

ALGEBRAIC NUMBER THEORY

0.1. **Algebraic Numbers.** *Algebraic number theory* is the study of extension fields $\mathbb{Q}(\alpha_1, \alpha_2, \dots, \alpha_n)$ 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* (definition below).

Recall that $\mathbb{Q}(\alpha_1, \alpha_2, \dots, \alpha_n)$ denotes the field of all numbers obtained by finitely many arithmetic operations, $+$, \times , $-$, \div , from rational numbers and the α_i .

Definition (Algebraic) 0.1.1. *A number $\alpha \in \mathbb{C}$ is called algebraic if it is the root of a monic polynomial*

$$(1) \quad x^n + a_1x^{n-1} + a_2x^{n-2} + \dots + a_{n-1}x + a_n = 0$$

with rational coefficients a_i . Otherwise, it is called a transcendental number.

In particular we are interested in defining for an algebraic number field K a subring \mathcal{O}_K called the *ring of integers*. These so-called algebraic integers will have properties akin to those of the usual ring of integers \mathbb{Z} of the rational number field \mathbb{Q} . To avoid confusion we henceforth call the ordinary integers \mathbb{Z} , *rational integers*.

Definition (Integer) 0.1.2. *An algebraic integer (or integer for short) $\alpha \in \mathbb{C}$ is a root of a monic polynomial*

$$(2) \quad x^n + b_1x^{n-1} + b_2x^{n-2} + \dots + b_{n-1}x + b_n = 0$$

with rational integer coefficients b_i . The ring of integers \mathcal{O}_K of an algebraic number field K is the subring of all integers contained in it.

A ring of integers \mathcal{O}_K clearly has no zero divisors and thus is actually an integral domain.

The set of *all* algebraic integers $\alpha \in \mathbb{C}$ also forms a ring (integral domain), whilst the set of *all* algebraic numbers is a field. However these objects are too general (for now) and we stick with the simpler algebraic number fields and their rings of integers as we have defined them.

Example 0.1.3. *The earliest example is the Gaussian integers of Gauss, denoted $\mathbb{Z}[i]$. Recall that this means all numbers obtained from rational integers and i by $+$, $-$ and \times , and thus is the ring of numbers of the form $a + bi$, with $a, b \in \mathbb{Z}$.*

Example 0.1.4. *Next came the cyclotomic number fields $\mathbb{Q}(\zeta_n)$ of Kummer, where ζ_n is a complex n^{th} root of unity, i.e. satisfying $x^n - 1 = 0$. The ring of integers of such a field is $\mathbb{Z}[\zeta_n]$.*

Example 0.1.5. *Another important example is the quadratic number field $\mathbb{Q}(\alpha)$ with α a root of $ax^2 + bx + c$. These come in two types:*

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

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

The following theorem simplifies matters somewhat.

Theorem 0.1.6. *Any algebraic number field is expressible as $K = \mathbb{Q}(\alpha)$ with a single algebraic generator α .*

Lemma 0.1.7. *The monic polynomial of minimum degree n that an algebraic number α satisfies, is unique. It is called the minimum polynomial of α . The degree n is called the degree of α denoted $\deg \alpha$.*

Definition 0.1.8. *For an algebraic number field $\mathbb{Q}(\alpha)$, the degree of the generator α is also called the degree of the field.*

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

Theorem 0.1.9. *If $K = \mathbb{Q}(\alpha)$ with $\deg \alpha = n$, then for any other $\beta \in K$ we have $\deg \beta \mid n$. If $\deg \beta = n$, then in fact $K = \mathbb{Q}(\beta)$, i.e. K can also be generated, as an extension of \mathbb{Q} , by β .*

Any element of an algebraic number field can be expressed in a simple way in terms of a generator.

Theorem 0.1.10. *Any $\beta \in \mathbb{Q}(\alpha)$ can be expressed in the form*

$$(3) \quad \beta = c_0 + c_1\alpha + c_2\alpha^2 + \cdots + c_{n-1}\alpha^{n-1}$$

with the $c_i \in \mathbb{Q}$.

All of the above works just as well with an arbitrary algebraic number field K for the base field instead of \mathbb{Q} . I.e: take any $\alpha \in L$, not already in K , satisfying a monic polynomial with coefficients in K and which generates the extension $L = K(\alpha)$. We say that this polynomial with coefficients in K is *over K* . The field L is called an extension of K and is often denoted L/K , “ L over K ”. If the minimum monic polynomial over K which α satisfies has degree n , we say L/K is of degree n and write $[L : K] = n$. In fact we have the following, which generalizes the previous theorem.

Theorem 0.1.11. *If L/K is an extension of algebraic number fields of degree n , then L is a vector space of dimension n over K . If $L = K(\alpha)$, then a basis is $[1, \alpha, \alpha^2, \dots, \alpha^{n-1}]$. I.e: each $\beta \in L$ can be expressed as*

$$(4) \quad \beta = c_0 + c_1\alpha + c_2\alpha^2 + \cdots + c_{n-1}\alpha^{n-1}$$

with $c_i \in K$.

