Algebraic number theory

F.Beukers

February 2011

1 Algebraic Number Theory, a crash course

1.1 Number fields

Let K be a field which contains $\mathbb{Q}$. Then K is a $\mathbb{Q}$-vector space.
We call K a *number field* if $\dim_{\mathbb{Q}}(K) < \infty$. The number $\dim_{\mathbb{Q}}(K)$ is called the *degree* of the number field. Notation: $[K : \mathbb{Q}]$.
Every $\alpha \in \overline{\mathbb{Q}}$ has a minimal polynomial $p(X) \in \mathbb{Q}[z]$, which we normalise by assuming that the leading coefficient is 1. Under these assumption $p(X)$ is uniquely determined and we can speak of *the* minimal polynomial. The *degree* of α is defined as the degree of $p(X)$. Notation $\deg(\alpha)$.

Theorem 1.1.1 *Let K be a number field of degree n. Then,*

1. *For every $\alpha \in K$ we have $\deg(\alpha)$ divides n.*
2. *There exists $\alpha \in K$ such that $\deg(\alpha) = n$. In particular we have*
$$K = \{a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1} \mid a_0, \ldots, a_{n-1} \in \mathbb{Q}\}.$$
3. *There exist n non-trivial field homomorphisms*
$$\sigma_i : K \to \mathbb{C} \quad (i = 1, 2, \ldots, n).$$

The set in item (2) is denoted by $\mathbb{Q}(\alpha)$ or $\mathbb{Q}[\alpha]$.
The homomorphisms in (3) arise as follows. Suppose $K = \mathbb{Q}(\alpha)$ and let $p(X)$ be the minimal polynomial of α. This polynomial, being irreducible over $\mathbb{Q}$, has n distinct complex zeros $\alpha_1, \alpha_2, \ldots, \alpha_n$. For every i the embedding $\sigma_i : K \to \mathbb{C}$ given by
$$\sigma_i : a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1} \mapsto a_0 + a_1\alpha_i + \cdots + a_{n-1}\alpha_i^{n-1}$$
is a field homomorphism. Moreover, every non-trivial field homomorphism $K \to \mathbb{C}$ is necessarily of this form.

ExampleLet $K = \mathbb{Q}(\sqrt[3]{2})$. Then $p(X) = X^3 - 2$. Notice

$$\alpha_1 = \sqrt[3]{2}, \quad \alpha_2 = \omega\sqrt[3]{2}, \quad \alpha_3 = \omega^2\sqrt[3]{2}, \quad , \omega = e^{2\pi i/3}.$$

The embeddings are generated by

$$\sigma_1 : \alpha \mapsto \sqrt[3]{2}, \quad \sigma_2 : \alpha \mapsto \omega\sqrt[3]{2}, \quad \sigma_3 : \alpha \mapsto \omega^2\sqrt[3]{2}.$$

When $\sigma_i(K) \subset \mathbb{R}$ we call σ_i a *real embedding*, when $\sigma_i(K) \not\subset \mathbb{R}$ we call σ_i a *complex embedding*. Note that if σ_i is a complex embedding, then so is σ_i followed by complex conjugation. So the complex embeddings come in pairs. Denote the number of real embeddings by r_1 and the number of pairs of complex embeddings by r_2. Then clearly, $r_1 + 2r_2 = n$, where $n = [K : \mathbb{Q}]$. We shall often make use of the *norm* of an algebraic number. Let K be a number field. Then the norm of $\alpha \in K$ with respect to K is defined by $N(\alpha) = \prod_{i=1}^{n} \sigma_i(\alpha)$. Notice that if the degree of α is d, then $N(\alpha) = (-1)^n a_0^{n/d}$, where a_0 is the constant coefficient of the minimal polynomial. For later use we note the following Lemma.

Lemma 1.1.2 *Choose a $\mathbb{Q}$-basis $\kappa_1, \ldots, \kappa_n$ of the number field K. Then, for any element $\alpha = x_1\kappa_1 + \cdots + x_n\kappa_n$ of K we have the estimate $|N(\alpha)| \leq (C \max_i |x_i|)^n$, where $C = n \max_{i,j} |\sigma_i(\kappa_j)|$.*

The proof consists of a straightforward estimate of

$$|N(a)| = \prod_{i=1}^{n} |x_1\sigma_i(\kappa_1) + \cdots + x_n\sigma_i(\kappa_n)|$$

The *trace* of $\alpha \in K$ is defined by $\mathrm{Tr}(\alpha) = \sum_{i=1}^{n} \sigma_i(\alpha)$.

1.2 Algebraic integers

Let $\alpha \in \overline{\mathbb{Q}}$. The *denominator* of α is defined as the least common multiple of the denominators of the coefficient of the minimal polynomial of α. Notation $\mathrm{den}(\alpha)$. An *algebraic integer* is an algebraic number with denominator 1.

