

Number Fields

Introduction

A *number field* is a field of finite degree over \mathbb{Q} . By the Primitive Element Theorem, any number field $K = \mathbb{Q}(\alpha)$ for some $\alpha \in K$.

The minimal polynomial

Let K be a number field and let $\alpha \in K$. The unique monic, irreducible polynomial $f \in \mathbb{Q}[X]$ of smallest degree such that $f(\alpha) = 0$ is called the *normalised minimal polynomial* (NMP) of α over \mathbb{Q} .

Norm and trace

For any number field K and any element $\beta \in K$, multiplication by β defines a \mathbb{Q} -linear map $i(\beta) : K \rightarrow K$. i is an injective ring homomorphism $K \rightarrow \text{End}_{\mathbb{Q}}(K)$. Let

$$P_{\beta} = \det(XI - i(\beta)) \in \mathbb{Q}[X]$$

be the characteristic polynomial of $i(\beta)$. Then $P_{\beta}(\beta) = 0$, since $i(P_{\beta}(\beta)) = P_{\beta}(i(\beta)) = 0$ by the Cayley–Hamilton Theorem.

We define the *norm* and *trace* of β to be

$$\begin{aligned} N_{K/\mathbb{Q}}(\beta) &= \det(i(\beta)) \\ \text{Tr}_{K/\mathbb{Q}}(\beta) &= \text{Tr}(i(\beta)). \end{aligned}$$

The norm and trace have the following properties:

$$\begin{aligned} N_{K/\mathbb{Q}}(\alpha\beta) &= N_{K/\mathbb{Q}}(\alpha) N_{K/\mathbb{Q}}(\beta) \\ \text{Tr}_{K/\mathbb{Q}}(\alpha + \beta) &= \text{Tr}_{K/\mathbb{Q}}(\alpha) + \text{Tr}_{K/\mathbb{Q}}(\beta) \end{aligned}$$

for all $\alpha, \beta \in K$. Also,

$$\begin{aligned} N_{K/\mathbb{Q}}(\lambda\alpha) &= \lambda^{[K:\mathbb{Q}]} N_{K/\mathbb{Q}}(\alpha) \\ \text{Tr}_{K/\mathbb{Q}}(\lambda\alpha) &= \lambda \text{Tr}_{K/\mathbb{Q}}(\alpha) \end{aligned}$$

for all $\lambda \in \mathbb{Q}$ and all $\alpha \in K$. Finally we have the formulae

$$\begin{aligned} N_{K/\mathbb{Q}}(\alpha) &= ((-1)^d a_0)^e \\ \text{Tr}_{K/\mathbb{Q}}(\alpha) &= -ea_{d-1}, \end{aligned}$$

where $X^d + a_{d-1}X^{d-1} + \dots + a_1X + a_0$ is the NMP of α over \mathbb{Q} and $e = [K : \mathbb{Q}(\alpha)]$.

Conjugates and embeddings

Let $K = \mathbb{Q}(\alpha)$ be a number field of degree n and let $f \in \mathbb{Q}[X]$ be the NMP of α . Then

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

where the α_i , the *conjugates* of α , are all distinct. For each α_i there is a corresponding embedding $\sigma_i : K \hookrightarrow \mathbb{C}$ sending α to α_i , and these are all the embeddings of K into \mathbb{C} .

We write r_1 for the number of real roots of f , and r_2 for the number of pairs of complex conjugate roots. Then $n = r_1 + 2r_2$.

The norm and trace of any $\beta \in K$ may be computed in terms of its conjugates, as

$$N_{K/\mathbb{Q}}(\beta) = \prod_{i=1}^n \sigma_i(\beta) \quad \text{Tr}_{K/\mathbb{Q}}(\beta) = \sum_{i=1}^n \sigma_i(\beta),$$

since $i(\beta)$ is diagonalizable over K , with diagonal elements $\sigma_i(\beta)$.

Discriminants

Let $K = \mathbb{Q}(\alpha)$ be a number field and let f be the NMP of α . Then the *discriminant* of f is

$$\text{disc}(f) = \prod_{1 \leq i < j \leq n} (\alpha_i - \alpha_j)^2 = \begin{vmatrix} 1 & 1 & \cdots & 1 \\ \alpha_1 & \alpha_2 & \cdots & \alpha_n \\ \vdots & \vdots & & \vdots \\ \alpha_1^{n-1} & \alpha_2^{n-1} & \cdots & \alpha_n^{n-1} \end{vmatrix} \begin{vmatrix} 1 & \alpha_1 & \cdots & \alpha_1^{n-1} \\ 1 & \alpha_2 & \cdots & \alpha_2^{n-1} \\ \vdots & \vdots & & \vdots \\ 1 & \alpha_n & \cdots & \alpha_n^{n-1} \end{vmatrix} = \det A$$

where $A = (A_{ij})$ and

$$A_{ij} = \sum_{k=1}^n \alpha_k^{i+j} = \text{Tr}_{K/\mathbb{Q}}(\alpha^{i+j}) = \text{Tr}_{K/\mathbb{Q}}(\alpha^i \alpha^j).$$

Let $\omega_1, \dots, \omega_n$ be a basis for K/\mathbb{Q} . The *discriminant* of this basis is $D(\omega_1, \dots, \omega_n) = \det A$, where $A = (A_{ij})$ and $A_{ij} = \text{Tr}_{K/\mathbb{Q}}(\omega_i \omega_j)$. We have $D(1, \alpha, \alpha^2, \dots, \alpha^{n-1}) = \text{disc}(f)$.

