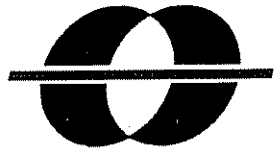


MÄLARDALENS HÖGSKOLA

Code: MdH-IMa-2000:005

BACHELOR THESIS IN MATHEMATICS / APPLIED MATHEMATICS

Quadratic and Cylcotomic fields, and elliptic curves

by

Daniel Ying

Kandidatarbete i matematik / tillämpad matematik

DEPARTMENT OF MATHEMATICS AND PHYSICS
MÄLARDALEN UNIVERSITY
SE-721 23 VÄSTERÅS, SWEDEN

Contents

Introduction

"Cuius rei demonstrationem mirabilem sane detexi hanc marginis exiguitas non caperet "

Pierre de Fermat

Number theory has been studied by mathematicians ever since the old Pythagoreans started looking at the so called Pythagorean triads, that is the three natural numbers that satisfy

$$a^2 + b^2 = c^2.$$

The Babylonian civilisation had earlier noted such triads empirically, but it was first when the Pythagoreans, who searched for truth via proof, were able to give an absolute proof of the existence of such triads, that it became widely known.

Though, the proof of Pythagoras theorem is geometric, number theorists started to investigate other equations, in hope of finding other such beautiful relations. One of the greatest number theorists of the 17th century was Pierre de Fermat (1601-1665). At the time he was working with mathematics, Fermat was studying a copy of the Arithmetica, a book written by Diophantus, which consisted of problems with whole number solutions. And it was while studying this that Fermat made his remarkable observation:

It is impossible for a cube to be written as a sum of two cubes or a fourth power to be written as the sum of two fourth powers, or in general, for any number which is a power greater that the second to be written as a sum of two like powers

That is the equation

$$x^n + y^n = z^n$$

for $0 \neq x, y, z \in \mathbb{Z}$ has no integer solution for $n > 2$.

Fermat, who was known to taunt other mathematicians by admitting he had the proof of a problem but would ask if anyone else had the proof too, was to leave one of the greatest riddles of them all to the rest of the world. After writing his observation, in the margin of Arithmetica, he jotted down an additional comment that would haunt generations of mathematicians:

I have a truly marvellous demonstration of this proposition which this margin is too narrow to contain

Fermat's last theorem, as it has been called, was finally proved by Andrew Wiles in 1993. The proof relies on verifying a conjecture born in the 1950s, the Taniyama-Shimura conjecture.

Many mathematicians before Wiles has attempted to give a full proof of the theorem, but have only succeeded in proving it for special cases such as for all primes $p = n$.

After the time of Fermat, mathematics evolved and number theorist started to realize that in order to solve equations such as $x^n + y^n = z^n$ and even more general $x^a + y^b = z^c$ they would need to have a way of factorising into number that are not elements of the natural numbers. Hence the algebraic numbers was born.

By extending to the algebraic numbers we can factorise the solution to Fermat's equation $x^n + y^n = z^n$ (if one exist that is). This is done by introducing the complex root of unity, $\xi = e^{2\pi i/n}$, i.e. the root of the polynomial $x^n - 1 = 0$. Then we can write $x^n + y^n = z^n$ as

$$(x+y)(x+\xi y)\ldots(x+\xi^n y) = z^n \qquad (1)$$

This factorisation takes place in the ring $Z[\xi]$, where elements are of the form $a_0 + a_1\xi + \ldots + a_r\xi^r$ and each $a_i \in Z$.

In 1847 the French mathematician Lamé announced a proof of Fermat's last theorem. In outline of the proof his proposal was to show that only the case where x, y have no common factors need to be considered, and then deduce that $x+y$, $x+\xi y, \ldots, x+\xi^{n-1}y$ have no common factors. He then argued that a product of relatively prime numbers in (1) can be equal to an nth power only if each of the factors is an nth. So

$$x + y = u_1^{\,n}$$
$$x + \xi y = u_2^{\,n}$$
$$\ldots$$
$$x + \xi^{n-1} y = u_n^{\,n}$$

On this basis Lamé derived a contradiction.

However it was immediately pointed out to him by Liouville that the deduction assumed uniqueness of factorisation. It was later proved by Kummer that uniqueness of factorisation fails in some cases and the first being for $n = 23$.

It was from this fact that the study of quadratic and cyclotomic fields rose and has evolved into what is called Algebraic number theory.

1. Basic algebra and definitions

For most theorems, stated in this chapter, the proofs have been omitted if they don't have any essential calculations that will help us later. The reader is referred to [ST] for complete proofs.

Given a field extension L of a field K and an element $\alpha \in L$, we say that α is algebraic over K if there exists a polynomial $p \in K[t]$ such that $p \neq 0$ and $p(\alpha) = 0$. For α algebraic there exists a unique monic polynomial q of minimal degree, and q is called the minimum polynomial of α over K. The minimum polynomial of α is irreducible over K.

Example:

Finding the minimum polynomial of $i+\sqrt{2}$ in Q:

$\left(x-(i+\sqrt{2})\right)\left(x+(i+\sqrt{2})\right) = x^2-(i+\sqrt{2})^2 = x^2-(-1+2i\sqrt{2}+2) = x^2-1-2i\sqrt{2}$

$\left((x^2-1)-2i\sqrt{2}\right)\left((x^2-1)+2i\sqrt{2}\right) = (x^2-1)^2+4\cdot 2 = x^4-2x^2+9$

Hence $p(x) = x^4-2x^2+9$ is the minimum polynomial of $i+\sqrt{2}$ in Q.

Theorem 1.1

If $L:K$ is a field extension and $\alpha \in L$, then α is algebraic over K if and only if $K(\alpha)$ is a finite extension of K. In this case, $[K(\alpha):K] = \partial p$ where p is the minimum polynomial of α over K, and $K(\alpha) = K[\alpha]$.

Proof:

This is just a sketch of the proof. If $[K(\alpha):K] = n < \infty$ then the powers of $1, \alpha, \alpha^2, \ldots, \alpha^n$ are linearly independent over K, so α is algebraic

Conversely suppose α is algebraic with minimum polynomial p, $\partial p = m$. Then $K(\alpha)$ is the vector space (call it V) over K spanned by $1, \alpha, \alpha^2, \ldots, \alpha^{m-1}$. It follows that $[K(\alpha):K] = \dim_K V = m$

Another useful result we will need later is

Theorem 1.2

Every subgroup H of a free abelian group G of rank n is free of rank $s \leq n$. Moreover there exists a basis $u_1, \ldots, u_n$ for G and positive integers $\alpha_1, \ldots, \alpha_s$ such that $\alpha_1 u_1, \ldots, \alpha_s u_s$ is a basis for H.

Theorem 1.3

Let G be a free abelian group of rank r, and H a subgroup of G. Then G/H is finite if and only if the ranks of G and H are equal. If this is the case, and if G and H have Z-bases $x_1,\ldots,x_r$ and $y_1,\ldots,y_r$ with $y_i = \sum_j a_{ij}x_j$, then

$$|G/H| = |\det(a_{ij})|.$$

The proofs of these two theorems are purely algebraic and will be left out here. The reader is referred to [ST] for a proof of this.

Definition

A complex number α is algebraic if it is algebraic over Q, that is, it satisfies a non-zero polynomial equation with coefficients in Q. The set of algebraic numbers is denoted by A.

Definition

A number field is a subfield K of C such that $[K:Q]$ is finite.

This implies that every element of K is algebraic, and hence $K \subseteq A$. Since A is not finite we will study K. One can prove that if K is a number field then $K = Q(\theta)$ for some algebraic number θ.

If $K = Q(\theta)$ there will in general be several distinct monomorphisms $\sigma_i : K \to C$. For example if we have $K = Q(\sqrt{-3})$ then we have the possibilities

$$\sigma_1(a+b\sqrt{-3}) = a+b\sqrt{-3}$$
$$\sigma_2(a+b\sqrt{-3}) = a-b\sqrt{-3}$$

Theorem 1.4

Let $K = Q(\theta)$ be a number field of degree n over Q. Then there are exactly n distinct monomorphisms $\sigma_i : K \to C$. The elements $\sigma_i(\theta) = \theta_i$ are the distinct zeros in C of the minimum polynomial of θ over Q.

Definition

For each $\alpha \in K = Q(\theta)$ define the field polynomial over K to be

$$f_\alpha(t) = \prod_{i=1}^{n}(t - \sigma_i(\alpha)).$$

Theorem 1.5

The coefficients of the field polynomial are rational numbers, so that $f_\alpha(t) \in Q[t]$.

The elements $\sigma_i(\alpha)$, for $i = 1,\ldots,n$ are called the K-conjugates of α. For $K = Q(\theta)$ the θ_i's are distinct by theorem 1.3 but the K-conjugates are not in general distinct for any element α in K

Theorem 1.6

For a number field $K = Q(\theta)$, and an element $\alpha \in K = Q(\theta)$ we have:

1) The field polynomial f_α is a power of the minimum polynomial.
2) The K-conjugates of α are the zeros of p_α (the minimum polynomial) in C, each repeated n/m times where $m = \partial p_\alpha$ is a divisor of n.
3) The element $\alpha \in Q$ if and only if all of its K-conjugates are equal.
4) $Q(\alpha) = Q(\theta)$ if and only if all K-conjugates of α are distinct.

Proof:

For (1), not that $q = p_\alpha$ is irreducible, and α is a zero of $f = f_\alpha$, so that $f = q`h$ where q and h are coprime and both are monic. We claim that h is constant. If not, some $\alpha_i = \sigma_i(\alpha) = r(\theta_i)$ is a zero of h, where $\alpha = r(\theta)$. Hence if $g(t) = H(r(t))$, then $g(\theta_i) = 0$. Let p be the minimum polynomial of θ over Q, and hence also of each θ_i. Then $p \mid g$, so that $g(\theta_j) = 0$ for all j, and in particular $g(\theta) = 0$

Therefore, $h(\alpha) = h(r(\theta)) = g(\theta) = 0$ and so q divides h, a contradiction. Hence h is constant and monic, so $h = 1$ and $f = q`$

(1) is an immediate consequence of (1)

For (3), it is clear that $\alpha \in Q$ implies that $\sigma_i(\alpha) \in Q$. Conversely if all $\sigma_i(\alpha)$ are equal then, since the zeros of $q = p_\alpha$ are distinct and $f_\alpha = q`$, then $\partial q = 1$ and so $\alpha \in Q$.

Finally for (4), if all θ_i are distinct then $\partial p_\alpha = n$, and hence $[Q(\alpha) : Q] = n = [Q(\theta) : Q]$. This implies that $Q(\alpha) = Q(\theta)$. Conversely if $Q(\alpha) = Q(\theta)$ then $\partial p_\alpha = n$ and so the $\sigma_i(\alpha)$ are distinct

Definition

For a number field $K = Q(\theta)$ of degree n, let $\{\alpha_1,\ldots,\alpha_n\}$ be a basis of K. Then we define the discriminant of this basis to be

$$\Delta[\alpha_1,\ldots,\alpha_n] = \left(\det[\sigma_i(\alpha_j)]\right)^2$$

Note that if we pick another basis $\{\beta_1,\ldots,\beta_n\}$ then $\beta_k = \sum_{i=1}^{n} c_{ik}\alpha_i$, $c_{ik} \in Q$, for $k = 1,\ldots,n$, and $\det(c_{ik}) \neq 0$. From the product formula of determinants and the fact that the σ_i are monomorphisms (and so they are the identity on Q) we get that

$$\Delta[\beta_1,\ldots,\beta_n] = [\det(c_{ik})]^2 \Delta[\alpha_1,\ldots,\alpha_n].$$

Theorem 1.7

The discriminant of any basis for $K = Q(\theta)$ is rational and non-zero. If all K-conjugates of θ are real then the discriminant of any basis is positive.

Definition

A complex number θ is an algebraic integer if there exist a monic polynomial $p(t)$ with integer coefficients such that $p(\theta) = 0$. In other words,

$$\theta^n + a_{n-1}\theta^{n-1} + \ldots + a_1\theta + a_0 = 0$$

where $a_i \in Z$ for all i. Write B for the set of algebraic integers.

From now on in we will call the usual integers (Z), rational integers. The algebraic integers B is a subring of A (see [ST])

Example:

$\theta = \sqrt{-5}$ is an algebraic integer, since it satisfies the monic $\theta^2 + 5 = 0$.

I the field $K = Q(\theta)$ for $\theta = e^{2\pi i/p}$, where p is a prime rational integer, we know that $\theta^p - 1 = 0$ So θ is an algebraic integer. However, $t^p - 1$ is not the minimum polynomial because by theorem 1.1 we must have that $[Q(\theta) : Q] = p - 1 = \partial q$ where q is the minimum polynomial of θ over K. Now, since $\theta - 1 \neq 0$ we get that

$$q(t) = \frac{t^p - 1}{t - 1} = t^{p-1} + t^{p-2} + \ldots + t + 1$$

is the minimum polynomial of θ over K.

Theorem 1.8

Let θ be a complex number satisfying a monic polynomial equation whose coefficients are algebraic integers. Then θ is an algebraic integer.

With this theorem and the result that the algebraic integers B is a subring of A, we can easily form new algebraic integers. Since clearly $\sqrt{3}$ and $\sqrt{5}$ are algebraic integers we get that numbers such as $\sqrt{3} + \sqrt{5}$, $7\sqrt{3} - 9\sqrt{5}$ and $\sqrt{3}(4 + \sqrt{5})^3$ are algebraic integers. Also the zeros of polynomials such as

$$t^7 - (\sqrt{2} + 1)t^4 + (\sqrt{5} - 3)^2 t + (\sqrt{2} + 7\sqrt{5})$$

are algebraic integers by theorem 1.7.

Definition

For any number field K we write

$$\mathcal{D} = K \cap B$$

and call $\mathcal{D}$ the ring of integers of K.

Since K and B are subrings of C, it follows that $\mathcal{D}$ is a subring of K The ring $\mathcal{D}$ of integers of K is an abelian group under addition.

Definition

A Z-basis for $(\mathcal{D},+)$ is called an integral basis for K.

Thus $\{\alpha_1,\ldots,\alpha_n\}$ is an integral basis if and only if all $\alpha_i \in \mathcal{D}$ and every element of $\mathcal{D}$ is uniquely expressible in the form

$$a_1\alpha_1 + \ldots + a_n\alpha_n$$

for rational integers $a_1,\ldots,a_n$.

Theorem 1.9

Every number field K possesses an integral basis, and the additive group of $\mathcal{D}$ is free abelian of rank n equal to the degree of K.

Definition

Let $K = Q(\theta)$ be a number field of degree n and let $\sigma_1,\ldots,\sigma_n$ be the monomorphisms $K \to C$. For any $\alpha \in K$ define the norm

$$N(\alpha) = \prod_{i=1}^{n} \sigma_i(\alpha)$$

and the trace

$$T(\alpha) = \sum_{i=1}^{n} \sigma_i(\alpha).$$

Since the σ_i are monomorphisms the norm is multiplicative, that is

$$N(\alpha\beta) = N(\alpha)N(\beta)$$

and

$$T(p\alpha + q\beta) = pT(\alpha) + qT(\beta)$$

for p,q rational numbers.

Proposition 1.10

Let $K = Q(\theta)$ be a number field where θ has minimum polynomial p of degree n. The Q-basis $\{1,\theta,\ldots,\theta^{n-1}\}$ has discriminant

$$\Delta[1,\theta,\ldots,\theta^{n-1}] = (-1)^{n(n-1)/2} N(Dp(\theta))$$

where Dp is the derivative of p.

2 Quadratic and cyclotomic fields

Quadratic fields

Definition

A quadratic field is a number field K of degree 2 over $\mathbb{Q}$.

Proposition 2.1

The quadratic fields are precisely those of the form $\mathbb{Q}(\sqrt{d})$ for d a square free rational integer.

Proof:

By the definition. $K = \mathbb{Q}(\theta)$ where θ is an algebraic integer and θ is a root of

$$t^2 - at + b = 0,\ (a, b \in \mathbb{Z})$$

Thus

$$\theta = \frac{-a \pm \sqrt{a^2 - 4b}}{2}$$

Let $a^2 - 4b = r^2 d$, where $r, d \in \mathbb{Z}$ and d is square free. Then

$$\theta = \frac{-a \pm \sqrt{a^2 - 4b}}{2},$$

and so $K = \mathbb{Q}(\sqrt{d})$

Examples:

$\mathbb{Q}(\sqrt{-1}), \mathbb{Q}(\sqrt{7}), \mathbb{Q}(\sqrt{-10})$ are quadratic fields where as $\mathbb{Q}(\sqrt{9})$ $\mathbb{Q}(\sqrt{-12})$ are not, since $9 = 3^2$ and $12 = 2^2\ 3$ are not square free.

Now to find the ring of integer of the quadratic field $\mathbb{Q}(\sqrt{d})$:

Theorem 2.2

Let d be a square free rational integer Then the integers of the quadratic field $\mathbb{Q}(\sqrt{d})$ are:

1) $Z[\frac{1}{2} + \frac{1}{2}\sqrt{d}]$ if $d \equiv 1 (\mathrm{mod}\, 4)$.
2) $Z[\sqrt{d}]$ if $d \not\equiv 1 (\mathrm{mod}\, 4)$.

Proof:

A general element in $\mathbb{Q}(\sqrt{d})$ is of the form $\alpha = r + s\sqrt{d}$ for $r, s \in \mathbb{Q}$. Thus $\alpha = \frac{a + b\sqrt{d}}{c}$ for $a, b, c \in \mathbb{Z}$, $c > 0$ and no primes divides a, b or c. Now α is an integer if and only if the coefficients of the minimum polynomial

$$\left(t - \left(\frac{a + b\sqrt{d}}{c}\right)\right)\left(t - \left(\frac{a - b\sqrt{d}}{c}\right)\right)$$

are integers. By doing the multiplication we obtain the following conditions on a, b and c:

$$\frac{a^2 - b^2 d}{c^2} \in \mathbb{Z}, \qquad (1)$$

$$\frac{2a}{c} \in \mathbb{Z} \qquad (2)$$

If a and c have a common prime factor p then (1) implies that p divides b (since d is square free) which contradicts our assumptions for a, b and c. Hence from (2) we have $c = 1$ or $c = 2$. If $c = 1$ then α is an integer of K in any case so suppose $c = 2$. Now a and b must both be odd and $\frac{a^2 - b^2 d}{4} \in \mathbb{Z}$. Hence

$$a^2 - b^2 d \equiv 0 (\mathrm{mod}\, 4)$$

Now an odd number $2k + 1$ has square $4k^2 + 4k + 1 \equiv 1 (\mathrm{mod}\, 4)$, hence $a^2 \equiv b^2 \equiv 1 (\mathrm{mod}\, 4)$, and this implies that $d \equiv 1 (\mathrm{mod}\, 4)$. Conversely, if $d \equiv 1 (\mathrm{mod}\, 4)$ then for odd a and b we have that α is an integer because (1) and (2) holds.

Theorem 2.3

a) If $d \not\equiv 1 (\mathrm{mod}\, 4)$ then $\mathbb{Q}(\sqrt{d})$ has an integer basis of the form $\{1, \sqrt{d}\}$ and discriminant $4d$.

b) If $d \equiv 1 (\mathrm{mod}\, 4)$ then $\mathbb{Q}(\sqrt{d})$ has an integral basis of the form $\{1, \frac{1}{2} + \frac{1}{2}\sqrt{d}\}$ and discriminant d.

Proof:

The monomorphisms $K \to \mathbb{C}$ are given by

$$\sigma_1(r + s\sqrt{d}) = r + s\sqrt{d}$$
$$\sigma_2(r + s\sqrt{d}) = r - s\sqrt{d}$$

So by theorem 2.2 we know the bases and can therefore compute the discriminants:

$$\begin{vmatrix} 1 & \sqrt{d} \\ 1 & -\sqrt{d} \end{vmatrix}^2 = (-2\sqrt{d})^2 = 4d$$

$$\begin{vmatrix} 1 & \frac{1}{2}+\frac{1}{2}\sqrt{d} \\ 1 & \frac{1}{2}-\frac{1}{2}\sqrt{d} \end{vmatrix}^2 = (-\sqrt{d})^2 = d$$

Since the discriminant of isomorphic fields are equal, no quadratic fields $Q(\sqrt{d})$, with distinct square free d are isomorphic.

Examples:

With the help of the above theorems we can find the integral bases and discriminants for quadratic fields. We have in

$Q(\sqrt{3})$: $3 \not\equiv 1 (\mathrm{mod}\, 4)$ so $Q(\sqrt{3})$ has integral basis $\{1, \sqrt{3}\}$ and discriminant $4 \cdot 3 = 12$.

$Q(\sqrt{-7})$: $-7 \equiv 1 (\mathrm{mod}\, 4)$ so $Q(\sqrt{-7})$ has integral basis $\{\frac{1}{2}, \frac{1}{2}\sqrt{-7}\}$ and discriminant -7.

$Q(\sqrt{-6})$: $-6 \not\equiv 1 (\mathrm{mod}\, 4)$ so $Q(\sqrt{-6})$ has integral basis $\{1, \sqrt{-6}\}$ and discriminant $4 \cdot (-6) = -24$.

Cyclotomic fields

Definition

A cyclotomic field is a number field K of the form $\mathbb{Q}(\xi)$ where $\xi = e^{2\pi i/p}$ is a primitive complex mth root of unity and p is an odd rational prime.

Lemma 2.4

The minimum polynomial of $\xi = e^{2\pi i/p}$, p an odd rational prime, over $\mathbb{Q}$ is

$$f(t) = t^{p-1} + \ldots + t^2 + t + 1.$$

The degree of $\mathbb{Q}(\xi)$ is $p-1$.

Proof:

Consider the polynomial

$$f(t) = \frac{t^p - 1}{t - 1} = t^{p-1} + \ldots + t^2 + t + 1$$

Since $\xi^p - 1 = 0$ and $\xi - 1 \neq 0$, it follows that $f(t) = 0$ Hence we need only to show that f is irreducible

Now we have $f(t+1) = \dfrac{(t+1)^p - 1}{t} = \displaystyle\sum_{r=1}^{p} \binom{p}{r} t^{r-1}$.

The binomial coefficient $\binom{p}{r}$ is divisible by p if $1 \leq r \leq p-1$, and $\binom{p}{1} = p$ is not divisible by p^2

Hence, by Eisenstein's criterion $f(t+1)$ is irreducible. Therefore $f(t)$ is irreducible and is the minimum polynomial of ξ.

Since the degree of f is $p-1$ we have $[\mathbb{Q}(\xi) : \mathbb{Q}] = p-1$ by theorem 1.1.

