ALGEBRAIC NUMBER THEORY

RAGHAVAN NARASIMHAN

S. RAGHAVAN

S. S. RANGACHARI

SUNDER LAL

Tata Institute of Fundamental Research, Bombay

School of Mathematics

Tata Institute of Fundamental Research, Bombay

1966

PREFACE

THIS pamphlet contains the notes of lectures given at a Summer School on the Theory of Numbers at the Tata Institute of Fundamental Research in 1965. The audience consisted of teachers and students from Indian Universities who desired to have a general knowledge of the subject. The speakers were Raghavan Narasimhan, S. Raghavan, S. S. Rangachari and Sunder Lal.

Chapter 1 sets out the necessary preliminaries from set theory and algebra; it also contains some elementary number-theoretic material. Chapter 2 deals with general properties of algebraic number fields; it includes proofs of the unique factorization theorem for ideals, the finiteness of class number, and Dirichlet's theorem on units. Chapter 3 gives a slightly more detailed analysis of quadratic fields, in particular from the analytic aspect; the course ends with Dirichlet's theorem on the infinitude of primes in an arithmetic progression.

Contents

Chapter 1

Preliminaries

1.1 Sets and maps

A set is a collection of objects which are called the *elements* of the set. We shall suppose that if any object is given, we can decide whether it belongs to the set or not. The set of all rational integers (i.e. integers positive, negative and zero) is denoted by $\mathbf{Z}$, the set of all non-negative integers by $\mathbf{Z}^+$, the set of all rational numbers by $\mathbf{Q}$, the set of all real numbers by $\mathbf{R}$, and the set of all complex numbers by $\mathbf{C}$.

If x is an element of a set A, we write $x \in A$. If x is not an element of A, we write $x \notin A$. If P is a property, the set of all objects with the property P will be denoted by $\{x \mid x \text{ possesses the property } P\}$. Thus $\{x \mid x \in \mathbf{Z}, x < 0\}$ is the set of all negative integers. The set which does not contain any element is called the *empty set* and is denoted by the symbol $\emptyset$.

Let X and Y be two sets. If every element of X is an element of Y, we say that X is a *subset* of Y (or X is *contained in* Y) and write $X \subset Y$ or $Y \supset X$. If $X \subset Y, X \neq Y$, we say that X is *properly contained in* Y. It is clear that if $X \subset Y$ and $Y \subset X$, then $X = Y$. If X and Y are two sets, we define

(i) the *union* $X \cup Y$ of X and Y as the set

$$\{z \mid z \in X \text{ or } z \in Y\};$$

(ii) the *intersection* $X \cap Y$ of X and Y as the set

$$\{z \mid z \in X \text{ and } z \in Y\};$$

(iii) the *cartesian product* $X \times Y$ of X and Y as

$$\{(x, y) \mid x \in X \text{ and } y \in Y\}.$$

We say X and Y are *disjoint* if $X \cap Y = \emptyset$. If $X \subset Y$, we define the complement, $Y - X$, as the set $\{z \mid z \in Y \text{ and } z \notin X\}$.

1.2 Maps

Let X and Y be two sets. A *map* $f: X \to Y$ is an assignment to each $x \in X$, of an element $f(x) \in Y$. If A is a subset of X, the *image* $f(A)$ is the set $\{f(x) \mid x \in A\}$. The *inverse image* of a subset B of Y, denoted by $f^{-1}(B)$, is the set $\{x \mid x \in X, f(x) \in B\}$. The map f is said to be *onto* or surjective, if $f(X) = Y$; if $f(x) = f(y)$ implies $x = y$, then f is said to be *one-one* or *injective*. If $f: X \to Y, g: Y \to Z$ are two maps, we define the *composite* $(g \circ f): X \to Z$ as follows: for $x \in X, (g \circ f)(x) = g(f(x))$. The map $X \to X$*which associates* to each $x \in X$, the element x itself called the *identity map* of X and denoted by I_X (or by I, if there is no confusion). If $f: X \to Y$ is both one-one and onto, there is a map from $Y \to X$, denoted by f^{-1}, such that $f \circ f^{-1} = I_Y, f^{-1} \circ f = I_X$. The map f^{-1} is called the *inverse* of f. If A is a subset of X, the map $j = j_A: A \to X$ which associates to each $a \in A$ the same element a in X is called the *inclusion map* of A in X. If $f: X \to Y$ is any map, the map $f \circ j_A: A \to Y$ is called the *restriction* of f to A and is denoted by $f \mid A$.

1.3 Equivalence Relations

Definition 1.1 *Let X be a set. An equivalence relation in X is subset R of $X \times X$ such that*

(i) for every $x \in X, (x, x) \in R$;

(ii) if $(x, y) \in R$, then $(y, x) \in R$; and

(iii) if $(x, y) \in R$ and $(y, z) \in R$ then $(x, z) \in R$.

We say that x is equivalent to y with respect to R and write xRy if $(x, y) \in R$. Then the conditions above simply require that

(i) every element x is equivalent to itself (*reflexivity*),

(ii) if x is equivalent to y, y is equivalent to x (*symmetry*), and

(iii) if x is equivalent to y and y to z then x is equivalent to z. (*transitivity*).

Let R be an equivalence relation in a set X. Then for any $x \in X$, the set of all elements of X equivalent to x with respect to R is called the *equivalence class of* R containing x and is denoted by $\bar{x}$. Consider the family of distinct equivalence classes of X with respect to R. It is easy to verify that they are pairwise disjoint and that their union is X. The set of these equivalence classes x is called the *quotient* of X by R and is denoted by X/R.

Example 1.1 *The subset $R \subset X \times X$ consisting of elements (x, x), $x \in X$ is an equivalence relation. This is called the identity relation.*

Example 1.2 *Let $n \in \mathbf{Z},\ n > 0$. Consider the set in $\mathbf{Z} \times \mathbf{Z}$ of pairs of integers (a, b) such $a - b$ is divisible by n. This is an equivalence relation in $\mathbf{Z}$ and the quotient of $\mathbf{Z}$ by this relation is denoted by $\mathbf{Z}/(n)$ or $\mathbf{Z}_n$.*

1.4 Abelian groups and homomorphisms

Definition 1.2 *Let G be a nonempty set and $\psi: G \times G \to G$ a mapping. Let, for $x, y \in G,\ \psi((x, y))$ be denoted by $x \cdot y$ or xy. Then the pair (G, ψ) is said to be an abelian group if the following conditions are satisfied:*

(a) $x(yz) = (xy)z$ for every x, y, z in G(associativity),

(b) there exists an element e, called the identity element of G, which satisfies $ex = xe = x$ for every x in G.

(c) for every $x \in G$, there exists in G an element x^{-1}, called the inverse of x, such that $xx^{-1} = x^{-1}x = e$, and

(d) for every $x, y \in G,\ xy = yx$ (commutativity).

Remark 1.1 *We often abbreviate (G, ψ) to G when it is clear from the context to which map ψ we are referring.*

Remark 1.2 *The map ψ is called the composition law in G. It is also called the multiplication in G.*

Remark 1.3 *The identity element is unique. In fact, if there is an element e' in G such that condition (b) above is valid for every x in G with e replaced by e', we have, in particular, $e = ee' = e'$.*

Remark 1.4 *The inverse of any element is unique.*

Remark 1.5 *In view of associativity, we define $xyz = (xy)z = x(yz)$ for every x, y, z in G.*

More generally, the product $x_1x_2\cdots x_n$ is well defined, where $x_1, x_2, \ldots, x_n \in G$. (Proof by induction). In particular, for any $x \in G$, we set

$$\begin{aligned} x^m &= xx\cdots x \ (m \text{ times}) \text{ for } m > 0 \text{ in } \mathbf{Z}, \\ x^0 &= e, \\ x^n &= (x^{-1})^{-n} \text{ for } n < 0 \text{ in } \mathbf{Z}. \end{aligned}$$

It is also customary to write the composition law in an abelian group additively, i.e. to write $x + y$ for what has been denoted by $x \cdot y$ above. In this case, one writes 0 for e, $-x$ for x^{-1}, mx for x^m, and refers to the composition law as addition.

Definition 1.3 *An abelian group G is said to be finite if it consists of only finitely many elements; the number of elements of a finite group is referred to as its order. We say G is infinite if it is not finite.*

Example 1.3 *The set $\mathbf{Z}\,(\mathbf{Q}, \mathbf{R}, \mathbf{C})$ of integers (rational numbers, real numbers, complex numbers respectively) with the 'usual' addition as composition law is an abelian group.*

Example 1.4 *The set $\mathbf{Z}/(n)$ in Example 1.2 on page 3 can be seen to be an abelian group with addition $(+)$ defined by $\bar{x} + \bar{y} = \overline{x + y}$ for $x, y \in \mathbf{Z}$. The order of $\mathbf{Z}/(n)$ is n as follows at once from the fact that for any $a \in \mathbf{Z}$, there is a unique b with $0 \leq b < n$ for which $a - b$ is divisible by n.*

Example 1.5 *Let $\mathbf{Q}^*(\mathbf{R}^*, \mathbf{C}^*)$ denote the set of non-zero rational (real, complex) numbers. With the 'usual' multiplication for composition law, these from abelian groups.*

In what follows, we shall often drop the adjective *abelian* and speak simply of *groups* where we mean abelian groups.

Definition 1.4 *Let G, G' be two groups. A homomorphism f from G to G' is a map $f: G \to G'$ such that $f(xy) = f(x)f(y)$ for every $x, y \in G$.*

Let $f: G \to G'$ be a homomorphism. Then $f(e) = e$. In fact, $f(e) = f(ee) = f(e)f(e)$ and multiplying both sides by $f(e)^{-1}$, we get $f(e) = e$ If $f: G \to G'$ and $g: G' \to G''$ are homomorphisms, then $g \circ f: G \to G''$ is also a homomorphism. For any group G, the identity map $I_G: G \to G$ is a homomorphism.

Definition 1.5 *A homomorphism $f: G \to G'$ is called an isomorphism if there exists a homomorphism $g: G' \to G$ such that $f \circ g = I_{G'}$ (the identity map of G') and $g \circ f = I_G$(the identity map of G).*

It is easy to see that a homomorphism $f: G \to G'$ is an isomorphism if and only if it is both injective and surjective.

Example 1.6 *The natural map $\eta: \mathbf{Z} \to \mathbf{Z}/(n)$ is a surjective homomorphism. For $n \neq 0$ it is not one-one and hence not an isomorphism.*

Example 1.7 *The map $f: \mathbf{Z} \to \mathbf{Z}$ given by $f(a) = 2a$ for $a \in \mathbf{Z}$ is an injective homomorphism. It is not onto and hence not an isomorphism.*

Example 1.8 *The map $g: \mathbf{Q}^* \to \mathbf{Q}^*$ given by $g(x) = 1/x$ for $x \in \mathbf{Q}^*$ is an isomorphism. Further $g \circ g = I_{\mathbf{Q}^*}$.*

Definition 1.6 *Let G be a group. A non-empty subset H of G is called a subgroup of G if for every x, y in H, xy^{-1} also belongs to H.*

In particular $e \in H$ and for any $x \in H$, $x^{-1} \in H$. It can be easily checked that with the 'composition' induced by that of G, H is a group with e as the identity element and x^{-1} as the inverse of x in H.

Let H be a subgroup of G. Then the inclusion map $j: H \to G$ is an injective homomorphism.

For any group G, the subsets $\{e\}$ and G are subgroups of G. Let G_1, G_2 be two groups and $f: G_1 \to G_2$, homomorphism of G_1 into G_2. Then the set of $x \in G_1$, for which $f(x) = e$ is easily verified to be a subgroup of G_1. It is called the *kernel* of f and is denoted by $\ker f$. The homomorphism f is an isomorphism if f is onto and $\ker f = \{e\}$.

Let G be a group and H a subgroup of G. The relation "$x \sim y$ $(x, y \in G)$ if and only if $xy^{-1} \in H$" is an equivalence relation. If $\bar{x}$ is the equivalence class containing x, then, on the set of equivalence classes we can introduce the structure of a group by setting $\bar{x}\bar{y} = \overline{xy}$. These classes are called *cosets of G modulo H*. This group is denoted by G/H and is

called the *quotient of G by H*. If G/H is finite, then its order is called the index of H in G. There is natural mapping of G onto G/H taking $x \in G$ to $\bar{x}$ and this mapping is a surjective homomorphism with kernel H.

Let $f: G_1 \to G_2$ be a homomorphism of a group G_1 into a group G_2 with $\ker f = H$. The image $f(G_1)$ of G_1 under f is a subgroup of G_2 and we define a homomorphism $\bar{f}: G_1/H \to f(G_1)$ by setting $f(\bar{x}) = f(x)$ for $x \in G_1$. Clearly f is an isomorphism of G_1/H onto $f(G_1)$ (*fundamental theorem of homomorphisms).*

Let G be a group and $a \in G$ such that every element of G is of the form a^n, where $n \in \mathbf{Z}$. Then we say that G is a *cyclic group generated by a.*

Example 1.9 *$(\mathbf{Z}, +)$ is an infinite cyclic group generated by the integer 1. The only subgroups of $\mathbf{Z}$ are of the form $m\mathbf{Z} = \{mx \mid x \in \mathbf{Z}\}$ for $m \geq 0$.*

Proposition 1.1 *Any cyclic group G is isomorphic to $\mathbf{Z}$ or $\mathbf{Z}/(m)$ for some $(m > 0)$.*

PROOF: Let G be generated by a. Consider the map $f: \mathbf{Z} \to G$ taking $n \in \mathbf{Z}$ to a^n. This is a surjective homomorphism and $\ker f$ is a subgroup $m\mathbf{Z}$ of $\mathbf{Z}$ generated by $m \geq 0$ in $\mathbf{Z}$. If $m = 0, G$ is isomorphic to $\mathbf{Z}$. If $m \geq 0,\ G$ is isomorphic to $\mathbf{Z}/(m)$.

Definition 1.7 *Let G be a group and $a \in G$. We say that a is of order n if the cyclic group generated by a in G is of order n.*

Example 1.10 *The element -1 in $\mathbf{Q}^*$ is of order 2.*

Remark 1.6 *If G is a group of order h and an element $a \in G$ is of order n, then n divides h and therefore $a^h = e$.*

1.5 Rings, modules and vector spaces.

Definition 1.8 *Let R be a nonempty set and let ϕ, ψ be mappings of $R \times R$ into R. Writing $\phi((x, y)) = x + y,\ \psi((x, y)) = xy$, the triple (R, ϕ, ψ) is said to be a ring if the following conditions are satisfied:*

(i) (R, ϕ) is an abelian group,

(ii) $x(yz) = (xy)z$ *for* x, y, z *in* R *(associativity).*

(iii) $x(y+z) = xy + xz,\ (y+z)x = yx + zx$ *in* R *(distributivity), and*

(iv) there exists in R *an element 1, called the unit element of* R*, such that* $x1 = 1x = x$ *for every* x *in* R*.*

Remark 1.7 *We call* ϕ *and* ψ *respectively the addition and the multiplication in* R*; we write* $+$ *for* ϕ *and* $\cdot$ *or* $\times$ *for* ψ*.*

Remark 1.8 *The identity element of* (R, ϕ) *is called the zero element of* R *and is denoted by* 0*.*

Remark 1.9 *The unit element in* R *is unique.*

Remark 1.10 *Associativity is valid for any finite number of elements in* R *(in a sense which is obvious).*

Remark 1.11 *We denote by* R^* *the set of non-zero elements of* R*.*

Definition 1.9 *A ring* R *is commutative if* $xy = yx$ *for every* x, y *in* R*.*

Hereafter, by a ring we shall always mean a commutative ring.

Definition 1.10 *A subring* S *of a ring* R *is a subgroup of* $(R, +)$ *such that* $1 \in S$ *and for* $x, y \in S,\ xy \in S$*.*

We observe that S is a ring under the operations induced from R.

If R is a ring, S a subring and E a subset of R, the ring $S[E]$ generated by E is the set consisting of 1 and all the elements of the form $\alpha = \sum_{i=1}^{n} s_i e_i,\ s_i \in S$ where each e_i is a product of finitely many elements of E. It is trivial that $S[E]$ is the smallest subring of R containing S and E.

Definition 1.11 *Let* R *be a ring and* $a, b \in R$*. Then we say that* a *divides* b *(or that* a *is a divisor of* b*,* $a|b$ *in symbols), if there exists* c *in* R *such that* $b = ac$*. If* a *does not divide* b*, we write* $a \nmid b$*.*

Definition 1.12 *If* $a, b, c \in R$*, then* a *is congruent to* b *modulo* c *(in symbols* $a \equiv b \pmod{c}$*) if* $c|(a-b)$*.*

Definition 1.13 *An element $a \in R$ is called a zero-divisor if there exists $x \neq 0$ in R such that $ax = 0$. Trivially, 0 is a zero-divisor.*

Definition 1.14 *A commutative ring R in which $1 \neq 0$, is an integral domain if R contains no zero-divisors other than 0.*

Definition 1.15 *An element $u \in R$ is called a unit in R if there exists $v \in R$ such that $uv = 1$. (R is commutative).*

The units u in R clearly form a multiplicative group which we denote by U.

Definition 1.16 *We call two elements a, b in R associates with respect to U if $a = ub$ for some $u \in U$. We say, briefly, that a and b are associates and otherwise we say that a and b are non-associate.*

Definition 1.17 *A commutative ring R is called a field, if the set R^* of elements $a \neq 0$ in R forms a group under multiplication (i.e. if every $a \neq 0$ in R is a unit). Clearly a field is an integral domain.*

Definition 1.18 *A subring R of a field K is called a subfield of K, if R is a field (with respect to the operations which make R a ring viz. the operations induced from K).*

Example 1.11 $\mathbf{Z}, \mathbf{Q}, \mathbf{R}$, *and* $\mathbf{C}$ *are commutative rings with the usual addition and multiplication of complex numbers, and, in fact, integral domains.* $\mathbf{C}, \mathbf{R}, \mathbf{Q}$ *are fields and* $\mathbf{Q}, \mathbf{R}$ *are subfields of* $\mathbf{C}$*; however,* $\mathbf{Z}$ *is not a field.*

Example 1.12 *The additive group $\mathbf{Z}/(m)$ consisting of residue classes (of $\mathbf{Z}$) modulo (an integer) $m(\neq 0)$ is a ring, the multiplication being defined by $\bar{r}\bar{s} = \overline{rs}$ for $r,\ s \in \mathbf{Z}$.*

Example 1.13 *A finite integral domain A is a field. In fact, let $A = \{x_1, x_2, \ldots, x_h\}$, and let $a \in A,\ a \neq 0$. Then the elements $ax_1, \ldots, ax_h$ are distinct, since A has no non-zero zero-divisors. Hence they must be all the x_i in some order, so that $ax_i = 1$ for some i.*

Definition 1.19 *A positive integer p in $\mathbf{Z}$ is called a prime if $p > 1$ and its only divisors in $\mathbf{Z}$ are $\pm 1,\ \pm p$.*

Proposition 1.2 *For $p > 0$ in $\mathbf{Z}$, $\mathbf{Z}/(p)$ is a field if and only if p is a prime.*

PROOF: In fact, if $p = rs,\ r, s \neq \pm 1$, then $\bar{r}\bar{s} = \bar{0}$. But neither $\bar{r}$ nor $\bar{s}$ is equal to $\bar{0}$. Hence $\mathbf{Z}/(p)$ is not even an integral domain, if p is not a prime. Conversely, if p is a prime, then for any $x \in \mathbf{Z}$ with $p \nmid x$, there exists $y \in \mathbf{Z}$ such that $xy \equiv 1(\text{mod p})$. For, consider the set of $r \in \mathbf{Z}$ such that $rx \equiv 0(\text{mod p})$. This is an additive subgroup G of $\mathbf{Z}$ and hence, by the example 1.9 on page 6, of the form $m\mathbf{Z},\ m \geq 0$. Since $p \in G,\ m = 1$ or p. But $m \neq 1$, since $p \nmid x$. Thus $m = p$ and as a consequence, the elements,

$$0, x, 2x, \ldots, (p-1)x$$

. are all distinct modulo p. Since the order of $\mathbf{Z}/(p)$ is p (see Example 1.4 page 4) there exists $y \in \mathbf{Z}\,(1 \leq y \leq p-1)$ such that $\overline{yx} = \bar{1}$, i.e. $yx \equiv 1(\text{ mod } p)$. [The last part of the argument is that of Example 1.13 above].

1.6 The Legendre symbol

Definition 1.20 *Let $p \in \mathbf{Z},\ p > 2$ be a prime. An integer a with $p \nmid a$ is said to be a quadratic residue modulo p, if there exists $x \in \mathbf{Z}$ such that $x^2 \equiv a(\text{ mod } p)$, and a quadratic non-residue modulo p if no such x exists in $\mathbf{Z}$.*

From the definition, it is clear that a is a quadratic residue modulo p if and only if $a + mp$ (for arbitrary $m \in \mathbf{Z}$) is so. We can thus talk of a (non-zero) residue class modulo p being quadratic residue or non-residue modulo p.

Consider now, for $p \nmid a$, the quadratic congruence $x^2 \equiv a(\text{ mod } p)$ for $x \in \mathbf{Z}$. If a is a quadratic non-residue modulo p, this congruence has no solution x. If a is a quadratic residue modulo p, say $a \equiv b^2(\text{ mod } p)$, then $x^2 \equiv b^2(\text{ mod } p)$, i.e. $(x-b)(x+b) \equiv 0(\text{ mod } p)$. Since by Proposition 1.2 $\mathbf{Z}/(p)$ is an integral domain, it follows that $x \equiv \pm b(\text{ mod } p)$ are the only two solutions of the congruence $x^2 \equiv a(\text{ mod } p)$. Further, since $p > 2,\ b \not\equiv -b(\text{ mod } p)$. Now consider the mapping $\bar{x} \to \bar{x}^2$ of $(\mathbf{Z}/(p))^*$ into itself. The image of $\bar{x}\ (\neq 0)$ under this mapping is always a quadratic residue modulo p and by what we have seen, each quadratic residue modulo p in $(\mathbf{Z}/(p))^*$ is the image of exactly two elements of $(\mathbf{Z}/(p))^*$

under this mapping. Thus there are $(p-1)/2$ quadratic residues modulo p. It follows that there are $(p-1)/2$ quadratic non-residues modulo p.

The product of two quadratic residues modulo p is again a residue. For, if $a \equiv x^2 (\bmod p)$ and $b \equiv y^2 (\bmod p)$ then $ab \equiv (xy)^2 (\bmod p)$.

The product of a quadratic residue a modulo p and a non-residue b modulo p is a quadratic non-residue modulo p. For, there exists $x \in \mathbf{Z}$ for which $x^2 \equiv a (\bmod p)$ and if $ab \equiv z^2 (\bmod p)$ for $z \in \mathbf{Z}$ choose by Proposition 1.2, $y \in \mathbf{Z}$ such that $xy \equiv 1 (\bmod p)$. Clearly we have then the congruence $b \equiv (yz)^2 (\bmod p)$, and b would be a residue modulo p.

The product of two quadratic non-residues a, b modulo p is a quadratic residue modulo p. For let $\bar{a}_1, \ldots, \bar{a}_q (q = \frac{1}{2}(p-1))$, be the quadratic residues modulo p. Then since $\mathbf{Z}/(p)$ is an integral domain, it follows from what we have seen above that $\overline{aa}_1, \ldots, \overline{aa}_q$ are precisely all the residue classes modulo p which are non-residues. Since ab is distinct from these, it must be a residue.

Definition 1.21 *Let $p \neq 2$ be a prime and $a \in \mathbf{Z}$. We define the Legendre symbol $(\frac{a}{p})$ by*

$$\left(\frac{a}{p}\right) = \begin{cases} +1 \text{ if } p \nmid a \text{ and } a \text{ is a quadratic residue modulo } p \\ -1 \text{ if } p \nmid a \text{ and } a \textit{ is a non-residue modulo } p, \\ 0 \text{ if } p \mid a. \end{cases}$$

It is clear from the earlier considerations that

$$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right) \quad \text{for } a, b \in \mathbf{Z} \tag{1.1}$$

1.7 The quotient field of an integral domain

Definition 1.22 *Let R, R' be two rings. A map $f: R \to R'$ is called a homomorphism if*

(i) $f(x+y) = f(x) + f(y)$,

(ii) $f(xy) = f(x)f(y)$ *for every* $x, y \in R$, *and*

(iii) $f(1) = 1$.

For any ring R, the identity map I_R is a homomorphism. The composite of two homomorphisms is again a homomorphism.

Definition 1.23 *A homomorphism $f: R \to R'$ is said to be an isomorphism if there exists a homomorphism $g: R' \to R$ such that $g \circ f = I_R$ and $f \circ g = I_{R'}$. The rings R and R' are then said to be isomorphic and we write $R \simeq R'$.*

An isomorphism $f: R \to R$ is called an automorphism of R. The image $f(R)$ of a ring R under a homomorphism $f: R \to R'$ is a subring of R'. A homomorphism is an isomorphism if and only if it is injective and surjective.

Remark 1.12 *The natural map $q: \mathbf{Z} \to \mathbf{Z}/(m)$ is a homomorphism.*

Proposition 1.3 *Every integral domain R can be embedded isomorphically in a field.*

PROOF: Let R be an integral domain and R^* the set of non-zero elements of R. On $R \times R^*$, we define the relation: $(a, b) \sim (c, d)$ if $ad = bc$. Since R contains no zero-divisors, it can be verified that this is an equivalence relation. We make the quotient $K = R \times R^* / \sim$ a ring by defining the ring operations as follows. If x/y denotes the equivalence class containing $(x, y) \in R \times R^*$ then define $a/b + c/d = (ad + bc)/bd$ and $(a/b)(c/d) = ac/bd$. These operations are well defined and K is a ring. In fact, K is a field, since b/a is an inverse for a/b, $a \neq 0$. The map $i: R \to K$ given only by $i(a) = a/1$ for $a \in R$ is a one-one homomorphism of R into K.

We shall identify R with the subring $i(R)$ of K.

Remark 1.13 *K is called the quotient field of R. If $f: R \to L$ is a one-one homomorphism of R into a field L, then f can be extended in a unique way to a one-one homomorphism $\bar{f}$ of K into L, by prescribing $\bar{f}(a/b) = f(a)f(b)^{-1}$, for $b \neq 0$. Further, this property characterises the quotient field upto isomorphism. Thus L contains the isomorphic image $\bar{f}(K)$ of K. We see then that if L contains an isomorphic image of K and in this sense, K is the "smallest" field containing R.*

Example 1.14 **Q** *is (isomorphic to) the quotient field of* $\mathbf{Z}$.

1.8 Modules

Let R be a (commutative) ring (containing 1)

Definition 1.24 *An R-module M is a triple $(M, +, \psi)$ where*

(i) $(M, +)$ *is an (abelian) group*

(ii) $\psi\colon R \times M \to M$ *is a map such that if we set*

$$\psi((\lambda, a)) = \lambda a, \text{ then for } \lambda,\ \mu \in R,\ \text{and } x, y \in M,\ \text{we have}$$

(1) $\lambda(x + y) = \lambda x + \lambda y$,

(2) $(\lambda + \mu)x = \lambda x + \mu x$

(3) $(\lambda\mu)x = \lambda(\mu x)$,

(4) $1 \cdot x = x$.

The elements of R are called scalars and ψ is called scalar multiplication.

Definition 1.25 *If R is a field, M is called a vector space over R (or an R-vector space) and the elements of R called vectors.*

Example 1.15 *Every (abelian) group $(G, +)$ can be regarded as a $\mathbf{Z}$-module $(G, +, \psi)$ by defining $\psi((n, x)) = nx$ for $x \in G$ and $n \in \mathbf{Z}$. Conversely, every $\mathbf{Z}$-module is of this type.*

Example 1.16 *Every (commutative) ring R with 1 is an R-module.*

Example 1.17 $\mathbf{R}$ *and* $\mathbf{C}$ *are vector spaces over* $\mathbf{Q}$.

Definition 1.26 *Let M be an R-module (resp. vector space over R). Then a subgroup N of M is called an R-submodule (resp. a subspace over R) if ψ maps $R \times N$ into N.*

Definition 1.27 *Let M be an R-module. A subset S of M is said to generate M over R if every $x \in M$ can be written in the form $x = \sum_{i=1}^{n} a_i x_i$ with $x_i \in S,\ a_i \in R$ and $n = n(x) \in \mathbf{Z}^+$.*

The elements of S are called generators of M over R. In particular, if there exists a finite subset S of M over R, then M is finitely generated over R. If $S = \emptyset$, by definition, the generating M module generated by S is $\{0\}$.

Proposition 1.4 *Let $\alpha_1, \alpha_2, \ldots, \alpha_n$ be a system of generators of a $\mathbf{Z}$-module M, and let N be a sub-module of M. Then there exist $\beta_1, \ldots, \beta_m$ in $N (m \leq n)$ that generate N over $\mathbf{Z}$ and have the form $\beta_i = \sum_{i \leq j} k_{ij}\alpha_j$ with $k_{ij} \in \mathbf{Z},\ k_{ii} \geq 0$ and $1 \leq i \leq m$.*

PROOF: Let us suppose that the proposition has been proved for all $\mathbf{Z}$-modules with $n-1$ generators at most, where $n \geq 1$. (Note that the proposition is trivial when $M = \{0\}$.) Let M be a module generated over $\mathbf{Z}$ by n elements $\alpha_1, \alpha_2, \ldots, \alpha_n$ and N a sub-module of M. Define M' to be the module generated by $\alpha_2, \alpha_3, \ldots, \alpha_n$ over $\mathbf{Z}$ and N' to be $N \cap M'$. If $n = 1,\ M' = \{0\}$. If $N = N'$ the proposition is true by the induction hypothesis. If $N \neq N'$, then let A be the subgroup of $\mathbf{Z}$ consisting of integers k for which there exist $k_2, \ldots, k_n$ in $\mathbf{Z}$ with $k\alpha_1 + k_2\alpha_2 + \cdots + k_n\alpha_n \in N$. Then A is of the form $k_{11}\mathbf{Z},\ k_{11} \geq 0$; let $\beta_1 = k_{11}\alpha_1 + k_{12}\alpha_2 + \cdots + k_{1n}\alpha_n \in N$. If $\alpha = \sum_{i=1}^{n} h_i\alpha_i$, with $h_1, h_2, \ldots, h_n \in \mathbf{Z}$, belongs to N, then $h_2 \in A$ so that $h_1 = mk_{11}$ for some $m \in \mathbf{Z}$. Thus $\alpha - m\beta_1 \in N'$. By the induction hypothesis, there exist $\beta_i = \sum_{j \leq i} k_{ij}\alpha_j$ $(i = 2, 3, \ldots, m,\ k_{ij} \in \mathbf{Z},\ k_{ii} \geq 0)$, in N', which generate N'. It is clear that $\beta_1, \beta_2, \ldots, \beta_m$ are generators of N having the required form.

Definition 1.28 *A subset S of an R-module M is linearly independent over R, if, for any finite set of elements $x_1, \ldots, x_n$ in S, a relation $\sum_{i=1}^{n} a_i x_i = 0,\ a_i \in R$ implies necessarily that $a_1 = \cdots = a_n = 0$. We say that S is linearly dependent, if it is not linearly independent.*

Definition 1.29 *A subset S of M is called a base of M over R (or an R-base) if S is linearly independent and generates M over R.*

Example 1.18 *The $\mathbf{Z}$-module of even integers has $\{2\}$ for a base.*

Example 1.19 $\mathbf{Q}$ *is a $\mathbf{Z}$-module but is not finitely generated over $\mathbf{Z}$. Trivially, $\mathbf{Q}$ if finitely generated over $\mathbf{Q}$.*

Example 1.20 $\mathbf{R}^2 = \mathbf{R} \times \mathbf{R}$ *has $\{(1,0), (0,1)\}$ as a base over $\mathbf{R}$.*

Proposition 1.5 *Let V be a vector space (over a field K) which has a set of generators consisting of m elements. If S is any linearly independent subset of V, then S contains at most m elements.*

PROOF: Let $x_1, \ldots, x_m$ be a set of generators for V over K. If possible, let S contain more than m elements, say $y_1, \ldots, y_{m+1}$. We can write $y_1 = \sum_{i=1}^{m} \lambda_i x_i,\ \lambda_i \in K$ and $\lambda_i \neq 0$ for at least one i. We may assume, without loss of generality, that $\lambda_1 \neq 0$. Then $x_1 = \lambda_1^{-1} y_1 - \sum_{i=2}^{m} \lambda_1^{-1} \lambda_i x_i$. Hence $y_1, x_2, \ldots, x_m$ generate V. Assume for some $i,\ 1 \leq i \leq m$, that $(y_1, \ldots, y_i, x_{i+1}, \ldots, x_m)$ generate V. (This is true for $i = 1$.) Then

$$y_{i+1} = \sum_{j=1}^{i} \alpha_j y_j + \sum_{k=i+1}^{m} \alpha_k x_k, \quad \alpha_1, \ldots, \alpha_m \in K.$$

Since $y_1, \ldots, y_{i+1}$ are linearly independent, $\alpha_k \neq 0$ for some $k \geq i+1$. Without loss of generality, we may suppose that $\alpha_{i+1} \neq 0$. Then

$$x_{i+1} = \sum_{j=1}^{i+1} \beta_j y_j + \sum_{k=i+2}^{m} \beta_k x_k$$

for $\beta_1, \ldots, \beta_{i+1}, \beta_{i+2}, \ldots, \beta_m \in K$. Thus $y_1, \ldots, y_{i+1}, x_{i+2}, \ldots, x_m$ generate V. By iteration of this process, it follows that $y_1, \ldots, y_m$ generate V. In particular $y_{m+1} = \sum_{i=1}^{m} \gamma_i y_i,\ \gamma_i \in K$, contradicting the linear independence of S.

Corollary 1.1 *If $x_1, \ldots, x_m$ and $y_1, \ldots, y_n$ are bases of V, then $m = n$.*

Remark 1.14 *We shall be concerned only with vector spaces, which are finitely generated (over a field).*

Remark 1.15 *Let V be a vector space, finitely generated over a field K. From the finitely many generators, we can clearly pick out a maximal set of linearly independent elements which suffice to generate V and constitute a base of V over K.*

Remark 1.16 *Let V be a vector space generated by $x_1, \ldots, x_m$ over K and let $x \neq 0$ in V. Then $x, x_1, \ldots, x_m$ again generate V over K and, from this set, we can always pick out a maximal linearly independent subset containing x. In other words, any $x \neq 0$ in V can be completed to a base of V.*

Definition 1.30 *A vector space V is said to be of dimension n over a field K (in symbols $\dim_k V = n$) if there exists a base of V over K containing n elements.*

Observe that, by Corollary 1.1, the dimension is defined independently of the base used.

We shall write merely $\dim V$ for $\dim_k V$ when it is clear from the context to which field K we are referring.

Corollary 1.2 *Let W be a subspace of V with $dim_k V = n$. Then W has a base consisting of at most n elements, i.e.* $\dim_k W \leq \dim_k V$. *If W is a proper subspace of V, then* $\dim W < \dim V$.

For, we know first, by Proposition 1.5, that any linearly independent set in W contains at most n elements. Choose a maximal set of linearly independent elements in W. This is a base for W and therefore $\dim W \leq n = \dim V$. Since any n linearly independent elements of V generate V, it follows that $\dim W < \dim V$ if W is properly contained in V.

Example 1.21 *Let K be a field and k a subfield of K. Let L be a field of which K is a subfield. We may clearly consider L as a K-(or k-) vector space, K as a k-vector space. Suppose the vector spaces L/K, K/k are of finite dimension, and that $u_1, \ldots, u_n \in K$ form a k-base of $K, v_1, \ldots, v_m \in L$ form a K-base of L. Then L is a finite dimensional k-vector space, and the products $u_i v_j$, $1 \leq i \leq n$, $1 \leq j \leq m$*(in L) *form a k-base of L.*

Definition 1.31 *Let V, V' be two vector space over a field K. By a homomorphism (or K-linear map) of V into V' we mean a homomorphism f of $(V, +)$ into $(V', +)$ which satisfies in addition the condition $f(\lambda x) = \lambda f(x)$ for $x \in V$, $\lambda \in K$.*

If the homomorphism f is one-one and onto, then f is an isomorphism and V, V' are isomorphic.