Theorem 1.2.1 *The algebraic integers form a subring of $\overline{\mathbb{Q}}$.*

In addition we have the following Lemma.

Lemma 1.2.2 *Let α be an algebraic number and d its denominator. Then $d\alpha$ is an algebraic integer.*

The proof of this Lemma is not very hard. Suppose the minimal polynomial of α is given by $X^n + a_1X^{n-1} + \cdots + a_{n-1}X + a_n$. Multiply this polynomial by d^n to get $(dX)^n + a_1d \cdot (dX)^{n-1} + \cdots + a_{n-1}d^{n-1} \cdot (dX) + a_nd^n$. Thus we see that the polynomial $X^n + a_1dX^{n-1} + \cdots + a_{n-1}d^{n-1}X + a_nd^n$ is the minimal polynomial of $d\alpha$. Moreover, it has integral coefficients. Hence $d\alpha$ is an algebraic integer. **qed**

Let K be an algebraic number field of degree n. The ring of all algebraic integers in K is called the *ring of integers* in K. Notation: $\mathcal{O}_K$. An important fact is that $\mathcal{O}_K$ is a rank n lattice contained in K.

Theorem 1.2.3 *Let K be an algebraic number field of degree n. Then there exist n algebraic integers $\omega_1, \omega_2, \ldots, \omega_n$ such that*

$$\mathcal{O}_K = \{m_1\omega_1 + m_2\omega_2 + \cdots + m_n\omega_n \mid m_1, m_2, \ldots, m_n \in \mathbb{Z}\}.$$

The numbers ω_i $(i = 1, 2, \ldots, n)$ form a so-called *basis of integers* in K.
The proof of the Theorem uses the idea of lattices. Choose a $\mathbb{Q}$-basis $\kappa_1, \kappa_2, \ldots, \kappa_n$ of K. We consider the $\mathbb{Q}$-linear mapping $\phi : K \to \mathbb{R}^n$ given by

$$\phi : a_1\kappa_1 + a_2\kappa_2 + \cdots + a_n\kappa_n \mapsto (a_1, a_2, \ldots, a_n).$$

Note that $\phi(\mathcal{O}_K)$ is an additive subgroup of $\mathbb{R}^n$. It remains to show that $\phi(\mathcal{O}_K)$ is discrete in $\mathbb{R}^n$ and that it has rank n. The latter is clear. If we denote the denominator of κ_i by d_i we see that $d_i\kappa_i$ is an algebraic integer. Its image under ϕ is d_i times the i-th standard basis vector in $\mathbb{R}^n$.
Finally assume that $\phi(\mathcal{O}_K)$ is not discrete in $\mathbb{R}^n$. Then, to every $\epsilon > 0$ there exists $a \in \mathcal{O}_K, a \neq 0$ such that $|\phi(a)| < \epsilon$. Suppose that $a = a_1\kappa_1 + \cdots + a_n\kappa_n$ with $a_1, \ldots, a_n \in \mathbb{Q}$. Then $|\phi(a)| < \epsilon$ implies $|a_i| < \epsilon$ for all i. Since a is a non-zero algebraic integer we have $|N(a)| \geq 1$. On the other hand, Lemma 1.1.2 gives the upper bound $|N(a)| \leq (C\epsilon)^n$ for some $C > 0$. Combining the estimate we get $1 < (C\epsilon)^n$ which is untenable if ϵ is sufficiently small. Hence $\phi(\mathcal{O}_K)$ is discrete in $\mathbb{R}^n$. As a conseqence we can find n $\mathbb{Z}$-basis vectors of $\phi(\mathcal{O}_K)$ and hence n $\mathbb{Z}$-basis vectors of $\mathcal{O}_K$ itself. **qed**

The integers $\omega_1, \omega_2, \ldots, \omega_n$ such that $\mathcal{O}_K = \langle \omega_1, \omega_2, \ldots, \omega_n \rangle_{\mathbb{Z}}$ is called a *basis of integers* of K.
Example 1 Let $d \in \mathbb{Z}$ with $d \neq 1$ and square-free. Let $K = \mathbb{Q}(\sqrt{d})$. Take any element $\alpha = a + b\sqrt{d}$ with $a, b \in \mathbb{Q}$ and suppose it is integral. The number α satisfies the equation $X^2 - 2aX + a^2 - b^2d = 0$. So we conclude that $2a, a^2 - b^2d \in \mathbb{Z}$. In particular $a \in \mathbb{Z}$ or $a = m + \frac{1}{2}$ for some $m \in \mathbb{Z}$. If $a \in \mathbb{Z}$ then, together with $a^2 - b^2d \in \mathbb{Z}$, this yields $b^2d \in \mathbb{Z}$. Since d is square-free we conclude that $b \in \mathbb{Z}$.
If $a = m + \frac{1}{2}$ for some $m \in \mathbb{Z}$, the number $\frac{1}{2} + b\sqrt{d}$ must be integral. Hence $\frac{1}{4} - b^2d \in \mathbb{Z}$ This is only possible if $b = n + \frac{1}{2}$ for some $n \in \mathbb{Z}$. Hence $\frac{1+\sqrt{d}}{2}$ is integral. This is true if and only if $d \equiv 1 (\text{mod } 4)$. So we conclude the following.