The reason that powers higher than α^{n-1} are not needed is because the minimum polynomial of α can always be used to express α^n in terms of lower powers

$$(5) \quad \alpha^n + a_1\alpha^{n-1} + a_2\alpha^{n-2} + \cdots + a_{n-1}\alpha + a_n = 0.$$

Thus in a similar manner we have

Lemma 0.1.12. *Given an algebraic integer α of degree n , every element β of the ring $\mathbb{Z}[\alpha]$ can be expressed in the form*

$$(6) \quad \beta = c_0 + c_1\alpha + \cdots + c_{n-1}\alpha^{n-1}$$

with $c_i \in \mathbb{Z}$.

The ring of integers of a number field $\mathbb{Q}(\alpha)$ is *not* always $\mathbb{Z}[\alpha]$.

Example 0.1.13. *Consider the quadratic number field $\mathbb{Q}(\alpha)$ with α a root of $ax^2 + bx + c$. Let $d = b^2 - 4ac$ be the discriminant of this field. Remove any odd square factors and factors of 16 from d . What is left is called a fundamental discriminant d and it is either $\equiv 0$ or $1 \pmod{4}$. Since $\sqrt{d} \in \mathbb{Q}(\alpha)$ and is quadratic over \mathbb{Q} , then we must have $K = \mathbb{Q}(\alpha) = \mathbb{Q}(\sqrt{d})$. The following two cases exist:*

$$(i) \text{ if } d \equiv 1 \pmod{4} \text{ then } \mathcal{O}_K = \mathbb{Z} \left[\frac{1+\sqrt{d}}{2} \right];$$

$$(ii) \text{ if } d = 4N \text{ then } \mathcal{O}_K = \mathbb{Z}[\sqrt{N}].$$

By analogy with the rational integers, we wish to have a concept of divisibility in the ring of integers \mathcal{O}_K of an algebraic number field K .

Definition 0.1.14. *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 $\alpha = \beta\gamma$.*

Definition 0.1.15. *An integer $\epsilon \in \mathcal{O}_K$ which divides all integers in \mathcal{O}_K is called a unit. In particular it divides the identity 1, i.e.: it has an inverse $\epsilon^{-1} \in \mathcal{O}_K$.*

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

Definition 0.1.16. *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.*

Association is an equivalence relation with units being the integers that are associated to 1.

Examples 0.1.17. *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 $\pm \left(\frac{1+\sqrt{5}}{2} \right)^n \forall n \in \mathbb{Z}$.*

0.2. Conjugate Fields.

Definition 0.2.1. Let the field $K = \mathbb{Q}(\alpha)$ be given with generator α having minimum polynomial $f(x)$ of degree n . The n roots of $f(x)$, $\alpha = \alpha_1, \alpha_2, \dots, \alpha_n$ are called conjugates of α .

Since $f(x)$ is a minimum polynomial, it cannot factorise. 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 in the form (3), the map σ_i which takes α to α_i in this expression, can be seen to define an isomorphism from K to the field $\mathbb{Q}(\alpha_i)$.

Definition 0.2.2. 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.

Definition 0.2.3. 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 $\text{Gal}(K/\mathbb{Q})$.

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 $\text{Gal}(L/K)$.

All of the above notions have a different expression in modern parlance. Instead of a collection of conjugate fields $\mathbb{Q}(\alpha_i)$ we like to think of a *single* abstract field K having n distinct embeddings into the complex numbers, $\sigma_i : K \hookrightarrow \mathbb{C}$. Thus the $\mathbb{Q}(\alpha_i)$ are “complex realisations” of the field K .

Definition 0.2.4. If the embedding σ 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 $\sigma' : \alpha \mapsto \bar{\alpha}_i$, where the bar denotes complex conjugation.

Definition 0.2.5. Any field K which has only real embeddings is called a totally real field.

0.3. Norm and Trace. We extend the notion of conjugates to arbitrary elements α of the field L of an extension L/K (we write $\alpha \in L/K$).

Definition 0.3.1. If σ_i are the embeddings of L fixing K , then for an arbitrary $\alpha \in L/K$ 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.

Definition 0.3.2. The norm, with respect to the extension L/K , of an arbitrary $\alpha \in L$ is the value

$$(7) \quad N_{L/K}(\alpha) = \prod_{\sigma} \sigma(\alpha)$$

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

Definition 0.3.3. 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 we have the following.

Theorem 0.3.4.

$$(8) \quad \mathcal{N}(a) = a^n \quad \forall a \in \mathbb{Q}$$

where n is the degree of the extension L/\mathbb{Q} .

Of course a similar result follows for relative extensions L/K by replacing \mathbb{Q} with K throughout.

Since each embedding σ respects multiplication

$$(9) \quad \sigma(\alpha\beta) = \sigma(\alpha)\sigma(\beta)$$

then we easily derive the following.

Theorem 0.3.5. For all $\alpha, \beta \in L/K$

$$(10) \quad N_{L/K}(\alpha\beta) = N_{L/K}(\alpha)N_{L/K}(\beta)$$

It is an easy exercise in Galois theory to prove

Theorem 0.3.6. For all $\alpha \in L/K$

$$(11) \quad N_{L/K}(\alpha) \in K.$$

In particular, if α is an integer of L , then the norm is an integer of K .

