Algebraic Number Theory

William B. Hart

Warwick Mathematics Institute

Abstract. We give a short introduction to algebraic number theory.

Algebraic number theory is the study of extension fields $\mathbb{Q}(\alpha_1, \alpha_2, \ldots, \alpha_n)$ of the rational numbers, known as *algebraic number fields* (sometimes *number fields* for short), in which each of the adjoined complex numbers α_i is *algebraic*, i.e. the root of a polynomial with rational coefficients.

Throughout this set of notes we use the notation $Z[\alpha_1, \alpha_2, \ldots, \alpha_n]$ to denote the ring generated by the values α_i. It is the smallest ring containing the integers $\mathbb{Z}$ and each of the α_i.

It can be described as the ring of all polynomial expressions in the α_i with integer coefficients, i.e. the ring of all expressions built up from elements of $\mathbb{Z}$ and the complex numbers α_i by finitely many applications of the arithmetic operations of addition and multiplication.

The notation $\mathbb{Q}(\alpha_1, \alpha_2, \ldots, \alpha_n)$ denotes the field of all quotients of elements of $Z[\alpha_1, \alpha_2, \ldots, \alpha_n]$ with nonzero denominator, i.e. the field of rational functions in the α_i, with rational coefficients.

It is the smallest field containing the rational numbers $\mathbb{Q}$ and all of the α_i. It can be thought of as the field of all expressions built up from elements of $\mathbb{Z}$ and the numbers α_i by finitely many applications of the arithmetic operations of addition, multiplication and division (excepting of course, divide by zero).

1 Algebraic numbers and integers

A number $\alpha \in \mathbb{C}$ is called *algebraic* if it is the root of a monic polynomial

$$f(x) = x^n + a_{n-1}x^{n-1} + a_{n-2}x^{n-2} + \ldots + a_1x + a_0 = 0$$

with *rational* coefficients a_i.

We say that such a number α is algebraic over $\mathbb{Q}$ because the coefficients of the polynomial $f(x)$ are in $\mathbb{Q}$.

If a number α in $\mathbb{C}$ is not algebraic it is called a *transcendental* number.

The monic polynomial of *minimum* degree n that an algebraic number α satisfies, is unique.

For, suppose that α is the root of two monic polynomials $f_1(x)$ and $f_2(x)$ of minimum degree n. Then α is a root of $f_1(x) - f_2(x)$. Dividing by the leading coefficient of this polynomial we find a monic polynomial of smaller degree than n of which α is a root, which is a contradiction.

We call this polynomial of minimum degree the *minimum polynomial* of α.

The minimum polynomial f of α is irreducible over $\mathbb{Q}$.

Assume that it is not, i.e. that $f(x) = g(x)h(x)$ for nonconstant polynomials $g(x)$ and $h(x)$. In fact g and h can both be made monic by scaling by a constant.

Since $g(\alpha)h(\alpha) = f(\alpha) = 0$, then either $g(\alpha) = 0$ or $h(\alpha) = 0$, since the quantities $f(\alpha), g(\alpha), h(\alpha)$ all lie in $\mathbb{C}$ which is an integral domain.

But this implies that there is a monic polynomial of smaller degree than f which has α as a root, contradicting the minimality of f.

Any polynomial $g(x)$ with rational coefficients of which α is a root is divisible by f.

For, by the division algorithm for polynomials, $g(x) = f(x)q(x) + r(x)$ for some polynomial $r(x)$ of degree less than the degree of $f(x)$.

Assume $r(x) \neq 0$ so that $f(x) \not| \, g(x)$.

Substituting α in to the division equation we get $r(\alpha) = 0$. Dividing r by its leading coefficient, it becomes monic. But now we have a monic polynomial of smaller degree than f of which α is a root, contradicting the minimality of f. Thus $r(x) = 0$ and $f(x) \mid g(x)$.

The degree n of the minimum polynomial $f(x)$ of α is called the *degree* of α.

If we adjoin finitely many algebraic numbers α_i to $\mathbb{Q}$ we get a subfield of $\mathbb{C}$ called an *algebraic number field*, i.e. an algebraic number field is of the form $\mathbb{Q}(\alpha_1, \alpha_2, \ldots, \alpha_m)$ for algebraic numbers α_i.

We will also be interested in the elements of a number field called algebraic integers.

An *algebraic integer* (or integer for short) $\alpha \in \mathbb{C}$ is a root of a *monic* polynomial

$$x^n + b_{n-1}x^{n-1} + b_{n-2}x^{n-2} + \ldots + b_1 x + b_0$$

with *rational integer* coefficients b_i.

To avoid confusion with more general algebraic integers, we henceforth call the ordinary integers $\mathbb{Z}$, the *rational integers.*

Of course the rational integers are examples of algebraic integers, since they are roots of monic, linear polynomials with rational integer coefficients.

The earliest historical example of algebraic integers is the *Gaussian integers*, denoted $\mathbb{Z}[i]$. This is the ring of numbers of the form $a + bi$ for rational integers a and b.

Note that we don't need to include terms involving $i^3, i^4, \ldots$, since $i^3 = -i, i^4 = 1$, etc.

It is easy to show that the Gaussian integers are the algebraic integers in the number field $K = \mathbb{Q}(i)$, called the Gaussian numbers.

Another historical example of number fields is given by *cyclotomic number fields* investigated extensively by Kummer when studying Fermat's Last Theorem.

These have the form $K = \mathbb{Q}(\zeta_n)$, where ζ_n is a primitive n^{th} root of unity, i.e: satisfying $x^n - 1 = 0$.

The set of algebraic integers in K turns out to be $\mathbb{Z}[\zeta_n]$.

Another important example is that of *quadratic number fields.* These are of the form $K = \mathbb{Q}(\alpha)$ with α a root of an irreducible quadratic $ax^2 + bx + c$ for $a, b, c \in \mathbb{Q}$.

These come in two types:

(i) *real quadratic* number fields, with discriminant $d = b^2 - 4ac > 0$ and thus α real.

(ii) *imaginary quadratic* number fields, with $d = b^2 - 4ac < 0$ and thus α complex with non-zero imaginary part.

Clearly if $d = m^2 d'$ then $\mathbb{Q}(\sqrt{d}) = \mathbb{Q}(\sqrt{d'})$. We also see that a discriminant is a square modulo 4, i.e. $d \equiv 0, 1 \pmod 4$. We call a discriminant *fundamental* if it is either $1 \pmod 4$ and squarefree, or $0 \pmod 4$ and 4 times a squarefree integer.

The set of algebraic integers in the quadratic number field $K = \mathbb{Q}(\sqrt{d})$ for fundamental discriminant d turns out to be of the form $\mathbb{Z}[\sqrt{d}]$ if $d \equiv 0 \pmod 4$, or $\mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right]$ for $d \equiv 1 \pmod 4$.

We will later see that the set of algebraic integers of a number field is in fact a subring, which we call the *ring of integers* of the number field K, denoted $\mathcal{O}_K$.

2 Simple algebraic extensions

The following theorem allows us to characterise number fields.

Theorem 1. *(Primitive element theorem) An algebraic number field with finitely many algebraic generators γ_i, i.e. $K = \mathbb{Q}(\gamma_1, \gamma_2, \ldots, \gamma_m)$, can be expressed as $K = \mathbb{Q}(\alpha)$ in terms of a* single *algebraic generator α.*

Proof: It is sufficient to show that if $K = K_1(\alpha, \beta)$ for algebraic numbers α and β and some number field K_1, there there is a single algebraic number θ for which $K = K_1(\theta)$. The general result then follows by induction on the number of generators of K over the rationals, as $\mathbb{Q}$ is also a number field.

Let the mimimum polynomials of α and β over K_1 be $p(x)$ and $q(x)$ respectively, i.e. the monic polynomials of minimum degree with coefficients in K_1, of which α and β are roots.

Suppose that $\alpha = \alpha_1, \alpha_2, \ldots, \alpha_n$ and $\beta = \beta_1, \beta_2, \ldots, \beta_m$ are the roots in $\mathbb{C}$ of p and q respectively.

The argument earlier for numbers which are algebraic over $\mathbb{Q}$ also shows that the minimum polynomials p and q are irreducible over K_1.

Now since p is irreducible, it cannot have any roots in common with its derivative, i.e. it is separable. For suppose that it did and let that root be α'. Then p is also the minimum polynomial of α' (since p is irreducible and by a previous result the minimum polynomial of α' must divide p). However p' has lower degree than p, contradicting the minimality of p.

But if p and p' have no common roots, then p has no repeated roots (this is easy to see if one writes $p(x)$ as a product of linear factors $(x - \alpha_i)$ and takes the derivative).

The same argument can be used to show that all the roots β_j of q are distinct.

Write $\delta_{ij} = \frac{\alpha_i - \alpha_1}{\beta_1 - \beta_j}$ for $j \neq 1$. We see that δ_{ij} is the unique solution of $\alpha_i + x\beta_j = \alpha_1 + x\beta_1$. Note that there are only a finite number of δ_{ij}.