Proposition 1.2.4 *Let d be a square free integer and $d \neq 1$. Let $K = \mathbb{Q}(\sqrt{d})$. Then $\mathcal{O}_K = \mathbb{Z}[\sqrt{d}]$ if $d \not\equiv 1 (\text{mod } 4)$ and $\mathcal{O}_K = \mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right]$ if $d \equiv 1 (\text{mod } 4)$.*

Example 2 Let $d \in \mathbb{Z}_{>1}$ be square-free. Let $K = \mathbb{Q}(\sqrt[3]{d})$. Suppose $\alpha = a + b\sqrt[3]{d} + c\sqrt[3]{d^2}$ is an algebraic integer. Its real value is denoted by α_1. The conjugates are given by $\alpha_2 = a + b\omega\sqrt[3]{d} + c\omega^2\sqrt[3]{d^2}$ and $\alpha_3 = a + b\omega^2\sqrt[3]{d} + c\omega\sqrt[3]{d^2}$ where $\omega = e^{2\pi i/3}$. The sum of these conjugates is $3a$. Hence $3a \in \mathbb{Z}$. Notice also that $\alpha_1 + \omega^2\alpha_2 + \omega\alpha_3 = 3b\sqrt[3]{d}$. Hence $(3b)^3 d \in \mathbb{Z}$. Since d is squarefree this implies that $3b$ should be an integer. Similarly we derive that $3c$ is integral. After some effort we get the following.

Proposition 1.2.5 *Let $d \in \mathbb{Z}_{>1}$ be a square-free integer. Then a basis of the ring of integers in $\mathbb{Q}(\sqrt[3]{d})$ is given by*

$$1, \sqrt[3]{d}, \sqrt[3]{d^2}$$

if $d \not\equiv 1 (\mathrm{mod}\ 9)$ and

$$1, \sqrt[3]{d}, \frac{1 + \sqrt[3]{d} + \sqrt[3]{d^2}}{3}$$

if $d \equiv 1 (\mathrm{mod}\ 9)$.

Let K be a number field and $\omega_1, \ldots, \omega_n$ a basis of integers. The *discriminant* of K is defined as

$$D_K = \det((\sigma_i(\omega_j))_{i,j=1,2,\ldots,n})^2.$$

Note that D_K is independent of the choice of the ω_i.
Let $\alpha \in \mathcal{O}_K$ and suppose $\deg(\alpha) = n$. The discriminant of α is defined by

$$D(\alpha) = \det((\sigma_i(\alpha)^{j-1})_{i,j=1,\ldots,n})^2.$$

Note that by VanderMonde,

$$\begin{aligned} D(\alpha) &= \prod_{i<j} (\sigma_i(\alpha) - \sigma_j(\alpha))^2 \\ &= \prod_{i<j} (\alpha_i - \alpha_j)^2 \end{aligned}$$

where the α_i are the complex and real zeros of the minimal polynomial of α. Note that $D(\alpha)$ is a symmetric function of the α_i, hence $D(\alpha) \in \mathbb{Q}$. Moreover, the lattice generated by $1, \alpha, \ldots, \alpha^{n-1}$ is a rank n sublattice of $\mathcal{O}_K$. Hence it has finite index in $\mathcal{O}_K$, say f. Then $D(\alpha) = D_K f^2$. The number f is also called the *index* of the algebraic integer α.
The above data provide us with an algorithm to determine the ring of integers in an algebraic number field K. Suppose the degree of K is n. First find an algebraic integer α which generates K, i.e. $K = \mathbb{Q}(\alpha)$. So we have the subring of integers $\mathbb{Z}[\alpha] \subset \mathcal{O}_K$. Determine its discriminant $D(\alpha)$. For every integer d whose square divides $D(\alpha)$ we check if there exist algebraic integers of the form

$$\frac{1}{d}(a_0 + a_1\alpha + a_2\alpha^2 + \cdots + a_{n-1}\alpha^{n-1}), \quad a_i \in \mathbb{Z}.$$

It suffices to verify this for all $a_i \in \{0, 1, \ldots, d-1\}$. This is a finite set of algebraic numbers for which we need to determine the minimal polynomial and see whether it has coefficients in $\mathbb{Z}$. Although the algorithm is not very efficient, it at least produces a basis of integers. Along the way one can usually find many shortcuts. For example, instead of determining the complete minimal polynomial it suffices to look at the norm and trace of elements. For fields of large degree or discriminant there exist more efficient algorithms.