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

The norm of an element is related to the constant coefficient of its minimal polynomial.

Theorem 0.3.7. *Suppose $\alpha \in L/K$ with $[L : K] = n$ and the minimum polynomial of α is $f(x)$ with degree h and constant coefficient a_0 , then*

$$(12) \quad N_{L/K}(\alpha) = (-1)^n a_0^{n/h}.$$

Using this theorem twice, we obtain

Theorem 0.3.8. *If $K \subset L \subset M$ is a tower of extensions, then for $\alpha \in L$*

$$(13) \quad N_{M/K}(\alpha) = (-1)^{[M:L]} N_{L/K}(\alpha)^{[M:L]}.$$

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.

We also define

Definition 0.3.9. *The trace of $\alpha \in L/K$ is given by*

$$(14) \quad Tr_{L/K}(\alpha) = \sum_{\sigma} \sigma(\alpha).$$

As per theorem (0.3.4) we have

Theorem 0.3.10. *For an extension L/K*

$$(15) \quad Tr_{L/K}(a) = [L : K] \cdot a \quad \forall a \in K.$$

Theorem 0.3.11. *With conditions as per theorem (0.3.7) we have*

$$(16) \quad Tr_{L/K}(\alpha) = -(n - h)a_{n-1}$$

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

Thus again

Theorem 0.3.12. *For all $\alpha \in L/K$*

$$(17) \quad Tr_{L/K}(\alpha) \in K,$$

with integers going to integers.

In fact the trace is a linear transformation between \mathbb{Q} -vector spaces $Tr_{L/K} : L \rightarrow K$, the most important property being

Theorem 0.3.13. *For all $\alpha, \beta \in L/K$*

$$(18) \quad Tr_{L/K}(\alpha + \beta) = Tr_{L/K}(\alpha) + Tr_{L/K}(\beta).$$

Theorem 0.3.14. *For $K \subset L \subset M$*

$$(19) \quad Tr_{M/K}(\alpha) = [M : L] \cdot Tr_{L/K}(\alpha).$$

0.4. The Discriminant. It is convenient to denote the value $\sigma(\alpha)$ for an embedding σ , by $\alpha\sigma$. This should not cause confusion since σ is an embedding rather than an element.

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.

Definition 0.4.1. *Given any n numbers, $\alpha_1, \alpha_2, \dots, \alpha_n$ in a field K of degree n over \mathbb{Q} , we define their discriminant by the determinant*

$$(20) \quad \Delta(\alpha_1, \alpha_2, \dots, \alpha_n) = \begin{vmatrix} \alpha_1\sigma_1 & \alpha_1\sigma_2 & \dots & \alpha_1\sigma_n \\ \alpha_2\sigma_1 & \alpha_2\sigma_2 & \dots & \alpha_2\sigma_n \\ \dots & \dots & \dots & \dots \\ \alpha_n\sigma_1 & \alpha_n\sigma_2 & \dots & \alpha_n\sigma_n \end{vmatrix}^2$$

where the σ_i are the n embeddings of the field K into the complex numbers.

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

Theorem 0.4.2. *The discriminant is equivalent to the following*

$$(21) \quad \Delta(\alpha_1, \alpha_2, \dots, \alpha_n) = \det(\text{Tr}(\alpha_i\alpha_j)).$$

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

$$(22) \quad \Delta(1, \theta, \theta^2, \dots, \theta^{n-1}) = \begin{vmatrix} 1 & 1 & \dots & 1 \\ \theta_1 & \theta_2 & \dots & \theta_n \\ \dots & \dots & \dots & \dots \\ \theta_1^{n-1} & \theta_2^{n-1} & \dots & \theta_n^{n-1} \end{vmatrix}^2$$

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

We can evaluate this using Vandermonde's theorem and obtain

Theorem 0.4.3.

$$(23) \quad \Delta(1, \theta, \theta^2, \dots, \theta^{n-1}) = \prod_{1 \leq i < j \leq n} (\theta_i - \theta_j)^2.$$

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

$$(24) \quad \Delta(1, \theta, \theta^2, \dots, \theta^{n-1}) \in \mathbb{Q}.$$

Definition 0.4.5. *For $\alpha \in K$ let α_i for $i = 1 \dots n$ be its conjugates. We call the following polynomial the characteristic polynomial of α*

$$(25) \quad f(x) = (x - \alpha_1)(x - \alpha_2) \cdots (x - \alpha_n).$$

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

Definition 0.4.6. Define the discriminant of $f(x)$ as follows

$$(26) \quad \text{Disc}(f) = (-1)^{n(n-1)/2} \prod_{j=1}^n f'(\alpha_j).$$

By evaluating the expression on the right we see that

Theorem 0.4.7. For any $\alpha \in K$ the discriminant of powers of α is equal to the discriminant of its characteristic polynomial

$$(27) \quad \Delta(1, \alpha, \dots, \alpha^{n-1}) = \text{Disc}(f).$$

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 $\alpha_1, \alpha_2, \dots, \alpha_n$ be a basis for K , with

$$(28) \quad \alpha_i = h_{i1} + h_{i2}\theta + \dots + h_{in}\theta^{n-1}$$

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

Theorem 0.4.8.