If we have a change of basis, given by an element $g \in \text{GL}_n(\mathbb{Q})$, then A is replaced by $g^T A g$ and the discriminant is multiplied by $\det(g)^2$. Thus we define the *discriminant* $\text{Disc}(K/\mathbb{Q})$ as the discriminant of any basis, modulo squares, that is

$$\text{Disc}(K/\mathbb{Q}) = D(\omega_1, \dots, \omega_n) \pmod{\mathbb{Q}^{*2}} \in \mathbb{Q}/\mathbb{Q}^2,$$

which does not depend on the choice of basis. Note that for a number field K , $\text{Disc}(K/\mathbb{Q}) \neq 0$.

A useful formula is

$$\begin{aligned} N_{\mathbb{Q}(\alpha)/\mathbb{Q}}(f'(\alpha)) &= \prod_{i=1}^n f'(\alpha_i) \\ &= \prod_{i=1}^n \prod_{j \neq i} (\alpha_i - \alpha_j) \\ &= (-1)^{n(n-1)/2} \prod_{1 \leq i < j \leq n} (\alpha_j - \alpha_i)^2 \\ &= (-1)^{n(n-1)/2} \text{disc}(f). \end{aligned}$$

Algebraic Integers

The ring of integers

Given a number field K , we want to identify a subring \mathcal{O}_K to be an analogue of the subring \mathbb{Z} of \mathbb{Q} . We want \mathcal{O}_K to be finitely generated as a \mathbb{Z} -module, and to be maximal subject to this constraint.

We notice that any subring R which is finitely generated as a \mathbb{Z} -module has the property that for all $\alpha \in R$ there exists a monic polynomial $f \in \mathbb{Z}[X]$ such that $f(\alpha) = 0$. With this in mind, we define an element $\alpha \in K$ to be an *algebraic integer* of K if α is the root of some monic polynomial in $\mathbb{Z}[X]$, and we denote the set of all algebraic integers in K by \mathcal{O}_K .

An element $\alpha \in K$ is an algebraic integer if and only if all the coefficients of the NMP of α are (rational) integers. Therefore, if $\alpha \in \mathcal{O}_K$, the trace and norm of α are (rational) integers.

Integral bases

Let K be a number field of degree n . We say that a basis $\alpha_1, \dots, \alpha_n$ for K over \mathbb{Q} is an *integral basis* if

$$\mathcal{O}_K = \mathbb{Z}\alpha_1 + \dots + \mathbb{Z}\alpha_n.$$

We shall show that every number field has an integral basis. First, however, we must show that \mathcal{O}_K is a subring. To do this we need the following lemma.

Lemma

Let K be a number field and let $\alpha \in K$. Then the following are equivalent:

1. $\alpha \in \mathcal{O}_K$,
2. The additive group $\mathbb{Z}[\alpha]$ is finitely generated,
3. There is a vector space V over K and a non-zero, finitely generated abelian subgroup $M = \mathbb{Z}v_1 + \dots + \mathbb{Z}v_m \subseteq V$ such that $\alpha M \subseteq M$.

Using this lemma, we may prove the following theorem.

Theorem

Let K be a number field. Then

1. If $\alpha_1, \dots, \alpha_n \in \mathcal{O}_K$ and $f \in \mathbb{Z}[X_1, \dots, X_n]$ then $f(\alpha_1, \dots, \alpha_n) \in \mathcal{O}_K$.
2. \mathcal{O}_K is a subring of K .
3. If $\beta \in K$ is a root of $X^n + \alpha_1 X^{n-1} + \dots + \alpha_n$, where $\alpha_1, \dots, \alpha_n \in \mathcal{O}_K$, then $\beta \in \mathcal{O}_K$.

It now remains to show that K has an integral basis. First we prove the following theorem, which gives us a method of ‘approximating’ \mathcal{O}_K .

Theorem

Let K be a number field of degree n , with $\alpha_1, \dots, \alpha_n \in \mathcal{O}_K$ a basis for K over \mathbb{Q} . Then

$$\mathbb{Z}\alpha_1 + \dots + \mathbb{Z}\alpha_n \subseteq \mathcal{O}_K \subseteq \mathbb{Z}\frac{\alpha_1}{d} + \dots + \mathbb{Z}\frac{\alpha_n}{d},$$

where $d = D(\alpha_1, \dots, \alpha_n) \in \mathbb{Z}$.

In particular, if $K = \mathbb{Q}(\alpha)$, where $\alpha \in \mathcal{O}_K$, and f is the NMP of α , then

$$\mathbb{Z}[\alpha] \subseteq \mathcal{O}_K \subseteq \frac{1}{d}\mathbb{Z}[\alpha],$$

where $d = D(1, \alpha, \dots, \alpha^{n-1}) = \text{disc}(f)$.

We are now able to prove that any number field has an integral basis. So \mathcal{O}_K is a subring which is finitely generated as a \mathbb{Z} -module, and since we have seen that every element of a ring which is finitely generated as a \mathbb{Z} -module is an algebraic integer, it is clear that \mathcal{O}_K is maximal. Thus \mathcal{O}_K is indeed the ring we set out to define.

Subgroups of \mathbb{Z}^n

Let $\text{GL}_n(\mathbb{Z}) = \{g \in M_n(\mathbb{Z}) \mid \det g = \pm 1\}$ be the group of linear automorphisms of \mathbb{Z}^n .