By an *endomorphism* of a vector space V, we mean a homomorphism of V into itself.

Let $f: V \to V'$ be K-linear. Let N be the kernel of f. Then N is a subspace of V and, similarly, the image $f(V)$ is a subspace of V'. The quotient group V/N can be made into a vector space over K. Further V/N is isomorphic of $f(V)$ *(Noether homomorphism theorem).* If $\dim_k V$ is finite, then $\dim_k V = \dim_k f(V) + \dim_K N$. Let V, V' be vector spaces over K, and let $(e_1, \ldots, e_n)$ form a base of V over K. Then given arbitrary elements $a_1, \ldots, a_n \in V'$ here is a unique K-linear map $f: V \to V'$ with $f(e_i) = a_i$. In fact, for $x \in V$, if $x = \sum_{i=1}^{n} \lambda_i e_i$, then we have only to set $f(x) = \sum_{i=1}^{n} \lambda_i a_i$. The uniqueness is obvious.

Definition 1.32 *Let V be a vector space over a field K and $\dim_k V = n$. By a K-linear form (or briefly, a linear form) on V, we mean a homomorphism of V into K (regarded as a vector space over itself).*

The set V^* of linear forms on V forms a vector space over K and is called the *dual* of V. If $\alpha_1, \ldots, \alpha_n$ is a base of V over K, define the linear forms $\alpha_1^*, \ldots, \alpha_n^*$ by $\alpha_i^*(\alpha_j) = \delta_{ij}$ (*the Kronecker delta*)$= 1$ if $i = j$ and 0 for $i \neq j$. We see at once that $\alpha_1^*, \ldots, \alpha_n^*$ are linearly independent over K. For, if $\sum_{i=1}^n a_i \alpha_i^* = 0$ with $a_1, \ldots, a_n = K$, then $a_j = \sum_{i=1}^n a_i \alpha_i^*(\alpha_j) = 0$ for $j = 1, \ldots, n$. Any linear form α^* can be written in the form $\alpha^* = \sum_{i=1}^n b_i \alpha_i^*$ where $\alpha^*(\alpha_i) = b_i \in K$. Thus $\dim_K V^* = n$. The base $\alpha_1 *, \ldots, \alpha_n^*$ ofV^* is called the *dual base* of the base $\alpha_1, \ldots, \alpha_n$ of V.

Definition 1.33 *Let V be a vector space over a field K. A bilinear form B on V is a mapping $B\colon V \times V \to K$ such that for any fixed $y \in V$ the mappings B'_y, B''_y of V into K, defined by $B'_y(x) = B(x, y)$ and $B''_y(x) = B(y, x)$ respectively, are linear forms on V.*

Definition 1.34 *A bilinear form $B(x, y)$ on V is non-degenerate if, for any fixed $y \neq 0$ in V, the linear form B'_y, is not zero, i.e. $B(x, y) \neq 0$ for at least one x, and for any fixed $x \neq 0$, the linear form B''_x is not zero.*

Let V be a vector space of dimension n over a field K. Then we have

Proposition 1.6 *Let $B(x, y)$ be a non-degenerate bilinear form on V. Then for any base $\alpha_1, \ldots, \alpha_n$ of V, there exists a base $\beta_1, \ldots, \beta_n$ of V such that $B(\alpha_i, \beta_j) = \delta_{ij}$ (the Kronecker delta) for $1 \leq i, j \leq n$.*

Proof: Consider the mapping of V to V^* taking $y \in V$ to the linear form B'_y in V^*. This is clearly a homomorphism of V into V^*. Since B is non-degenerate, this mapping is injective. Since $\dim V = \dim V^* = n$, it follows by Noether's homomorphism theorem and Corollary 1.2 above that this mapping is onto V^*. Let $\alpha_1, \ldots, \alpha_n$ be a base of V over K and $\alpha_1^*, \ldots, \alpha_n^*$ the corresponding dual base of V^*. Let $\beta_1, \ldots, \beta_n$ be the elements of V which are mapped into $\alpha_1^*, \ldots, \alpha_n^*$ respectively by the homomorphism above. Then $B(\alpha_i, \beta_j) = \alpha_j^*(\alpha_i) = \delta_{ij}$.

1.9 Ideals and quotient rings

Let R be a (commutative) ring (with 1). Then R can be regarded as a module over itself.

Definition 1.35 *By an ideal of R, we mean an R-submodule of R.*

Clearly an ideal I of R, is a subgroup of $(R,+)$ such that for any $x \in I$ and $a \in R$, we have $ax \in I$.

Example 1.22 *R and $\{0\}$ are ideals of a ring R.*

Example 1.23 *Subgroups of $(\mathbf{Z},+)$ are ideals of the ring $\mathbf{Z}$ with the usual addition and multiplication. Any ideal of $\mathbf{Z}$ is clearly of the form $m\mathbf{Z}$, $m \in \mathbf{Z}$.*

Example 1.24 *Let R, R' be two rings and $f\colon R \to R'$ be a homomorphism. Then* $\ker f$ *is an ideal of R.*

An integral domain $R \neq \{0\}$ is a field if and only if R and $\{0\}$ are the only ideals of R, as can be easily proved.

Definition 1.36 *If $\mathfrak{a}, \mathfrak{b}$ are two ideals of R, the product $\mathfrak{ab}$ of $\mathfrak{a}$ and $\mathfrak{b}$ is the set of all finite sums of the form $\sum_i a_i b_i$ with $a_i \in \mathfrak{a}$ and $b_i \in \mathfrak{b}$.*

It is easy to check that $\mathfrak{ab}$ is again an ideal of R. Clearly $\mathfrak{ab} = \mathfrak{ba}$.

Definition 1.37 *An ideal $\mathfrak{a}$ of a ring R divides an ideal $\mathfrak{b}$ of R, if $\mathfrak{a} \supset \mathfrak{b}$.*

Definition 1.38 *By a proper ideal of a ring R, we mean an ideal of R different from R and $\{0\}$.*

Definition 1.39 *Let S be a subset of a ring R. An ideal $\mathfrak{a}$ of R is generated by S, if it is generated by S as an R-module. We say $\mathfrak{a}$ is finitely generated, if it is finitely generated as an R-module.*

Definition 1.40 *If an ideal $\mathfrak{a}$ of a ring R is generated by a single element $\alpha \in R$, then $\mathfrak{a}$ is called a principal ideal of R. (We denote it by αR in this case or just by (α).)*

Example 1.25 *R and $\{0\}$ are principal ideals of R.*

Definition 1.41 *An integral domain R all of whose ideals are principal ideals is called a principal ideal domain.*

Example 1.26 $\mathbf{Z}$ *is a principal ideal domain (see Example* 1.23*, p.* 17*).*

Let $\mathfrak{a}$ be an ideal of a ring R. The additive group of $R/\mathfrak{a}$ (in words, R modulo $\mathfrak{a}$) is a ring called the *the quotient ring* of R by $\mathfrak{a}$, with multiplication defined by $(x+\mathfrak{a})(y+\mathfrak{a}) = xy+\mathfrak{a}$ for $x, y \in R$. (Since $\mathfrak{a}$ is an ideal of R, this multiplication is well defined.) The natural map $q\colon R \to R/\mathfrak{a}$ is a surjective homomorphism with kernel $\mathfrak{a}$.

Example 1.27 $\mathbf{Z}/(m)$ *is the quotient ring of* $\mathbf{Z}$ *by the ideal* (m)*. This ring is called the ring of residue classes modulo* m*. (See Example* 1.12*, page* 8*.) It is a field if and only if* m *is a prime, by Proposition* 1.2*.*

Let $f\colon R \to R'$ be a homomorphism of a ring R onto a ring R' and let $\mathfrak{a} = \ker f$. The homomorphism f induces a homomorphism $\bar{f}\colon R/\mathfrak{a} \to R'$, by setting $\bar{f}(x+\mathfrak{a}) = f(x)$ for $x \in R$. Clearly f is an isomorphism of rings. *(Fundamental theorem of homomorphisms for rings.)*

Remark 1.17 *Let K be a field. Consider the ring homomorphism $f\colon \mathbf{Z} \to K$ given by $f(n) = n\cdot 1 (= 1+\cdots+1,\ n$ times). By the fundamental theorem of homomorphisms referred to above, $\mathbf{Z}/\ker f \simeq f(\mathbf{Z})$. We have $\ker f = (p)$ for some $p \geq 0$. in $\mathbf{Z}$. We call p the characteristic of K. Observe that p is a prime, if $p > 0$. For, if $p = rs$, $1 < r, s < p$ then $f(r)f(s) = f(rs) = 0$. But neither $f(r)$ nor $f(s)$ is zero, contradicting the fact that K is an integral domain. If $p = 0$, then K contains $f(\mathbf{Z})$ which is isomorphic to $\mathbf{Z}$ and hence contains a subfield isomorphic to $\mathbf{Q}$ (see remark on 11). Thus every field contains a subfield isomorphic to either $\mathbf{Q}$ or $\mathbf{Z}/(p)$ (for a prime p). The fields $\mathbf{Q}$ and $\mathbf{Z}/(p)(p$ prime) are called prime fields.*

Definition 1.42 *A proper ideal $\mathfrak{p}$ of an integral domain R is called a prime ideal if, for $a, b \in R$, $ab \in \mathfrak{p}$ implies that either a or b is in $\mathfrak{p}$.*

Example 1.28 *In* $\mathbf{Z}$ *a prime p generates a prime ideal and conversely every prime ideal of* $\mathbf{Z}$ *is generated by a prime p.*

Remark 1.18 *A proper ideal $\mathfrak{p}$ is a prime ideal of a ring R if and only if $R/\mathfrak{p}$ is an integral domain.*

Remark 1.19 *If a prime ideal* $\mathfrak{p}$ *of a ring* R *divides the product of two ideals* $\mathfrak{a}$ *and* $\mathfrak{b}$*, then* $\mathfrak{p}$ *divides either* $\mathfrak{a}$ *or* $\mathfrak{b}$*. For, if* $\mathfrak{p}$ *divides neither* $\mathfrak{a}$ *nor* $\mathfrak{b}$ *there exist* $a \in \mathfrak{a},\ b \in \mathfrak{b}$ *while* $ab \in \mathfrak{ab} \subset \mathfrak{p}$ *which is a contradiction.*

Definition 1.43 *A proper ideal* $\mathfrak{a}$ *of* R *is maximal if* $\mathfrak{a}$ *is not contained in any other proper ideal of* R*.*

Remark 1.20 *An ideal* $\mathfrak{a}$ *of a ring* R *is a maximal ideal, if and only if* $R/\mathfrak{a}$ *is a field.*

Remark 1.21 *A maximal ideal is clearly prime.*

1.10 Linear mappings and matrices

Let V be a vector space of dimension n over a field K. Let ϕ be a linear mapping (i.e. a homomorphism) of V into V. Taking a *fixed* base $e_1, \ldots, e_n$ of V over K, let $\phi(e_j) = \sum_{i=1}^{n} a_{ij} e_i (j = 1, \ldots, n)$ with $a_{ij} \in K$. To the linear mapping ϕ, we associate the ordered set

$$\begin{bmatrix} a_{11} & \cdots & a_{1n} \\ & \cdots & \\ & \cdots & \\ a_1 n & \cdots & a_{nn} \end{bmatrix}$$

of the n^2 elements $a_{11}, a_{12}, \ldots, a_{nn}$, which will be referred to as the corresponding 'matrix'(a_{ij}). The elements $a_{pq} (p = 1, 2, \ldots, n)$ are said to constitute the pth 'row' of (a_{ij}) and the elements $a_{pq} (p = 1, 2, \ldots, n)$ constitute the qth 'column' of (a_{ij}). The matrix (a_{ij}) has thus n rows and n columns and is called an n-rowed square matrix (or an $n \times n$ matrix) with elements in K.

Conversely, given an n-rowed square matrix (a_{ij}) with elements in K, we can find a unique linear mapping ϕ of V into itself for which $\phi(e_j) = \sum_{i=1}^{n} a_{ij} e_i$. Thus, once a base of V is chosen, the linear mappings of V into itself stand in one-one correspondence with the set $\mathcal{M}_n(K)$ of n-rowed square matrices with elements in K. In $\mathcal{M}_n(K)$,we can introduce the structure of a ring as follows. If $A = (a_{ij}),\ B = (b_{ij})$ are in $\mathcal{M}_n(K)$ define $A + B$ to be the n-rowed square matrix (c_{ij}) with $c_{ij}) = a_{ij} + b_{ij}$ and the product AB to be the element (d_{ij}) of $\mathcal{M}_n(K)$ with

$$d_{ij} = \sum_{p=1}^{n} a_{ip} b_{pj}.$$

The usual laws of addition and multiplication for a ring can be verified to be true. However, this ring is not, in general, commutative. To the identity mapping $I_V: V \to V$ corresponds the matrix $I = I_n = (\delta_{ij})$ and this serves as the unit element in the ring $\mathcal{M}_n(K)$. Note that if ϕ, ψ are two linear mappings of V into itself, and if A, B are the corresponding matrices, then $\phi + \psi$ corresponds to $A + B$ and $\phi \circ \psi$ to $A \cdot B$. For $A = (a_{ij}) \in \mathcal{M}_n(K)$, we define the *trace* $\mathrm{Tr}\,(A)$ of A to be the sum $\sum_{i=1}^{n} a_{ii}$. Clearly for $A = (a_{ij}),\ B = (b_{ij})$ in $\mathcal{M}_n(K)$, we have $\mathrm{Tr}\,(AB) = \sum_{i,j=1}^{n} a_{ij}b_{ji} = \mathrm{Tr}\,(BA)$ and further $\mathrm{Tr}\,(I) = n$. For $A \in \mathcal{M}_n(K)$, we denote by $\det A$, the *determinant* of A. For $A = I, \det\ I = 1$.

We shall not define the *determinant.* It has the following properties which are the only ones we shall use. (See e.g. Halmos [2],)

Let $A = (a_{ij}),\ 1 \leq i,\ j \leq n$. Then

(a) $\det A$ is a homogeneous polynomial in the elements a_{ij} of degree n;

(b) $\det A$ is linear considered as a function of any row of (a_{ij}); it is linear also in the columns of (a_{ij});

(c) if $A = (a_{ij})$ and $A^t = (b_{ij})$ where $b_{ij} = a_{ji}$,then $\det A^t = \det A$;

(d) if $A = (a_{ij})$ and $a_{ij} = 0$ for $i > j$, then $\det A = a_{11} \ldots a_{nn}$; in particular $\det I = 1$;

(e) for any two $n \times n$ matrices A and B, we have $\det(AB) = \det A \cdot \det B$.

Let $f_1, \ldots, f_n$ constitute another base of V over K, and let

$$f_j = \sum_{i=1}^{n} p_{ij}e_i,\ e_j = \sum_{i=1}^{n} q_{ij}f_i,\ j = 1, \ldots, n,\ p_{ij}, q_{ij} \in K.$$

Then to the linear mapping ϕ of V into V, taking e_j to f_j corresponds the matrix $P = (p_{ij})$. Let ψ be the linear mapping of V taking f_j to e_j. Denote by Q the corresponding matrix (q_{ij}). The composite mappings $\phi \circ \psi$ and $\psi \circ \phi$ are clearly both equal to the identity mapping of V into itself. The corresponding matrices are PQ and QP respectively. Hence $PQ = QP = I_n$ and Q is the inverse P^{-1} of P in $\mathcal{M}_n(K)$.

Suppose now, that instead of the base $e_1, \ldots, e_n$ of V, we had referred everything to another fixed base $f_1, \ldots, f_n$ with $f_j = \sum_{i=1}^{n} p_{ij}e_i (j = 1, \ldots, n)$. Then the linear mapping ψ taking e_j to $\sum_{i=1}^{n} a_{ij}e_i (j =$

$1, \ldots, n)$ would take f_j to $\sum_{i=1}^{n}(\sum_{k,l=1}^{n} q_{il}a_{lk}p_{kj})f_i$ and the corresponding matrix would be $QAP = P^{-1}AP \in \mathfrak{M}_n(K)$. Now $\mathrm{Tr}\,(P^{-1}AP) = \mathrm{Tr}\,(APP^{-1}) = \mathrm{Tr}\,(A)$. Consequently, if ϕ is an endomorphism of V, and A the matrix corresponding to it with respect to a base of V, then $\mathrm{Tr}\,(A)$ is independent of the base chosen, and we set $\mathrm{Tr}\,(\phi) = \mathrm{Tr}\,(A)$ and speak of the *trace of the endomorphism.* Similarly, since

$$\det(P^{-1}AP) = \det P^{-1} \cdot \det A \cdot \det P = \det A \cdot \det P^{-1} \cdot \det P = \det A$$

we may define $\det \phi$ to be $\det A$ where $A \in \mathfrak{M}_n(K)$ is a matrix corresponding to ϕ with respect to a base of V. For $\phi = I_V,\ \det \phi = 1$.

Remark 1.22 *A one-one linear mapping ϕ of V into V is necessarily onto V. For, $\dim \phi(V) = \dim V$ by the homomorphism theorem. Since $\phi(V)$ is a subspace of V of the same dimension as V, we have $\phi(V) = V$ i.e. ϕ is onto V.*

Remark 1.23 *A linear mapping ϕ of V into V is one-one if and only if $\det \phi \neq 0$.*

Proof: If ϕ is one-one, then ϕ is onto V by Remark 1.22 above. Clearly there exists a linear mapping ψ of V into V such that $\phi \circ \psi = I_V$. Since $\det(\phi \circ \psi) = \det \phi \cdot \det \psi = \det I_V = 1$, it follows that $\det \phi \neq 0$. Conversely, if $\det \phi \neq 0$, let, if possible, $\phi(e_1) = 0$ for $e_1 \neq 0$. But, by Remark 14 on page 14, e_1 can be completed to a base $e_1, e_2, \ldots, e_n$ of V. For this base, the corresponding matrix A in $\mathfrak{M}_n(K)$ has the form (a_{ij}) with $a_{i1} = 0$ for $i = 1, \ldots, n$ and therefore $\det \phi = \det A = 0$,(since $\det A$ is linear in the columns of A). We are thus led to a contradiction.

1.11 Polynomial rings

Let R be a commutative ring (containing 1). Let M be the set of all mappings $f\colon \mathbf{Z}^+ \to R$ such that $f(n) = 0$ for all but finitely many n.

We introduce on M the structure of an R-module by defining, for $f,\ g \in M,\ a \in R,\ f + g, af$ by

$$(f + g)(n) = f(n) + g(n), (af)(n) = a \cdot f(n),\ n \in \mathbf{Z}^+.$$

We make M a ring by defining $f \cdot g$ by $(f \cdot g)(n) = \sum_{i=0}^{n} f(i)g(n-i)$. The map e for which $e(0) = 1,\ e(n) = 0$ for $n > 0$ is the unit of M. We have a map $i\colon R \to M$ defined by $i(a)(0) = a,\ i(a)(n) = 0$ for $n > 0, i$

is an isomorphism of R onto a subring of M, so that we may identity R with $i(R)$. Let $X \in M$ denote the map for which $X(1) = 1,\ X(n) = 0$ if $n \neq 1$. Then (with multiplication defined as above) X^k is the map for which $X^k(k) = 1,\ X^k(n) = 0$ if $n \neq k$. Hence any $f \in M$ can be written uniquely in the form

$$f = \sum a_k X^k, \quad a_k \in R;$$

the sum is finite, i.e. $a_k = 0$ for large k.

Definition 1.44 *The ring M is denoted by $R[X]$ and is called the polynomial ring in one variable over R. The elements of $R[X]$ are called polynomials with coefficients in R or polynomials over R.*

Definition 1.45 *If $f = \sum_{i=1}^{n} a_i X^i \in R[X]$ and $f \neq 0$, we define the degree n of f (in symbols deg f) to be the largest integer i such that $a_i \neq 0$. We call a_n the leading coefficient of f. If this $a_n = 1$, we say f is a monic polynomial. If f is of degree 1, we call f a linear polynomial. If $f = 0$, we set* $\deg f = -\infty$.

Remark 1.24 *If $f,\ g \in R[X]$ we have*

$$\deg(f + g) \leq \max(\deg f, \deg g).$$

If $\deg f \neq \deg g$, *then* $\deg(f + g) = \max(\deg f, \deg g)$.

Remark 1.25 *If R is an integral domain and $f,\ g \in K[X]$ with $f \neq 0,\ g \neq 0$, then $fg \neq 0$, i.e. $R[X]$ is an integral domain. Further,* $\deg(fg) = \deg f + \deg g$.

Remark 1.26 *Let K be a field and let $f,\ g \in K[X]$ with* $\deg g > 0$. *Then there exist $h,\ j \in K[X]$ such that $f = gh + j$ where* $\deg j < \deg g$. *(Division algorithm in $K[X]$.)*

Remark 1.27 *Given any ideal $\mathfrak{a} \neq \{0\}$ of the polynomial ring $K[X]$ over a field K, it is clear by Remark* 1.26 *that $\mathfrak{a}$ is generated over $K[X]$ by a polynomial t in $\mathfrak{a}$ of minimal positive degree. Thus $K[X]$ is a principal ideal domain.*

Let R, R' be two rings and $\phi\colon R \to R'$ be a homomorphism. Then we can extend ϕ uniquely to a homomorphism ϕ of $R[X]$ to $R'[X]$ by prescribing that $\phi(X) = X$ and, in general

$$\phi\Big(\sum_i a_i X^i\Big) = \sum_i \phi(a_i) X^i \quad \text{for } \sum_i a_i X^i \in R[X].$$

Let R be a ring with $R \subset \mathbf{C}$ and let $R' = \mathbf{C}$. For any $\alpha \in \mathbf{C}$ we have a unique R-linear ring homomorphism $\psi\colon R[X] \to \mathbf{C}$ such that $\psi(X) = \alpha$; in fact we have only to set $\psi(\sum a_i X^i) = \sum a_i \alpha^i,\ a_i \in R$. We denote the image of $R[X]$ under ψ by $R[\alpha]$ and for $f = \sum_i a_i X^i \in R[X]$, we write $f(\alpha) = \sum_i a_i \alpha^i$.

Definition 1.46 *A complex number α is a root of $f \in R[X]$, if $f \in \ker \psi$, i.e. $f(\alpha) = 0$.*

Example 1.29 *Take $R = \mathbf{C}$. The complex numbers $\pm\sqrt{(-5)}$ are roots of the polynomial $x^2 + 5$.*

Remark 1.28 *If $R = K$ is a field and $f \in K[X]$, then $\alpha \in K$ is a root of f if and only if $(X - \alpha)|f$. In fact, there is $\beta \in K[X]$ of degree $0\,(\text{or } -\infty)$, i.e. $\beta \in K$, such that $f = q \cdot (X - \alpha) + \beta,\ q \in K[X]$. Then $f(\alpha) = \beta = 0$.*

Definition 1.47 *If $R = K$ is a field, $\alpha \in K$ is called a repeated root of $f \in K[X]$ if $(X - \alpha)^2 | f$.*

Definition 1.48 *If $f = \sum_{i \geq 0} a_i X^i \in K[X]$, then the polynomial $f' = \sum_{i \geq 1} i a_i X^{i-1}$ is called the derivative of f.*

Remark 1.29 *It is easily seen that $(f+g)' = f' + g',\ (fg)' = fg' + gf'$ and if K has characteristic 0, that $f' = 0$ if and only if $f \in K$. When K has characteristic $p > 0,\ f' = 0$ if and only if $f \in K[X^p]$.*

The quotient field of the polynomial ring $K[X]$ over a field K is denoted by $K(X)$ and called the *field of rational functions in one variable over K*.

1.12 Factorial rings

Let R be an integral domain.

Definition 1.49 *An element $a \in R^*$ which is not a unit in R is called irreducible, if, whenever $a = bc$ for $b, c \in R$, either b or c is a unit in R.*

Definition 1.50 *An element $p \in R^*$ is said to be prime if it is not a unit and whenever p divides ab, with $a, b \in R, p$ divides either a or b.*

Example 1.30 *A prime number p in $\mathbf{Z}$ is prime in $\mathbf{Z}$ (Proposition 1.2).*

Remark 1.30 *A prime element is always irreducible but not conversely, (in general). In $\mathbf{Z}$, every irreducible element is (upto sign) a prime number, by the very definition of a prime number.*

Remark 1.31 *In a principal ideal domain, an irreducible element generates a maximum ideal.*

Definition 1.51 *An integral domain R is a factorial ring (or a unique factorization domain) if every non-unit $a \in R^*$ can be written in the form $a = q_1 \cdots q_r$ where $q_1, \ldots, q_r$ are irreducible elements of R determined uniquely by a upto multiplication by units of R and upto order. the decomposition $a = q_1 \cdots q_r$ is called the factorization of a (into irreducible elements).*

Remark 1.32 *In a factorial ring R, every irreducible elements is prime (and hence, by Remark 1.30 above, the notions of 'prime' and 'irreducible' coincide in such a ring). For, if an irreducible element a divides bc, then a must occur in the factorization of bc and hence in that of at least one of b, c.*

Remark 1.33 *Let $a = p_1 \cdots p_r$ be a factorization of an element a into irreducible elements. Clubbing together the irreducible elements which are associated, we can write a in the form $up_1^{n_1} \cdots p_s^{n_s}$, where $n_1, \ldots, n_s \in \mathbf{Z}$, $n_i > 0$, $p_1, \ldots, p_s$ are irreducible elements in R which are non-associate, and u is a unit.*

Definition 1.52 *Let $a_1, \ldots, a_r$ be elements of the factorial ring R and $a_i = u_i \prod_{j=1}^{s} p_j^{n_{j,i}}$ with $n_{j,i} \in \mathbf{Z}^+$ and irreducible $p_1, \ldots, p_s$ (some of the $n_{j,i}$ may be zero). The greatest common divisor (briefly g.c.d.) of $a_1, \ldots, a_r$ is defined to be $\prod_{j=1}^{s} p_j^{\alpha_j}$ where $\alpha_j = \min(n_{j,i}, \ldots, n_{j,r})$, $j = 1, \ldots, s$. Similarly, the least common multiple of $a_1, \ldots, a_r$ is defined to be $\prod_{j=1}^{s} p_j^{\beta_j}$ where, for $j = 1, \ldots, s$, $\beta_j = \max(n_{j,i}, \ldots, n_{j,r})$. These are uniquely determined upto units.*

Proposition 1.7 *(Fundamental theorem of arithmetic.) $\mathbf{Z}$ is a factorial ring.*

PROOF: The only units in $\mathbf{Z}$ are $+1$ and -1. It suffices to prove that every positive integer can be written uniquely as a product of positive

irreducible elements of $\mathbf{Z}$, in other words, of prime numbers (in view of Remark 1.30 above). If two prime numbers are associated, they must be the same.

We shall first prove that if a factorization of $a > 0$ in $\mathbf{Z}$ into primes exists it is unique. Let, in fact, for $a > 0$ in $\mathbf{Z}$, $a = p_1 \cdots p_r = q_1 \cdots q_s$ where $p_1, \ldots, p_r,\ q_1, \ldots, q_s$ are primes. Now q_1 divides $p_1 \cdots p_r$ and hence divides one of the p_i, say p_1. Then $q_1 = p_1$. Now $p_2 \cdots p_r = q_2 \cdots q_s$. By repeating the argument above, q_2 is equal to one of $p_2, \ldots, p_r$, say $q_2 = p_2$. In finitely many steps, we can thus prove that $r = s$ and that $q_1, \ldots, q_s$ coincide with $p_1, \ldots, p_r$ order.

We now prove the existence of a factorization for any $a > 0$ in $\mathbf{Z}$ by induction. For $a = 2$, this is trivial. Assume that a factorization into primes exists for all positive integers less than a. Now if a is a prime, we have nothing to prove. if a is not prime, then a is divisible by $b \in \mathbf{Z}$ with $1 < b < a$. In other words, $a = bc$ with $b,\ c \in \mathbf{Z}$ and $1 < b, c < a$. By the induction hypothesis, b and c have a factorization into primes and therefore $a = bc$ admits a similar factorization too. The theorem is thus completely proved.

Proposition 1.8 *If K is a field, the polynomial ring $K[X]$ in one variable is a factorial ring.*

PROOF: First, let us observe that the set of units in $K[X]$ is precisely K^*. If this were not true, let, if possible, $f = a_n X^n + \cdots + a_0$ with $a_n \neq 0,\ n \geq 1$ be a unit in $K[X]$. Then, there exists $g = b_m X^m + \cdots + b_0$ with $b_m \neq 0$ such that $fg = 1$. Then $0 = \deg 1 = \deg(fg) = n + m > 1$, which is a contradiction.

We start with the existence of a factorization. Let f be a non-constant polynomial in $K[X]$. If f is an irreducible element, then there is nothing to prove. If not, f has a non-constant divisor g not associated with f, i.e. $f = gh$ with $0 < \deg g, \deg h < \deg f$. Employing induction on the degree of elements in $K[X]$, it follows that g, h have factorizations into irreducible elements of $K[X]$ and consequently $f = gh$ also can be so factorized.

The uniqueness of factorization can be established exactly as in the proof of Proposition 1.7, provided we have the following

Lemma 1.1 *In $K[X]$, every irreducible element is prime.*

PROOF: Let p be an irreducible element of $K[X]$ and let p divide the product gh of two polynomials g, h in $K[X]$, and suppose that $p \nmid g$.

Consider the set $\mathfrak{a}$ of polynomials of the form $up+vg$ where $u, v \in K[X]$. Then $\mathfrak{a}$ is a non-zero ideal of $K[X]$ and, since $K[X]$ is a principal ideal domain, there is $t \in K[X]$ with $\mathfrak{a} = (t)$. Thus t divides p, but since p is irreducible, it follows that either $p = ct$ with $c \in K^*$, or $t \in K^*$. If $p = ct$, then since t divides every element of $\mathfrak{a}$ and, in particular, g it follows that $p \mid g$. This contradicts our assumption. Hence $t \in K^*$ and therefore there exists u_1, v_1 in $K[X]$ such that $u_1 p + v_1 g = 1$. Since $gh = pw$ where $w \in K[X]$, we have $h = h(u_1 p + v_1 g) = p(u_1 h + v_1 w)$, i.e. $p \mid h$.

Remark 1.34 *It can be shown, by similar reasoning, that any principal ideal domain is a factorial ring.*

We now give an example of a ring R which is not a factorial ring. Take R to be the subring of $\mathbf{C}$ consisting of numbers of the form $a + b\sqrt{(-5)}$ with $a, b \in \mathbf{Z}$ and $\sqrt{(-5)}$ being a root of the polynomial $x^2 + 5$. In R, there are two distinct factorizations of 6, viz. $6 = 2 \cdot 3 = (1 + \sqrt{(-5)})(1 - \sqrt{(-5)})$. (It is not hard to see that the four numbers occurring here are irreducible.) Thus R cannot be a factorial ring and in R, an irreducible element is not prime in general.

We shall see however that R belongs to a general class of rings admitting unique factorization of ideals into prime ideals, which will be the object of our study in Chapter 2.

1.13 Characters of a finite abelian group

Let G be a finite abelian group, of order h. A *character* χ of G is a mapping $\chi: G \to \mathbf{C}$ such that $\chi \not\equiv 0$, and $\chi(ab) = \chi(a)\chi(b)$ for $a, b \in G$.

If $a \in G$ is such that $\chi(a) \neq 0$, then for any $b \in G$, $\chi(a) = \chi(b)\chi(ab^{-1})$, so that $\chi(b) \neq 0$. Hence χ is a *homomorphism of G into* $\mathbf{C}^*$. Further, since $b^h = e$ we have $[\chi(b)]^h = 1$ for any b. Since there are only finitely many *hth* roots of unity in $\mathbf{C}$, it follows that *there are only finitely many characters of G.*

If we define the product $\chi_1\chi_2$ of two characters χ_1, χ_2 by $(\chi_1\chi_2)(a) = \chi_1(a)\chi_2(a)$, then the characters form a finite abelian group $\widehat{G}$.

Proposition 1.9 *Let G be a finite abelian group and let $a \in G,\ a \neq e$. Then there exists a character χ of G such that $\chi(a) \neq 1$.*

PROOF: Let $a_0 = e,\ a_1 = a,\ a_3, \ldots, a_{h-1}$ be the elements of G. Let V be the set of formal linear combinations $\sum \lambda_i a_i,\ \lambda_i \in \mathbf{C}$. Clearly, V is a

vector space of dimension h over $\mathbf{C}$, and the elements of G form a base of V.

We shall use repeatedly the following remark.

Remark 1.35 *Let $W \neq \{0\}$ be a finite dimensional vector space over $\mathbf{C}$, and $T: W \to W$ an endomorphism. Then there exists $x \neq 0,\ x \in W$ such that $Tx = \lambda x,\ \lambda \in \mathbf{C}$.*

In fact, every polynomial over $\mathbf{C}$ has a root in $\mathbf{C}$, we can find $\lambda \in \mathbf{C}$ such that $\det(t - \lambda I) = 0$. $I: W \to W$ being the identity map. then $T - \lambda I$ cannot be one-one by Remark 1.23 on page 21. Hence there is $x \neq 0$ in W with $Tx - \lambda x = 0$. Such a λ is called an *eigenvalue* of T.

Any element a_i $(i = 0, 1, \ldots, h-1)$ gives rise to a permutation of the elements of G viz, the permutation given by the mapping $x \mapsto a_i x$ of G onto G. There is a uniquely determined linear mapping A_i $(i = 0, 1, \ldots, h-1)$ of V which maps any element x in G to $a_i x$. Further, if the linear mappings A_i, A_j of V correspond in this way to a_i, a_j in G respectively, then clearly $A_i A_j$ corresponds to $a_i a_j$. Moreover, since G is abelian, we have $A_i A_j = A_j A_i$. In addition, A_0 is the identity mapping I of V and $A_i^h = I$ for $i = 0, 1, \ldots, h-1$. Let us write A for the linear mapping A_1 corresponding to $a_1 = a$.

We first prove that the linear mapping A corresponding to $a \in G$ has at least one eigenvalue $\lambda \neq 1$, i.e. there exists $\lambda \neq 1$ in $\mathbf{C}$ and $x \neq 0$ in V with $Ax = \lambda x$. Clearly $A \neq I$, so that the space $W = \{Ax - x,\ x \in V\} \neq \{0\}$. Also A maps W into itself since $A(Ax - x) = Ay - y$ where $y = Ax$. Hence by the remark above, there exist $y_0 \neq 0$ in W and λ in $\mathbf{C}$ such that $ay_0 = \lambda y_0$. Suppose, if possible that $\lambda = 1$. Let $y_0 = Ax_0 - x_0$. Then $A^k(Ax_0 - x_0) = Ax_0 - x_0$ for any $k \geq 0$ in $\mathbf{Z}$. Since $A^h = I$, we have $(I + A + A^2 + \cdots + A^{h-1})(A - I) = 0$ so that

$$(I + A + A^2 + \cdots + A^{h-1})(Ax_0 - x_0) = 0.$$

But, since $A^k(Ax_0 - x_0) = Ax_0 - x_0$ this gives us $h(Ax_0 - x_0) = 0$, contrary to our assumption that $y_0 = Ax_0 - x_0 \neq 0$. Hence λ cannot be equal to 1 and our assertion is proved.