Choose any value $c \in K_1$ which is not equal to any of the δ_{ij}. Now $\alpha_i + c\beta_j \neq \alpha_1 + c\beta_1 = \alpha + c\beta$ for all $1 \leq i \leq n$, $2 \leq j \leq m$.

Define $\theta = \alpha + c\beta$. Clearly $K_1(\theta) \subseteq K_1(\alpha, \beta)$.

Since $\alpha = \theta - c\beta$, if we can prove that $\beta \in K_1(\theta)$ then $\alpha \in K_1(\theta)$ and we will have shown that $K_1(\alpha, \beta) \subseteq K_1(\theta)$ and thus $K_1(\alpha, \beta) = K_1(\theta)$ as required.

Now $p(\theta - c\beta) = p(\alpha) = 0$. So define $r(x) = p(\theta - cx) \in K_1(\theta)[x]$, so that $r(x)$ has β as a root in common with $q(x)$.

Suppose that $r(x)$ and $q(x)$ have another root ζ in common. Then ζ is one of the $\beta_1, \ldots, \beta_m$, β_k say, and $\theta - c\zeta$ is one of $\alpha_1, \ldots, \alpha_n$, α_i say. But this means $\alpha_i = \theta - c\beta_k$.

But from the above, the only possibility is that $\beta_k = \beta_1$, i.e. $\zeta = \beta_1 = \beta$. In other words, the only common root of $r(x)$ and $q(x)$ is β.

Let $h(x)$ be the minimum polynomial of β over $K_1(\theta)$. Then $h(x) \mid q(x)$ and $h(x) \mid r(x)$. But $q(x)$ and $r(x)$ have only one common zero in $\mathbb{C}$, so we must have degree $h = 1$, i.e. $h(x) = x + \mu$ for $\mu \in K_1(\theta)$.

Then $0 = h(\beta) = \beta + \mu$ so that $\beta = -\mu \in K_1(\theta)$ as was to be shown. □

Theorem 2. *Given a number field $K = \mathbb{Q}(\alpha)$, any $\beta \in K$ can be expressed uniquely in the form*

$$\beta = c_0 + c_1\alpha + c_2\alpha^2 + \cdots + c_{n-1}\alpha^{n-1}$$

for some coordinates $c_i \in \mathbb{Q}$.

Proof: Let $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$ be the minimum polynomial of α.

By writing $f(x) = xg(x) + a_0$ and noting that $f(\alpha) = 0$, we can write $1/\alpha = -g(\alpha)/a_0$, which has rational coefficients. Thus $1/\alpha \in \mathbb{Q}[\alpha]$.

As we can write any $\beta \in K$ as a quotient of elements of $\mathbb{Z}[\alpha]$, then using the partial fraction expansion, we can write β as a sum of quotients with numerators in $\mathbb{Q}[\alpha]$ and denominators of the form $1/\alpha$.

In this way, we can show that β is contained in $\mathbb{Q}[\alpha]$, i.e. $K = \mathbb{Q}[\alpha]$.

By expanding and rearranging the expression $f(\alpha) = 0$ we can write α^n as a linear combination of lower powers of α. Thus any power of α greater than or equal to n can be written as a linear combination of lower powers.

From this we obtain the first part of the theorem.

To show uniqueness, suppose that β has two expressions of the required form with coordinates c_i and c'_i respectively.

As the difference of the two expressions is zero, the coefficients of the difference, $c_i - c'_i$, must all be zero. Otherwise we obtain a polynomial of degree less than n which α satisfies.

Thus $c_i = c'_i$ for all i and the expression given in the theorem is unique. □

What we have shown is that $\mathbb{Q}(\alpha)$ is a vector space over $\mathbb{Q}$ of dimension n where n is the degree of α.

We see immediately that if $K = \mathbb{Q}(alpha_1) = \mathbb{Q}(\alpha_2)$ then α_1 and α_2 have the same degree, as it is equal to the dimension of K as a vector space over $\mathbb{Q}$.

The same arguments as above apply equally with any number field as base field, instead of $\mathbb{Q}$. That is, if $L = K(\alpha_1) = K(\alpha_2)$ for a number field K and algebraic numbers α_1 and α_2 then the degree n of α_1 over K is the same as the degree of α_2 over K, as L is a vector space over K of dimension n, etc.

For an algebraic number field $K = \mathbb{Q}(\alpha)$, the degree of the generator α is also called the *degree* of the number field.

As we have just seen, this definition does not depend on the choice of α as generator.

In more generality, if $L = K(\alpha)$ for some number field K, then we say that L/K is an *extension* of number fields and that the *degree* of the extension is the degree n of the minimum polynomial of α over K.

Again, this definition does not depend on the choice of α.

The degree of the extension L/K is denoted $n = [L : K]$.

Not every element of an algebraic number field has the same degree n, however we have the following.

Theorem 3. *If $L = K(\alpha)$ with the degree of α of degree n over K, then for any other $\beta \in L$ we have that the degree of β over K divides n. If the degree of β over K actually equals n, then in fact $L = K(\beta)$.*

3 The ring of integers

We can show that the set of algebraic integers in an algebraic number field $K = \mathbb{Q}(\alpha)$ is a ring.

It suffices to show that if β_1 and β_2 are algebraic integers in K then so are $\beta_1 + \beta_2$, $\beta_1\beta_2$ and $-\beta_1$.

To show this, consider the ring $R = \mathbb{Z}[\beta_1][\beta_2]$ and let m and n be the respective degrees of the minimum polynomials of β_1 and β_2 over $\mathbb{Z}$.

By making use of the minimum polynomial of β_2, any power of β_2 higher than $n-1$ can be rewritten in terms of a lower power with rational integer coefficients. Similarly, any power of β_1 higher than $m-1$ can be rewritten in terms of lower powers with rational integer coefficients.

Therefore, any element of R can be written as a linear combination of $\beta_1^i\beta_2^j$ for $0 \leq i < m$ and $0 \leq j < n$. Let us write $\beta_1, \beta_2, \ldots, \beta_{mn}$ for the mn values $\beta_1^i\beta_2^j$.

Now we will use this fact to show that any element of R is an algebraic integer.

Suppose γ is in R. Write $\gamma\beta_i = \sum_j a_{i,j}\beta_j$ for each $1 \leq i \leq mn$ and some $a_{i,j} \in \mathbb{Z}$.

We can rearrange these sums by moving the terms on the left hand side to the other side, yielding linear combinations of the β_i that give zero.

As γ is in R we know that this homogeneous set of equations in the β_i has a solution. But it has a solution if and only if the determinant of the associated matrix of coefficients has zero determinant.

But the determinant of this matrix is a monic polynomial in γ with coefficients in $\mathbb{Z}$. Thus γ is an algebraic integer.

As $\gamma = \beta_1 + \beta_2$, $\gamma = \beta_1\beta_2$ and $-\beta_1$ are all in R, we have shown that they are all algebraic as required.

We call the ring of algebraic integers in $K = \mathbb{Q}(\alpha)$ the *ring of integers* of K and denote it $\mathcal{O}_K$.

4 The unit group

By analogy with the rational integers, an integer $\alpha \in \mathcal{O}_K$ is *divisible* by another $\beta \in \mathcal{O}_K$, if there is a third integer $\gamma \in \mathcal{O}_K$ such that $\alpha = \beta\gamma$.

An integer $\epsilon \in \mathcal{O}_K$ which divides all integers in $\mathcal{O}_K$ is called a *unit.* In particular it divides the 1, i.e: it has an inverse $\epsilon^{-1} \in \mathcal{O}_K$.

The set of all units in $\mathcal{O}_K$ is a group, called the *unit group* of (the ring of integers of) K. It is denoted U_K.

Note that the properties of divisibility and being a unit depend on the particular number field K under consideration.

If two algebraic integers are related by $\alpha = \beta\epsilon$ with ϵ a unit, then since ϵ has an inverse, we have that α and β both divide each other. We call α and β *associates.*

The following examples give some indication of some of the things that can happen with units:

(i) The rational integers $\mathbb{Z}$ have only the units ± 1.

(ii) The units of the imaginary quadratic number field $\mathbb{Q}(i)$ are $\pm 1, \pm i$.

(iii) The units of $\mathbb{Q}(\sqrt{5})$ are $\pm \left(\frac{1+\sqrt{5}}{2}\right)^n \forall\, n \in \mathbb{Z}$.

5 Conjugate Fields

Let the field $K = \mathbb{Q}(\alpha)$ be given with generator α having minimum polynomial $f(x)$ of degree n. The n roots of $f(x)$, $\alpha = \alpha_1, \alpha_2, \ldots, \alpha_n$ are called *conjugates* of α.

Since $f(x)$ is a minimum polynomial, it is irreducible. Thus it is the minimum polynomial of all its roots. Neither can it have repeated roots α_i, otherwise we would have that α_i was a root of $f'(x)$, which is of smaller degree than $f(x)$, contradicting the minimality of the latter.