A general \mathbb{Z} -basis of \mathbb{Z}^n is of the form e_1, \dots, e_n , where $(e_1 \mid \dots \mid e_n) \in \text{GL}_n(\mathbb{Z})$. More generally, if $v_1, \dots, v_n \in \mathbb{Z}^n$ set $g = (v_1 \mid \dots \mid v_n) \in M_n(\mathbb{Z})$ and let $L = \mathbb{Z}v_1 + \dots + \mathbb{Z}v_n \subseteq \mathbb{Z}^n$ be the lattice generated by the v_i . Then

$$(\mathbb{Z}^n : L) = \begin{cases} |\det g| & \text{if } \det g \neq 0 \\ \infty & \text{if } \det g = 0. \end{cases}$$

This follows from the Theorem on Elementary Divisors.

\mathbb{Z} -lattices

Let K be a number field. A subgroup A of the additive group of K is called a \mathbb{Z} -lattice in K if there exists a basis $\alpha_1, \dots, \alpha_n$ of K over \mathbb{Q} such that $A = \mathbb{Z}\alpha_1 + \dots + \mathbb{Z}\alpha_n$, or equivalently, if A is finitely generated and contains a basis of K over \mathbb{Q} .

The discriminant of a \mathbb{Z} -lattice

The *discriminant* of a \mathbb{Z} -lattice A in K is

$$\text{Disc}(A/\mathbb{Z}) = D(\alpha_1, \dots, \alpha_n)$$

for a \mathbb{Z} -basis $\alpha_1, \dots, \alpha_n$ of A . This is independent of the choice of \mathbb{Z} -basis. The *discriminant* of a number field K is

$$D_K = \text{Disc}(\mathcal{O}_K/\mathbb{Z}) = D(\alpha_1, \dots, \alpha_n)$$

for any integral basis $\alpha_1, \dots, \alpha_n$.

If A and B are \mathbb{Z} -lattices in K with $B \subseteq A$, then

$$\text{Disc}(B/\mathbb{Z}) = \text{Disc}(A/\mathbb{Z}) \cdot (A : B)^2.$$

Therefore, if A is a \mathbb{Z} -lattice in K with squarefree discriminant, then $A = \mathcal{O}_K$.

Units

We wish to describe the group of units \mathcal{O}_K^* of \mathcal{O}_K . If $\alpha \in \mathcal{O}_K$, then $\alpha \in \mathcal{O}_K^*$ if and only if $N_{K/\mathbb{Q}}(\alpha) = \pm 1$. Note, however, that there exist elements $\alpha \in K \setminus \mathcal{O}_K$ with norm ± 1 .

Dirichlet's Theorem on Units

Let K be a number field, with r_1 and r_2 as defined as above. Let $r = r_1 + r_2 - 1$ and let $\mu(K)$ denote the group of roots of unity in K . Then

$$\mathcal{O}_K^* \cong \mu(K) \times \mathbb{Z}^r.$$

Thus there are elements $\epsilon_1, \dots, \epsilon_r \in \mathcal{O}_K^*$, called the *fundamental units* of \mathcal{O}_K , such that each $u \in \mathcal{O}_K^*$ has a unique expression of the form

$$u = \zeta \epsilon_1^{n_1} \cdots \epsilon_r^{n_r},$$

where $\zeta \in \mu(K)$ and $n_i \in \mathbb{Z}$.

Units in imaginary quadratic fields

Let K be an imaginary quadratic field. Then $r_1 = 0$ and $r_2 = 1$, and so $r = 0$. Then \mathcal{O}_K^* is

$$\begin{array}{ll} K = \mathbb{Q}(\sqrt{-1}) & \mathcal{O}_K^* = \{\pm 1, \pm i\} \\ K = \mathbb{Q}(\sqrt{-3}) & \mathcal{O}_K^* = \{\pm 1, \pm \rho, \pm \rho^2\} \\ K = \text{other} & \mathcal{O}_K^* = \{\pm 1\}. \end{array}$$

Units in real quadratic fields

Let K be a real quadratic field. Then $r_1 = 2$ and $r_2 = 0$, and so $r = 1$. $\mu(K) = \{\pm 1\}$, and so

$$\mathcal{O}_K^* = \{\pm \epsilon^r \mid r \in \mathbb{Z}\},$$

where ϵ is the fundamental unit of \mathcal{O}_K .

An *order* in a number field K is a subring which is also a \mathbb{Z} -lattice. A subring $R \subset K$ is an order if and only if $R \subseteq \mathcal{O}_K$ and $(\mathcal{O}_K : R) < \infty$. Thus \mathcal{O}_K is the unique maximal order in K .

In a quadratic field K , every order is of the form $R_f = \mathbb{Z} + f\mathcal{O}_K$ for a unique $f \in \{1, 2, 3, \dots\}$. R_f is called the order of *conductor* f .

Algorithm for computing ϵ

The following algorithm for computing ϵ is based on the properties of continued fractions. Let $K = \mathbb{Q}(\sqrt{d})$, where $d \geq 2$ is squarefree, and let

$$\theta = \begin{cases} \sqrt{d} & \text{if } d \not\equiv 1 \pmod{4} \\ \frac{1+\sqrt{d}}{2} & \text{if } d \equiv 1 \pmod{4}. \end{cases}$$

Let $f \geq 1$ and let $\alpha_0 = \alpha = -f\bar{\theta}$. We want to compute the continued fraction expansion of α , namely $[a_0, \overline{a_1, \dots, a_m}]$. To do this, we let

$$a_n = \lfloor \alpha_n \rfloor \quad \text{and} \quad \alpha_{n+1} = \frac{1}{\alpha_n - a_n}$$

for each $n \geq 0$. Note that $a_n \geq 1$ for each n . We continue until we find that $\alpha_{m+1} = \alpha_1$, at which point the sequence repeats.