By looking at the unit circle we also see that $\xi^2, \xi^3, \xi^4, \ldots, \xi^{p-1}$ are roots of unity not equal to 1, and so they also have f as minimum polynomial. Also

$$f(t) = (t-\xi)(t-\xi^2)\cdots(t-\xi^{p-1}),$$

so the monomorphisms $\mathbb{Q}(\xi) \to \mathbb{C}$ are given by $\sigma_i(\xi) = \xi^i$ for $1 \leq i \leq p-1$. Now a basis for $\mathbb{Q}(\xi)$ is $\{1, \xi, \xi^2, \ldots, \xi^{p-2}\}$ so a general element of $\mathbb{Q}(\xi)$ is of the form $\alpha = a_0 + a_1\xi + \ldots + a_{p-2}\xi^{p-2}$ and we have $\sigma_i(\alpha) = a_0 + a_1\xi^i + \ldots + a_{p-2}\xi^{i(p-2)}$.

From this we can calculate the norm and trace:

$$N(\alpha) = \prod_{i=1}^{p-1} \sigma_i(\alpha) \text{ and } T(\alpha) = \sum_{i=1}^{p-1} \sigma_i(\alpha).$$

Now to do some special cases of the norms and traces of elements in a cyclotomic field we start by looking at the norm of ξ. By the definition we have $N(\xi) = \xi\xi^2\xi^3\ldots\xi^{p-1}$ and since $\xi\xi^{p-1} = \xi^p = 1$ and $p-1$ is even all pairs match up and we get $N(\xi) = 1$. Now since the norm is multiplicative we can write $N(\xi^i) = (N(\xi))^i = (1)^i = 1$ for $1 \leq i \leq p-1$

The trace of ξ is easily calculated by using the fact that the minimal polynomial of ξ is zero and so we get $T(\xi) = \xi + \xi^2 + \ldots + \xi^{p-1} = -1$ and $T(\xi^i) = T(\xi) = -1$ for $1 \le i \le p-1$.

Now for any element $a \in \mathbb{Q}$ we have $N(a) = a^{p-1}$ and $T(a) = (p-1)a$.
Because the exponent of ξ always can be reduced modulo p we can extend the above formulas to

$$\begin{aligned} N(\xi^r) &= 1, && \forall r \in \mathbb{Z} \\ T(\xi^r) &= -1, && r \not\equiv 0 (\mathrm{mod}\ p) \\ T(\xi^r) &= p-1 && r \equiv 0 (\mathrm{mod}\ p) \end{aligned}$$

We can calculate the trace for a general element of $\mathbb{Q}(\xi)$ by

$$T\left(\sum_{i=0}^{p-2} a_i \xi^i\right) = \sum_{i=0}^{p-2} T(a_i \xi^i) = T(a_0) + \sum_{i=1}^{p-2} T(a_i \xi^i) = (p-1)a_0 - \sum_{i=1}^{p-2} a_i$$

The case of the norm of a general element is more complicated, but a special case that will be used later is

$$N(1-\xi) = \prod_{i=1}^{p-1} (1-\xi^i) = f(1) = p.$$

Now that we have learned about these tools we can use them to show the following:

Theorem 2.5

The ring of integers $\mathcal{D}$ of $\mathbb{Q}(\xi)$ is $\mathbb{Z}(\xi)$.

Proof:

Suppose $\alpha = a_0 + a_1\xi + \ldots + a_{p-2}\xi^{p-2}$ is an integer in $\mathbb{Q}(\xi)$. then we have to show that the rational coefficients are actually rational integers.
Now for $0 \le k \le p-2$ the element $\alpha\xi^{-k} - \alpha\xi$ is an integer and so the trace of it is a rational integer Hence,

$$\begin{aligned} T(\alpha\xi^{-k} - \alpha\xi) &= T(a_0\xi^{-k} + \ldots + a_k + \ldots + a_{p-2}\xi^{p-k-2} - a_0\xi - \ldots a_{p-2}\xi^{p-1}) = \\ &= pa_k - (a_0 + \ldots + a_{p-2}) - (-a_0 - \ldots - a_{p-2}) = pa_k \end{aligned}$$

so if we let $b_k = pa_k$, this is a rational integer.
Put $\lambda = 1 - \xi$. then

$$p\alpha = b_0 + b_1\xi + b_{p-2}\xi^{p-2} = c_0 + c_1\lambda + \ldots + c_{p-2}\lambda^{p-2} \qquad (*)$$

where

$$c_i = \sum_{j=i}^{p-2} (-1)^j \binom{j}{i} b_j$$

All c_i are here divisible by p. By induction, we assume this for all c_i with $i \le k-1$, where $0 \le k \le p-2$. Since $c_0 = b_0 + \ldots + b_{p-2} = p(-T(\alpha) + b_0)$, we have $p \mid c_0$, so it is true for $k = 0$. Now by our previous discussion about the norm of $N(1-\xi)$ we get

$$p = \prod_{i=1}^{p-1}(1-\xi^i) = (1-\xi)^{p-1}\prod_{i=1}^{p-1}(1+\xi+\ldots+\xi^{i-1}) = \lambda^{p-1}\kappa,$$

where $\kappa \in \mathbb{Z}[\xi] \subseteq \mathcal{D}$. Now by considering (*) as congruence modulo the ideal $\langle \lambda^{k+1} \rangle$ of $\mathcal{D}$. We then have by the last equation $p \equiv 0(\mathrm{mod}\langle \lambda^{k+1} \rangle)$ and so the left hand side of (*) and the terms up to $c_{k-1}\lambda^{k-1}$ vanishes, further the terms from $c_{k+1}\lambda^{k+1}$ and onwards are just multiples of λ^{k+1} so they vanish too. We're left with $c_k\lambda^k \equiv 0(\mathrm{mod}\langle \lambda^{k+1} \rangle)$. Hence $c_k\lambda^k = \mu\lambda^{k+1}$ for some $\mu \in \mathcal{D}$, from which we get $c_k = \mu\lambda$. Now by taking norms we get

$$c_k^{p-1} = N(c_k) = N(\mu)N(\lambda) = pN(\mu),$$

since $N(\lambda) = N(1-\xi) = p$. Hence $p \mid c_k^{p-1}$, so $p \mid c_k$. Hence by the induction hypothesis $p \mid c_k, \forall k$, and then (*) shows that $p \mid b_k, \forall k$. Therefore $a_k \in \mathbb{Z}, \forall k$ which proves the theorem.

From this theorem we see that as a basis for the ring of integers $\mathcal{D}$ of $\mathbb{Q}(\xi)$ we can take $\{1, \xi, \ldots, \xi^{p-2}\}$.
Now to compute the discriminant we make use of some of the previous results about discriminants.

Theorem 2.6

The discriminant of $\mathbb{Q}(\xi)$, where $\xi = e^{2\pi i/p}$ and p is an odd rational prime, is $(-1)^{(p-1)/2}p^{p-2}$.

Proof:

Since the integral basis is $\{1, \xi, \ldots, \xi^{p-2}\}$ we can make use of proposition 1.10, which tells us that the discriminant is equal to

$$(-1)^{(p-1)(p-2)/2}N(Df(\xi))$$

where $f(t)$ is the minimal polynomial. Since p is odd the first factor reduces to $(-1)^{(p-1)/2}$.
The second factor comes from

$$f(t) = \frac{t^p - 1}{t-1} \quad \text{and} \quad Df(t) = \frac{(t-1)pt^{p-1} - (t^p - 1)}{(t-1)^2}$$

which gives

$$Df(\xi) = \frac{-p\xi^{p-1}}{\lambda}$$

Hence

$$N(Df(\xi)) = \frac{N(p)N(\xi)^{p-1}}{N(\lambda)} = \frac{(-p)^{p-1}1^{p-1}}{p} = p^{p-2}$$

One can easily check that this seems reasonable by noting that in the case of $p=3$, $\mathbb{Q}(\xi)$ is a quadratic field, and our two formulas for the discriminant matches up. To see this note that the degree of $\mathbb{Q}(e^{2\pi i/3})$ is $p-1=2$, so it is a quadratic field and since

$$e^{2\pi i/3}=\frac{-1+\sqrt{3}}{2}$$

it is equal to $\mathbb{Q}(\sqrt{3})$. The discriminant of $\mathbb{Q}(e^{2\pi i/3})$ is $(-1)^{2/2}3^1=-3$ by theorem 2.6 and for the quadratic field $\mathbb{Q}(\sqrt{3})$, since $-3\equiv 1(\mathrm{mod}\,4)$, the discriminant is -3.

Example:

Let $K=\mathbb{Q}(\xi)$ where $\xi=e^{2\pi i/5}$. We will calculate the norm and trace for the following elements of K: ξ^2, $\xi+\xi^2$ and $1+\xi+\xi^2+\xi^3+\xi^4$.

We know that $N(\xi^r)=(N(\xi))^r$ so $N(\xi^2)=(N(\xi))^2$ and since $N(\xi)=1$, $N(\xi^2)=1$.

Similarly we get the trace $T(\xi^2)=T(\xi)=-1$.

To calculate $N(\xi+\xi^2)$, we will do direct computation by the definition:

$$N(\xi+\xi^2)=\sigma_1(\xi+\xi^2)\sigma_2(\xi+\xi^2)\sigma_3(\xi+\xi^2)\sigma_4(\xi+\xi^2)$$
$$=(\xi+\xi^2)(\xi^2+\xi^4)(\xi^3+\xi^6)(\xi^4+\xi^8)=(\xi+\xi^2)(\xi^2+\xi^4)(\xi^3+\xi)(\xi^4+\xi^3)$$
$$=(\xi^3+\xi^4+1+\xi)(\xi^3+\xi)(\xi^4+\xi^3)=(\xi+\xi^2+\xi^3+\xi^4+\xi^4+1+\xi+\xi^2)(\xi^4+\xi^3)$$
$$=-(1+\xi^3)(\xi^4+\xi^3)=-(\xi^4+\xi^2+\xi^3+\xi)=-(-1)=-1$$

where we have used the fact that $\xi^4+\xi^3+\xi^2+\xi=-1$, from the minimum polynomial of ξ.

The trace becomes

$$T(\xi+\xi^2)=\sigma_1(\xi+\xi^2)+\sigma_2(\xi+\xi^2)+\sigma_3(\xi+\xi^2)+\sigma_4(\xi+\xi^2)$$
$$=(\xi+\xi^2)+(\xi^2+\xi^4)+(\xi^3+\xi)+(\xi^4+\xi^3)=2(\xi+\xi^2+\xi^3+\xi^4)=-2$$

For $1+\xi+\xi^2+\xi^3+\xi^4$, note that from the minimum polynomial we get that $1+\xi+\xi^2+\xi^3+\xi^4=0$. So $N(1+\xi+\xi^2+\xi^3+\xi^4)=N(0)=0$ and similar for the trace $T(1+\xi+\xi^2+\xi^3+\xi^4)=T(0)=0$.

Example:

Let $K = Q(\xi)$ where $\xi = e^{2\pi i/p}$ for a rational prime p. In the ring of integers $Z[\xi]$, $\alpha \in Z[\xi]$ is a unit if and only if $N(\alpha) = \pm 1$.

To see this, suppose α is a unit, then there exist $\beta \in Z[\xi]$ such that $\alpha\beta = 1$. Now by taking norms we get $N(\alpha\beta) = N(1) = 1 = N(\alpha)N(\beta)$ and since the norm is a rational integer, $N(\alpha) = \pm 1$.

Conversely, suppose $N(\alpha) = \pm 1$, then by the definition of the norm $N(\alpha) = \sigma_1(\alpha)\ldots\sigma_{p-1}(\alpha)$. But $\sigma_i(\alpha) = \alpha$ for some $i : 1 \le i \le p-1$, say $i = 1$. Then $\alpha\left|\sigma_2(\alpha)\ldots\sigma_{p-1}(\alpha)\right| = \pm 1$ Hence α is a unit.

Example:

Next we will show that there are 6 units in $Z[\xi]$ for $K = Q(\xi)$ where $\xi = e^{2\pi i/3}$

First note that the minimum polynomial is $P_\xi(x) = x^2 + x + 1$ so $\xi^2 + \xi + 1 = 0$ which implies that $\xi^2 = -(\xi + 1)$. Hence we can take $\{1, \xi\}$ as an integral basis for $Z[\xi]$.

Thus a general element of $Z[\xi]$ is of the form $\alpha = a + b\xi$, so

$N(\alpha) = (a + b\xi)(a + b\xi^2) = a^2 + ab\xi + ab\xi^2 + b^2 = a^2 + b^2 + ab\xi + ab(-\xi - 1)$

$= a^2 - ab + b^2 = (a + b)^2 - 3ab$

Now $a, b \in Z[\xi]$ and are the roots of the equation $x^2 + cx + d = 0$. Hence $c = a + b$ and $d = ab$. Thus

$N(\alpha) = c^2 - 3d$

By our previous result we know that for α to be a unit we must have $N(\alpha) = \pm 1$, so $c^2 - 3d = \pm 1$, which has the only integer solutions:

$c = \pm 1,\ d = 0 \quad \Rightarrow a + b = \pm 1$

$c = \pm 2,\ d = 1 \quad \Rightarrow a + b = \pm 2,\ ab = 1$

This gives us the six solutions:

$$(a, b) = (\pm 1, 0), (0, \pm 1)$$
$$(a, b) = (-1, -1), (1, 1)$$

Hence the units are $1, -1, \xi, -\xi, 1 + \xi, -1 - \xi$.

Example:

Let $K = Q(\xi)$ with $\xi = e^{2\pi i/5}$. For an element α of K of the form $\alpha = a + b\xi$ we have the norm

$$N(\alpha) = N(a+b\xi) = (a+b\xi)(a+b\xi^2)(a+b\xi^3)(a+b\xi^4)$$

$$= (a^2 + ab(\xi+\xi^2) + b\xi^3)(a^2 + ab(\xi^3+\xi^4) + b\xi^2)$$

$$= a^4 + a^3b(\xi+\xi^2+\xi^3+\xi^4) + ab^3(\xi+\xi^2+\xi^3+\xi^4) + a^2b^2\left((\xi+\xi^2)(\xi^3+\xi^4) + (\xi^2+\xi^3)\right) + b^4$$

$$= a^4 - a^3b - ab^3 + a^2b^2(\xi^4 + 1 + 1\xi + \xi^2 + \xi^3) + b^4$$

$$= a^4 - a^3b + a^2b^2 - ab^3 + b^4 = \frac{a^5+b^5}{a+b}$$

Hence we have found a formula for calculating the norm of an element of the form $\alpha = a + b\xi$ in $K = Q(\xi)$ with $\xi = e^{2\pi i/5}$. That is $N(a+b\xi) = \dfrac{a^5+b^5}{a+b}$.

Now we can easily calculate the norm of $\xi+2$, $\xi-2$ and $\xi+3$:

$$N(\xi+2) = \frac{1+2^5}{1+2} = \frac{33}{3} = 11$$

$$N(\xi-2) = \frac{1+(-2)^5}{1-2} = 31$$

$$N(\xi+3) = \frac{1+3^5}{4} = 61$$

But since 11, 31 and 61 are rational prime integers we see that there cannot exist any proper factors $\alpha, \beta \in K$ such that $\alpha\beta = \xi+2$, $\alpha\beta = \xi-2$ or $\alpha\beta = \xi+3$. So $\xi+2$, $\xi-2$ and $\xi+3$ have no proper factors in $Z[\xi]$. Hence they are irreducible and we can factorise 11, 31 and 61 in the following way:

$$11 = (2+\xi)(2+\xi^2)(2+\xi^3)(2+\xi^4)$$

$$31 = (2-\xi)(2-\xi^2)(2-\xi^3)(2-\xi^4)$$

$$61 = (3+\xi)(3+\xi^2)(3+\xi^3)(3+\xi^4)$$

3 Factorisation into irreducibles

When working with the rational integers we know that factorisation is unique into irreducibles. However now that we have introduced other number fields we might ask if such factorisations will work there too. We shall see that this is not the case for all fields and we will classify the fields there after.
First we take a look at some basic facts we know since earlier.

If p is a prime in Z then we have the following

1) If $m \mid p$, then $m = \pm p$ or $m = \pm 1$.
2) If $p \mid mn$, then $p \mid m$ or $p \mid n$.

Definition

An element u in a ring R is a unit if there exists $v \in R$ such that $uv = 1$.

We say that an element x is trivially factorised if $x = uy$ for some unit u. If there exists such a factorisation we say that y is an associate of x. A factorisation, $x = yz$, is said to be proper if none of y and z are zero or units.
Denote the set of units of a ring R by $U(R)$; this set forms a group under multiplication.

Proposition 3.1

The group of units U of the integers in $Q(\sqrt{d})$ where d is a square free negative rational integer is as follows:

a) For $d = -1$, $U = \{\pm 1, \pm i\}$.
b) For $d = -3$, $U = \{\pm 1, \pm\omega, \pm\omega^2\}$ where $\omega = e^{2\pi i/3}$.
c) For all other $d < 0$, $U = \{\pm 1\}$.

Proof:

Suppose α is a unit in the ring of integers of $Q(\sqrt{d})$ with inverse β, then $\alpha\beta = 1$, so taking norms we get $N(\alpha)N(\beta) = 1$. But the norm is a rational integer so $N(\alpha) = \pm 1$. Now, if $\alpha = a + b\sqrt{d}$ the norm is $N(\alpha) = a^2 - db^2$ and so $N(\alpha) = 1$ for negative d. Hence we have to solve the equation

$a^2 - db^2 = 1$.

If $a, b \in Z$, then for $d = -1$, this reduces to $a^2 + b^2 = 1$, which has the only integer solutions $a = \pm 1, b = 0$ or $a = 0, b = \pm 1$. This gives us $U = \{\pm 1, \pm i\}$.

For $d < -3$ we conclude that $b = 0$ or $a^2 - db^2 > 1$. So the only rational integer solutions are $a = \pm 1, b = 0$. If $d \not\equiv 1 \pmod 4$, then $a, b \in Z$, so the only solutions are those already discovered. For $d \equiv 1 \pmod 4$, we must also consider the additional possibility $a = A/2$ and $b = B/2$ where both A and B are odd rational integers. In this case $A^2 - dB^2 = 4$. For $d < -3$ we deduce that $B = 0$ and there are no additional solution. This completes (c).

For $d=-3$, we find additional solutions $A=\pm 1$, $B=\pm 1$. The case $A=1$ and $B=1$, gives $\alpha=\frac{1}{2}(-1+\sqrt{-3})=e^{2\pi i/3}=\omega$. The other three cases give $-\omega,\omega^2,-\omega^2$, which together with the solutions already found give (b).

Example:

By proposition 3.1 we can easily find the group of units of the integers in different number fields $\mathbb{Q}(\sqrt{d})$ for d negative and square free. We have in

$\mathbb{Q}(\sqrt{-1})$: $U=\{\pm 1,\pm i\}$

$\mathbb{Q}(\sqrt{-2})$: $U=\{\pm 1\}$

$\mathbb{Q}(\sqrt{-3})$: $U=\{\pm 1,\pm e^{2\pi i/3},\pm e^{4\pi i/3}\}$

$\mathbb{Q}(\sqrt{-5})$: $U=\{\pm 1\}$.

Example:

The group of units of the integers in number fields $\mathbb{Q}(\sqrt{d})$ for d positive and square free is more difficult to handle but we can make out some of them. For in $\mathbb{Q}(\sqrt{3})$ the elements of the integers are of the form $\alpha=a+b\sqrt{3}$. Now α is a unit if and only if there exists β in the ring of integers such that $\alpha\beta=1$. Then using the norm we get that $N(\alpha)N(\beta)=1$ which implies that $N(\alpha)=\pm 1$.

But $N(\alpha)=N(a+b\sqrt{3})=(a+b\sqrt{3})(a-b\sqrt{3})=a^2-3b^2$ and so we get the two equations

$$a^2-3b^2=1 \text{ and } a^2-3b^2=-1$$

and the only integer solutions to these equations are

$$(a,b)=\begin{cases}(\pm 1,0)\\(\pm 2,\pm 1)\end{cases}$$

Hence $U=\{1,-1,2+\sqrt{3},-2+\sqrt{3},2-\sqrt{3},-2-\sqrt{3}\}$

Proposition 3.2

For a domain D,

1) x is a unit if and only if $x\mid 1$.
2) Any two units are associates and any associate of a unit is a unit.
3) x and y are associates if and only if $x\mid y$ and $y\mid x$.
4) x is irreducible if and only if every divisor of x is an associate of x or a unit.
5) An associate of an irreducible is irreducible.

Proof:

To prove (1) suppose x is a unit then $xy=1$ so $x\mid 1$. Conversely if $x\mid 1$, then $1=ax$ so x is a unit.

For (2), if $xy = 1$ and $ab = 1$ then $1 = xyab$ showing that any two units are associates. For any unit u such that we have $u = vx$, where v is a unit and x an associate, we have $au = avx = (av)x = 1$. So x is a unit.

To prove (3), suppose $x \mid y$ and $y \mid x$, then there exist $a, b \in D$ such that $y = ax$ and $x = by$ and so substituting we get $x = bax$. Now either $x = 0$, in which case $y = 0$ also and so they are associates, or $x \neq 0$ and we can cancel x to get $1 = ba$, so $a, b \in D$ are units. Hence x, y are associates. The converse is trivial.

(4) and (5) are straightforward from the definitions.

Proposition 3.3

If D is a domain and x, y are non-zero elements of D then

1) $x \mid y$ if and only if $\langle x \rangle \supseteq \langle y \rangle$.
2) x and y are associates if and only if $\langle x \rangle = \langle y \rangle$.
3) x is a unit if and only if $\langle x \rangle = D$.
4) x is irreducible if and only if $\langle x \rangle$ is maximal among the proper principal ideals of D.

Proof:

1) If $x \mid y$ then $y = zx \in \langle x \rangle$ for some $z \in D$, hence $\langle y \rangle \subseteq \langle x \rangle$. Conversely, if $\langle y \rangle \subseteq \langle x \rangle$ then $y \in \langle x \rangle$, so $y = zx$ for some $z \in D$.
2) Is immediate from 1).
3) If x is a unit then clearly $\langle x \rangle = D$. Conversely, if $\langle x \rangle = D$, $1 \in x$ and so $1 = zx$ for some $z \in D$. Hence x is a unit.
4) Suppose x is irreducible, with $\langle x \rangle \subset \langle y \rangle \subset D$. Then $y \mid x$ but is neither a unit nor an associate of x, contradicting 3.2 (4). Conversely, if no such y exists, then every divisor of x is either a unit or an associate, so x is irreducible.

