s-1} f_j^{d_{ij}}.$$

Therefore,

$$f_i = \zeta^{b_i} \prod_{j=1}^{r+s-1} (\zeta^{c_j} \prod_{k=1}^{r+s-1} f_k^{d_{jk}})^{a_{ij}} = \zeta^{b_i + \sum_j a_{ij} c_j} \prod_{k=1}^{r+s-1} f_k^{\sum_{j=1}^{r+s-1} a_{ij} d_{jk}}.$$

By uniqueness, we have

$$\sum_{j=1}^{r+s-1} a_{ij} d_{jk} = \delta_{ik}.$$

Let A, D be the matrices such that $A_{ij} = a_{ij}$ and $D_{ij} = d_{ij}$. Then $AD = I$ and so $\det A \det D = 1$. But $A_{ij}, D_{ij} \in \mathbb{Z}$ for all i, j and so

$$|\det A| = |\det B| = 1.$$

Let σ_k be any embedding, then

$$|\sigma_k(f_i)| = \prod_{j=1}^{r+s-1} |\sigma_k(e_j)|^{a_{ij}}$$

and so

$$\log |\sigma_k(f_i)| = \sum_{j=1}^{r+s-1} a_{ij} \log |\sigma_k(e_j)|.$$

Let E and F be the $(r+s-1) \times (r+s-1)$ matrices with entries $\log |\sigma_k(e_i)|, \log |\sigma_k(f_i)|$ respectively where $k = 1, \ldots, r+s-1$. Then

$$F = AE$$

and so $|\det F| = |\det A \det E| = |\det E|$. □

Definition 6.13. *Let K be an algebraic number field. The Dedekind ζ function is defined as*

$$\zeta_K(s) = \sum_{0 \neq I \subset \mathcal{O}_K} \frac{1}{N(I)^s}.$$

The following class number formula is (computationally) useful to approximate the regulator and hence (sometimes) helps to find a fundamental system of units.

Theorem 6.14 (Class number formula). *Let $h(K)$ be the class number of K and $\omega(K)$ be the number of roots of unity in K. Then*

$$\lim_{s \to 1^+} (s-1)\zeta_K(s) = \frac{2^r (2\pi)^s h(K) R(K)}{\omega(K) \sqrt{|\mathcal{D}_K|}}.$$

6.4 Exercises

1. (i) Find the fundamental unit in $\mathbb{Q}(\sqrt{3})$. Determine all the integer solutions of the equation $x^2 - 3y^2 = 13$.

   (ii) Find the fundamental unit in $\mathbb{Q}(\sqrt{10})$. Determine all the integer solutions of the equation $x^2 - 10y^2 = 6$.

2. Let $u \in U_K$ be a unit such that $|\sigma_i(u)| = 1$ for all i. Show that $u \in \mu_K$.

3. Let K be a CM (complex multiplication) field, that is K is an imaginary quadratic extension of a totally real number field L. Let $\mu_K U_L$ be the composite group of μ_K and U_L inside U_K. By considering the map
$$\lambda : U_K \to U_K, \quad \alpha \mapsto \frac{\alpha}{\bar{\alpha}}$$
show that the index of $\mu_K U_L$ inside U_K is at most 2.

4. Let $K = \mathbb{Q}(\zeta_8)$. Find a fundamental unit of K.

5. Let $K = \mathbb{Q}(\zeta_{12})$. Compute $N_{K/L}(1 + \zeta_{12})$ where $L = K \cap \mathbb{R}$. Find a fundamental unit of K.

6. (i) For all $x, \theta\ in \mathbb{R}$, show that $\sin^2\theta(x - 2\cos\theta)^2 < x^2 + 4$.

   (ii) Let K be a cubic number field with one real and two complex embeddings. Let $u > 1$ be the fundamental unit of $\mathcal{O}_K$. Write u and $\bar{u}$ in terms of $re^{\pm i\theta}$, show that the discriminant of $\mathbb{Z}[u]$ is
$$-4\sin^2\theta(r^3 + r^{-3} - 2\cos\theta)^2.$$
   Show further that
$$\left|-4\sin^2\theta(r^3 + r^{-3} - 2\cos\theta)^2\right| < 4(u^3 + u^{-3} + 6).$$

   (iii) If $|\mathcal{D}_K| > 32$, show that
$$\left|u^3 - \left(\frac{|\mathcal{D}_K|}{8} - 3\right)\right| > \frac{|\mathcal{D}_K|}{8} - \frac{15}{4}$$
   and hence show that
$$u^3 > \frac{|\mathcal{D}_K| - 27}{4}.$$

   (iv) Find the fundamental unit of $\mathbb{Q}(\theta)$ where θ is the real root of $x^3 - x^2 + x - 2 = 0$.

7. Let p be a prime with $p \equiv 1 \bmod 4$ and $K = \mathbb{Q}(\sqrt{p})$. Let u be the fundamental unit. By considering the principal ideal $\langle\gamma\rangle$ where
$$\gamma = \frac{1 + u}{m}$$
and m is the largest integer such that $m | 1 + u$, show that $N(u) = -1$.

8. Compute the class number of $K = \mathbb{Q}(\sqrt{7})$. Show that if (x, y) is an integer solution of
$$x^3 = y^2 - 7$$
then
$$y + \sqrt{7} = u^n(a + b\sqrt{7})^3$$
where $u = 8 + 3\sqrt{7}, n = 0, \pm 1$ and $a, b \in \mathbb{Z}$. Hence show that $x^3 = y^2 - 7$ has no integer solution.

9. Let K be an algebraic number field such that U_K contains a non-real root of unity. Prove that $N_{K/\mathbb{Q}}(\alpha) > 0$ for every $\alpha \in K \backslash \{0\}$.