UNIVERSITY OF CAPE TOWN

DEPARTMENT OF MATHEMATICS

STUDIES ON THE NUMBER THEORY OF ORDERS

BY

M R OMAR

A thesis prepared under the supervision of Dr K R Hughes
in fulfilment of the requirements for the degree of
Master of Arts in Mathematics

CONTENTS

ACKNOWLEDGEMENTS

I wish to thank my supervisor, Dr K R Hughes, for suggesting the topic of this thesis and for continually guiding my enquiries therein. His views and suggestions contributed in a fundamental way to the completion of this thesis. I gratefully acknowledge, too, the ready access he provided to his personal library.

I thank Professor K O Househam, Head of the Department of Mathematics at the University of Cape Town, for providing me with a teaching assistantship in the Department for the duration of my registration as an MA student.

I am grateful to the Council for Scientific and Industrial Research for granting me bursaries during 1980 and 1981.

Finally, I must also thank Mrs W M Fouquet for her competent and efficient typing of the manuscript, and Mr W A de Beer for the final reproduction of this thesis.

INTRODUCTION

In the nineteenth century no distinction was drawn between maximal and nonmaximal orders in a numberfield. Most of the work on orders in this period was done by Dedekind and Kronecker.

The twentieth century has witnessed a relative neglect of the nonmaximal orders of a numberfield, which are the algebraic analogues of singular curves, although a few texts, for example the one by Borevich and Shafarevich, do discuss arbitrary orders.

In this dissertation we attempt to present a connected account of the theory of nonmaximal orders, highlighting some of their important properties.

In Chapter One we discuss the factorization of ideals in nonmaximal orders, and use this to define a zeta function for an arbitrary order in a numberfield. We also relate this to a novel approach to zeta functions suggested by Dr K R Hughes, viz. via artinian injective modules over certain types of rings. This approach contrasts with the Hasse-Weil zeta function of a curve, which is restricted to the nonsingular case.

In Chapter Two we attempt to define the Class Group of a nonmaximal order, and prove a relationship between the usual Class Number and that of a nonmaximal order.

We shall assume standard results from commutative algebra, including the theory of the tensor product, from number theory, especially the theory of valuations, and from general topology, especially metric space theory. Less well-known results will be stated explicitly, sometimes without proof.

We use the following conventions :

All rings are commutative with identity.

If R is a ring, R^* denotes the multiplicative group of units of R, unless it is stated otherwise.

A finite module means a finitely generated module.

All local rings are necessarily noetherian.

P-adic valuations are normalized so that $|x|_p = (\text{Norm } P)^{-\text{ord}_P x}$.

The symbols $\subset$ or $\subseteq$ mean inclusion, proper or otherwise, while $\subsetneq$ means proper inclusion.

CHAPTER ONE

THE ZETA FUNCTION OF A NONMAXIMAL ORDER

1.1 Preliminaries

A *numberfield* K is a finite algebraic extension of $\mathbb{Q}$.

A *lattice* M in K is a finitely generated $\mathbb{Z}$-submodule of K.

The lattice is *full* if its dimension = $[K:\mathbb{Q}]$.

An *order* $\mathbb{O}$ of K is a full lattice which is also a ring with unity.

We now show that in a numberfield there is a unique maximal order containing all other orders.

Suppose R is a domain contained in a field K.

An element $\alpha \in K$ is said to be *integral over* R if

(i) $\alpha M \subseteq M$ for some finitely generated R-module M in K

or (ii) α satisfies an equation $\alpha^n + b_{n-1}\alpha^{n-1} + \ldots + b_0 = 0$, $b_i \in R$.

The equivalence of (i) and (ii) is readily established (see, for example, Lang [2]).

The ring of all elements of K integral over R is called the *integral closure* of R in K, written $\tilde{R}_K$.

It is clear that $\tilde{R}_K$ is, in fact, a ring, and that the operation of taking integral closure is idempotent.

The integral closure of $\mathbb{Z}$ in a numberfield K, written $\mathbb{O}_K$, is called the *ring of (algebraic) integers* of K.

Theorem 1 Every order in a numberfield K is contained in $\mathbb{O}_K$, which is an order and thus the unique maximal order of K.