In a domain D an element $x \in D$ is reducible if we can write it as a product of a finite number of irreducibles. Factorisation into irreducibles is not always possible, for example in the ring of all algebraic integers B. For if α is not zero or a unit, neither is $\sqrt{\alpha}$. Since $\alpha = \sqrt{\alpha}\sqrt{\alpha}$ and $\sqrt{\alpha}$ are integers, it follows that α is not irreducible. Thus B has no irreducibles at all and so factorisation into irreducibles is not possible.

In the ring of integers of a number field, however, factorisation is possible which we will prove next. But first we will need some tools for that.

Definition

A domain D is said to be noetherian if every ideal in D is finitely generated.

An example of a non-noetherian domain is the polynomial ring $Z[t]$ or the power series ring $Z[[t]]$.

The ascending chain condition. Given a chain of ideals $I_0 \subseteq I_1 \subseteq \ldots \subseteq I_n \subseteq \ldots$, then there exists some N for which $I_n = I_N$ for all $n \leq N$.

The maximal condition. Every non-empty set of ideals has a maximal element that is an element, which is not properly contained in every other element.

Example

We can verify the ascending chain condition for the ideal $\langle 120 \rangle$. Then we start with finding all ideals containing $\langle 120 \rangle$. They are the ideals generated by divisors of 120, i.e. generated by 2,3,4,5,6,10,15,30,40,60. Hence we can make the following inclusion diagram:

$$\langle 120 \rangle \subset \begin{cases} \langle 60 \rangle \subset \langle 30 \rangle \subset \begin{cases} \langle 15 \rangle \subset \begin{cases} \langle 5 \rangle \\ \langle 3 \rangle \end{cases} \\ \langle 10 \rangle \subset \begin{cases} \langle 2 \rangle \\ \langle 5 \rangle \end{cases} \end{cases} \\ \langle 40 \rangle \subset \langle 20 \rangle \subset \langle 10 \rangle \subset \begin{cases} \langle 2 \rangle \\ \langle 5 \rangle \end{cases} \\ \langle 30 \rangle \subset \begin{cases} \langle 15 \rangle \subset \begin{cases} \langle 5 \rangle \\ \langle 3 \rangle \end{cases} \\ \langle 10 \rangle \subset \begin{cases} \langle 2 \rangle \\ \langle 5 \rangle \end{cases} \end{cases} \end{cases}$$

We see here that all possible chains eventually stops

Proposition 3.4

The following conditions are equivalent for an integral domain D

1) D is noetherian.
2) D satisfies the ascending chain condition.
3) D satisfies the maximal condition.

Proof:

($1 \Rightarrow 2$) Assume that (1) holds. Consider an ascending chain $I_0 \subseteq I_1 \subseteq \ldots \subseteq I_n \subseteq \ldots$ and let $I = \bigcup_{n=1}^{\infty} I_n$. Then I is an ideal, so is finitely generated. Say $I = \langle x_1, \ldots, x_m \rangle$. Each x_i belongs to some $I_{n(i)}$. If we let $N = \max_i n(i)$, then we have $I = I_n$ and it follows that $I_n = I_N$ for all $n \leq N$.

($2 \Rightarrow 3$) Assume that (2) holds. Consider a non-empty set S of ideals. We will prove the contra positive of $2 \Rightarrow 3$ that is that if D does not satisfy the maximal condition it does not satisfies the ascending chain condition. Now, suppose that S does not have a maximal element. Pick $I_0 \in S$. Since I_0 is not maximal we can pick $I_1 \in S$ with $I_0 \subset I_1$. Hence by induction, we can always pick an ideal containing the former ones that is not maximal and so we have an ascending chain, which does not stop.

($3 \Rightarrow 1$) Finally suppose that (3) holds. Let I be any ideal and let S be the set of all finitely generated ideals contained in I. Then $\langle 0 \rangle \in S$, so S is non-empty and thus has a maximal element J. If $J \neq I$.

pick $x \in I - J$. Then $\langle J, x \rangle$ is finitely generated and strictly larger than J, a contradiction. Hence $J = I$ and I is finitely generated.

Theorem 3.5

If a domain D is noetherian, then factorisation into irreducibles is possible in D.

Proof:

Suppose D is noetherian, but there exists a non-unit $x \neq 0$ in D which cannot be expressed as a product of a finite number of irreducibles. Choose x so that $\langle x \rangle$ is maximal subject to these conditions on x, which is possible by the maximal condition. By its definition, this x cannot be irreducible, so $x = yz$ where y, z are not units. Then $\langle y \rangle \supseteq \langle x \rangle$ by Proposition 3.3 (1). If $\langle y \rangle = \langle x \rangle$ then x and y are associates by 3.3 (2) and this is not the case because it implies that z is a unit. So $\langle y \rangle \supset \langle x \rangle$, and similarly $\langle z \rangle \supset \langle x \rangle$. By maximality of $\langle x \rangle$ we must have

$y = p_1 \ldots p_r$,

$z = q_1 \ldots q_s$,

where each p_i and q_j are irreducible. Multiplying these together express x as a product of irreducibles, a contradiction. Hence the assumption that there existed a non-unit $\neq 0$, which is not a finite product of irreducibles, is false, and factorisation into irreducibles is always possible.

Example:

Any homomorphic image of a noetherian domain D is noetherian. To see this let $f : D \to f(D)$ be a homomorphism such that $f(x) = y$, for $x \in D, y \in f(D)$. Since D is noetherian x factorises into irreducibles $x = a_1 \ldots a_n$ in D. So we have $f(x) = f(a_1 \ldots a_n) = y$. But since f is a homomorphism $f(a_1 \ldots a_n) = f(a_1) \ldots f(a_n) = y$, so y factorises into irreducibles, $f(a_i)$ in $f(D)$. If not then we must have $f(a_j) = f(b_1) \ldots f(b_s)$ for some $j : 1 \leq j \leq n$. But this mean that $f(a_j) = f(b_1) \ldots f(b_s) = f(b_1 \ldots b_s)$ which contradicts the irreducibility of the a_i's.

Theorem 3.6

The ring of integers $\mathcal{D}$ in a number field K is noetherian.

Proof:

We prove that every ideal I of $\mathcal{D}$ is finitely generated and hence noetherian. Now $(\mathcal{D}, +)$ is free abelian of rank n equal to the degree of K by theorem 1.9. Hence $(I, +)$ is free abelian of rank $s \leq n$. If $\{x_1, \ldots, x_s\}$ is a Z-basis for $(I, +)$, then clearly $\langle x_1, \ldots, x_s \rangle = I$, so I is finitely generated and $\mathcal{D}$ is noetherian.

Now from this we can immediately deduce the following.

Corollary 3.7

Factorisation into irreducibles is possible in the ring of integers $\mathcal{D}$.

We want some methods to find the units and irreducibles in $\mathcal{D}$, and conveniently we find that the norm will be a powerful tool for this

Proposition 3.8

Let $\mathcal{D}$ be the ring of integers in a number field K, and let $x, y \in \mathcal{D}$. Then

1) x is a unit if and only if $N(x) = \pm 1$.
2) If x and y are associates, then $N(x) = \pm N(y)$.
3) If $N(x)$ is a rational prime, then x is irreducible in $\mathcal{D}$.

Proof:

1) If $xu = 1$, then $N(x)N(u) = 1$. Since $N(x), N(u) \in Z$, we have $N(x) = \pm 1$. Conversely, if $N(x) = \pm 1$, then $\sigma_1(x)\sigma_2(x)\ldots\sigma_n(x) = \pm 1$ where the σ_i are the monomorphisms $K \to C$. One factor, without loss in generality $\sigma_1(x)$, is equal to x and all the others are integers. Put $u = \pm\sigma_2(x)\ldots\sigma_n(x)$. Then $xu = 1$, so $u = x^{-1} \in K$. Hence $u \in K \cap B = \mathcal{D}$, and x is a unit.
2) If x and y are associates then $x = uy$ for a unit u, so $N(x) = N(uy) = N(u)N(y) = \pm N(y)$ by (1)
3) Let $x = yz$. Then $N(x) = N(y)N(z) = p$ for some rational prime. So one of $N(y)$ and $N(z)$ is $\pm p$ and the other is ± 1. By (1), one of y and z is a unit, so x is irreducible.

Non-unique factorisation into irreducibles

A factorisation into irreducibles in a domain D is unique if whenever we have two different factorisations

$p_1 \cdots p_r = q_1 \cdots q_s$

where every p_i and q_j is irreducible in D, it follows that

1) $r = s$
2) There is a permutation π of $\{1,\ldots,r\}$ such that p_i and $q_{\pi(i)}$ are associates for all $i = 1,\ldots r$.

Now we are ready to tackle the problem of whether factorisation is unique in some rings of integers of algebraic number fields. We will start with the quadratic fields.

Theorem 3.9

Factorisation into irreducibles is not unique in the ring of integers of $\mathbb{Q}(\sqrt{d})$ for at least the following values of d: $-5,-6,-10,-13,-14,-15,-17,-21,-22,-23,-26,-29,-30$.

Proof:

The proof of all these number fields are rather similar so we will show it for one of them and then make some remarks about some small tricks one has to think of when working the others out

In $\mathbb{Q}(\sqrt{-13})$ we have the factorisation

$$14 = 2 \cdot 7 = (1+\sqrt{-13})(1-\sqrt{-13})$$

Now we claim that 2, 7, $1+\sqrt{-13}$, $1-\sqrt{-13}$ are irreducible. The norm is by definition

$$N(a+b\sqrt{-13}) = a^2 + 13b^2$$

and so the norms of the factors are respectively 4, 49, 14, 14

Now, if $2 = xy$ where $x, y \in \mathcal{D}$ and non-units, then $4 = N(2) = N(x)N(y)$ so $N(x) = \pm 2$ and $N(y) = \pm 2$ Similarly if $7 = zw$ we get $N(z) = \pm 7$ and $N(w) = \pm 7$ While divisors of $1 \pm \sqrt{-13}$ must have norm ± 2 or ± 7

Since $-13 \equiv 1 (\mathrm{mod}\ 4)$ integers are of the form $a + b\sqrt{-13}$ so we are led to the equations

$$a^2 + 13b^2 = \pm 2, \pm 7$$

Now if $|b| = 1$ then $a^2 + 13b^2 > 7$ so we must have that $b = 0$ But then the equations will be reduced to

$$a^2 = \pm 2, \pm 7$$

Which is impossible in the integers. Hence no such divisors exist and hence 2, 7, $1+\sqrt{-13}$, $1-\sqrt{-13}$ are irreducible.

Now we are only left with showing that they are not associates to each other, but this is also easily seen with the norm. For example, norm of 2 is 4 where as norm of $1 \pm \sqrt{-13}$ is 14.

To do the other values of d is similar and the factorisations to start with are:

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

$\mathbb{Q}(\sqrt{-6}) : 6 = 2 \cdot 3 = (\sqrt{-6})(-\sqrt{-6})$

$\mathbb{Q}(\sqrt{-10}) : 14 = 2 \cdot 7 = (2+\sqrt{-10})(2-\sqrt{-10})$

$\mathbb{Q}(\sqrt{-14}) : 15 = 3 \cdot 5 = (1+\sqrt{-14})(1-\sqrt{-14})$

$\mathbb{Q}(\sqrt{-15}) : 4 = 2 \cdot 2 = (\frac{1+\sqrt{-15}}{2})(\frac{1-\sqrt{-15}}{2})$

$\mathbb{Q}(\sqrt{-17}) : 18 = 2 \cdot 3 \ \ 3 = (1+\sqrt{-17})(1-\sqrt{-17})$

$\mathbb{Q}(\sqrt{-21}) : 22 = 2 \ \ 11 = (1+\sqrt{-21})(1-\sqrt{-21})$

$\mathbb{Q}(\sqrt{-22}) : 26 = 2 \ \ 13 = (2+\sqrt{-22})(2-\sqrt{-22})$

$\mathbb{Q}(\sqrt{-23}) : 6 = 2 \cdot 3 = (\frac{1+\sqrt{-23}}{2})\frac{(1-\sqrt{-23}}{2})$

$\mathbb{Q}(\sqrt{-26}) : 27 = 3 \ \ 3 \ \ 3 = (1+\sqrt{-26})(1-\sqrt{-26})$

$\mathbb{Q}(\sqrt{-29}) : 30 = 2 \ \ 3 \ \ 5 = (1+\sqrt{-29})(1-\sqrt{-29})$

$\mathbb{Q}(\sqrt{-30}) : 34 = 2 \ \ 17 = (2+\sqrt{-30})(2-\sqrt{-30})$

Now in the case of -15 and -23 note that $d \equiv 1 (\mathrm{mod}\, 4)$, so we have to be a bit more careful in these proofs. Take for example in $\mathbb{Q}(\sqrt{-15})$, the integers are of the form $b\sqrt{-15}$ so we are led to the equations

$$13b^2 = \pm 2, \pm 8$$

Now if $|b| = 1$ then $15b^2 > 8$ so we must have that $b = 0$. From this we can continue as in the case of $\mathbb{Q}(\sqrt{-13})$.

For real quadratic fields there are similar results but these are harder to find. This is because the norm in this case is $a^2 - db^2$, so we have a lot more difficult to prove the given numbers to be irreducible. However we can do the following.

Theorem 3.10

Factorisation into irreducibles is not unique in the ring of integers of $\mathbb{Q}(\sqrt{d})$ for at least the following values of d: 10,15,26,30.

Proof:

In the integers of $\mathbb{Q}(\sqrt{10})$ we have factorisations

$$6 = 2 \cdot 3 = (4 + \sqrt{10})(4 - \sqrt{10})$$

We will prove that 2, 3 and $4 \pm \sqrt{10}$ are irreducible. Looking at norms this is equivalent to showing that the equations

$$a^2 - 10b^2 = \pm 2, \pm 3$$

have no integer solutions. Now we cannot use the same methods as before because of the minus sign. But by using modulo we get

$$a^2 \equiv \pm 2 (\mathrm{mod}\, 10) \text{ or } a^2 \equiv \pm 3 (\mathrm{mod}\, 10)$$

or equivalently

$$a^2 \equiv 2, 3, 7, 8 (\mathrm{mod}\, 10)$$

The squares $(\mathrm{mod}\, 10)$ are in order, $0,1,4,9,6,5,6,9,4,1$; and since our numbers are not squares $(\mathrm{mod}\, 10)$ there cannot exist any such solutions. Hence the factors are irreducible. Now 2 and $4 \pm \sqrt{10}$ are not associates since their norms are 4 and 6, respectively.

In the integers of $\mathbb{Q}(\sqrt{15})$ we have factorisations

$$10 = 2 \cdot 5 = (5 + \sqrt{15})(5 - \sqrt{15})$$

Again by looking at norms we get to the equations

$$a^2 - 15b^2 = \pm 2, \pm 5$$

And in $(\mathrm{mod}\, 15)$ this gives us

$$a^2 \equiv \pm 2, \pm 5 (\mathrm{mod}\, 15)$$

or

$$a^2 \equiv 2, 5, 10, 13 (\mathrm{mod}\, 15)$$

Now the squares $(\mathrm{mod}\, 15)$ are $0,1,4,9,1,10,6,4,4,6,10,1,9,4,1$, here one of the numbers occur in the list so 5 and 10 are solutions of the congruence. Now if $a = 5$, we cannot have $b = 0$, so then we get

$$25 - 15b^2 = \pm 2, \pm 5$$

and so $b^2 = \frac{23}{15}, \frac{27}{15}, \frac{4}{3}, 2$. But these have no integer solutions so there cannot be a factor of the form $25 - 15b^2$. If $a = 10$, similarly we cannot have $b = 0$ so we get

$$100 - 15b^2 = \pm 2, \pm 5$$

and so $b^2 = \frac{98}{15}, \frac{102}{15}, \frac{19}{3}, 7$. But these have no integer solutions so there cannot be a factor of the form $100 - 15b^2$. Hence the factors are irreducible
The other factorisations follow in a similar way

Note that in the theorems we have used a weak statement about the existence of square free numbers d such that factorisation is not unique. We would preferably like to know when unique factorisation is possible. It has been proved [Birch, Deuring and Siegel] that the ring of integers of $\mathbb{Q}(\sqrt{d})$ for negative square free integer d has unique factorisation if and only if d takes one of the following values:

$$-1, -2, -3, -7, -11, -19, -43, -67, -163.$$

For positive d it is not known whether unique factorisation occurs for finitely many $d > 0$. But factorisation is unique in many more cases than in negative d. For example the list of numbers for $d < 100$:

$$2,3,5,6,7,11,13,14,17,19,21,22,23,29,31,33,37,38,41,43,$$
$$46,47,53,57,59,61,62,67,69,71,73,77,83,86,89,93,94,97$$

Factorisation into primes

In a domain D an element $p \in D$ is called prime if p is not a unit or zero, and whenever $x \mid ab$ this implies that $x \mid a$ or $x \mid b$.

Proposition 3.11

A prime in a domain D is always irreducible.

Proof:

Suppose that D is a domain, $x \in D$ is prime, and $x = ab$. Then $x \mid ab$, so $x \mid a$ or $x \mid b$.
If $x \mid a$, then $a = xc$ for some $c \in D$. So $x = xcb$, and by cancelling x we see that $1 = cb$. Hence b is a unit. In the same way, $x \mid b$ we see that a is a unit.

The converse of this is not true in general; there are many domains in which irreducibles are not prime. An easy example is in $\mathbb{Z}[\sqrt{-13}]$, we have

$$14 = 2 \cdot 7 = (1 + \sqrt{-13})(1 - \sqrt{-13})$$

We have already seen in the proof of Theorem 3.9 that all factors here are irreducible. But since $2 \nmid (1 \pm \sqrt{-13})$, so 2 is not a prime.

Example:

In $Z[\sqrt{-5}]$ we have that $\sqrt{-5} \mid (a+b\sqrt{-5})$ if and only if $5 \mid a$. To see this, suppose that $\sqrt{-5} \mid (a+b\sqrt{-5})$ then we must have that $\sqrt{-5} \mid a$. But since $a \in Z$, $a \neq d\sqrt{-5}$ for some $d \in Z$. Hence we must have that $a = \sqrt{-5}\sqrt{-5} \cdot k$ for some $k \in Z$, which is an element of Z. So $5 \mid a$.

Conversely, if $5 \mid a$ then clearly $a = 5d = \sqrt{-5}\sqrt{-5} \cdot d$ so $\sqrt{-5} \mid (a+b\sqrt{-5})$.

Now let $e = a+b\sqrt{-5}$ and $f = c+d\sqrt{-5}$ then $ef = (ac-5bd)+(ad+bc)\sqrt{-5}$. Then, if $\sqrt{-5} \mid ef$ we must have that $5 \mid (ac-5bd)$, so $5 \mid ac$ which implies that

either $5 \mid a$ and $\sqrt{-5} \mid e$,

or $5 \mid c$ and $\sqrt{-5} \mid d$.

Hence $\sqrt{-5}$ is prime in $Z[\sqrt{-5}]$. Then by proposition 3.11 $\sqrt{-5}$ is irreducible and so 5 factorises into irreducibles in $Z[\sqrt{-5}]$.

Theorem 3.12

In a domain in which factorisation into irreducibles is possible, factorisation is unique if and only if every irreducible is prime.

Proof:

Let D be a domain. Another way of expressing the possibility to factorise an element $x \in D$ as $x = up_1 \ldots p_n$, where u is a unit and $p_1, \ldots, p_n$ are irreducibles Now suppose that factorisation is unique and p is irreducible.

Now if $p \mid ab$, then $ab = pc$ for some $c \in D$ If $a, b, c \neq 0$ we factorise them into irreducibles as follows

$$a = u_1 p_1 \ldots p_n$$
$$b = u_2 q_1 \ldots q_m$$
$$c = u_3 r_1 \ldots r_s$$

where each u_i is a unit and p_i, q_i, r_i are irreducible Then

$$p(u_3 r_1 \ldots r_s) = (u_1 p_1 \ldots p_n)(u_2 q_1 \ldots q_m)$$

and unique factorisation implies that p is an associate and hence divides one of p_i or q_i, so divides a or b.

Conversely, suppose that every irreducible is a prime We need to show that in

$$u_1 p_1 \ldots p_n = u_2 q_1 \ldots q_m,$$

where each u_i is a unit and p_i, q_i are irreducible, $m = n$ and there is a permutation π of $\{1, \ldots, m\}$ such that p_i and $q_{\pi(i)}$ are associates

This is an easy result that will be left out here.

Example:

Let p be an odd prime and $\xi = e^{2\pi i/p}$. If α is a prime element in $Z[\xi]$, then the rational integers, which are divisible by α, are precisely the rational integer multiples of some prime rational integer q

To see this, not that by the definition of the norm we have

$$N(\alpha) = \prod_{i=1}^{p-1} \sigma_i(\alpha),$$

and $\sigma_j(\alpha) = \alpha$ for some j. Hence $\alpha \mid N(\alpha) = u \cdot p_1 \ldots p_n$ for u a unit and p_i rational primes. Therefore $\alpha \mid p_q$ for some $q \in \{1, \ldots, n\}$.

Now if $N(\alpha)$ is not a prime in Z, there exists some $\overline{\sigma} = \sigma_1(\alpha) \ldots \sigma_r(\alpha)$ such that $\alpha \mid \overline{\sigma}$, and so the only possibility for an element to be divisible by α is if it is of the form ξp_q for some $\xi \in Z$.

Definition

A domain D is called a unique factorisation domain (UFD) if factorisation into irreducibles is possible and unique.

With this we can now generalize the ideas of factorisation in the usual sense to a unique factorisation domain. That is we can define the highest common factor, coprime and lowest common factor in the same way as we are used to.

Example:

We will examine the two elements 6 and $2(1+\sqrt{-5})$ in $Z[\sqrt{-5}]$ and see whether they have a highest common factor and a lowest common multiple. First of all note that we have the factorisation

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

So 6 and $2(1+\sqrt{-5})$ both have 2 and $(1+\sqrt{-5})$ as factors. Now suppose that $HCF(6, 2(1+\sqrt{-5})) = 2$ then, since $(1+\sqrt{-5}) \mid 6$ and $(1+\sqrt{-5}) \mid 2(1+\sqrt{-5})$, we must (by the definition of HCF) have that $(1+\sqrt{-5}) \mid 2$ but in $Z[\sqrt{-5}]$ we would then have that $2 = k(1+\sqrt{-5})$ for some $k \in Z[\sqrt{-5}]$. This cannot happen because then

$$k = \frac{2}{(1+\sqrt{-5})} = \frac{2(1-\sqrt{-5})}{(1+\sqrt{-5})(1-\sqrt{-5})} = \frac{2}{6}(1-\sqrt{-5}) \notin Z[\sqrt{-5}].$$

Similarly, if $HCF(6, 2(1+\sqrt{-5})) = (1+\sqrt{-5})$, we have that $2 \mid (1+\sqrt{-5})$ since 2 is a common factor of both numbers, and we would have $(1+\sqrt{-5}) = 2l$ for some $l \in Z[\sqrt{-5}]$ but we see that $l = \frac{1}{2}(1+\sqrt{-5}) \notin Z[\sqrt{-5}]$. Hence $HCF(6, 2(1+\sqrt{-5})) = 1$.