Then we recursively compute the convergents to α , that is the values of p_n and q_n such that $p_n/q_n = [a_0, a_1, \dots, a_n]$ with $\gcd(p_n, q_n) = 1$ and $q_n \geq 1$, by using the formulae

$$\begin{aligned} p_n &= p_{n-1}a_n + p_{n-2} \\ q_n &= q_{n-1}a_n + q_{n-2} \end{aligned}$$

and building up a table like the one below:

n	-2	-1	0	1	2	3	4
a_n			a_0	a_1	a_2	a_3	a_4
p_n	0	1					
q_n	1	0					

Then the fundamental unit in R_f is

$$\epsilon_f = p_{m-1} + q_{m-1}f\theta.$$

Ideals and Unique Factorisation

If K is a number field then it is not necessarily the case that \mathcal{O}_K is a UFD. To make up for this, we consider factorization of ideals in \mathcal{O}_K . We shall show that the non-zero ideals in \mathcal{O}_K factorise uniquely as a product of non-zero prime ideals.

Summary of properties of ideals

An *ideal* I in a ring R is a non-empty subset which is closed under addition, and closed under multiplication from outside. Ideals are precisely the kernels of ring homomorphisms. I is a *prime ideal* if $I \neq R$ and $ab \in I \Rightarrow a \in I$ or $b \in I$. I is a *maximal ideal* if $I \neq R$ and the only ideal $J \supset I$ is $J = R$.

I is a prime ideal iff R/I is a domain and $I \neq R$. I is a maximal ideal iff R/I is a field (and so $I \neq R$ necessarily). Thus every maximal ideal is prime.

If I and J are ideals, then so are $I \cap J$, $I + J$ and $IJ \subseteq I \cap J$. If $I = (\alpha_1, \dots, \alpha_n)$ and $J = (\beta_1, \dots, \beta_m)$ are finitely generated, then so are

$$\begin{aligned} I + J &= (\alpha_1, \dots, \alpha_n, \beta_1, \dots, \beta_m) \\ IJ &= (\alpha_1\beta_1, \dots, \alpha_n\beta_m). \end{aligned}$$

Ideals behave in a similar manner to integers. We can think of the inclusion $I \supseteq J$ as meaning $I \mid J$. Then $I \cap J$ represents $\text{lcm}(I, J)$ and $I + J$ represents $\text{hcf}(I, J)$. Furthermore, if \mathfrak{p} is a prime ideal and $\mathfrak{p} \supseteq IJ$, then $\mathfrak{p} \supseteq I$ or $\mathfrak{p} \supseteq J$, so prime ideals behave like prime elements.

Properties of \mathcal{O}_K

Our proof of unique factorisation of ideals below holds in fact for any *Dedekind ring*. \mathcal{O}_K is a Dedekind ring, which means, among other things, that

1. \mathcal{O}_K is a domain (this is obvious).
2. \mathcal{O}_K is Noetherian (and hence factorisation into irreducibles is possible).
3. The prime ideals in \mathcal{O}_K are just (0) together with all the maximal ideals.

Some ring theory

In any ring, primes are always irreducible. In a domain in which factorisation into irreducibles is possible — in particular, in \mathcal{O}_K — factorisation is unique iff every irreducible is prime.

Any Euclidean domain is a PID, and any PID is a UFD.

A number field is a UFD iff it is a PID, but this is not easy to prove — it is a consequence of the proof below (check this).

A motivating example (taken from Stewart)

In $\mathbb{Q}(\sqrt{15})$ we have the following situation:

$$2 \cdot 5 = (5 + \sqrt{15})(5 - \sqrt{15}),$$

where all four of these factors are irreducible. Thus we do not have unique factorisation. In a sense, the problem is that we have irreducible elements which aren't prime — if 2, say, were prime then 2 would divide one of the factors on the RHS of the equation and then that factor wouldn't be irreducible.

If we could introduce $\sqrt{5}$ into the system then we could split up the factors as

$$\begin{aligned} 2 &= (\sqrt{5} + \sqrt{3})(\sqrt{5} - \sqrt{3}) & (5 + \sqrt{15}) &= (\sqrt{5})(\sqrt{5} + \sqrt{3}) \\ 5 &= (\sqrt{5})(\sqrt{5}) & (5 - \sqrt{15}) &= (\sqrt{5})(\sqrt{5} - \sqrt{3}) \end{aligned}$$

and we see that the two possible factorisations of 10 above were just given by different groupings of our four new factors. So if we extend $\mathbb{Q}(\sqrt{15})$ to $\mathbb{Q}(\sqrt{5}, \sqrt{3})$ then we have unique factorisation of elements in $\mathbb{Q}(\sqrt{15})$ into primes in $\mathbb{Q}(\sqrt{5}, \sqrt{3})$.