Since each element of $K = \mathbb{Q}(\alpha)$ can be expressed as a linear combination of powers of α, the map σ_i which takes α to another root α_i of $f(x)$, in this expression, can be seen to define an isomorphism from K to the field $\mathbb{Q}(\alpha_i)$.

We call these fields $\mathbb{Q}(\alpha_i)$, isomorphic to K, *conjugate fields.*

Conversely, consider any isomorphism σ of $\mathbb{Q}(\alpha)$ that preserves $\mathbb{Q}$. The minimum polynomial expression $f(\alpha) = 0$ is preserved by σ and hence α can only be taken to another root of $f(x)$ by σ, i.e: to one of its conjugates α_i.

There is no reason why the α_i should all define different fields. For example the root α_i might already belong to $K = \mathbb{Q}(\alpha)$ and the associated isomorphism simply defines an automorphism of K. It may even be the case that all the roots are in the same field.

When all the conjugates α_i of α are in $K = \mathbb{Q}(\alpha)$, we call K a *Galois* number field.

In this case the set of automorphisms σ_i of K that fix $\mathbb{Q}$ is a group called the *Galois* group of K, denoted $\mathrm{Gal}(K/\mathbb{Q})$.

More generally we have *relative Galois extensions* L/K, where the conjugates of a generator α of the extension are all in L, and thus each isomorphism of L that fixes K is an automorphism of L. Here we denote the Galois group $\mathrm{Gal}(L/K)$.

Note that whilst the $\mathbb{Q}(\alpha_i)$ may be distinct, they are all isomorphic, and thus there is a *single* abstract number field K having n distinct embeddings into the complex numbers, $\sigma_i : K \hookrightarrow \mathbb{C}$, with images $\mathbb{Q}(\alpha_i)$ respectively.

We can think of the abstract number field K as the field $\mathbb{Q}[x]/(f)$, i.e. the set of polynomials over $\mathbb{Q}$ reduced modulo f. Clearly this definition does not depend in any way on a given root of f. We can see that this field is isomorphic to $\mathbb{Q}(\alpha_i)$ by sending x to α_i.

If one of the embeddings σ_i takes K wholly into the reals, $\mathbb{R}$, it is called a *real* embedding. Otherwise it is called a *complex* embedding.

Since the complex roots of polynomials come in conjugate pairs then so do complex embeddings. If $\sigma : \alpha \mapsto \alpha_i$ defines a complex embedding for a generator $\alpha \in K$ and a particular root $\alpha_i \in \mathbb{C}$, then it has a conjugate embedding $\sigma' : \alpha \mapsto \overline{\alpha_i}$, where the bar denotes complex conjugation.

Any field K which has only real embeddings is called a *totally real* field.

We can extend the notion of conjugates to arbitrary elements α of an extension L/K, i.e. with $\alpha \in L$.

If σ_i are the embeddings of L fixing K, then for an arbitrary $\alpha \in L$ we call the values $\sigma_i(\alpha)$ the *conjugates* of α.

This definition agrees with our former definition. However note that the conjugates will not all be distinct now, unless α happens to generate the extension as before.

6 Norm and Trace

Given an extension of number fields L/K, the *norm* (with respect to the extension) of an arbitrary $\alpha \in L$ is the value

$$\mathcal{N}_{L/K}(\alpha) = \prod_{\sigma} \sigma(\alpha),$$

i.e: the product of all the conjugates of α.

When the base field K is $\mathbb{Q}$ we sometimes denote the norm by $\mathcal{N}(\alpha)$ and call it the *absolute norm* of L.

In this case, since all the embeddings fix the rational number field, then for all elements a of $\mathbb{Q}$, we have that $\mathcal{N}(a) = a^n$, where n is the degree of the extension $L/\mathbb{Q}$.

A similar result follows for relative extensions L/K by replacing $\mathbb{Q}$ with K throughout.

Since each embedding σ respects multiplication

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

then we easily see that for all $\alpha, \beta \in L$

$$\mathcal{N}_{L/K}(\alpha\beta) = N_{L/K}(\alpha)N_{L/K}(\beta).$$

If we have an extension of number fields L/K, then for any α in L we have that $\mathcal{N}_{L/K}(\alpha)$ is invariant under the action of each automorphism of L that fixes K. Thus from Galois theory we have that $N_{L/K}(\alpha) \in K$.

Note that if α is an integer of L then so are all its conjugates, and thus the norm is an integer of K.

What we have shown is that the norm is a multiplicative group homomorphism $N_{L/K} : L^{\times} \to K^{\times}$, where the cross indicates that we are taking the multiplicative group of non-zero elements of the respective field.

The following is a useful result for computing the norm of an element.

Theorem 4. *Suppose that L/K is an extension with $[L : K] = n$ and α an element of L with minimum polynomial $f(x)$ of degree h. Let the constant coefficient of h be a_0. Then*

$$\mathcal{N}_{L/K}(\alpha) = (-1)^n a_o^{n/h}.$$

Using this theorem twice, we see that if $K \subset L \subset M$ is a tower of extensions, then for $\alpha \in L$

$$\mathcal{N}_{M/K}(\alpha) = (-1)^{[M:L]} \mathcal{N}_{L/K}(\alpha)^{[M:L]}.$$

This shows that the norm of an algebraic number is not an invariant but depends on the particular extension that the norm is defined over.

Given an extension L/K, the *trace* of α (with respect to the extension) is given by

$$Tr_{L/K}(\alpha) = \sum_{\sigma} \sigma(\alpha).$$

As per the analogous result for the norm, we have that for an extension L/K and an element a of the base field K

$$Tr_{L/K}(a) = [L : K] \cdot a.$$

We can also relate the trace of an element of L to its minimum polynomial.

Theorem 5. *With conditions as per Theorem 4 we have*

$$Tr_{L/K}(\alpha) = -(n-h)a_{n-1}$$

where a_{n-1} is the coefficient of x^{n-1} in the minimum polynomial $f(x)$.

Also as per the norm, we have for all $\alpha \in L$ that $Tr_{L/K}(\alpha) \in K$, and similarly that traces of algebraic integers in L are algebraic integers in K.

The trace is a linear transformation between $\mathbb{Q}$-vector spaces $Tr_{L/K} : L \to K$. The most important property of the trace is that for all $\alpha, \beta \in L$ we have that

$$Tr_{L/K}(\alpha + \beta) = Tr_{L/K}(\alpha) + Tr_{L/K}(\beta).$$

If we have a tower of fields, $K \subset L \subset M$, then

$$Tr_{M/K}(\alpha) = [M : L] \cdot Tr_{L/K}(\alpha),$$

so once again, the trace of an element depends on the extension it is taken relative to.

7 The Discriminant

It is convenient to denote the value $\sigma(\alpha)$ for an embedding σ, by $\sigma\alpha$.

We now restrict ourselves to extensions $K/\mathbb{Q}$. The more general case of relative extensions requires more algebra in general, which we deal with in another place.

Given any n numbers, $\alpha_1, \alpha_2, \ldots, \alpha_n$ in a field K of degree n over $\mathbb{Q}$, we define their *discriminant* by

$$\Delta(\alpha_1, \alpha_2, \ldots, \alpha_n) = \begin{vmatrix} \sigma_1\alpha_1 & \sigma_2\alpha_1 & \ldots \sigma_n\alpha_1 \\ \sigma_1\alpha_2 & \sigma_2\alpha_2 & \ldots \sigma_n\alpha_2 \\ \ldots & \ldots & \ldots\ldots \\ \sigma_1\alpha_n & \sigma_2\alpha_n & \ldots \sigma_n\alpha_n \end{vmatrix}^2$$

where the σ_i are the n embeddings of the field K into the complex numbers and the expression on the right is the square of the determinant of the given matrix.

For any matrices it is true that $det(A^2) = det(AA^T)$. The following is therefore clear from the definition.

Theorem 6. *The discriminant is equivalent to the following*

$$\Delta(\alpha_1, \alpha_2, \ldots, \alpha_n) = det(Tr(\alpha_i\alpha_j)).$$

If $K = \mathbb{Q}(\theta)$ for a generator θ, the discriminant of powers of θ is given by the expression

$$\Delta(1, \theta, \theta^2, \ldots, \theta^{n-1}) = \begin{vmatrix} 1 & 1 & \ldots 1 \\ \theta_1 & \theta_2 & \ldots \theta_n \\ \ldots & \ldots & \ldots\ldots \\ \theta_1^{n-1} & \theta_2^{n-1} & \ldots \theta_n^{n-1} \end{vmatrix}^2$$

where $\theta_i = \sigma_i\theta$, is the i-th conjugate of θ.

We can evaluate this using Vandermonde's Theorem and obtain

Theorem 7.

$$\Delta(1, \theta, \theta^2, \ldots, \theta^{n-1}) = \prod_{1 \leq i < j \leq n} (\theta_i - \theta_j)^2.$$

Since none of the θ_i are equal (they are conjugates of a generator), this discriminant is non-zero. The symmetry of this expression also leads to

Theorem 8. *If* $K = \mathbb{Q}(\theta)$ *then*

$$\Delta(1, \theta, \theta^2, \ldots, \theta^{n-1}) \in \mathbb{Q}.$$

For $\alpha \in K$ let α_i for $i = 1 \ldots n$ be its conjugates. We call the following polynomial the *characteristic polynomial* of α

$$f(x) = (x - \alpha_1)(x - \alpha_2) \cdots (x - \alpha_n).$$

It is clearly a power of the minimum polynomial of α.