Finally we have an important theorem on the units in $\mathcal{O}_K$, denoted by $\mathcal{O}_K^*$.

Theorem 1.2.6 (Dirichlet) *The group $\mathcal{O}_K^*$ is isomorphic to $U \times \mathbb{Z}^{r_1+r-2-1}$, where U is the (finite) group of roots of unity contained in K.*

Examples

1. Note that $r_1 + r_2 - 1 = 0$ if and only if $K = \mathbb{Q}$ or an imaginary quadratic extension of $\mathbb{Q}$. Only in those fields the group of units is finite.

2. $K = \mathbb{Q}(\sqrt{5})$. Then $r_1 = 2, r_2 = 0$ and

$$\mathcal{O}_K^* = \{\pm \left(\frac{1+\sqrt{5}}{2}\right)^k \mid k \in \mathbb{Z}\}$$

3. $K = \mathbb{Q}(\sqrt[3]{2})$. Then $r_1 = 1, r_2 = 1$ and

$$\mathcal{O}_K^* = \{\pm(1+\sqrt[3]{2})^k \mid k \in \mathbb{Z}\}$$

4. $K = \mathbb{Q}(\zeta_7)$ where $\zeta_7 = e^{2\pi i/7}$. Then $r_1 = 0, r_2 = 3$, $\mathcal{O}_K = \mathbb{Z}[\zeta_7]$ and

$$\mathcal{O}_K^* = \{\pm\zeta_7^k(\zeta_7+\zeta_7^{-1})^l(\zeta_7^2+\zeta_7^{-2})^m \mid k = 0, 1, \ldots, 6;\ l, m \in \mathbb{Z}\}$$

5. $K = \mathbb{Q}(2\cos(2\pi/7))$. This is the real subfield of $\mathbb{Q}(\zeta_7)$ of degree 3. We have $r_1 = 3, r_2 = 0$, $\mathcal{O}_K = \mathbb{Z}[2\cos(2\pi i/7)]$ and

$$\mathcal{O}_K^* = \{\pm(\zeta_7+\zeta_7^{-1})^k(\zeta_7^2+\zeta_7^{-2})^l \mid k, l \in \mathbb{Z}\}$$

1.3 Ideals

Let K be an algebraic number field and $\mathcal{O}_K$ its ring of integers. An *ideal* I in $\mathcal{O}_K$ is a non-empty subset of $\mathcal{O}_K$ with the following properties,

1. $a, b \in I \Rightarrow a + b \in I$.

2. $a \in I, r \in \mathcal{O}_K \Rightarrow ra \in I$.

The ideal consisting only of 0 is denoted by (0). Notice that any ideal is an additive subgroup of $\mathcal{O}_K$ because of property (1). Suppose $I \neq (0)$ and let a be a non-zero element of I. Then , if $\omega_1, \ldots, \omega_n$ is an integral basis of K, we see that all products $a\omega_i$ are contained in I because of property (2). These elements are $\mathbb{Q}$-linear independent, so I is a sublattice of $\mathcal{O}_K$ of maxinal rank n. Its index is called the *norm* of the ideal I. Notation: $N(I)$. Notice that $N(I)$ is at the same time the cardinality of the quotient ring $\mathcal{O}_K/I$.
Because any ideal $I \neq (0)$ is a lattice of rank n we see that any ideal I is finitely generated as ideal. In fact, it is known that any ideal in a ring of integers can be generated by one or two elements, depending on the ideal. We shall not prove this here.
A *principal ideal* I is an ideal which can be generated (as ideal) by a single element. More precisely, there exists $\alpha \in I$ such that $I = \{r\alpha | r \in \mathcal{O}_K\}$.

Lemma 1.3.1 *Let I be a principal ideal generated by $a \in \mathcal{O}_K$. Then $N(I) = |N(a)|$.*

To see this, notice that $a\omega_1, \ldots, a\omega_n$ is a $\mathbb{Z}$-basis of I if $\omega_1, \ldots, \omega_n$ is a basis of integers. There exists an $n \times n$-matrix $M = (m_{ij})$ with integral entries such that $a\omega_i = \sum_{j=1}^n m_{ij}\omega_j$ for all i. We need to determine $|\det(M)|$, which of course equals $N(I)$. By taking all embeddings we also see that $(\sigma_i(a\omega_j)) = M(\sigma_i(\omega_j))$. Next take the determinants on both sides to obtain

$$\prod_{i=1}^n \sigma_i(a) \det(\sigma_i(\omega_j)) = \det(M) \det(\sigma_i(\omega_j)).$$

We conclude that $\det(M) = \prod_{i=1}^n \sigma_i(a)$ and after taking absolute values our Lemma follows. **qed**

For later purposes we also consider so-called fractional ideals. A *fractional ideal* J in K is a finitely generated $\mathcal{O}_K$-module. More concretely, a fractional ideal of K is a non-empty subset of K which has the form

$$J = \{r_1a_1 + r_2a_2 + \cdots + r_ma_m | r_1, \ldots, r_m \in \mathcal{O}_K\}$$

for some fixed set $a_1, a_2, \ldots, a_m \in K$. The following easy Lemma characterises such fractional ideals.