Now consider the situation from the perspective of ideals. We have that any $a \in \mathbb{Q}(\sqrt{15})$ can be written uniquely as $a = p_1 \cdots p_n$ for some primes $p_i \in \mathbb{Q}(\sqrt{3}, \sqrt{5})$. Hence we have

$$(a) = (p_1 \cdots p_n) = (p_1) \cdots (p_n),$$

a factorisation of a principal ideal in $\mathbb{Q}(\sqrt{3}, \sqrt{5})$ as a product of more principal ideals. Now we can intersect each ideal above with $\mathcal{O}_{\mathbb{Q}(\sqrt{15})}$ to get a factorisation of ideals in $\mathbb{Q}(\sqrt{15})$ — but these might not be *principal* ideals, for example we could get

$$(a) = (b_1, b_2)(b_3, b_4),$$

so this factorisation of ideals doesn't necessarily give rise to a factorisation of the element a .

The non-principal ideals are like the $\sqrt{5}$ factors we need to introduce.

Fractional ideals

A *fractional ideal* in K is a subset of the form $\alpha I \subset K$, where $\alpha \in K^*$ and $I \subset \mathcal{O}_K$ is a non-zero ideal. There is an obvious multiplication defined on fractional ideals, by

$$(\alpha I)(\beta J) = \alpha\beta(IJ).$$

This is well-defined, as

1. If $\alpha, \beta \in K^*$, then $\alpha\beta \in K^*$, and if I and J are non-zero ideals of \mathcal{O}_K , then so is IJ .
2. If $\alpha_1 I_1 = \alpha_2 I_2$ and $\beta_1 J_1 = \beta_2 J_2$, then $\alpha_1 \beta_1 (I_1 J_1) = \alpha_2 \beta_2 (I_2 J_2)$.

Furthermore, $R = 1(1)$ is the identity element for this multiplication, and so the fractional ideals in K form a monoid. In fact, the fractional ideals form a group, with inverses given by

$$I^{-1} = \{x \in K \mid xI \subseteq \mathcal{O}_K\}.$$

This is a fractional ideal, for if $\alpha \in I$, αI^{-1} is easily seen to be an ideal. The three main stages in proving that the fractional ideals are a group are summarised below:

1. If $II^{-1} = \mathcal{O}_K$ for all non-zero prime ideals $\mathfrak{p} \subseteq \mathcal{O}_K$ then it holds for all fractional ideals.
2. Let $\mathfrak{p} \subseteq \mathcal{O}_K$ be a non-zero prime ideal. Then $\mathfrak{p}^{-1} \not\subseteq \mathcal{O}_K$.
3. $\mathfrak{p}\mathfrak{p}^{-1} = \mathcal{O}_K$.

Proof of unique factorisation of ideals

Existence. Let

$$S = \{I \subseteq \mathcal{O}_K \mid I \text{ is a non-zero ideal, } I \neq \mathfrak{p}_1 \cdots \mathfrak{p}_r \text{ for any } r \geq 0 \text{ and non-zero prime ideals } \mathfrak{p}_i\}.$$

If $S \neq \emptyset$ then there exists a maximal element (w.r.t. inclusion) $I \in S$, since \mathcal{O}_K is noetherian. Since $I \neq \mathcal{O}_K$ there exists a maximal ideal \mathfrak{p} such that $I \subseteq \mathfrak{p}$. Since \mathfrak{p} is maximal, it is also prime. Set $J = I\mathfrak{p}^{-1} \subseteq \mathcal{O}_K$; then $I = J\mathfrak{p} \subset J$. But then the maximality of I implies that $J \notin S$ and so $J = \mathfrak{p}_1 \cdots \mathfrak{p}_r$. But then $I = \mathfrak{p}_1 \cdots \mathfrak{p}_r \mathfrak{p}$ — a contradiction.

Uniqueness. Suppose that $\mathfrak{p}_1 \cdots \mathfrak{p}_r = \mathfrak{q}_1 \cdots \mathfrak{q}_s$. Then $\mathfrak{p}_1 \supseteq \mathfrak{q}_1 \cdots \mathfrak{q}_s$ and so $\mathfrak{p}_1 \supseteq \mathfrak{q}_i$ for some i — wlog we may assume that $i = 1$. But since \mathfrak{p}_1 and \mathfrak{q}_1 are both maximal ideals it must be the case that $\mathfrak{p}_1 = \mathfrak{q}_1$. Multiplying by \mathfrak{p}_1^{-1} we see that $\mathfrak{p}_2 \cdots \mathfrak{p}_r = \mathfrak{q}_2 \cdots \mathfrak{q}_s$. The result follows by induction.

The Chinese Remainder Theorem

Let R be a ring and let $I_1, \dots, I_n \subseteq R$ be ideals such that $\text{hcf}(I_i, I_j) = I + J = R$ for every i and j . Then

$$R/(I_1 \cap \cdots \cap I_n) \longrightarrow R/I_1 \oplus \cdots \oplus R/I_n$$

is an isomorphism. In particular, if $\mathfrak{p}_1, \dots, \mathfrak{p}_n \subset \mathcal{O}_K$ are distinct non-zero prime ideals then the canonical map

$$\mathcal{O}_K/\mathfrak{p}_1^{a_1} \cdots \mathfrak{p}_n^{a_n} \longrightarrow \mathcal{O}_K/\mathfrak{p}_1^{a_1} \oplus \cdots \oplus \mathcal{O}_K/\mathfrak{p}_n^{a_n}$$

is an isomorphism.