Define the *discriminant* of $f(x)$ as follows

$$Disc(f) = (-1)^{n(n-1)/2} \prod_{j=1}^{n} f'(\alpha_j).$$

By evaluating the expression on the right we see that

Theorem 9. *For any $\alpha \in K$ the discriminant of powers of α is equal to the discriminant of its characteristic polynomial*

$$\Delta(1, \alpha, \ldots, \alpha^{n-1}) = Disc(f).$$

Since all the given expressions are zero when α is not a generator of K, this theorem applies in general, not just for α a generator of K.

We note that the discriminant as it has been defined is not invariant under change of basis for the $\mathbb{Q}$-vector space K. For, let $\alpha_1, \alpha_2, \ldots, \alpha_n$ be a basis for K, with

$$\alpha_i = h_{i1} + h_{i2}\theta + \cdots + h_{in}\theta^{n-1}$$

given in terms of the basis $1, \theta, \theta^2, \ldots, \theta^{n-1}$. With a little work, the following expression relating the discriminants can be obtained

Theorem 10.

$$\Delta(\alpha_1, \alpha_2, \ldots, \alpha_n) = det(h_{ij})^2 \cdot \Delta(1, \theta, \theta^2, \ldots, \theta^{n-1}).$$

There is no reason to suppose that $det(h_{ij})$ is unity, or even a rational integer. In fact, in general it can be any square of a rational number. We need some canonical basis to remedy this situation.

A further observation is that the determinant of all the h_{ij} is non-zero if and only if the α_i are a basis of K. Thus

Theorem 11. *$\Delta(\alpha_1, \alpha_2, \ldots, \alpha_n)$ is non-zero iff $\alpha_1, \alpha_2, \ldots, \alpha_n$ is a basis of K.*

To create a canonical basis for K, we first describe bases consisting of integers $\alpha_i \in \mathcal{O}_K$.

Firstly consider the minimum polynomial of an arbitrary $\omega_i \in K$. If we multiply ω_i by the lowest common denominator d_i, of the coefficients of that polynomial, we obtain a value $\alpha_i = d_i\omega_i$, which is actually an integer of K. But the set of integers α_i still forms a $\mathbb{Q}$-basis for K. We now apply the following straightforward theorem

Theorem 12. *For any $\alpha_1, \alpha_2, \ldots, \alpha_n \in \mathcal{O}_K$ we have*

$$\Delta(\alpha_1, \alpha_2, \ldots, \alpha_n) \in \mathbb{Z}.$$

From Theorem 10 we see that the signs of these discriminants are always the same. Amongst their values must be a non-zero one with the smallest absolute value.

We call the discriminant of values $\alpha_1, \alpha_2, \ldots, \alpha_n \in \mathcal{O}_K$ with the smallest non-zero absolute value, *the discriminant* of the ring of integers $\mathcal{O}_K$ (and, by abuse of language, of the field K) and denote it

$$\mathcal{D}_K = \Delta(\alpha_1, \alpha_2, \ldots, \alpha_n).$$

8 Unique Factorization

We turn now to the question of unique factorization in the ring of integers $\mathcal{O}_K$ of a number field. We wish to have a unique decomposition of integers upto order and the presence of units, into something like the primes of the rational integers.

The Gaussian integers have unique factorization. For example we have the decomposition $2 = -i(1+i)^2$. Here $-i$ is a unit and $(1+i)$ is irreducible in $\mathbb{Z}[i]$ and in fact a prime of $\mathbb{Z}[i]$.

The ring $\mathbb{Z}[i]$ is an example of a Euclidean domain.

An integral domain $\mathcal{O}$ is a *Euclidean domain* if it possesses a norm (a map $n : \mathcal{O} \to \mathbb{Z}_{\geq 0}$) with

(i) $n(1) = 1$,

(ii) $n(ab) = n(a)n(b) \; \forall \; a, b \in \mathcal{O}$;

and such that, given $\alpha, \beta \in \mathcal{O}, \beta \neq 0$, there exist $\gamma, \delta \in \mathcal{O}$ such that

$$\alpha = \gamma\beta + \delta \text{ with } n(\delta) < n(\beta),$$

i.e: the ring has a Euclidean algorithm.

For $\alpha = a + bi \in \mathbb{Z}[i]$ choose the norm to be $n(\alpha) = a^2 + b^2$.

We recall the following result.

Theorem 13. *A Euclidean domain possesses unique factorization. The rings of integers of $\mathbb{Q}(\sqrt{-2}), \mathbb{Q}(\sqrt{-3}), \mathbb{Q}(\sqrt{-7}), \mathbb{Q}(\sqrt{2})$ and $\mathbb{Q}(\sqrt{3})$ are all Euclidean domains.*

Now consider the field $K = \mathbb{Q}(\sqrt{-5})$ which has $\mathcal{O}_K = \mathbb{Z}[\sqrt{-5}]$. In this ring

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

We now use the following theorem to show that both pairs of factors here are irreducible in $\mathbb{Z}[\sqrt{-5}]$.

Theorem 14. *If $\alpha \mid \beta$ for $\alpha, \beta \in \mathcal{O}_K$ then $\mathcal{N}(\alpha) \mid \mathcal{N}(\beta)$.*

We apply this to (1). The only conjugate of $\sqrt{-5}$ is $-\sqrt{-5}$. Thus $\mathcal{N}(1+\sqrt{-5}) = \mathcal{N}(1-\sqrt{-5}) = 6$. But no $\alpha \in \mathcal{O}_K$ has $\mathcal{N}(\alpha) = 2$ or 3. Thus by the theorem, $1+\sqrt{-5}$ and $1-\sqrt{-5}$ are irreducible. Similarly 2 and 3 are irreducible. So 6 has two distinct factorizations into irreducibles in $\mathcal{O}_K$. (We check easily that the only units in $\mathcal{O}_K$ are ± 1).

We conclude that $\mathcal{O}_K$ does not possess unique factorization!

9 Ideals

To resolve this embarrassment Kummer introduced additional formal numbers called *ideal numbers* to act as divisors of these otherwise irreducible factors.

Dedekind extended this concept, creating the notion of an *ideal.* Again ideals are introduced to act as 'factors' of these irreducibles. However unlike the purely formal notion of ideal numbers, ideals are concrete entities related to the ring of integers. They are based on the observation that for $\alpha, \beta \in \mathbb{Z}$ the *ideal* of numbers

$$(\alpha, \beta) = \{m\alpha + n\beta : m, n \in \mathbb{Z}\}$$

consists of all rational integers divisible by the greatest common divisor of α and β.

We thus make the following definition.

For each $\alpha, \beta \in \mathcal{O}_K$ define the *ideal*

$$(\alpha, \beta) = \{\gamma\alpha + \delta\beta : \gamma, \delta \in \mathcal{O}_K\}.$$

Clearly if $1 \in (\alpha, \beta)$ then $(\alpha, \beta) = \mathcal{O}_K$. In fact, this is true if any unit ϵ of K is in (α, β).

In analogy with the case of rational integer ideals, if $1 \in (\alpha, \beta) = \mathcal{O}_K$ we say that α and β are *coprime.*

Dedekind made use of an extension of this notation in his definition of an ideal (although we later see that the ideal definition above (α, β) is all that is in fact necessary):

An *ideal* is a set of integers

$$(\alpha_1, \alpha_2, \ldots, \alpha_k) = \{\gamma_1\alpha_1 + \gamma_2\alpha_2 + \cdots + \gamma_k\alpha_k : \gamma_i \in \mathcal{O}_K\},$$

for some finite set of algebraic integers $\alpha_i \in \mathcal{O}_K$.

Once again we can think of an ideal as a kind of greatest common divisor of the α_i. Ideals are often denoted by gothic letters, e.g: $\mathfrak{a} = (\alpha_1, \alpha_2, \ldots, \alpha_k)$.

An ideal of the form

$$(\alpha) = \{\gamma\alpha : \gamma \in \mathcal{O}_K\}$$

for some $\alpha \in \mathcal{O}_K$ is called a *principal ideal.*

Principal ideals are a good device for avoiding the inconvenience of units.

For $\alpha, \beta \in \mathcal{O}_K$ we have that $(\alpha) = (\beta)$ iff α and β are associates, i.e: $\alpha = \beta\epsilon$ for some unit ϵ.

Thus there is a 1-1 correpsondence between principal ideals and integers modulo units.

The great idea of Dedekind was to consider the set of ideals of $\mathcal{O}_K$ as an arithmetic in its own right, which extends that of the integers themselves. The following is a list of standard properties of ideals which he developed.