$$(29) \quad \Delta(\alpha_1, \alpha_2, \dots, \alpha_n) = \det(h_{ij})^2 \cdot \Delta(1, \theta, \theta^2, \dots, \theta^{n-1}).$$

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 only non-zero if and only if the α_i are a basis of K . Thus

Theorem 0.4.9. $\Delta(\alpha_1, \alpha_2, \dots, \alpha_n)$ is non-zero iff $\alpha_1, \alpha_2, \dots, \alpha_n$ 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 theorem

Theorem 0.4.10. For any $\alpha_1, \alpha_2, \dots, \alpha_n \in \mathcal{O}_K$ we have

$$(30) \quad \Delta(\alpha_1, \alpha_2, \dots, \alpha_n) \in \mathbb{Z}.$$

From theorem (0.4.8) 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.

Theorem 0.4.11. We call the discriminant of values $\alpha_1, \alpha_2, \dots, \alpha_n \in \mathcal{O}_K$ 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

$$(31) \quad \mathcal{D}_K = \Delta(\alpha_1, \alpha_2, \dots, \alpha_n).$$

0.5. 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.

Example 0.5.1. 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 functions as a prime.

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

Definition 0.5.2. An integral domain \mathcal{O} is a Euclidean domain if it possesses a norm (a map $n : \mathcal{O} \rightarrow \mathbb{Z}_{\geq 0}$) with

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

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

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

$$(32) \quad \alpha = \gamma\beta + \delta \quad \text{with } n(\delta) < n(\beta),$$

i.e: the ring has a Euclidean algorithm.

Example 0.5.3. For $\alpha = a + bi \in \mathbb{Z}[i]$ choose the norm to be $n(\alpha) = a^2 + b^2$.

Theorem 0.5.4. 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 $\mathcal{O}_K = \mathbb{Z}[\sqrt{-5}]$, by Example (0.1.13). In this ring

$$(33) \quad 6 = 2 \times 3 = (1 + \sqrt{-5})(1 - \sqrt{-5}).$$

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

Theorem 0.5.5. If $\alpha \mid \beta$ for $\alpha, \beta \in \mathcal{O}_K$ then $\mathcal{N}(\alpha) \mid \mathcal{N}(\beta)$.

We apply this to (33). 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!

0.6. 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 following observation.

Theorem 0.6.1. *For $\alpha, \beta \in \mathbb{Z}$ the ideal of numbers*

$$(34) \quad (\alpha, \beta) = \{m\alpha + n\beta : m, n \in \mathbb{Z}\}$$

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

We thus make the following definition.

Definition 0.6.2. *For each $\alpha, \beta \in \mathcal{O}_K$ define the ideal*

$$(35) \quad (\alpha, \beta) = \{\gamma\alpha + \delta\beta : \gamma, \delta \in \mathcal{O}_K\}.$$

Clearly if $1 \in (\alpha, \beta)$ then $(\alpha, \beta) = \mathcal{O}_K$.

Definition 0.6.3. *If $1 \in (\alpha, \beta) = \mathcal{O}_K$ we call α and β 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).

Definition 0.6.4. *An ideal is a set of integers*

$$(36) \quad (\alpha_1, \alpha_2, \dots, \alpha_k) = \{\gamma_1\alpha_1 + \gamma_2\alpha_2 + \dots + \gamma_k\alpha_k : \gamma_i \in \mathcal{O}_K\},$$

given for each finite set of 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: $\mathfrak{a} = (\alpha_1, \alpha_2, \dots, \alpha_k)$.

Definition 0.6.5. *An ideal of the form*

$$(37) \quad (\alpha) = \{\gamma\alpha : \gamma \in \mathcal{O}_K\}$$

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

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

Lemma 0.6.6. *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 correspondence 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.

Properties 0.6.7. *The following definitions and results describe an arithmetic of ideals:*

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

(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 $\mathfrak{a} = (\alpha_1, \alpha_2, \dots, \alpha_k), \mathfrak{b} = (\beta_1, \beta_2, \dots, \beta_m)$ define the product of these two ideals by $\mathfrak{a}\mathfrak{b} = (\alpha_1\beta_1, \alpha_1\beta_2, \dots, \alpha_k\beta_m)$. (Thinking of ideals as a G.C.D. helps with motivating 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 $\mathfrak{a} \mid \mathfrak{a}\mathfrak{b}$ and $\mathfrak{b} \mid \mathfrak{a}\mathfrak{b}$ for all ideals $\mathfrak{a}, \mathfrak{b}$, as we might hope.

Theorem 0.6.8. *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*

$$(38) \quad \alpha = m_1\alpha_1 + m_2\alpha_2 + \dots + m_n\alpha_n \text{ with all } m_i \in \mathbb{Z}.$$

This applies in particular for the identity ideal, \mathcal{O}_K itself. (For a proof of this see Hilbert's theorem 5).