Let now $\lambda_1 \neq 1$ be an eigenvalue of $A_1 = A$ and let $V_0 = V$ and $V_1 = \{x \in V_0 | A_1 x = \lambda_1 x\}$. Then $V_1 \neq \{0\}$ and further, the mapping A_i of V corresponding to any $a_i \in G$ maps V_1 into itself; in fact, if $x \in V_1$, then $A_1(A_i x) = A_i(A_1 x) = A_i(\lambda_1 x) = \lambda_1(A_i x)$ so that $A_i x \in V_1$. Hence again by our earlier remark, there exist λ_2 in $\mathbf{C}$ and $x \neq 0$ in V_1 with $A_2 x = \lambda_2 x$. Let $V_2 = \{x \in V_1 \mid A_2 x = \lambda_2 x\}$. Again, each

A_i maps V_2 into itself and we may continue the process above. let $V_{i+1} = \{x \in V_i \mid A_{i+1}x = \lambda_{i+1}x\}$ for $i = 0, 1, 2, \ldots, h-2$, where λ_{i+1} is an eigenvalue of $A_{i+1}|V_i$. For any $x \neq 0$ in V_{h-1} we have $A_i x = \lambda_i x$, $i = 0, 1, 2, \ldots, h-1$. Clearly $\lambda_0 = 1$. If we set $\chi(a_i) = \lambda_i$ for $i = 0, 1, 2, \ldots, h-1$, we obtain a character of G in fact, since$(A_iA_j)x = A_i(\lambda_j x) = \lambda_i\lambda_j x$, we have $\chi(a_ia_j) = \chi(a_i)\chi(a_j)$. Further $\chi(a) = \lambda_1 \neq 1$. This proves Proposition 1.9.

Proposition 1.10 *(Orthogonality relations.) We have*

$$S = \sum_{a\in G} \chi_1(a)\bar{\chi_2}(a) = \begin{cases} h \text{ if } \chi_1 = \chi_2, \\ 0 \text{ otherwise,} \end{cases}$$

$$\widehat{S} = \sum_{\chi\in\widehat{G}} \chi(a)\bar{\chi}(b) = \begin{cases} k = \text{ order of } \widehat{G} \text{ if } a = b, \\ 0 \text{ otherwise.} \end{cases}$$

Here $\bar{\chi}(a)$ denotes the complex conjugate of $\chi(a)$.

Proof: Since $|\chi(a)| = 1$, we have $\bar{\chi}(a) = \chi(a)^{-1}$. If $\chi_1 = \chi_2$, we clearly have $\sum_{a\in G} \chi_1(a)\bar{\chi_1}(a) = \sum_{a\in G} 1 = h$. If $\chi_1 \neq \chi_2$, let $b \in G$ be such that $\chi_1(b) \neq \chi_2(b)$. Then we have $S \cdot (\chi_1\bar{\chi_2})(b) = \sum_{a\in G}(\chi_1\bar{\chi_2})(ab) = S$ since ab runs over all the elements of G when a does so. Since $\chi_1\bar{\chi_2}(b) \neq 1$, we have $S = 0$.

Similarly, if $a = b$, clearly $\widehat{S} = k$. If $a \neq b$, let $\chi_1 \in \widehat{G}$ be such that $\chi_1(ab^{-1}) \neq 1$. (This exists by Proposition 1.9.) Then

$$\widehat{S}\chi_1(ab^{-1}) = \sum_{\chi\in\widehat{G}} \chi\chi_1(ab^{-1}) = \widehat{S},$$

so that $\widehat{S} = 0$.

It can be proved that G and $\widehat{G}$ are isomorphic, so that $k = h$. This is, however, unnecessary for our purposes and we do not go into this question.

Chapter 2

Algebraic Number Fields

2.1 Algebraic numbers and algebraic integers

Definition 2.1 *A complex number α is said to be algebraic if α is a root of a polynomial $a_nX^n + \cdots + a_0,\ a_0, \ldots, a_n$ in $\mathbf{Q}$ not all zero.*

If α is algebraic then the mapping from $\mathbf{Q}[X]$ to $\mathbf{C}$ taking $\sum_{i=0}^{n} a_iX^i$ to $\sum a_i\alpha^i$ is a homomorphism with *kernel* $\neq 0$.

Definition 2.2 *A complex number α is called transcendental if it is not algebraic.*

Let $\mathfrak{a}$ be the set of all polynomials in $\mathbf{Q}[X]$ having a fixed algebraic number α as a root. Clearly $\mathfrak{a}$ is an ideal of $\mathbf{Q}[X]$ and, in fact, generated over $\mathbf{Q}[X]$ by a non-constant polynomial, say t in view of Remark 1.27 on page 22. Now t is necessarily irreducible. Otherwise, $t = uv$ with $0 \leq \deg u,\ \deg v < \deg t$ and since $0 = t(\alpha) = u(\alpha)v(\alpha)$ at least one of u, v is in $\mathfrak{a}$, contradicting the minimality of $\deg t$. The polynomial t is clearly determined uniquely upto a constant factor. We may suppose therefore that the leading coefficient of t is 1; so normalized, it is called the minimal polynomial of x.

Definition 2.3 *By the degree of an algebraic number α, we mean the degree of the minimal polynomial of α.*

Example 2.1 *The "quadratic irrationality" $\sqrt{(-5)}$ is of degree 2.*

Let α be an algebraic number of degree n. Consider the subring $\mathbf{Q}[\alpha]$ of $\mathbf{C}$ consisting of numbers of the form $\sum_{i=0}^{m} a_i\alpha^i$ with $a_i \in \mathbf{Q}$. We now

assert that $\mathbf{Q}[\alpha]$ is a field. Let, in fact, f be the minimal polynomial of α. Consider the mapping $q\colon \mathbf{Q}[X] \to \mathbf{C}$ taking $\sum_{i=0}^{m} b_i X^i$ to $\sum_{i=0}^{m} b_i \alpha^i$. This is a homomorphism onto $\mathbf{Q}[\alpha]$ with kernel $f\mathbf{Q}[X] = (f)$. By the homomorphism theorem $\mathbf{Q}[X]/(f)$ is isomorphic to $\mathbf{Q}[\alpha]$. Let now $g \in \mathbf{Q}[X]/(f)$ be such that $g \neq 0$ i.e. $f \nmid g$. The ideal generated by f and g in $\mathbf{Q}[X]$ is a principal ideal $\mathfrak{b}$ generated by, say h. Since h divides f, we have $h = cf,\ c \in \mathbf{Q}^*$ unless $h \in \mathbf{Q}^*$. The former case is impossible, since $h \mid g$ and $f \nmid g$. Thus $\mathfrak{b} = \mathbf{Q}[X]$ and consequently there exist k, l in $\mathbf{Q}[X]$, such that $kf + lg = 1$, so that $\bar{g}\bar{l} = 1$. This proves that $\mathbf{Q}[X]/(f)$, and $\mathbf{Q}[\alpha]$ is a field.

We denote the field $\mathbf{Q}[\alpha]$ by $\mathbf{Q}(\alpha)$.

Definition 2.4 *A subfield K of $\mathbf{C}$ is called an algebraic number field if its dimension as a vector space over $\mathbf{Q}$ is finite. The dimension of K over $\mathbf{Q}$ is called the degree of K, and is denoted by $[K : \mathbf{Q}]$.*

Example 2.2 *$\mathbf{Q}$ and $\mathbf{Q}(\sqrt{(-5)})$ are algebraic number fields of degree 1 and 2 respectively.*

Remark 2.1 *Any element α of an algebraic number field K is algebraic. (For, if $[K : \mathbf{Q}] = n$ then $1, \alpha, \alpha^2, \ldots, \alpha^n$ are necessarily linearly dependent over $\mathbf{Q}$.)*

Remark 2.2 *If α is an algebraic number of degree n, then $\mathbf{Q}[\alpha]$ is an algebraic number field of degree $n (\mathbf{Q}(\alpha) = \mathbf{Q}[\alpha])$.*

Remark 2.3 *Any monic irreducible polynomial f in $\mathbf{Q}[X]$ is the minimal polynomial of any of its roots. For, if α is a root of f, then α is an algebraic number and its minimal polynomial ϕ certainly divides f since $f(\alpha) = 0$. Now, ϕ cannot be in $\mathbf{Q}$ so that the irreducibility of f gives $f = c \cdot \phi$ for $c \neq 0$ in $\mathbf{Q}$. Since both f and ϕ are monic, it follows that $\phi = f$.*

Remark 2.4 *Let α be an algebraic number of degree $n (\geq 1)$ and $f = \sum_{i=0}^{n} a_i X^i (a_n = 1)$ be its minimal polynomial in $\mathbf{Q}[X]$. We now claim that all the roots of f are distinct, i.e. f has no repeated roots. In fact, suppose that $f = (X - \alpha)^2 g$. Then, the derivative f' of f is $2(X-\alpha)g + (X - \alpha)^2 g'$, so that $f'(\alpha) = 0$. Since f is the minimal polynomial of α, this implies that $f | f'$. Since $\deg f' < \deg f$, this is impossible unless $f' = 0$, so that $f \in K$, which is absurd.*

Remark 2.5 *Let α_1 and α_2 be two algebraic numbers with the same minimal polynomial in $\mathbf{Q}[X]$. Then, for any g in $\mathbf{Q}[X]$, we see that $g(\alpha_1) = 0$ if and only if $g(\alpha_2) = 0$. It is easy now to deduce that the mapping $\phi\colon \mathbf{Q}[\alpha_1] \to \mathbf{Q}[\alpha_2]$ defined by*

$$\phi\Big(\sum_{i=0}^{m} a_i\alpha_1^i\Big) = \sum_{i=0}^{m} a_i\alpha_2^i \quad (a_0, a_1, \ldots, a_m \in \mathbf{Q})$$

is an isomorphism of $\mathbf{Q}(\alpha_1)$ onto $\mathbf{Q}(\alpha_2)$. The mapping ϕ is the identity on $\mathbf{Q}$ and takes α_1 to α_2. Conversely, let α_1 be any algebraic number with minimal polynomial f and ϕ an isomorphism of $\mathbf{Q}(\alpha_1)$ into $\mathbf{C}$ such that $\phi(a) = a$, for any $a \in \mathbf{Q}$. Then for any $g \in \mathbf{Q}[X]$, $g(\alpha_1) = 0$ if and only if $g(\phi(\alpha_1)) = 0$. The set of all polynomials in $\mathbf{Q}[X]$ having $\phi(\alpha_1)$ as a root is precisely the ideal $f\mathbf{Q}[X]$ and therefore $\phi(\alpha_1)$ is an algebraic number with f as its minimal polynomial.

Definition 2.5 *Two algebraic numbers α_1 and α_2 as in Remark* 2.5 *above are said to be conjugates of each other (over $\mathbf{Q}$).*

Remark 2.6 *Let K be an algebraic number field of degree n. Then there exists $\theta \in K$ such that $K = \mathbf{Q}(\theta)$. (Observe that such a number θ is an algebraic number of degree n, by Remarks* 2.1 *and* 2.2 *above).*

For proving this, we remark first that the intersection of any family of subfields of a fixed field is again a field, and denote by $\mathbf{Q}(\alpha_1, \ldots, \alpha_p)$ the intersection of all subfields of $\mathbf{C}$ containing $\mathbf{Q}$ and the complex numbers $\alpha_1, \alpha_2, \ldots, \alpha_p$. (This field is also referred to as the subfield of $\mathbf{C}$ generated by $\alpha_1, \alpha_2, \ldots, \alpha_p$ over $\mathbf{Q}$). Since $[K : \mathbf{Q}] = n$, there exist $\omega_1, \omega_2, \ldots, \omega_q (q \leq n)$ in K such that $K = \mathbf{Q}(\omega_1, \ldots, \omega_q)$. By Remarks 2.1 and 2.4 above, $\omega_1, \ldots, \omega_q$. are all "separably algebraic" over $\mathbf{Q}$ i.e. the minimal polynomial of any ω_i has no repeated roots. If $q = 1$, there is nothing to prove. Let first $q = 2$. We shall prove that $K = \mathbf{Q}(\omega_1, \omega_2)$ contains θ_1 such that $K = \mathbf{Q}(\theta_1)$. For simplicity of notation, let us denote ω_1, ω_2 by γ, δ respectively and let f and ϕ be their respective minimal polynomials. By the 'fundamental theorem of algebra', we have $f = (X - \gamma_1)\cdots(X - \gamma_r)$ and $\phi = (X - \delta_1)\cdots(X - \delta_s)$ where we may assume, without loss of generality, that $\gamma = \gamma_1$, $\delta = \delta_1$. Further, by Remark 2.4 above, $\delta_1, \delta_2, \ldots, \delta_s$ are pairwise distinct. Since $\mathbf{Q}$ is infinite, we can find $\lambda \neq 0$ in $\mathbf{Q}$ such that $\gamma_i + \lambda\delta_j \neq \gamma_{i_1} + \lambda\delta_{j_1}$ unless $j = j_1$ and $i = i_1$ (We have just to choose λ in $\mathbf{Q}$ different from 0 and

$-(\gamma_i - \gamma_{i1})/(\delta_j - \delta_{j_1})$ for $j \neq j_1$). Set $\theta_1 = \gamma + \lambda\delta = \gamma_1 + \lambda\delta_1$ and denote $\mathbf{Q}(\theta_1)$ by L; obviously, $L \subset K$. The polynomial $\psi(X) = f(\theta_1 - \lambda X) \in L[X]$ has δ_1 as a root, since $\psi(\delta_1) = f(\theta_1 - \lambda\delta_1) = f(\gamma_1) = 0$. Further, for $i \neq 1, \psi(\delta_i) \neq 0$ since, otherwise, $f(\theta_1 - \lambda\delta_i) = 0$ would give us $\theta_1 - \lambda\delta_i = \gamma_j$ for some j i.e. $\gamma_1 + \lambda\delta_1 = \gamma_j + \lambda\delta_i$ for $i \neq 1$ contrary to our choice of λ. Thus ϕ and ψ have exactly one root γ_1 in common. Let X be the greatest common divisor of ϕ and ψ in $L[X]$. Then every root of χ in $\mathbf{C}$ is a common root of ϕ and ψ. Thus χ is necessarily of degree 1 and hence of the form $\mu(X - \gamma_1)$. In other words, $\mu, \mu\gamma_1 \in L$. i.e. $\gamma_1 = \theta_1 - \lambda\delta_1 \in L(= \mathbf{Q}(\theta_1))$. Therefore γ_1 and $\delta_1 \in L$, i.e. $K \subset L$. This implies that $K = \mathbf{Q}(\theta_1)$. Let now $q \geq 3$. Assume by induction, that every algebraic number field of the form $\mathbf{Q}(\alpha_1, \alpha_2 \ldots, \alpha_r)$ with $r \leq q-1$ contains a number α such that $\mathbf{Q}(\alpha_1, \alpha_2, \ldots, \alpha_r) = \mathbf{Q}(\alpha)$. Then $K_1 = \mathbf{Q}(\omega_1, \omega_2, \ldots, \omega_{q-1}) = \mathbf{Q}(\theta_1)$ for some $\theta_1 \in K_1$. Further $K = K_1(\omega_q) = \mathbf{Q}(\theta_1, \omega_q) = \mathbf{Q}(\theta)$ for some $\theta \in K$(because of the special case $q = 2$ established above).

Remark 2.7 *Let K be an algebraic number field of degree n. Then there exist precisely n distinct isomorphisms $\sigma_1, \sigma_2, \ldots \sigma_n$ of K into $\mathbf{C}$ which are the identity on $\mathbf{Q}$. By Remark* 2.6 *above $K = \mathbf{Q}(\theta)$ for a number $\theta \in K$ whose minimal polynomial f in $\mathbf{Q}[X]$ is of degree n. Let $\theta_1(= \theta)$, $\theta_2, \ldots, \theta_n$ be all the distinct root of f. Then, by Remark 2.5, above, there exists, for each θ_i $(i = 1, 2, \ldots, n)$ an isomorphism σ_i of $\mathbf{Q}(\theta_1)$ onto $\mathbf{Q}(\theta_i) \subset \mathbf{C}$ defined by $\sigma_i\left(\sum_{j=0}^{m} a_j\theta_1^j\right) = \sum_{j=0}^{m} a_j\theta_i^j$ for $a_0, a_1, \ldots a_m \in \mathbf{Q}$. By definition $\sigma_i(a) = a$ for all $a \in \mathbf{Q}, \sigma_1$ is the identity isomorphism of K. Since $\theta_i \neq \theta_j$ for $i \neq j$, the isomorphism $\sigma_1, \sigma_2, \ldots, \sigma_n$ are all distinct. On the other hand, let σ be any isomorphism of $K = \mathbf{Q}(\theta_1)$ into $\mathbf{C}$ which is the identity on $\mathbf{Q}$. By Remark* 2.5 *above, $\sigma(\theta_1) = \theta_i$ for some $i(1 \leq i \leq n)$ and therefore for $a_0, a_1, \ldots, a_m \in \mathbf{Q}$, $\sigma(\sum_{j=0}^{m} a_j\theta_1^j) = \sum_{j=0}^{m} a_j\theta_i^j$. Thus σ is necessarily one of the n isomorphisms $\sigma_1, \sigma_2, \ldots, \sigma_n$.*

Let K be an algebraic number field of degree n, and $\sigma_1, \sigma_2, \sigma_n$ the n distinct isomorphism of K into $\mathbf{C}$. We denote the image $\sigma_i(K)$ of K by $K^{(i)}$ and, for $\alpha \in K$, $\sigma_i(\alpha)$ by $\alpha^{(i)}$. Let σ_1 be the identity isomorphism of K; we have then $K^{(1)} = K$ and $\alpha^{(1)} = \alpha$ for any $\alpha \in K$. Since each σ_i is an isomorphism which is the identity on $\mathbf{Q}$, it follows that $K^{(1)}, \ldots, K^{(n)}$ are again algebraic number fields of degree n. They are referred to as the *"conjugates"* of K. If $K^{(i)} \subset \mathbf{R}$, we call it a *real conjugate* of K and if $K^{(i)} \not\subset \mathbf{R}$, then we call it a complex conjugate

of K. We now claim that the complex conjugates of K occur in pairs, i.e. the distinct isomorphisms $\sigma_i$with $\sigma_i(K) \not\subset \mathbf{R}$ occur in pairs σ, ρ with $\rho = \bar{\sigma}$, where $\bar{\sigma}(\alpha) = \overline{\sigma(\alpha)}$ is the complex conjugate of $\sigma(\alpha)$. For, by Remark 2.6 above, $K = \mathbf{Q}(\theta)$ for some $\theta \in K$. If $K^{(i)} = \sigma_i(K)$ is a complex conjugate of K, then necessarily $\theta^{(i)} = \sigma_i(\theta)$ is a complex number which is not real Now $\theta^{(i)}$ is a root of the minimal polynomial $\sum_{i=0}^{n} a_i X^i$ of θ and, since $a_0, a_1, \ldots, a_n \in \mathbf{Q}$, it follows that the complex conjugate $\overline{\theta^{(i)}}$ of $\theta^{(i)}$ is also a root of $\sum a_i X^i$. Hence by Remark 2.7 above, $\mathbf{Q}(\overline{\theta^{(i)}})$ too occurs among the conjugates $K^{(i)}, \ldots, K^{(n)}$. Let r_1 be the number of real conjugates of K and let s be the number of complex conjugate of K. By the foregoing, $s = 2r_2$ for $r_2 \in \mathbf{Z}^+$. Further we have $r_1 + 2r_2 = n$.

Remark 2.8 *Let K be an algebraic number field and $\omega_1, \omega_2, \ldots, \omega_n$ be a base of K over $\mathbf{Q}$. With the notation introduced above, let Ω denote the n-rowed complex square matrix $(\omega_j^{(i)})$ with $(\omega_1^{(i)}, \omega_2^{(i)}, \ldots, \omega_n^{(i)})$ as its i-th row. Then Ω has an inverse in $\mathcal{M}_n(\mathbf{C})$.*

In fact, $K = \mathbf{Q}(\theta)$ for some algebraic number in K of degree n, by Remark 2.6, above. Further, if $\sigma_1, \sigma_2, \ldots, \sigma_n$ are the distinct isomorphisms of K into $\mathbf{C}$, then $\theta^{(1)} = \sigma_1(\theta) = \theta$, $\theta^{(2)} = \sigma_2(\theta), \ldots, \theta^{(n)} = \sigma_n(\theta)$ are all conjugates of θ (by Remark 2.5, above). Moreover, they are distinct, (by Remark 2.4). Now $\alpha_1 = 1$, $\alpha_2 = \theta, \ldots, \alpha_n = \theta^{n-1}$ form a base of K over $\mathbf{Q}$. Let $A = (\alpha_j^{(i)})$ be the matrix for the base $\alpha_1, \alpha_2, \ldots, \alpha_n$, built as Ω was from the base $\omega_1, \ldots, \omega_n$. Then, $\det A$ is the well-known Vandermonde determinant and is equal to $\pm \prod_{1 \le i < j \le n} (\theta^{(i)} - \theta^{(j)})$, so that $\det A \neq 0$. If $\omega_1, \omega_2, \ldots, \omega_n$ is any base of K over $\mathbf{Q}$, then clearly, for $1 \le i,\ j \le n$, we have $\omega_j^{(i)} = \sum_{k=1}^{n} p_{jk} \alpha_k^{(i)}$ with $p_{jk} \in \mathbf{Q}$. Since both $\{\alpha_1, \alpha_2, \ldots, \alpha_n\}$ and $\{\omega_1, \omega_2, \ldots, \omega_n\}$ form bases of K, it follows that the n-rowed matrix $P = (p_{jk})$ with $(p_{1k}, p_{2k}, \ldots, p_{nk})$ as its kth row has an inverse in $\mathcal{M}_n(\mathbf{Q})$. Clearly, $\Omega = AP$ so that $\det \Omega = \det A \cdot \det P \neq 0$. Thus Ω has in inverse in $\mathcal{M}_n(\mathbf{C})$.

In what follows, we shall prove a few of the important theorems concerning algebraic number fields.

Definition 2.6 *A complex number α is said to be an algebraic integer if α is a root of a monic polynomial in $\mathbf{Z}[X]$.*

Remark 2.9 *An algebraic integer is an algebraic number.*

Remark 2.10 *An element of* $\mathbf{Z}$ *is an algebraic integer.*

Remark 2.11 *If* $\alpha \in \mathbf{Q}$ *is an algebraic integer, then* $\alpha \in \mathbf{Z}$*.*

Remark 2.12 *For any algebraic number* α*, there exists* $m \neq 0$ *in* $\mathbf{Z}$ *such that* $m\alpha$ *is an algebraic integer. (For, if* $\alpha^n + a_{n-1}\alpha^{n-1} + \cdots + a_0 = 0$*, with* $a_0, a_1, \ldots, a_{n-1} \in \mathbf{Q}$ *then take* $m \in \mathbf{Z}$ *such that* $ma_0, ma_1, \ldots, ma_{n-1} \in \mathbf{Z}$*.)*

Definition 2.7 *A polynomial* $f = a_nX^n + \cdots + a_0 \in \mathbf{Z}[X]$ *is said to be primitive if the* $\gcd(a_0, a_1, \ldots, a_n)$ *of* $a_0, a_1, \ldots, a_n$ *is* 1*.*

In particular, a monic polynomial in $\mathbf{Z}[X]$ is primitive. It is clear that any polynomial $f \in \mathbf{Z}[X]$ can be written in the form cg where $c \in \mathbf{Z}$ and g is primitive.

Remark 2.13 *Any polynomial* $f \in \mathbf{Q}[X]$ *can be written in the form* $(a/b)g$ *where* g *is primitive and* $a, b \in \mathbf{Z}$ *are such that* $(a, b) = 1$*.* (a, b) *stands for the g.c.d. of* a *and* b*.*

Lemma 2.1 *(Gauss.) The product of two primitive polynomials in* $\mathbf{Z}[X]$ *is primitive.*

PROOF: Let $\phi = a_nX^n + \cdots + a_0$, $\psi = b_mX^m + \cdots + b_0$ be in $\mathbf{Z}[X]$ with $(a_0, a_1, \ldots, a_n) = 1 = (b_0, b_1, \ldots, b_m)$. Suppose that p is a prime dividing all the coefficients of $f = \phi\psi$. Consider the natural map $\eta\colon \mathbf{Z} \to \mathbf{Z}/(p)$; this induces a homomorphism (which we denote again by) $\eta\colon \mathbf{Z}[X] \to \mathbf{Z}/(p)[X]$. We have $\eta(f) = 0$, while, since the gcd of the coefficients of ϕ, ψ is 1, we have $\eta(\phi) \neq 0$, $\eta(\psi) \neq 0$, so that since $\mathbf{Z}/(p)$ is a field $\mathbf{Z}/(p)[X]$ is an integral domain, and $\eta(f) = \eta(\phi) \cdot \eta(\psi) \neq 0$, a contradiction. Hence f is primitive.

Proposition 2.1 *The following statements are equivalent.*

(*i*) α *is an algebraic integer.*

(*ii*) *The minimal polynomial of* α *is a (monic) polynomial in* $\mathbf{Z}[X]$*.*

(*iii*) $\mathbf{Z}[\alpha]$ *is a finitely generated* $\mathbf{Z}$*-module.*

(*iv*) *There exists a finitely generated* $\mathbf{Z}$*-submodule* $M \neq \{0\}$ *of* $\mathbf{C}$ *such that* $\alpha M \subset M$*.*

PROOF: (i)⇒ (ii). Let $\alpha^n + a_{n-1}\alpha^{n-1} + \cdots + a_0 = 0$ with $a_i \in \mathbf{Z}$ and $\phi = X^n + a_{n-1}X^{n-1} + \cdots + a_0$. Let f be the minimal polynomial of α in $\mathbf{Q}[X]$. By definition, $\phi = f\psi$, where $\psi \in \mathbf{Q}[X]$. Further, by the Remark 2.13 on page 34, let $f = (a/b)f_1$, $\psi = (c/d)\psi_1$ with primitive f_1 and ψ_1 and $a, b, c, d \in \mathbf{Z}$ such that $(a, b) = (c, d) = 1$. Now $bd\phi = acf_1\psi_1$. By Gauss' Lemma, $f_1\psi_1$ is primitive. Let us compare the g.c.d. of the coefficients on both sides. Since ϕ is monic and hence primitive, we have $ac = \pm bd$. Thus $\phi = \pm f_1\psi_1$; comparison of leading coefficients implies that the leading coefficient of f_1 is ± 1; since $f_1(\alpha) = 0$, it follows from the definition of the minimal polynomial that $f = \pm f_1$, so that $f \in \mathbf{Z}[X]$.

(ii)⇒ (iii): Let $\phi = X^n + a_{n-1}X^{n-1} + \cdots + a_0 \in \mathbf{Z}[X]$ be a polynomial with $\phi(\alpha) = 0$. Then clearly $\mathbf{Z}[\alpha]$ is generated by $1, \alpha, \ldots, \alpha^{n-1}$ over $\mathbf{Z}$.

(iii)⇒ (iv): It is obvious that $\alpha\mathbf{Z}[\alpha] \subset \mathbf{Z}[\alpha]$. Take $M = \mathbf{Z}[\alpha]$.

(iv)⇒ (i): Let $M = \mathbf{Z}v_1 + \cdots + \mathbf{Z}v_n \subset \mathbf{C}$ be a finitely generated $\mathbf{Z}$-module such that $\alpha M \subset M$. Then $\alpha v_i = \sum_{j=1}^n a_{ij}v_j$ $(i = 1, 2, \ldots, n)$ with $a_{ij} \in \mathbf{Z}$. Let $A = (a_{ij})$ and $B = \alpha I_n - A = (b_{ij})$. Then $\sum_{j=1}^n b_{ij}v_j = 0$ for $i = 1, 2, \ldots, n$. Let V be a vector space of dimension n over $\mathbf{C}$ and $e_1, e_2, \ldots, e_n$ a base of V. The linear mapping ϕ of V into itself taking e_j to $\sum_{i=1}^n b_{ij}e_i$ $(j = 1, 2, \ldots, n)$ takes the non-zero element $\sum_{j=1}^n v_j e_j$to 0. By the remark 1.23 on page 21, $\det\phi = \det B = 0$. Expanding $\det B = \det(\alpha I_n - A)$, we see that $\alpha^n + a_{n-1}\alpha^{n-1} + \cdots + a_0 = 0$ for $a_0, a_1, \ldots, a_{n-1} \in \mathbf{Z}$.

Proposition 2.1 is now completely proved.

Let K be an algebraic number field. Denote by $\mathcal{O}$ the set of algebraic integers in K. If $\alpha, \beta \in \mathcal{O}$, then $\mathbf{Z}[\alpha]$, $\mathbf{Z}[\beta]$ are finitely generated $\mathbf{Z}$-modules by Proposition 2.1. Hence the ring $M = \mathbf{Z}[\alpha, \beta]$, is a finitely generated $\mathbf{Z}$-module. Since if γ is one of $\alpha \pm \beta$, $\alpha\beta$ we clearly have $\gamma M \subset M$, it follows from Proposition 2.1 that $\alpha \pm \beta$, $\alpha\beta$ are in $\mathcal{O}$ so that $\mathcal{O}$ is a ring. By Remark 2.12 on page 34, K is the quotient field of $\mathcal{O}$.

If α, β are algebraic, there exists $m \in \mathbf{Z}$ such that $m\alpha$, $m\beta$ are algebraic integers, by Remark 2.12. Since $m(\alpha \pm \beta)$ and $m^2\alpha\beta$ are algebraic integers by the considerations above, it follows that $\alpha \pm \beta$ and $\alpha\beta$ are algebraic. Further, if $\alpha \neq 0$ is algebraic, so is α^{-1}. Thus, algebraic numbers form a subfield of $\mathbf{C}$.

Let K be an algebraic number field of degree n and $\omega_1, \ldots, \omega_n$ be a base of K over $\mathbf{Q}$. For any $\alpha \in K$,the mapping $x \mapsto \alpha x$ is a linear mapping of K into itself considered as a vector space over $\mathbf{Q}$. We define the *trace* $\mathrm{Tr}(\alpha) = \mathrm{Tr}_K(\alpha)$, and *norm* $N(\alpha) = N_K(\alpha)$ of the element

α to respectively, the trace and determinant of this linear mapping. If $\alpha w_j = \sum_{i=1}^{n} a_{ij} w_i,\ j = 1, 2, \ldots, n$, and $A = (a_{ij})$, we have $\mathrm{Tr}_K(\alpha) = \mathrm{Tr}(A),\ N_K(\alpha) = \det A$; hence $\mathrm{Tr}_K(\alpha),\ N_K(\alpha) \in \mathbf{Q}$.

For $\alpha \in K,\ (\alpha w_j)^{(k)} = \alpha^{(k)} w_j^{(k)} = \sum_{i=1}^{n} a_{ij} w_i^{(k)}$ for $j = 1, 2, \ldots, n$. Denote the n-rowed square matrix $(w_j^{(k)})$ by Ω, as on page 33, and the n-rowed square matrix $(\alpha^{(i)}\delta_{ij})$ by A_0 where $\delta_{ij} = 1$ for $i = j$ and $\delta_{ij} = 0$ for $i \neq j$. Then we have $A_0\Omega = \Omega A$. Since, by Remark 2.8 on page 33, Ω has an inverse Ω^{-1}, we have $A_0 = \Omega A \Omega^{-1}$. Hence we have

$$N_K(\alpha) = \det A = \det(\Omega A \Omega^{-1}) = \det A_0 = \alpha^{(1)} \cdots \alpha^{(n)}. \tag{2.1}$$

$$\mathrm{Tr}_K(\alpha) = \mathrm{Tr}(A) = \mathrm{Tr}(\Omega A \Omega^{-1}) = \mathrm{Tr}(A_0) = \alpha^{(1)} + \cdots + \alpha^{(n)}.$$

Further, if A corresponds to $\alpha \in K,\ B$ to $\beta \in K$, then to $\alpha + \beta$ corresponds $A + B$ and to $\alpha\beta,\ AB$ Hence the mapping $\alpha \mapsto A$ is a homomorphism of K into $\mathfrak{M}_n(\mathbf{Q})$. It is called a *regular representation* of K (viz. that corresponding to the base $w_1, \ldots, w_n$ of K.) We verify immediately that if $\alpha, \beta \in K$, we have

$$\mathrm{Tr}_K(\alpha + \beta) = \mathrm{Tr}_K(\alpha) + \mathrm{Tr}_K(\beta) \ \text{ and } N_K(\alpha\beta) = N_K(\alpha) N_K(\beta).$$

Let α be an algebraic integer in K. By Proposition 2.1, we can suppose that the minimal polynomial of α is $X^m + a_{m-1}X^{m-1} + \cdots + a_0$ where $a_0, a_1, \ldots, a_{m-1} \in \mathbf{Z}$. Now α is of degree m and $\mathbf{Q}(\alpha)$ has $1, \alpha, \ldots, \alpha^{m-1}$ as a base over $\mathbf{Q}$. (Clearly $m \leq n$.) Let $A \in \mathfrak{M}_n(\mathbf{Q})$ correspond to α in the regular representation of $\mathbf{Q}(\alpha)$, with respect to the base $1, \alpha, \ldots, \alpha^{m-1}$ of $\mathbf{Q}(\alpha)$. Let $\beta_1, \beta_2, \ldots, \beta_l$ be a base of K considered as a vector space over $\mathbf{Q}(\alpha)$. Then $\beta_1, \beta_1\alpha, \ldots, \beta_1\alpha^{m-1}, \beta_2, \beta_2\alpha, \ldots, \beta_2\alpha^{m-1}$, $\ldots, \beta_l, \ldots, \beta_l\alpha^{m-1}$ constitute a base of K over $\mathbf{Q}$. (Incidentally $l \cdot m = n$ and so $m \mid n$.) Let A_1 correspond to α in the regular representation of K with respect to this $\mathbf{Q}$-base. Then

$$A_1 = \begin{pmatrix} A & 0 & \cdots & 0 \\ 0 & A & \cdots & 0 \\ 0 & 0 & \cdots & A \end{pmatrix} \in \mathfrak{M}_n(\mathbf{Q}) \text{ and } \mathrm{Tr}(A_1) = l \cdot \mathrm{Tr}(A).$$

Since α is an algebraic integer, all the elements of A are in $\mathbf{Z}$ so that $\mathrm{Tr}(A)$ and $\mathrm{Tr}(A_1) = l \cdot \mathrm{Tr}(A) = l a_{m-1}$ are integers. Thus, for an *algebraic integer* $\alpha \in K$, $\mathrm{Tr}_K(\alpha)$ *is an integer. Similarly,* $N_K(\alpha) = \det A_1 = (\det A)^l \in \mathbf{Z}$.

The mapping $\alpha \mapsto \mathrm{Tr}_K(\alpha)$ is clearly a $\mathbf{Q}$-linear mapping of K into $\mathbf{Q}$. We define a bilinear form $B(x, y)$ on the $\mathbf{Q}$-vector space K by setting $B(x, y) = \mathrm{Tr}_K(xy)$ for $x, y \in K$.

Proposition 2.2 *The bilinear form* $B(x,y) = \mathrm{Tr}_K(xy)$ *for* $x, y \in K$ *is non-degenerate.*

PROOF: Let $x \neq 0$ be in K. Then $B''_x(y) = \mathrm{Tr}_K(xy)$ is not identically zero in y, since, for $y = x^{-1}$, $B'_x(x^{-1}) = \mathrm{Tr}_K(1) = n$. Similarly for $y \neq 0$ in K, $B'_y(x)$ is not identically zero in x.

If we apply Proposition 1.6 to this bilinear form on $V = K$, we obtain the

Corollary 2.1 *To any* $\mathbf{Q}$*-base* $w_1, \ldots, w_n$ *of* K*, there corresponds a base* $w'_1, \ldots, w'_n$ *such that* $\mathrm{Tr}_K(w_i, w'_j) = \delta_{ij},\ 1 \leq i,\ j \leq n$.

If R is a subset of K and if $a \in K$ then, by definition,

$$aR = \{ar \mid r \in R\}.$$

The following theorem gives more information concerning the structure of the ring of algebraic integers in a given algebraic number field.

Theorem 2.1 *Let* K *be an algebraic number field of degree* n *and* $\mathcal{O}$ *the ring of algebraic integers in* K*. Then there exists a* $\mathbf{Q}$*-base* $\omega_1, \ldots, \omega_n$ *of* K *such that* $\omega_i \in \mathcal{O}$ *and* $\mathcal{O} = \mathbf{Z}\omega_1 + \cdots + \mathbf{Z}\omega_n$.

(Elements $\omega_1, \ldots, \omega_n$ with this property are said to form an integral base of $\mathcal{O}$.)