Proof: If $x \in \mathbb{O}$, an order of K, then $x\mathbb{O} \subseteq \mathbb{O}$, and since $\mathbb{O}$ is finitely generated over $\mathbb{Z}$, x is integral over $\mathbb{Z}$, so $x \in \mathbb{O}_K$. $\mathbb{O}_K$ is obviously a ring and a lattice, and it is full because it contains a full lattice (any order) and its dimension cannot exceed $[K:\mathbb{Q}]$. □

It is clear that, if $\mathbb{O}$ is nonmaximal, not every $\mathbb{O}$-ideal is and $\mathbb{O}_K$-ideal.
The largest $\mathbb{O}$-ideal which is also an $\mathbb{O}_K$-ideal is called the *conductor of* $\mathbb{O}$, written $F_{\mathbb{O}}$, or just F.

In the case of a quadratic field $K = \mathbb{Q}(\sqrt{d})$, d a square-free integer, the orders are easily characterised. For then the discriminant

$$D = \begin{cases} d & \text{if } d \equiv 1 \mod 4 \\ 4d & \text{otherwise,} \end{cases}$$

and the maximal order $\mathbb{O}_K$ is $\mathbb{Z} \oplus \mathbb{Z}[\omega]$, also written $[1,\omega]$, where $\omega = \frac{D + \sqrt{D}}{2}$; all other orders are of the form $[1,g\omega]$, $g = 2, 3, \ldots$.
The conductor of the order $\mathbb{O} = [1,g\omega]$ is just $g\mathbb{O}_K$ (Cohn [1]).

A similar characterization exists for the orders of arbitrary pure cubic fields (Cohn [1]), but not all sublattices containing 1 of the maximal order are rings.

For example, if $K = \mathbb{Q}(\sqrt[3]{2})$, then $\mathcal{O}_K = [1, \sqrt[3]{2}, \sqrt[3]{4}]$, but $[1, \sqrt[3]{2}, 2\sqrt[3]{4}]$ is not an order, although $[1, 2\sqrt[3]{2}, \sqrt[3]{4}]$ is.

1.2 Factorisation of ideals in non-maximal orders

A celebrated result of Dedekind states that every ideal of the ring of integers of a number field can be uniquely expressed as the product of powers of prime ideals (See, for example, Lang [2]).

This depends on the fact that $\mathcal{O}_K$ is *Dedekind*, i.e. it possesses the following three properties :

(i) It is integrally closed in K .

(ii) It has *Krull dimension one*, i.e. every nonzero prime ideal is maximal.

(iii) It is *noetherian*, i.e. every ideal is finitely generated, or, equivalently, every ascending chain of ideals stabilizes.

The latter two properties are possessed by all orders, not only the maximal one, as we see now :

Proposition 1 Any order $\mathcal{O}$ in a numberfield K is noetherian and has Krull dimension one.

Proof (Folklore): $\mathcal{O}$ is noetherian since it is finitely generated as a $\mathbb{Z}$-module. To see that it also has Krull dimension one, consider the diagram

$$\begin{array}{ccc} \mathbb{Z} & \hookrightarrow & \mathbb{O} \\ \downarrow & & \downarrow \\ \mathbb{F}_p = \mathbb{Z}/p\mathbb{Z} = \mathbb{Z}/(\mathbb{Z} \cap P) & \hookrightarrow & \mathbb{O}/P \end{array}$$

in which P is a prime ideal of $\mathbb{O}$.

$\mathbb{Z} \cap P$ $(= p\mathbb{Z}$ for some prime $p \in \mathbb{Z})$ is a prime ideal of $\mathbb{Z}$, hence also maximal. ($\mathbb{Z}$ is Dedekind)

So $\mathbb{O}/P$, an integral domain, is a finite extension of the finite field $\mathbb{F}_p$, and hence is also a finite field.

So P must be maximal. □

However, it is easily seen that a nonmaximal order, e.g. $[1, 2i]$ in $\mathbb{Q}(i)$, is not integrally closed, and hence not Dedekind. (In this case i is integral over $\mathbb{O}$, but $i \notin \mathbb{O}$). There is thus no unique factorisation of ideals into products of prime powers, but a weaker result does hold.

First we need some prerequisites :

An R-ideal Q is *primary* if $ab \in Q$, $a \notin Q$ implies $b^n \in Q$ for some positive integer n.

If Q is primary, the *radical of* Q, $P = \sqrt{Q} = \{x \in R: x^n \in Q$ for some $n \in \mathbb{Z}^+\}$ is prime. It is called the *associated prime* of Q. We say Q is P-*primary*. It is easy to see that $\sqrt{Q}$ is the minimal prime containing Q.