Valuations

Let K be a number field and let $x \in K^*$. Then

$$(x) = \prod \mathfrak{p}_i^{a_i}$$

for some distinct non-zero prime ideals \mathfrak{p}_i and $n_i \in \mathbb{Z}$, and we define

$$\text{ord}_{\mathfrak{p}_i}(x) = n_i.$$

$\text{ord}_{\mathfrak{p}}$ has the following properties:

1. $\text{ord}_{\mathfrak{p}}(xy) = \text{ord}_{\mathfrak{p}}(x) + \text{ord}_{\mathfrak{p}}(y)$.
2. $\text{ord}_{\mathfrak{p}}(x + y) \geq \min(\text{ord}_{\mathfrak{p}}(x), \text{ord}_{\mathfrak{p}}(y))$.
3. $x \in \mathcal{O}_K \setminus \{0\} \iff \text{ord}_{\mathfrak{p}}(x) \geq 0$ for all non-zero prime ideals \mathfrak{p} .

Norms of ideals

If $I \subseteq \mathcal{O}_K$ is an ideal, then the *norm* of I is defined by

$$N(I) = \begin{cases} 0 & \text{if } I = (0) \\ (\mathcal{O}_K : I) & \text{if } I \neq (0). \end{cases}$$

The norm has the following two properties:

1. $N((\alpha)) = |\text{N}_{K/\mathbb{Q}}(\alpha)|$ for all $\alpha \in \mathcal{O}_K$.
2. $N(IJ) = N(I)N(J)$.

For any $n \in \mathbb{Z}$, there are only finitely many ideals in \mathcal{O}_K with norm n .

Decomposition of primes in \mathcal{O}_K

Let \mathfrak{p} be a non-zero prime ideal in \mathcal{O}_K . The *residue field* of \mathfrak{p} is $k(\mathfrak{p}) = \mathcal{O}_K/\mathfrak{p}$. This is a finite field, of characteristic $p > 0$ for some prime $p \in \mathbb{Z}$. We say that \mathfrak{p} *lies above* p , and write $\mathfrak{p} \mid p$. The *degree* of \mathfrak{p} is $f(\mathfrak{p}) = \deg(\mathfrak{p}) = [k(\mathfrak{p}) : \mathbb{F}_p]$, and so

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

Observe that if $n \in \mathbb{Z}$ then

$$\mathfrak{p} \mid (n) \iff n \in \mathfrak{p} \iff n = 0 \in k(\mathfrak{p}) \iff p \mid n.$$

So $\mathfrak{p} \mid (p)$ but $\mathfrak{p} \nmid (q)$ for all primes $q \neq p$. Now fix a prime p and decompose (p) as

$$(p) = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_r^{e_r},$$

where the \mathfrak{p}_i are distinct non-zero prime ideals. Then the \mathfrak{p}_i are precisely the prime ideals lying above p . We define the *ramification index* of \mathfrak{p}_i to be $e(\mathfrak{p}_i) = e_i$. We say that \mathfrak{p}_i is *ramified* if $e_i > 1$, or *unramified* otherwise. p is called *ramified* if there exists a \mathfrak{p} lying above p such that \mathfrak{p} is ramified.

Finally, if

$$(p) = \prod_{\mathfrak{p} \mid p} \mathfrak{p}^{e(\mathfrak{p})}$$

as above, then

$$\sum_{\mathfrak{p} \mid p} e(\mathfrak{p})f(\mathfrak{p}) = [K : \mathbb{Q}] = n.$$

The Ideal Class Group

The *ideal class group* of K , written Cl_K , is the group of equivalence classes of fractional ideals in K , where two fractional ideals I, J are said to be equivalent, written $I \sim J$, if there exists $\alpha \in K^*$ such that $I = (\alpha)J$. Every ideal class has a representative $I \subseteq \mathcal{O}_K$.

The ideal class group is always finite. The *class number* of K is $h_K = |Cl_K|$.

Minkowski's Theorem

Suppose $S \subseteq \mathbb{R}^n$ is centrally symmetric, convex and measurable. If $\Gamma \subset \mathbb{R}^n$ is a lattice such that

$$\text{vol}(S) > 2^n \text{vol}(\mathbb{R}^n/\Gamma)$$

then there exists a non-zero point $\alpha \in \Gamma \cap S$. Moreover, if S is also compact then such an α exists when

$$\text{vol}(S) = 2^n \text{vol}(\mathbb{R}^n/\Gamma).$$

Proof of the finiteness of the ideal class group

See lecture notes.

The Minkowski bound

Every class in Cl_K is represented by an ideal $I \subseteq \mathcal{O}_K$ with

$$N(I) \leq \frac{n!}{n^n} \left(\frac{4}{\pi}\right)^{r_2} |D_K|^{1/2}.$$

The Minkowski bound gives us a lower bound on the discriminant of a number field.

The Kummer–Dedekind Theorem

Let $K = \mathbb{Q}(\alpha)$ be a number field with $\alpha \in \mathcal{O}_K$. Let f be the minimal polynomial for α over \mathbb{Q} and let p be a prime number such that $p \nmid (\mathcal{O}_K : \mathbb{Z}[\alpha])$. Write

$$\bar{f} = \bar{g}_1^{e_1} \cdots \bar{g}_r^{e_r}$$

in $\mathbb{F}_p[X]$, where \bar{g}_i are distinct irreducible monic polynomials. Choose representatives $g_i \in \mathbb{Z}[X]$ for the \bar{g}_i and put $\mathfrak{p}_i = (p, g_i(\alpha)) \subseteq \mathcal{O}_K$. Then $\mathfrak{p}_1, \dots, \mathfrak{p}_r$ are distinct prime ideals in \mathcal{O}_K with

$$f(\mathfrak{p}_i) = \deg(\mathfrak{p}_i) = \deg(\bar{g}_i),$$

and (p) decomposes as

$$(p) = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_r^{e_r}.$$

Consequences

1. Under the assumptions of the Kummer–Dedekind Theorem, p is ramified in K/\mathbb{Q} iff $p \mid D_K$.
2. Only finitely many primes p ramify in K/\mathbb{Q} .