Lemma 1.3.2 *Let $J \subset K$. Then J is a fractional ideal if and only if there exists $a \in \mathbb{Z}$ such that aJ (all elements of J multiplied by a) is an ideal in $\mathcal{O}_K$.*

To see this we start with a fractional ideal J. Let $a_1, \ldots, a_m \in K$ be a set of generators. Let D be a common denominator of the a_i. Then DJ is the ideal generated by $Da_1, \ldots, D\alpha_m$. Conversely, if aJ is an ideal, it can be generated by a finite number of elements $b_1, \ldots, b_m$. Hence J is generated by the finite set $b_1/a, \ldots, b_m/a$. **qed**

A *principal fractional ideal* is a fractional ideal generated by one element from K.
Two fractional ideals I, J can be multiplied as follwos.

$$IJ = \{\sum_i a_ib_i | a_i \in I, b_i \in J\}.$$

All sums in this definition are finite sums.
There is also a sum operator on fractional ideals, which is

$$I + J = \{a + b | a \in I, b \in J\}$$

In other words, $I+J$ is the smallest fractional ideal which contains both I and J. But beware, fractional ideals do not form a ring with these two operators. Addition of ideals does not form a group.
With respect to muliplication we have the following theorem.

Theorem 1.3.3 *The non-zero fractional ideals form a group under multiplication.*

We come back to this theorem later, but mention some consequences here. Suppose we have an inclusion of fractional ideals $I \subset J$. Then the product IJ^{-1} is an ideal. This follows by multiplication with J^{-1}, namely $I \subset J$ implies $IJ^{-1} \subset JJ^{-1} = \mathcal{O}_K$.
Another consequence is that $N(IJ) = N(I)N(J)$ for any two ideals. This can be seen from $[\mathcal{O}_K : IJ] = [\mathcal{O}_K : J][J : IJ]$. However, by multiplication with J^{-1} we can see that $[J : IJ] = [\mathcal{O}_K : I]$. We conclude that

$$N(IJ) = [\mathcal{O}_K : IJ] = [\mathcal{O}_K : I][\mathcal{O}_K : J] = N(I)N(J).$$

We note here that inclusion of ideals can be considered as a divisibility property. To get an idea, let us consider two ideals in $\mathbb{Z}$, say $(a), (b)$ and suppose that $(b) \subset (a)$. Then there exists $c \in \mathbb{Z}$ such that $b = ac$. Conversely, if b is a multiple of a, we naturally have $(b) \subset (a)$. So inclusion of ideals can be thought of as a divisibility property. If we now look for the smallest ideal which contains both (a) and (b), then we should look for the greatest common divisor of a and b. And indeed, $(a) + (b) = \{ma + nb | m, n \in \mathbb{Z}\} = (\gcd(a, b))$.
An important class of ideals is formed by the prime ideals. An ideal $\wp$ is called*prime* if it does not equal $\mathcal{O}_K$ and for any $a, b \in \mathcal{O}_K$ with $ab \in \wp$ we have either $a \in \wp$ or $b \in \wp$. We have the following important property.

Proposition 1.3.4 *Every non-zero prime ideal $\wp$ in $\mathcal{O}_K$ is maximal.*

This can be seen as follows. Take any $a \in \mathcal{O}_K$, but $a \notin \wp$. Consider the powers $1, a, a^2, \ldots (\text{mod } \wp)$. Since $\mathcal{O}_K/\wp$ is a finite ring there exist integers $k > l$ such that $a^k \equiv a^l (\text{mod } \wp)$. Since $\wp$ is a prime ideal and $a \notin \wp$ we conclude that $a^{k-l} \equiv 1 (\text{mod } \wp)$. In other words, a^{k-l-1} is the inverse of a modulo $\wp$. Hence $\mathcal{O}_K/\wp$ is a field and we conclude that $\wp$ is maximal. **qed**

A nice consequence of the maximality of prime ideals is the following.