An R-ideal I is *irreducible* if $I = J \cap L$ implies $I = J$ or $I = L$, where J, L are also R-ideals.

The *residual quotient* of an R-ideal I by an R-ideal J is the R-ideal $I:J = \{x \in R: xJ \subseteq I\}$. It is easily seen that $I:J$ is an R-ideal.

The following properties will be used in the sequel :

Proposition 2 Q is P-primary if (a) $P \supseteq Q$ (b) $x \in P \Rightarrow x^n \in Q$ for some $n > 0$ (c) $ab \in Q$, $a \notin P \Rightarrow b \in Q$.

Proof (Northcott [1]): Suppose $ab \in Q$, $b \notin Q$.
By (c), $a \in P$, so by (b) $a^n \in Q$ for some $n > 0$.
Therefore Q is primary.
We need to show $P = \sqrt{Q}$.
By (b) $P \subseteq \sqrt{Q}$. Conversely, if $x \in \sqrt{Q}$, let i be minimal such that $x^i \in Q$.
If $i = 1$, then $x \in Q \subseteq P$ (by (a)) and we are done.
If $i > 1$, then $x^i = x.x^{i-1} \in Q$; but $x^{i-1} \notin Q$ by minimality of i , so $x \in P$ (by (c)), as required. □

Proposition 3 A finite intersection of P-primary ideals is P-primary.

Proof (Northcott [1]): Suppose $Q = Q_1 \cap \ldots \cap Q_n$, each Q_i P-primary. We show P,Q satisfy (a), (b), (c) of Proposition 2.
(a) $P \supseteq Q_i$ all i , so $P \supseteq Q$.

(b) If $x \in P$, then for each i there is a positive integer m_i such that $x^{m_i} \in Q_i$.
Put $m = \max\{m_i\}$. Then $x^m \in Q_i$ for all i, so $x^m \in Q$.

(c) If $ab \in Q$, $a \notin P$, then $ab \in Q_i$ for all i, $a \notin P = \sqrt{Q_i}$ i.e. $a^n \notin Q_i$ for all $n \geq 0$, so $b \in Q_i$ for all i (Q_i primary). Hence $b \in Q$. □

Proposition 4 (a) $I \subseteq I:J$; $(I:J).J \subseteq I$.

(b) $(\cap I_i):J = \cap(I_i:J)$

(c) $(I:J):K = I:JK$.

Proof: Immediate from the definitions. □

Proposition 5 Let Q be P-primary, I, J ideals.

(a) If $IJ \subseteq Q$ and $I \not\subseteq P$, then $J \subseteq Q$.

(b) If $I \subseteq P$, then $Q:I = Q$.

Proof (Northcott [1]): (a) Choose $a \in I$, $a \notin P$, $b \in J$.
Then $ab \in IJ \subseteq Q$, and since $a \notin P$, $b \in Q$.
So $J \subseteq Q$.

(b) By Proposition 4(a), $I.(Q:I) \subseteq Q$, so putting $J = (Q:I)$, we have $Q:I \subseteq Q$ by (a).

But always $Q \subseteq Q:I$, so $Q:I = Q$. □

We now proceed to establish the first part of the main result, Theorem 2, first proved by Emmy Noether. A modern reference is Zariski-Samuel [1].

Lemma 1 If a ring R is noetherian, every ideal can be represented as the intersection of finitely many irreducible ideals.

Proof: If there are any ideals which are not representable in this manner, there will be a maximal such counterexample, M, by the noetherian condition. M is not irreducible, so there exist ideals B, C properly containing M with $M = B \cap C$. By maximality of M, B and C must each be an intersection of finitely many irreducible ideals, and hence so must M be, a contradiction. □

Lemma 2 If R is noetherian every irreducible ideal is primary.

Proof: We assume the ideal I is not primary, and show it cannot be irreducible.

Since I is not primary, there exist $b,c \in R$ such that $bc \in I$, $c \notin I$ and $b^n \notin I$ for all $n \geq 0$.

Obviously $I \subseteq I:bR$, and since $bc \in I$, $c \notin I$, we have in fact $I \subsetneq I:bR$.

Using Proposition 4 we obtain

$I: b^rR \subseteq [I: b^rR]: bR = I: b^{r+1}R$, and hence

$I \subsetneq I: bR \subseteq I: b^2R \subseteq \ldots$.