(i) For $\alpha, \beta \in \mathcal{O}_K$ we have $(\alpha) \supseteq (\beta)$ iff $\alpha \mid \beta$ in $\mathcal{O}_K$.

(ii) For ideals $\mathfrak{a}, \mathfrak{b} \subseteq \mathcal{O}_K$ define $\mathfrak{a} \mid \mathfrak{b}$ to mean $\mathfrak{a} \supseteq \mathfrak{b}$ (considered as sets of integers), thus generalizing (i).

(iii) For ideals $\mathfrak{a} = (\alpha_1, \alpha_2, \ldots, \alpha_k)$, $\mathfrak{b} = (\beta_1, \beta_2, \ldots, \beta_m)$ define the product of these two ideals by $\mathfrak{ab} = (\alpha_1\beta_1, \alpha_1\beta_2, \ldots, \alpha_k\beta_m)$. (Thinking of ideals as a greatest common divisor helps motivate this definition).

(iv) For any $\mathfrak{a}$ an ideal, $\mathcal{O}_K\mathfrak{a} = \mathfrak{a}\mathcal{O}_K = \mathfrak{a}$. Thus $\mathcal{O}_K$ acts as an identity.

(v) With the product definition of (iii) we have that $\mathfrak{a} \mid \mathfrak{ab}$ and $\mathfrak{b} \mid \mathfrak{ab}$ for all ideals $\mathfrak{a}, \mathfrak{b}$, as we might hope.

Theorem 15. *For a field K of degree n, each ideal of $\mathcal{O}_K$ is an infinite Abelian group, with a finite basis over $\mathbb{Z}$ consisting of exactly n integers $\alpha_i \in \mathcal{O}_K$, i.e. each element α of an ideal $\mathfrak{a}$ has a representation in the form*

$$\alpha = m_1\alpha_1 + m_2\alpha_2 + \cdots + m_n\alpha_n \textit{ with all } m_i \in \mathbb{Z}.$$

This applies in particular for the identity ideal, $\mathcal{O}_K$ itself.

Proof: Let $v = \{\alpha_1, \alpha_2, \ldots, \alpha_n\}$ be a $\mathbb{Q}$-basis of K. We can multiply each α_i by a sufficiently large integer so that each α_i is contained in $\mathfrak{a}$. This is always possible because we can first multiply by an integer so that α_i is contained in $\mathcal{O}_K$, then by the norm of one of the generators of $\mathfrak{a}$.

Now let M be the set $\{m_1\alpha_1 + m_2\alpha_2 + \cdots m_n\alpha_n$ with all $m_i \in \mathbb{Z}\}$. As the α_i are a $\mathbb{Q}$-basis of K then $\mathit{\Delta}(\alpha_1, \alpha_2, \ldots, \alpha_n)^2$ is a positive integer. We will choose the α_i as above such that $\mathit{\Delta}(\alpha_1, \alpha_2, \ldots, \alpha_n)^2$ is minimal.

We claim that $\{\alpha_1, \alpha_2, \ldots, \alpha_n\}$ is the basis required by the theorem.

If not, then there is an element α in $\mathfrak{a}$ but not in M.

Write $\alpha = \sum c_i\alpha_i$ for some $c_i \in \mathbb{Q}$. If we add a $\mathbb{Z}$-multiple of α_i to α then the result is in $\mathfrak{a}$ but not in M. Therefore by adding $\mathbb{Z}$-multiples of the α_i to α we can ensure that $|c_i| \leq 1/2$ for each i.

As α is not in M it is not zero, and so one of the c_i must be nonzero. Let w be the $\mathbb{Q}$-basis of K obtained by replacing v_i in v by α. We still have that all of the elements of w are in $\mathfrak{a}$.

But it is easy to show that $|\Delta(w)|^2 = c_i^2 |\Delta(v)|^2 < |\Delta(v)|^2$. But this contradicts the minimality of $|\Delta(v)|^2$. Thus α is in M after all. Thus $\mathfrak{a}$ is contained in M and the reverse inclusion is obvious, giving the required result. □

The set of n integers $\alpha_1, \alpha_2, \ldots, \alpha_n$ generating a particular ideal $\mathfrak{a}$ as in the theorem, is called a *$\mathbb{Z}$-basis* for the ideal. The ideal then has the following two expressions

$$\mathfrak{a} = (\alpha_1, \alpha_2, \ldots, \alpha_n) = \mathbb{Z}\alpha_1 + \mathbb{Z}\alpha_2 + \cdots + \mathbb{Z}\alpha_n.$$

We emphasize that though some of the values α_i may be redundant in the first expression (e.g: only one value is required to write a principal ideal), there need to be exactly n values in a $\mathbb{Z}$-basis.

Note that $\mathcal{O}_K$ is an ideal and therefore has a $\mathbb{Z}$-basis, which we call an *integral basis* for K.

10 Prime Decomposition of Ideals

We will see that in terms of the arithmetic on ideals that we have just defined, there is a unique factorization of ideals into prime ideals.

An ideal $\mathfrak{p}$, properly contained in $\mathcal{O}_K$, is *prime* if $\mathfrak{p} \mid \mathfrak{a}\mathfrak{b}$ for ideals $\mathfrak{a}$ and $\mathfrak{b}$ implies that either $\mathfrak{p} \mid \mathfrak{a}$ or $\mathfrak{p} \mid \mathfrak{b}$.

We have the following nontrivial but important result.

Theorem 16. *For any ideal $\mathfrak{a}$ there exists a non-zero ideal $\mathfrak{b}$ such that $\mathfrak{a}\mathfrak{b}$ is principal.*

We can use this to prove the following.

Theorem 17. *If $\mathfrak{a}\mathfrak{b} = \mathfrak{a}\mathfrak{c}$ and $\mathfrak{a} \neq (0)$ then $\mathfrak{b} = \mathfrak{c}$.*

Proof: Choose an ideal $\mathfrak{m}$ as per the previous theorem, such that $\mathfrak{m}\mathfrak{a} = (\alpha)$ is principal. Then $(\alpha)\mathfrak{b} = (\alpha)\mathfrak{c}$ and the result follows easily. □

For ideals, there is a concept of greatest common divisor with respect to ideal multiplication as we have defined it.

Theorem 18. *Each pair $\mathfrak{a} = (\alpha_1, \alpha_2, \ldots, \alpha_k), \mathfrak{b} = (\beta_1, \beta_2, \ldots, \beta_m)$ of ideals, possesses a greatest common divisor $\mathfrak{g} = gcd(\mathfrak{a}, \mathfrak{b})$. It has the form*

$$\mathfrak{g} = (\alpha_1, \alpha_2, \ldots, \alpha_k, \beta_1, \beta_2, \ldots, \beta_m).$$

Proof: Clearly $\mathfrak{g}$ consists of all elements of the form $\alpha + \beta$ with $\alpha \in \mathfrak{a}, \beta \in \mathfrak{b}$. Since every ideal contains the integer 0 then $\mathfrak{g} \supseteq \mathfrak{a}$ and $\mathfrak{g} \supseteq \mathfrak{b}$, thus $\mathfrak{g} \mid \mathfrak{a}$ and $\mathfrak{g} \mid \mathfrak{b}$. The result follows by noting that if $\mathfrak{h} \mid \mathfrak{a}$ and $\mathfrak{h} \mid \mathfrak{b}$ for some ideal $\mathfrak{h}$ then $\mathfrak{h} \supseteq \mathfrak{a}$ and $\mathfrak{h} \supseteq \mathfrak{b}$ and so $\mathfrak{h} \supseteq \mathfrak{g}$. □

From the expression for $\mathfrak{g}$ in the theorem, and the definition of ideal multiplication, we obtain immediately

Theorem 19. *For ideals* $\mathfrak{a}, \mathfrak{b}$ *and* $\mathfrak{c}$

$$\mathfrak{c} \cdot gcd(\mathfrak{a}, \mathfrak{b}) = gcd(\mathfrak{c}\mathfrak{a}, \mathfrak{c}\mathfrak{b}).$$

We call an ideal *irreducible* if it is not the product of two nontrivial ideals (we refer to $\mathcal{O}_K$ as the trivial ideal).

Note that if the greatest common divisor of two ideals $\mathfrak{a}$ and $\mathfrak{b}$ is trivial then the ideals are coprime.

Theorem 20. *If* $\mathfrak{p}$ *is an irreducible ideal and* $\mathfrak{p} \mid \mathfrak{a}\mathfrak{b}$ *then* $\mathfrak{p}$ *divides* $\mathfrak{a}$ *or* $\mathfrak{b}$*, i.e.* $\mathfrak{p}$ *is a prime ideal.*

Proof: If $\mathfrak{p} \not| \ \mathfrak{b}$ then $\mathrm{gcd}(\mathfrak{p}, \mathfrak{b}) = (1)$ since $\mathfrak{p}$ has no other factors. Thus

$$\mathfrak{a} = \mathfrak{a}(1) = \mathfrak{a} \cdot \mathrm{gcd}(\mathfrak{p}, \mathfrak{b}) = \mathrm{gcd}(\mathfrak{a}\mathfrak{p}, \mathfrak{a}\mathfrak{b})$$

and since $\mathfrak{p} \mid \mathfrak{a}\mathfrak{b}$ then this equation says that $\mathfrak{p} \mid \mathfrak{a}$. □

Because we have a greatest common divisor, ideals factor uniquely into prime ideals by a standard argument (as for rational integers), once we have the following.