Proposition 1.3.5 *Let I, J be two ideals such that $IJ \subset \wp$ for some prime ideal $\wp$. Then either $I \subset \wp$ or $J \subset \wp$.*

Note that this is in keeping with our interpretation of inclusion of ideals as expressing divisibility.
The proposition can be proved as follows. Suppose that I, J are not contained in $\wp$. Then the ideal $I + \wp$ properly contains $\wp$. By the maximality of $\wp$ we then have $I + \wp = \mathcal{O}_K$. Similarly, $J + \wp = \mathcal{O}_K$. So, $(I + \wp)(J + \wp) = \mathcal{O}_K$. On the other hand, $(I + \wp)(J + \wp) = IJ + I\wp + J\wp + \wp^2 \subset \wp$. So we have a contradiction. We must either have $I \subset \wp$ r $J \subset \wp$.**qed**

There exist many number fields in which every ideal in the integers is principal. Consequently we also have unique factorisation into irreducibles in such rings of integers. However, there also exist number fields where we do not have unique factorisation. The classical example is $\mathbb{Z}[\sqrt{-5}]$. As is well-known the number 9 can be written both as 3×3 and $(2+\sqrt{-5})(2-\sqrt{-5})$. All four factors are irreducible in $\mathbb{Z}[\sqrt{-5}]$. The only units in $\mathbb{Z}[\sqrt{-5}]$ are ±1. So we see that we do not have unique factorisation in $\mathbb{Z}[\sqrt{-5}]$.
However, we do have the following substitute for unique factorisation in rings of integers.

Theorem 1.3.6 (Fundamental theorem of arithmetic) *Let K be a number field and $\mathcal{O}_K$ its ring of integers. Then every non-zero ideal in $\mathcal{O}_K$ can be factored uniquely into a product of prime ideals.*

This theorem and Theorem 1.3.3 follow from the fact that rings of algebraic integers are examples of so-called Dedekind rings.

Definition 1.3.7 *A domain R is called is a Dedekind domain if the following properties hold.*

1. *Every ideal in R is finitely generated (i.e. R is a Noetherian ring)*
2. *Every non-zero prime ideal is maximal.*
3. *R is integrally closed in its quotient field $K = Q(R)$*

The condition on R being integrally closed means that any element of the quotient field K which is a zero of a monic polynomial in $R[X]$ should itself be contained in R. For example, the ring $\mathbb{Z}[\sqrt{5}]$ is not integrally closed in $\mathbb{Q}(\sqrt{5})$ (do you see why?). Fortunately we have the following Proposition.

Proposition 1.3.8 *Let K be a number field and $\mathcal{O}_K$ its ring of integers. Then $\mathcal{O}_K$ is integrally closed in K.*

This establishes property (3) of Dedekind rings for rings of integers. We have established properties (1) and (2) before and we can now conclude that rings of integers in number fields are Dedekind rings. Theorems 1.3.3 and 1.3.6 follow from the main theorem on Dedekind rings.

Theorem 1.3.9 *Let R be a Dedekind ring with quotient field K. Then*

1. *The non-zero fractional ideals in K form a group.*
2. *Every nonzero ideal in R can be written uniquely, up to ordering of factors, as a product of prime ideals.*

1.4 The class group

To quantify how far we are from unique factorisation within a number field K we introduce the *class group*. Denote the group of non-zero fractional ideals by $\mathcal{I}$ and the group of non-zero principal frcational ideals by $\mathcal{P}$. The the quotient $\mathcal{I}/\mathcal{P}$ is called the class group of K. Notation: $\mathrm{Cl}(K)$. We have the following Theorem.

Theorem 1.4.1 *The class group* $\mathrm{Cl}(K)$ *is finite.*

To see this Theorem we use the following Proposition.

Proposition 1.4.2 *Let I be an ideal in $\mathcal{O}_K$. Then I contains a non-zero element $a \in I$ such that*

$$|N(a)| \leq C_K N(I)$$

where $C_K = \frac{n!}{n^n}\frac{4}{\pi}^{r_2}\sqrt{|D_K|}$.

The constant C_K is known as *Minkowski's constant*. The proof of the Proposition we apply Minkowski's Theorem on convex basis and lattices. The lattice we use is $\mathcal{O}_K$. Let $\omega_1, \ldots, \omega_n$ be a basis of integers and consider the embedding

$$\phi : m_1\omega_1 + \cdots + m_n\omega_n \mapsto (m_1, \ldots, m_n) \in \mathbb{R}^n.$$

Then $\phi(\mathcal{O}_K) = \mathbb{Z}^n$. We consider the sublattice of index $N(I)$ given by $\phi(I)$. The convex set we use is given by

$$B_\lambda = \{(x_1, \ldots, x_n) \in \mathbb{R}^n | \sum_{i=1}^{n} |x_1\sigma_i(\omega_1) + \cdots + \sigma_i(\omega_n)| \leq \lambda\} >$$

One can calculate the volume of B_λ to be $2^n \left(\frac{\pi}{4}\right)^{r_2} \frac{\lambda^n}{n!\sqrt{|D_K|}}$. Let us choose λ such that $\lambda^n = n!N(I)\left(\frac{4}{\pi}\right)^{r_2}\sqrt{|D_K|}$. Then Minkowski's Theorem tells us that there is a non-zero element $a \in I$ such that $\phi(a) \in B_\lambda$. We can write down the following estimates. Using that the geometric mean is less than the arithmetic mean we get

$$|N(a)| = \prod_{i=1}^{n} |\sigma_i(a)| \leq \left(\frac{|\sigma_1(a)| + \cdots + |\sigma_n(a)|}{n}\right)^n \leq \left(\frac{\lambda}{n}\right)^n.$$