Quadratic Fields

There follows a collection of results regarding quadratic fields.

Quadratic extensions

Let K/\mathbb{Q} be a quadratic extension. Then $K = \mathbb{Q}(\alpha)$, where $\alpha \in K$ has minimal polynomial

$$f(X) = X^2 + bX + c$$

over \mathbb{Q} . Since f is irreducible, $b^2 - 4c$ is not a square in \mathbb{Q} . Thus $\alpha = (-b \pm \sqrt{b^2 - 4c})/2$ and so in fact $K = \mathbb{Q}(\sqrt{d})$, where $d = b^2 - 4c \in \mathbb{Q}$. Furthermore, we may assume that $d \in \mathbb{Z}$, by multiplying by the square of the denominator of d , and we may assume that d is squarefree, by dividing by any repeated factor. The resulting d cannot be 0 or 1 since otherwise d would have to have been a square originally.

Conversely, if $d \in \mathbb{Z} \setminus \{0, 1\}$ is squarefree, then \sqrt{d} has minimal polynomial

$$f(X) = X^2 - d$$

over \mathbb{Q} and hence $\mathbb{Q}(\sqrt{d})/\mathbb{Q}$ is a quadratic extension.

Therefore the quadratic number fields are just $\mathbb{Q}(\sqrt{d})$, where $d \in \mathbb{Z} \setminus \{0, 1\}$ is squarefree. If we have two such values $d_1 \neq d_2$ then it is easy to see that $\mathbb{Q}(\sqrt{d_1}) \neq \mathbb{Q}(\sqrt{d_2})$.

In what follows d is assumed to satisfy this condition and K is taken to be $\mathbb{Q}(\sqrt{d})$.

The ring of integers

Let $\alpha = a + b\sqrt{d} \in K$, where $a, b \in \mathbb{Q}$. Then either

1. $b = 0$, in which case $\alpha \in \mathcal{O}_K$ iff $a \in \mathbb{Z}$, or
2. $b \neq 0$, in which case α satisfies $(X - a)^2 - b^2d = 0$, and so since $\alpha \notin \mathbb{Q}$ the minimal polynomial of α is

$$X^2 - 2aX + (a^2 - b^2d).$$

But $\alpha \in \mathcal{O}_K$ iff the minimal polynomial of α is in $\mathbb{Z}[X]$, and so $\alpha \in \mathcal{O}_K$ iff

$$\begin{aligned} 2a &\in \mathbb{Z} \\ a^2 - b^2d &\in \mathbb{Z}. \end{aligned}$$

Now either

- (a) $a \in \mathbb{Z}$, in which case $b^2d \in \mathbb{Z}$ and, since d is squarefree, $b \in \mathbb{Z}$, or
- (b) $a \in \mathbb{Z} + \frac{1}{2}$, in which case $b^2d \in \mathbb{Z} + \frac{1}{4}$. But then $(2b)^2d \in 4\mathbb{Z} + 1$ and so $b \in \mathbb{Z} + \frac{1}{2}$ and $d \equiv 1 \pmod{4}$.

Therefore, if $d \not\equiv 1 \pmod{4}$ then $\alpha \in \mathcal{O}_K$ iff $a, b \in \mathbb{Z}$, and if $d \equiv 1 \pmod{4}$ then $\alpha \in \mathcal{O}_K$ iff $a, b \in \mathbb{Z}$ or $a, b \in \mathbb{Z} + \frac{1}{2}$. We may summarise this as

$$\mathcal{O}_K = \begin{cases} \mathbb{Z} + \mathbb{Z}\sqrt{d} & \text{if } d \not\equiv 1 \pmod{4} \\ \mathbb{Z} + \mathbb{Z}\frac{1+\sqrt{d}}{2} & \text{if } d \equiv 1 \pmod{4}. \end{cases}$$

If we define

$$\theta = \begin{cases} \sqrt{d} & \text{if } d \not\equiv 1 \pmod{4} \\ \frac{1+\sqrt{d}}{2} & \text{if } d \equiv 1 \pmod{4} \end{cases}$$

then $\mathcal{O}_K = \mathbb{Z} + \mathbb{Z}\theta$ and so $\{1, \theta\}$ is an integral basis for K .

The discriminant

The minimal polynomial for θ is

$$f(X) = \begin{cases} X^2 - d & \text{if } d \not\equiv 1 \pmod{4} \\ X^2 - X + \frac{1-d}{4} & \text{if } d \equiv 1 \pmod{4}. \end{cases}$$

and so the discriminant of K is

$$D_K = \begin{cases} 4d & \text{if } d \not\equiv 1 \pmod{4} \\ d & \text{if } d \equiv 1 \pmod{4}. \end{cases}$$

Norm and trace

Write $\overline{a + b\sqrt{d}}$ to mean $a - b\sqrt{d}$, the conjugate of $a + b\sqrt{d}$. Then

$$\begin{aligned} N_{K/\mathbb{Q}}(x + y\theta) &= (x + y\theta)\overline{(x + y\theta)} \\ &= (x + y\theta)(x + y\bar{\theta}) \\ &= \begin{cases} x^2 - dy^2 & \text{if } d \not\equiv 1 \pmod{4} \\ x^2 + xy + \left(\frac{1-d}{4}\right)y^2 & \text{if } d \equiv 1 \pmod{4} \end{cases} \end{aligned}$$

and

$$\begin{aligned} \text{Tr}_{K/\mathbb{Q}}(x + y\theta) &= x \text{Tr}_{K/\mathbb{Q}}(1) + y \text{Tr}_{K/\mathbb{Q}}(\theta) \\ &= \begin{cases} 2x & \text{if } d \not\equiv 1 \pmod{4} \\ 2x + y & \text{if } d \equiv 1 \pmod{4}. \end{cases} \end{aligned}$$