Theorem 21. *Each ideal* $\mathfrak{i}$ *has only finitely many ideal factors.*

Proof: Suppose $\mathfrak{a} = (\alpha_1, \alpha_2, \ldots, \alpha_k)$ is a factor of $\mathfrak{i}$ and that i is any algebraic integer in $\mathfrak{i}$. Let its norm be $n = \mathcal{N}(i) \in \mathbb{Z}$. Since $\mathfrak{i} \mid (i) \mid (n)$ we have that $\mathfrak{a} \mid (n)$, i.e: $\mathfrak{a}$ contains n. Now express each of the α_i of $\mathfrak{a}$ in terms of a $\mathbb{Z}$-basis $\omega_1, \omega_2, \ldots, \omega_n$ of the ring of integers $\mathcal{O}_K$

$$\mathfrak{a} = (a_{11}\omega_1 + a_{12}\omega_2 + \cdots + a_{1n}\omega_n, \ldots, a_{k1}\omega_1 + a_{k2}\omega_2 + \cdots + a_{kn}\omega_n)$$

with $a_{ij} \in \mathbb{Z}$ for all i, j. Now by reducing the a_{ij} modulo n we obtain

$$\mathfrak{a} = (a'_{11}\omega_1 + a'_{12}\omega_2 + \cdots + a'_{1n}\omega_n, \ldots, a'_{k1}\omega_1 + a'_{k2}\omega_2 + \cdots + a'_{kn}\omega_n, n)$$

with $a_{ij} \in \{0, 1, \ldots, n-1\}$ for all i, j. But there are only finitely many such ideals, and we are done. □

So we finally have the result

Theorem 22. *Every ideal* $\mathfrak{a}$ *of* $\mathcal{O}_K$ *has a unique factorization into prime ideals, upto order.*

With a little work it is possible to use this result to construct the following.

Theorem 23. *For any given nonzero ideals* $\mathfrak{a}, \mathfrak{b}$ *there exists an integer* ω *such that* $(\omega, \mathfrak{a}\mathfrak{b}) = \mathfrak{a}$*, i.e: there exists an algebraic integer* ω *in* K *which is divisible by* $\mathfrak{a}$ *but coprime with* $\mathfrak{b}$*.*

By letting $\mathfrak{b}$ be the ideal of Theorem 16 with $\mathfrak{a}\mathfrak{b} = (\beta)$ we obtain the following special case of this result.

Theorem 24. *Every ideal* $\mathfrak{a}$ *has a representation* $\mathfrak{a} = (\omega, \beta)$ *for* two *algebraic integers* ω *and* β *of* K*.*

11 Norms of Ideals

We wish to define a norm on ideals which is compatible with the norm we have on elements of the field. Since units divide every integer, their norms must divide the norm of every integer. Thus they can only have the values ±1. It makes sense therefore to have the norm of a principal ideal defined by

$$\mathcal{N}((\alpha)) = |\mathcal{N}(\alpha)|. \tag{2}$$

For any ideal $\mathfrak{a}$ we define two integers α, β to be *congruent* modulo $\mathfrak{a}$ if $\alpha - \beta \in \mathfrak{a}$; denoted as usual by $\alpha \equiv \beta \pmod{\mathfrak{a}}$.

Congruence modulo $\mathfrak{a}$ is an equivalence relation on the set of integers $\mathcal{O}_K$.

The *norm* of $\mathfrak{a}$, $\mathcal{N}(\mathfrak{a})$, is defined to be the number of congruence classes of integers modulo $\mathfrak{a}$, i.e: the maximum number of integers which are all mutually incongruent modulo $\mathfrak{a}$.

Since $\mathfrak{a}$ is the class of integers congruent to 0 modulo $\mathfrak{a}$ and since $\mathfrak{a}$ is a subgroup of $\mathcal{O}_K$, then the following result is clear.

Theorem 25. *The norm $\mathcal{N}(\mathfrak{a})$ is equal to the index of $\mathfrak{a}$ in $\mathcal{O}_K$ when they are considered as Abelian groups.*

It is clear from this that the norm of an ideal is always finite.

If $\mathfrak{a} = (\alpha_1, \alpha_2, \ldots, \alpha_n)$ with $\{\alpha_i\}$ a $\mathbb{Z}$-basis of $\mathfrak{a}$ and $\alpha_i = a_{i1}\omega_1 + a_{i2}\omega_2 + \ldots + a_{in}\omega_n$ for elements $a_{ij} \in \mathbb{Z}$ the expression for α_i in terms of a $\mathbb{Z}$-basis $\{\omega_i\}$ of $\mathcal{O}_K$, then it is clear that $\mathcal{N}(\mathfrak{a})$ is equal to the absolute value of the determinant of the coefficients a_{ij}. For this determinant gives the index of $\mathfrak{a}$ in $\mathcal{O}_K$.

Upon fixing a $\mathbb{Z}$-basis $\{\omega_i\}$ of $\mathcal{O}_K$, the definition of a discriminant leads directly to

Theorem 26. *If $\alpha_1, \alpha_2, \ldots, \alpha_n$ is a $\mathbb{Z}$-basis for $\mathfrak{a}$ then*

$$\mathcal{N}(\mathfrak{a}) = \left| \sqrt{\frac{\Delta(\alpha_1, \alpha_2, \ldots, \alpha_n)}{\mathcal{D}_K}} \right|.$$

We now see that this definition of the norm of an ideal is compatible with equation (2). For, a basis of a principal ideal (α) is given by $\alpha\omega_1, \alpha\omega_2, \ldots, \alpha\omega_n$. From the definition of a discriminant it is also clear that

$$\Delta(\alpha\omega_1, \alpha\omega_2, \ldots, \alpha\omega_n) = \mathcal{N}(\alpha)^2 \Delta(\omega_1, \omega_2, \ldots, \omega_n).$$

Thus equation (2) holds by the theorem.

Theorem 27. *For any two ideals $\mathfrak{a}, \mathfrak{b}$ we have*

$$\mathcal{N}(\mathfrak{a}\mathfrak{b}) = \mathcal{N}(\mathfrak{a})\mathcal{N}(\mathfrak{b}).$$

Proof: From Theorem 23 we can find (α), for an integer α, divisible by $\mathfrak{a}$ such that $(\alpha)/\mathfrak{a}$ is coprime to $\mathfrak{b}$. If ζ_i form a complete set of integers incongruent modulo $\mathfrak{a}$ and η_j such a set modulo $\mathfrak{b}$, then $\zeta_i + \alpha\eta_j$ form such a set modulo $\mathfrak{ab}$. □

Theorem 28. *For $\mathfrak{p}$ a prime ideal*

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

for some rational prime p and rational integer $f < n$ where n is the degree of the field K over $\mathbb{Q}$.

Proof: Since the rational integers cannot all be incongruent modulo $\mathfrak{p}$, let $a \equiv b \pmod{\mathfrak{p}}$ for some $a, b \in \mathbb{Z}$, i.e: $\mathfrak{p} \mid (a-b)$. But since $\mathfrak{p}$ is prime, it must divide one of the factors (p) of $(a-b)$ with p a rational prime. I.e: $(p) = \mathfrak{pa}$ for some ideal $\mathfrak{a}$. Thus $p^n = \mathcal{N}(\mathfrak{p})\mathcal{N}(\mathfrak{a})$. Thus $\mathcal{N}(\mathfrak{p}) = p^f$ with $f \leq n$. □

Furthermore we have

Theorem 29. *Every (p) for p a rational prime can be decomposed into at most n factors.*

Proof: Let (p) be decomposed into prime factors $(p) = \mathfrak{p}_1\mathfrak{p}_2 \dots \mathfrak{p}_r$. Then, taking norms, $p^n = \mathcal{N}(\mathfrak{p}_1)\mathcal{N}(\mathfrak{p}_2)\dots\mathcal{N}(\mathfrak{p}_r)$. Thus it is clear that $r \leq n$. □

12 Fractional Ideals

Thus far our ideals obey a cancellation law, but there is no concept of the inverse of an ideal. Since ideal multiplication is clearly associative, and even commutative from the definition, the existence of inverses would turn the set of ideals into an Abelian group. Fractional ideals rectify this situation.

A *fractional ideal* is a set of elements of K

$$\mathfrak{g} = (\rho_1, \rho_2, \dots, \rho_r) = \{\gamma_1\rho_1 + \gamma_2\rho_2 + \dots + \gamma_r\rho_r \text{ with all } \gamma_i \in \mathcal{O}_K\}$$

defined for a finite set of $\rho_i \in K$. An ideal where all the ρ_i are integral as before, will be called an *integral ideal.*

Principal fractional ideals are now of the form (ω) with $\omega \in K$.