Now to find the least common multiple we can use the formula

$$HCF(6, 2(1+\sqrt{-5})) \cdot LCM(6, 2(1+\sqrt{-5})) = 6 \cdot 2(1+\sqrt{-5})$$

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

Euclidian domains

In order to prove unique factorisation, a crucial tool is a division algorithm. Here we will generalize this into:

Definition

Let D be a domain. A Euclidian function for D is a function $\phi \quad D-\{0\} \to \mathbb{N}$ such that

1) If $a,b \in D-\{0\}$ and $a \mid b$ then $\phi(a) \le \phi(b)$.
2) If $a,b \in D-\{0\}$ then there exist $q,r \in D$ such that $a = qb - r$ where $r = 0$ or $\phi(r) < \phi(b)$.

Example:

In the polynomial ring $R[x]$, we have that the operator ∂, the degree of an element in $R[x]$, is a Euclidian function. We can easily see this from polynomial division. That is for any two elements $f,g \in R[x]$, if $g \mid f$ then $\partial(g) \le \partial(f)$ and there exists, $q,r \in R[x]$ such that $f = qg + r$ where $r = C$ or $\partial(r) < \partial(g)$.

If a domain has a Euclidian function we call it a Euclidian domain (ED). Also a domain in which every ideal is principal is called a principal ideal domain (PID). We will show that every Euclidian domain is a unique factorisation domain by showing first that $ED \Rightarrow PID$ and then $PID \Rightarrow UFD$.

Theorem 3.13

Every Euclidian domain is a principal ideal domain.

Proof:

Let D be a Euclidian domain, I and ideal of D. If $I = 0$ it is principal, so we may assume that there exists a non-zero element x of I. Pick $x \in I$ such that $\phi(x) \le \phi(y)$ for all $y \in I-\{0\}$. We can do this because any set of the natural numbers has a least element. If $y \in I$, then $y = qx + r$, where either $r = 0$ or $\phi(r) < \phi(x)$. Now $r \in I$ but the way we have chosen x we cannot have an element with smaller value of the Euclidian function. Hence $r = 0$, so y is a multiple of x so $I = \langle x \rangle$ is principal.

Theorem 3.14

Every principal ideal domain is a unique factorisation domain.

Proof:

Let D be a principal domain. Since this implies that D is noetherian, factorisation into irreducibles is possible by theorem 3.5.

To prove the converse it is enough to show that every irreducible is prime.

Suppose p is irreducible, then $\langle p \rangle$ is maximal amongst the principal ideals of D by 3.3(4), but since every ideal is principal, this means $\langle p \rangle$ is maximal amongst all ideals.

Suppose $p \mid ab$ but $p \nmid a$. Then $\langle p \rangle \subset \langle a, p \rangle$, so by maximality $\langle a, p \rangle = D$. Then $1 \in \langle a, p \rangle$, so $1 = cp + da$ for some $c,d \in D$. But by multiplying with b we get $b = cpb + dab$.

Hence $p \mid b$ so p is prime.

By combining the two theorems 3.13 and 3.14 we get the important

Theorem 3.15
Every Euclidian domain is a unique factorisation domain.

Theorem 3.16
The ring of integers $\mathcal{D}$ of $Q(\sqrt{d})$ is Euclidian for $d = -1,-2,-3,-7,-11$.

Theorem 3.17
For square free $d < -11$ the ring of integers of $Q(\sqrt{d})$ is not Euclidian.

Theorem 3.18
The ring of integers of $Q(\sqrt{d})$, for positive d, is Euclidian if and only if $d = 2,3,5,6,7,11,13,17,19,21,29,33,37,41,55,73$.

The proof of theorem 3.17 and theorem 3.18 can be found in [ST] and the proof of theorem 3.19 is too difficult to prove with the techniques given in this thesis.

4. Ideals

First we will restate some properties of ideals.

Let R be a ring. Then an ideal $\mathbf{a}$ of R is maximal if $\mathbf{a}$ is a proper ideal of R and there are no ideals of R strictly between $\mathbf{a}$ and R.
The ideal $\mathbf{a} \neq R$ is prime if, whenever $\mathbf{b}$ and $\mathbf{c}$ are ideals of R with $\mathbf{bc} \subseteq \mathbf{a}$, then either $\mathbf{c} \subseteq \mathbf{a}$ or $\mathbf{b} \subseteq \mathbf{a}$.

In an integral domain D a principal ideal $\langle p \rangle$ is prime if and only if p is a prime or zero.
To see this, suppose $\langle p \rangle$ is prime. Then by the definition if $\mathbf{a}$, $\mathbf{b}$ are ideals D such that $\mathbf{ab} \subseteq \langle p \rangle$ then $\mathbf{a} \subseteq \langle p \rangle$ or $\mathbf{b} \subseteq \langle p \rangle$.
Now $\mathbf{ab} \subseteq \langle p \rangle$, means that elements of $\mathbf{ab}$ are multiples of p, that is if $\alpha \in \mathbf{ab}$, then $\alpha = kp$ for some $k \in D$, $p \nmid k$. Now $\alpha = \sum x_i y_i$, $(x_i \in \mathbf{a}, y_i \in \mathbf{b})$, so $p \mid \alpha \Rightarrow p \mid \sum x_i y_i \Rightarrow p \mid x_i$ or $p \mid y_i$. Hence p is prime. The result is trivial if $p = 0$.
Conversely, suppose p is prime or zero, then $p \mid ab$ implies $p \mid a$ or $p \mid b$. Thus $\langle a \rangle \langle b \rangle \subseteq \langle p \rangle$ implies that $\langle a \rangle \subseteq \langle p \rangle$ or $\langle b \rangle \subseteq \langle p \rangle$.

Lemma 4.1
Let R be a ring and $\mathbf{a}$ an ideal of R. Then
1) $\mathbf{a}$ is maximal if and only if $R/\mathbf{a}$ is a field.
2) $\mathbf{a}$ is prime if and only if $R/\mathbf{a}$ is a domain.

Proof:
The ideals of $R/\mathbf{a}$ are in bijective correspondence with the ideals of R lying between $\mathbf{a}$ and R. Hence $\mathbf{a}$ is maximal if and only if $R/\mathbf{a}$ has no non-zero proper ideals. Now a ring S has no non-zero proper ideals if and only if S is a field. Hence by taking S as $R/\mathbf{a}$ the result follows.
To prove (2), first suppose $\mathbf{a}$ is prime. If $x, y \in R$ are such that in $R/\mathbf{a}$ we have

$$(\mathbf{a} + x)(\mathbf{a} + y) = 0$$

and then $x, y \in \mathbf{a}$, so $\langle x \rangle \langle y \rangle \subseteq \mathbf{a}$. Hence either $\langle x \rangle \subseteq \mathbf{a}$ or $\langle y \rangle \subseteq \mathbf{a}$, so either $x \in \mathbf{a}$ or $y \in \mathbf{a}$. Hence one of $(\mathbf{a} + x)$ or $(\mathbf{a} + y)$ is zero in $R/\mathbf{a}$, and therefore $R/\mathbf{a}$ has no zero divisors so is an integral domain.
Conversely suppose $R/\mathbf{a}$ is an integral domain. Then $R/\mathbf{a} \neq 1$, so $\mathbf{a} \neq R$. Suppose if possible that $\mathbf{bc} \subseteq \mathbf{a}$ but $\mathbf{b} \not\subseteq \mathbf{a}$ or $\mathbf{c} \not\subseteq \mathbf{a}$. Then we can find elements $b \in \mathbf{b}$ and $c \in \mathbf{c}$ with $b, c \notin \mathbf{a}$ but $bc \in \mathbf{a}$. This means that $(\mathbf{a} + x)$ and $(\mathbf{a} + y)$ are zero divisors in $R/\mathbf{a}$, which is a contradiction.

Corollary 4.2
Every maximal ideal is prime.

Now we list some important properties of the ring of integers of a number field.

Theorem 4.3

The ring of integers $\mathcal{D}$ of a number field K has the following properties:

1) It is a domain, with field of fractions K.
2) It is noetherian.
3) If $\alpha \in K$ satisfies a monic polynomial equation with coefficients in $\mathcal{D}$ then $\alpha \in \mathcal{D}$.
4) Every non-zero prime ideal of $\mathcal{D}$ is maximal.

Proof:

1) Is obvious
2) By theorem 1.9 the group $(\mathcal{D},+)$ is free abelian of rank n. It follows by theorem 1.2 that if $\mathbf{a}$ is an ideal of $\mathcal{D}$ then $(\mathbf{a},+)$ is free abelian of rank $\leq n$. Now any Z-basis for $(\mathbf{a},+)$ generates $\mathbf{a}$ as an ideal, so every ideal of $\mathcal{D}$ is finitely generated and so $\mathcal{D}$ is noetherian.
3) Follow immediate from theorem 1.8.
4) Let $\mathbf{p}$ be a prime ideal of $\mathcal{D}$. Let $0 \neq \alpha \in \mathbf{p}$. Then $N = N(\alpha) = \alpha_1 \ldots \alpha_n \in \mathbf{p}$ where the α_i are conjugates of α. Therefore $\langle N \rangle \subseteq \mathbf{p}$, and hence $\mathcal{D}/\mathbf{p}$ is a quotient ring of $\mathcal{D}/N\mathcal{D}$ which, being a finitely generated abelian group with every element of finite order, is finite. Since $\mathcal{D}/\mathbf{p}$ is a domain by lemma 4.1(2) and is finite, it is a field. Hence $\mathbf{p}$ is a maximal ideal by lemma 4.1(1).

Note that property (4) is not true for rings in general. A ring, which satisfies the conditions 4.3(1)-(4), is called a Dedekind ring, after the mathematician who made ring-theoretic advances in this area.

To be able to prove uniqueness of factorisation in ideals we need to define what will work as inverse multiplication of ideals.

Definition

An $\mathcal{D}$-submodule $\mathbf{a}$ of K is called a fractional ideal of $\mathcal{D}$ if there exists some non-zero $c \in \mathcal{D}$ such that $c\mathbf{a} \subseteq \mathcal{D}$.

In other words the set $\mathbf{b}c = \mathbf{a}$ is an ideal of $\mathcal{D}$, and $\mathbf{a} = c^{-1}\mathbf{b}$. Thus the fractional ideals of $\mathcal{D}$ are the ideals of the form $c^{-1}\mathbf{b}$ where $\mathbf{b}$ is an ideal of $\mathcal{D}$ and c is a non-zero element of $\mathcal{D}$.

Theorem 4.4

The non-zero fractional ideal of $\mathcal{D}$ form an abelian group under multiplication.

Theorem 4.5

Every non-zero ideal of $\mathcal{D}$ can be written as a product of prime ideals uniquely up to the order of the factors.

Lemma A

Let $\mathbf{a} \neq 0$ be an ideal of $\mathcal{D}$. Then there exist prime ideals $\mathbf{p}_1, \ldots, \mathbf{p}_r$ such that $\mathbf{p}_1 \ldots \mathbf{p}_r \subseteq \mathbf{a}$.

Proof:

Suppose the contrary. Then since $\mathcal{D}$ is noetherian we may choose $\mathbf{a}$ maximal, subject to the non-existence of such $\mathbf{p}$'s. Then $\mathbf{a}$ is not prime, so there exist ideals $\mathbf{b}$ and $\mathbf{c}$ of $\mathcal{D}$ with $\mathbf{bc} \subseteq \mathbf{a}$, $\mathbf{b} \not\subseteq \mathbf{a}$, $\mathbf{c} \not\subseteq \mathbf{a}$. Let $\mathbf{a}_1 = \mathbf{a} + \mathbf{b}$ and $\mathbf{a}_2 = \mathbf{a} + \mathbf{c}$. Then $\mathbf{a}_1\mathbf{a}_2 \subseteq \mathbf{a}$, $\mathbf{a}_1 \supset \mathbf{a}$, $\mathbf{a}_2 \supset \mathbf{a}$. By maximality of $\mathbf{a}$ there exist prime ideals $\mathbf{p}_1, \ldots, \mathbf{p}_s, \mathbf{p}_{s+1}, \ldots, \mathbf{p}_r$ such that

$$\mathbf{p}_1 \ldots \mathbf{p}_s \subseteq \mathbf{a}_1$$
$$\mathbf{p}_{s+1} \ldots \mathbf{p}_r \subseteq \mathbf{a}_2$$

Hence

$$\mathbf{p}_1 \ldots \mathbf{p}_r \subseteq \mathbf{a}_1\mathbf{a}_2 \subseteq \mathbf{a}$$

Contrary to the choice of $\mathbf{a}$.

Definition

For each ideal $\mathbf{a}$ of $\mathcal{D}$, define

$$\mathbf{a}^{-1} = \{ x \in K : x\mathbf{a} \subseteq \mathcal{D} \}$$

It is clear that $\mathbf{a}^{-1}$ is a $\mathcal{D}$-submodule. If $\mathbf{a} \neq 0$ then for any $c \in \mathbf{a}$, $c \neq 0$, we have $c\mathbf{a}^{-1} \subseteq \mathcal{D}$, so $\mathbf{a}^{-1}$ is a fractional ideal. Clearly $\mathcal{D} \subseteq \mathbf{a}^{-1}$, so $\mathbf{a} = \mathbf{a}\mathcal{D} \subseteq \mathbf{a}^{-1}\mathbf{a}$. From the definition we have $\mathbf{a}\,\mathbf{a}^{-1} = \mathbf{a}^{-1}\mathbf{a} \subseteq \mathcal{D}$. This means that the fractional ideal $\mathbf{a}\mathbf{a}^{-1}$ is an ideal of $\mathcal{D}$. Further, for ideals $\mathbf{p}$, if $\mathbf{a} \subseteq \mathbf{p}$, then $\mathcal{D} \subseteq \mathbf{p}^{-1} \subseteq \mathbf{a}^{-1}$.

Lemma B

If $\mathbf{a}$ is a proper ideal, then $\mathbf{a}^{-1} \supset \mathcal{D}$.

Proof:

Since $\mathbf{a} \subseteq \mathbf{p}$ for some maximal ideal $\mathbf{p}$, whence $\mathbf{p}^{-1} \subseteq \mathbf{a}^{-1}$, it is sufficient to prove that $\mathbf{p}^{-1} \neq \mathcal{D}$ for $\mathbf{p}$ maximal. We must therefore find a non-integer in $\mathbf{p}^{-1}$. We start with any $a \in \mathbf{p}$, $a \neq 0$. By lemma A we can choose the smallest r such that

$$\mathbf{p}_1 \ldots \mathbf{p}_r \subseteq \langle a \rangle$$

for $\mathbf{p}_1, \ldots, \mathbf{p}_r$ prime ideals. Since $\langle a \rangle \subseteq \mathbf{p}$ and $\mathbf{p}$ is prime, some $\mathbf{p}_i \subseteq \mathbf{p}$. Without loss of generality $\mathbf{p}_1 \subseteq \mathbf{p}$. Hence $\mathbf{p}_1 = \mathbf{p}$ since prime ideals in $\mathcal{D}$ are maximal and further

$$\mathbf{p}_2 \ldots \mathbf{p}_r \not\subseteq \langle a \rangle$$

by minimality of r. Hence we can find $b \in \mathbf{p}_2 \ldots \mathbf{p}_r \setminus \langle a \rangle$. But $b\,\mathbf{p} \subseteq \langle a \rangle$ so $ba^{-1}\mathbf{p} \subseteq \mathcal{D}$ and $ba^{-1} \in \mathbf{p}^{-1}$. But $b \notin a\,\mathcal{D}$ and so $ba^{-1} \notin \mathcal{D}$, whence $\mathbf{p}^{-1} \neq \mathcal{D}$.

Lemma C

If $\mathbf{a}$ is a non-zero ideal and $\mathbf{a}S \subseteq \mathbf{a}$ for any subset $S \subseteq K$, then $S \subseteq \mathcal{D}$.

Proof:

We must show that if $\mathbf{a}\theta \subseteq \mathbf{a}$ for $\theta \in S$, then $\theta \in \mathcal{D}$. Because $\mathcal{D}$ is noetherian, $\mathbf{a} = \langle a_1, \ldots a_m \rangle$ where not all the a_i are zero. Then $\mathbf{a}\theta \subseteq \mathbf{a}$ implies

$$a_1\theta = b_{11}a_1 + \ldots + b_{1m}a_m$$
$$\ldots \qquad \text{for } b_{ij} \in \mathcal{D}$$
$$a_m\theta = b_{m1}a_1 + \ldots + b_{mm}a_m$$

Now because the equations

$$(b_{11}-\theta)x_1+\ldots+b_{1m}x_m=0$$

$$\ldots$$

$$b_{m1}x_1+\ldots+(b_{mm}-\theta)x_m=0$$

has a non-zero solution $x_1=a_1,\ldots,x_m=a_m$, then the determinant of the array of coefficients is non-zero. This gives a monic polynomial equation in θ with coefficients in $\mathcal{D}$, hence $\theta\in\mathcal{D}$

Lemma D

If **p** is a maximal ideal, then $\mathbf{pp}^{-1}=\mathcal{D}$.

Proof:

From the definition, $\mathbf{pp}^{-1}$ is an ideal where $\mathbf{p}\subseteq\mathbf{pp}^{-1}\subseteq\mathcal{D}$. Since **p** is maximal, $\mathbf{pp}^{-1}$ is equal to **p** or $\mathcal{D}$. But if $\mathbf{pp}^{-1}=\mathbf{p}$, then lemma C would imply $\mathbf{p}^{-1}=\mathcal{D}$, contradicting lemma B. So $\mathbf{pp}^{-1}=\mathcal{D}$

Lemma E

For every ideal $\mathbf{a}\neq 0$, $\mathbf{aa}^{-1}=\mathcal{D}$.

Proof:

If not choose **a** maximal subject to $\mathbf{aa}^{-1}\neq\mathcal{D}$. Then $\mathbf{a}\subseteq\mathbf{p}$ where **p** is maximal. From the definition, $\mathcal{D}\subseteq\mathbf{p}^{-1}\subseteq\mathbf{a}^{-1}$, so

$$\mathbf{a}\subseteq\mathbf{ap}^{-1}\subseteq\mathbf{aa}^{-1}\subseteq\mathcal{D}$$

In particular, $\mathbf{ap}^{-1}\subseteq\mathrm{D}$ implies that $\mathbf{ap}^{-1}$ is an ideal. Now we cannot have $\mathbf{a}=\mathbf{ap}^{-1}$, this would imply that $\mathbf{p}^{-1}\subseteq\mathrm{D}$ by lemma C, contradicting lemma B again. So $\mathbf{a}\subset\mathbf{ap}^{-1}$ and the maximality condition on **a** implies that the ideal $\mathbf{ap}^{-1}$ satisfies

$$\mathbf{ap}^{-1}(\mathbf{ap}^{-1})^{-1}=\mathcal{D}$$

By the definition of $\mathbf{a}^{-1}$ this means

$$\mathbf{p}^{-1}(\mathbf{ap}^{-1})^{-1}\subseteq\mathbf{a}^{-1}$$

Thus

$$\mathcal{D}=\mathbf{ap}^{-1}(\mathbf{ap}^{-1})^{-1}\subseteq\mathbf{aa}^{-1}\subseteq\mathcal{D}$$

from which the result follows.

Lemma F

Every fractional ideal **a** has an inverse $\mathbf{a}^{-1}$ such that $\mathbf{aa}^{-1}=\mathcal{D}$.

Proof:

The set of fractional ideals is already known to be a commutative semi group, so given a fractional ideal **a**, we need only to find another ideal **a'** such that $\mathbf{aa'}=\mathcal{D}$. But there exists an ideal **b** and a non-zero element $c\in\mathcal{D}$ such that $\mathbf{a}=c^{-1}\mathbf{b}$. Let $\mathbf{a'}=c\,\mathbf{b}^{-1}$, then $\mathbf{aa'}=\mathcal{D}$ as required

Lemma G

Every non-zero ideal **a** is a product of prime ideals.

Proof:

If not, let **a** be maximal subject to the condition of not being a product of ideals. Then **a** is not prime, but we will have $\mathbf{a}\subseteq\mathbf{p}$ for some maximal (hence prime) ideal, and as in lemma E,

$$\mathbf{a}\subset\mathbf{ap}^{-1}\subseteq\mathcal{D}$$

By the maximality condition on **a**,

$$\mathbf{a}\mathbf{p}^{-1} = \mathbf{p}_2 \cdots \mathbf{p}_r$$

for prime ideals $\mathbf{p}_2, \ldots, \mathbf{p}_r$, whence

$$\mathbf{a} = \mathbf{p}\mathbf{p}_2 \cdots \mathbf{p}_r$$

Lemma H

Prime factorisation is unique.

Proof:

By analogy with factorisation of elements, for ideals **a**, **b** we shall say that **a** divides **b** if there is an ideal **c** such that $\mathbf{b} = \mathbf{ac}$. This condition is equivalent to $\mathbf{a} \supseteq \mathbf{b}$ since we may then take $\mathbf{c} = \mathbf{a}^{-1}\mathbf{b}$. The definition of prime ideals **p** shows that if $\mathbf{p} | \mathbf{ab}$ then either $\mathbf{p} | \mathbf{a}$ or $\mathbf{p} | \mathbf{b}$. If we now have prime ideals $\mathbf{p}_1, \ldots, \mathbf{p}_r$, $\mathbf{q}_1, \ldots, \mathbf{q}_s$ with

$$\mathbf{p}_1 \cdots \mathbf{p}_r = \mathbf{q}_1 \cdots \mathbf{q}_s$$

then $\mathbf{p}_1$ divides some $\mathbf{q}_i$, so by maximality $\mathbf{p}_1 = \mathbf{q}_i$. Multiplying with $\mathbf{p}_1^{-1}$ and using induction we obtain uniqueness of prime factorisation up to the order of the factors.

Thus we have now proved the two theorems 4.4 and 4.5
One result from lemma G is worth to note as a special statement:

Proposition 4.6

For ideals **a**,**b** of $\mathcal{D}$, $\mathbf{a} | \mathbf{b}$ if and only if $\mathbf{a} \supseteq \mathbf{b}$.