A simpler expression is

$$\begin{aligned} N_{K/\mathbb{Q}}(a + b\sqrt{d}) &= a^2 - db^2 \\ \text{Tr}_{K/\mathbb{Q}}(a + b\sqrt{d}) &= 2a. \end{aligned}$$

Units

Let K be an imaginary quadratic field ($d < 0$) and let $\alpha = x + y\theta$. Then α is a unit iff $N_{K/\mathbb{Q}}(\alpha) = \pm 1$. Now if $d \not\equiv 1 \pmod{4}$ then

$$N_{K/\mathbb{Q}}(\alpha) = x^2 + (-d)y^2 = \pm 1$$

and so $x = \pm 1, y = 0$, or $d = -1$ and $x = 0, y = \pm 1$. If $d \equiv 1 \pmod{4}$ then

$$\begin{aligned} N_{K/\mathbb{Q}}(\alpha) &= x^2 + xy + \left(\frac{1-d}{4}\right)y^2 = \pm 1 \\ (2x + y)^2 + (-d)y^2 &= \pm 4 \end{aligned}$$

and so $x = \pm 1, y = 0$, or $d = -3$ and either $x = 0, y = \pm 1$, or $x = 1, y = -1$, or $x = -1, y = 1$.

To summarise, the units in an imaginary quadratic field are

$$\begin{aligned} \{\pm 1, \pm i\} & \quad \text{if } d = -1 \\ \{\pm 1, \pm \rho, \pm \rho^2\} & \quad \text{if } d = -3 \\ \{\pm 1\} & \quad \text{otherwise} \end{aligned}$$

where $\rho = \frac{1 + \sqrt{-3}}{2}$.

Now let K be a real quadratic field ($d > 0$). The only roots of unity in \mathcal{O}_K are ± 1 , since $K \subset \mathbb{R}$. Therefore by Dirichlet's Units Theorem, the units in \mathcal{O}_K are

$$\mathcal{O}_K^* = \{\pm \epsilon^r \mid r \in \mathbb{Z}\},$$

where ϵ is a *fundamental unit*, computed using the algorithm described on page 6.

The ideal class group

Here are the class numbers of some quadratic fields: h gives the class number of $\mathbb{Q}(\sqrt{d})$ and h' gives the class number of $\mathbb{Q}(\sqrt{-d})$.

d	h	h'	d	h	h'	d	h	h'	d	h	h'
1	—	1	26	2	6	53	1	6	78	2	4
2	1	1	29	1	6	55	2	4	79	3	5
3	1	1	30	2	4	57	1	4	82	4	4
5	1	2	31	1	3	58	2	2	83	1	3
6	1	2	33	1	4	59	1	3	85	2	4
7	1	1	34	2	4	61	1	6	86	1	10
10	2	2	35	2	2	62	1	8	87	2	6
11	1	1	37	1	2	65	2	8	89	1	12
13	1	2	38	1	6	66	2	8	91	2	2
14	1	4	39	2	4	67	1	1	93	1	4
15	2	2	41	1	8	69	1	8	94	1	8
17	1	4	42	2	4	70	2	4	95	2	8
19	1	1	43	1	1	71	1	7	97	1	4
21	1	4	46	1	4	73	1	4			
22	1	2	47	1	5	74	2	10			
23	1	3	51	2	2	77	1	8			

In fact, the only imaginary quadratic fields which are UFDs are $\mathbb{Q}(\sqrt{d})$ where $d = -1, -2, -3, -7, -11, -19, -43, -67$ or -163 . If $d = -1, -2, -3, -7$ or -11 then $\mathbb{Q}(\sqrt{d})$ is norm-Euclidean; if $d = 19, -43, -67$ or -163 then $\mathbb{Q}(\sqrt{d})$ is *not* Euclidean.

The real norm-Euclidean quadratic fields are precisely those with $d = 2, 3, 5, 6, 7, 11, 13, 17, 19, 21, 29, 33, 37, 41, 55$ or 73 . It is not known whether there exists a real quadratic field which is Euclidean but not norm-Euclidean.

Decomposition of primes: the Kummer–Dedekind Theorem

Let $\beta = \sqrt{d}$, so the minimal polynomial of β is $g(X) = X^2 - d$ and $(\mathcal{O}_K : \mathbb{Z}[\beta]) \leq 2$. Let p be an odd prime. Then

1. If $p \mid d$ then $X^2 - d \equiv X^2 \pmod{p}$.
2. If $p \nmid d$ and d is not a quadratic residue modulo p then $X^2 - d$ is irreducible modulo p .
3. If $d \equiv a^2 \pmod{p}$ then $X^2 - d \equiv (X - a)(X + a) \pmod{p}$.

Thus by the Kummer–Dedekind Theorem,

1. In case (1) we have that $(p) = (p, \sqrt{d})^2$.
2. In case (2) we have that (p) is prime.
3. In case (3) we have that $(p) = (p, \sqrt{d} - a)(p, \sqrt{d} + a)$.