PROOF: Let $w_1, \ldots, w_n$ be a $\mathbf{Q}$-base of K. By Remark 2.12 on page 34 there exists $m \neq 0$ in $\mathbf{Z}$ such that $mw_1, \ldots, mw_n$ are in $\mathcal{O}$. We can thus assume without loss of generality that $w_1, \ldots, w_n$ are already in $\mathcal{O}$. Let $w'_1, \ldots, w'_n$ be a base of K for which

$$\mathrm{Tr}_K(w_i, W'_j) = \delta_{ij} \quad (1 \leq i,\ j \leq n). \tag{2.2}$$

We know that for any $z \in \mathcal{O},\ z = \sum_{i=1}^n a_i w'_i$ with $a_1, \ldots, a_n \in \mathbf{Q}$. Since $zw_i \in \mathcal{O}$ for $1 \leq i \leq n$, we have, because of (2.2), $a_i = \mathrm{Tr}_K(zw_i) \in \mathbf{Z}$. Thus we obtain

$$\mathcal{O} \subset \mathbf{Z}w'_1 + \cdots + \mathbf{Z}w'_n.$$

By Proposition 1.4 (Chapter 1) there exist $\omega_1, \ldots, \omega_m \in \mathcal{O},\ m \leq n$, such that

$$\mathcal{O} = \mathbf{Z}\omega_1 + \cdots + \mathbf{Z}\omega_m.$$

We claim that, necessarily, $m = n$. In fact, if $m < n$, then, the $\mathbf{Q}$-subspace of K generated by $\omega_1, \ldots, \omega_m$, which is clearly K itself, would

have dimension $\leq m < n$ over $\mathbf{Q}$, contrary to our assumption that K is of degree n. Further, we see that $\omega_1, \ldots, \omega_n$ are $\mathbf{Q}$-independent, so that, necessarily, the sum above is direct. This proves Theorem 2.1.

Remark 2.14 *Any set of elements $\omega_1, \ldots, \omega_n$ as above forms a $\mathbf{Q}$-base of K. We have only to repeat the argument in the last few lines above.*

Remark 2.15 *Let $\mathfrak{a}$ be any non-zero ideal in $\mathcal{O}$. Then $\mathfrak{a} \cap \mathbf{Z} \neq \{0\}$. In fact if $\alpha \neq 0$ is an algebraic integer in $\mathfrak{a}$ and if $\alpha^r + a_{r-1}\alpha^{r-1} + \cdots + a_0 = 0$ where $a_i \in \mathbf{Z},\ a_0 \neq 0$, then $a_0 = -\alpha(a_1 + \cdots + a^{r-1}) \in \mathbf{Z}$. It follows that for any $\alpha \in K$, there is $a \in \mathbf{Z},\ a \neq 0$ such that $a\alpha \in \mathfrak{a}$.*

If $\omega_1, \ldots, \omega_n$ are as in Theorem 2.1, then $\mathfrak{a} \subset \mathcal{O} = \mathbf{Z}\omega_1 + \cdots + \mathbf{Z}\omega_n$. By Proposition 1.4 (Chapter 1), there exist $\alpha_1, \ldots, \alpha_m \in \mathfrak{a},\ m \leq n$, such that

$$\mathfrak{a} = \mathbf{Z}\alpha_1 + \cdots + \mathbf{Z}\alpha_m.$$

As in Remark 2.14,we must have $m = n$. The α_i are said to constitute an *integral base* of $\mathfrak{a}$.

Further, we may choose the α_i so that $\alpha_i = \sum_{j \geq i} p_{ij}\omega_j,\ p_{ij} \in \mathbf{Z}$.

Remark 2.16 *As in Remark* 2.14*, any elements $\alpha_1, \ldots, \alpha_n$ such that $\mathfrak{a} = \mathbf{Z}\alpha_1 + \cdots + \mathbf{Z}\alpha_n$ form a $\mathbf{Q}$-base of K. In particular, any non-zero ideal of $\mathfrak{a}$ contains n elements which are linearly independent over $\mathbf{Q}$. It follows that if $\alpha_i = \sum_{j \geq i} p_{ij}\omega_j$,then $p_{ii} \neq 0$.*

Remark 2.17 *If $\mathfrak{a} \neq \{0\}$ is an ideal of $\mathcal{O}$, then by Remark* 2.15*, there exists $0 \neq a \in \mathbf{Z}$ such that $a\mathcal{O} \subset \mathfrak{a} \subset \mathcal{O}$. Now if $\mathcal{O} = \mathbf{Z}\omega_1 + \cdots + \mathbf{Z}\omega_n$, then $a\mathcal{O} = \mathbf{Z}a\omega_1 + \cdots + \mathbf{Z}a\omega_n$ so that $\mathcal{O}/a\mathcal{O}$ is of order a^n. Therefore $\mathcal{O}/a$ is also finite.*

Remark 2.18 *If $\mathfrak{p}$ is a prime ideal in $\mathcal{O}$ then $\mathfrak{p}$ contains exactly one prime number $p > 0$ of $\mathbf{Z}$.*

In fact, let $a = p_1 \cdots p_k$ in $\mathfrak{p} \cap \mathbf{Z}$ with primes $p_1, \ldots, p_k \in \mathbf{Z}$. Since $\mathfrak{p}$ is prime, at least one $p_i \in \mathfrak{p}$. If p, q are distinct primes in $\mathfrak{p}$, we can find integers x, y with $xp + yq = 1$; then $1 \in \mathfrak{p}$ and $\mathfrak{p} = \mathcal{O}$, a contradiction.

Definition 2.8 *For any ideal $\mathfrak{a} \neq \{0\}$ of $\mathcal{O}$, the number of elements in the residue class ring $\mathcal{O}/\mathfrak{a}$ is called the norm of $\mathfrak{a}$ and denoted by $N(\mathfrak{a})$; if $\mathfrak{a} = \{0\}$ we set $N(\mathfrak{a}) = 0$.*

Clearly $N(\mathcal{O}) = 1$. For a proper ideal $\mathfrak{a}$ of $\mathcal{O}$, $N(\mathfrak{a}) > 1$.

Proposition 2.3 *Let $\mathfrak{a} \neq \{0\}$ be an ideal of $\mathcal{O} = \mathbf{Z}\omega_1 + \cdots + \mathbf{Z}\omega_n$. Then there exist $\alpha_i = \sum_{j=1}^{n} p_{ij}\omega_j$, $p_{ii} > 0$, $p_{ij} \in \mathbf{Z}$ such that $\mathfrak{a} = \mathbf{Z}\alpha_1 + \cdots + \mathbf{Z}\alpha_n$. Further $N(\mathfrak{a}) = p_{11}p_{22}\cdots p_{nn}$.*

Proof: By Remark 2.15 above, $\mathfrak{a}$ has an integral base $\alpha_1, \ldots, \alpha_n$ of the required form.

We claim that the $p_{11}p_{22}\cdots p_{nn}$ numbers

$$\eta = \eta(x_1, \ldots, x_n) = \sum_{i=1}^{n} x_i\omega_i, \quad 0 \leq x_i < p_{ii},\ x \in \mathbf{Z}$$

form a complete system of residue of $\mathcal{O}$ modulo $\mathfrak{a}$, In fact, if

$$\xi = \sum_{i=1}^{n} c_i\omega_i \in \mathcal{O}, \quad c_i \in \mathbf{Z},$$

and we set $\mathcal{O}_i = \mathcal{O} \cap (\mathbf{Z}\omega_{i+1} + \cdots + \mathbf{Z}\omega_n)$, then there exist x_1, $0 \leq x_1 < p_{11}$ and $m_1 \in \mathbf{Z}$ with

$$\xi_1 = \xi - x_1\omega_1 - m_1\alpha_1 \in \mathcal{O}_1;$$

further, x_1, m_1 are determined by the relation

$$c_1 = m_1p_{11} + x_1.$$

We can, in the same way, find $m_2 \in \mathbf{Z}$, $0 \leq x_2 < p_{22}$ with

$$\xi_2 = \xi_1 - x_2\omega_2 - m_2\alpha_2 \in \mathcal{O}_2;$$

continuing in this way, we find that

$$\xi = \sum_{i=1}^{n} (m_i\alpha_i + x_i\omega_i),\ m_i \in \mathbf{Z},\ 0 \leq x_i < p_{ii},$$

so that the η generate $\mathcal{O}$ modulo $\mathfrak{a}$.

Now, if $\sum_{i=1}^{n} x_i\omega_i = \sum_{i=1}^{n} m_i\alpha_i$, where $m_i \in \mathbf{Z}$, $0 \leq x < p_{ii}$, we note that $\sum_{i=1}^{n} m_i\alpha_i = \sum_{i=1}^{n} c_i\omega_i$, where $c_1 = m_ip_{11}$. Since the ω_i are linearly independent, we have $x_1 = m_1p_{11}$ and since $0 \leq x_1 < p_{11}$, we conclude that $m_1 = x_1 = 0$. This implies that $c_2 = m_2p_{22}$, which in turn implies that $x_2 = m_2 = 0$, and so on; hence $x_i = 0$. This proves that the η's are distinct modulo $\mathfrak{a}$ and with it, the proposition.

2.2 Unique Factorization Theorem

Let K be an algebraic number field of degree n and $\mathcal{O}$ the ring algebraic integers in K . Let $\mathfrak{p}$ be a prime ideal in $\mathcal{O}$. Then $\mathcal{O}/\mathfrak{p}$ is finite and indeed a commutative integral domain with 1, by Remark 1.18 on page 18. By Example 1.13, page 8, $\mathcal{O}/\mathfrak{p}$ is a field. Thus:

(D_1) *Every prime ideal of* $\mathcal{O}$ *is maximal.*

We say that an element $\alpha \in \mathbf{C}$ is *integral over* $\mathcal{O}$ if there exists a monic polynomial f with coefficients in $\mathcal{O}$ such that $f(\alpha) = 0$. As in Proposition 2.1, one can prove that $\alpha \in \mathbf{C}$ is integral over $\mathcal{O}$ if and only if there is a non-zero finitely generated $\mathcal{O}$-module $M \subset \mathbf{C}$ with $\alpha M \subset M$ (alternatively, if and only if $\mathcal{O}[\alpha]$ is finitely generated over $\mathcal{O}$.) By Theorem 2.1, such a module M is finitely generated over $\mathbf{Z}$, and consequently an element $\alpha \in \mathbf{C}$ *integral over* $\mathcal{O}$ *is an algebraic integer.*

It follows at once that, if K is an algebraic number field and $\mathcal{O}$ the ring of algebraic integers in K, then any $\alpha \in K$ *which is integral over* $\mathcal{O}$ *belongs to* $\mathcal{O}$. If we define, for any integral domain R the *integral closure of* R *in its quotient field* as the set of all elements of the quotient field of R which are roots of monic polynomials with coefficients in R, we can therefore assert the following:

(D_2) *The integral closure of* $\mathcal{O}$ *in* K *is* $\mathcal{O}$ *itself.*

To each ideal $\mathfrak{a} \neq \{0\}$, associate its norm $N(\mathfrak{a}) > 0$ in $\mathbf{Z}$. The mapping $N\colon \mathfrak{a} \mapsto N(\mathfrak{a})$ is, in general, not one-one. However, if $\mathfrak{a} \subset \mathfrak{b}$ and $\mathfrak{a} \neq \mathfrak{b}$, then $N(\mathfrak{a}) > N(\mathfrak{b})$. [For, let $f\colon (\mathcal{O}/\mathfrak{a}, +) \to (\mathcal{O}/\mathfrak{b}, +)$ be the map defined by $f(x + \mathfrak{a}) = x + \mathfrak{b}$. Then f is well-defined, onto $(\mathcal{O}/\mathfrak{b}, +)$ but is *not one-one* since there exists $y \in \mathfrak{b},\ y \notin \mathfrak{a}$. We deduce at once the following statements.

(N1) If $\mathfrak{a}_1 \subset \mathfrak{a}_2 \subset \cdots \subset \mathfrak{a}_n \subset \mathfrak{a}_{n+1} \subset \cdots$ is an increasing sequence of ideals in $\mathcal{O}$ then $\mathfrak{a}_m = \mathfrak{a}_{m+1}$ for $m \geq m_0 \in \mathbf{Z}^+$.

(N2) Any non-empty set $\mathcal{S}$ of ideals in $\mathcal{O}$ contains a maximal element, i.e. an ideal $\mathfrak{a}$ such that $\mathfrak{a} \not\subset \mathfrak{b}$ for any $\mathfrak{b} \in \mathcal{S},\ \mathfrak{b} \neq \mathfrak{a}$. (For, any set of positive integers contains a least element.)

(N3) Any ideal $\mathfrak{a}$ in $\mathcal{O}$ with $\mathfrak{a} \neq \mathcal{O}$ is contained in a maximal ideal of $\mathcal{O}$.

(Take for $\mathcal{S}$ in (N2) the set of all proper ideals $\mathfrak{b}$ with $\mathfrak{a} \subset \mathfrak{b} \subset \mathcal{O}$.)

Remark 2.19 *A ring* R *is noetherian if the statement* $(N1)$ *is true of ideals in* R. *One can show that* R *is noetherian if and only if statement* $(N2)$ *is true of ideals in* R. *This is further equivalent to the statement that any ideal of* R *is finitely generated (as an* R*-module). Statement*

$(N3)$ is true in arbitrary (even non-commutative) rings with unity, and, in this generality, is due to Krull.

We have thus proved that

(D_3) $\mathcal{O}$ is noetherian.

Any commutative integral domain R satisfying the conditions (D_1), $(D_2), (D_3)$ is known as a *Dedekind domain* and these conditions are themselves known as *axioms of classical ideal-theory.* The ring of algebraic integers in an algebraic number field is therefore a Dedekind domain.

Definition 2.9 *By a fractional ideal in K, we mean an $\mathcal{O}$ submodule $\mathfrak{a}$ of K for which there exists $m \neq 0$ in $\mathbf{Z}$ such that $m\mathfrak{a} \subset \mathcal{O}$.*

Any ideal in $\mathcal{O}$ is trivially a fractional ideal. By analogy with $\mathbf{Z}$ we may call an ideal in $\mathcal{O}$ an *integral ideal* in K. Any fractional ideal $\mathfrak{a}$ can be written as $a^{-1}\mathfrak{b}$ for $a \neq 0$ in $\mathbf{Z}$ and an integral ideal $\mathfrak{b}$. If $\mathfrak{c}$ is an integral ideal, then for any $b \neq 0$ in $\mathbf{Z}$, $b^{-1}\mathfrak{c}$ is clearly a fractional ideal in K. If $\mathfrak{c}, \mathfrak{d}$, are fractional ideals in K, then for a suitable $c \in \mathbf{Z}$, $c \neq 0$, $c\mathfrak{c}, c\delta$ are both integral ideals and the sum $\mathfrak{c} + \mathfrak{d} = c^{-1}(c\mathfrak{c} + c\mathfrak{d})$ and the product $\mathfrak{c}\mathfrak{d} = c^{-2}(c\mathfrak{c} \cdot c\mathfrak{d})$ are again fractional ideals in K.

We now prove the important

Theorem 2.2 *(Dedekind.) Any proper ideal of the ring $\mathcal{O}$ of algebraic integers in an algebraic number field K can be written as the product of prime ideals in $\mathcal{O}$ determined uniquely upto order.*

For the proof of the theorem, we need two lemmas.

Lemma 2.2 *Any proper ideal $\mathfrak{a} \subset \mathcal{O}$ contains a product of prime ideals in $\mathcal{O}$.*

Proof: Let $\mathcal{S}$ be the set of proper integral ideals not containing a product of prime ideals. If $\mathfrak{s} \neq \emptyset$, then by statement (N2), $\mathcal{S}$ contains a maximal element, say $\mathfrak{a}$. Clearly $\mathfrak{a}$ cannot be prime. Thus there exist $x_1, x_2 \in \mathcal{O}$, $x_1x_2 \in \mathfrak{a}$ but $x_1, x_2 \notin \mathfrak{a}$. Let $\mathfrak{a}_i$ $(i = 1, 2)$ be the ideal generated by $\mathfrak{a}$ and x_i. Then a_1 and $\mathfrak{a}_2$ contain $\mathfrak{a}$ properly. By the maximality of $\mathfrak{a}$ in $\mathfrak{s}$, $\mathfrak{a}_1 \notin \mathcal{S}$, $\mathfrak{a}_2 \notin \mathcal{S}$. Hence $\mathfrak{a}_1 \supset \mathfrak{p}_1\mathfrak{p}_2 \cdot \mathfrak{p}_r$ and $\mathfrak{a}_2 \supset \mathfrak{q}_1 \cdots \mathfrak{q}_s$ where $\mathfrak{p}_1, \ldots \mathfrak{p}_r, \mathfrak{q}_1, \ldots, \mathfrak{q}_s$ are prime ideals in $\mathcal{O}$. Since $\mathfrak{a}_1\mathfrak{a}_2 \subset \mathfrak{a}$, we have $\mathfrak{p}_1 \cdots \mathfrak{p}_r\mathfrak{q}_1 \cdots \mathfrak{q}_3 \subset \mathfrak{a}$ giving us a contradiction. Hence $\mathcal{S} = \emptyset$.

Lemma 2.3 *Any prime ideal $\mathfrak{p} \subset \mathcal{O}$ is invertible, i.e. there exists a fractional ideal $\mathfrak{p}^{-1}$ such that $\mathfrak{p}\mathfrak{p}^{-1} = \mathcal{O}$.*

PROOF: Let $\mathfrak{p}^{-1}$ be the set of $x \in K$ such that $x\mathfrak{p} \subset \mathcal{O}$. Clearly $\mathfrak{p}^{-1}$ is an $\mathcal{O}$-module containing $\mathcal{O}$. Since $\mathfrak{p}$ contains $n \neq 0$ in $\mathbf{Z}$ (see Remark 2.15 on page 38), we have $n\mathfrak{p}^{-1} \subset \mathfrak{p}^{-1}\mathfrak{p} \subset \mathcal{O}$. Hence $\mathfrak{p}^{-1}$ is a fractional ideal. Now $\mathfrak{p} \subset \mathfrak{p}\mathfrak{p}^{-1} \subset \mathcal{O}$. Since $\mathfrak{p}$ is maximal, either $\mathfrak{p}\mathfrak{p}^{-1} = \mathcal{O}$ in which case our lemma will be proved or $\mathfrak{p} = \mathfrak{p}\mathfrak{p}^{-1}$.

If $\mathfrak{p} = \mathfrak{p}\mathfrak{p}^{-1}$, then every $x \in \mathfrak{p}^{-1}$ satisfies $x\mathfrak{p} \subset \mathfrak{p}$. Since $\mathfrak{p}$ is a finitely generated $\mathbf{Z}$-module (vide Remark 2.15 on page 38), we see that $x \in \mathcal{O}$ in view of Proposition 2.1. Hence $\mathfrak{p}^{-1} \subset \mathcal{O}$ i.e. $\mathfrak{p}^{-1} = \mathcal{O}$. This, as we now show, is impossible. Take $x \in \mathfrak{p}$ such that $x\mathcal{O} \neq \mathcal{O}$. Then $x\mathcal{O}$ is a proper integral ideal and by Lemma 2.2, $\mathfrak{p}_1 \cdots \mathfrak{p}_r \subset x\mathcal{O}$ for prime ideals $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$. Assume r so chosen that $x\mathcal{O}$ does not contain a product of $r-1$ prime ideals in $\mathcal{O}$. Now $\mathfrak{p} \supset x\mathcal{O} \supset \mathfrak{p}_1 \cdots \mathfrak{p}_r$. By Remark 1.19 on page 19 $\mathfrak{p}$ divides one of $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$, say $\mathfrak{p}_1$. But by Property (D_1), $\mathfrak{p} = \mathfrak{p}_1$. Now $\mathfrak{p}_2 \cdots \mathfrak{p}_r$, is not contained in $x\mathcal{O}$, by minimality of r. Hence there exists $b \in \mathfrak{p}_2 \cdots \mathfrak{p}_r$, $b \notin x\mathcal{O}$, i.e. $x^{-1}b \notin \mathcal{O}$. But since $bx^{-1}\mathfrak{p} \subset \mathfrak{p}_2 \cdots \mathfrak{p}_r(x^{-1}\mathcal{O})\mathfrak{p} = x^{-1}\mathcal{O} \cdot \mathfrak{p}_1 \cdots \mathfrak{p}_r \subset x^{-1}\mathcal{O} \cdot x\mathcal{O} = \mathcal{O}$, we have $bx^{-1} \in \mathfrak{p}^{-1}$. But $x^{-1}b \in \mathcal{O}$, i.e. $\mathfrak{p}^{-1} \neq \mathcal{O}$. Thus $\mathfrak{p}\mathfrak{p}^{-1} = \mathcal{O}$.

We may now give the following

PROOF OF THEOREM 2.2. As in Proposition 1.7, the proof is split into two parts.

(i) *Existence of a factorization.* Let $\mathcal{S}$ be the set of proper ideals of $\mathcal{O}$ which cannot be factorized into prime ideals. We have to show that $\mathcal{S} = \emptyset$. Suppose then that $\mathcal{S} \neq \emptyset$. Then by (N2) $\mathcal{S}$ contains a maximal element say $\mathfrak{a} \subset \mathcal{O}$. Now obviously, $\mathfrak{a}$ cannot be prime. Hence by (N3) $\mathfrak{a} \subset \mathfrak{p}$, $\mathfrak{a} \neq \mathfrak{p}$ where $\mathfrak{p}$ is prime. By Lemma 2.3, there exists an ideal $\mathfrak{p}^{-1}$ such that $\mathfrak{p}\mathfrak{p}^{-1} = \mathcal{O}$. Thus $\mathfrak{a}\mathfrak{p}^{-1}$ is a proper ideal in $\mathcal{O}$ and contains $\mathfrak{a}$ properly since $\mathfrak{p}^{-1}$ contains $\mathcal{O}$ properly. But if $\mathfrak{a}\mathfrak{p}^{-1} = \mathfrak{p}_1 \cdots \mathfrak{p}_r$ for prime ideals $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ then $\mathfrak{a} = \mathfrak{p}\mathfrak{p}_1 \cdots \mathfrak{p}_r$ contradicting the assumption that $\mathfrak{a} \in \mathcal{S}$. Hence $\mathfrak{a}\mathfrak{p}^{-1} \in \mathcal{S}$ but this contradicts the maximality of $\mathfrak{a}$ in $\mathcal{S}$. Thus $\mathcal{S} = \emptyset$, i.e. every proper ideal of $\mathcal{O}$ can be factorized into prime ideals.

(ii) *Uniqueness of factorization.* If possible, let a proper ideal $\mathfrak{a}$ in $\mathcal{O}$ have two factorizations $\mathfrak{a} = \mathfrak{p}_1 \cdots \mathfrak{p}_r = \mathfrak{q}_1 \cdots \mathfrak{q}_r$ where $\mathfrak{p}_1, \ldots, \mathfrak{p}_r, \mathfrak{q}_1, \ldots, \mathfrak{q}_s$, are prime ideals. This means that $\mathfrak{q}_1$ divides $\mathfrak{p}_1 \cdots \mathfrak{p}_r$ and by Remark 1.19, $\mathfrak{q}_1$ divides one of the ideals $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ say $\mathfrak{p}_1$. But since $\mathfrak{p}_1$ is maximal, $\mathfrak{q}_1 = \mathfrak{p}_1$. Now by Lemma 2.3, $\mathfrak{q}_1^{-1}\mathfrak{a} = \mathfrak{q}_1^{-1}\mathfrak{q}_1 \cdots \mathfrak{q}_s = \mathfrak{q}_2 \cdots \mathfrak{q}_s$ and $\mathfrak{q}_1^{-1}\mathfrak{a} = \mathfrak{p}_1^{-1}\mathfrak{p}_1 \cdots \mathfrak{p}_r = \mathfrak{p}_2 \cdots \mathfrak{p}_r$. Thus $\mathfrak{p}_2 \cdots \mathfrak{p}_r = \mathfrak{q}_2 \cdots \mathfrak{q}_s$. By repeating the

argument above, $\mathfrak{q}_2$ is equal to one of the prime ideals $\mathfrak{p}_2, \ldots, \mathfrak{p}_r$, say $\mathfrak{p}_2$. In finitely many steps, we can thus prove that $r = s$ and that $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ coincide with $\mathfrak{q}_1, \ldots, \mathfrak{q}_r$ upto order.

Corollary 2.2 *Any fractional ideal $\mathfrak{a}$ can be written uniquely in the form*

$$\mathfrak{a} = \frac{\mathfrak{q}_1 \cdots \mathfrak{q}_s}{\mathfrak{p}_1 \cdots \mathfrak{p}_r} \quad \left(\frac{1}{\mathfrak{p}} \text{ stands for } \mathfrak{p}^{-1}\right)$$

where the $\mathfrak{q}_i$, $\mathfrak{p}_j$ are prime; and no $\mathfrak{q}_i$ is a $\mathfrak{p}_j$.

This follows immediately if we choose $c \neq 0$, $c \in \mathbf{Z}$ with $\mathfrak{b} = c\mathfrak{a} \subset \mathcal{O}$, and write $(c) = \mathfrak{p}_1 \cdots \mathfrak{p}_r$, $\mathfrak{b} = \mathfrak{q}_1 \cdots \mathfrak{q}_{s'}$ and 'cancel' equal $\mathfrak{q}_i$ and $\mathfrak{p}_j$ in pairs.

Corollary 2.3 *Given any fractional ideal $\mathfrak{a} \neq \{0\}$ in K, there exists a fractional ideal $\mathfrak{a}^{-1}$ such that $\mathfrak{a}\mathfrak{a}^{-1} = \mathcal{O}$.*

For proving this, it suffice to show that every integral ideal is invertible. But this is an immediate consequence of Theorem 2.2 and Lemma 2.3.

Remark 2.20 *Let $\mathfrak{a} = \mathfrak{p}_1^{a_1} \cdots \mathfrak{p}_r^{a_r}$, $\mathfrak{b} = \mathfrak{p}_1^{b_1} \cdots \mathfrak{p}_r^{b_r}$ be integral ideals $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ being prime ideals $a_1, \ldots, a_r, b_1, \ldots, b_r \in \mathbf{Z}^+$. (We define $\mathfrak{p}_i^0 = \mathcal{O}$, $i = 1, 2, \ldots, r$.) The greatest common divisor $(\mathfrak{a}, \mathfrak{b})$ of $\mathfrak{a}$ and $\mathfrak{b}$ is defined to be $\mathfrak{p}_1^{c_1} \cdots \mathfrak{p}_r^{c_r}$ where $c_i = \min(a_i, b_i)$ $i = 1, 2, \ldots, r$. Clearly c_i is the largest integer c such that $\mathfrak{p}_i^c$ divides both $\mathfrak{a}$ and $\mathfrak{b}$. But now if $\mathfrak{c}, \mathfrak{d}$ are integral ideals then $\mathfrak{c}$ divides $\mathfrak{d}$ if and only if $\mathfrak{d} = \mathfrak{c}\mathfrak{c}_1$ for $\mathfrak{c}_1 \subset \mathcal{O}$. (For, if $\mathfrak{c} \supset \mathfrak{d}$, then $\mathfrak{c}_1 = \mathfrak{d}\mathfrak{c}^{-1} \subset \mathcal{O}$ and conversely if $\mathfrak{d} = \mathfrak{c}\mathfrak{c}_1$ with $\mathfrak{c}_1 \subset \mathcal{O}$ then $\mathfrak{c} \supset \mathfrak{d}$.) Thus the greatest common divisor of $\mathfrak{a}$ and $\mathfrak{b}$ is actually the smallest ideal dividing $\mathfrak{a}$ and $\mathfrak{b}$ which is nothing but $\mathfrak{a} + \mathfrak{b}$. For any set of s ideals $\mathfrak{a}_1, \ldots, \mathfrak{a}_s$ the greatest common divisor of $\mathfrak{a}_1, \ldots, \mathfrak{a}_s$ may be similarly defined.*

2.3 The class group of K

Let K be an algebraic number field of degree n. By Corollary 2.3 to Theorem 2.2, the non-zero fractional ideals in K form a multiplicative group which we denote by Δ. The ring $\mathcal{O}$ of algebraic integers is the identity element of Δ.

A fractional ideal in K is said to be principal if it is of the form $\alpha\mathfrak{O}$ with $\alpha \in K$. Clearly the principal (fractional) ideals $\mathfrak{a} \neq \{0\}$ form a subgroup Π of Δ. The quotient group $\mathfrak{h} = \Delta/\Pi$ is called the *group of ideal classes* in K or briefly the class group of K.

Definition 2.10 *Two ideals $\mathfrak{a}, \mathfrak{b} \neq \{0\}$ in K are in the same ideal class, or are equivalent if and only if $\mathfrak{a} = (\alpha)\mathfrak{b}$ for some $\alpha \in K$.*

We shall prove in this section that $\mathfrak{h}$ is a *finite group.* The order denoted by $h\,(= h(K))$ is called the class number of K.

If $h = 1$, then $\mathfrak{O}$ is a principal ideal domain.

For proving that h is finite, we need a few lemmas.

Let $\mathfrak{a}$ be an integral ideal in K and let

$$\mathfrak{a} = \mathbf{Z}\alpha_1 + \cdots + \mathbf{Z}\alpha_n = \mathbf{Z}\beta_1 + \cdots + \mathbf{Z}\beta_n \text{ with } \alpha_1, \ldots, \alpha_n,\ \beta_1, \ldots, \beta_n \in \mathfrak{a}.$$

Clearly $\alpha_i = \sum_{j=1}^{n} q_{ij}\beta_j,\ q_{ij} \in \mathbf{Z}$ and $\beta_i = \sum_{j=1}^{n} r_{ij}\alpha_j,\ r_{ij} \in \mathbf{Z}$ for $i = 1, 2, \ldots, n$. Denoting the n-rowed square matrices $(q_{ij}),\ (r_{ij})$ by Q, R respectively, we see that if $QR = (s_{ij})$, then $\alpha_i = \sum_{j=1}^{n} s_{ij}\alpha_j$. By Remark 2.16 after Theorem 2.1, $\alpha_1, \ldots, \alpha_n$ are linearly independent over $\mathbf{Q}$. Thus $s_{ij} = \delta_{ij}$ (the Kronecker delta) for $1 \leq i,\ j \leq n$ i.e. $QR = I_n$. Taking determinants, it follows that $\det Q \cdot \det R = 1$ and since $\det Q \cdot \det R \in \mathbf{Z}$, we have $\det Q = \det R = \pm 1$.

We now use the foregoing remarks to identity the norm $N((\alpha))$ of the principal ideal (α) generated by $\alpha \neq 0$ in $\mathfrak{O}$ with the absolute value $|N_K(\alpha)|$ of the norm $N_K(\alpha)$.

Lemma 2.4 *For $\alpha \neq 0$ in $\mathfrak{O}$, $N((\alpha)) = |N_K(\alpha)|$.*

PROOF: If $\mathfrak{O} = \mathbf{Z}\omega_1 + \cdots = \mathbf{Z}\omega_n$, then by Proposition 2.3, there exist $\beta_i = \sum_{j=1}^{n} p_{ji}\omega_j,\ i = 1, 2, \ldots, n; p_{ji} \in \mathbf{Z},\ p_{11}, \ldots, p_{nn} > 0$ such that $(\alpha) = \mathbf{Z}\beta_1 + \cdots + \mathbf{Z}\beta_n$ and $N((\alpha)) = p_{11}p_{22}\cdots p_{nn}$. Let Q stand for the n-rowed square matrix (q_{ij}) where $q_{ij} = 0$ for $1 \leq i < j \leq n$ and $q_{ij} = p_{ij}$ otherwise. Since $(\alpha) = \mathbf{Z}\alpha\omega_1 + \cdots + \mathbf{Z}\alpha\omega_n$ as well, we have in view of the remark immediately preceding this lemma, $\alpha\omega_i = \sum_{j=1}^{n} r_{ji}\beta_j,\ i = 1, \ldots, n$, and if R denotes the n-rowed square matrix (r_{ij}), then $\det R = \pm 1$. Let S be the matrix QR. Taking the regular representation with respect to the base $\omega_1, \ldots, \omega_n$, we have $N_K(\alpha) = \det S$. But

$$\det S = \det Q \cdot \det R = \pm \det Q = \pm p_{11}\cdots p_{nn} = \pm N((\alpha)).$$

Thus $N((\alpha)) = |N_K(\alpha)|$.

Corollary 2.4 *For $t \in \mathbf{Z}$, $N(t\mathcal{O}) = |N(t)| = |t^n|$.*

Lemma 2.5 *For any two integral ideals $\mathfrak{a}, \mathfrak{b}$ there exists $\omega \in \mathcal{O}$, such that* $\gcd(\mathfrak{ab}, (\omega))$ *is $\mathfrak{a}$.*

PROOF: Let $\mathfrak{a} = \mathfrak{p}_1^{a_1} \cdots \mathfrak{p}_r^{a_r}$, $\mathfrak{b} = \mathfrak{p}_1^{b_1} \cdots \mathfrak{p}_r^{b_r}$, $a_i, b_i \in \mathbf{Z}^+$ and $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ are all the prime ideals dividing $\mathfrak{a}$ and $\mathfrak{b}$. We can find an element $\pi_i \in \mathfrak{p}_1^{a_1+1} \cdots \mathfrak{p}_{i-1}^{a_{i-1}+1} \mathfrak{p}_i^{a_i} \mathfrak{p}_{i+1}^{a_{i+1}+1} \cdots \mathfrak{p}_r^{a_r+1}$ but $\pi_i \notin \mathfrak{p}_1^{a_1+1} \cdots \mathfrak{p}_i^{a_i+1} \cdots \mathfrak{p}_n^{a_n+1}$ (since $\mathfrak{p}_i \neq \mathcal{O}$). Take $\omega = \pi_1 + \cdots + \pi_n$. Clearly $\mathfrak{p}_i^{a_i+1}$ divides π_j(for $j \neq i$) and $\mathfrak{p}_i^{a_i}$ is the highest power of $\mathfrak{p}_i$ dividing π_i. Hence $\mathfrak{p}_i^{a_i}$ and no higher power of $\mathfrak{p}_i$ divides ω. Consequently $(\mathfrak{ab}, (\omega)) = \prod_{i=1}^r \mathfrak{p}_i^{a_i} = \mathfrak{a}$.

Remark 2.21 *Given any integral ideal $\mathfrak{a}$ there exists $t \neq 0$ in $\mathbf{Z}$ such that $\mathfrak{b} = t\mathfrak{a}^{-1} \subset \mathcal{O}$, i.e. $\mathfrak{ab} = t\mathcal{O}$. By Lemma* 2.5*, $\mathfrak{a} = (t\mathcal{O}, \omega\mathcal{O}) = t\mathcal{O} + \omega\mathcal{O}$ by the remark on page* 43*. In other words, any integral ideal can be generated, over $\mathcal{O}$ by two algebraic integers in K.*

The following lemma proves the multiplicative nature of the norm of ideals in $\mathcal{O}$

Lemma 2.6 *Let $\mathfrak{a}$ and $\mathfrak{b}$ be integral ideals. Then $N(\mathfrak{ab}) = N(\mathfrak{a})N(\mathfrak{b})$.*

PROOF: Let $\lambda = N(\mathfrak{a})$ and $\mu = N(\mathfrak{b})$. Let $\xi_1, \ldots, \xi_\lambda$ and $\eta_1, \ldots, \eta_\mu$ be a complete set of representative of $\mathcal{O}$ modulo $\mathfrak{a}$ and of $\mathcal{O}$ modulo $\mathfrak{b}$ respectively. By Lemma 2.5, there is $\omega \in \mathcal{O}$ such that $(\mathfrak{ab},\ (\omega)) = \mathfrak{a}$. We claim that the $\lambda\mu$ elements $\xi_i + \omega\eta_j (i = 1, 2, \ldots, \lambda,\ j = 1, 2, \ldots, \eta)$ form a complete set of representatives of $\mathcal{O}$ modulo $\mathfrak{ab}$.(and this will prove the lemma). First, they are all distinct modulo $\mathfrak{ab}$. For, if $\xi_i + \omega\eta_j \equiv \xi_k + \omega\eta_l (\text{mod } \mathfrak{ab})$, then $\xi_i - \xi_k \in \mathfrak{a}$ and therefore $i = k$ But then $\omega(\eta_j - \eta_i) \in \mathfrak{ab}$ and since $(\mathfrak{ab},\ (\omega)) = \mathfrak{a}$, it follows by Theorem 2.2 that $\eta_j - \eta_l \in \mathfrak{b}$ i.e. $j = l$. Given any $x \in \mathcal{O}$, there exists a unique $\xi_i (1 \leq i \leq \lambda)$ such that $x - \xi_i \in \mathfrak{a}$. Now $\mathfrak{a} = (\mathfrak{ab},\ (\omega)) = \mathfrak{ab} + (\omega)$. Hence $x - \xi_i = \omega\eta + y$ with $y \in \mathfrak{ab}$. This gives us $x - \xi_i \equiv \omega\eta_j (\text{mod } \mathfrak{ab})$ for some $\eta_j (1 \leq j \leq \mu)$, since $\omega \in \mathfrak{a}$. Thus for any $x \in \mathcal{O},\ x \equiv \xi_i + \omega\eta_j (\text{mod } \mathfrak{ab})$ for some i and j and we are through.