Now that we have established the unique factorisation for ideals we can again use our old knowledge about factorisation. Hence there exist a greatest common divisor, **g**, and a least common multiple, **l**, such that the following conditions hold:

- if $\mathbf{g} | \mathbf{a}$ and $\mathbf{g} | \mathbf{b}$ and there exists a $\mathbf{g}'$ such that $\mathbf{g}' | \mathbf{a}$ and $\mathbf{g}' | \mathbf{b}$ then $\mathbf{g}' | \mathbf{g}$.
- if $\mathbf{a} | \mathbf{l}$ and $\mathbf{b} | \mathbf{l}$ and there exists an **l** such that $\mathbf{a} | \mathbf{l}'$ and $\mathbf{b} | \mathbf{l}'$ then $\mathbf{l} | \mathbf{l}'$.

We can extend this even further. Suppose we can factorise **a** and **b** into primes as

$$\mathbf{a} = \prod p_i^{e_i} \quad \text{and} \quad \mathbf{b} = \prod p_i^{f_i}$$

where the p_i are prime ideals. Then we can write the greatest common divisor and the least common multiple as

$$\mathbf{g} = \prod p_i^{\max(e_i, f_i)}$$
$$\mathbf{l} = \prod p_i^{\min(e_i, f_i)}$$

Another way of putting this is

Lemma 4.7

If **a** and **b** are ideals of $\mathcal{D}$ and **g**, **l** are the greatest common divisor and least common multiple, respectively, of **a** and **b**, then

$$\mathbf{g} = \mathbf{a} + \mathbf{b}, \qquad \mathbf{l} = \mathbf{a} \cap \mathbf{b}.$$

Proof:

We know that $\mathbf{x} | \mathbf{a}$ if and only if $\mathbf{x} \supseteq \mathbf{a}$, by proposition 4.6. Hence **g** must be the smallest ideal containing **a** and **b**, and **l** the largest ideal contained in **a** and **b**

Example:

If $\mathbf{p}$ and $\mathbf{q}$ are distinct prime ideals in the ring of integers $\mathcal{D}$ then we have that

$$\mathbf{p}+\mathbf{q}=\mathcal{D} \text{ and } \mathbf{p}\cap\mathbf{q}=\mathbf{pq}.$$

To see this, note that $\mathbf{p}$ and $\mathbf{q}$ are maximal ideals and since $\mathbf{p}\subset\mathbf{p}+\mathbf{q}$ and $\mathbf{q}\subset\mathbf{p}+\mathbf{q}$ we must have that the ideal $\mathbf{p}+\mathbf{q}=\mathcal{D}$.

For the second equation note that if $a\in\mathbf{p}\cap\mathbf{q}$ then $a=bc$ for some $b\in\mathbf{p}$ and $c\in\mathbf{q}$. Hence $a\in\mathbf{pq}$, so we have established $\mathbf{p}\cap\mathbf{q}\subseteq\mathbf{pq}$.

Conversely, if $a\in\mathbf{pq}$ then $a=\sum\mathbf{p}_i\mathbf{q}_i\in\mathbf{p}\cap\mathbf{q}$ and so we have $\mathbf{p}\cap\mathbf{q}\supseteq\mathbf{pq}$. Hence the result follows.

Now if $\mathbf{a}$ is a non-zero ideal of $\mathcal{D}$ then the quotient ring $\mathcal{D}/\mathbf{a}$ is finite (by theorem 4.3). We define the norm of an ideal $\mathbf{a}$ to be

$$\mathrm{N}(\mathbf{a})=|\mathcal{D}/\mathbf{a}|$$

Clearly $\mathrm{N}(\mathbf{a})$ is a positive integer and applies only on ideals.

However, it can be a bit tedious to calculate the norm of an ideal from this definition. Luckily there are easier ways to do this:

Theorem 4.8

1) Every ideal $\mathbf{a}$ of $\mathcal{D}$ with $\mathbf{a}\neq 0$ has a Z-basis $\{\alpha_1,\ldots,\alpha_n\}$ where n is the degree of K.
2) We have $\mathrm{N}(\mathbf{a})=\left|\dfrac{\Delta[\alpha_1,\ldots,\alpha_n]}{\Delta}\right|^{1/2}$, where Δ is the discriminant of K.

Proof:

We have already used the fact that $(\mathcal{D},+)$ is free abelian of rank n. Now since $\mathcal{D}/\mathbf{a}$ is finite it follows (from theorem 1.3) that $(\mathbf{a},+)$ is free abelian of rank n. Hence $(\mathbf{a},+)$ has a Z-basis of the form $\{\alpha_1,\ldots,\alpha_n\}$. This proves (1).

Now, let $\{\omega_1,\ldots,\omega_n\}$ be a Z-basis for $\mathcal{D}$, and suppose that $\alpha_i=\sum c_{ij}\omega_j$. Then by theorem 1.3,

$$\mathrm{N}(\mathbf{a})=|\mathcal{D}/\mathbf{a}|=\left|\det c_{ij}\right|.$$

Now by the definition of the discriminant and the formula for the change of basis

$$\Delta[\alpha_1,\ldots,\alpha_n]=\left(\det c_{ij}\right)^2\Delta[\omega_1,\ldots,\omega_n]$$

So

$$\mathrm{N}(\mathbf{a})=\left(\det c_{ij}\right)=\left(\frac{\Delta[\alpha_1,\ldots,\alpha_n}{\Delta}\right)$$

Note that when taking the square root of $\left(\det c_{ij}\right)^2$ we cannot choose the negative root because of our definition of $\mathrm{N}(\mathbf{a})$.

Corollary 4.9

If $\mathbf{a}=\langle a\rangle$ is a principal ideal then $\mathrm{N}(\mathbf{a})=|N(a)|$.

Proof:

A Z-basis for **a** is given by $\{a\omega_1, \ldots, a\omega_n\}$. The definition of the discriminant gives us

Hence

$$N(\mathbf{a}) = \left| \frac{\Delta[a\omega_1, \ldots, a\omega_n]}{\Delta[\omega_1, \ldots, \omega_n]} \right|$$

by the definition of norm. Now the definition of discriminant gives us

$$\Delta[\alpha_1, \ldots, \alpha_n] = \left(\det[\sigma_i(\alpha_j)]\right)^2$$

Now note that

$$\det[\sigma_i(a\omega_j)] = \det[\sigma_i(a)]\det[\sigma_i(\omega_j)]$$

Which gives the desired result.

Now we can make a straightforward calculation of the norm of a principal ideal.

Example:

Let $\mathcal{D}$ be the ring of integers of $Q(\sqrt{d})$ for a square free rational integer d, then

$$N(\langle a + b\sqrt{d}\rangle) = |a^2 - db^2|$$

and in particular in $\mathcal{D} = Z[\sqrt{-17}]$, then

$$N(\langle 18\rangle) = 18^2$$

This new norm is multiplicative,

Theorem 4.10

If **a** and **b** are non-zero ideals of $\mathcal{D}$, then

$$N(\mathbf{ab}) = N(\mathbf{a})N(\mathbf{b}).$$

Proof:

Because we have already established uniqueness of factorisation we can use induction on the number of factors so we need only to show that N(**ap**) = N(**a**)N(**p**), for **p** prime ideal.

This is done by noting the relations

$$|\mathcal{D}/\mathbf{ap}| = |\mathcal{D}/\mathbf{a}|\,|\mathbf{a}/\mathbf{ap}|$$
$$|\mathbf{a}/\mathbf{ap}| = |\mathcal{D}/\mathbf{p}|$$

Thus

$$N(\mathbf{ap}) = |\mathcal{D}/\mathbf{ap}| = |\mathcal{D}/\mathbf{a}|\,|\mathbf{a}/\mathbf{ap}| = |\mathcal{D}/\mathbf{a}|\,|\mathcal{D}/\mathbf{p}| = N(\mathbf{a})N(\mathbf{p})$$

The relations are a bit tedious, but follow from basic ring theory. They will be left out here and the reader is referred to [ST] for complete details.

It is convenient to introduce another way of describing division with ideals. We will write that if **a** is an ideal of $\mathcal{D}$ and b is an element of $\mathcal{D}$ such that $\mathbf{a} \mid \langle b\rangle$, then we also write $\mathbf{a} \mid b$ and say that **a** divides b. It should be clear that $\mathbf{a} \mid b$ if and only if $b \in \mathbf{a}$.

We can now write, if **p** is a prime ideal and $\mathbf{p} \mid \langle a\rangle\langle b\rangle$, then we must have $\mathbf{p} \mid \langle a\rangle$ or $\mathbf{p} \mid \langle b\rangle$.

So for **p** prime we have

$$\mathbf{p} \mid ab \text{ implies that } \mathbf{p} \mid \langle b\rangle \text{ or } \mathbf{p} \mid b.$$

Theorem 4.11

Let $\mathbf{a}$ be an ideal of $\mathcal{D}$, $\mathbf{a} \neq 0$,

1) If $N(\mathbf{a})$ is prime then so is $\mathbf{a}$.
2) $N(\mathbf{a})$ is an element of $\mathbf{a}$, or equivalently, $\mathbf{a} | N(\mathbf{a})$.
3) If $\mathbf{a}$ is prime it divides exactly one rational prime and then

$$N(\mathbf{a}) = p^m$$

where $m \leq n$ the degree of K.

Proof:

1) Write $\mathbf{a}$ as a product of primes and calculate the norm of $\mathbf{a}$.
2) Note that since $N(\mathbf{a}) = |\mathcal{D}/\mathbf{a}|$ it follow that for any $x \in \mathcal{D}$ we have $N(\mathbf{a})\, x \in \mathbf{a}$. Now put $x = 1$.
3) Note that by (2) $\mathbf{a} | N(\mathbf{a}) = p_1^{m_1} \ldots p_r^{m_r}$. So we have $\mathbf{a} | p_i$ for some rational p_i. If p and q where distinct rational primes. both divisible by $\mathbf{a}$, we could find integers u, v such that $up + vq = 1$, and then deduce that $\mathbf{a} | 1$ which implies that $\mathbf{a} = \mathcal{D}$, a contradiction. Then $N(\mathbf{a}) | N(\langle p \rangle) = p^n$, so that $N(\mathbf{a}) = p^m$ for some $m \leq n$.

Note that the converse of 4.11(1) is not true in general. A prime ideal can have a norm that is not prime by 4.11(3).

Theorem 4.12

1) Every non-zero ideal of $\mathcal{D}$ has a finite number of divisors.
2) A non-zero rational integer belongs to only a finite number of ideals of $\mathcal{D}$.
3) Only finitely many ideals of $\mathcal{D}$ have given norm.

Proof:

1) This is an immediate consequence of prime factorisation.
2) A special case of (1).
3) Follows from (2) using theorem 4.11(2).

We now know that every ideal of $\mathcal{D}$ is finitely generated. In fact we can prove an even stronger condition.

Lemma 4.13

If $\mathbf{a}$ and $\mathbf{b}$ are non-zero ideals of $\mathcal{D}$ then there exists $\alpha \in \mathbf{a}$ such that

$$\alpha \mathbf{a}^{-1} + \mathbf{b} = \mathcal{D}.$$

Proof:

First note that if $\alpha \in \mathbf{a}$ so that $\alpha \mathbf{a}^{-1}$ is an ideal and just not a fractional ideal. Now $\alpha \mathbf{a}^{-1} + \mathbf{b}$ is the greatest common divisor of $\alpha \mathbf{a}^{-1}$ and $\mathbf{b}$, so it is sufficient to choose $\alpha \in \mathbf{a}$ so that

$$\alpha \mathbf{a}^{-1} + \mathbf{p}_i = \mathcal{D} \qquad i = 1, \ldots, r$$

where $\mathbf{p}_1, \ldots, \mathbf{p}_r$ are the distinct prime ideals dividing $\mathbf{b}$. This will follow if

$$\mathbf{p}_i \nmid \alpha \mathbf{a}^{-1}$$

since $\mathbf{p}_i$ is a maximal ideal. So it is sufficient to choose $\alpha \in \mathbf{a} \backslash \mathbf{a}\mathbf{p}_i$ for all $i = 1, \ldots, r$.

If $r = 1$ this is easy, for unique factorisation of ideals implies $\mathbf{a} \neq \mathbf{a}\mathbf{p}_i$. For $r > 1$ let

$$\mathbf{a}_i = \mathbf{a}\mathbf{p}_1 \ldots \mathbf{p}_{i-1}\mathbf{p}_{i+1} \ldots \mathbf{p}_r$$

By the case $r = 1$ we can choose

$$\alpha_i \in \mathfrak{a}_i \backslash \mathfrak{a}_i \mathfrak{p}_i$$

Define

$$\alpha = \alpha_1 + \ldots + \alpha_r$$

Then each $\alpha_i \in \mathfrak{a}_i \subseteq \mathfrak{a}$, so $\alpha \in \mathfrak{a}$. Suppose if possible that $\alpha \in \mathfrak{a}\mathfrak{p}_i$. If $j \neq i$ then $\alpha_j \in \mathfrak{a}_j \subseteq \mathfrak{a}\mathfrak{p}_i$, so it follows that

$$\alpha_i = \alpha - \alpha_1 - \ldots - \alpha_{i-1} - \alpha_{i+1} - \ldots - \alpha_r \in \mathfrak{a}\mathfrak{p}_i$$

Hence $\mathfrak{a}\mathfrak{p}_i \mid \langle \alpha_i \rangle$. On the other hand $\mathfrak{a}_i \mid \langle \alpha_i \rangle$, and so we have $\mathfrak{a}_i\mathfrak{p}_i \mid \langle \alpha_i \rangle$. This contradicts the choice of α_i.

Theorem 4.14

Let $\mathfrak{a} \neq 0$ be an ideal of $\mathcal{D}$, and $0 \neq \beta \in \mathfrak{a}$. Then there exists $\alpha \in \mathfrak{a}$ such that $\mathfrak{a} = \langle \alpha, \beta \rangle$.

Proof:

Let $\mathfrak{b} = \beta\,\mathfrak{a}^{-1}$. By lemma 4.13 there exists $\alpha \in \mathfrak{a}$ such that

$$\alpha\ \mathfrak{a}^{-1} + \mathfrak{b} = \alpha\ \mathfrak{a}^{-1} + \beta\,\mathfrak{a}^{-1} = \mathfrak{D}.$$

Hence

$$\left(\langle \alpha \rangle + \langle \beta \rangle\right)\mathfrak{a}^{-1} = \mathfrak{D},$$

so that

$$\mathfrak{a} = \langle \alpha \rangle + \langle \beta \rangle = \langle \alpha, \beta \rangle$$

We can now characterize those $\mathcal{D}$ for which factorisation into irreducibles is unique:

Theorem 4.15

Factorisation of elements of $\mathcal{D}$ into irreducibles is unique if and only if every ideal of $\mathcal{D}$ is principal.

Proof:

If every ideal is principal, then unique factorisation of elements follows by theorem 3.14. To prove the converse, if factorisation of elements is unique, it will be sufficient to prove that every prime ideal is principal. This is because every non-prime ideal is a product of prime ideals, which is principal.

Let $\mathfrak{p} \neq 0$ be a prime ideal of $\mathcal{D}$. By theorem 4.11(2) there exists a rational integer $N = \mathrm{N}(\mathfrak{p})$ such that $\mathfrak{p} \mid N$. Now we can factorise N into irreducible elements in $\mathcal{D}$ as

$$N = \pi_1 \ldots \pi_s$$

Since $\mathfrak{p} \mid N$ and $\mathfrak{p}$ is a prime ideal, it follows that $\mathfrak{p} \mid \pi_i$, or equivalently, $\mathfrak{p} \mid \langle \pi_i \rangle$. But since factorisation is unique in $\mathcal{D}$, the irreducible π_i is actually prime by theorem 3.12, and then the principal ideal $\langle \pi_i \rangle$ is prime by the results in the beginning of this chapter. Thus $\mathfrak{p} \mid \langle \pi_i \rangle$ where both $\mathfrak{p}$ and $\langle \pi_i \rangle$ are prime and by uniqueness of factorisation $\mathfrak{p} = \langle \pi_i \rangle$ so $\mathfrak{p}$ is principal.

Now we can summit this chapter by noting the discovered relation between factorisation of elements and ideals. Take an irreducible element π, which is not prime. Then $\langle \pi \rangle$ is not prime, so it has a proper factorisation into prime ideals

$$\langle \pi \rangle = \mathfrak{p}_1 \ldots \mathfrak{p}_r$$

Now none of these $\mathbf{p}_i$ can be principal for we would then have that $\mathbf{p}_i = \langle a \rangle$, then $\langle a \rangle \mid \langle \pi \rangle$ which implies that $\pi \mid a$. Since π is irreducible, a would either be a unit (contradicting the fact that $\langle a \rangle$ is prime) or a would be an associate of π, whence $\langle \pi \rangle = \mathbf{p}_1$, contradicting the fact that $\langle \pi \rangle$ has a proper factorisation.

We see that if $\mathcal{D}$ has unique factorisation of elements into irreducibles, then these irreducibles are all primes; and factorisation of elements corresponds precisely to factorisation of the corresponding principal ideals.

On the other hand, if $\mathcal{D}$ does not have unique factorisation of elements, then not all irreducibles are prime, and any non-prime irreducible generates a principal ideal, which has a proper factorisation into non-principal ideals. Although the ideals are non-principal we have managed to show that they are at least near principal in the sense that they have precisely two generators.

Example:

In $Z[\xi]$ we define the ideals

$$\mathbf{p} = \langle 2, 1 + \sqrt{-5} \rangle$$
$$\mathbf{q} = \langle 3, 1 + \sqrt{-5} \rangle$$
$$\mathbf{r} = \langle 3, 1 - \sqrt{-5} \rangle$$

These ideals are maximal; hence they are prime ideals by corollary 4.2.

To see this, we start with $\mathbf{p}$:

Elements of $\mathbf{p}$ are of the form $r + s\sqrt{-5}$ where $r, s \in Z[\xi]$. Hence we have

$$r + s\sqrt{-5} = 2(a + b\sqrt{-5}) + (c + d\sqrt{-5})(1 + \sqrt{-5}) = (2a + c - 5d) + (2b + c - d)\sqrt{-5}$$

Now $r - s = 2a - 2b - 6d = 2(a - b - 3d)$ and so $r - s$ is an even number, which means that r and s have the same parity. Hence $\mathbf{p}$ cannot be the whole ring $Z[\xi]$.

Suppose there is some ideal $\mathbf{a}$ containing $\mathbf{p}$ such that there exist elements of the form $m + n\sqrt{-5}$ that are in $\mathbf{a}$ but not in $\mathbf{p}$. Then m and n must be odd and even respectively (or vice versa), and so

$$\langle \mathbf{p}, m + n\sqrt{-5} \rangle = Z[\sqrt{-5}]$$

Showing that $\mathbf{p}$ is maximal in $Z[\xi]$.

Similarly, for $\mathbf{q}$, a general element is of the from

$$r + s\sqrt{-5} = 3(a + b\sqrt{-5}) + (c + d\sqrt{-5})(1 + \sqrt{-5}) = (3a + c - 5d) + (3b + c + d)\sqrt{-5}$$

and so $r - s = 3(a - b - 2d) \Rightarrow r \equiv s \pmod 3$. By a similar argument as above we find that $\mathbf{q}$ is maximal.

The case for $\mathbf{r}$ is identical to $\mathbf{q}$, so is also maximal.

Now we claim that

$$\mathbf{p}^2 = \langle 2 \rangle \qquad \mathbf{qr} = \langle 3 \rangle$$
$$\mathbf{pq} = \langle 1 + \sqrt{-5} \rangle \qquad \mathbf{pr} = \langle 1 - \sqrt{-5} \rangle$$

To see this note that we have that

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

so clearly $6 \in \mathbf{p}$, which gives that $\langle 6\rangle \subseteq \mathbf{p}$. But we also have that

$$6 = (1+\sqrt{-5})(2-(1+\sqrt{-5}) \in \mathbf{p}^2$$

hence $\langle 6\rangle \subseteq \mathbf{p}^2$, and so $\mathbf{p}^2$ is a factor of $\langle 6\rangle$.

It is easy to see that $\mathbf{q}$ and $\mathbf{r}$ are also factors of $\langle 6\rangle$, so by using theorem 4.5 we get that

$$\langle 6\rangle \subseteq \mathbf{p}^2\mathbf{qr}$$

Next we calculate the norms of $\mathbf{p}$, $\mathbf{q}$ and $\mathbf{r}$:

Since we are working in $K = Q(\sqrt{-5})$, by theorem 2.3 the discriminant of K, is $\Delta = -4 \cdot 5$ and by the definition of the norm of an ideal we have

$$N(\mathbf{a}) = \left|\frac{\Delta[\alpha_1, \alpha_2]}{\Delta}\right|^{1/2}.$$

Thus for $\mathbf{p}$ we can choose integral basis $\{2, 1+\sqrt{-5}\}$ and so we get

$$\Delta[2, 1+\sqrt{-5}] = \begin{vmatrix} 2 & 1+\sqrt{-5} \\ 2 & 1-\sqrt{-5} \end{vmatrix}^2 = (2(1-\sqrt{-5}) - 2(1+\sqrt{-5}))^2 = (-4\sqrt{-5})^2 = -16 \cdot 5$$

so

$$N(\mathbf{p}) = \left|\frac{-16 \cdot 5}{-4 \cdot 5}\right|^{1/2} = \sqrt{4} = 2.$$

For $\mathbf{q}$ we can choose integral basis $\{3, 1+\sqrt{-5}\}$ and so we get

$$\Delta[3, 1+\sqrt{-5}] = \begin{vmatrix} 3 & 1+\sqrt{-5} \\ 3 & 1-\sqrt{-5} \end{vmatrix}^2 = (3(1-\sqrt{-5}) - 3(1+\sqrt{-5}))^2 = (-6\sqrt{-5})^2 = -36 \cdot 5$$

so

$$N(\mathbf{q}) = \left|\frac{-36 \cdot 5}{-4 \cdot 5}\right|^{1/2} = \sqrt{9} = 3.$$

For $\mathbf{r}$ we can choose integral basis $\{3, 1-\sqrt{-5}\}$ and so we get

$$\Delta[3, 1-\sqrt{-5}] = \begin{vmatrix} 3 & 1-\sqrt{-5} \\ 3 & 1+\sqrt{-5} \end{vmatrix}^2 = (3(1+\sqrt{-5}) - 3(1-\sqrt{-5}))^2 = (6\sqrt{-5})^2 = -36 \cdot 5$$

so

$$N(\mathbf{r}) = \left|\frac{-36 \cdot 5}{-4 \cdot 5}\right|^{1/2} = \sqrt{9} = 3.$$

By using the norm and the fact that $\langle 6\rangle \subseteq \mathbf{p}^2\mathbf{qr}$, we get that $\langle 6\rangle = \mathbf{p}^2\mathbf{qr}$, because

$$N(\langle 6\rangle = 36 = 2^2 \cdot 3 \cdot 3 = N(\mathbf{p})^2 N(\mathbf{q}) N(\mathbf{r})$$

Form the factorisations $\langle 6\rangle = \langle 2\rangle\langle 3\rangle$ and $\langle 6\rangle = \langle 1+\sqrt{-5}\rangle\langle 1-\sqrt{-5}\rangle$ and by again using the norm we get the desired results, i.e. that

$$\mathbf{p}^2 = \langle 2\rangle \qquad \mathbf{qr} = \langle 3\rangle$$
$$\mathbf{pq} = \langle 1+\sqrt{-5}\rangle \qquad \mathbf{pr} = \langle 1-\sqrt{-5}\rangle$$

5. Lattices

Lattices are subsets of R^n. They are discrete subgroups of R^n and in some sense they generalize the way Z is embedded in R.