Definition 0.6.9. *The set of n integers $\alpha_1, \alpha_2, \dots, \alpha_n$ 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*

$$(39) \quad \mathfrak{a} = (\alpha_1, \alpha_2, \dots, \alpha_n) = \mathbb{Z}\alpha_1 + \mathbb{Z}\alpha_2 + \dots + \mathbb{Z}\alpha_n.$$

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.

0.7. 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.

Definition 0.7.1. *An ideal \mathfrak{p} , properly contained in \mathcal{O}_K , is prime if it has no factors other than $(1) = \mathcal{O}_K$ and \mathfrak{p} .*

The proof of unique factorization of ideals usually proceeds along the following lines, starting with the non-trivial result

Theorem 0.7.2. *For any ideal \mathfrak{a} there exists a non-zero ideal \mathfrak{b} such that $\mathfrak{a}\mathfrak{b}$ is principal.*

Theorem 0.7.3. *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. \square

Theorem 0.7.4. *Each pair $\mathfrak{a} = (\alpha_1, \alpha_2, \dots, \alpha_k), \mathfrak{b} = (\beta_1, \beta_2, \dots, \beta_m)$ of ideals, possesses a greatest common divisor $\mathfrak{d} = \gcd(\mathfrak{a}, \mathfrak{b})$. It has the form*

$$(40) \quad \mathfrak{d} = (\alpha_1, \alpha_2, \dots, \alpha_k, \beta_1, \beta_2, \dots, \beta_m).$$

Proof: Clearly \mathfrak{d} 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 $\mathfrak{d} \supseteq \mathfrak{a}$ and $\mathfrak{d} \supseteq \mathfrak{b}$, thus $\mathfrak{d} \mid \mathfrak{a}$ and $\mathfrak{d} \mid \mathfrak{b}$. Similar kinds of arguments suffice to demonstrate the maximality and uniqueness therein of \mathfrak{d} as a common divisor of \mathfrak{a} and \mathfrak{b} . \square

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

Theorem 0.7.5. *For ideals $\mathfrak{a}, \mathfrak{b}$ and \mathfrak{c}*

$$(41) \quad \mathfrak{c} \cdot \gcd(\mathfrak{a}, \mathfrak{b}) = \gcd(\mathfrak{c}\mathfrak{a}, \mathfrak{c}\mathfrak{b}).$$

Theorem 0.7.6. *If \mathfrak{p} is prime and $\mathfrak{p} \mid \mathfrak{a}\mathfrak{b}$ then \mathfrak{p} divides \mathfrak{a} or \mathfrak{b} .*

Proof: If $\mathfrak{p} \nmid \mathfrak{b}$ then $\gcd(\mathfrak{p}, \mathfrak{b}) = (1)$ since \mathfrak{p} has no other factors. Thus

$$(42) \quad \mathfrak{a} = \mathfrak{a}(1) = \mathfrak{a} \cdot \gcd(\mathfrak{p}, \mathfrak{b}) = \gcd(\mathfrak{a}\mathfrak{p}, \mathfrak{a}\mathfrak{b})$$

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

Essentially the unique factorization result now follows from this as in the case of the analogous result for the rational integers. However we also need the following.

Theorem 0.7.7. *Each ideal \mathfrak{i} has only finitely many ideal factors.*

Proof: Suppose $\mathfrak{a} = (\alpha_1, \alpha_2, \dots, \alpha_k)$ is a factor of \mathfrak{i} and that i is any 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 $\omega_1, \omega_2, \dots, \omega_n$ of the ring of integers \mathcal{O}_K

$$(43) \quad \mathfrak{a} = (a_{11}\omega_1 + a_{12}\omega_2 + \dots + a_{1n}\omega_n, \dots, a_{k1}\omega_1 + a_{k2}\omega_2 + \dots + a_{kn}\omega_n)$$

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

$$(44) \quad \mathfrak{a} = (a'_{11}\omega_1 + a'_{12}\omega_2 + \dots + a'_{1n}\omega_n, \dots, a'_{k1}\omega_1 + a'_{k2}\omega_2 + \dots + a'_{kn}\omega_n, n)$$

with $a_{ij} \in \{0, 1, \dots, n-1\} \forall i, j$. But there are only finitely many such ideals, and we are done. \square

So we finally have the result

Theorem 0.7.8. *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 0.7.9. *For any given non-zero ideals $\mathfrak{a}, \mathfrak{b}$ there exists an integer ω such that $(\omega, \mathfrak{a}\mathfrak{b}) = \mathfrak{a}$. I.e: there exists an integer ω which is divisible by \mathfrak{a} but coprime with \mathfrak{b} .*

By letting \mathfrak{b} be the ideal of theorem (0.7.2) with $\mathfrak{a}\mathfrak{b} = (\beta)$ we obtain the following special case of this result.

Theorem 0.7.10. *Every ideal \mathfrak{a} has a representation $\mathfrak{a} = (\omega, \beta)$ for two integers ω and β .*

0.8. 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

$$(45) \quad \mathcal{N}((\alpha)) = |\mathcal{N}(\alpha)|.$$

Definition 0.8.1. *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 .