Lemma 2.7 *For any integer $x > 0$, the number of ideals $\mathfrak{a} \subset \mathcal{O}$ for which $N(\mathfrak{a}) \leq x$ is finite.*

PROOF: Let $\mathfrak{a} = \mathfrak{p}_1^{\lambda_1} \cdots \mathfrak{p}_r^{\lambda_r}$ be any integral ideal with $N(\mathfrak{a}) \leq x$, (here $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ are prime and $\lambda_1, \ldots, \lambda_r > 0$ in $\mathbf{Z}$). By Lemma 2.6,

$(N(\mathfrak{p}_1))^{\lambda_1} \cdots (N(\mathfrak{p}_r))^{\lambda_r} \leq x$. Since $N(\mathfrak{p}_i) \geq 2$, we have $2^{\lambda_i} \leq N(\mathfrak{p}_i)^{\lambda_i} \leq N(\mathfrak{p}_1)^{\lambda_1} \cdots N(\mathfrak{p}_r)^{\lambda_r} \leq x$. The number of λ_i's is finite. To prove the lemma, it therefore suffices to prove that the number of prime ideals in $\mathcal{O}$ of norm $\leq x$ is finite. Now any prime ideal $\mathfrak{p}$ contains exactly one prime $p \in \mathbf{Z}$ (Remark 2.18) and hence $\mathfrak{p}$ occurs in the factorization of $p\mathcal{O}$ into prime ideals. Moreover, $N(\mathfrak{p}) \mid (N(p)) = p^n$, so that, since $N(\mathfrak{p}) \neq 1$,we have $N(\mathfrak{p}) = p^f,\ f \geq 1$, and $p \leq N(\mathfrak{p}) \leq x$. But there are at most n prime ideals occurring in the factorization of $p\mathcal{O}$ into prime ideals since ($p\mathcal{O} = \mathfrak{q}_1^{a_1} \cdots \mathfrak{q}_s^{a_s}, \mathfrak{q}_i$prime) implies by Lemma 2.6 and the corollary to Lemma 2.4, that $p^n = N(p\mathcal{O}) = N(\mathfrak{q}_1)^{a_1} \cdots N(\mathfrak{q}_s)^{a_s}$ leading to $s \leq n$. Since $p \leq x$, the lemma is completely proved.

Lemma 2.8 *There exists a constant C depending only on K such that every integral ideal $\mathfrak{a} \neq \{0\}$ contains $\alpha \neq 0$ with $|N_K(\alpha)| \leq CN(\mathfrak{a})$.*

PROOF: By Theorem 2.2, $\mathcal{O} = \mathbf{Z}\omega_1 + \cdots + \mathbf{Z}\omega_n$. Let t denote the largest integer $\leq (N(\mathfrak{a}))^{1/n}$. Then among the $(t+1)^n$ numbers $\sum_{i=1}^n a_i\omega_i$ with $a_i \in \mathbf{Z},\ 0 \leq a_i \leq t,\ i = 1, 2, \ldots, n$, there should exist at least two distinct numbers whose difference is in $\mathfrak{a}$ (since $N(\mathfrak{a}) =$ order of $\mathcal{O}/\mathfrak{a} < (t+1)^n$). Thus there exists $\alpha = a_1\omega_1 + \cdots + a_n\omega_n \neq 0$ in $\mathfrak{a}$ with $a_i \in \mathbf{Z},\ |a_i| \leq t,\ i = 1, 2, \ldots, n$. Let A_i be the n-rowed square matrix with elements in $\mathbf{Z}$, corresponding to ω_i under the regular representation with respect to the base $\omega_1, \ldots, \omega_n$ of K over $\mathbf{Q}$. Hence to α corresponds the matrix $A = \sum_{i=1}^N a_i A_i$ all of whose elements are integers $\leq t\mu$ (in absolute value) where $\mu = \mu(A_1, \ldots, A_n)$ depends only on $\omega_1, \ldots, \omega_n$ i.e. only on K. It is now immediate that $|N_K(\alpha)| = |\det A| \leq C \cdot t^n \leq C \cdot N(\mathfrak{a})$ for a constant C depending only on K.

Remark 2.22 *The constant C obtained in Lemma 2.8 is not the best possible. By using a theorem due to Minkowski, one can obtain a better constant.*

We have now all the material necessary to prove.

Theorem 2.3 *The class number of K is finite.*

PROOF: We shall prove that in *every* class of ideals, there exists an integral ideal of norm $\leq C$ where C is a constant depending only on K. By Lemma 2.7, the number of ideal classes, i.e. h, will then be finite. Let $\mathcal{R}$ be an ideal class. Take an ideal $\mathfrak{a}$ in the inverse class $\mathcal{R}^{-1}$ (and we can assume $\mathfrak{a}$ to be integral without loss of generality). By Lemma 2.8,

there exists $\alpha \in \mathfrak{a}$ such that $|N(\alpha)| \leq C \cdot N(\mathfrak{a})$ for a constant $C = C(K)$. But now $\mathfrak{b} = (\alpha)\mathfrak{a}^{-1} \in \mathcal{R}$ and $N(\mathfrak{a})N(\mathfrak{b}) = N(\mathfrak{ab}) = |N_K(\alpha)| \leq CN(\mathfrak{a})$, which gives us $N(\mathfrak{b}) \leq C$. Theorem 2.3 is completely proved.

2.4 The group of units

Let K be an algebraic number field of degree n and let $K^{(1)}(= K)$, $K^{(2)}$, $\ldots, K^{(n)}$ be all the conjugates of K.

Let $\mathcal{O}$ be the ring of the algebraic integers in K.

Definition 2.11 *A non-zero element α in $\mathcal{O}$ is called a unit of K if $\alpha^{-1} \in \mathcal{O}$.*

Clearly the units of K form a subgroup $\mathcal{U}$ of K^*.

We observe that if $\alpha \in \mathcal{O}$ is a unit then $N_K(\alpha) = \pm 1$. For if α is a unit, there is $\beta \in \mathcal{O}$ with $\alpha\beta = 1$. Thus $1 = N_K(\alpha\beta) = N_K(\alpha)N_K(\beta)$. Since both $N_K(\alpha)$ and $N_K(\beta)$ are in $\mathbf{Z}$, we must have $N_K(\alpha) = \pm 1$. [The converse is also true: if $\alpha \in \mathcal{O}$ satisfies $N_K(\alpha) = \pm 1$ then α is a unit, as follows from the fact that the norm of α is the product of the conjugates of α.]

Example 2.3 *Let $K = \mathbf{Q}(\sqrt{5})$. Then $\frac{1\pm\sqrt{5}}{2}$ are units in K.*

Lemma 2.9 *The number of integers $\alpha \in \mathcal{O}$ such that $|\alpha^{(i)}| \leq C$ for $i = 1, 2, \ldots, n$, is finite.*

Proof: Let $\omega_1, \ldots, \omega_n$ be an integral base of $\mathcal{O}$. Then, any $\alpha \in \mathcal{O}$ can be written

$$\alpha = x_1\omega_1 + \cdots + \alpha_n\omega_n, \ x_i \in \mathbf{Z}.$$

We then have

$$\alpha^{(i)} = x_1\omega_1^{(i)} + \cdots + x_n\omega_n^{(i)}, \ i = 1, 2, \ldots, n;$$

this can be written

$$A = \Omega X$$

where A is the column $\begin{bmatrix} \alpha^{(1)} \\ \vdots \\ \alpha^{(n)} \end{bmatrix}$, X the column $\begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix}$ and Ω the matrix $(\omega_j^{(k)})$. Since Ω has an inverse Ω^{-1} in $\mathcal{M}_n(\mathbf{C})$, this gives

$$X = \Omega^{-1}A.$$

By assumption, $|\alpha^{(i)}| \leq C$. This clearly implies that

$$|x_i| \leq MC$$

where M depends only on the matrix Ω^{-1}, thus only on K. Since the number of rational integers (x_i) satisfying $|x_i| \leq MC$ is finite the lemma follows.

Definition 2.12 *A complex number α is called a root of unity if $\alpha^m = 1$ for some $m \in \mathbf{Z},\ m \neq 0$. If ρ is a root of unity in K, then $\rho^m = 1$ for some $m \in \mathbf{Z},\ m \neq 0$, so that $|\rho^{(i)}| = 1$ for $i = 1, 2, \ldots, n$.*

Every root of unity in K in is a unit but not conversely. For example, in $K = \mathbf{Q}(\sqrt{2}),\ 1 + \sqrt{2}$ is a unit but not a root of unity.

Taking $C = 1$, we deduce from Lemma 2.9 the following.

Corollary 2.5 *The number of roots of unity in K is finite.*

Let Z be the group of roots of unity in K, and let $\zeta_k = e^{2\pi i p_k/q_k},\ k = 1, \ldots, w$ be the elements of Z. Let $q_0 = q_1 \cdots q_w$ and let A be the subgroup of $\mathbf{Z}$ consisting of integers p for which $e^{2\pi i p/q_0} \in Z$. A is of the form $p_0\mathbf{Z},\ p_0 > 0$. Clearly Z is generated by $\zeta = e^{2\pi i p_o/q_o}$. Thus we have

Lemma 2.10 *The roots of unity in K form a finite cyclic group.*

We denote the order of this group by w.

Lemma 2.11 *Let m and n be positive integers, with $0 < m < n$. Let $(a_{ij},\ 1 \leq i \leq m,\ 1 \leq j \leq n$ be real numbers. Then, for any integer $t > 1$, there exist integers $x_1, \ldots, x_n$ not all zero, $|x_j| \leq t$, such that $|y_i| \leq ct^{1-n/m}$, where $y_i = \sum_{j=1}^{n} a_{ij}x_j$ and c is constant depending only on (a_{ij}).*

PROOF: Let $a = \max_i \sum_{j=1}^{n} |a_{ij}|$. Then, for $|x_j| \leq t$, we have $|y_i| \leq at$. Consider the cube $-at \leq y_i \leq at,\ i = 1, \ldots, m$ in $\mathbf{R}^m$, and divide it into h^m smaller cubes of side $2at/h$(h being an integer≥ 1.) If we assign to the x_j the values $0, 1, \ldots, t$, the $(t+1)^n$ points $(y_1, \ldots, y_m)$ lie in the big cube, so that, if $h^m < (t+1)^n$, at least two of them lie in the same cube of side $2at/h$; let these points correspond to $(x_1', \ldots, x_n')$ and $(x_1'', \ldots, x_n'');\ 0 \leq x_j',\ x_j'' \leq t$. If $x_j = x_j' - x_j''$, then $|y_i| \leq 2at/h$, and

$|x_j| \le t$, not all the x_j are zero. Now, since $t > 1,\ n/m > 1$, we have $(t+1)^{n/m} - t^{n/m} > 1$; hence, there is an integer h with

$$t^{n/m} < h < [(t+1)]^{n/m}.$$

Hence, there exist integers x_j, not all zero, $|x_j| \le t$, with $|y_i| < 2at^{1-n/m}$.

Let $K = K^{(1)}, \ldots, K^{(r_1)}$ be the real conjugates of K, and let K^{r_1+1}, $\ldots, K^{r_1+r_2}$ be the distinct complex conjugates of K, and let $K^{(r_1+r_2+i)} = \bar{K}^{r_1+i)},\ 1 \le i \le r_2$. Consider the set E of integers $1 \le k \le r_1 + r_2$; for any $k \in E$, we set $\bar{k} = k$ if $k \le r_1$, and $\bar{k} = k + r_2$ if $r_1 < k \le r_2$, and, for any subset A of E, we set $\bar{A} = \{\bar{k} \mid k \in A\}$.

Lemma 2.12 *Let A and B be two nonempty subsets of E with $A \cap B = \emptyset,\ A \cup B = E$. Let m be the number of elements in $A \cup \bar{A}$. Then, there exists a constant c_1 depending only on K such that for any integer $t > t_0$, there exists $\alpha \in \mathcal{O}$ for which*

$$\begin{aligned} c_1^{-m+1} t^{1-n/m} &\le |\alpha^{(k)}| \le c_1 t^{1-n/m},\ k \in A, \\ c_1^{-m} t &\le |\alpha^{(k)}| \le t,\ k \in B \end{aligned} \qquad (*)$$

Proof: Let $\omega_1, \ldots, \omega_n$ be a set of n integers of K which are independent over $\mathbf{Q}$. Then, if $\alpha = \sum x_j \omega_j$, we have $\alpha^{(k)} = \sum_{i=1}^{n} x_j \omega^{(k)}$. Let $k_1, \ldots, k_u$ be the elements of A with $\bar{k_i} = k_i, l_1, \ldots, l_v$ those with $\bar{l_i} \ne l_i$. Then $m = u + 2v$. We set $a_{ij} = \omega_j^{(k_i)},\ i \le u, a_{u+i,j} = \operatorname{Re} \omega_j^{(l_i)},\ 1 \le i \le v,\ a_{u+v+i,j} = \operatorname{Im} \omega_j^{(l_i)},\ 1 \le i \le v$. By Lemma 2.11, it follows that there are integers x_j, not all zero, $|x_j| \le t$, with

$$|\alpha^{(k)}| \le 2ct^{1-n/m}, \alpha = \sum_{j=1}^{n} x_j \omega_j.$$

Thus, there exists $c' > 0$, such that, for $t > 1$, there is $\alpha \in \mathcal{O},\ \alpha \ne 0$ with

$$|\alpha^{(k)}| \le c' t^{1-n/m},\ k \in A,\ |\alpha^{(l)}| \le c' t \text{ for all } \ell.$$

Replacing t by t/c', we see that for $t > t_0 (= c')$, there is an integer $\alpha \in \mathcal{O},\ \alpha \ne 0$ with

$$|\alpha^{(k)}| \le c_1 t^{1-n/m},\ k \in A,\ |\alpha^{(l)}| \le t \text{ for all } \ell.$$

Note that $|\alpha^{(k)}| \le c_1 t^{1-n/m}$ for $k \in \bar{A}$, since $\alpha^{(\bar{k})} = \overline{\alpha^{(k)}}$.

We assert that we have the inequalities $(*)$ for this α. In fact, since $\alpha \neq 0, N_K(\alpha)$ is a rational integer $\neq 0$. Using (1.1) we have

$$\begin{aligned} I \leq |N_K(\alpha)| &= \prod_{l=1}^{n} |\alpha^{(l)}| = \prod_{k \in A \cup \bar{A}} |\alpha^{(k)}| \prod_{k \in B \cup \bar{B}} |\alpha^{(l)}| \\ &\leq c_1^m t^{m(1-n/m)} \cdot |\alpha^{(l)}| \cdot t^{n-m-1} = c_1^m t^{-1} |\alpha^{(l)}|. \end{aligned}$$

for any $l \in B$ (since there are m elements in $A \cup \bar{A}$ and $n-m$ in $B \cup \bar{B}$); i.e.

$$|\alpha^{(l)}| \geq c_1^{-m} t, \ l \in B.$$

Further

$$\begin{aligned} 1 \leq |N(\alpha)| = \prod_{k \in A \cup \bar{A}} |\alpha^{(k)}| \prod_{l \in B \cup \bar{B}} |\alpha^{(l)}| &\leq c_1^{m-1} t^{(m-1)(1-n/m)} l^{n-m} |\alpha^{(k)}| \\ &= c_1^{m-1} t^{-(1-n/m)} |\alpha^{(k)}|, \end{aligned}$$

for any $k \in A$. This proves Lemma 2.12.

In the following two lemmas, A, and B have the same significance as in Lemma 2.12.

Lemma 2.13 *There exists a sequence of non-zero integers $\alpha_v \in \mathcal{O}$ $v = 1, 2, \ldots,$ with*

$$|\alpha_\nu^{(k)}| > |\alpha_{\nu+1}^{(k)}|, \ k \in A, \ |\alpha_v^{(k)}| < |\alpha_{\nu+1}^{(k)}|, \ k \in B$$

and

$$|N_K(\alpha_\nu)| \leq c_1^m.$$

PROOF: Let $t_{\nu+1} = M t_\nu$, where M is a suitable constant, and let $\alpha_\nu \in \mathcal{O}$ satisfy

$$c_1^{-m+1} t_\nu^{1-n/m} \leq |\alpha_\nu^{(k)}| \leq c_1 t_\nu^{1-n/m}, \ k \in A,$$

$$c_1^{-m} t_\nu \leq |\alpha_v^{(k)}| \leq t_\nu, k \in B.$$

Suppose that $M > c_1^m$, $M^{n/m-1} > c_1^m$. Then we have $c_1^{-m+1} t_v^{1-n/m} > c_1 t_{\nu+1}^{1-n/m}$, so that $|\alpha_{\nu+1}^{(k)}| < |\alpha_v^{(k)}|$, for $k \in A$, while $t_v < c_1^{-m} t_{\nu+1}$, so that $|\alpha_{v+1}^{(k)}| > |\alpha_v^{(k)}|$, $k \in B$. It is trivial that

$$|N_K(\alpha_\nu)| = \prod_{i \in A \cup \bar{A}} |\alpha_v^{(j)}| \prod_{j \in B \cup \bar{B}} |\alpha_\nu^{(j)}| \leq c_1^m \cdot t^{m(1-n/m)} \cdot t^{n-m} = c_1^m.$$

Lemma 2.14 *There exists a unit ϵ with*

$$|\epsilon^{(k)}| < 1,\ k \in A,\ |\epsilon^{(k)}| > 1,\ k \in B.$$

PROOF: Let $\{\alpha_\nu\}$ be a sequence of integers as in Lemma 2.13, and let $\mathfrak{a}_\nu$ be the principal ideal (α_ν). Then by Lemma 2.4 and 2.13 , $N(\mathfrak{a}_\nu) = |N_K(\alpha_v)| \leq c_1^m$. Hence, there exist $v, \mu,\ v < \mu$ with $\mathfrak{a}_v = \mathfrak{a}_\mu$ (since, by Lemma 2.7 the number of integral ideals of norm $\leq$ const. is finite). This means that

$$\alpha_u = \epsilon\alpha_\nu,\ \epsilon \text{ a unit.}$$

We have

$$|\epsilon^{(k)}| = \frac{|\alpha_\mu^{(k)}|}{|\alpha_v^{(k)}|} \begin{cases} < 1 \text{ if } k \in A \\ > 1 \text{ if } k \in B. \end{cases}$$

A subset S of $\mathbf{R}^m$ is said to be bounded if for all $(x_1, \ldots, x_m) \in S$, we have $|x_i| \leq M$ for a constant M depending only on S.

Lemma 2.15 *Let Γ be an (additive) subgroup of $\mathbf{R}^m$ such that any bounded subset of $\mathbf{R}^m$ contains only finitely many elements of Γ. Then there exist $r \leq m$ elements $\gamma_1, \ldots, \gamma_r$ of Γ which are linearly independent over $\mathbf{R}$ and which generate Γ as a group.*

PROOF: Let γ_1' be a non-zero element of Γ. Consider the set A_1 of all $\lambda \in \mathbf{R}$ for which $\lambda\gamma_1' \in \Gamma \cdot A_1$ contains a smallest positive element $\mu_1,\ 0 < \mu_1 \leq 1$ since there are, by assumption, only finitely many $\lambda,\ |\lambda| \leq 1$, with $\lambda\gamma_1' \in \Gamma$ and $\gamma_1' \in \Gamma$. Let $\gamma_1 = \mu_1\gamma_1'$. If $\gamma = \lambda\gamma_1 \in \Gamma,\ \lambda \in \mathbf{R}$, and if n is an integer with $0 \leq \lambda - n < 1$ then $\gamma - n\gamma_1 = (\lambda - n)\gamma_1 = (\lambda - n)\mu_1\gamma_1' \in \Gamma$, which is not possible unless $\lambda = n$,(by minimality of μ_1) Hence if $\lambda\gamma_1 \in \Gamma$ for $\lambda \in \mathbf{R}$, *then* $\lambda \in \mathbf{Z}$. In particular, the lemma is proved if $m = 1$.

Suppose the lemma already proved for subgroups of $\mathbf{R}^{m-1}$, and let $e_2, \ldots, e_m \in \mathbf{R}^m$ be such that $(\gamma_1, e_2, \ldots e_m)$ form a base of $\mathbf{R}^m$. Let $f : \mathbf{R}^m \to \mathbf{R}^{m-1}$ be the map defined by $f(\lambda_1\gamma_1 + \sum_{i\geq 2} \lambda_i e_i) = (\lambda_2, \ldots, \lambda_m)$ which linear over $\mathbf{R}$, and let Γ_1 be the image of Γ under f. We claim that *any bounded subset of $\mathbf{R}^{m-1}$ contains only finitely many elements* of Γ_1. In fact, let $\gamma' = (\lambda_2, \ldots, \lambda_m) \in \Gamma_1,\ |\lambda_i| \leq M,\ i \geq 2$. Then, there exists $\lambda_1 \in \mathbf{R}$ such that $\gamma = \lambda_1\gamma_1 + \sum_{i\leq 2} \lambda_i e_i \in \Gamma$. Since $\gamma_1 \in \Gamma$, we may suppose that $0 \leq \lambda_1 < 1$. But then $|\lambda_i| \leq M + 1,\ i > 1$, so that there are only finitely many such γ. This proves our claim.

By induction, there exist $\gamma_2', \ldots, \gamma_r' \in \Gamma_1,\ r \leq m$, which are linearly independent over $\mathbf{R}$ and generate Γ_1. Let $\gamma_2, \ldots, \gamma_r \in \Gamma$ be such that

$f(\gamma_i) = \gamma_i',\ i \geq 2$. We assert that $\gamma_1, \ldots, \gamma_r$ (a) are linearly independent over $\mathbf{R}$ and (b) generate Γ.

Proof of (a):

If $\sum_{i=1}^r \lambda_i \gamma_i = 0$ then $\sum_{i=1}^r \lambda_i f(\gamma_i) = \sum_{i=2}^r \lambda_i \gamma_i' = 0$; hence $\lambda_2 = \cdots = \lambda_r = 0$, hence $\lambda_1 \gamma_1 = 0$, hence $\lambda_1 = 0$.

Proof of (b):

If $\gamma \in \Gamma$, then $f(\gamma) \in \Gamma_1$, hence

$$f(\gamma) = \sum_{i=2}^{r} n_i \gamma_i', \quad n_i \in \mathbf{Z},$$

so that $f(\gamma - \sum_{i=2}^r n_i \gamma_i) = 0$. This means that $\gamma - \sum_{i=2}^r n_i \gamma_i = \lambda_1 \gamma_1,\ \lambda_1 \in \mathbf{R}$. Since clearly this is an element of Γ we must have $\lambda_1 = n_1 \in \mathbf{Z}$, so that $\gamma = \sum_{i=1}^r n_i \gamma_i$.

With assertions (a) and (b), Lemma 2.15 is completely proved.

Theorem 2.4 *Let r_1 be the number of real conjugates of $K, 2r_2$ the number of complex conjugates, and let $r = r_1 + r_2 - 1$. Then there exist $\epsilon_1, \ldots, \epsilon_r$ and a root of unity ζ in K such that any unit in K can be written in the form*

$$\epsilon = \zeta^k \epsilon_1^{k_1} \cdots \epsilon_r^{k_r}, \quad k, k_1, \ldots,\ k \in \mathbf{Z}.$$

The $k_i,\ i \geq 1$ are uniquely determined, and k is uniquely determined modulo w where w is the order of the group Z of roots of unity in K.

Proof: Let $\mathfrak{U}$ be the group of units in K. Consider the homomorphism $f: \mathfrak{U} \to \mathbf{R}^r$ defined by

$$f(\epsilon) = (\log|\epsilon^{(1)}|, \ldots, \log|\epsilon^{(r)}|), \quad r = r_1 + r_2 - 1.$$

We assert that (a) the kernel of f is Z and that (b) $f(\mathfrak{U}) = \Gamma$ has the property that any bounded subset of $\mathbf{R}^r$ contains only finitely many elements of Γ.

Proof of (a): If $f(\epsilon) = 0$, then $|\epsilon^{(1)}| = 1, \ldots, |\epsilon^{(r)}| = 1$. This implies that $|\epsilon^{(r_1+r_2+1)}| = 1, \ldots, |\epsilon^{r_2+2r_2-1}| = 1$. Since further $\prod_{k=1}^n |\epsilon^{(k)}| = 1$, we conclude that $|\epsilon^{(r+1)}| = 1$. The integers α in $\mathfrak{O}$ for which $|\alpha^{(i)}| = 1,\ i = 1, 2, \ldots, n$, form a finite group, by Lemma 2.9. Hence $\alpha^k = 1$ for any such α for some $k \in \mathbf{Z}$. Thus $\epsilon^k + 1$, i.e., ϵ is a root of unity.

Proof of (b): If $-M < \log|\epsilon^{(i)}| < M, i = 1, \ldots, r$, then $e^{-M} < |\epsilon^{(i)}| < e^M$ for $i \neq r+1, n$. (since $\epsilon^{(\bar{i})} = \epsilon^{(\bar{i})}$). Since, further, $\prod_1^n |\epsilon^{(k)}| =$

1, this implies that $|\epsilon^{(r+1)}| < e^{nm},\ |\epsilon^{(n)}| < e^{nm}$, so that, by Lemma 2.9, the number of such ϵ is finite.

By Lemma 2.15, there are units $\epsilon_1, \ldots, \epsilon_t,\ t \leq r$ such that $f(\mathcal{U})$ is generated by $f(\epsilon_1), \ldots, f(\epsilon_t)$ which are independent over $\mathbf{R}$. This means that if $\epsilon \in \mathcal{U}$ there are uniquely determined integers $k_1, \ldots, k_t$ so that $\epsilon \cdot \epsilon_1^{-k_1} \cdots \epsilon_t^{-k_t} \in Z$. Since, by Lemma 2.10, Z is a cyclic group of order w, the theorem will be proved if we show that $t = r$.

We now prove that $t = r$. Suppose, if possible, that $t < r$. Then, the subspace V of $\mathbf{R}^r$ generated by $f(\epsilon_1), \ldots, f(\epsilon_t)$ has dimension $t \leq r - 1$. Hence there are real numbers $c_1, \ldots, c_r$ not all zero such that if $(x_1, \ldots, x_r) \in V$ then $c_1 x_1 + \cdots + c_r x_r = 0$; in particular, $c_1 \log|\epsilon^{(1)}| + \cdots + c_r \log|\epsilon^{(r)}| = 0$ for all $\epsilon \in \mathcal{U}$. We may suppose without loss of generality, that at least one $c_i < 0$. Let A be the set of $k \leq r - 1$ with $c_k < 0$, and B the complement of A in the set E of integers $\leq r + 1$. Clearly $A \cap B = \emptyset,\ A \cup B = E$, and A and B are nonempty (B contains $r+1$.) By Lemma 2.14, there is $\epsilon \in \mathcal{U}$ with $|\epsilon^{(k)}| < 1$ for $k \in A,\ |\epsilon^{(k)}| > 1$ for $k \in B$. But then, for all $k, c_k \log|\epsilon^{(k)}| \geq 0$, and is zero only if $c_k = 0$, so that $\sum_1^r c_k \log|\epsilon^{(k)}| > 0$. This contradiction proves that $t = r$, and Theorem 2.4 is completely established.

Remark 2.23 *The above proof of Theorem* 2.4 *follows, in essentials a proof given by C.L. Siegel in a course of lectures in Göttingen. It does not seem to be available in the literature.*

Chapter 3

Quadratic Fields

3.1 Generalities

Definition 3.1 *By a quadratic field we mean an algebraic number field of degree* 2.

Let K be a quadratic field and let $\alpha \neq 0$ be in K. Since $[K : \mathbf{Q}] = 2, 1, \alpha, \alpha^2$ are linearly dependent over $\mathbf{Q}$, i.e $a_0 + a_1\alpha + a_2\alpha^2 = 0$ for a_0, a_1, a_2 in $\mathbf{Q}$ not all zero. Thus, any α in K is a root of an irreducible polynomial in $\mathbf{Q}[X]$ of degree at most 2. But K should contain at least one element β whose irreducible polynomial in $\mathbf{Q}[X]$ is of degree 2, since, otherwise, $K = \mathbf{Q}$. Then $1, \beta$ form a base of K over $\mathbf{Q}$ i.e. $K = \mathbf{Q}(\beta)$. Let $a_2\beta^2 + a_1\beta + a_0 = 0$ where, without loss of generality, we may suppose that $a_0, a_1, a_2 \in \mathbf{Z},\ a_2 \neq 0$. Multiplying by $4a_2$, we have $(2a_2\beta + a_1)^2 = a_1^2 - 4a_0a_2$. Setting $\gamma = 2a_2\beta + a_1$ we have $K = \mathbf{Q}(\gamma)$. Denoting $a_1^2 - 4a_0a_2$ by $m \in \mathbf{Z}$ we see that $K = \mathbf{Q}(\sqrt{m})$ where by $\sqrt{m}$ we mean the positive square root of m if $m > 0$ and the square root of m with positive imaginary part if $m < 0$. We could further suppose, without loss of generality, that m is square-free (i.e $m \neq 1$ and m is not divisible by the square of any prime).

Definition 3.2 *A quadratic field K is called a real or an imaginary quadratic field according as $K \subset \mathbf{R}$ or not.*

A quadratic field K is real if and only if $K = \mathbf{Q}(\sqrt{m})$ with square free $m > 1$ in $\mathbf{Z}$. Note that if K is an imaginary quadratic field, then $K \cap \mathbf{R} = \mathbf{Q}$.

Any $\alpha \in K$ is of the form $p + q\sqrt{m},\ p, q \in \mathbf{Q}$; define the conjugate α' of α by $\alpha' = p - q\sqrt{m}$. It is clear that α is a root of the polynomial $(X-\alpha)(X-\alpha') = X^2-(\alpha+\alpha')X+\alpha\alpha' = X^2-2pX+p^2-q^2m \in \mathbf{Q}[X]$. It follows that α' is the conjugate of α in the sense of Chapter II. Taking the regular representation of K with respect to the base $(1, \sqrt{m})$ of K over $\mathbf{Q}$, the matrix $A = \begin{pmatrix} p & qm \\ q & p \end{pmatrix}$ corresponds to α and the polynomial above is merely $\det(XI_2 - A) = \det \begin{pmatrix} X-p & -qm \\ -q & X-p \end{pmatrix}$. Observe that for $\alpha \in K$, $\mathrm{Tr}_K(\alpha) = \mathrm{Tr}\,(A) = 2p = \alpha + \alpha'$ and $N_K(\alpha) = \det A = p^2 - q^2m = \alpha\alpha'$. If K is imaginary quadratic, then α' is the complex conjugate of $\alpha \in K$, so that, for any $\alpha \neq 0$ in an imaginary quadratic field K, the norm $N_K(\alpha)$ is always positive.

Let $\mathcal{O}$ be the ring of algebraic integers in K. Any $\alpha \in \mathcal{O}$ is of the form $p + q\sqrt{m}$ for some $p, q \in \mathbf{Q}$. If the minimal polynomial of α is of degree 1, then by Proposition 2.1, it is necessarily of the form, $X - a$ for $a \in \mathbf{Q}$ so that $p = a \in \mathbf{Z}$ and $q = 0$. Thus $\alpha + \alpha' = 2p = 2a$ and $\alpha\alpha' = p^2-q^2m = a^2$ are both in $\mathbf{Z}$. Let now the minimal polynomial of α which is a monic polynomial in $\mathbf{Z}[X]$, be of degree 2, say X^2+cX+d with $c, d \in \mathbf{Z}$. Since α is a root of the polynomial $X^2-2pX+p^2-q^2m \in \mathbf{Q}[X]$, we have necessarily $X^2 - 2pX + p^2 - q^2m \equiv X^2 + cX + d$ i.e $-c = 2p = \alpha + \alpha' = \mathrm{Tr}_K(\alpha)$ and $d = p^2 - q^2m = \alpha\alpha' = N_K(\alpha)$. Conversely, for $p, q \in \mathbf{Q}$, if $2p$ and $p^2 - q^2m$ are in $\mathbf{Z}$, then $\alpha = p + q\sqrt{m} \in \mathcal{O}$. Thus, for $\alpha = p + q\sqrt{m} \in K$ to belong to $\mathcal{O}$, it is necessary and sufficient that $\mathrm{Tr}_K(\alpha) = 2p$ and $N_K(\alpha) = p^2 - q^2m$ are both in $\mathbf{Z}$. We use this to construct, explicitly, an integral base of $\mathcal{O}$.

For $p, q \in \mathbf{Q}$, let $\alpha = p + q\sqrt{m}$ be in $\mathcal{O}$. Then $a = 2p,\ b = p^2 - q^2m$ belong to $\mathbf{Z}$. Hence $\frac{a^2-4q^2m}{4} \in \mathbf{Z}$. In particular, $4q^2m \in \mathbf{Z}$. Since m is square-free, it follows that $q = f/2$ with $f \in \mathbf{Z}$. Now $a^2 - f^2m \equiv 0(\mathrm{mod}\ 4)$. We have to distinguish between two cases.

(1) Let $m \equiv 1(\mathrm{mod}\ 4)$. Then $a^2 \equiv f^2(\mathrm{mod}\ 4)$ i.e. f and a are both even or both odd. In this case, it is clear that $\alpha = a + b\frac{1+\sqrt{m}}{2}$ with $a, b \in \mathbf{Z}$, i.e. $\mathcal{O} = \mathbf{Z} + \mathbf{Z}\frac{1+\sqrt{m}}{2}$. [Note that, if m $\equiv$ 1(mod 4), $\frac{1+\sqrt{\mathrm{m}}}{2} \in \mathcal{O}$].

(2) Let $m \equiv 2, 3(\mathrm{mod}\ 4)$. Then $a^2 \equiv f^2m(\,\mathrm{mod}\ 4)$ if and only if a and f are both even showing that $\alpha = a' + b'\sqrt{m}$ with $a', b' \in \mathbf{Z}$, i.e

$$\mathcal{O} = \mathbf{Z} + \mathbf{Z}\sqrt{m}.$$

Thus we have

$$\mathcal{O} = \begin{cases} \mathbf{Z} + \mathbf{Z}\frac{1+\sqrt{m}}{2}, \text{for } m \equiv 1(\text{mod } 4), \\ \mathbf{Z} + \mathbf{Z}\sqrt{m}, \text{for m} \equiv 2, 3(\text{mod } 4) \end{cases} \tag{3.1}$$

(Since m is square-free, the case $m \equiv 0(\text{mod } 4)$ does not arise.) Observe that if $\alpha = a + b\sqrt{m} \in \mathcal{O}$, so does $\alpha' = a - b\sqrt{m}$.