Definition

Let $e_1, \ldots, e_m$ be a linearly independent set of vectors in R^n where $m \leq n$. Then we say that the additive subgroup of $(R^n, +)$ generated by $e_1, \ldots, e_m$ is a lattice of dimension m.

Theorem 5.1

An additive subgroup of R^n is a lattice if and only if it is discrete.

The proof of this theorem is made up of algebraic and topological properties and will be left out here. It is given in [ST].

Definition

If L is a lattice generated by $\{e_1, \ldots, e_m\}$ we say that the fundamental domain $\boldsymbol{T}$ is all elements $\sum a_i e_i$, $a_i \in R$, for which $0 \leq a < 1$.

The fundamental domain is dependent of the generators of the lattice.

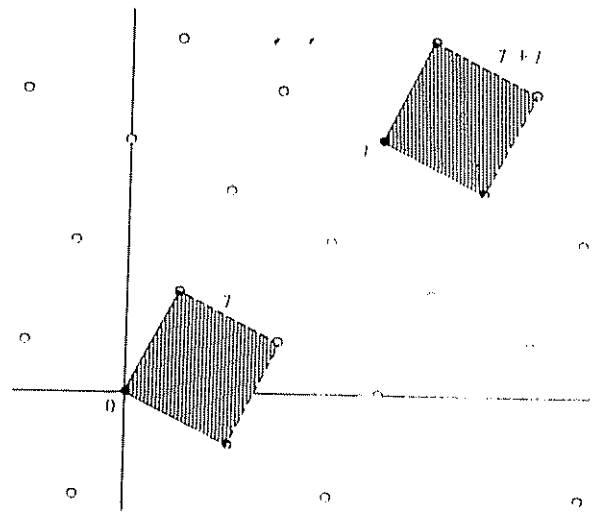
Lemma 5.2

Each element of R^n lies in exactly one of the sets $\boldsymbol{T} + l$ for $l \in L$.

Proof:

Chopping of the integer parts of the coefficients sees this.

The result of the lemma is easy to see in this picture.



The quotient torus

Let L be a lattice in R^n, and assume that L has dimension n. We will study the quotient group R^n / L.

Let S denote the set of all complex numbers modulus 1. That is

$$S = \{a \in \mathbb{C} : a = \alpha + \beta i, 0 \le \alpha, \beta \le 1\}.$$

Under multiplication S is a group, called for obvious reasons the circle group.

Lemma 5.3

The quotient group R/Z is isomorphic to the circle group S.

Proof:

Define a map $\phi : R \to S$ by

$$\phi(x) = e^{2\pi x}.$$

Then ϕ is a surjective homomorphism with kernel Z, and the lemma follows from the isomorphism theorem.

Definition

Let T^n denote the direct product of n copies of S, and call this the n-dimensional torus.

For example $T^2 = S \times S$ is the usual torus or donut.

Theorem 5.4

If L is an n-dimensional lattice in R^n then R^n / L is isomorphic to the n-dimensional torus T^n.

Proof:

Let $\{e_1, \ldots, e_n\}$ be generators for L. Then $\{e_1, \ldots, e_n\}$ is a basis for R^n. Define $\phi : R^n \to T^n$ by

$$\phi(a_1 e_1, \ldots, a_n e_n) = (e^{2\pi a_1}, \ldots, e^{2\pi a_n})$$

Then ϕ is a surjective homomorphism, and the kernel of ϕ is L.

Lemma 5.5

The map ϕ defined above, when restricted to the fundamental domain $\boldsymbol{T}$ yields a bijection $\boldsymbol{T} \to T^n$.

Geometrically, T^n is obtained by glueing opposite faces of the closure of the fundamental domain.

If the dimension of the lattice L is less than n, we have a similar result.

Theorem 5.6

Let L be an m-dimensional lattice in R^n. Then R^n / L is isomorphic to $T^m \times R^{n-m}$.

Proof:

Let V be the subspace spanned by L, and choose a complement W so that $\mathbb{R}^n = V \oplus W$. Then $L \subseteq V$, $V / L \cong T^m$ by previous theorem, and the result follows

Definition

The volume $v(X)$ of a subset $X \subseteq R^n$ is defined in the usual way as

$$\int_X dx_1 \ldots dx_n$$

where $(x_1, \ldots, x_n)$ are coordinates in R^n. Of course the volume exists only when the integral does

Let $L \subseteq R^n$ be a lattice of dimension n, so that $R^n / L \cong T^n$. Let $\boldsymbol{T}$ be a fundamental domain of L. We know there is a bijection $\phi : \boldsymbol{T} \to T^n$, so for any subset X of T^n we can define the volume $v(X)$ by

$$v(X) = v(\phi^{-1}(X))$$

which exists if and only if $\phi^{-1}(X)$ has a volume in R^n.

Let $\nu_N : R^n \to T^n$ be the natural homomorphism with kernel L. ν_N is intuitively "locally volume-preserving". That is, for each $x \in R^n$ there exists a ball of radius ε centred at x, $B_\varepsilon(x)$, such that for all subsets $X \subseteq B_\varepsilon(x)$ for which $v(X)$ exists we have

$$v(X) = v(\nu_N(X)).$$

It is also clear that if an injective map is locally volume preserving then it is volume preserving.

Theorem 5.7

If X is a bounded subset of R^n and $v(X)$ exists, and if $v(\nu_N(X)) \neq v(X)$, then $\nu_N|_X$ is not injective.

Proof:

Assume $\nu_N|_X$ is injective. Now since X is bounded it intersects only a finite number of the sets $\boldsymbol{T} + l$, for $\boldsymbol{T}$ a fundamental domain and $l \in L$. Put

$$X_l = X \cap (\boldsymbol{T} + l).$$

Then we have

$$X = X_{l_1} \cup \ldots \cup X_{l_m}$$

For each l_i define

$$Y_{l_i} = X_{l_i} - l_i$$

so that $Y_{l_i} \subseteq \boldsymbol{T}$. Since $\nu_N(x - l_i) = \nu_N(x)$ for all $x \in R^n$, from the assumed injectivity of ν_N we get that the Y_{l_i} are disjoint. Now

$$v(X_{l_i}) = v(Y_{l_i})$$

for all i. Also

$$\nu_N(X_{l_i}) = \phi(Y_{l_i})$$

where ϕ is the bijection $\boldsymbol{T} \to T''$. Hence

$$\begin{aligned} v(\nu_N(X)) &= v(\nu_N(\bigcup X_{l_i})) \\ &= v(\bigcup Y_{l_i}) \\ &= \sum v(Y_{l_i}) \\ &= \sum v(X_{l_i}) \\ &= v(X), \end{aligned}$$

which is a contradiction.

Minkowski's theorem

First we will need some definitions about some properties of a subset.

Definition

A subset $X \subseteq R^n$ is said to be convex if whenever $x, y \in X$ then all points on the straight line segment joining x to y also lie in X.

Another way of saying this is that X is convex if, whenever $x, y \in X$, the point

$$\lambda x + (1-\lambda)y$$

is an element of X for all real λ such that $0 \le \lambda \le 1$.

Examples are a circle, a square, an ellipse or a triangle. They are all convex in R^2, but a torus is not convex in R^3.

Definition

A subset $X \subseteq R^n$ is said to be symmetric if $x \in X$ implies that $-x \in X$.

Geometrically this means that X is invariant under reflection in the origin.

Theorem 5.8 (Minkowski's theorem)

Let L be an n-dimensional lattice in R^n with fundamental domain $\boldsymbol{T}$, and let X be a bounded symmetric convex subset of R^n. If

$$v(X) > 2^n v(\boldsymbol{T})$$

then X contains a non-zero point of L.

Proof:

Double the size of L to obtain a lattice $2L$ with fundamental domain $2T$ of volume $2^n v(\boldsymbol{T})$. Consider the torus

$$T'' = R'' / 2L$$

By definition.

$$v(T'') = v(2\boldsymbol{T}) = 2^n v(\boldsymbol{T}).$$

Now the natural map $\nu_N : R'' \to T''$ cannot preserve the volume of X, since this is strictly larger than $v(T'')$. Since $\nu_N(X) \subseteq T''$ we have

$$v(\nu_N(X)) \le v(T'') = 2^n v(\boldsymbol{T}) < v(X)$$

It follows by theorem 5.7 that $\nu_N|_X$ is not injective. Hence there exists $x_1 \neq x_2$, $x_1, x_2 \in X$, such that

$$\nu_N(x_1) = \nu_N(x_2),$$

or equivalently

$$x_1 - x_2 \in 2L. \qquad (*)$$

But $x_2 \in X$, so $-x_2 \in X$ by symmetry, and by convexity we get

$$\frac{1}{2}x_1 + \frac{1}{2}(-x_2) \in X$$

that is

$$\frac{1}{2}(x_1 - x_2) \in X$$

But by (*)

$$\frac{1}{2}(x_1 - x_2) \in L$$

Hence

$$0 \neq \frac{1}{2}(x_1 - x_2) \in X \cap L$$

as required.

As a consequence of Minkowski's theorem in number theory we have the following two theorems, the two-squares theorem and the four-squares theorem. The two-square theorem goes back to Fermat who stated it in a letter to Mersenne in 1640. It was proved by Euler in 1754.
Euler spent 40 years trying to prove the four-square theorem but Lagrange succeeded in 1770.

Theorem 5.9

If p is prime of the form $4k+1$ then p is a sum of two integer squares.

Proof:

The multiplicative group of the field Z_p, G, is cyclic and has order $p-1 = 4k$. It therefore contains an element u of order 4. Then $u^2 \equiv -1 (\mathrm{mod}\, p)$ since -1 is the only element of order 2 in G.

Let $L \subseteq Z^2$ be the lattice in R^2 consisting of all pairs (a,b), $a,b \in Z$, such that $b \equiv ua (\mathrm{mod}\, p)$. This is a subgroup of Z^2 of index p so the volume of a fundamental domain for L is p. By Minkowski's theorem any circle, centred at the origin, of radius r, which has area $\pi r^2 > 4p$

contains a non-zero point of L This is the case for $r^2 = 3p/2$ So there exists a point $(a,b) \in L$, not the origin, for which

$$0 \neq a^2 + b^2 \leq r^2 = 3p/2 < 2p$$

But modulo p we have

$$a^2 + b^2 \equiv a^2 + ua^2 \equiv 0$$

Hence $a^2 + b^2$, being a multiple of p strictly between 0 and $2p$, must equal p

Theorem 5.10

Every positive integer is a sum of four integer squares.

Proof:

We prove the theorem by proving it for all primes p and then extending the result to all integers Because we have

$$2 = 1^2 + 1^2 + 0^2 + 0^2$$

we may assume that p is an odd prime. The congruence

$$u^2 + v^2 \equiv 0 (\text{mod } p)$$

has a solution $u, v \in Z$. Because u^2 takes exactly $(p+1)/2$ distinct values for $u = 0, \ldots, p-1$, and $-1 - v^2$ also takes $(p+1)/2$ distinct values, so for the congruence to have no solution all these $p+1$ values must be distinct. But then we would have $p+1 \leq p$ which is a contradiction

For such a choice of u, v consider the lattice $L \subseteq Z^4$ consisting of (a,b,c,d) such that $c \equiv ua + vb (\text{mod } p)$ and $d \equiv ub - va (\text{mod } p)$. Then L has index p^2 in Z^4 so the volume of a fundamental domain is p^2.

Now a four dimensional sphere, centred at the origin, has volume $\pi^2 r^4 / 2$ and we choose r to make this greater than $16p^2$, say $r^2 = 1.9p$ Then there exists a lattice point $0 \neq (a,b,c,d)$ in this sphere such that

$$0 \neq a^2 + b^2 + c^2 + d^2 \leq r^2 = 1.9p < 2p$$

Modulo p, it is easy to see that $a^2 + b^2 + c^2 + d^2 \equiv 0$ and hence must equal p.

To deal with an arbitrary integer n, it suffices to factorise n into primes and then use the identity

$$(a^2 + b^2 + c^2 + d^2)(A^2 + B^2 + C^2 + D^2) = (aA - bB - cC - dD)^2 +$$
$$+ (aB + bA + cD - dC)^2 + (aC - bD - cA - dB)^2 + (aD + bC - cB + dA)^2$$

6. Geometric representation of algebraic numbers

Let $K = Q(\theta)$ be a number field of degree n, where θ is an algebraic integer. Let $\sigma_1, \ldots, \sigma_n$ be the set of all monomorphisms $K \to C$. If $\sigma_j(K) \subseteq R$, which happens if and only if $\sigma_j(\theta) \in R$, we say that σ_j is real; otherwise σ_j is complex. Define

$$\overline{\sigma_j}(\alpha) = \overline{\sigma_j(\alpha)}$$

where the bar denotes complex conjugate. Since complex conjugation is an automorphism of C it follows that $\overline{\sigma_j}$ is a monomorphism $K \to C$, so equals σ_j for some j. Now $\sigma_j = \overline{\sigma_j}$ if and only if σ_j is real, and $\overline{\sigma_j} = \sigma_j$, so the complex monomorphisms comes in conjugate pairs. Hence

$$n = s + 2t$$

where s is the number of real monomorphisms and $2t$ is the number of complex monomorphisms. We can rearrange the monomorphisms so that the system of monomorphisms $K \to C$ is

$$\sigma_1, \ldots, \sigma_s, \sigma_{s+1}, \overline{\sigma_{s+1}}, \ldots, \sigma_{s+t}, \overline{\sigma_{s+t}}$$

where $\sigma_1, \ldots, \sigma_s$ are real and the rest are complex.

Definition

The set of all $(s+t)$-tuples, $x = (x_1, \ldots, x_s, x_{s+1}, \ldots, x_{s+t})$ where $x_1, \ldots x_s \in R$ and $x_{s+1}, \ldots x_{s+t} \in C$, is a vector space over R, and a ring (in fact it is an R-algebra). Hence we can define

$$L^n = R^s \times C^t$$

As a vector space over R it has dimensions $s + 2t = n$.

For $x \in L^n$ we define the norm as

$$N(x) = x_1 \ldots x_s \, |x_{s+1}|^2 \ldots |x_{s+t}|^2 .$$

The norm has two obvious properties:

1) $N(x)$ is real for all x.
2) $N(xy) = N(x)N(y)$.

We define a map

$$\sigma : K \to L^n$$

by

$$\sigma(\alpha) = \left(\sigma_1(\alpha), \ldots, \sigma_s(\alpha), \sigma_{s+1}(\alpha), \ldots, \sigma_{s+t}(\alpha)\right)$$

for all $\alpha \in K$. Clearly

$$\sigma(\alpha + \beta) = \sigma(\alpha) + \sigma(\beta)$$
$$\sigma(\alpha\beta) = \sigma(\alpha)\sigma(\beta)$$

for all $\alpha, \beta \in K$; so σ is a ring homomorphism. If r is a real number then

$$\sigma(r\alpha) = r\sigma(\alpha)$$

so σ is a Q-algebra homomorphism.

Since

$$N(\alpha) = \sigma_1(\alpha) \ldots \sigma_s(\alpha)\sigma_{s+1}(\alpha)\overline{\sigma_{s+1}}(\alpha) \ldots \sigma_{s+t}(\alpha)\overline{\sigma_{s+t}}(\alpha)$$

we have that

$$N(\sigma(\alpha)) = N(\alpha).$$

Example:

For the number field $K = Q(\sqrt{d})$ we have

If $d > 0$:

Then $\theta_1 = \sqrt{d}$, $\theta_2 = -\sqrt{d}$. So for $k \in K$ we have $k = a + b\sqrt{d}$ for $a, b \in Q$. Then $\sigma : K \to L^{(r)}$ is given by

$$a + b\sqrt{d} \mapsto (a + b\sqrt{d}, a - b\sqrt{d})$$

so the norm is

$$N(\sigma(a + b\sqrt{d})) = (a + b\sqrt{d})(a - b\sqrt{d}) = a^2 - db^2 = N(a + b\sqrt{d}).$$

If $d < 0$:

Then $\theta_1 = i\sqrt{d}$, $\theta_2 = -i\sqrt{d}$. So for $\alpha \in K$ we have $\alpha = a + bi\sqrt{d}$ for $a, b \in Q$. Then $\sigma : K \to L^{(r)}$ is given by

$$\alpha \mapsto (\alpha, \overline{\alpha}) = (a + bi\sqrt{d}, a - bi\sqrt{d})$$

so the norm is

$$N(\sigma(\alpha)) = \alpha\overline{\alpha} = a^2 + db^2 = N(\alpha).$$

Lemma 6.1

σ is injective.

Proof:

The kernel of σ is an ideal of K since σ is a ring homomorphism. Since K is a field this means that either σ is identically zero or σ is injective. But

$$\sigma(1) = (1, 1, \ldots, 1) \neq 0$$

so σ must be injective.

Theorem 6.2

If $\{\alpha_1, \ldots, \alpha_n\}$ is a basis for K over Q then $\sigma(\alpha_1), \ldots, \sigma(\alpha_n)$ are linearly independent over R.

Proof:

Linear independence over Q is immediate since σ is injective But we have to show linear independence over R Let

$\sigma_k(\alpha_l) = x_k^{\,l}$ $\qquad (k = 1, \ldots, s)$

$\sigma_{s+j}(\sigma_l) = y_j^{\,l} + iz_j^{\,l}$ $\qquad (j = 1, \ldots, t)$

where $x_k^{\,l}$, $y_k^{\,l}$ and $z_k^{\,l}$ are real Then

$$\sigma(\alpha_l) = \left(x_1^{\,l}, \ldots, x_s^{\,l} : y_1^{\,l} + iz_1^{\,l}, \ldots, y_t^{\,l} + iz_t^{\,l}\right)$$

so it is sufficient to prove that the determinant

$$D = \begin{vmatrix} x_1^{(1)} & \cdots & x_s^{(1)} & y_1^{(1)} & z_1^{(1)} & \cdots & y_t^{(1)} & z_t^{(1)} \\ \vdots & & \vdots & \vdots & \vdots & & \vdots & \vdots \\ x_1^{(n)} & \cdots & x_s^{(n)} & y_1^{(n)} & z_1^{(n)} & \cdots & y_t^{(n)} & z_t^{(n)} \end{vmatrix}$$

is not zero Put

$$\mathbf{E} = \begin{vmatrix} x_1^{(1)} & \cdots & x_s^{(1)} & y_1^{(1)} + iz_1^{(1)} & y_1^{(1)} - iz_1^{(1)} & \cdots \\ \vdots & & \vdots & \vdots & \vdots & \\ x_1^{(n)} & \cdots & x_s^{(n)} & y_1^{(n)} + iz_1^{(n)} & y_1^{(n)} - iz_1^{(n)} & \cdots \end{vmatrix}$$

$$= \begin{vmatrix} \sigma_1(\alpha_1) & \cdots & \sigma_s(\alpha_1) & \sigma_{s+1}(\alpha_1) & \overline{\sigma_{s+1}}(\alpha_1) & \cdots \\ \vdots & & \vdots & \vdots & \vdots & \\ \sigma_1(\alpha_n) & \cdots & \sigma_s(\alpha_n) & \sigma_{s+1}(\alpha_n) & \overline{\sigma_{s+1}}(\alpha_n) & \cdots \end{vmatrix}$$

Then

$$\mathbf{E}^2 = \Delta[\alpha_1, \ldots, \alpha_n]$$

by the definition of the discriminant, and by theorem 1 7 $\mathbf{E}^2 \neq 0$ Now elementary properties of determinants give

$$\mathbf{E} = (-2i)^t \mathbf{D}$$

so that $\mathbf{D} \neq 0$ as required

Corollary 6.3

Q-linearly independent elements of K map under σ to R-linearly independent elements of L^{st}

Corollary 6.4

If G is a finitely generated subgroup of $(K,+)$ with Z-basis $\{\alpha_1, \ldots, \alpha_m\}$ then the image of G in L^{st} is a lattice with generators $\sigma(\alpha_1), \ldots, \sigma(\alpha_m)$

Now we want to define the length of a vector and the distance between two points in the space L^{st} We can easily pick a basis such that the element

$$(x_1, \ldots, x_s; y_1 + iz_1, \ldots, y_t + iz_t)$$

of L^{st} has coordinates

$$(x_1, \ldots, x_s, y_1, z_1, \ldots, y_t, z_t)$$

Then the inner product is defined by

$$(x, x') = x_1 x_1' + \ldots + x_{s+2t} x_{s+2t}'$$

The length of a vector is then

$$\| x \| = \sqrt{(x, x)}$$

and the distance between two vectors x and x' is $\| x - x' \|$

Hence for $x = (x_1, \ldots, x_s; y_1 + iz_1, \ldots, y_t + iz_t)$ we have

$$\| x \| = \sqrt{x_1^2 + \ldots + x_s^2 + y_1^2 + z_1^2 + \ldots + y_t^2 + z_t^2}$$

7. The class-group and class number

We will develop some methods to measure the extent to which ideals are non-principal or to which extent factorisation is not unique.

Let $\mathcal{D}$ be the ring of integers of a number field K of degree n. We know that prime factorisation is unique if and only if every ideal of $\mathcal{D}$ is principal. So we whish to study how far away the ideals are from being principal.

To do this we will use the group of fractional ideals. Recall that $\mathbf{a}$ is a fractional ideal if there exists some non-zero $c \in \mathcal{D}$ such that $c\mathbf{a} \subseteq \mathcal{D}$. We say that a fractional ideal is principal if it is of the form $c^{-1}\mathbf{a}$ where $\mathbf{a}$ is principal in $\mathcal{D}$.

Let $\mathcal{F}$ denote the group of fractional ideals under multiplication. Then the set $\mathcal{P}$ of principal fractional ideals is a subgroup of $\mathcal{F}$.