Definition 0.8.2. *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 0.8.3. *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.*

If $\mathfrak{a} = (\alpha_1, \alpha_2, \dots, \alpha_n)$ with the α_i a \mathbb{Z} -basis of \mathfrak{a} and $\alpha_i = a_{i1}\omega_1 + a_{i2}\omega_2 + \dots + a_{in}\omega_n$; $a_{ij} \in \mathbb{Z}$ the expression for α_i in terms of a \mathbb{Z} -basis ω_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 .

Note: it is clear from this that the norm of an ideal is always finite.

By choosing the ω_i to be a canonical basis of \mathcal{O}_K , the definition of a discriminant leads directly to

Theorem 0.8.4. *If $\alpha_1, \alpha_2, \dots, \alpha_n$ is a \mathbb{Z} -basis for \mathfrak{a} then*

$$(46) \quad \mathcal{N}(\mathfrak{a}) = \left| \sqrt{\frac{\Delta(\alpha_1, \alpha_2, \dots, \alpha_n)}{\mathcal{D}_K}} \right|.$$

We now see that this definition of the norm of an ideal is compatible with equation (45). For, a basis of a principal ideal (α) is given by $\alpha\omega_1, \alpha\omega_2, \dots, \alpha\omega_n$. From the definition of a discriminant it is also clear that

$$(47) \quad \Delta(\alpha\omega_1, \alpha\omega_2, \dots, \alpha\omega_n) = \mathcal{N}(\alpha)^2 \Delta(\omega_1, \omega_2, \dots, \omega_n).$$

Thus equation (45) holds by the theorem.

Theorem 0.8.5. *For any two ideals $\mathfrak{a}, \mathfrak{b}$ we have*

$$(48) \quad \mathcal{N}(\mathfrak{a}\mathfrak{b}) = \mathcal{N}(\mathfrak{a})\mathcal{N}(\mathfrak{b}).$$

Proof: From theorem (0.7.9) 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 $\mathfrak{a}\mathfrak{b}$. \square

Theorem 0.8.6. *For \mathfrak{p} a prime ideal*

$$(49) \quad \mathcal{N}(\mathfrak{p}) = p^f$$

for some rational prime p and rational integer f .

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: $(p) = \mathfrak{p}\mathfrak{a}$ for some ideal \mathfrak{a} . Thus $p^n = \mathcal{N}(\mathfrak{p})\mathcal{N}(\mathfrak{a})$. Thus $\mathcal{N}(\mathfrak{p}) = p^f$ with $f \leq n$. \square

Furthermore we have

Theorem 0.8.7. *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 $r \leq n$. \square

0.9. 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.

Definition 0.9.1. *A fractional ideal is a set of elements of K*

$$(50) \quad \mathfrak{g} = (\rho_1, \rho_2, \dots, \rho_r) = \{\gamma_1\rho_1 + \gamma_2\rho_2 + \dots + \gamma_r\rho_r : \gamma_i \in \mathcal{O}_K\}$$

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

According to the remarks after theorem (0.4.9) 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 (0.6.8) 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 (0.7.2).

Theorem 0.9.2. *For any fractional ideal \mathfrak{a} , there is an integral ideal \mathfrak{b} such that $\mathfrak{a}\mathfrak{b}$ is principal (and indeed integral).*

Theorem (0.7.3) then also follows verbatim for fractional ideals.

We now prove

Theorem 0.9.3. *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 0.9.4. *The set of fractional ideals of K is an Abelian group with respect to ideal multiplication.*

From theorem (0.9.2) it is immediate that

Theorem 0.9.5. *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.

Definition 0.9.6. *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*

$$(51) \quad \mathcal{N}(\mathfrak{g}) = \frac{\mathcal{N}(\mathfrak{a}_1)}{\mathcal{N}(\mathfrak{a}_2)}.$$

Once again theorem (0.8.5) 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 (0.8.4) 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) .

0.10. 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 ideals P .

Definition 0.10.1. *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 $\mathfrak{a}\mathfrak{c} \sim \mathfrak{b}\mathfrak{c}$, and if $\mathfrak{c} \neq 0$ the converse holds by the analogue of theorem (0.7.3) 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 0.10.2. *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 (0.8.3)), 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 $\mathfrak{a} \mid (N)$. \square

Theorem 0.10.3. *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. \square

Theorem 0.10.4. *There exists a non-zero element $a \in \mathfrak{a}$ for each non-zero integral ideal \mathfrak{a} such that*

$$(52) \quad |N_{K/\mathbb{Q}}(a)| \leq \mathcal{N}(\mathfrak{a}) \cdot \mu,$$

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

Proof: Let $\alpha_1, \alpha_2, \dots, \alpha_n$ be an integral \mathbb{Z} -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 $x_i^{(1)}, x_i^{(2)}, \dots, x_i^{(n)}$ be the conjugates of x_i , then

$$(53) \quad |\mathcal{N}_{K/\mathbb{Q}}(\mathfrak{a})| = \prod_{j=1}^n \left| \sum_{i=1}^n a_i x_i^{(j)} \right| \leq \prod_{j=1}^n k \left(\sum_{i=1}^n |x_i^{(j)}| \right) = k^n \cdot \prod_{j=1}^n \left(\sum_{i=1}^n |x_i^{(j)}| \right).$$