Since R is noetherian, there exists an integer $m > 0$ so that $I: b^nR = I: b^mR$ for all $n \geq m$.

We complete the proof by showing that $I = (I: b^mR) \cap (I + b^mR)$,

for, by construction, both $I: b^m R$ and $I + b^m R$ strictly contain I .

It suffices to show $(I: b^m R) \cap (I + b^m R) \subseteq I$.

If $x \in (I: b^m R) \cap (I + b^m R)$, then $x = a + rb^m$, $a \in I$, $r \in R$.

But also $x \in I: b^m R$, so $xb^m = (a + rb^m)b^m$

$= ab^m + rb^{2m} \in I$.

This shows that $rb^{2m} \in I$, so $r \in I: b^{2m} R = I: b^m R$.

Hence $rb^m \in I$, and $x \in I$ as required. □

Theorem 2 Every ideal in a noetherian ring can be expressed as a finite intersection of primary ideals.

Proof: Immediate from Lemmas 1 and 2. □

This representation is usually highly non-unique. A great deal of the arbitrariness can be eliminated by restricting to certain types of decompositions :

A decomposition $Q_1 \cap \ldots \cap Q_n$ in which no Q_i contains $\bigcap_{j \neq i} Q_j$ is called *irredundant*.

An irredundant decomposition in which the primes associated to the various primary components are all different is called *normal*.

Proposition 6 Each primary decomposition of an ideal can be refined to one which is normal.

Proof: Suppose $I = Q_1 \cap \ldots \cap Q_n$, where Q_i is P_i-primary, and suppose $P_{i_1} = \ldots = P_{i_r} = P$.
By Proposition 3 $Q = Q_{i_1} \cap \ldots \cap Q_{i_r}$ is P-primary, so, replacing $Q_{i_1} \cap \ldots \cap Q_{i_r}$ by Q, we then have only one primary belonging to P in the decomposition.
Repeating this process with all the other associated primes, we can, in a finite number of steps, reduce the decomposition into one in which all the associated primes are different. The decomposition is then rendered normal by omitting any primary component which contains the intersection of the remaining components. □

In the presence of the noetherian and dimension one conditions, much stronger uniqueness properties can be obtained, and the decomposition can be written as a product. The following result is easily proved in the special case we are interested in, but we prove it in its most general form :

Proposition 7 The number of components and the associated primes in a normal decomposition of a decomposable ideal in an arbitrary ring are unique.

Proof (Northcott [1]): Let $I = Q_1 \cap \ldots \cap Q_m = Q'_1 \cap \ldots \cap Q'_n$ be two normal decompositions of the proper ideal I (if $I = R$ the result is obvious), where Q_i is P_i-primary and Q'_j is P'_j-primary. Since $I \neq R$ and the decompositions are irredundant, all the P_i and P'_j are proper ideals.

From this finite set of prime ideals, we choose one which is not strictly contained in any of the others. Renumbering, if necessary, we suppose this is P_m .

We now show $P_m = P'_{j_0}$ for some j_0 , and for this it suffices to show $P_m \subseteq P'_{j_0}$, by choice of P_m .

In fact since P_m is the minimal prime containing Q_m , it is enough to show $Q_m \subseteq P'_{j_0}$ for some j_0 .

Suppose $Q_m \nsubseteq P'_j$ for all j . By Proposition 5 $Q'_j : Q_m = Q'_j$ for all j , so by Proposition 4

$$I : Q_m = (Q'_1 : Q_m) \cap \ldots \cap (Q'_n : Q_m)$$
$$= Q'_1 \cap \ldots \cap Q'_n = I .$$

For $1 \leqslant i < m$ we have $P_m \nsubseteq P_i$ for otherwise $P_m = P_i$, by choice of P_m , and this is impossible as all the P_i are distinct. Then $Q_m \nsubseteq P_i$, $1 \leqslant i < m$, again because P_m is the minimal prime containing Q_m . So by Proposition 5, $Q_i : Q_m = Q_i$ for $1 \leqslant i < m$, while $Q_m : Q_m = R$.

Using Proposition 4 and the above relations, we then have

$$I = I : Q_m = (Q_1 \cap \ldots \cap Q_m) : Q_m$$
$$= (Q_1 : Q_m) \cap \ldots \cap (Q_m : Q_m)$$
$$= Q_1 \cap \ldots \cap Q_{m-1} .$$

This contradicts our assumption of normality.