Let $\mathfrak{a}$ be an integral ideal, and (α_1, α_2) an integral base of $\mathfrak{a}$. We define the *discriminant* of $\mathfrak{a}$, written $\Delta(\mathfrak{a})$, to be the square $\Delta(\alpha_1, \alpha_2)$ of the determinant of the matrix $\begin{pmatrix} \alpha_1 & \alpha_2 \\ \alpha_1' & \alpha_2' \end{pmatrix}$ (the prime are conjugates as defined above) i.e.

$$\Delta(\mathfrak{a}) = \Delta(\alpha_1, \alpha_2) = (\alpha_1\alpha_2' - \alpha_1'\alpha_2)^2$$

If (β_1, β_2) is another base of $\mathfrak{a}$ then $\beta_1 = p\alpha_1 + q\alpha_2$, $\beta_2 = r\alpha_1 + s\alpha_2$ where, we have $p, q, r, s \in \mathbf{Z}$. If $P = \begin{pmatrix} p & q \\ r & s \end{pmatrix}$, we have $\det P = \pm 1$. It follows that $\Delta(\beta_1, \beta_2) = \Delta(\alpha_1, \alpha_2)(\det P)^2 = \Delta(\alpha_1, \alpha_2)$ so that the above definition is independent of the integral base of $\mathfrak{a}$. If $\mathfrak{a} = \mathcal{O}$, we write $d = d(K) = \Delta(\mathcal{O})$, and call it the discriminant of the field K. Using (3.1) we find that

$$d = \begin{cases} m \text{ for } m \equiv 1(\text{mod } 4) \\ 4m \text{ for } m \equiv 2, 3(\text{mod } 4) \end{cases}$$

and therefore d is always congruent to 0 or 1 modulo 4. We have thus proved

Proposition 3.1 *For a quadratic field K with discriminant d, we have $K = \mathbf{Q}(\sqrt{d})$ and further $1, \frac{d+\sqrt{d}}{2}$ is an integral base of the ring $\mathcal{O}$ of algebraic integers in K.*

Corollary 3.1 *The discriminant uniquely determines a quadratic field.*

Remark 3.1 *Let $\{\alpha_1, \alpha_2\}$ be an integral base of an integral ideal $\mathfrak{a}$ chosen as in Proposition* 3.1, *i.e. $\alpha_1 = p_{11}\omega_1 + p_{12}\omega_2$, $\alpha_2 = p_{22}\omega_2$, p_{11}, p_{12}, $p_{22} \in \mathbf{Z}$, $p_{11}, p_{22} > 0$ and $\mathcal{O} = \mathbf{Z}\omega_1 + \mathbf{Z}\omega_2$. Then it is clear that $\Delta(\alpha_1, \alpha_2) = p_{11}^2 p_{22}^2 \Delta(\omega_1, \omega_2) = p_{11}^2 p_{22}^2 \cdot d$. But $p_{11}p_{22}$ is precisely $N(\mathfrak{a})$. Thus*

$$\Delta(\mathfrak{a}) = (N(\mathfrak{a}))^2 d. \tag{3.2}$$

In future, K will always stand for a quadratic field with discriminant d, K will be real quadratic or imaginary quadratic according as $d > 0$ or $d < 0$.

The mapping taking $\alpha = x + y\sqrt{d}$ $(x, y \in \mathbf{Q})$ to $\alpha' = x - y\sqrt{d}$ may be seen to be an automorphism of K. An element $\alpha \in K$ satisfies $\alpha = \alpha'$ if and only if $\alpha \in \mathbf{Q}$. For any subset S of K, let us denote by S' the image of S under this automorphism. Since $\mathcal{O} = \mathcal{O}'$ it is clear that for any fractional ideal $\mathfrak{a}, \mathfrak{a}'$ is again a fractional ideal. Clearly $N(\mathfrak{a}) = N(\mathfrak{a}')$.

For any integral ideal $\mathfrak{a}$, we claim that $\mathfrak{a}\mathfrak{a}' = n\mathcal{O}$ where $n = N(\mathfrak{a}) \in \mathbf{Z}$. Let $\mathfrak{p}$ be any prime ideal in $\mathcal{O}$. Now, $\mathfrak{p}$ contains a unique prime number $p > 0$, $p \in \mathbf{Z}$ by Remark 2.18 Further, $\mathfrak{p}$ occurs in the factorization $\mathfrak{p}_1 \cdots \mathfrak{p}_r$ of $p\mathcal{O}$ into prime ideals $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$. By the corollary to Lemma 2.4 and by Lemma 2.6, we have $p^2 = N_K(p) = N(p\mathcal{O}) = N(\mathfrak{p}_1) \cdots N(\mathfrak{p}_r)$. Since $\mathbf{Z}$ is a factorial ring, we have $r \leq 2$ and $N(\mathfrak{p}_i) = p$ or p^2. Thus $p\mathcal{O} = \mathfrak{p}\mathfrak{p}'$ or $\mathfrak{p}$. But if $\mathfrak{p}$ divides $p\mathcal{O}$ so does $\mathfrak{p}'$. Thus we have either

$$\begin{aligned} p\mathcal{O} &= \mathfrak{p}\mathfrak{p}', \ \mathfrak{p} \neq \mathfrak{p}' \\ &\text{or} \\ p\mathcal{O} &= \mathfrak{p} = \mathfrak{p}' \\ &\text{or} \\ p\mathcal{O} &= \mathfrak{p}^2, \ \mathfrak{p} = \mathfrak{p}' \end{aligned} \tag{3.3}$$

In any case, $\mathfrak{p}\mathfrak{p}' = p\mathcal{O}$ or $p^2\mathcal{O}$ i.e. $\mathfrak{p}\mathfrak{p}' = N(\mathfrak{p})\mathcal{O}$. By Lemma 2.6, $\mathfrak{a}\mathfrak{a}' = N(\mathfrak{a})\mathcal{O}$ for any integral ideal $\mathfrak{a}$.

3.2 Factorization of rational primes in K

Let K be a quadratic field of discriminant d and $\mathcal{O}$ the ring of algebraic integers in K. Let p be a prime number in $\mathbf{Z}$. We start from the three possibilities given by 3.3.

Definition 3.3 *If $p\mathcal{O} = \mathfrak{p}\mathfrak{p}'$, $\mathfrak{p} \neq \mathfrak{p}'$, we say that p splits in K. If $\mathfrak{p} = \mathfrak{p}'$, then either $p\mathcal{O} = \mathfrak{p}$ in which case we say that p stays prime in K or $p\mathcal{O} = \mathfrak{p}^2$ in which case we say that p is ramified in K.*

If p is an odd prime, the following proposition gives criteria for the factorization of $p\mathcal{O}$ in K.

Proposition 3.2 *For an odd prime p and a quadratic field of discriminant d, we have*

(i) $p\mathcal{O} = \mathfrak{p}^2$, $\mathfrak{p}$ *prime if and only if* $(\frac{d}{p}) = 0$,

(ii) $p\mathcal{O} = \mathfrak{p}\mathfrak{p}'$, $\mathfrak{p} \neq \mathfrak{p}'$, $\mathfrak{p}$ *prime if and only if* $(\frac{d}{p}) = +1$,

(iii) $p\mathcal{O} = \mathfrak{p}$ *prime if and only if* $(\frac{d}{p}) = -1$.

where $(\frac{d}{p})$ *is the Legendre symbol.*

PROOF:

(i) Let $p\mathcal{O} = \mathfrak{p}^2$, $\mathfrak{p}$ prime. Then there exists $\pi = m + n\frac{d+\sqrt{d}}{2} \in \mathfrak{p}$, $\pi \notin p\mathcal{O}$, $m, n \in \mathbf{Z}$. Now, since $\pi^2 \in p\mathcal{O}$ we see that p divides both $(2m+nd)+d\cdot n^2$ and $n(2m+nd)$. If now $p \mid n$, then $p \mid (2m+nd)$. Since p is odd, this would imply that $p \mid m$, but then $p\mathcal{O}$ divides π, which is a contradiction. Thus $p \mid (2m + nd)$ and $p \nmid n$. Since, further, $p \mid dn^2$, this implies that $p \mid d$, i.e. $(\frac{d}{p}) = 0$.

Conversely, if $(\frac{d}{p}) = 0$, consider $\mathfrak{p} = p\mathcal{O} + \sqrt{d}\mathcal{O}$. Then $\mathfrak{p}^2 = (p^2, p\sqrt{d},\ d)\mathcal{O} = p\mathcal{O}$ since p is the gcd of d and p^2. Further, $\mathfrak{p}$ is necessarily a prime ideal, since at most two prime ideals of $\mathcal{O}$ can divide $p\mathcal{O}$ (see page 58.)

(ii) Let $(\frac{d}{p}) = 1$. Then there exists $a \in \mathbf{Z}$ such that $a^2 \equiv d(\mathrm{mod}\ p)$. Let $\mathfrak{p}$ be the ideal generated by p and $a + \sqrt{d}$. Then clearly, $\mathfrak{p}\mathfrak{p}' = (p^2,\ p(a+\sqrt{d}),\ p(a-\sqrt{d}), a^2 - d)\mathcal{O} = p\mathcal{O}$ [$p \in \mathfrak{p}\mathfrak{p}'$ since $p =$ g.c.d. $(p^2,\ 2ap)$]. Hence $\mathfrak{p}, \mathfrak{p}'$ are prime ideals. However $\mathfrak{p} + \mathfrak{p}' = \mathcal{O}$ and therefore $\mathfrak{p} \neq \mathfrak{p}'$.

Conversely, let $p\mathcal{O} = \mathfrak{p}\mathfrak{p}'$, $\mathfrak{p} \neq \mathfrak{p}'$, $\mathfrak{p}$ prime. Then $N(\mathfrak{p}) = N(\mathfrak{p}') = p$. There exists $\alpha \in \mathfrak{p}$, $\alpha \notin p\mathcal{O} = \mathfrak{p}\mathfrak{p}'$. Then $\alpha = x + y\frac{d+\sqrt{d}}{2}$ with $x, y \in \mathbf{Z}$, p not dividing both x and y. Since $\alpha\mathcal{O} = \mathfrak{p}\mathfrak{q}$ with $\mathfrak{q} \subset \mathcal{O}$, it follows, on taking norms, that $p = N(\mathfrak{p})$ divides $N(\alpha\mathcal{O}) = |N_K(\alpha)| = |(x + y\frac{d}{2})^2 - y^2\frac{d}{4}|$. Hence $(2x + dy)^2 \equiv y^2 d(\mathrm{mod}\ p)$. If $p \mid y$, then $p|(2x + dy)^2$, i.e. $p \mid 2x$. Since p is odd, $p \mid x$, i.e. $p \mid (x, y)$. We have thus a contradiction. Hence $p \nmid y$ and since $\mathbf{Z}/(p)$ is a field, we have $z^2 \equiv d(\mathrm{mod}\ p)$ for $z \in \mathbf{Z}$, i.e. $(\frac{d}{p}) = 1$.

(iii) The validity of (iii) is an immediate consequence of (i) and (ii).

Before we consider the factorization of $2\mathcal{O}$ in K, we define Kronecker's quadratic residue symbol $(\frac{d}{2})$ with denominator 2 by

$$\left(\frac{d}{2}\right) = \begin{cases} 0 \text{ if } d \equiv 0(\mathrm{mod}\ 4) \\ 1 \text{ if } d \equiv 1(\mathrm{mod}\ 8) \\ -1 \text{ if } d \equiv 5(\mathrm{mod}\ 8) \end{cases}$$

(Recall that the discriminant d of K is congruent to 0 or 1 modulo 4.)

Proposition 3.3 *Let $\mathcal{O}$ be the ring of algebraic integers in a quadratic field of discriminant d. Then we have*

(i) $2\mathcal{O} = \mathfrak{p}^2,\ \mathfrak{p}$ *prime if and only if* $(\frac{d}{2}) = 0$,

(ii) $2\mathcal{O} = \mathfrak{p}\mathfrak{p}', \mathfrak{p} \neq \mathfrak{p}', \mathfrak{p}$ *prime if and only if* $(\frac{d}{2}) = +1$

(iii) $2\mathcal{O} = \mathfrak{p}$ *prime if and only if* $(\frac{d}{2}) = -1$,

where $(\frac{d}{2})$ *is Kronecker's quadratic residue symbol.*

PROOF: (i) Let $(\frac{d}{2}) = 0$. Let $\mathfrak{p} = (2, 1 + \frac{\sqrt{d}}{2})$ or $(2, \frac{\sqrt{d}}{2})$ according as 8 does not or does divide d. Clearly $\mathfrak{p}^2 = 2\mathcal{O}$ and $\mathfrak{p}$ is necessarily prime.

Conversely, let $2\mathcal{O} = \mathfrak{p}^2, \mathfrak{p}$ prime. If $d \equiv 0 (\text{mod } 4), (\frac{d}{2}) = 0$ and there is nothing to prove. Let then $d \equiv 1 (\text{mod } 4)$ so that $\mathcal{O} = \mathbf{Z} + \mathbf{Z}(\frac{1+\sqrt{d}}{2})$. Since $\mathfrak{p}^2 \neq \mathfrak{p}$, there exists $\pi \in \mathfrak{p},\ \pi \notin \mathfrak{p}^2 = 2\mathcal{O}$. Let $\pi = x + y\frac{1+\sqrt{d}}{2}$ with $x, y \in \mathbf{Z}$. We can assume that x and y are either 0 or 1 for along with $\pi,\ \pi + 2\alpha$ for any $\alpha \in \mathcal{O}$ also satisfies $\pi + 2\alpha \in \mathfrak{p}$ but $\notin \mathfrak{p}^2$.

If $y = 0$, then $x \neq 0$ since otherwise $\pi = 0$ and $\pi \in \mathfrak{p}^2$. Further $x \neq 1$, since then $\pi = 1$ and $\pi \notin \mathfrak{p}$. So $y = 1$ and x can be 0 or 1. Now $\pi^2 = \left(x + \frac{1+\sqrt{d}}{2}\right)^2 = a + b\left(\frac{1+\sqrt{d}}{2}\right)$ for $a, b \in \mathbf{Z}$. Then $b = 2\left(x + \frac{1}{2}\right) = 2x + 1$ is necessarily odd. But since $\pi^2 \in 2\mathcal{O}, b$ must be even and so we arrive at a contradiction if we assume that $d \equiv 1 (\text{ mod } 4)$. Consequently $d \equiv 0 (\text{ mod } 4)$ so that $(\frac{d}{2}) = 0$.

(ii) Let $(\frac{d}{2}) = 1$. Then $d \equiv 1 (\text{ mod } 4)$ necessarily, so that $\mathcal{O} = \mathbf{Z} + \frac{1+\sqrt{d}}{2}\mathbf{Z}$. Defining $\mathfrak{p} = 2\mathcal{O} + \frac{1+\sqrt{d}}{2}\mathcal{O}$, we see that $\mathfrak{p}\mathfrak{p}' = (4, 1 + \sqrt{d},\ 1 - \sqrt{d}, \frac{1-\sqrt{d}}{4}\Big)$. Since $2 = 1 + \sqrt{d} + 1 - \sqrt{d}$ and $4, 1 + \sqrt{d},\ 1 - \sqrt{d}$ and $\frac{1-d}{4}$ are all in $2\mathcal{O}$ we have $\mathfrak{p}\mathfrak{p}' = 2\mathcal{O}$. (Here $\mathfrak{p} \neq \mathfrak{p}'$ since otherwise, we would have $2\mathcal{O} = \mathfrak{p}^2$ and $4 \mid d$ by (ii).)

Conversely, let $2\mathcal{O} = \mathfrak{p}\mathfrak{p}',\ \mathfrak{p} \neq \mathfrak{p}',\ \mathfrak{p}$ prime. Then $N(\mathfrak{p}) = 2$. Further there exists $\pi = x + y\frac{d+\sqrt{d}}{2} \in \mathfrak{p},\ \pi \notin \mathfrak{p}\mathfrak{p}' = 2\mathcal{O}$, so that x, y are integers which are not both even. Since $2 = N(\mathfrak{p})$ divides $N(\pi\mathcal{O}) = |N(\pi)|$ we have $(2x + yd)^2 \equiv y^2 d (\text{ mod } 8)$. Now $2 \nmid d$, since otherwise, by (i), we would have $2\mathcal{O} = \mathfrak{p}^2$ and then $\mathfrak{p} = \mathfrak{p}'$. If y is even, let first $y = 2y_1,\ 2 \nmid y_1,\ y_1 \in \mathbf{Z}$. Then $2|((x + y_1 d)^2 + y_1^2 d)$, and $2 \nmid y_1 d$ together give us $2 \nmid (x + y_1 d)$ and this in turn implies that $2 \mid x$. But then x

and y are both even which is impossible. If $4 \mid y$, then $4 \mid (2x + yd)$ implying that $4 \mid 2x$, i.e. $2 \mid x$. This contradicts the fact $\pi \notin 2\mathcal{O}$. Therefore y has to be odd. Find $y_2 \in \mathbf{Z}$ such that $yy_2 \equiv 1 (\mathrm{mod}\ 8)$. (We have only to choose $y_2 = \pm 1 \pm 5$.) Then $d \equiv (2x + yd)^2 y_2^2 (\mathrm{mod}\ 8)$. Since $2 \nmid d$, $(2x + yd)y_2$ is odd so that $d \equiv 1 (\mathrm{mod}\ 8)$ and consequently $(\frac{d}{2}) = 1$.

(iii) The proof is trivial, if we use (i) and (ii) above.

As an application of the criteria for splitting of rational primes given above, we shall determine the class number h of a quadratic field $\mathbf{Q}(\sqrt{m}), m$ being square-free in $\mathbf{Z}$, for special values of m.

For this, we need to determine explicitly the constant C of Lemma 2.8 for the special case of a quadratic field. We claim that C can be chosen to be $1 + |m|$ if $m \equiv 2, 3 (\mathrm{mod}\ 4)$ and $2 + \frac{|m-1|}{4}$ if $m \equiv 1 (\mathrm{mod}\ 4)$. For $m \equiv 2, 3 (\mathrm{mod}\ 4)$, $d = 4m$ and taking the regular representation with respect to the integral base $\{1, \sqrt{m}\}$ of $\mathcal{O}$ the matrices $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ and $\begin{pmatrix} 0 & m \\ 1 & 0 \end{pmatrix}$ correspond to $1, \sqrt{m}$ respectively and $\det \left(\alpha_1 \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} + \alpha_2 \begin{pmatrix} 0 & m \\ 1 & 0 \end{pmatrix} \right) = \alpha_1^2 - m\alpha_2^2$ so that C can be chosen to be $1 + |m|$. The case $m \equiv 1 (\mathrm{mod}\ 4)$ is dealt with in a similar fashion.

(1) Consider $K = \mathbf{Q}(\sqrt{2})$. Here, $d = 8$ and $\mathcal{O} = \mathbf{Z} + \mathbf{Z}\sqrt{2}$. Further we may take $C = 3$ in this case. Following the proof of Theorem 2.3, in order to find the number of ideal classes in K, it suffices to consider the splitting of prime ideals of norm at most 3. Now $2\mathcal{O} = (\sqrt{2}\mathcal{O})^2$, while $3\mathcal{O}$ is prime since $(\frac{8}{3}) = -1$. Thus prime ideals of norm ≤ 3 are principal. Any integral ideal of norm ≤ 3 is therefore principal so that $h = 1$.

(2) Consider $K = \mathbf{Q}(\sqrt{-1})$. Here $d = -4$ and $\mathcal{O} = \mathbf{Z} + \mathbf{Z}\sqrt{-1}$. The constant C may now be chosen to be 2. To find h, it suffices to investigate the prime ideals of norm at most 2. But $2\mathcal{O} = (1 - \sqrt{-1})\mathcal{O} \cdot (1 + \sqrt{-1})\mathcal{O} = \mathfrak{p}^2$ where $\mathfrak{p} = (1 + \sqrt{-1})\mathcal{O}$. Thus any integral ideal of norm ≤ 2 is principal and consequently $h = 1$.

(3) Take $K = \mathbf{Q}(\sqrt{-5})$. Here $d = -20$ and $\mathcal{O} = \mathbf{Z} + \mathbf{Z}\sqrt{-5}$ which is not a factorial ring as remarked on page 26. Thus the class number h of K clearly cannot be 1. Now the constant $C = 6$ and from the relations $2\mathcal{O} = ((2, 1 + \sqrt{-5})\mathcal{O})^2$, $3\mathcal{O} = (3, 1 + \sqrt{-5})\mathcal{O} \cdot (3, 1 - \sqrt{-5})\mathcal{O}$, $5 = (\sqrt{-5}\mathcal{O})^2$ $3(2, 1 - \sqrt{-5})\mathcal{O}) = (1 + \sqrt{-5})(3, 1 - \sqrt{-5})\mathcal{O}$ it is easy to see that $h = 2$ in this case.

Remark 3.2 *In the first two examples above one can show directly that*

the ring $\mathcal{O}$ of algebraic integers possesses a Euclidean algorithm namely, for $\alpha, \beta,\ \beta \neq 0$ in $\mathcal{O}$ there exists $\gamma, \delta \in \mathcal{O}$ such that $\alpha = \gamma\beta + \delta$ with $0 \leq |N(\delta)| < |N(\beta)|$. This leads easily to the fact that $\mathcal{O}$ is a principal ideal domain so that the class number of K is 1.

Let p be an odd prime in $\mathbf{Z}$. By Proposition 3.2, $p\mathcal{O} = \mathfrak{p}\mathfrak{p}',\ \mathfrak{p} \neq \mathfrak{p}'$ in $K = \mathbf{Q}(\sqrt{-1})$, if and only if $(\frac{-4}{p}) = (\frac{4}{p})(\frac{-1}{p}) = (\frac{-1}{p})$ is equal to 1. In $\mathbf{Q}(\sqrt{-1})$ every ideals is principal so that $\mathfrak{p} = \alpha\mathcal{O}$ for $\alpha = a + b\sqrt{-1}$ with $a, b \in \mathbf{Z}$. Since $N_K(\alpha) > 0$, we have $a^2 + b^2 = N_k(\alpha) = N(\mathfrak{p}) = p$. Thus we have

Remark 3.3 *An odd prime p is a sum of two squares of integers if and only if $(\frac{-1}{p}) = 1$.*

3.3 The group of units

Let K be a quadratic field of discriminant d. In the notation of Chapter 2 §4 we see that $r_1 = 2, r_2 = 0$ if $d > 0$ and $r_1 = 0, r_2 = 1$ for $d < 0$.

In the case of a real quadratic field K, the only roots of unity in K are real roots of unity, namely, 1 and -1. By Theorem 2.4, every unit ϵ in K can be written in the form $\pm\epsilon_1^n,\ n \in \mathbf{Z}$ for a fixed unit ϵ_1 in K. Further $\epsilon_1 \neq \pm 1$. If ϵ_1 has this property, so have $\epsilon_1^{-1},\ -\epsilon_1, -\epsilon_1^{-1}$. But among $\epsilon_1, \epsilon_1^{-1}, -\epsilon_1, -\epsilon_1^{-1}$, exactly one of them is greater than 1. We denote it by η and call it the *fundamental unit* of K. It is uniquely determined and every unit ϵ is of the form $\pm\eta^n$ for $n \in \mathbf{Z}$.

Any unit $\epsilon \in K = \mathbf{Q}(\sqrt{d})$ of discriminant $d > 0$ gives rise to a solution of the Diophantine equation

$$x^2 - dy^2 = \pm 4, \quad x, y \in \mathbf{Z}, \tag{3.4}$$

since $N_K(\epsilon) = N_K \dfrac{(x + y\sqrt{d})}{2} = \dfrac{x^2 - dy^2}{4}$ and $N_K(\epsilon) = \pm 1$ in view of ϵ being a unit in K. Conversely, if, for $d > 0$ in $\mathbf{Z}$, there exist x, y in $\mathbf{Z}$ satisfying (3.4), then $(x \pm y\sqrt{d})/2$ is a unit in $k = \mathbf{Q}(\sqrt{d})$. In the case when d is the discriminant of a real quadratic field, we have by Theorem 4, a non-trivial solution of the Diophantine equation (3.4). This equation is commonly referred to as Pell's equation but it seems that Pell was neither the first to notice the equation nor did he find a non-trivial solution of it.

If $d < 0, K$ is an imaginary quadratic field and $r = 0$. Thus every unit in K is a root of unity, by Theorem 2.4. By Lemma 2.10, we see that

the units in K form a finite cyclic group of order w. One can, however, check directly that $w = 2, 4$ or 6 according as $d < -4$, $d = -4$ or $d = -3$ respectively. To prove this, we proceed as follows. Let $\alpha = p + q\frac{d+\sqrt{d}}{2}$ be a unit in K. Then

$$N_K(\alpha) = \left(p + \frac{qd}{2}\right)^2 + \frac{q^2}{4}|d| = 1 \quad (\text{since } N_K(\alpha) = \alpha\bar{\alpha} > 0).$$

Thus $(p + \frac{qd}{2})^2 \leq 1$ and $q^2 \leq \frac{4}{|d|}$. If $d < -4$, then, of necessity, $q = 0$ and therefore. $\delta\alpha = p = \pm 1$ are the only units in K. Thus $w = 2$ for $d < -4$. If $d = -4$, the $q = 0, 1$ or -1. If $q = 0, p = \pm 1$. If $q = 1, p = 2$ and if $q = -1$, then $p = -2$. Hence in $K = \mathbf{Q}(\sqrt{-4})$, the only units are $\pm 1,\ \pm - 1$ so that $w = 4$. Take now $K = \mathbf{Q}(\sqrt{-3})$. Then $q = 0, 1$ or -1. If $q = 0,\ p = \pm 1$. If $q = \pm 1$ then $p - \frac{3q}{2} = \pm\frac{1}{2}$. Hence the only units here are $\pm 1, \pm\frac{1}{2} + \frac{\sqrt{-3}}{2},\ \pm\frac{1}{2} - \frac{\sqrt{-3}}{2}$ so that $w = 6$.

3.4 Laws of quadratic reciprocity

In Chapter 2, §3 we introduced the class group of an algebraic number field and proved that it is of finite order h.

Let K be a quadratic field of discriminant d and $\mathcal{O}$ the ring of algebraic integers in K. Let Π_0 denote the group of principal ideals $\lambda\mathcal{O}$ with $\lambda \in K$ for which $N_K(\lambda) = \lambda\lambda' > 0$. The quotient group of Δ (the group of all non-zero fractional ideals in K) modulo Π_0 is denoted by $\mathfrak{h}_0$ and called the *restricted class* group of K. Now Π_0 is of index at most 2 in Π and the order h_0 of $\mathfrak{h}_0$ is equal to h or $2h$ according as the index of Π_0 in Π is 1 or 2. If $d < 0$, trivially $\Pi_0 = \Pi$ since for $\alpha \neq 0$ in K, we always have $N_K(\alpha) > 0$. If $d > 0$, then $\Pi = \Pi_0$ if and only if there exists in K a unit of norm -1. (For $\sqrt{d}\mathcal{O}$ is in the same coset of Δ modulo Π_0 as $\mathcal{O}$ if and only if $\sqrt{d} = \epsilon\rho$ with $N_K(\rho) > 0$. But, since $N_K(\sqrt{d}) < 0$, this can happen, if and only if the unit ϵ has norm -1).

Definition 3.4 *The fractional ideals $\mathfrak{a}, \mathfrak{b}$ different from 0 are equivalent in the restricted sense (in symbols, $\mathfrak{a} \approx \mathfrak{b}$) if $\mathfrak{a}$ and $\mathfrak{b}$ belong to the same coset of Δ modulo Π_0 (i.e. $\mathfrak{a} = \rho\mathcal{O}\mathfrak{b}$ with $\rho \in K$ and $N_K(\rho) > 0$).*

It is clear that when $K = \mathbf{Q}(\sqrt{d}),\ d < 0$ or when $d > 0$ and K contains a unit of norm -1, this concept coincides with the concept of equivalence introduced in Chapter 2, §3. In the case when $d > 0, \Pi_0$ may be also defined to be the group of principal ideals $\lambda\mathcal{O}$ with $\lambda \in K$

and $\lambda > 0,\ \lambda' > 0$. Such numbers of a real quadratic field are referred to as totally positive numbers (in symbols, $\lambda \succ 0$). Thus Π_0 consists of all principal fractional ideals in K generated by a totally positive number.

Definition 3.5 *A class of ideals C in $\mathfrak{h}_0 = \Delta/\Pi_0$ is said to be ambiguous if $C^2 = 1$ in $\mathfrak{h}_0$.*

We shall now find the number of ambiguous classes in $\mathfrak{h}_0$.

The following theorem is of great importance by itself, although it may look a little out of place in our scheme. It is connected with the so-called 'genus characters' in Gauss' theory of binary quadratic forms and we are not able to go into this here. We have, however, used it to deduce the laws of quadratic reciprocity.

Theorem 3.1 *The number of ambiguous ideal classes in a quadratic field K of discriminant d is 2^{t-1} where t is the number of distinct prime numbers dividing d.*

PROOF: Let $|d| = p_1^{\alpha_1} p_2 \cdots p_t$, where $\alpha_1 = 1$ or $\alpha_1 = 2$ or 3 according as d is odd or even. Then, because of the remarks at the end of Chapter 3,§1 $p_i\mathfrak{O} = \mathfrak{p}_i^2$ where $\mathfrak{p}_i$ is a prime ideal in $\mathfrak{O}$ of norm p_i; further, $\mathfrak{p}_i = \mathfrak{p}_i'$. The class of each $\mathfrak{p}_i, i = 1, \ldots, t$ in $\mathfrak{h}_0$ is ambiguous.

Let $\mathfrak{a}$ be any nonzero ideal with $\mathfrak{a} = \mathfrak{a}'$. We assert that

$\mathfrak{a}$ *can be written uniquely in the form*

$$\mathfrak{a} = r \cdot \mathfrak{p}_1^{a_1} \cdots \mathfrak{p}_t^{a_t}, \quad r \in \mathbf{Q},\ r > 0,\ a_i = 0 \text{ or } 1. \tag{3.5}$$

Proof of (3.5): Let $n > 0,\ n \in \mathbf{Z}$ be such that $n\mathfrak{a} = \mathfrak{b}$ is integral. Then $\mathfrak{b} = \mathfrak{b}'$. Let $\mathfrak{b} = \mathfrak{q}_1 \cdots \mathfrak{q}_l$ be the factorization of $\mathfrak{b}$ into prime ideals. Since $\mathfrak{b} = \mathfrak{b}'$, we have, for any $i, \mathfrak{q}_i' = \mathfrak{q}_j$ for some j. If $i = j$, then, unless $\mathfrak{q}_i$ is one of the ideals $\mathfrak{p}_k$ we have $\mathfrak{q}_i = q_i\mathfrak{O}$, where q_i is a rational prime. If $i \neq j$, then $\mathfrak{q}_i\mathfrak{q}_j = (N(\mathfrak{q}_i))\mathfrak{O}$. Hence $\mathfrak{b} = c' \cdot \mathfrak{p}_1^{\alpha_1} \cdots \mathfrak{p}_t^{\alpha_t}$, where $c', \alpha_1, \ldots, \alpha_t \in \mathbf{Z},\ \alpha_i \geq 0$. Since $\mathfrak{p}_i^2 = p_i\mathfrak{O},\ \mathfrak{b} = c \cdot \mathfrak{p}_1^{a_1} \cdots \mathfrak{p}_t^{a_t},\ c \in \mathbf{Z},\ a_i = 0$ or 1. Since $\mathfrak{a} = n^{-1}\mathfrak{b}$,

$$\mathfrak{a} = r \cdot \mathfrak{p}_1^{a_1} \cdots \mathfrak{p}_t^{a_t}, \quad r \in \mathbf{Q},\ r > 0.$$

If, furthermore $\mathfrak{a} = r_1 \cdot \mathfrak{p}_1^{b_1} \cdots p_t^{b_t},\ b_i = 0$ or $1,\ r_1 > 0$, then $N(\mathfrak{a}) = r^2 \cdot \mathfrak{p}_1^{a_1} \cdots \mathfrak{p}_t^{a_t} = r_1^2 \cdot \mathfrak{p}_1^{b_1} \cdots \mathfrak{p}_t^{b_t}$, so that $a_i \equiv b_i (\mathrm{mod}\ 2)$. Since each of a_i, b_i is 0 or 1, we must have $a_i = b_i$. Hence $r\mathfrak{O} = r_1\mathfrak{O}$, and since $r > 0,\ r_1 > 0$, this implies that $r = r_1$.

Suppose that $\mathfrak{b}$ is a fractional ideal with $\mathfrak{b}^2 \approx \mathcal{O}$. By multiplying $\mathfrak{b}$ by an integer, we may suppose that $\mathfrak{b}$ is integral. Since, further $\mathfrak{b}\mathfrak{b}' \approx \mathcal{O}$ we conclude that $\mathfrak{b} = \omega\mathfrak{b}'$ where $\omega \in K$, $N_K(\omega) > 0$ and $\omega \succ 0$ If $d > 0$. Moreover, since $N_K(\omega) > 0$, $\omega\omega' = N_K(\omega) = N_K(\mathfrak{b})/N_K(\mathfrak{b}') = 1$. Hence $\omega = \dfrac{1+\omega}{1+\omega'}$, so that if $\mathfrak{a} = (1+\omega)^{-1}\mathfrak{b}$, we have $\mathfrak{a} = \mathfrak{a}'$. By what we have shown above, $\mathfrak{a} = r\mathcal{O}\mathfrak{p}_1^{t_1}\cdots\mathfrak{p}_k^{t_k}$ where $r \in \mathbf{Q}$, $t_i = 0$ or 1. Further $N_K(1+\omega) = \omega(1+\omega')^2 > 0$ if $d > 0$. Hence $\mathfrak{b} \approx \mathfrak{p}_1^{t_1}\cdots\mathfrak{p}_k^{t_k}$ where $t_i = 0$ or 1. Hence any ambiguous ideal class is equivalent, in the restricted sense to one of the at most 2^t ideal classes containing $\mathfrak{p}_1^{t_1}\cdots\mathfrak{p}_k^{t_k}$, $t_i = 0$ or 1.

To complete the proof of the theorem we have therefore only to prove the following:

there is exactly one relation of the form

$$\mathfrak{p}_1^{a_1}\cdots\mathfrak{p}_t^{a_t} \approx \mathcal{O} \text{ where } a_i = 0 \text{ or } 1, \sum_{i=1}^{t} a_i > 0. \tag{3.6}$$

We prove first the uniqueness of a relation of this form. Let $\mathfrak{p}_1^{a_1}\cdots\mathfrak{p}_t^{a_t} = \rho\mathcal{O}$ with $N_K(\rho) > 0$. Clearly $\rho\mathcal{O} = \rho'\mathcal{O}$, so that

$$\rho = \eta\rho' \quad \text{where } \eta \text{ is a unit.} \tag{3.7}$$

Further, if $d > 0$, we have $\eta \succ 0$. Let ϵ be a generator of the group of the totally positive units in K if $d > 0$, and of the group of all units in K if $d < 0$; we have always $\epsilon \neq 1$. Replacing ρ by $\rho\epsilon^n$ for a suitable $n \in \mathbf{Z}$ we may suppose that, in (3.7)

$$\rho = \eta\rho' \text{ with } \eta = 1 \text{ or } \epsilon. \tag{3.8}$$

We claim that $\eta \neq 1$. In fact, if $\eta = 1$, then $\rho \in \mathbf{Z}$, hence $\mathcal{O} = \rho^{-1}\mathfrak{p}_1^{a_1}\cdots\mathfrak{p}_t^{a_t} = \mathfrak{p}_1^0\cdots\mathfrak{p}_t^0$, contradicting the *uniqueness* asserted by (3.5). Hence $\eta = \epsilon$, and we have $\rho = \epsilon\rho'$. Let $\mu = \sqrt{d}(1-\epsilon)(\neq 0)$. Then $\mu = \epsilon\mu'$, so that $\left(\dfrac{\rho}{\mu}\right)' = \dfrac{\rho}{\mu}$, and $\dfrac{\rho}{\mu} = r \in \mathbf{Q}$. Hence $\mu\mathcal{O} = r^{-1}\mathfrak{p}_1^{a_1}\cdots\mathfrak{p}_t^{a_t}$ and the uniqueness assertion in (3.5) shows that this determines $a_1, \ldots, a_t$. (Note that $\mu = \sqrt{d}(1-\epsilon)$ is uniquely determined by the field K.)