According to the remarks after Theorem 11 an arbitrary element of K can be expressed as the quotient of two integers of K. Doing this for each of the ρ_i above, we can express all the ρ_i over a common denominator, $\rho_i = \frac{\alpha_i}{\nu}$ say. Thus it is clear that $(\nu)\mathfrak{g}$ is the integral ideal $\mathfrak{a} = (\alpha_1, \alpha_2, \dots, \alpha_r)$.

Once again, fractional ideals are infinite Abelian groups, and the analogue of Theorem 15 holds. For if $\beta_1, \beta_2, \dots, \beta_n$ is a $\mathbb{Z}$-basis for $\mathfrak{a}$, then clearly $\frac{\beta_1}{\nu}, \frac{\beta_2}{\nu}, \dots, \frac{\beta_n}{\nu}$ is a $\mathbb{Z}$-basis for $\mathfrak{g}$.

Ideal multiplication is defined as for integral ideals and is again clearly commutative and associative. The ideal $\mathcal{O}_K$ still acts as an identity.

Since we can always make $\mathfrak{g}$ integral by multiplying by the integral ideal (ν) for a suitable integer ν, we have the analogue of Theorem 16.

Theorem 30. *For any fractional ideal $\mathfrak{a}$, there is an integral ideal $\mathfrak{b}$ such that $\mathfrak{a}\mathfrak{b}$ is principal and integral.*

Theorem 17 then also follows verbatim for fractional ideals.

It is now easy to prove the following results.

Theorem 31. *If $\mathfrak{g}_1$ and $\mathfrak{g}_2$ are fractional ideals with $\mathfrak{g}_1 \neq (0)$ then there exists a unique fractional ideal $\mathfrak{l}$ such that $\mathfrak{g}_1\mathfrak{l} = \mathfrak{g}_2$.*

Note that by setting $\mathfrak{g}_2 = (1)$ we guarantee the existence of inverses. This justifies the notation $\mathfrak{l} = \frac{\mathfrak{g}_2}{\mathfrak{g}_1}$.

Theorem 32. *The set of fractional ideals of K is an Abelian group with respect to ideal multiplication.*

From Theorem 30 it is immediate that

Theorem 33. *Each fractional ideal can be expressed uniquely as the quotient of two relatively prime integral ideals $\mathfrak{g} = \frac{\mathfrak{a}_1}{\mathfrak{a}_2}$.*

We call these ideals the numerator and denominator.

The norm of a fractional ideal $\mathfrak{g}$ expressed as a quotient of integral ideals $\mathfrak{g} = \frac{\mathfrak{a}_1}{\mathfrak{a}_2}$ is defined to be

$$\mathcal{N}(\mathfrak{g}) = \frac{\mathcal{N}(\mathfrak{a}_1)}{\mathcal{N}(\mathfrak{a}_2)}.$$

Once again Theorem 27 holds verbatim for fractional ideals.

Also if $\alpha_1, \alpha_2, \dots, \alpha_n$ is a $\mathbb{Z}$-basis for a fractional ideal $\mathfrak{a}$ then Theorem 26 applies unchanged. The proof is much the same, but requires one to first convert $\mathfrak{a}$ to an integral ideal by multiplying by a suitable (ν).

13 The Class Number

We define an equivalence relation on fractional ideals. We say that ideals $\mathfrak{a}$ and $\mathfrak{b}$ are equivalent, denoted $\mathfrak{a} \sim \mathfrak{b}$ if there exists a principal ideal (c) such that $\mathfrak{a} = \mathfrak{b}(c)$. This equivalence relation partitions the Abelian group of non-zero fractional ideals $\mathcal{F}$ into equivalence classes which are cosets of the subgroup of non-zero principal fractional ideals P.

We call the quotient group $Cl_K = \mathcal{F}/P$ the *ideal class group* of the number field K.

Our aim in this section is to show that Cl_K is always a finite Abelian group. It is already clear that it is an Abelian group. This can also be seen by noting that if $\mathfrak{a} \sim \mathfrak{b}$ then $\mathfrak{ac} \sim \mathfrak{bc}$, and if $\mathfrak{c} \neq 0$ the converse holds by the analogue of Theorem 17 for fractional ideals. Thus multiplication respects ideal classes and the group multiplication of ideal classes is well defined.

It remains only to prove that the class group is finite. Firstly we prove

Theorem 34. *Let $N = \mathcal{N}(\mathfrak{a})$ for a non-zero integral ideal $\mathfrak{a}$, then $\mathfrak{a} \mid (N)$.*

Proof: In the quotient group $\mathcal{O}_K/\mathfrak{a}$ which is of order N (by Theorem 25), every element has order dividing N. Thus for any $x \in \mathcal{O}_K$ we have $Nx \in \mathfrak{a}$. Taking $x = 1$ we have $N \in \mathfrak{a}$, thus $\mathfrak{a} \mid (N)$. □

Theorem 35. *There are only finitely many integral ideals with norm equal to a positive integer N.*

Proof: Since (N) has only finitely many divisors, then by the previous theorem, the result follows. □

Theorem 36. *There exists a non-zero element $a \in \mathfrak{a}$ for each non-zero integral ideal $\mathfrak{a}$ such that*

$$|N_{K/\mathbb{Q}}(a)| \leq \mathcal{N}(\mathfrak{a}) \cdot \mu,$$

where μ is a positive integer dependent only on the number field K.

Proof: Let $\alpha_1, \alpha_2, \ldots, \alpha_n$ be an integral basis of K. Let k be the integer such that $k^n \leq \mathcal{N}(\mathfrak{a}) < (k+1)^n$. Let S be the set of all elements $\sum_{i=1}^n d_i x_i$ with $0 \leq d_i \leq k$. Since $(k+1)^n > \mathcal{N}(\mathfrak{a})$ there must be two elements $b, c \in S$ which are not equal and such that $a = b - c = \sum_{i=1}^n a_i x_i$ is in $\mathfrak{a}$. Clearly $|a_i| \leq k$. Letting $x_i^{(1)}, x_i^{(2)}, \ldots, x_i^{(n)}$ be the conjugates of x_i, then

$$\left|\mathcal{N}_{K/\mathbb{Q}}(\mathfrak{a})\right| = \prod_{j=1}^n \left|\sum_{i=1}^n a_i x_i^{(j)}\right| \leq \prod_{j=1}^n k \left(\sum_{i=1}^n \left|x_i^{(j)}\right|\right) = k^n \cdot \prod_{j=1}^n \left(\sum_{i=1}^n \left|x_i^{(j)}\right|\right).$$

Note that each $|x_i^{(j)}|$ is an algebraic integer. Also each of the conjugates in K of $\mu = \prod_{j=1}^n \left(\sum_{i=1}^n \left|x_i^{(j)}\right|\right)$ have the same value. Thus μ is a rational integer which is manifestly positive. Note μ only depends on K, and $k^n \leq \mathcal{N}(\mathfrak{a})$ leads to $\left|\mathcal{N}_{K/\mathbb{Q}}(\mathfrak{a})\right| \leq \mathcal{N}(\mathfrak{a}) \cdot \mu$ as required. □

Theorem 37. *The class number Cl_K is finite.*

Proof: By Theorem 35 there are only a finite number of ideals $\mathfrak{a}_1, \mathfrak{a}_2, \ldots, \mathfrak{a}_k$ which are nonzero and such that $\mathcal{N}(\mathfrak{a}_i) \leq \mu$.

Let $\mathfrak{b}$ be any fractional ideal of $\mathcal{O}_K$. By our comments after the definition of a fractional ideal, there exists a non-zero $\nu \in \mathcal{O}_K$ such that $\nu\mathfrak{b}^{-1}$ is integral. By Theorem 36 there is a non-zero $b \in \nu\mathfrak{b}^{-1}$ such that $\mathcal{N}((b)) \leq \mathcal{N}(\nu\mathfrak{b}^{-1}) \cdot \mu$. Multiply by $\mathcal{N}(\mathfrak{b})$ and note that $b\nu^{-1}\mathfrak{b}$ is an integral ideal, since $b \in \nu\mathfrak{b}^{-1}$. Thus

$$\mathcal{N}(b\nu^{-1}\mathfrak{b})\,\mathcal{N}((\nu)) = \mathcal{N}(b\mathfrak{b}) = \mathcal{N}((b))\,\mathcal{N}(\mathfrak{b}) \leq \mathcal{N}(\nu\mathfrak{b}^{-1})\,\mathcal{N}(\mathfrak{b})\mu = \mathcal{N}((\nu))\mu.$$

That is, $\mathcal{N}(b\nu^{-1}\mathfrak{b}) \leq \mu$.

Thus each class contains an ideal of norm bounded by μ, of which there are finitely many, and we are done. □

The number $h = h_K$ of ideal classes is called the *class number* of K.

Since raising any element of a group to a power equal to the order of that group will give the identity, we have

Theorem 38. *Let $\mathfrak{a}$ be a non-zero fractional ideal of $\mathcal{O}_K$, then $\mathfrak{a}^h$ is principal.*

14 Minkowski's Theorem

We would like to place a bound on the class number of an algebraic number field. For this we require methods from the geometry of numbers. It involves considering the ring of integers as a lattice in a certain space, and ideals as sublattices.