Note that each $|x_i^{(j)}|$ is an algebraic integer. Also each of the conjugates in K of $\mu = \prod_{j=1}^n \left(\sum_{i=1}^n |x_i^{(j)}| \right)$ 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 $|\mathcal{N}_{K/\mathbb{Q}}(\mathfrak{a})| \leq \mathcal{N}(\mathfrak{a}) \cdot \mu$ as required. \square

Theorem 0.10.5. *The class number Cl_K is finite.*

Proof: By theorem (0.10.3) there are only a finite number of non-zero ideals $\mathfrak{a}_1, \mathfrak{a}_2, \dots, \mathfrak{a}_k$ 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

νfrb^{-1} is integral. By theorem (0.10.4) 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

$$(54) \quad \mathcal{N}(b\nu^{-1}\mathfrak{b})\mathcal{N}((\nu)) = \mathcal{N}(b\mathfrak{b}) = \mathcal{N}((b))\mathcal{N}(\mathfrak{b}) \leq \mathcal{N}(\nu\mathfrak{b}^{-1})\mathcal{N}(\mathfrak{b})\mu = \mathcal{N}((\nu))\mu.$$

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

Definition 0.10.6. *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 0.10.7. *Let \mathfrak{a} be a non-zero fractional ideal of \mathcal{O}_K , then \mathfrak{a}^h is principal.*

0.11. 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 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 $\sigma_1, \sigma_2, \dots, \sigma_n$ be the embeddings of K into the complex numbers. In fact let $\sigma_1, \sigma_2, \dots, \sigma_r$ be the real embeddings and $\sigma'_1, \sigma'_2, \dots, \sigma'_s$ be the complex embeddings, each with a conjugate $\bar{\sigma}'_i$. 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

$$(55) \quad \sigma(\alpha) = (\sigma_1(\alpha), \sigma_2(\alpha), \dots, \sigma_r(\alpha), \sigma'_1(\alpha), \sigma'_2(\alpha), \dots, \sigma'_s(\alpha)).$$

Now any integral \mathbb{Z} -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 0.11.1. *Let χ be the lattice given by embedding $Eu\mathcal{O}_K$, and Λ the lattice corresponding to the integral ideal \mathfrak{a} of norm N , then*

$$(56) \quad \text{vol}(\chi) = \frac{1}{2^s} \sqrt{|\mathcal{D}_K|}$$

$$(57) \quad \text{vol}(\Lambda) = N \cdot \text{vol}(\chi).$$

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

Theorem 0.11.2. *Let Λ be a lattice in \mathbb{R}^n and A be a bounded convex symmetric subset of \mathbb{R}^n . If $\text{vol}(A) > 4 \cdot \text{vol}(\Lambda)$ then there is at least one lattice point in A .*

We prove the following lemma

Lemma 0.11.3. *Let $D_1 = \{(\alpha_1, \alpha_2, \dots, \alpha_n) \in \mathbb{R}^n : \prod_{j=1}^r |\alpha_j| \cdot \prod_{i=r+1}^{r+s} (\alpha_i^2 + \alpha_{i+s}^2) \leq 1\}$. For every symmetric, convex $D \subseteq D_1$ there is a non-zero element $a \in \mathfrak{a}$ such that*

$$(58) \quad |\mathcal{N}(a)| \leq \frac{2^{r+s}}{\text{vol}(D)} \mathcal{N}(\mathfrak{a}) \cdot \sqrt{|\mathcal{D}_K|}.$$

Proof: 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 $\rho D = \{\rho\alpha : \alpha \in D\}$, then $\text{vol}(\rho D) = \rho^n \cdot \text{vol}(D) = 2^n \cdot \text{vol}(\Lambda)$ as per the previous theorem.

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. \square

Theorem 0.11.4. *For each non-zero integral ideal \mathfrak{a} of K , there is a non-zero $a \in \mathfrak{a}$ such that*

$$(59) \quad |\mathcal{N}(a)| \leq \left(\frac{4}{\pi}\right) \frac{n!}{n^n} \sqrt{|\mathcal{D}_K|} \cdot \mathcal{N}(\mathfrak{a}).$$

Proof: Choose $D = \{(\alpha_1, \alpha_2, \dots, \alpha_n) \in \mathbb{R}^n : |\alpha_1| + \dots + |\alpha_r| + 2\sqrt{\alpha_{r+1}^2 + \alpha_{r+s+1}^2} + \dots + 2\sqrt{\alpha_{r+s}^2 + \alpha_n^2} \leq n\}$. 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. \square

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

Corollary 0.11.5.

$$(60) \quad |\mathcal{D}_K| \geq \left(\frac{\pi}{4}\right)^{2s} \left(\frac{n^n}{n!}\right)^2.$$

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.

0.12. The Unit Group. We now apply the methods of Minkowski to the group of units U , i.e: invertible elements of \mathcal{O}_K .