Because of our choice of λ the inequality $|N(a)| \leq C_K N(I)$ follows. **qed**

To prove finiteness of the number of ideal classes we first note that the number of ideals in $\mathcal{O}_K$ with norm $\leq C_K$ is finite. Denote this set of ideals by $J_1, \ldots, J_r$. Let now I be any ideal. Choose $a \in I$, non-zero, such that $|N(a)| \leq C_K N(I)$. Then aI^{-1} is an ideal with norm $\leq C_K$. Hence $aI^{-1} = J_i$ for some i. So, I is modulo principal fractional ideals equivalent to one of the ideals $J_1^{-1}, \ldots, J_r^{-1}$. We thus conclude that the class group consists of at most r elements. **qed**

The number of elements of $\mathrm{Cl}(K)$ is denoted by $h(K)$, the *class number* of K.

1.5 Factorisation of primes

Let K be a number field of degree n and $\mathcal{O}_K$ its ring of integers. A question of major importance is how prime numbers in $\mathbb{Z}$ factor into ideals in $\mathcal{O}_K$. Let p be a prime in $\mathbb{Z}$. Then we have $(p) = \wp_1^{e_1}\wp_2^{e_2}\cdots\wp_g^{e_g}$ where we assume the $\wp_i$ to be distinct prime ideals. The numbers e_i are called the *ramification indices* corresponding to p. Suppose that $N(\wp_i) = p^{f_i}$. Then we get $p^n = N(p) = p^{e_1 f_1}p^{e_i f_i}\cdots p^{e_g f_g}$. Hence $n = e_1 f_1 + \cdots + e_g f_g$. To see how a particular prime factors in $\mathcal{O}_K$ we use the following Theorem.

Theorem 1.5.1 (Dedekind's criterion) *Let p be a prime in $\mathbb{Z}$ and $\alpha \in \mathcal{O}_K$ such that $K = \mathbb{Q}(\alpha)$ and p does not divide the index of α. Let $A(X)$ be the minimal polynomial of α and let $A(X) \equiv A_1(X)^{e_1}\cdots A_r(X)^{e_r} (\mathrm{mod}\ p)$ be its factorisation into distinct irreducible factors $A_i(X)$ modulo p. Then the ideals $\wp_i = (p, A_i(\alpha))$ are prime ideals and we have $(p) = \wp_1^{e_1}\cdots\wp_r^{e_r}$.*

First of all notice that $\mathcal{O}_K/(p) = \mathbb{Z}[\alpha]/(p)$ because p does not divide the index of α. Hence $\mathcal{O}_K/\wp_i = \mathbb{Z}[\alpha]/\wp_i = \mathbb{Z}[X]/(p, A_i(X))$ Since $A_i(X)$ is irreducible modulo p, the ideal $(p, A_i(X))$ is maximal. Hence $\mathcal{O}_K/\wp_i$ is a field and $\wp_i$ is maximal. In particular it is prime. The number of elements in the residue field $\mathbb{Z}[\alpha]/(p, A_i(\alpha))$ is $p^{\deg(A_i)}$ and hence $N(\wp_i) = p^{\deg(A_i)}$.
Furthermore, one easily checks that

$$\prod_{i=1}^{r}(p, A_i(\alpha)^{e-i}) \subset (p, \prod_{i=1}^{r} A_i(\alpha)^{e_i}) \subset (p).$$

Hence $\wp_1^{e_1}\cdots\wp_r^{e_r} \subset (p)$. The norm of $\wp_1^{e_1}\cdots\wp_r^{e_r}$ is easily seen to be $p^{\sum_i e_i \deg(A_i)} = p^n = N(p)$. Hence we conclude that $\wp_1^{e_1}\cdots\wp_r^{e_r} = (p)$. **qed**

Example Let $d \neq 1$ be a square-free integer and let $K = \mathbb{Q}(\sqrt{d})$. Let p be a prime. The ideal (p) can factor in three possible ways in $\mathcal{O}_K$,

1. (p) is prime. We then say that p is *inert* in $\mathcal{O}_K$.
2. $(p) = \pi_1\pi_2$ where π_1 and π_2 are distinct prime ideals. We say that p *splits* in $\mathcal{O}_K$.
3. $(p) = \wp^2$ for some prime ideal $\wp$. We say that p *ramifies* in $\mathcal{O}_K$.