If $m = 1$, we obtain $I = I : Q_m = R$, again a contradiction.

We may as well take $i_0 = n$, so we have shown $P_m = P'_n$.

Now put $Q = Q_m \cap Q'_n$. Then, by Proposition 3, Q is a primary ideal belonging to $P_m = P'_n$.

We have, for $1 \leqslant i < m$, $P_m \nsubseteq P_i$, so, as before, $Q \nsubseteq P_i$, and hence $Q_i : Q = Q$ for $1 \leqslant i < m$, and since $Q \subseteq Q_m$,

$Q_m : Q = R$. Thus $I : Q = Q_1 \cap \ldots \cap Q_{m-1}$ as before.
The same argument applied to Q'_n , P'_n gives

$$I : Q = Q'_1 \cap \ldots \cap Q'_{n-1} \quad .$$

Thus $Q_1 \cap \ldots \cap Q_{m-1} = Q'_1 \cap \ldots \cap Q'_{n-1} = I_1$, say, both decompositions being normal.

Applying the entire argument to I_1 we obtain, renumbering if necessary, $P_{m-1} = P'_{n-1}$ and
$Q_1 \cap \ldots \cap Q_{m-2} = Q'_1 \cap \ldots \cap Q'_{n-2} = I_2$, say, both decompositions again being normal.

It therefore remains to show that $m = n$.

If $m < n$, say, then after m steps we would obtain

$$R = Q'_1 \cap \ldots \cap Q'_{n-m}$$
$$\subseteq P'_1 \cap \ldots \cap P'_{n-m} \quad ,$$

which is impossible as all the P'_j are proper ideals. □

We have thus proved that, in a noetherian ring, every ideal I has a normal decomposition into a finite intersection of primary ideals, and that the primes associated to I , and the number of components, are unique. The fact that an order also has Krull dimension one allows two further simplifications.

Lemma 3 Let $\{A_i\}_{i \in I}$ be a set of pairwise comaximal ideals in a ring R (i.e. $A_i + A_j = R$ if $i \neq j$). Then $\bigcap_{i \in I} A_i = \prod_{i \in I} A_i$.

Proof (Zariski & Samuel [1]): The proof is by induction.

If A_1, A_2 are comaximal, we get

$$A_1 \cap A_2 = (A_1 + A_2)(A_1 \cap A_2) = A_1(A_1 \cap A_2) + A_2(A_1 \cap A_2)$$
$$\subseteq A_1A_2 + A_2A_1 = A_1A_2,$$

and the reverse inclusion is obvious.

To prove the inductive step, we first observe that A_n is comaximal with $A_1 \cdot \ldots \cdot A_{n-1}$, and hence with $A_1 \cap \ldots \cap A_{n-1}$, because

$$R = R^{n-1} = (A_n + A_1) \ldots (A_n + A_{n-1}) \subset A_n + (A_1 \ldots A_{n-1}) \subset R .$$

Now suppose that $A_1 \cdot \ldots \cdot A_{n-1} = A_1 \cap \ldots \cap A_{n-1}$.

Since A_n is comaximal with $A_1 \cap \ldots \cap A_{n-1}$, we have

$$(A_1 \cap \ldots \cap A_{n-1}) \cap A_n = (A_1 \cap \ldots \cap A_{n-1}).A \quad \text{(by the first step)}$$
$$= (A_1 \ldots A_{n-1}).A_n ,$$

by the inductive hypothesis. □

Lemma 4 The ideals $\{A_i\}_{i \in I}$ are comaximal if and only if their radicals are.

Proof: Necessity is obvious as $A_i \subseteq \sqrt{A_i}$.

Sufficiency is proved by induction :

Suppose $R = \sqrt{A_1} + \sqrt{A_2}$. Then $1 = c_1 + c_2$, $c_1 \in \sqrt{A_1}$, $c_2 \in \sqrt{A_2}$. So there is $k \in \mathbb{Z}^+$ so that both $c_1^k \in A_1$ and $c_2^k \in A_2$.

Now in the binomial expansion of $1 = (c_1 + c_2)^{2k-1}$, each term has a factor $c_1^i c_2^j$ with either $i \geq k$ or $j \geq k$, and hence it is either in A_1 or in A_2 .