To prove the existence of a relation (3.6), define $\mu = \sqrt{d}(1-\epsilon)$ as above. Then $\mu\mathcal{O} = (\mu\mathcal{O})'$, so that $\mu\mathcal{O} = c\mathfrak{p}_1^{a_1}\cdots\mathfrak{p}_t^{a_t}$, where $c \in \mathbf{Q}, a_i = 0$ or 1. Since $\mu \succ 0$ if $d > 0$, we have only to show that $\sum_{i=1}^{t} a_i > 0$. If this were not the case, then $\mu = c\zeta$, where ζ is a unit and $\zeta \succ 0$ if $d > 0$.

Since $\mu = \epsilon\mu'$ this gives $c\zeta = c\epsilon\zeta' = \dfrac{c\epsilon}{\zeta}$ so that $\epsilon = \zeta^2$, contradicting the definition of ϵ. Thus $\sum_{i=1}^{t} a_i > 0$, and the theorem is proved.

Proposition 3.4 *If the discriminant d of a quadratic field K is divisible only by one prime number then h_0 is odd and so equal to the class number h of K. In this case, if $d > 0$, then K contains a unit of norm -1.*

PROOF: By Theorem 3.1, the restricted class containing $\mathcal{O}$ is the sole ambiguous class $\mathfrak{h}_0$ i.e. $\mathfrak{h}_0$ does not contain elements of order 2.

We shall now prove that $\mathfrak{h}_o$ is of odd order. For $x \in \mathfrak{h}_0$, let A_x denote the subset of $\mathfrak{h}_0$ consisting of x and x^{-1}. Now, $\mathfrak{h}_0 = A_1 \cup \bigcup_{\substack{x\in\mathfrak{h}_0 \\ x\neq 1}} A_x$ and $A_1 \cap A_x = \emptyset$ if $x \neq 1$. Further, since no element of $\mathfrak{h}_0$ is of order $2, A_x$ consists of 2 elements for every $x \neq 1$ in $\mathfrak{h}_0$. But $A_1 = \{1\}$. Thus the order h_0 of $\mathfrak{h}_0$ is odd.

By the remarks at the beginning of this section, we necessarily have $h_0 = h$. It is clear that if $d > 0, K$ contains a unit of norm -1.

We shall make use of the above results to deduce the well-known laws of quadratic reciprocity.

Proposition 3.5 *If p is an odd prime, then*

$$(i)\ \left(\frac{-1}{p}\right) = (-1)^{(p-1)/2}, \qquad (ii)\ \left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8}$$

PROOF: (i) If $p \equiv 1 (\bmod 4)$, then $(-1)^{(p-1)/2} = 1$. We shall prove that $(\frac{-1}{p}) = 1$ in this case. In fact, $\mathbf{Q}(\sqrt{p})$ contains a unit $\epsilon = (\frac{a+b\sqrt{p}}{2})$ of norm -1, in view of Proposition 3.4. Hence $a^2 \equiv -4 (\bmod p)$, i.e. $1 = (\frac{-4}{p}) = (\frac{-1}{p})(\frac{4}{p}) = (\frac{-1}{p})(\frac{2}{p})^2 = (\frac{-1}{p})$. Conversely, if $a^2 \equiv -1 (\bmod\ p)$ where $p \nmid a$ we obtain, by the remark on page 16 that $1 \equiv a^{p-1} \equiv (a^2)^{(p-1)/2} \equiv (-1)^{(p-1)/2} (\bmod\ p)$ so that $p \equiv 1 (\bmod\ 4)$.

(ii) Let, first $(\frac{2}{p}) = 1$. Since $(\frac{8}{p}) = (\frac{4}{p})(\frac{2}{p}) = (\frac{2}{p}) = 1$. we see, by Proposition 3.3, that $p = \mathfrak{p}\mathfrak{p}'$ in $\mathbf{Q}(\sqrt{2})$. We have shown that $h = 1$ for $K = \mathbf{Q}(\sqrt{2})$ (page 61). Since $1 + \sqrt{2}$ is a unit of norm -1 in $\mathbf{Q}(\sqrt{2})$, $h_0 = h = 1$. Hence $p = x^2 - 2y^2$ for some $x, y \in \mathbf{Z}$. If $2 \mid y$, then $x^2 \equiv p (\bmod\ 8)$, and if $2 \nmid y$. $p \equiv x^2 - 2 (\bmod\ 8)$. In any case, $2 \nmid x$ so that $p \equiv \pm 1 (\bmod\ 8)$. Conversely, if $p \equiv \pm 1 (\bmod\ 8)$, consider $K = \mathbf{Q}(\sqrt{q})$ where $q = \pm p$ and $q \equiv 1 (\bmod\ 8)$. The discriminant of $\mathbf{Q}(\sqrt{q})$ is q. Since $(\frac{q}{2}) = 1$, we have $2\mathcal{O} = \mathfrak{p}\mathfrak{p}'$ for prime ideals $\mathfrak{p} \neq \mathfrak{p}'$. By Proposition 3.4, h_0 is odd. Since $\mathfrak{p}^{h_0} = \alpha\mathcal{O}$ for $\alpha \in \mathcal{O}$ with $N_K(\alpha) > 0$,

we have, on taking norms, $N_K(\alpha) = 2^{h_0}$, i.e. $2^{h_0+2} = x^2 - qy^2$ with $x, y \in \mathbf{Z}$. Since h_0 is odd, it follows that $(\frac{2}{p}) = 1$. Thus $(\frac{2}{p}) = 1$ if and only if $p \equiv \pm 1 (\mathrm{mod}\ 8)$ i.e. $(\frac{2}{p}) = (-1)^{(p^2-1)/8}$.

We deduce the well-known result due to Fermat, namely

Proposition 3.6 *An odd prime p is a sum of two squares of integers if and only if $p \equiv 1 (\mathrm{mod}\ 4)$.*

Proof: By Proposition 3.5, $(\frac{-1}{p}) = (-1)^{(p-1)/2}$. By the remark on page 61 , $(\frac{-1}{p}) = 1$ if and only if p is a sum of two squares of integers. Hence the proposition follows.

Proposition 3.7 *Let K be a quadratic field of discriminant $d = q_1 q_2$ where q_1, q_2 are distinct primes congruent to 3 modulo 4. Then, either q_1 or q_2 is the norm of an element $\alpha \in K,\ \alpha \succ 0$ (but not both).*

Proof: Observe first that for any unit $\epsilon \in K$, $N_K(\epsilon) = 1$. For if there exists $\alpha = \dfrac{x + y\sqrt{d}}{2}$ with $x, y \in \mathbf{Z}$ and $N_K(\alpha) = -1$, then $-4 \equiv x^2 (\mathrm{mod}\ \ q_1 q_2)$, i.e. $(\frac{-1}{q_1}) = (\frac{-4}{q_1}) = 1$ which, by Proposition 3.5, contradicts our assumption that $q_1 \equiv 3 (\mathrm{mod}\ , 4)$.

Now, if $\mathcal{O}$ is the ring of algebraic integers in K, then $q_1\mathcal{O} = \mathfrak{q}_1^2,\ q_2\mathcal{O} = \mathfrak{q}_2^2$ for prime ideals $\mathfrak{q}_1\mathfrak{q}_2$ by Proposition 3.2. Then by Theorem 3.1, there exist a_1, a_2 which are equal to 0 or 1 and such that $a_1 + a_2 > 0$ and $\mathfrak{q}_1^{a_1}\mathfrak{q}_2^{a_2} \approx \mathcal{O}$. If both a_1 and a_2 were equal to 1, then $\mathfrak{q}_1\mathfrak{q}_2 = \alpha\mathcal{O}$ with $\alpha \succ 0$. On the other hand $\sqrt{d}\mathcal{O} = \sqrt{(q_1 q_2)}\mathcal{O} = \mathfrak{q}_1\mathfrak{q}_2$ since $d = q_1 q_2$ and $q_1 q_2 \mathcal{O} = \mathfrak{q}_1^2\mathfrak{q}_2^2$. Hence $\alpha = \epsilon\sqrt{d}$ for a unit ϵ. But then $N_K(\epsilon) = -1$, whereas we have just proved that K contains no units of norm -1. Thus, either $a_1 = 0$ and $a_2 = 1$, or $a_1 = 1$ and $a_2 = 0$. Then either $\mathfrak{q}_2 \approx \mathcal{O}$ or $\mathfrak{q}_1 \approx \mathcal{O}$. Since $N(\mathfrak{q}_1) = q_1,\ N(\mathfrak{q}_2) = q_2$ we see that either q_1 or q_2 is the norm of $\alpha \in \mathcal{O}$ with $\alpha \succ 0$.

We have now the necessary preliminaries for the proof of the celebrated Law of Quadratic Reciprocity.

Theorem 3.2 *(Gauss.) For odd primes p and q.*

$$\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right)(-1)^{(p-1)(q-1)/4}.$$

Proof: Let r be the discriminant of a quadratic field K such that $\pm r$ is an odd prime and let s be an odd prime different from $|r|$. Let $(\frac{r}{s}) = 1$

Then, if $\mathcal{O}$ is the ring of algebraic integers in K, we have $s\mathcal{O} = \mathfrak{p}\mathfrak{p}'$ by Proposition 3.2. Further, $\mathfrak{p}^{h_0} = \alpha\mathcal{O}$ where $\alpha = \frac{x+y\sqrt{r}}{2} \succ 0$, and h_0 is the order of the restricted class group of K. Taking norms, $s^{h_0} = \frac{x^2-ry^2}{4}$. But h_0 is odd by Proposition 3.4. Hence $4s^{h_0}$ and consequently s is a quadratic residue modulo $|r|$ i.e. $\left(\frac{s}{|r|}\right) = 1$. We use this fact to prove the Law of Quadratic Reciprocity. We may suppose that $p \neq q$, since, otherwise, the theorem is trivial.

(i) Let $p \equiv 1 (\bmod\ 4)$. Taking $r = p, s = q$, we have

$$\left(\frac{p}{q}\right) = 1 \Rightarrow \left(\frac{q}{p}\right) = 1.$$

Similarly, if $q \equiv 1 (\bmod\ 4)$, we have, by the symmetry between p and q.

$$\left(\frac{q}{p}\right) = 1 \Rightarrow \left(\frac{p}{q}\right) = 1.$$

Thus, if $p \equiv q \equiv 1 (\bmod\ 4)$, then $(\frac{p}{q}) = (\frac{q}{p})$.

(ii) Let $p \equiv 1 (\bmod\ 4)$, $q \equiv 3 (\bmod\ 4)$. By (i) we have first

$$\left(\frac{p}{q}\right) = 1 \Rightarrow \left(\frac{q}{p}\right) = 1.$$

Conversely, let $(\frac{q}{p}) = 1$. Then $(\frac{-1}{p}) = 1$ by Proposition 3.5, and therefore $(\frac{-q}{p}) = (\frac{q}{p})(\frac{-1}{p}) = 1$. Taking $r = -q$, $s = p$ in the foregoing, we have $(\frac{p}{q}) = (\frac{p}{|r|}) = 1$. Thus we have shown that if $p \equiv 1 (\bmod 4)$ and $q \equiv 3 (\bmod 4)$,then $(\frac{p}{q}) = (\frac{q}{p})$. Again, by the symmetry between p and q, it follows that for $p \equiv 3 (\bmod 4)$ and $q \equiv 1 (\bmod 4) \cdot (\frac{p}{q}) = (\frac{q}{p})$.

(iii) Let $p \equiv q \equiv 3 (\bmod\ 4)$. Then, by Proposition 3.7, either p or q is the norm of an algebraic integer $\frac{x+y\sqrt{(pq)}}{2} \succ 0$. Without loss of generality, let $4p = x^2 - pqy^2$. This means that $p \mid x$, i.e. $x = pu$, $u \in \mathbf{Z}$. Hence $4 = pu^2 - qy^2$ and $-qy^2 \equiv 4 (\bmod\ p)$. Now $p \nmid y$ since $p \nmid 4$. Since $\mathbf{Z}/(p)$ if a field, $-q$ is a quadratic residue modulo p i.e $(\frac{-q}{p}) = 1$. Similarly, $pu^2 \equiv 4 (\bmod\ q)$ gives us $(\frac{p}{q}) = 1$. Since $(\frac{-1}{p}) = -1$ by Proposition 3.5, we have $(\frac{p}{q}) = -(\frac{q}{p}) = (-1)^{(p-1)(q-1)/4}(\frac{q}{p})$. We now use Legendre's symbol to define the Jacobi symbol $(\frac{a}{q})$ for odd composite denominators q. For two integers a and n of which n is odd and positive, we define the Jacobi symbol $(\frac{a}{n})$ by $(\frac{a}{n}) = (\frac{a}{p_1})^{r_1} \cdots (\frac{a}{p_k})^{r_k}$ where $n = p_1^{r_1} \cdots p_k^{r_k}$ and $p_1, \ldots, p_k$ are odd primes. Clearly, if any of $p_1, p_2, \ldots, p_k$ divides $a, (\frac{a}{n}) = 0$. Further it is easy to check that $(\frac{ab}{n}) = (\frac{a}{n})(\frac{b}{n})$ for odd positive n and $(\frac{a}{n}) = (\frac{a'}{n})$ if $a \equiv a' (\bmod\ n)$.

Remark 3.4 *For composite n, $(\frac{a}{n}) = 1$ does not, in general, ensure the existence of $x \in \mathbf{Z}$ for which $x^2 \equiv a(\bmod n)$.*

For negative odd n, we define $(\frac{a}{n})$ to be the Jacobi symbol $(\frac{a}{|n|})$. For Jacobi symbols, we have the general laws of reciprocity given by

Proposition 3.8 *For odd integers P, Q, we have*

$$\begin{aligned}\left(\frac{-1}{P}\right) &= (-1)^{(P-1)/2+(\operatorname{sgn} P-1)/2}\\ \left(\frac{2}{P}\right) &= (-1)^{(P^2-1)/8}\\ \left(\frac{P}{Q}\right) &= \left(\frac{Q}{P}\right)(-1)^{(P-1)(Q-1)/4+(\operatorname{sgn} P-1)(\operatorname{sgn} Q-1)/4}\end{aligned}$$

where, for real $x \neq 0$, $\operatorname{sgn} x = \frac{x}{|x|}$.

Proof: For odd $a, b \in \mathbf{Z}$, we have $(a-1)(b-1) \equiv 0(\bmod 4)$ i.e. $ab - 1 \equiv a - 1 + b - 1(\bmod\ 4)$ i.e.

$$\frac{ab-1}{2} \equiv \frac{a-1}{2} + \frac{b-1}{2}(\bmod\ 2). \tag{3.9}$$

Similarly, for a, b odd $(a^2-1)(b^2-1) \equiv 0(\bmod\ 16)$ and therefore

$$\frac{a^2b^2-1}{8} \equiv \frac{a^2-1}{8} + \frac{b^2-1}{8}(\bmod\ 2) \tag{3.10}$$

By iteration of (3.9) and (3.10) we see that for any r odd numbers $p_1, p_2, \ldots, p_r$ we have

$$\frac{p_1p_2\cdots p_r - 1}{2} \equiv \sum_{i=1}^{r} \frac{p_i - 1}{2}(\bmod 2) \tag{3.11}$$

and

$$\frac{(p_1p_2\cdots p_r)^2 - 1}{8} \equiv \sum_{i=1}^{r} \frac{p_i^2 - 1}{8}(\bmod 2) \tag{3.12}$$

Let us first suppose that $P, Q > 0$ and let $P = p_1p_2\cdots p_r$, $Q = q_1q_2\cdots q_s$, where $p_1, p_2, \ldots, p_r$, $q_1, q_2, \ldots, q_s$ are odd primes. By the definition of $(\frac{a}{p})$ and by Proposition 3.5, we have

$$\left(\frac{-1}{P}\right) = \left(\frac{-1}{p_1}\right)\cdots\left(\frac{-1}{p_r}\right) = (-1)^{\sum_{i=1}^{r}(p_i-1)/2} = (-1)^{(P-1)/2}$$

in view of (3.11) and

$$\left(\frac{2}{P}\right) = (-1)^{\sum_{i=1}^{r} \frac{p_i^2-1}{8}} = (-1)^{(p^2-1)/8}$$

in view of (3.12). Finally, by Theorem 3.2

$$\left(\frac{P}{Q}\right) = \prod_{\substack{1\le i\le r\\ 1\le j\le s}} \left(\frac{p_i}{q_j}\right) = \left\{ \prod_{\substack{1\le i\le r\\ 1\le j\le s}} \left(\frac{q_j}{p_i}\right)\right\}(-1)^{\sum_i (p_i-1)/2 \sum_j (q_j-1)/2}$$

so that, by (3.11), we have

$$\left(\frac{P}{Q}\right) = \left(\frac{Q}{P}\right)(-1)^{((P-1)/2((Q-1)/2} \quad \text{for odd } P, Q > 0. \tag{3.13}$$

If P is not necessarily positive,

$$\left(\frac{-1}{P}\right) = \left(\frac{-1}{|P|}\right) = (-1)^{(|P|-1)/2} = (-1)^{(P-1)/2+(\text{sgn } P-1)/2}$$

since $P = |P| \cdot \text{sgn } P$ and, by (3.9),

$$\frac{P-1}{2} \equiv \frac{|P|-1}{2} + \frac{\text{sgn } P-1}{2} (\text{mod } 2) \tag{3.14}$$

Hence, for odd P, Q, we have

$$\begin{aligned} \left(\frac{P}{Q}\right) &= \left(\frac{P}{|Q|}\right) = \left(\frac{\text{sgn } P}{Q}\right)\left(\frac{|P|}{Q}\right) \qquad (3.15)\\ &= \left(\frac{|P|}{Q}\right)(-1)^{((\text{sgn } P-1)/2)((\text{sgn } Q-1)/2+((\text{sgn } P-1)/2((\text{sgn } Q-1)/2))} \end{aligned}$$

Further, by (3.11)

$$\begin{aligned} \left(\frac{|P|}{Q}\right) &= \left(\frac{|P|}{|Q|}\right) = \left(\frac{|Q|}{|P|}\right)(-1)^{((|P|-1)/2)((|Q|-1)/2)}\\ &= \left(\frac{|Q|}{P}\right)(-1)^{((|P|-1)/2\cdot((|Q|-1)/2)}\\ &= \left(\frac{Q}{P}\right)(-1)^{(\text{sgn } Q-1)(P-1)/4+(\text{sgn } Q-1)(\text{sgn } P-1)/4+(|P|-1)(|Q|-1)/4}\\ &\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad (\text{by } (3.15))\\ &= \left(\frac{Q}{P}\right)(-1)^{((\text{sgn } Q-1)/2\cdot(|P|-1)/2+(|P|-1)/2(|Q|-1)/2} \quad (\text{by } (3.14)) \end{aligned}$$

Using (3.13) again, we have

$$\left(\frac{P}{Q}\right) = \left(\frac{Q}{P}\right)(-1)^{(P-1)(Q-1)/4+(\text{sgn } P-1)(\text{sgn } Q-1)/4}$$

We now define the Kronecker symbol $(\frac{a}{n})$ for any integer $a \equiv 0$ or $1(\bmod 4)$ as follows. First we define

$$\left(\frac{a}{2}\right) = \left(\frac{a}{-2}\right) = \begin{cases} 0 & \text{if } a \equiv 0(\bmod 4) \\ 1 & \text{if } a \equiv 1(\bmod 8) \\ -1 & \text{if } a \equiv 5(\bmod 8) \end{cases}$$

This agrees with our definition of $(\frac{d}{2})$ for the discriminant d of a quadratic field on page 61. By Proposition 3.8, $(\frac{a}{2}) = (\frac{2}{a})$, whenever $a \equiv 1(\bmod 4)$ Further, clearly $(\frac{a}{2}) = (\frac{a'}{2})$ for $a \equiv a'(\bmod 8)$ and $(\frac{aa'}{2}) = (\frac{a}{2})(\frac{a'}{2})$. In general, if $a \equiv 0$ or $1(\bmod 4)$, we introduce the Kronecker symbol $(\frac{a}{n})$ for arbitrary denominator n by setting $(\frac{a}{2^c}) = (\frac{a}{2})^c$ and $(\frac{a}{n}) = (\frac{a}{n_1}) \cdot (\frac{a}{2^c})$ where $n = n_1 \cdot 2^c,\ c \geq 0$ and n_1 is odd. By the very definition, it is clear that $(\frac{a}{xy}) = (\frac{a}{x})(\frac{a}{y})$ for $x, y \in \mathbf{Z}$.

For the discriminant d of a quadratic field, we see that $(\frac{d}{xy}) = (\frac{d}{x})(\frac{d}{y})$ for $x, y \in \mathbf{Z}$. i.e. $(\frac{d}{z})$ is multiplicative in z. We now prove another interesting property of $(\frac{d}{n})$.

Proposition 3.9 *If d is the discriminant of a quadratic field and m, n are positive integers, then*

$$\left(\frac{d}{n}\right) = \left(\frac{d}{m}\right) \text{ for } n \equiv m(\bmod\ d) \tag{3.16}$$

$$\left(\frac{d}{n}\right) = \left(\frac{d}{m}\right) \text{sgn } d \text{ for } n \equiv -m(\bmod\ \ d) \tag{3.17}$$

PROOF: Let $d = 2^a \cdot d',\ n = 2^b \cdot n',\ m = 2^c \cdot m'$ with odd d', n', m' and $a, b, c \geq 0$ in $\mathbf{Z}$.

(i) Let $a > 0$. The case $b > 0$ is trivial, for then, by assumption, $c > 0$, and both the symbols in this proposition are zero, by definition. Let then $b = c = 0$. By Proposition 3.8

$$\left(\frac{d}{n}\right) = \left(\frac{2^a \cdot d'}{n}\right) = \left(\frac{2}{n}\right)^a \left(\frac{d'}{n}\right) = (-1)^{a(n^2-1)/8}\left(\frac{n}{d'}\right)(-1)^{(n-1)(d'-1)/4}$$

and similarly

$$\left(\frac{d}{m}\right) = \left(\frac{2^a d'}{m}\right) = (-1)^{a(m^2-1)/8}\left(\frac{m}{d'}\right)(-1)^{(m-1)(d'-1)/4}$$

Since $4 \mid d$, the first factors coincide for m and n. The same is true also of the other two factors, in the case $n \equiv m(\bmod d)$. But if $n \equiv -m(\bmod d)$, they differ exactly by the factor $\operatorname{sgn} d' = \operatorname{sgn} d$.

(ii) Let $a = 0$. Consequently, $d \equiv 1(\bmod 4)$. Then

$$\left(\frac{d}{n}\right) = \left(\frac{d}{2^b n'}\right) = \left(\frac{d}{2}\right)^b \cdot \left(\frac{d}{n'}\right) = \left(\frac{2}{d}\right)^b \left(\frac{d}{n'}\right)$$

since $(\frac{d}{2}) = (\frac{2}{d})$ for $d \equiv 1(\bmod 4)$. Further, by Proposition 3.8,

$$\left(\frac{d}{n'}\right) = \left(\frac{n'}{d}\right)(-1)^{(d-1)(n'-1)/4} = \left(\frac{n'}{d}\right)$$

since n' is odd and $d \equiv 1(\bmod 4)$. Thus $(\frac{d}{n}) = (\frac{n}{d})$. Further $(\frac{-1}{d}) = \operatorname{sgn} d$. Therefore $(\frac{d}{m}) = (\frac{d}{n})$ for $m, n > 0$ and $m \equiv n(\bmod d)$ and $(\frac{d}{n}) = (\frac{n}{d}) = (\frac{-m}{d}) = \operatorname{sgn} d \cdot (\frac{m}{d}) = (\frac{d}{m}) \cdot \operatorname{sgn} d$ if $n \equiv -m(\bmod d)$.

Remark 3.5 *Thus, for positive integers n, $(\frac{d}{n})$ represents a so-called "residue class character" modulo d, i.e. $(\frac{d}{m}) = (\frac{d}{n})$ for $m, n > 0, m \equiv n(\bmod d)$ and $(\frac{d}{mn}) = (\frac{d}{m})(\frac{d}{n})$ for $m, n > 0$. In particular, if p_1, p_2 are two primes satisfying $p_1 \equiv p_2(\bmod d)$ and $p_1 \nmid d$, then either both p_1 and p_2 split or both stay prime in $\mathbf{Q}(\sqrt{d})$.*

In what follows, a *discriminant* will stand for an integer $d \neq 1$ which is the discriminant of a quadratic field; in other words, it will denote either a square-free integer $d \neq 1$ with $d \equiv 1(\bmod 4)$ or $d = 4d'$ where d' is square-free and $d' \equiv 2$ or $3(\bmod 4)$. Whenever $n, m > 0$, $n \equiv m(\bmod d)$, we have $(\frac{d}{n}) = (\frac{d}{m})$.

Remark 3.6 (1) *Any discriminant d can be written in the form $d = d_1 d_2$, where d_1 is 1 or a discriminant, d_2 is an odd discriminant and the only prime divisor of d_1 if 2 if $|d_1| > 1$.*

(2) *If a, b are integers with $(a, b) = 1$, and α, β are any integers, there exists $n > 0$ with $n \equiv \alpha(\bmod a)$, $n \equiv \beta(\bmod b)$; in fact, if x, y are integers with $xa \equiv \beta(\bmod b)$, $yb \equiv \alpha(\bmod a)$, we may take $n = xa + yb + k|ab|$, where k is a large integer.*

Proposition 3.10 *If d is a discriminant, there exists $n > 0$, $n \in \mathbf{Z}$ with $(\frac{d}{n}) = -1$.*

PROOF: CASE 1. d is odd. If d is odd, then, for any odd $n > 0$ we have, by Proposition 3.9, (case (ii) of the proof)

$$\left(\frac{d}{n}\right) = \left(\frac{n}{d}\right) = \left(\frac{n}{|d|}\right).$$

Let $|d| = pa$, where p is an odd prime. We have $p \nmid a$ a since d is square-free. Let u be a quadratic non-residue modulo p. By our remark above, there is an (odd) $n > 0$ such that $n \equiv u(\bmod p)$, $n \equiv 1(\bmod 2a)$. Then

$$\left(\frac{d}{n}\right) = \left(\frac{n}{p}\right)\left(\frac{n}{a}\right) = \left(\frac{u}{p}\right)\left(\frac{1}{a}\right) = -1.$$

CASE 2. d is even. Let $d = d_1 d_2$, where d_1 is an even discriminant, and d_2 is an odd discriminant. Then, for $n > 0$ in $\mathbf{Z}$, we have $(\frac{d}{n}) = (\frac{d_1}{n})(\frac{d_2}{n})$ (by definition). Again, by definition, it is easy to check that there exists a with $(\frac{d_1}{a}) = -1$. Choose $n > 0$ such that $n \equiv a(\bmod\ d_1)$ and $n \equiv 1(\bmod\ d_2)$. We then have $(\frac{d}{n}) = -1$.

Proposition 3.11 *Let d be a discriminant and $S_m = \sum_{n=1}^{m} (\frac{d}{n})$. Then $|S_m| \leq \frac{1}{2}|d|$.*

PROOF: We first prove the following: let $a_1, \ldots, a_r$, $r = |d|$, denote a complete system of residues modulo r, i.e. a system of integers which are congruent to the integers $0, 1, \ldots, r-1$ modulo r (in some order). Then $S = \sum_{i=1}^{r} (\frac{d}{a_i}) = 0$. In fact, let n be a positive integer with $(n, d) = 1, (\frac{d}{n}) = -1$; then the numbers $na_1, \ldots, na_r$ also form a complete system of residues modulo r. Now $(\frac{d}{b}) = (\frac{d}{c})$ if $b \equiv c(\bmod\ r)$. We have therefore

$$S = \sum_{i=1}^{r} \left(\frac{d}{na_i}\right) = -\sum_{i=1}^{r} (\frac{d}{a_i}) = -S, \text{ so that } S = 0.$$

Given $m > 0$, let k be a positive integer for which $|m - kr|$ is minimal. Then we have $|m - kr| \leq \frac{1}{2}r$; Hence $|S_m - S_{kr}| \leq \frac{1}{2}$; but S_{kr} is the sum of k terms $\sum_{i=1}^{r} (\frac{d}{a_i})$ where $a_1, \ldots, a_r$ runs over a complete residue system modulo r, and is hence zero. Thus $|S_m| \leq \frac{1}{2}r$.

3.5 The Dirichlet class-number formula

Let K be an algebraic number field of degree n. The group $\mathfrak{h}$ of ideal classes of K is a finite group of order $h = h(K)$. We shall obtain, in this section, a formula for h in the case when K is a quadratic field.

Let $C_0 = 1, C_1, \ldots, C_{h-1}$ denote the different ideal classes. For each class C, we define the *zeta-function* of C, denoted $\zeta_K(s, C)$, by

$$\zeta_K(s, C) = \sum_{\mathfrak{a} \in C}{}' (N(\mathfrak{a}))^{-1};$$

the summation is over all non-zero integral ideals $\mathfrak{a}$ in C and s is a real number > 1. The zeta-function $\zeta_K(s)$ of the field K is defined by

$$\zeta_K(s) = \sum_{C \in \mathfrak{h}} \zeta_K(s, C) = \sum_{\mathfrak{a}}{}' (N(\mathfrak{a}))^{-s}$$

the summation now being over all nonzero integral ideals of K.

We assert now that all these series converge (absolutely) for $s > 1$. It is, of course, sufficient to verify this for the series defining $\zeta_K(s)$. Let $x > 0$ be any real number. We have

$$\sum_{N(\mathfrak{a}) \leq x} \frac{1}{N(\mathfrak{a}))^s} \leq \prod_{N(\mathfrak{p}) \leq x} (1 - (N(\mathfrak{p}))^{-s})^{-1} \tag{3.18}$$

the product being over all prime ideal $\mathfrak{p}$ with $N(\mathfrak{p}) \leq x$. To prove this, we remark that

$$(1 - (N(\mathfrak{p}))^{-s})^{-1} = 1 + (N(\mathfrak{p}))^{-s} + (N(\mathfrak{p}))^{-2s} + \cdots \tag{3.19}$$

and that any integral ideal $\mathfrak{a}$ can be written uniquely as a product of prime ideals; further if $N(\mathfrak{a}) \leq x$, then every prime divisor $\mathfrak{p}$ of $\mathfrak{a}$ satisfies $N(\mathfrak{p}) \leq x$. Inequality (3.18) follows on multiplying out the finitely many absolutely convergent series (3.19) with $N(\mathfrak{p}) \leq x$; moreover, we have

$$\prod_{N(\mathfrak{p}) \leq x} (1 - (N(\mathfrak{p}))^{-s})^{-1} - \sum_{N(\mathfrak{a}) \leq x} (N(\mathfrak{a}))^{-s} = \sum_{N(\mathfrak{a}) > x} (N(\mathfrak{a}))^{-s} \tag{3.20}$$

where the latter summation is over the integral ideals $\mathfrak{a}$ of norm $> x$ all of whose prime divisors are of norm $\leq x$.

Any prime ideal $\mathfrak{p}$ contains a unique prime number $p \in \mathbf{Z}$, by Remark 2.18. We have $N(\mathfrak{p}) = p^f$ for a certain integer $f \geq 1$, so that

$p \leq x$ if $N(\mathfrak{p}) \leq x$. Further, there are at most n distinct prime ideals $\mathfrak{p}_1, \ldots, \mathfrak{p}_g$, $g \leq n$ containing a given p; in fact, they are uniquely determined by the equation

$$p\mathcal{O} = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_g^{e_g}$$

and then

$$p^n = N(p\mathcal{O}) = \prod_{i=1}^{g} N(\mathfrak{p}_i)^{e_i} = \prod_{i=1}^{g} p^{f_i e_i} \geq p^g \text{ (since } f_i \geq 1, e_i \geq 1),$$

so that $g \leq n$. Hence (3.18) gives

$$\sum_{N(\mathfrak{a}) \leq x} (N(\mathfrak{a}))^{-s} \leq \prod_{p \leq x} (1 - p^{-s})^{-n};$$

since the product $\prod (1 - p^{-s})^{-1}$ is absolutely convergent for $s > 1$, the series $\sum (N(\mathfrak{a}))^{-s}$ converges for $s > 1$. If we now let $x \to \infty$ in (3.20) we obtain the Euler product for $\zeta_K(S)$, viz.

$$\zeta_K(s) = \prod_{\mathfrak{p}} (1 - (N(\mathfrak{p}))^{-s})^{-1}.$$

Note that this equation also holds when s is complex and $\operatorname{Re} s > 1$.

Remark 3.7 *The same reasoning shows that if $\{a_m\}$ is a sequence of complex numbers with $a_1 = 1$, $a_{mk} = a_m a_k$ for all integers $m, k \geq 1$, and if $\sum_{m=1}^{\infty} |a_m| < \infty$,then*

$$\sum_{m=1}^{\infty} a_m = \prod_{p} (1 - a_p)^{-1}.$$

In particular, for $\operatorname{Re} s > 1$, *we have*

$$\zeta(s) = \sum_{m=1}^{\infty} m^{-s} = \prod_{p} (1 - p^{-s})^{-1}.$$

Lemma 3.1 *Let $\{a_m\}$ be a sequence of real numbers, X a real positive number. Let $A(X) = \sum_{m<X} a_m$. Suppose that*

$$\lim_{X \to \infty} \frac{A(X)}{X} = c. \tag{3.21}$$

Then the series

$$f(s) = \sum_{m=1}^{\infty} \frac{a_m}{m^s}$$

converges for $s > 1$ *and we have*

$$\lim_{s \to 1+0} (s-1) f(s) = c.$$

PROOF: Since $A(1) = 0$, we have, for $M > 0$ in $\mathbf{Z}$.

$$\begin{aligned} \sum_{m=1}^{M} a_m m^{-s} &= \sum_{m=1}^{M} \{A(m+1) - A(m)\} m^{-s} \\ &= A(M+1)M^{-s} + \sum_{m=1}^{M-1} A(m+1)\{m^{-s} - (m+1)^{-s}\}. \end{aligned} \tag{3.22}$$

Now $\sum_{m=1}^{\infty} m^{-s} = \zeta(s)$ converges for $s > 1$, and as $M \to \infty$, $A(M+1)M^{-s} \to 0$, for $s > 1$. We see, on applying this to the sequence $\{a_m = 1\}$, that

$$\sum_{m=1}^{\infty} m\{m^{-s} - (m+1)^{-s}\} = \zeta(s).$$

Now $m^{-s} - (m+1)^{-s} = s \int_m^{m+1} x^{-s-1} dx$, and $0 \le x - m \le 1$ in the interval $(m, m+1)$. Hence

$$\left| \zeta(s) - \sum_{m=1}^{\infty} s \int_m^{m+1} x^{-s} dx \right| < s \int_1^{\infty} x^{-s-1} dx = 1,$$

i.e.

$$\left| \zeta(s) - s \int_1^{\infty} x^{-s} dx \right| = \left| \zeta(s) - \frac{s}{s-1} \right| < 1;$$

in particular

$$\lim_{s \to 1+0} (s-1)\zeta(s) = 1. \tag{3.23}$$

Since, by (3.21), $|A(m+1)| \le K_1 m$ for some $K_1 > 0$, and since $\sum_{m=1}^{\infty} m\{m^{-s} - (m+1)^{-s}\}$ converges (absolutely) for $s > 1$,(3.22) implies that $\sum_{m=1}^{\infty} a_m m^{-s} = f(s)$ converges for $s > 1$; moreover, we have

$$|f(s) - c\zeta(s)| = \sum_{m=1}^{\infty} |A(m+1) - cm| \{m^{-s} - (m+1)^{-s}\}$$

Given $\epsilon > 0$, there exists, by (3.21), an $m_0 = m_0(\epsilon)$ with $|A(m+1) - cm| < \epsilon m$ for $m > m_0$. Then, for $s > 1$,

$$\begin{aligned} |f(s) - c\zeta(s)| &\leq \sum_{m=1}^{m_0} |A(m+1) - cm| + \epsilon \sum_{m>m_0} m\{m^{-s} - (m+1)^{-s}\} \\ &\leq C(m_0) + \epsilon\zeta(s). \end{aligned}$$

Since $(s-1)\zeta(s) \to 1$ as $s \to 1+0$, we obtain

$$\limsup_{s\to+0} (s-1)|f(s) - c\zeta(s)| \leq \epsilon.$$

Since this is true for any $\epsilon > 0$, we obtain

$$\lim_{s\to1+0}(s-1)f(s) = c \lim_{s\to1+0}(s-1)\zeta(s) = c.$$

As an application of these remarks, we prove

Proposition 3.12 *$\zeta(s)$ is meromorphic in* $\mathrm{Re}\ s > 0$*, its only singularity in the half-plane* $\mathrm{Re}\ s > 0$ *is at $s = 1$ where it has a simple pole with residue 1.*

Proof: We have, for $s > 1$,

$$\begin{aligned} \zeta(s) &= \sum_{m=1}^{\infty} m\{m^{-s} - (m+1)^s\} = s\sum_{m=1}^{\infty} m \int_m^{m+1} u^{-s-1}du \\ &= s\sum_{m=1}^{\infty} \int_m^{m+1} [u]u^{-s-1}du = s\int_1^{\infty} \frac{[u]}{u^{s+1}}du \end{aligned}$$

where $[u]$ is the largest integer $\leq u$. Now $[u] = u - (u)$, where $0 \leq (u) < 1$. Hence, for $s > 1$,

$$\zeta(s) = s\int_1^{\infty} u^{-s}du - s\int_1^{\infty} \frac{(u)}{u^{s+1}}du = \frac{s}{s-1} - s\int_1^{\infty} \frac{(u)}{u^{s+1}}du.$$

Now, for $\mathrm{Re}\ \geq \delta > 0$, $|(u)u^{-s-1}| < u^{-\delta-1}$, so that the latter integral converges uniformly for $\mathrm{Re}\ s \geq \delta > o$ for any $\delta > 0$, and so defines a holomorphic function $g(s)$ for $\mathrm{Re}\ s > 0$. Since, for $s > 1$, $\zeta(s) - \frac{s}{s-1} = -sg(s)$ the proposition follows.