Proposition 1.5.2 *We have the following properties:*

1. *p ramifies in $\mathcal{O}_K$ if and only if $p|D_K$.*
2. *Suppose p does not divide D_K and p is odd. Then p splits in $\mathcal{O}_K$ if and only if D_K is a quadratic residue modulo p.*
3. *Suppose D_K is odd. Then 2 splits in $\mathcal{O}_K$ if and only if $D_K \equiv 1 (\mathrm{mod}\ 8)$*

We had seen before that $D_k = d$ is $d \equiv 1(\mathrm{mod}\ 4)$ and $D_K = 4d$ otherwise. Suppose first of all that $p \neq 2$. The index of $\sqrt{d}$ in $\mathcal{O}_K$ is either 1 or 2. So we can apply Dedekind's criterion to p and $X^2 - d$. We get,

1. $(p) = (p, \sqrt{d})^2$ if $p|d$.
2. $(p) = (p, a - \sqrt{d})(p, a + \sqrt{d})$ if a satisfies $a^2 \equiv d (\text{mod } p)$.
3. (p) is prime if $x^2 \equiv d (\text{mod } p)$ has no solution.

These three consequences prove our Proposition for $p \neq 2$.
Suppose now that $p = 2$. When $d \not\equiv (\text{mod } 4)$ the algebraic integer $\sqrt{d}$ has index 1 and we can apply Dirichlet's criterion. We get $(2) = (2, \sqrt{d} - d)^2$. Now suppose that $d \equiv 1 (\text{mod } 4)$. Then $\frac{1+\sqrt{d}}{2}$ has index 1. Its minimal polynomial reads $X^2 - X + \frac{1-d}{4}$. It is irreducible modulo 2 if $d \equiv 5 (\text{mod } 8)$ and reducible into $X(X+1) (\text{mod } 2)$ if $d \equiv 1 (\text{mod } 8)$. Using Dedekind's criterion we get our Proposition for $p = 2$. **qed**

In general we say that a prime p *ramifies* in a ring of integers $\mathcal{O}_K$ if at least one of the ramification indices is strictly bigger than 1. There are only finitely many ramifying primes for every number field. More precisely we have:

Theorem 1.5.3 (Dedekind) *A prime p ramifies in the ring of integers of a field K if and only if p divides D_K.*

1.6 Exercises

Exercise 1.6.1 *Let d be a square free integer not equal to 1. Using Proposition 1.2.4 compute the discriminant $\mathbb{Q}(\sqrt{d})$.*

Exercise 1.6.2 *Let d be a square free integer not equal to 1. Using Proposition 1.2.5 compute the discriminant of $\mathbb{Q}(\sqrt[3]{d})$.*

Exercise 1.6.3 *Determine a basis of integers and discriminant of the following number fields,*

1. $\mathbb{Q}(\sqrt[3]{10})$
2. $\mathbb{Q}(\sqrt[4]{2})$
3. $\mathbb{Q}(\sqrt{3}, \sqrt{5})$
4. $\mathbb{Q}(\sqrt{2}, i)$

Exercise 1.6.4 *Determine the group of units in $\mathbb{Q}(\sqrt{-3})$.*

Exercise 1.6.5 *For which fields is the rank of the unit group equal to 1?*

Exercise 1.6.6 *1. Let K be a quadratic extension of $\mathbb{Q}$ and $\alpha, \beta \in K$. Denote the conjugation $K \to K$ by σ. Show that*

$$\begin{vmatrix} \alpha & \beta \\ \sigma(\alpha) & \sigma(\beta) \end{vmatrix}^2 = \begin{vmatrix} \text{Tr}(\alpha^2) & \text{Tr}(\alpha\beta) \\ \text{Tr}(\alpha\beta) & \text{Tr}(\beta)^2 \end{vmatrix}.$$

2. *Let K be any number field and $\sigma_1, \ldots, \sigma_n$ its embeddings in $\mathbb{C}$. Let $\omega_1, \ldots, \omega_n \in K$. Prove that*
$$\det((\sigma_i(\omega_j))_{i,j})^2 = \det((\mathrm{Tr}(\omega_i\omega_j))_{i,j}).$$

3. *Let K be as in the previous part and $\alpha \in K$. Prove that*
$$D(\alpha) = \det((\mathrm{Tr}(\alpha^{i+j-2})_{i,j}).$$

Exercise 1.6.7 *Let p be an odd prime and $\zeta = e^{2\pi i/p}$. It is given that the field $\mathbb{Q}(\zeta)$ hase degree $p-1$ and its ring of integers is $\mathbb{Z}[\zeta]$.*

1. *What is the minimal polynomial of ζ? Show that a basis of integers is given by $1, \zeta, \zeta^2, \ldots, \zeta^{p-2}$.*

2. *Prove that $p = \prod_{k=1}^{p-1}(1-\zeta^k)$*

3. *Show that the discriminant of ζ equals $\pm p^{p-2}$ (hint: use VanderMonde determinants and try $p = 3$ or $p = 5$ first).*

4. *Show that for any integer k the element $(1-\zeta^k)/(1-\zeta)$ is a unit in the ring of integers.*

5. *Show that there exists a unit η such that $p = \eta(1-\zeta)^{p-1}$.*