Definition

The class-group of $\mathcal{D}$ is the quotient group

$$\mathcal{H} = \mathcal{F}/\mathcal{P}$$

and the class number, h, is the order of $\mathcal{H}$. That is $h = \left|\mathcal{F}/\mathcal{P}\right|$

We can describe the elements of $\mathcal{H}$ in a more convenient way:

For the set $\mathcal{F}$ of all ideals, define a relation ~ by $x \sim n$ if and only if there exist principal ideals $\mathbf{d}, \mathbf{e}$ such that $\mathbf{xd} = \mathbf{ne}$. Then $\mathcal{H}$ is the set of equivalence classes $[\mathbf{x}]$, with group operation defined by $[\mathbf{x}][\mathbf{n}] = [\mathbf{xn}]$.

The use of the class group is that it captures the extent to which factorisation is not unique, as we see in the following theorem.

Theorem 7.1

Factorisation in $\mathcal{D}$ is unique if and only if the class-group $\mathcal{H}$ has order 1, or equivalently the class number $h = 1$.

Proof:

Factorisation is unique if and only if every ideal of $\mathcal{D}$ is principal by theorem 4.15. which in turn is true if and only if every fractional ideal is principal, which is equivalent to $\mathcal{F} = \mathcal{P}$, which is equivalent to $|\mathcal{H}| = h = 1$.

Lemma 7.2

If M is a lattice in L^n of dimension $s + 2t$ having fundamental domain of volume V, and if $c_1, \ldots, c_{s+t}$ are positive real numbers whose product

$$c_1 \ldots c_{s+t} > \left(\frac{4}{\pi}\right)^t V$$

then there exists in M a non-zero element

$$x = (x_1, \ldots, x_{s+t})$$

such that

$$|x_1| < c_1, \ldots, |x_s| < c_s$$
$$|x_{s+1}|^2 < c_{s+1}, \ldots, |x_{s+t}|^2 < c_{s+t}.$$

Proof:

Let X be the set of all points $x \in L^n$ for which the inequalities holds. By computing the volume of X we get

$$v(X) = \int_{-c_1}^{c_1} dx_1 \cdots \int_{-c_s}^{c_s} dx_s \times \iint_{y_1^2+z_1^2<c_{s+1}} dy_1 dz_1 \times \cdots \times \iint_{y_t^2+z_t^2<c_{s+t}} dy_t dz_t$$
$$= 2c_1 \; 2c_2 \cdots 2c_s \; \pi c_{s+1} \cdots \pi c_{s+t}$$
$$= 2^s \pi^t c_1 \cdots c_{s+t}$$

Now X is a cartesian product of line segments and circular discs, so X is bounded symmetric and convex. Hence by Minkowski's theorem such an element exists if

$$2^s \pi^t c_1 \cdots c_{s+t} > 2^{s+2t} V$$

By rearranging the factors we obtain the result:

$$c_1 \cdots c_{s+t} > \left(\frac{4}{\pi}\right)^t V$$

Theorem 7.3

Let L be an n-dimensional lattice in R^n with basis $\{e_1, \ldots, e_n\}$. Suppose

$$e_i = (a_{1i}, \ldots, a_{ni}).$$

Then the volume of the fundamental domain T of L defined by this basis is

$$v(T) = |\det a_{ij}|.$$

Proof:

We have

$$v(T) = \int_T dx_1 \cdots dx_n.$$

Define new variables by

$$x_i = \sum_j a_{ij} y_j.$$

The Jacobian of this transformation is equal to $\det a_{ij}$, and T is the set of points $\sum b_i y_i$ with $0 \le b_i < 1$. By the transformation formula for multiple integrals we have

$$v(T) = \int_T |\det a_{ij}| dy_1 \cdots dy_n = |\det a_{ij}| \int_0^1 dy_1 \cdots \int_0^1 dy_n = |\det a_{ij}|$$

Theorem 7.4

Let K be a number field of degree $n = s + 2t$, with ring of integers $\mathcal{D}$, and let $0 \neq \mathfrak{a}$ be an ideal of $\mathcal{D}$. Then the volume of a fundamental domain for $\sigma(\mathfrak{a})$ in L^n is equal to

$$2^{-t} N(\mathbf{a})\sqrt{|\Delta|}$$

where Δ is the discriminant of K.

Proof:

Let $\{\alpha_1, \ldots, \alpha_n\}$ be a Z -basis for $\mathbf{a}$. Then, in the notation of theorem 6.2, a Z -basis for $\sigma(\mathbf{a})$ in L^M is

$$\left(x_1^{\,1}, \ldots x_s^{\,1}, y_{s+1}^{\,1}, z_{s+1}^{\,1}, \ldots, y_{s+t}^{\,1}, z_{s+t}^{\,1}\right),$$

$$\cdots\cdots\cdots$$

$$\left(x_1^{\,n}, \ldots x_s^{\,n}, y_{s+1}^{\,n}, z_{s+1}^{\,n}, \ldots, y_{s+t}^{\,n}, z_{s+t}^{\,n}\right).$$

Hence by lemma 7.3, if T is a fundamental domain for $\sigma(\mathbf{a})$ we have

$$v(T) = |D|$$

where D is as in theorem 6.2. Using the notation of that theorem we have

$$\mathbf{D} = (-2i)^{-t}\mathbf{E}$$

so that

$$|\mathbf{D}| = 2^{-t}|\mathbf{E}|$$

now $\mathbf{E}^2 = \Delta[\alpha_1, \ldots, \alpha_n]$ and

$$N(\mathbf{a}) = \left|\frac{\Delta[\alpha_1, \ldots, \alpha_n]}{\Delta}\right|$$

by theorem 4.8, whence the result.

We can now combine the results from theorem 7.4 and lemma 7.2 to yield the important

Theorem 7.5

If $\mathbf{a} \neq 0$ is an ideal of $\mathcal{D}$, then $\mathbf{a}$ contains an integer α with

$$N(\alpha) \leq \left(\frac{2}{\pi}\right)^t N(\mathbf{a})\sqrt{|\Delta|}$$

where Δ is the discriminant of K.

Proof:

For a fixed but arbitrary $\varepsilon > 0$ choose positive real numbers $c_1, \ldots, c_{s+t}$ with

$$c_1 \ldots c_{s+t} = \left(\frac{2}{\pi}\right)^t N(\mathbf{a})\sqrt{|\Delta|} + \varepsilon$$

By lemma 7.2 and theorem 7.4 it follows that there exists $0 \neq \alpha \in \mathbf{a}$ such that

$$|\sigma_1(\alpha)| < c_1, \ldots, |\sigma_s(\alpha)| < c_s$$

$$|\sigma_{s+1}(\alpha)|^2 < c_{s+1}, \ldots |\sigma_{s+t}(\alpha)|^2 < c_{s+t}$$

Multiplying all these inequalities together we get

$$N(\alpha) \leq c_1 \ldots c_{s+t} = \left(\frac{2}{\pi}\right)^t N(\mathbf{a})\sqrt{|\Delta|} + \varepsilon$$

Since a lattice is discrete, it follows that the set A_ε of such α is finite. Also $A_\varepsilon \neq \emptyset$, so that $A = \bigcap_\varepsilon A_\varepsilon = \emptyset$ If we pick $\alpha \in A$ then

$$N(\alpha) \leq \left(\frac{2}{\pi}\right)^t N(\mathbf{a})\sqrt{|\Delta|}$$

Corollary 7.6

Every non-zero ideal $\mathbf{a}$ of $\mathcal{D}$ is equivalent to an ideal whose norm is $\leq \left(\frac{2}{\pi}\right)^t \sqrt{|\Delta|}$.

Proof:

The class of fractional ideals equivalent to $\mathbf{a}^{-1}$ contains an ideal $\mathbf{c}$, so $\mathbf{ac} \sim \mathcal{D}$. We can use theorem 7.5 to find an integer $\gamma \in \mathbf{c}$ such that

$$N(\gamma) \leq \left(\frac{2}{\pi}\right)^t N(\mathbf{c})\sqrt{|\Delta|}.$$

Since $\mathbf{c} \mid \gamma$ we have

$$\langle \gamma \rangle = \mathbf{cb}$$

for some ideal $\mathbf{b}$ Since $N(b)N(c) = N(bc) = N(\langle\gamma\rangle) = |N(\gamma)|$ we have

$$N(\mathbf{b}) \leq \left(\frac{2}{\pi}\right)^t \sqrt{|\Delta|}$$

Since $\mathbf{c} \sim \mathbf{a}^{-1}$ and $\mathbf{b} \sim \mathbf{c}^{-1}$ we must have that $\mathbf{b} \sim \mathbf{a}$

Next we will show the finiteness of the class-number.

Theorem 7.7

The class-group of a finite number field is a finite abelian group. The class-number h is finite.

Proof:

Let K be a number field, of discriminant Δ, and degree $n = s + 2t$ as usual. We know that the class-group $\mathcal{H} = \mathcal{F}/\mathcal{P}$ is abelian, so it remains to prove that $\mathcal{H}$ is finite Well, $\mathcal{H}$ is finite if and only if the number of distinct equivalence classes of ideals is finite Let $[\mathbf{c}]$ be such an equivalence class. Then $[\mathbf{c}]$ contains an ideal $\mathbf{a}$, and by corollary 7.6 $\mathbf{a}$ is equivalent to an ideal $\mathbf{b}$ with $N(\mathbf{b}) \leq (2/\pi)^t \sqrt{|\Delta|}$ Since only finitely many ideals have a given norm (theorem 4.12) there are only finitely many choices for $\mathbf{b}$. Since $[\mathbf{c}] = [\mathbf{a}] = [\mathbf{b}]$ it follows that there are only finitely many equivalence classes $[\mathbf{c}]$, whence $\mathcal{H}$ is a finite group and $h = |\mathcal{H}|$ is finite

Proposition 7.8

Let K be a number field of class-number h, and $\mathbf{a}$ an ideal of the ring of integers $\mathcal{D}$. Then

1) $\mathbf{a}^h$ is principal.

2) If q is prime to h and $\mathbf{a}^q$ is principal, then $\mathbf{a}$ is principal.

Proof:

Since $h = |\mathcal{H}|$ we have $[\mathbf{a}]^h = [\mathcal{D}]$ for all $[\mathbf{a}] \in \mathcal{H}$, because $[\mathcal{D}]$ is the identity element of $\mathcal{H}$. Hence $[\mathbf{a}^h] = [\mathbf{a}]^h = [\mathcal{D}]$, so $\mathbf{a}^h \sim \mathcal{D}$ and hence $\mathbf{a}^h$ is principal.

For the second part choose $u, v \in \mathbb{Z}$ such that $uh + vq = 1$. Then $[\mathbf{a}]^q = [\mathcal{D}]$, so we have

$$[\mathbf{a}] = [\mathbf{a}]^{uh+vq} = ([\mathbf{a}]^h)^u ([\mathbf{a}]^q)^v = [\mathcal{D}]^u [\mathcal{D}]^v = [\mathcal{D}]$$

Hence again $\mathbf{a}$ is principal.

Example:

We can find all square free integers d in $-20 < d < 20$ such that the class number of $Q(\sqrt{d})$ is 1. By using the theorems 3.17, 3.18 and 3.19 and combining these with theorem 3.16 we get that the numbers of d are: $-11,-7,-3,-2,-1,2,3,5,7,11,13,17,19$.

Example:

We can also calculate the class number of $Q(\sqrt{d})$ for d square free and $-10 < d < 10$. We know so far that

d	-7	-6	-5	-3	-2	-1	2	3	5	6	7
$\lvert\Delta\rvert$	7	24	20	3	8	4	8	12	5	24	28
$\frac{2}{\pi}\sqrt{\lvert\Delta\rvert} \approx$	1,68	3,12	2,84	1,10	1,80	1,27	1,80	2,21	1,42	3,12	3,36
Norm of ideals $\leq$	1	3	2	1	1	1	1	2	1	3	3

Because we know the integers d for which the class number is 1 from the previous example we have only to calculate the class number for d: $-6,-5,3,6$.

Starting of with $Q(\sqrt{-6})$ we have that the ideals of $\mathcal{D}$ have norms 1,2 or 3. An ideal of norm 1 is the whole ring $\mathcal{D}$, hence principal. An ideal $\mathbf{a}$ of norm 2 satisfies $\mathbf{a} \mid 2$ so by theorem 4.11(2) $\mathbf{a}$ is a factor of $\langle 2 \rangle$. Similarly, an ideal $\mathbf{b}$ of norm 3 satisfies $\mathbf{b} \mid 3$ and so $\mathbf{b}$ is a factor of $\langle 3 \rangle$. But

$$\langle 2 \rangle = \langle 2, \sqrt{-6} \rangle^2,$$
$$\langle 3 \rangle = \langle 3, \sqrt{-6} \rangle^2,$$

where $\langle 2, \sqrt{-6} \rangle$ and $\langle 3, \sqrt{-6} \rangle$ are prime and has norm 2 and 3, respectively. Hence $\langle 2, \sqrt{-6} \rangle$ and $\langle 3, \sqrt{-6} \rangle$ are the only ideals of norm 2 and 3, and so $h \leq 3$. It is easy to see that the ideals $\langle 2, \sqrt{-6} \rangle$ and $\langle 3, \sqrt{-6} \rangle$ are equivalent fractional ideals ($\langle 2, \sqrt{-6} \rangle \langle 3, \sqrt{-6} \rangle = \langle 6 \rangle \langle 3, \sqrt{-6} \rangle$), so we must have that $h = 2$.

For $Q(\sqrt{-5})$ we get similarly that there is an ideal $\mathbf{a}$ of norm 2 and so we get

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

where $\langle 2,1+\sqrt{-5}\rangle$ is prime and has norm 2, is the only ideal of norm 2. Hence every ideal is equivalent to $\mathcal{D}$ or to $\langle 2,1+\sqrt{-5}\rangle$. Hence $h=2$.

For $\mathcal{Q}(\sqrt{3})$ ideals have norm 1 or 2. So from

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

where $\langle 2,1+\sqrt{3}\rangle$ is prime and has norm 2, we see that $2-(1+\sqrt{3})\in\langle 2,1+\sqrt{3}\rangle$ but $2-(1+\sqrt{3})=1-\sqrt{3}\in\langle 2,1+\sqrt{3}\rangle$ and so $\langle 2,1+\sqrt{3}\rangle=\langle 1-\sqrt{3}\rangle$. Hence $\langle 2,1+\sqrt{3}\rangle$ is equivalent to the whole group $\mathcal{D}$ and so we get that $h=1$

For $\mathcal{Q}(\sqrt{6})$ the are ideals of $\mathcal{D}$ have norm 1,2 or 3. Now the ideals $\langle 2,\sqrt{6}\rangle$ and $\langle 3,\sqrt{6}\rangle$ are prime and have norms 2 and 3 respectively but we can easily check that they are equivalent

$$\langle 2,\sqrt{6}\rangle\langle 3\sqrt{6}\rangle = \langle 3,\sqrt{6}\rangle\langle 6\rangle$$

Hence there are only ideals equivalent to $\mathcal{D}$ or to $\langle 2,\sqrt{6}\rangle$. But, by noting that $2-\sqrt{6}\in\langle 2,\sqrt{6}\rangle$ we get that $2=-(2-\sqrt{6})(2+\sqrt{6})$ and so $\langle 2,\sqrt{6}\rangle=\langle 2+\sqrt{6}\rangle$. Hence all ideals are equivalent to $\mathcal{D}$ and thus the class number is $h=1$.

To sum up we have calculated:

d	-7	-6	-5	-3	-2	-1	2	3	5	6	7
Class number	1	2	2	1	1	1	1	1	1	1	1

8. Computational methods of the class-number

We will now develop some methods of calculating the class-number of a number field in a practical way. We will start by studying how a rational prime breaks up into prime ideals in a number field.

If p is a rational prime number in $\mathbb{Z}$ it is not generally true that the ideal generated by p, $\langle p \rangle$, is a prime ideal in the ring of integers $\mathcal{D}$ of a number field K. For example, in $\mathbb{Q}(\sqrt{-1})$ we have the factorisation

$$\langle 2 \rangle = \langle 1 + \sqrt{-1} \rangle^2 .$$

It would be convenient to us if we were able to compute the prime factors of $\langle p \rangle$. In the case where the ring of integers is generated by a single element (which is the case with quadratic and cyclotomic fields) we have the following useful theorem by Dedekind.

Theorem 8.1

Let K be a number field of degree n with ring of integers $\mathcal{D} = \mathbb{Z}[\theta]$ generated by $\theta \in \mathcal{D}$. Given a rational prime p, suppose the minimum polynomial f of θ over $\mathbb{Q}$ gives rise to the factorisation into irreducibles over $\mathbb{Z}_p$:

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

where the bar denotes the natural map $\mathbb{Z}[t] \to \mathbb{Z}_p[t]$. Then if $f_i \in \mathbb{Z}[t]$ is any polynomial mapping onto $\overline{f}_i$, the ideal

$$\mathfrak{p}_i = \langle p \rangle + \langle f_i(\theta) \rangle$$

is prime and the prime factorisation of $\langle p \rangle$ in $\mathcal{D}$ is

$$\langle p \rangle = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_r^{e_r}$$

Proof:

Let θ_i be a root of $\overline{f}_i$ in $\mathbb{Z}_p[\theta_i] \cong \mathbb{Z}_p[t] / \langle \overline{f}_i \rangle$. There is a natural map $\nu_i : \mathbb{Z}[\theta] \to \mathbb{Z}_p[\theta_i]$ given by

$$\nu_i(p(\theta)) = \overline{p}(\theta)$$

The image of ν_i is $\mathbb{Z}_p[\theta_i]$, which is a field, so $\ker \nu_i$ is a prime ideal of $\mathbb{Z}[\theta] = \mathcal{D}$. Clearly

$$\langle p \rangle + \langle f_i(\theta) \rangle \subseteq \ker \nu_i$$

But if $g(\theta) \in \ker \nu_i$ then $\overline{g}(\theta) = 0$, so $\overline{g} = \overline{f}_i \overline{h}$ for some $\overline{h} \in \mathbb{Z}_p[t]$. This means that $g - f_i h \in \mathbb{Z}[t]$ has coefficients divisible by p. Thus

$$g(\theta) = \big(g(\theta) - f_i(\theta)h(\theta)\big) + f_i(\theta)h(\theta) \in \langle p \rangle + \langle f_i(\theta) \rangle$$

which shows that

$$\ker \nu_i = \langle p \rangle + \langle f_i(\theta) \rangle$$

Let

$$\mathfrak{p}_i = \langle p \rangle + \langle f_i(\theta) \rangle .$$

then for each $\overline{f}_i$ the ideal $\mathbf{p}_i$ is prime and satisfies $\langle p\rangle \subseteq \mathbf{p}_i$, i.e. $\mathbf{p}_i \mid \langle p\rangle$

For any ideals $\mathbf{a}$, $\mathbf{b}_1$ and $\mathbf{b}_2$ we have

$$(\mathbf{a}+\mathbf{b}_1)(\mathbf{a}+\mathbf{b}_2) \subseteq \mathbf{a}+\mathbf{b}_1\mathbf{b}_2,$$

so by induction

$$\mathbf{p}_1^{e_1} \cdots \mathbf{p}_r^{e_r} \subseteq \langle p\rangle + \langle f_1(\theta)^{e_1} \cdots f_r(\theta)^{e_r}\rangle \subseteq \langle p\rangle + \langle f(\theta)\rangle = \langle p\rangle$$

Thus $\langle p\rangle \mid \mathbf{p}_1^{e_1} \cdots \mathbf{p}_r^{e_r}$, and the only prime factors of $\langle p\rangle$ are $\mathbf{p}_1, \ldots, \mathbf{p}_r$, hence

$$\langle p\rangle = \mathbf{p}_1^{k_1} \cdots \mathbf{p}_r^{k_r} \qquad (1)$$

where $0 < k_i \le e_i$, $1 \le i \le r$

The norm of $\mathbf{p}_i$ is by definition $\mid \mathcal{D}/\mathbf{p}_i \mid$ and by using the isomorphisms

$$\mathcal{D}/\mathbf{p}_i = Z[\theta]/\mathbf{p}_i \cong Z_p[\theta_i]$$

we find

$$N(\mathbf{p}_i) = \mid Z_p[\theta_i] \mid = p^{d_i}$$

where $d_i = \partial \overline{f}_i = \partial f_i$. Also

$$N(\langle p\rangle) = \mid Z[\theta]/\langle p\rangle \mid = p^n,$$

so taking norms in (1) we get

$$p^n = N(\langle p\rangle) = N(\mathbf{p}_1)^{k_1} \cdots N(\mathbf{p}_r)^{k_r} = p^{d_1k_1 + \cdots + d_rk_r}$$

which implies that

$$d_1k_1 + \cdots + d_rk_r = n = d_1e_1 + \cdots + d_re_r$$

Hence we must have $k_i = e_i$ for $1 \le i \le r$.

Example:

In $K = Q(\sqrt{3})$ we can factorise the ideal $\langle 2\rangle$ by the following:

The minimal polynomial is $x^2 - 3$ so for $p = 2$ we have in $Z_2[t]$:

$$x^2 - 3 \equiv x^2 - 1 \equiv (x-1)(x+1)$$

So with the notation as from the theorem we have

$$\overline{f} = \overline{f}_1\overline{f}_2 = (x-1)(x+1)$$

thus

$$\mathbf{p}_1 = \langle p\rangle + \langle -1+\sqrt{3}\rangle$$

$$\mathbf{p}_2 = \langle p\rangle + \langle 1+\sqrt{3}\rangle$$

Hence $\langle 2\rangle = \left(\langle p\rangle + \langle -1+\sqrt{3}\rangle\right)\left(\langle p\rangle + \langle 1+\sqrt{3}\rangle\right)$.

In $K = Q(\sqrt{5})$ we can factorise the ideal $\langle 3\rangle$:

The minimal polynomial is $x^2 - 5$ so for $p = 3$ we have in $Z_3[t]$:

$$x^2 - 5 \equiv x^2 - 2$$

But $x^2 - 2$ is irreducible in $Z_3[t]$, so we get that $\langle 3\rangle$ is irreducible in $K = Q(\sqrt{5})$.

Example:

In $K = Q(\xi)$, where $\xi = e^{2\pi i/5}$, we have the minimal polynomial $x^4 + x^3 + x^2 + x + 1$. So we factorise the ideal $\langle 2 \rangle$ by noting that in $Z_2[t]$ we have that

$$x^4 + x^3 + x^2 + x + 1 \equiv x + x^2 + x + x + 1 \equiv x^2 + x + 1,$$

where we have used the number theoretic fact that $x^p \equiv x (\mathrm{mod}\, p)$. The polynomial $x^2 + x + 1$ is easily seen to be irreducible so we get that

$$\langle 2 \rangle = \langle 2 \rangle + \langle e^{4\pi i/5} + e^{2\pi i/5} + 1 \rangle.$$

Minkowski's constants

Because the results that are given from lemma 7.2 are much stronger than needed in theorem 7.5 we may improve this, using Minkowski's theorem.