Remark 3.8 *If we set $A'(X) = \sum_{m\leq X} a_m$, then (3.21) holds if and only if $X^{-1}A'(X) \to c$ as $X \to \infty$. In fact, either of these conditions implies that $m^{-1}a_m \to 0$ as $m \to \infty$, and they are therefore equivalent.*

Definition 3.6 *By a lattice point in the plane* $\mathbf{R}^2$ *we mean a point* $\zeta = (\xi_1, \xi_2)$ *with* $\xi_1, \xi_2 \in \mathbf{Z}$.

Lemma 3.2 *Let* Ω *be a bounded open set in the plane* $\mathbf{R}^2$. *For* $X > 0$, *let* $\Omega_X = \{\zeta = (\xi_1, \xi_2) \in \mathbf{R}^2 \mid (\frac{\xi_1}{X}, \frac{\xi_2}{X}) \in \Omega\}$. *Let* $N_\Omega(X)$ *denote the number of lattice points in* Ω_X. *Then*

$$\lim_{X\to\infty} X^{-2} N_\Omega(X) = \iint_\Omega d\xi_1\, d\xi_2 = \text{ area of } \Omega$$

provided that this integral exists in the sense of Riemann.

PROOF: Divide the plane into closed squares S of sides $\frac{1}{X}$ parallel to the coordinate axes. For any S, let $P(S)$ denote the point whose coordinates have smallest values ("the lower left vertex"). Clearly $N_\Omega(X) = \{\text{number of } S \text{ with } P(S) \in \Omega\}$.

Now, if N_1, N_2 denote, respectively, the number of S with $S \subset \Omega$, $S \cap \Omega \neq \emptyset$, then, by the definition of the Riemann integral, $X^{-2}N_1$, $X^{-2}N_2 \to \int\int_\Omega d\xi_1\, d\xi_2$; since $N_1 \leq N_\Omega(X) \leq N_2$, the lemma follows.

Theorem 3.3 *(Dedekind.) Let* K *be a quadratic field of discriminant* d *and* w *the number of roots of unity in* K. *Let* C *be an ideal class of* K *and* $N(X, C)$ *the number of non-zero integral ideals* $\mathfrak{a} \in C$ *with* $N(\mathfrak{a}) < X$. *Then*

$$\lim_{X\to\infty} \frac{N(X, C)}{X} = \kappa$$

exists and we have

$$\kappa = \begin{cases} \dfrac{2\log\eta}{\sqrt{d}} \text{ if } d > 0, \eta > 1 \text{ being the fundamental unit;} \\ 2\pi/(w\sqrt{|d|} \text{ if } d < 0. \end{cases}$$

PROOF: Let $\mathfrak{b}$ be an integral ideal in C^{-1} then, for any integral ideal $\mathfrak{a} \in C$, $\mathfrak{a}\mathfrak{b} = \alpha\mathcal{O}$ where $\alpha \in \mathfrak{b}$. Conversely, if $\alpha \in \mathfrak{b}$, $\mathfrak{a} = \mathfrak{b}^{-1}\alpha\mathcal{O}$ is an integral ideal in C; moreover, $|N_K(\alpha)| = N(\mathfrak{a})N(\mathfrak{b})$ so that $N(\mathfrak{a}) < X$ if and only if $|N_K(\alpha)| < XN(\mathfrak{b}) = Y$(say). Consequently $N(X, C)$ is the number of non-zero principal ideals $\alpha\mathcal{O}$, $\alpha \in \mathfrak{b}$, $|N_K(\alpha)| < Y$; in other words, $N(X, C) =$ the number of $\alpha \in \mathfrak{b}$, $\alpha \neq 0$, which are pairwise non-associates and for which $|N_K(\alpha)| < Y$.

Case (i) $d > 0$. Let $\eta > 1$ be the fundamental unit. Clearly for any $\alpha \in \mathfrak{b},\ \alpha \neq 0$, there is an integer m such that if $\omega = \eta^m \alpha$, we have

$$0 \leq \log \left| \frac{\omega}{|N_K(\omega|^{\frac{1}{2}}} \right| < \log \eta. \tag{3.24}$$

Conversely, if ω_1, ω_2 are associate elements of $\mathfrak{b}$ satisfying (3.24), then $\omega_1 = \epsilon \omega_2$, where ϵ is a unit with $1 \leq |\epsilon| < \eta$, so that $\epsilon = \pm 1$. Hence

$$2N(X, C) = \begin{cases} \text{the number of } \omega \in \mathfrak{b} \text{ with} \\ 0 < |N_K(\omega)| < Y,\ 0 \leq \log \left| \dfrac{\omega}{|N_K(\omega)|^{\frac{1}{2}}} \right| < \log \eta \end{cases} \tag{3.25}$$

Case (ii) $d < 0$. Clearly we have now, $wN(X, C) =$ the number of integers $\omega \in \mathfrak{b}$ with $0 < |N_K(\omega)| < Y$.

In either case, let (β_1, β_2) be an integral base of $\mathfrak{b}$ and let β_1', β_2' be the conjugates of β_1, β_2 respectively. Let Ω denote the following open set in the plane: if $d > 0$,

$$\Omega = \Big\{ \zeta = (\xi_1, \xi_2) \in \mathbf{R}^2 \mid 0 < |\xi_1\beta_1 + \xi_2\beta_2||\xi_1\beta_1' + \xi_2\beta_2'| < 1,$$

$$0 < \log \frac{|\xi_1\beta_1 + \xi_2\beta_2|}{|\xi_1\beta_1 + \xi_2\beta_2|^{\frac{1}{2}} |\xi_1\beta_1' + \xi_2\beta_2'|^{\frac{1}{2}}} < \log \eta \Big\},$$

and if $d < 0$,

$$\Omega = \{ \zeta = (\xi_1, \xi_2) \in \mathbf{R}^2 \mid 0 < |\xi_1\beta_1 + \xi_2\beta_2|^2 < 1 \}.$$

We verify that Ω is bounded as follows. For $d > 0$, since

$$|\xi_1\beta_1 + \xi_2\beta_2||\xi_1\beta_1' + \xi_2\beta_2'| < 1$$

and

$$1 \leq |\xi_1\beta_1 + \xi_2\beta_2| / |\xi_1\beta_1' + \xi_2\beta_2'| < \eta^2,$$

we see that both $\xi_1\beta_1 + \xi_2\beta_2,\ \xi_1\beta_1' + \xi_2\beta_2'$ are bounded in Ω. Thus ξ_1, ξ_2 are again bounded in Ω, since $\beta_1\beta_2' - \beta_2\beta_1' \neq 0$ (in fact $= \pm N(\mathfrak{b})\sqrt{d}$ by (3.2)). If $d < 0$, then $|\xi_1\beta_1 + \xi_2\beta_2| = |\xi_1\beta_1' + \xi_2\beta_2'| < 1$, and again, since $\beta_1\beta_2' - \beta_2\beta_1' \neq 0,\ \xi_1, \xi_2$ are bounded in Ω. According to what we have proved above, we have

$$wN(X, C) = \begin{cases} \text{number of lattice points in } \Omega_{\sqrt{Y}} \text{ if} d < 0 \\ \text{number of lattice points in } \Omega_{\sqrt{Y}} + \text{the number } A_Y \\ \text{of lattice points } (\xi_1, \xi_2) \text{ with } |\xi_1\beta_1 + \xi_2\beta_2|^2 \leq Y \\ \text{and } |\xi_1\beta_1 + \xi_2\beta_2| = |\xi_1\beta_1' + \xi_2\beta_2'| \neq 0 \text{ if } d < 0. \end{cases}$$

Since, as is easily verified. $A_Y = O(\sqrt{Y}) = O(\sqrt{X})$, we conclude that

$$\begin{aligned}\lim_{X\to\infty}\frac{wN(X,C)}{X} &= N(\mathfrak{b})\lim_{Y\to\infty}\frac{N_\Omega(\sqrt{Y})}{Y}\\ &= N(\mathfrak{b})\iint_\Omega d\xi_1\, d\xi_2 \qquad (3.26)\end{aligned}$$

(The last equation holds by Lemma 3.2.) If $d>0$, we set $u_1=\xi_1\beta_1+\xi_2\beta_2,\ u_2=\xi_2\beta_1'+\xi_2\beta_2'$ then, since $|\beta_1\beta_2'-\beta_2\beta_1'|=N(\mathfrak{b})\sqrt{d}$, we have

$$\iint_\Omega d\xi_1\, d\xi_2 = \frac{4}{N(\mathfrak{b})\sqrt{d}}\iint_{U^*} du_1\, du_2,$$

where

$$U^*=\Big\{(u_1,u_2)\mid 0<u_1u_2<1;\ 1<\frac{u_1}{u_2}<\eta^2,\ u_1,u_2>0\Big\}.$$

Making the change of variables $v_1=u_1u_2,\ v_2=u_1/u_2$ we see that $\iint_\Omega d\xi_1 d\xi_2 = \dfrac{4\log\eta}{N(\mathfrak{b})\sqrt{d}}$ so that, with (3.26) this gives us Theorem 3.3 when $d>0$. If $d<0$, we set $u_1=\mathrm{Re}\,(\xi_1\beta_1+\xi_2\beta_2),\ u_2=\mathrm{Im}\,(\xi_1\beta_1+\xi_2\beta_2)$ and find that

$$\iint_\Omega d\xi_1\, d\xi_2 = \frac{2}{N(\mathfrak{b})\sqrt{d}}\iint_{u_1^2+u_2^2<1} du_1\, du_2 = \frac{2\pi}{n(\mathfrak{b})\sqrt{d}}$$

and Theorem 3.3 is completely proved.

Let K be, as above, a quadratic field of discriminant d, and, for $X>0, N(X,K)$ the number of integral ideals $\mathfrak{a}$ of norm $N(\mathfrak{a})<X$. Since the number κ in Theorem 3.3 is independent of the class C, we conclude that

$\lim_{X\to\infty}\frac{N(X;K)}{X}=h\cdot\kappa,\ h$ being the class number

Further, if a_m denotes the number of integral ideals of norm $=m$, then $N(X;K)=\sum_{m<X}a_m$, while $\zeta_K(S)=\sum_{m=1}^{\infty}\frac{a_m}{m^2}$. Hence, by Lemma 3.1, we obtain

Proposition 3.13 *(Dedekind) We have*

$$\lim_{s\to 1+0}(s-1)\zeta_K(S)=h\cdot\kappa,$$

where h is the class number of the quadratic field K, and κ is the number defined in Theorem 3.3.

We shall evaluate the above limit in another way. We have already proved that

$$\zeta_K(s) = \prod_{\mathfrak{p}} (1 - (N(\mathfrak{p}))^{-s})^{-1}.$$

Let p be any (rational) prime number; then there are at most two prime ideals $\mathfrak{p}, \mathfrak{p}'$ dividing p. We claim that the product

$$\prod_{\mathfrak{p} \supset p} (1 - (N(\mathfrak{p}))^{-s})^{-1} = (1 - p^{-s})^{-1} \left(1 - \left(\frac{d}{p}\right) p^{-s}\right)^{-1}$$

In fact, by Propositions 3.2 and 3.3 $(\frac{d}{p}) = 0$ for $p \mid d$ and there is a unique $\mathfrak{p} \supset p\mathcal{O}$ with $\mathfrak{p}^2 = p\mathcal{O}$ and $N(\mathfrak{p}) = p$. If $(\frac{d}{p}) = -1$, there is a unique $\mathfrak{p} \supset p\mathcal{O}$; indeed $\mathfrak{p} = p\mathcal{O}$, so that $N(\mathfrak{p}) = p^2$ and then $1 - (N(\mathfrak{p}))^{-s} = (1 - p^{-2s}) = (1 - p^{-s})(1 + p^{-s})$. If $(\frac{d}{p}) = 1$, there are two distinct prime ideals $\mathfrak{p}$ with $\mathfrak{p} \supset p\mathcal{O}$ and $N(\mathfrak{p}) = p$ for each of them, so that $\prod_{\mathfrak{p} \supset p} (1 - N(\mathfrak{p})^{-s})^{-1} = (1 - p^{-s})^2$. We see therefore that

$$\zeta_K(s) = \prod_{p} (1 - p^{-s})^{-1} \left(1 - \left(\frac{d}{p}\right) p^{-s}\right)^{-1}$$

The Euler product for $\zeta_K(s)$ applied to the field $K = \mathbf{Q}$ gives us

$$\zeta(s) = \sum_{m=1}^{\infty} m^{-s} = \prod_{p} (1 - p^{-s})^{-1}.$$

The remark after the proof of the Euler product for $\zeta_K(s)$ applied to $a_m = (\frac{d}{m}) m^{-s}$ gives us

$$L_d(s) = \sum_{m=1}^{\infty} \left(\frac{d}{m}\right) m^{-s} = \prod_{p} \left(1 - \left(\frac{d}{p}\right) p^{-s}\right)^{-1}.$$

Hence we have

Proposition 3.14 *For $s > 1$, we have*

$$\zeta_K(s) = \zeta(s) L_d(s).$$

We assert that the series defining $L_d(s)$ converges for $s > 0$. In fact, after Proposition 3.11, this follows from

Proposition 3.15 *If $\{a_m\}$ is a sequence of complex numbers such that $A_m = \sum_{k=1}^{m} a_k$ is bounded as $m \to \infty$, then the series*

$$f(s) = \sum_{1}^{\infty} \frac{a_m}{m^s}$$

converges for $\sigma = \mathrm{Re}\ s > 0$, and uniformly on any bounded subset of the half plane $\sigma \geq \delta$, for fixed $\delta > 0$.

PROOF: We have

$$\sum_{m=a}^{b} a_m m^{-s} = A_b b^{-s} - A_a a^{-s} + \sum_{m=a+1}^{b} A_m (m^{-s} - (m+1)^{-s})$$

For $\sigma \geq \delta$,we have $|m^{-s} - (m+1)^{-s}| = |s \int_m^{m+1} u^{-s-1} du| \leq \frac{s}{\sigma} m^{-\delta-1}$. Hence, if $|A_m \leq M$ for all $m > 0$ in $\mathbf{Z}$, then

$$\Big| \sum_{a}^{b} a_m m^{-s} \Big| \leq M \Big\{ b^{-\delta} + a^{-\delta} + \frac{|s|}{\sigma} \sum_{m=a+1}^{b} m^{-\delta-1} \Big\} \to 0$$

as $a, b \to \infty$ uniformly in any bounded subset of $\sigma \geq \delta$. This proves the proposition.

Using the fact that $(s-1)\zeta(s) \to 1$ as $s \to 1+0$ we obtain, by Propositions 3.13, 3.14 and Theorem 3.3, the following.

Theorem 3.4 *(Dirichlet) Let K be a quadratic field of discriminant d. Let h be the class number of K. Then we have*

$$h = \begin{cases} \dfrac{\sqrt{d}}{2 \log \eta} L_d(1) & \text{if } d > 0 \\ \dfrac{w\sqrt{d}}{2\pi} L_d(1) & \text{if } d < 0. \end{cases} \tag{3.27}$$

Note that (3.27) implies that $L_d(1) > 0$. It is possible to express the series $L_d(1)$ as a finite (elementary) sum. Moreover, the fact that $L_d(1) > 0$ is one of the key propositions in the proof of Dirichlet's theorem that for any integer l with $(l, d) = 1$, *there exist infinitely many primes $p \equiv l (\mathrm{mod}\ d)$*; this theorem will be proved in the next section.

Definition 3.7 *The degree of prime ideal $\mathfrak{p}$ is the integer f for which $N(\mathfrak{p}) = p^f$ where p is a rational prime.*

Proposition 3.16 *Let K be a quadratic field of discriminant d. Then there exist in K infinitely many prime ideals of degree* 1*, and infinitely many prime ideals of degree* 2*.*

PROOF: Clearly, for any prime ideal $\mathfrak{p}$, we have $N(\mathfrak{p}) = p$ with $f = 1$ or 2. Suppose that $f > 1$ for all but finitely many $\mathfrak{p}$. Then for $s > 1$,

$$\prod_p (1 - N(\mathfrak{p})^{-s})^{-1} \leq \prod_{q \in F} (1 - q^{-s})^{-2} \prod_p (1 - p^{-2s})^{-1}$$

where F is a finite set of (rational) primes, and p runs over all (rational) primes. The product $\prod_{\mathfrak{p}} (1 - N(\mathfrak{p})^{-s})^{-1}$ would thus converge for all $s > \frac{1}{2}$ Since for $s > 1$, this product $= \zeta_K(s)$, we could conclude that $\zeta_K(s)$ is bounded as $s \to 1 + 0$. But we know that this is not the case, since $\lim_{s \to 1+0}(s-1)\zeta_K(s) \neq 0$ by Proposition 3.13 .

Suppose now that the degree of $\mathfrak{p}$ is 1 for all but finitely many $\mathfrak{p}$. We would have, for $s > 1$,

$$\zeta_K(s) = \prod_p (1 - N(\mathfrak{p})^{-s})^{-1} = \prod_{p > p_0} (1 - p^{-s})^{-2} \times \prod_{p \leq p_0} \prod_{\mathfrak{p} \supset p} (1 - N(\mathfrak{p})^{-s})^{-1},$$

where p_0 is large enough. (If $p_0 \geq |d|$, then p splits or stays prime in K for $p > p_0$, so that there would be exactly two prime divisors $\mathfrak{p}$ of $p\mathcal{O}$ except for finitely many p.) By (3.23) we have clearly $\lim_{s \to 1+0}(s - 1) \prod_{p > p_0} (1 - p^{-s})^{-1} = c_0 \neq 0$. This would give $\lim_{s \to 1+0}(s-1)^2 \zeta_K(s) = c_0^2 \cdot \prod_{p \leq p_0} \prod_{\mathfrak{p} \supset p} (1 - N(\mathfrak{p})^{-1})^{-1} \neq 0$. This contradicts Proposition 3.13.

Remark 3.9 *Proposition* 3.14 *asserts simply the existence of infinitely many primes p of which a given discriminant d is (is not) a quadratic residue. This would of course follow from Dirichlet's theorem on the existence of infinitely many primes in an arithmetic progression (to be proved in the following section).*

3.6 Primes in an arithmetic progression

Lemma 3.3 *Let $\{a_m\}$ be a sequence of non-negative numbers. Suppose that there is a real s such that $\sum_{m=1}^{\infty} a_m m^{-s}$ is convergent. Then there exists $s_0 \in \mathbf{R}$ such that $f(s) = \sum_{m=1}^{\infty} a_m m^{-s}$ converges for $s > s_0$, diverges for $s < s_0$ (unless the series converges for all values of s). Further, the series converges for any complex s with* $\mathrm{Re\ s} > \mathrm{s_0}$ *uniformly*

in any half plane $\operatorname{Re} s \geq s_0 + \delta$, *with* $\delta > 0$. *Also, for any integer* k, *we have* $f^{(k)}(s) = (-1)^k \sum_{m=1}^{\infty} a_m (\log m)^k m^{-s}$ *for* $\operatorname{Re} s > s_0$, *where* $f^{(k)}(s)$ *denotes the* k^{th} *derivative of* $f(s)$.

PROOF: Suppose $\sum a_m m^{-s'} < \infty$ for some $s' \in \mathbf{R}$. We claim that $\sum |a_m m^{-s}| < \infty$ for $\operatorname{Re} s > s'$, and the convergence is uniform in this region. In fact, since $a_m \geq 0$

$$\sum |a_m m^{-s}| = a_m m^{-\operatorname{Re}\ s} \leq a_m m^{-s'}$$

The existence of s_0 and the uniform convergence of the series in the half-plane $\operatorname{Re} s \geq s_0 + \delta$ follows at once. As for the, derivative, if $\operatorname{Re} s > s_0$ and if $s = \sigma + it$, let $s_0 < \sigma_1 < \sigma$. We have $\sum a_m m^{-\sigma_1} < \infty$. Hence

$$\sum |a_m (\log m)^{-k} m^{-s}| \leq \sum a_m m^{-\sigma_1} \frac{(\log m)^k}{m^{\sigma - \sigma_1}} < \infty$$

since for each k, $\dfrac{(\log m)^k}{m^{\sigma-\sigma_1}} \to 0$ as $m \to \infty$. Since the k-th derivative of m^{-s} is $(-1)^k (\log m)^k m^{-s}$ the result follows.

Definition 3.8 *The real number* s_0 *defined by Lemma* 3.3 *is called the abscissa of convergence of the series* $\sum a_m m^{-s}$; *if the series converges for all, we set* $s_0 = -\infty$.

Lemma 3.4 *Let* $\{a_m\}$ *be a sequence of non-negative numbers, and let* s_0 *be the abscissa of convergence of the series* $\sum a_m m^{-s}$. *Then, the series* $\sum a_m m^{-s} = f(s)$ *defines a holomorphic function* $\operatorname{Re} s > s_0$ *which is singular at the point* $s = s_0$.

PROOF: That $f(s)$is holomorphic in $\operatorname{Re} s > s_0$ follows at once from Lemma 3.3. Suppose f is not singular at $s = s_0$. Then there exists a disc $\mathcal{D}$: $\{|s - s_1| < \delta\}$ where $s_1 > s_0$, such that $|s_0 - s_1| < \delta$ and a holomorphic function g in $\mathcal{D}$ such that $g(s) = f(s)$ for $\operatorname{Re} s > s_0, s \in \mathcal{D}$. We have, by Taylor's formula

$$g(s) = \sum_{k=0}^{\infty} \frac{g^{(k)}(s_1)}{k!}(s - s_1)^k = \sum_{k=0}^{\infty} \frac{f^{(k)}(s_1)}{k!}(s_1 - s)^k$$

(since $g(s) = f(s)$ for s in a neighbourhood of s_1 so that the series $\sum_{k=0}^{\infty} \frac{(-1)^k f^{(k)}(s_1)}{k!}(s_1 - s)^k$ converges absolutely for any s in $\mathcal{D}$ and, in

particular, for real s with $s_1 - \delta < s < s_1$. Now,

$$(-1)^k f^{(k)}(s_1) = \sum_{m=1}^{\infty} a_m (\log m)^k m^{-s_1}$$

so that the repeated series

$$\sum_{k=0}^{\infty} \frac{(s_1 - s)^k}{k!} \sum_{m=1}^{\infty} a_m (\log m)^k m^{-s_1} < \infty \quad \text{for } s_1 - \delta < s < s_1.$$

Since all terms here are non-negative, we may rearrange the series as we like; hence the repeated series is equal to

$$\sum_{m=1}^{\infty} a_m m^{-s_1} \sum_{k=0}^{\infty} \frac{(s_1 - s)^k}{k!} (\log m)^k < \infty, \quad s_1 - \delta < s < s_1.$$

But the inner sum is $e^{(s_1 - s)\log m} = m^{s_1 - s}$. Hence

$$\sum_{m=1}^{\infty} a_m m^{-s_1} \cdot m^{s_1 - s} = \sum_{m=1}^{\infty} a_m m^{-s} < \infty \quad \text{for } s_1 - \delta < s < s_1.$$

Since $s_1 - \delta < s_0$, this contradicts the definition of s_0 and f must be singular at $s = s_0$.

In what follows, sums and products of the type $\sum_p$, $\prod_p$ will always be taken over the primes $p > 1$. (If any additional conditions are to imposed, these will be indicated below the summation or product.)

Let $D > 1$ be a positive integer. If $a \in \mathbf{Z}$ is such that $(a, D) = 1$, then $ab + Dc = 1$ for some $b, c \in \mathbf{Z}$. Then the residue class $\bar{a}$ containing a has an inverse $\bar{b}$ in $\mathbf{Z}/(D)$. If $a' \in \bar{a}$, then clearly $(a', D) = 1$. By a *prime residue class* modulo D, we mean a residue class $\bar{x}$ modulo D such that for any $x' \in \bar{x}$, we have $(x', D) = 1$. Clearly the prime residue classes modulo D form a finite group G ;under the multiplication induced from $\mathbf{Z}/(D)$. Let χ be a character of G. We define a function, also denoted by χ on $\mathbf{Z}$, by

$$\begin{aligned} \chi(m) &= \chi(\bar{m}) \text{ if } (m, D) = 1, \text{ where } \bar{m} \text{ is the residue class of } m, \\ \chi(m) &= 0 \text{ if } (m, D) > 1. \end{aligned}$$

For $s \in \mathbf{C}$, $\operatorname{Re} s > 1$, we define

$$L(s, \chi) = \sum_{m=1}^{\infty} \chi(m) m^{-s}.$$

Using the results of §4, we see that for $\operatorname{Re} s > 1$,

$$L(s,\chi) = \prod_p (1 - \chi(p)p^{-s})^{-1}.$$

Further, because of the orthogonality relations (Proposition 1.10, Chapter 1), we have

$$\sum_{m=1}^{D} \chi(m) = \sum_{a \in G} \chi(\bar{a}) = 0 \quad \text{if } \chi \neq \chi_0.$$

where χ_0 is the principal character defined by $\chi_0(m) = 1$ if $(m, D) = 1$, $\chi_0(m) = 0$ otherwise. Hence, as in Proposition 3.11, we can show that

$$\Big| \sum_{k=1}^{m} \chi(k) \Big| \leq \frac{1}{2} D \text{ for any m.}$$

Hence, by Proposition 3.15, the series defining $L(s,\chi)$ converges for $\operatorname{Re} s > 0$, uniformly in any bounded subset of $\operatorname{Re} s \geq \delta > 0$. Hence we have

Lemma 3.5 *If $\chi \neq \chi_0$, $L(s,\chi)$ is holomorphic for $\operatorname{Re} s > 0$. Moreover,*

$$L(s,\chi_0) = \prod_{p \nmid D} (1 - p^{-s})^{-1} = \zeta(s) \prod_{p|D} (1 - p^{-s}).$$

From Lemma 3.5 and from (3.23), we deduce

Lemma 3.6 $\lim_{s \to 1+0} (s-1) L(s,\chi_0) = \prod_{p|D} (1 - \frac{1}{p})$*; in particular,* $L(s,\chi_0) \to \infty$ *as* $s \to 1 + 0$.

Now, for $\operatorname{Re} s > 1$,

$$\log L(s,\chi) = \sum_p \log \frac{1}{1 - \chi(p)p^{-s}} = \sum_p \sum_{m=1}^{\infty} \frac{\chi(p^m)}{m p^{ms}}$$

Let $l \geq 1$ be any integer with $(l, D) = 1$. Using the orthogonality relations, (Proposition 1.10, Chapter 1), we obtain

Lemma 3.7 *For $\operatorname{Re} s > 1$ we have*

$$\begin{aligned} \sum_\chi \log L(s,\chi) &= h \sum_{p^m \equiv 1 \,(D)} \frac{1}{m p^{ms}} \\ \sum_\chi \bar{\chi}(l) \log L(s,\chi) &= h \sum_{p^m \equiv l \,(D)} \frac{1}{m p^{ms}} \end{aligned}$$

Here the summation is over all the characters of G, and h is the order of the character group $\hat{G}$ of G.

Corollary 3.2 *The function $f(s) = \prod_\chi L(s,\chi)$ has, for $\operatorname{Re} s > 1$, an expansion as a Dirichlet series $\sum c_m m^{-s}$ where $c_m \geq 0$.*

PROOF: Clearly, the series expansion for $f(s) = \prod_\chi L(s,\chi)$ can be obtained by formal substitution of $x = h \sum_{p^m \equiv 1\,(D)} \frac{1}{mp^{ms}}$ in $e^x = \sum_{k=0}^\infty \frac{x^k}{k!}$. Since all terms in the series for x are non-negative the corollary is proved.

Now we have

$$\log L(s,\chi) = \sum_p \frac{\chi(p)}{p^s} + \sum_p \sum_{m\geq 2} \frac{\chi(p^m)}{mp^{ms}}$$

If $\sigma = \operatorname{Re} s$ we have

$$\sum_p \sum_{m\geq 2} \frac{1}{|mp^{ms}|} \leq \sum_p \sum_{m\geq 2} \frac{1}{p^{m\sigma}} = \sum_p \frac{1}{p^\sigma(p^\sigma - 1)}$$

This latter series converges for $\sigma = \frac{1}{2}$. Hence, for $\sigma > 1$,

$$\log \zeta(s) = \sum_p \frac{1}{p^s} + R(s); \quad \sum_\chi \bar{\chi}(l) \log L(s,\chi) = h \sum_{p^m \equiv 1\,(D)} \frac{1}{p^s} + R_1(s) \tag{3.28}$$

where $|R(s)| \leq \sum_p \frac{1}{p^\sigma(p^\sigma-1)}$, $|R_1(s)| \leq h \sum_p \frac{1}{p^\sigma(p^\sigma-1)}$. In particular, since $\zeta(s) \to \infty$ as $s \to 1+0$ and $R(s)$ is bounded as $s \to 1+0$, $\sum_p \frac{1}{p^s} \to \infty$ as $s \to 1+0$, so that $\sum_p \frac{1}{p} = \infty$

Lemma 3.8 *If $f(s) = \prod_{\chi\in\hat{G}} L(s,\chi) = \sum_1^\infty c_m m^{-s}$, then $c_m \geq 0$, and $\sum_{m=1}^\infty c_m m^{-s} = \infty$ for $s = \frac{1}{\phi(D)}$ where $\phi(D)$ is the order of the group G.*

PROOF: We have already seen that $c_m \geq 0$ (by the corollary to Lemma 3.2). Now, for real s, $\sum_{p^m \equiv 1\,(\mathrm{mod}\,D)} \frac{1}{mp^{ms}} \geq \sum_{p>D} \frac{1}{\phi(D)p^{\phi(D)s}}$ since, for $p > D$, we have $p^{\phi(D)} \equiv 1\,(\mathrm{mod}\,D)$. Since $\sum_{p>D} \frac{1}{p} = \infty$ it follows that $\sum_{p^m \equiv 1(\mathrm{\ mod\ }D)} \frac{1}{mp^{ms}} = \infty$ for $s = \frac{1}{\phi(D)}$. Since $e^x = 1 + x + \cdots$, and the series for $f(s)$ is obtained by formal substitution of $x = h \sum_{p^m \equiv 1\,(D)} \frac{1}{mp^{ms}}$ in the series for e^x, $\sum_{m=1}^\infty c_m m^{-s}$ diverges for $s = \frac{1}{\phi(D)}$.

Proposition 3.17 *We have* $L(1,\chi) \neq 0$ *for* $\chi \neq \chi_0$.

PROOF: Consider $f(s) = \prod_\chi L(s,\chi) = L(s,\chi_0)\prod_{\chi\neq\chi_0} L(s,\chi)$. Since $L(s,\chi_0) = \zeta(s)\prod_{p|D}(1-p^{-s})$, this is meromorphic in $\operatorname{Re} s > 0$, with a single simple pole at $s=1$. If $L(1,\chi)=0$ for some $\chi \neq \chi_0$ it follows that $f(s)$ is holomorphic for $\operatorname{Re} s > 0$. Since, for $\operatorname{Re} s > 1$, $f(s) = \sum c_m m^{-s}$, $c_m \geq 0$, it follows from Lemma 3.4 that the abscissa of convergence of this series is ≤ 0. This contradicts Lemma 3.8.

Theorem 3.5 *(Dirichlet.) Let* $1 \geq 1$, $D > 1$ *be integers with* $(l,D)=1$. *Then there exist infinitely many primes* $p \equiv l (\bmod D)$.

PROOF: For $s > 1$, we have, by (3.28)

$$\sum_{\chi\in\hat{G}} \bar{\chi}(l)\log L(s,\chi) = h \sum_{p^m\equiv 1(D)} \frac{1}{p^s} + R_1(s)$$

where $|R_1(s)| \leq h\sum_p \frac{1}{p^s(p^s-1)}$ which is bounded as $s \to 1+0$.

Now, the term with $\chi = \chi_0$ is $\log L(s,\chi_0)$ which tends to ∞ as $s \to 1+0$ by Lemma 3.6. Every other term $\bar{\chi}(l)\log L(s,\chi)$ remains bounded as $s \to 1+0$ since $L(1,\chi) \neq 0$. Hence

$$\sum_\chi \bar{\chi}(l)\log L(s,\chi) \to \infty \quad \text{as } s \to 1+0;$$

since $R_1(s)$ is bounded, we conclude that $\sum_{p^m\equiv l(D)} \frac{1}{p^s} \to \infty$ as $s \to 1+0$.

Clearly this implies Theorem 3.5.

Proposition 3.16 follows immediately from Proposition 3.9 and Theorem 3.5, since there exist infinitely many primes p for which $(\frac{d}{p}) = 1$ and infinitely many primes q for which $(\frac{d}{q}) = -1$.

Bibliography

[1] N. Bourbaki: *Algébre*, Chapters I and II, Paris (1949).

[2] P.R. HALMOS: *Finite-dimensional Vector Spaces*, Van Nostrand, Princeton (1958).

[3] N. JACOBSON: *Lectures in Abstract Algebra*, Vol. I and II, Van Nostrand, Princeton (1953).

[4] B.L. VAN DER WAERDEN: *Modern Algebra*, Ungar, New York (1950).

[5] E. ARTIN: *Theory of Algebraic Numbers*, (Lecture notes) Göttingen, 1959.

[6] H. HASSE: *Vorlesungen über Zahlentheorie*, Springer-Verlag, (1950).

[7] E. HECKE: *Vorlesungen über die Theorie der algebraischen Zahlen*, Chelsea, New York, (1948).

[8] D.HILBERT: *Berichtüber die Theorie der algebraishchen Zahlkörper*, Jahresbericht der D.M.V., Bd.**4** (1897), pp.177–546.

[9] S. LANG: *Algebraic Numbers*, Addison-Wesley, 1964.

[10] H. WEYL: *Algebraic Theory of Numbers*, Ann. of Math. Studies, Princeton, 1940.

[11] C.L. SIEGEL: *Lectures on Analytic Number Theory*, New York, (1945).

[12] C.L. SIEGEL: *Lectures on Advanced Analytic Number Theory*, Tata Institute, Bombay, (1961).