For a number field K of degree n we consider the so called Etale algebra $\mathcal{O}_K \otimes \mathbb{R}$. We don't need to know about this except that it embeds $\mathcal{O}_K$ into $\mathbb{R}^n$ as follows. Take $\alpha \in \mathcal{O}_K$. Let $\sigma_1, \sigma_2, \ldots, \sigma_n$ be the embeddings of K into the complex numbers. In fact let $\sigma_1, \sigma_2, \ldots, \sigma_r$ be the real embeddings and $\sigma'_1, \sigma'_2, \ldots, \sigma'_s$ be the complex embeddings, each with a conjugate $\overline{\sigma}'_i$. Think of the complex plane as $\mathbb{R}^2$, so each σ'_i embeds into $\mathbb{R}^2$. Then define our embedding of $\alpha \in \mathcal{O}_K$ into $\mathbb{R}^n$ by

$$\sigma(\alpha) = (\sigma_1(\alpha), \sigma_2(\alpha), \ldots, \alpha_r(\alpha), \sigma'_1(\alpha), \sigma'_2(\alpha), \ldots, \sigma'_s(\alpha)).$$

Now any integral basis for $\mathcal{O}_K$ becomes n independent vectors in $\mathbb{R}^n$ under this embedding, and thus $\mathcal{O}_K$ becomes a full lattice in $\mathbb{R}^n$.

Considering that the norm N of an integral ideal $\mathfrak{a}$ is the index of $\mathfrak{a}$ in $\mathcal{O}_K$ as a subgroup, embedding this ideal $\mathfrak{a}$ in the same way introduces it as a sublattice in $\mathbb{R}^n$ of the ring of integers $\mathcal{O}_K$ of index N.

We can define the volume of a lattice to be given by the volume of a fundamental region for that lattice. Then we have the following important theorem.

Theorem 39. *Let χ be the lattice given by embedding $\mathcal{O}_K$, and Λ the lattice corresponding to the integral ideal $\mathfrak{a}$ of norm N, then*

$$vol(\chi) = \frac{1}{2^s}\sqrt{|\mathcal{D}_K|}$$
$$vol(\Lambda) = N \cdot vol(\chi).$$

The theorem from the geometry of numbers that we will apply is

Theorem 40. *(Minkowski) Let Λ be a lattice in $\mathbb{R}^n$ and A be a bounded convex symmetric subset of $\mathbb{R}^n$. If $vol(A) > 4 \cdot vol(\Lambda)$ then there is at least one lattice point in A.*

Let $D_1 = \{(\alpha_1, \alpha_2, \dots, \alpha_n) \in \mathbb{R}^n$ such that $\prod_{j=1}^{r} |\alpha_i| \cdot \prod_{i=r+1}^{r+s} (\alpha_i^2 + \alpha_{i+s}^2) \leq 1\}$. We will show that for every symmetric, convex $D \subseteq D_1$ there is a non-zero element $a \in \mathfrak{a}$ such that

$$|\mathcal{N}(a)| \leq \frac{2^{r+s}}{\text{vol}(D)}\mathcal{N}(\mathfrak{a}) \cdot \sqrt{|\mathcal{D}_K|}.$$

Let $\rho \in \mathbb{R}^+$ be such that $\rho^n = \frac{2^{r+s}}{\text{vol}(D)}\mathcal{N}(\mathfrak{a}) \cdot \sqrt{|\mathcal{D}_K|}$. Consider

$$\rho D = \{\rho\alpha \text{ such that } \alpha \in D\},$$

then $\text{vol}(\rho D) = \rho^n \cdot \text{vol}(D) = 2^n \cdot \text{vol}(\Lambda)$ as per Theorem 39.

Thus by Minkowski's theorem, there is a non-zero $\zeta \in D$ such that $\rho\zeta \in \Lambda$, i.e: there is a lattice point in Λ. So there is an $a \in \mathfrak{a}$ such that $\rho\zeta = \sigma(a)$. Now $\sigma(a) \in \rho D \subseteq \rho D_1$ so that $\sigma(a) = (\rho\alpha_1, \rho\alpha_2, \dots, \rho\alpha_n)$ for some $(\alpha_1, \alpha_2, \dots, \alpha_n) \in D_1$.

But $|\mathcal{N}(a)| = \prod_{j=1}^{n} |a^{(j)}|$. Also $a^{(r+s+i)} = \overline{a^{(r+i)}}$ for $i = 1, 2, \dots, s$. Thus $|a^{(r+s+i)}| \cdot |a^{(r+i)}| = (\text{Re } a^{(r+i)})^2 + (\text{Im } a^{(r+i)})^2 = \rho^2(\alpha_{r+i}^2 + \alpha_{r+s+i}^2)$. Similarly $|a^{(i)}| = \rho|\alpha_i|$ for $i = 1, 2, \dots, r$.

Thus we have that $|\mathcal{N}(a)| \leq \rho^n$ from the definition of D_1, and the result follows.

Theorem 41. *For each non-zero integral ideal $\mathfrak{a}$ of K, there is a non-zero $a \in \mathfrak{a}$ such that*

$$|\mathcal{N}(a)| \leq \left(\frac{4}{\pi}\right) \frac{n!}{n^n} \sqrt{|\mathcal{D}_K|} \cdot \mathcal{N}(\mathfrak{a}).$$

Proof: Choose $D = \{(\alpha_1, \alpha_2, \dots, \alpha_n) \in \mathbb{R}^n$ such that

$$|\alpha_1| + \cdots + |\alpha_r| + 2\sqrt{\alpha_{r+1}^2 + \alpha_{r+s+1}^2} + \cdots + 2\sqrt{\alpha_{r+s}^2 + \alpha_n^2} \leq n\}.$$

By the A.M. $\geq$ G.M. inequality $D \subseteq D_1$. Also it is clear that D is symmetric and convex. The volume of D is computed by induction on r and s using integration. Thus $\text{vol}(D) = \frac{2^r \left(\frac{\pi}{2}\right)^s n^n}{n!}$. The result follows. □

By taking $\mathfrak{a} = \mathcal{O}_K$ we deduce

Corollary 1.

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

By explicit computation, all the prime ideals whose norm is less than the Minkowski bound can be quickly found and thus the class number can be bounded. Although not best possible, the Minkowski bound does help narrow the possibilities down quickly in numerous practical situations.

15 The Unit Group

The methods of Minkowski can also be applied to the group of units U_K, i.e: the group of invertible elements of $\mathcal{O}_K$.

This time the map that is used is

$$f(\alpha) = (\log|\sigma_1(\alpha)|, \ldots, \log|\sigma_r(\alpha)|, \log(|\sigma_{r+1}(\alpha)|^2), \ldots, \log(|\sigma_{r+s}(\alpha)|^2))$$

for any $\alpha \in \mathcal{O}_K$. This maps the non-zero integers into $\mathbb{R}^{r+s}$ and induces a homomorphism ϕ of the unit group U_K into $\mathbb{R}^{r+s}$.

We firstly prove that the kernel of g is finite. Indeed for any bounded subset $Z \subset \mathbb{R}^{r+s}$ the preimage $\phi^{-1}(Z)$ is finite. For, Z bounded means that for all $\phi(u) \in Z$ there is a uniform c such that $|\sigma_i(u)| \leq c$ for all i. But then the coefficients of the characteristic polynomial of u, $\prod_{i=1}^{n}(X - \sigma_i(u))$ are bounded (and rational integers). Thus there can only be finitely many such u. Thus the kernel of ϕ is a finite subgroup of $\mathcal{O}_K$. In particular it is a finite subgroup of the multiplicative group $K^\times$ of the field K. It is therefore cyclic.

It is clear however that all the roots of unity in K belong to this kernel. For if z is such a root of unity, $m \cdot \phi(z) = \phi(z^m) = \phi(1) = 0$ so that $\phi(z) = 0$ (recall it is a vector in $\mathbb{R}^{r+s}$). Thus it is clear that this kernel actually consists of the roots of unity.

For any unit u of K we have $\mathcal{N}(u) = \pm 1$, for it must be simultaneously a unit of K (the norm of a unit is a product of units) and a rational integer. Thus $\prod |\sigma_i(u)| = 1$ and so we have

$$\log|\sigma_1(u)| + \cdots + \log|\sigma_r(u)| + \log(|\sigma_{r+1}(u)|^2) + \cdots + \log(|\sigma_{r+s}(u)|^2)) = 0.$$

Thus $\phi(U_K)$ is contained in the hyperplane H of $\mathbb{R}^{r+s}$ given by the equation $y_1 + y_2 + \cdots + y_{r+s} = 0$.

The main result which follows by applying Minkowski's Theorem in this situation is the following.

Theorem 42. *The unit group U_K is a finitely generated Abelian group of rank $r + s - 1$.*

A set of generators for U_K is called a set of *fundamental units* of K.