The proof of the theorem contains an inequality between the arithmetic and geometric means:

$$(a_1 \ldots a_n)^{1/n} \leq \frac{1}{n}(a_1 + \ldots + a_n)$$

Theorem 8.2

If $\mathbf{a} \neq 0$ is an ideal of $\mathcal{D}$ then $\mathbf{a}$ contains an element α with

$$|N(\alpha)| \leq \left(\frac{4}{\pi}\right)^t \frac{n!}{n^n}\sqrt{|\Delta|}N(\mathbf{a}),$$

where n is the degree of K and Δ is the discriminant.

Proof:

Let X_c be the set of all $x \in L^n$ such that

$$|x_1| + \ldots + |x_s| + 2\sqrt{y_1 + z_1} + \ldots + 2\sqrt{y_t + z_t} < c,$$

where c is a positive real number. Then X_c is convex and centrally symmetric, and the volume is

$$v(X_c) = 2^s\left(\frac{\pi}{2}\right)^t \frac{1}{n!}c^n.$$

By Minkowski's theorem X_c contains a point $\alpha \neq 0$ of $\sigma(\mathbf{a})$ provided that

$$v(X_c) > 2^{s+2t}v(\boldsymbol{T})$$

where $\boldsymbol{T}$ is a fundamental domain for $\sigma(\mathbf{a})$. By theorem 7.4 we have

$$v(\boldsymbol{T}) = 2^{-t}N(\mathbf{a})\sqrt{|\Delta|}$$

so the condition on X_c becomes

$$2^s\left(\frac{\pi}{2}\right)^t \frac{1}{n!}c^n > 2^{s+2t}2^{-t}N(\mathbf{a})\sqrt{|\Delta|}$$

which is

$$c^n > \left(\frac{4}{\pi}\right)^t n! N(\mathbf{a})\sqrt{|\Delta|}$$

For such α we have

$$|N(\alpha)| = |\sigma_1(\alpha)\ldots\sigma_s(\alpha)\sigma_{s+1}(\alpha)^2\ldots\sigma_{s+t}(\alpha)^2| \le \left(\frac{c}{n}\right)^n$$

by the inequality between arithmetic mean.
Using ε's as in theorem 7.5 we may assume that α can be found for

$$c^n = \left(\frac{4}{\pi}\right)^t n! N(\mathbf{a})\sqrt{|\Delta|}$$

and then

$$|N(\alpha)| = \left(\frac{4}{\pi}\right)^t \frac{n!}{n^n} N(\mathbf{a})\sqrt{|\Delta|}.$$

Corollary 8.3

Every class of fractional ideals contains an ideal $\mathbf{a}$ with

$$N(\mathbf{a}) \le \left(\frac{4}{\pi}\right)^t \frac{n!}{n^n}\sqrt{|\Delta|}.$$

Proof:

The class of fractional ideals equivalent to $\mathbf{a}^{-1}$ contains an ideal $\mathbf{c}$ such that $\mathbf{ac} \sim \mathcal{D}$. We can use theorem 8.2 to find an integer α with such that

$$|N(\alpha)| \le \left(\frac{4}{\pi}\right)^t \frac{n!}{n^n}\sqrt{|\Delta|}N(\mathbf{c})$$

Since $\mathbf{c} \mid \alpha$ we have

$$\langle\alpha\rangle = \mathbf{cb}$$

for some ideal $\mathbf{b}$. Since $N(\mathbf{b})N(\mathbf{c}) = N(\mathbf{bc}) = N(\langle\alpha\rangle) = |N(\alpha)|$ we have

$$N(\mathbf{b}) \le \left(\frac{4}{\pi}\right)^t \frac{n!}{n^n}\sqrt{|\Delta|}$$

Now since $\mathbf{c} \sim \mathbf{a}^{-1}$ and $\mathbf{b} \sim \mathbf{c}$, the result follows.

For an easier notation we introduce the Minkowski's constants:

$$M_{s,t} = \left(\frac{4}{\pi}\right)^t \frac{(s+2t)!}{(s+2t)^{s+2t}}$$

We are now in position to give a criterion for a number field to have class-number 1

Theorem 8.4

Let $\mathcal{D}$ be the ring of integers of a number field K of degree $n = s + 2t$ and with discriminant Δ. Suppose that for every prime $p \in Z$ with $p \le M_{s,t}\sqrt{|\Delta|}$, every prime ideal $\langle p\rangle$ is principal. Then $\mathcal{D}$ has class-number $h = 1$.

Proof:

Every class of fractional ideals contains an ideal $\mathbf{a}$ with $N(\mathbf{a}) \le M_{11}\sqrt{|\Delta|}$ Now $N(a) = p_1 \cdots p_k$ where $p_1, \ldots, p_k \in Z$ and $p_i \le M_{11}\sqrt{|\Delta|}$ Since $\mathbf{a} \mid N(\mathbf{a})$, $\mathbf{a}$ is a product of prime ideals each dividing some p_i By our assumption each of these prime ideals are principal, so $\mathbf{a}$ is principal. Therefore every class of fractional ideals is equal to $[\mathcal{D}]$, and hence $h = 1$.

Example:

We are now in position to do some class number calculations.

In the field $Q(\sqrt{-19})$ the ring of integers is $\mathcal{D} = Z[\frac{1}{2} + \frac{1}{2}\sqrt{-19}]$ and the discriminant is -19. The minimal polynomial is $f(x) = x^2 - x + 5$. Now we have that

$$M_{01} = \frac{4}{\pi}\cdot\frac{2!}{2^2} \approx 0.637$$

so $M_{01}\sqrt{19} \approx 2.77$. Hence, by theorem 8.3 we get that every class of fractional ideals contains an ideal with norm $\le M_{01}\sqrt{19} \approx 2.77$ so we need only to check for the prime 2. $f(x) = x^2 - x + 5 \equiv x^2 + x + 1 (\mathrm{mod}\, 2)$, which is irreducible in $Z_2[x]$, so the ideal dividing $\langle 2\rangle$ is principal by theorem 8.4. Hence $[\langle 2\rangle] = [\mathcal{D}]$ and so $h = 1$.

In the field $Q(\sqrt{-17})$ the ring of integers is $\mathcal{D} = Z[\sqrt{-17}]$ and the discriminant is $-4\cdot 17 = 68$.

Minimal polynomial: $f(x) = x^2 + 17$

$M_{01} = 0.637$

$M_{01}\sqrt{68} \approx 5.23$

So we need to investigate primes less than or equal to 7, that is 2,3,5,7. Now

$x^2 + 17 \equiv x^2 - 1 = (x-1)(x+1) (\mathrm{mod}\, 2)$

$x^2 + 17 \equiv x^2 - 1 = (x-1)(x+1) (\mathrm{mod}\, 3)$

$x^2 + 17 \equiv x^2 + 2 (\mathrm{mod}\, 5)$ (Irreducible)

$x^2 + 17 \equiv x^2 + 3 = (x+2)(x+5) (\mathrm{mod}\, 7)$

so we get the following prime factorisations:

$\langle 2\rangle = \langle 2, 1 - \sqrt{-17}\rangle\langle 2, 1 + \sqrt{-17}\rangle$

$\langle 3\rangle = \langle 3, 1 - \sqrt{-17}\rangle\langle 3, 1 + \sqrt{-17}\rangle$

$\langle 7\rangle = \langle 7, 2 + \sqrt{-17}\rangle\langle 7, 5 + \sqrt{-17}\rangle$

All of the factors are prime and from the equations

$2 - (1 - \sqrt{-17}) = 1 + \sqrt{-17}$

$3(-7 + 2\sqrt{-17}) + (6 + \sqrt{-17})(1 - \sqrt{-17}) = 2 + \sqrt{-17}$

$3(9 + 2\sqrt{-17}) + (-8 + \sqrt{-17})(1 + \sqrt{-17}) = 2 - \sqrt{-17}$

we get that $\langle 2,1-\sqrt{-17}\rangle \Leftrightarrow \langle 2,1+\sqrt{-17}\rangle$ are equivalent. And also

$\langle 3,1-\sqrt{-17}\rangle \Leftrightarrow \langle 7,5+\sqrt{-17}\rangle$

$\langle 3,1+\sqrt{-17}\rangle \Leftrightarrow \langle 7,2+\sqrt{-17}\rangle$

Hence $h=4$.

In the field $Q(\sqrt{-15})$ the ring of integers is $\mathcal{D}=Z[\frac{1}{2}+\frac{1}{2}\sqrt{-15}]$ and the discriminant is -15.

Minimal polynomial: $f(x)=x^2-x+4$

$M_{0,1}=0.637$

$M_{0,1}\sqrt{15}\approx 2.47$

So we need to investigate primes less than or equal to 3, that is 2,3. Now

$x^2-x+4\equiv x(x+1)(\mathrm{mod}\,2)$

$x^2-x+4\equiv x^2+2x+1=(x+1)^2(\mathrm{mod}\,3)$

so we get the following prime factorisations:

$\langle 2\rangle=\langle 2,\sqrt{-15}\rangle\langle 2,1+\sqrt{-15}\rangle$

$\langle 3\rangle=\langle 3,1+\sqrt{-15}\rangle^2$

All of the factors are prime and from the equations

$2(8+\sqrt{-15})-(-1+\sqrt{-15})\sqrt{-15}=1+\sqrt{-15}$

$2(1-\sqrt{-15})+(1+\sqrt{-15})=3$

we get that $\langle 2,\sqrt{-15}\rangle \Leftrightarrow \langle 2,1+\sqrt{-15}\rangle$ are equivalent. And also

$\langle 2,1+\sqrt{-15}\rangle \Leftrightarrow \langle 3,1+\sqrt{-15}\rangle$

Hence $h=2$.

In the field $Q(\sqrt{-14})$ the ring of integers is $\mathcal{D}=Z[\sqrt{-14}]$ and the discriminant is $-4\cdot 14=56$.

Minimal polynomial: $f(x)=x^2+14$

$M_{0,1}=0.637$

$M_{0,1}\sqrt{56}\approx 4.76$

So we need to investigate primes less than or equal to 5, that is 2,3,5. Now

$x^2+14\equiv x^2(\mathrm{mod}\,2)$

$x^2+14\equiv x^2-1=(x-1)(x+1)(\mathrm{mod}\,3)$

$x^2+14\equiv x^2-1=(x-1)(x+1)(\mathrm{mod}\,5)$

so we get the following prime factorisations:

$\langle 2\rangle=\langle 2,\sqrt{-14}\rangle^2$

$\langle 3\rangle=\langle 3,1+\sqrt{-14}\rangle\langle 3,1-\sqrt{-14}\rangle$

$\langle 5\rangle=\langle 5,1+\sqrt{-14}\rangle\langle 5,1-\sqrt{-14}\rangle$

All of the factors are prime and from the equations

$\langle 3,1+\sqrt{-14}\rangle\langle 1-\sqrt{-14}\rangle = \langle 3\rangle\langle 5,1-\sqrt{-14}\rangle$

$\langle 5,1+\sqrt{-14}\rangle\langle 1-\sqrt{-14}\rangle = \langle 5\rangle\langle 3,1-\sqrt{-14}\rangle$

we get that $\langle 3,1+\sqrt{-14}\rangle \Leftrightarrow \langle 5,1-\sqrt{-14}\rangle$ are equivalent. And also

$\langle 5,1+\sqrt{-17}\rangle \Leftrightarrow \langle 3,1-\sqrt{-14}\rangle$

Since $\langle 2,\sqrt{-14}\rangle$ is not equivalent to any of these two we have four different equivalence classes in the class group. Hence $h=4$.

In the field $Q(\sqrt{-13})$ the ring of integers is $\mathcal{D} = Z[\sqrt{-13}]$ and the discriminant is $-4\ 13 = 52$.

Minimal polynomial: $f(x) = x^2 + 13$

$M_{01} = 0.637$

$M_{01}\sqrt{52} \approx 4.59$

So we need to investigate primes less than or equal to 5, that is 2,3,5. Now

$x^2 + 13 \equiv x^2 - 1 = (x-1)(x+1) \pmod 2$

$x^2 + 13 \equiv x^2 + 1 \pmod 3$ (irreducible)

$x^2 + 13 \equiv x^2 - 2 \pmod 5$ (irreducible)

so we get the following prime factorisations:

$\langle 2\rangle = \langle 2,1+\sqrt{-13}\rangle\langle 2,1-\sqrt{-13}\rangle$

All of the factors are prime and from the equation

$2-(1+\sqrt{-13}) = 1-\sqrt{-13}$

we get that $\langle 2,1+\sqrt{-13}\rangle \Leftrightarrow \langle 2,1-\sqrt{-13}\rangle$ are equivalent. Since $\langle 2,1+\sqrt{-13}\rangle$ is not equivalent to the whole ring of integer we get that $h=4$.

In the field $Q(\sqrt{-11})$ the ring of integers is $\mathcal{D} = Z[\frac{1}{2}+\frac{1}{2}\sqrt{-11}]$ and the discriminant is -11.

Minimal polynomial: $f(x) = x^2 - x + 3$

$M_{01} = 0.637$

$M_{01}\sqrt{11} \approx 2.11$

So we need to investigate primes less than or equal to 3, that is 2,3. Now

$x^2 - x + 3 \equiv x^2 + x + 1 \pmod 2$ (irreducible)

$x^2 - x + 4 \equiv x^2 - x = x(x-1) \pmod 3$

so we get the following prime factorisation:

$\langle 3\rangle = \langle 3,\sqrt{-11}\rangle\langle 3,1-\sqrt{-11}\rangle$

All of the factors are prime and from the equation

$3(4+\sqrt{-11}) + (-4+\sqrt{-11})\sqrt{-11} = 1-\sqrt{-11}$

we get that $\langle 3,\sqrt{-11}\rangle \Leftrightarrow \langle 3,1-\sqrt{-11}\rangle$ are equivalent. And so $h \le 2$ but from $3(4+\sqrt{-11})+(-3+\sqrt{-11})\sqrt{-11}=1$, we get that $1 \in \langle 3,\sqrt{-11}\rangle \Rightarrow \langle 3,\sqrt{-11}\rangle = \mathcal{D}$
Hence $h=1$.

In the field $Q(\sqrt{-10})$ the ring of integers is $\mathcal{D}=Z[\sqrt{-10}]$ and the discriminant is $-4\cdot 10=40$.
Minimal polynomial: $f(x)=x^2+10$
$M_{01}=0.637$
$M_{01}\sqrt{40}\approx 4.03$
So we need to investigate primes less than or equal to 5, that is 2,3,5. Now
$x^2+10\equiv x^2 \pmod 2$
$x^2+10\equiv x^2+1 \pmod 3$ (irreducible)
$x^2+10\equiv x^2 \pmod 5$
so we get the following prime factorisations:
$\langle 2\rangle = \langle 2,\sqrt{-10}\rangle^2$
$\langle 5\rangle = \langle 5,\sqrt{-10}\rangle^2$
All of the factors are prime and from the equation
$\langle 2,\sqrt{-10}\rangle\langle 5\sqrt{-10}\rangle = \langle 10\rangle\langle 5,\sqrt{-10}\rangle$
we get that $\langle 2,\sqrt{-10}\rangle \Leftrightarrow \langle 5,\sqrt{-10}\rangle$ are equivalent. Now we ask if $\langle 5,\sqrt{-10}\rangle$ is equivalent to the whole ring of integers? That is, is $1 \in \langle 5,\sqrt{-10}\rangle$. If so then we would have
$5(a+b\sqrt{-10})+\sqrt{-10}(c+d\sqrt{-10})=1$ for $a,b,c,d \in Z$. Solving this we get the equations
$$\begin{cases} 5a-10d=1 \\ 5b-c=0 \end{cases}$$
which does not have any integer solutions. Hence there are two equivalence classes so $h=2$.

9. Elliptic curves

In this section we will give some applications of the theory and look at some of the consequences of the class number.

We will start of by restating some properties about the lattices we saw in chapter 5 and their relation to the complex structure of the associated tori. Since $R^2 \cong C$, and we will work with elliptic curves, we will use lattices L generated by $\{\omega_1, \omega_2\}$ where $\omega_1, \omega_2 \in C$.
If $\omega_1', \omega_2' \in C$ then we can write them with respect to the basis of the lattice as

$$\omega_1' = a\omega_1 + b\omega_2$$
$$\omega_2' = c\omega_1 + d\omega_2$$

for $a, b, c, d \in Z$. Then $\{\omega_1', \omega_2'\}$ is a basis if and only if $ad - bc = \pm 1$. Thus the linear transformation such that the determinant is ± 1, called the modular group denoted $PSL(2, Z)$, gives us a new basis.
As we have seen before the fundamental domain of a lattice gives us an isomorphism between the quotient space C/L and the torus. Since this uses congruence's modular the lattice on the complex space C, we are led to define functions that work nicely with this. Such functions are periodic with respect to the lattices, so we are led to the definition:
A function is doubly periodic if $f : C \to C$ such that $f(z + \omega) = f(z)$ for any $\omega \in L$.

Thus a doubly periodic functions behaviour in C is determined by its behaviour on a fundamental domain T (as in chapter 5, lemma 5.2).

Definition

We call a *meromorphic function* $f : C \to C$ elliptic with respect to a lattice $L \subseteq C$ if f is doubly periodic with respect to L.

Example:

Weierstrass p-function is an example of an elliptic function: $p : C \to C$ s. t.

$$p(z) = \frac{1}{z^2} + \sum_{\omega_i \in L - \{0\}} \left(\frac{1}{(z + \omega_i)^2} - \frac{1}{\omega_i^2} \right)$$

An *elliptic curve* is a cubic curve of the form $y^2 = ax^3 + bx^2 + cx + d$ where the polynomial on the right hand side has distinct roots. It can be shown that, by transformations, we can write the elliptic curve in standard form

$$y^2 = 4x^3 - px - q$$

with $p^3 - 27q^2 \neq 0$. The last condition just tells us that the roots of the cubic are distinct.

Example:

It can be shown that Weierstrass p-function can be written as

$$(p'(z))^2 = 4p(z)^3 - g_2 p(z) - g_3$$

where

$$g_2 = 60 \sum_{\omega \in L-\{0\}} \frac{1}{\omega^4}$$

$$g_3 = 140 \sum_{\omega \in L-\{0\}} \frac{1}{\omega^6}$$

We have seen that the quotient space $\mathbb{C}/L$ is a torus. By letting $[z]_L$ denote the class of elements congruent to z modular L, then the map

$$(p(z), p'(z)) \to [z]_L$$

sets up a homeomorphism from the elliptic curve to the torus $\mathbb{C}/L$. (This is a functorial correspondence). In this sense we may regard the elliptic curve as a torus and the torus as an elliptic curve.

To see when two tori are equivalent, we first form the ratio

$$\tau = \frac{\omega_2}{\omega_1},$$

for a lattice generated by ω_1, ω_2. Because $\omega_1, \omega_2 \in \mathbb{C}$ we can always interchange the fraction so that the imaginary part of τ is always positive. Hence $\tau \in H$, the upper half plane in the complex plane (the hyperbolic plane). Thus the lattice determining the torus is the one generated by $\{1, \tau\}$.

Lemma

The values of τ that give rise to maps on the torus with a Euclidian structure are precisely those for which

$$\tau = \frac{p + iq}{r} \text{ or } \tau = \frac{p + \rho q}{r}$$

where $p, q, r \in \mathbb{Z}$ and $hcf(p, q, r) = 1$.

Now in order to relate the value of τ (defining the torus) to the equation of the elliptic curve, we introduce the somewhat remarkable j-function called the elliptic modular function $j : H \to \mathbb{C}$ such that

$$j(\tau) = \frac{1728 g_2^3}{g_2^3 - 27 g_3^2}$$

where g_2, g_3 are functions of a lattice determined by τ.

Properties of the j-function:

1) $j(T(\tau)) = j(\tau)$ for all $T \in PSL(2, \mathbb{Z})$. Thus j is invariant with respect to the modular group.

2) $j(\tau_1) = j(\tau_2)$ if and only if there exists $T \in PSL(2, Z)$ such that $T(\tau_1) = \tau_2$. Given an elliptic curve, we can determine a value of τ and now we see that the values of $j(\tau)$ determine this curve.
3) If τ is quadratic imaginary, that is satisfies the equation $a\tau^2 + b\tau + c = 0$ for $a, b, c \in Z$ where $a > 0$ and $hcf(a, b, c) = 1$, then $j(\tau)$ is an algebraic number of degree $h(d)$ where $d = b^2 - 4ac < 0$ is the discriminant and $h(d)$ is the class number of primitive quadratic forms of discriminant d.

To find the values of τ representing Euclidian toroidal maps that give rational elliptic curves we make use of the lemma above. So in this case we have

$$\tau = \frac{p + iq}{r} \text{ or } \tau = \frac{p + \rho q}{r}$$

Thus τ is a quadratic imaginary. If the elliptic curve corresponding to τ is rational then by property (3) of the j-function, $h(d) = 1$. If $\tau = (p + iq)/r$ then

$$(r\tau - p)^2 + q^2 = 0$$

and so

$$r^2\tau^2 - 2pr\tau + (p^2 + q^2) = 0$$

So the discriminant of the number field $Q(\tau)$ is

$$d = 4p^2r^2 - 4(p^2 + q^2)r^2 = -4q^2r^2$$

thus the discriminant is $-4 \times$ a square.
Similarly, if $\tau = (p + \rho q)/r$ then we get that the discriminant is $-3 \times$ a square.
Now the only solutions for d with a class number equal to 1 and with a discriminant as above are

$$d = -3, -4, -12, -16, -27$$

Thus we have showed

Theorem

There are 5 rational elliptic curves that correspond to Euclidian toroidal maps. All other rational elliptic curves correspond to hyperbolic toroidal maps.

d	τ	$j(\tau)$	Elliptic curve E_τ
-3	ρ	0	$y^2 = 4x^3 - 1$
-4	i	1728	$y^2 = 4x^3 - x$
-12	$1 + 2\rho$	54000	$y^2 = 4x^3 - 15x - 11$
-16	$2i$	287496	$y^2 = 4x^3 - 11x - 7$
-27	$2 + 3\rho$	-12288000	$y^2 = 4x^3 - 120x - 253$

References

[J] N. Jacobson, Basic Algebra II, Freeman and Co.
[JS] G.A. Jones and D. Singerman, Function of one Complex Variable, Cambridge University Press.
[SiT] D. Singerman and R. Syddall, Elliptic Curves and Uniform maps on the torus. To appear in Glasgow Maths. J.
[ST] I. N. Stewart and D. O. Tall, Algebraic Number Theory, second edition Chapman and Hall.