This time the map we will consider is

$$(61) \quad f(\alpha) = (\log|\sigma_1(\alpha)|, \dots, \log|\sigma_r(\alpha)|, \log(|\sigma_{r+1}(\alpha)|^2), \dots, \log(|\sigma_{r+s}(\alpha)|^2))$$

for any $\alpha \in \mathcal{O}_K$. This time we have mapped the non-zero integers into \mathbb{R}^{r+s} . This map f induces a homomorphism g of the units group U into \mathbb{R}^{r+s} .

We firstly prove that

Theorem 0.12.1. *The unit group U is a finitely generated Abelian group of rank $r + s - 1$.*

We firstly prove that the kernel of g is finite. Indeed for any bounded subset $Z \subset \mathbb{R}^{r+s}$ the preimage $g^{-1}(Z)$ is finite. For, Z bounded means that for all $g(u) \in Z$ 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 g is a finite subgroup of \mathcal{O}_K . In particular it is a finite subgroup of the multiplication group K^\times of the field K . By a well known theorem 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, $m \cdot g(z) = g(z^m) = g(1) = 0$ so that $g(z) = 0$ (recall it is a vector in \mathbb{R}^{r+s}). Thus it is clear that this kernel actually consists of these 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

$$(62) \quad \log|\sigma_1(u)| + \dots + \log|\sigma_r(u)| + \log(|\sigma_{r+1}(u)|^2) + \dots + \log(|\sigma_{r+s}(u)|^2) = 0.$$

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

As per the above argument, for any bounded $Z \subset \mathbb{R}^{r+s}$ the preimage $g^{-1}(Z)$ is a finite subset of U . I.e: $g(U) \cap Z$ is a finite set. Thus $g(U)$ is a discrete subgroup of \mathbb{R}^{r+s} , and in fact of the hyperplane H . Thus it has a \mathbb{Z} -basis y_i consisting of $m \leq r + s - 1$ vectors.

Thus we have that if U_1 is the subgroup of the units generated by a set of representatives $\{z_i\}$ such that $g(z_i) = y_i$, then $U/\ker g \cong g(U)$ where $T = \ker g$ is the so-called torsion part. Also we have that $U = TU_1$ and $T \cap U_1 = \{1\}$ and thus $U = T \times U_1$, the direct product.

We now use Minkowski's theorem to show that there are exactly $r + s - 1$ independent vectors.

Consider the region defined by some $a \in \mathcal{O}_K$, i.e: those points of \mathbb{R}^{r+s} , $(\beta_1, \beta_2, \dots, \beta_{r+s})$, with $\beta_i < \alpha_i$ for all $i \neq k$, where $f(a) = (\alpha_1, \alpha_2, \dots, \alpha_{r+s})$. It is an unbounded region since β_k can be anything for the distinguished k .

Now considering the points $f(b) = (\beta_1, \beta_2, \dots, \beta_{r+s})$ satisfying this condition, adding the extra condition that $|\mathcal{N}(b)| \leq c$ bounds the region

we are considering. For c large enough the volume is great enough that there is, for each $1 \leq k \leq r + s$, some $b = h_k(a) \in \mathcal{O}_K \setminus \{0\}$ satisfying these conditions. We can even make the bound c uniform for all $1 \leq k \leq r + s$.

For each particular k we construct a sequence a_i . Let $a_1 = a$ and let $a_j = h_k(a_j - 1) \in \mathcal{O}_K$ for all $j \geq 2$. Since the norms $|\mathcal{N}(a_j)| \leq c$ are bounded, there are only finitely many ideals (a_j) . Thus $(a_j) = (a_k)$ for some $j < k$. Then $u_k = a_k a_j^{-1}$ is a unit such that the i -th coordinate of $g(u_k) = f(a_k) - f(a_j) = (\alpha_1^{(k)}, \dots, \alpha_l^{(k)})$ is negative for $i \neq k$. Thus $\alpha_k^{(k)}$ is positive since $\sum_i \alpha_i^{(k)} = 0$. We thus have $r + s$ units u_i , each with this property for a different k . We claim that the first $r + s - 1$ of them are linearly independent. We check that the first $r + s - 1$ rows of the matrix $(\alpha_i^{(k)})$ are linearly independent.

If this were not the case, there would be a non-zero vector $(t_1, t_2, \dots, t_{r+s-1})$ such that $\sum_{k=1}^{r+s-1} t_k \alpha_i^{(k)} = 0$ for all $1 \leq i \leq r + s$, since the matrix would be singular.

Without loss of generality assume $t_i = 1$ and $t_j \leq 1$ for the others (simply reorder and scale). Then $t_i \alpha_i^{(i)} = \alpha_i^{(i)}$ and for the others, $t_j \alpha_i^{(j)} \geq \alpha_i^{(j)}$ since $\alpha_i^{(j)} < 0$ by construction. Thus

$$(63) \quad 0 = \sum_{k=1}^{r+s-1} t_k \alpha_i^{(k)} \geq \sum_{k=1}^{r+s-1} \alpha_i^{(k)} > \sum_{k=1}^{r+s} \alpha_i^{(k)} = 0$$

a contradiction. Thus the rank is $r + s - 1$.

□

E-mail address: whart@maths.mq.edu.au