It follows that each term is in $A_1 + A_2$, so $1 \in A_1 + A_2$, so $R = A_1 + A_2$.

Suppose the result holds for $n - 1$ comaximal ideals.

Now if $\sqrt{A_1}, \ldots, \sqrt{A_n}$ are comaximal, then so are $\sqrt{A_1}, \ldots, \sqrt{A_{n-1}}$, and, by inductive hypothesis, $A_1, \ldots, A_{n-1}$ are then comaximal. It remains to show that $A_n + A_i = R$ for $1 \leqslant i < n$.

But this is obvious by the first step because $\sqrt{A_n} + \sqrt{A_i} = R$ for $1 \leqslant i < n$. □

A prime ideal P containing an ideal I is called a *minimal prime of* I if no prime containing I is strictly contained in P .

Lemma 5 Suppose $I = Q_1 \cap \ldots \cap Q_n$ is a normal decomposition of a decomposable ideal I in a ring R , Q_i P_i-primary. If some P_{i_0} is a minimal prime of I then Q_{i_0} is uniquely determined.

Proof: Suppose P_1 is a minimal prime of I .

Let S be the multiplicative set $R - P_1$.

Put $I_S = \{x \in R : cx \in I \text{ for some } c \in S\}$. Then I_S depends only on I , for by Proposition 7 I determines the P_i uniquely.

We show $I_S = Q_1$, and this will give the result.

If $x \in I_S$, then $cx \in I = Q_1 \cap \ldots \cap Q_n$ for some $c \in S$.

Then $cx \in Q_1$ and $c \notin P_1$, so $x \in Q_1$ as Q_1 is P_1-primary.

Conversely, let $x \in Q_1$. Clearly $P \cap S \neq \phi$ for $i \neq 1$, for otherwise $P_i \subset R - S = P_1$, implying $P_i = P_1$ by minimality of P_1 . This contradicts normality.
So for each $i \neq 1$, we can choose $c_i \in P_i \cap S$, and for N sufficiently large, $(c_2,.....c_n)^N \in Q_2 \cap \ldots \cap Q_n$.
Then $x.(c_2.....c_n)^N \in Q_1 \cap \ldots \cap Q_n = I$, and since S is multiplicative, $(c_2,.....c_n)^N \in S$, so $x \in I_S$ as required. □

Theorem 3 In an order $\mathbb{O}$ of a numberfield K , every non-zero ideal I has a unique normal decomposition into a product of primary ideals.

Proof: Since $\mathbb{O}$ has Krull dimension one, every non-zero prime is maximal hence every prime belonging to I is a minimal prime of I ; so uniqueness follows by Lemma 5.
The primes of $\mathbb{O}$ are comaximal, so by Lemma 4 the primaries occurring in the decomposition of I are comaximal. Then by Lemma 3 the intersection of these primaries can be expressed as their product. □

Theorem 3 is thus a generalization of the Dedekind result referred to at the beginning of this section. The essential point is that, if the order is nonmaximal, not all primaries are prime powers.

Example: If we consider the order $\mathbb{O} = [1,2i]$ in $K = \mathbb{Q}(i)$, for example, then the conductor $F = [2,2i]$ is easily seen

to be prime. However there are several ideals - e.g. $2\mathfrak{O}$, $2i\mathfrak{O}$, $4\mathfrak{O}$, $4i\mathfrak{O}$, etc. - which are F-primary but not powers of F .

We conclude this section by showing that, in a noetherian ring of Krull dimension one, a decomposition into a product can be normalized as in Proposition 6.
For this we need to show that a *product* of P-primary ideals is P-primary, a fact which follows from :

Proposition 8 If R is noetherian, P maximal, then Q is P-primary if and only if $Q \supseteq P^m$ for some $m \in \mathbb{Z}^+$.

Proof (Northcott [1]): Suppose Q is P-primary.
As R is noetherian, $P = Ra_1 + \ldots + Ra_n$, $a_i \in P$.
For each i , $\exists\, m_i$ such that $a_i^{m_i} \in Q$. Put $m = \Sigma m_i$.
We show $Q \supseteq P^m$.
Now P^m is generated over R by elements of the form $a_1^{\mu_1} \ldots\ldots a_n^{\mu_n}$, the μ_i being nonnegative integers satisfying $\Sigma \mu_i = m = \Sigma m_i$.
Thus for some i_0 , $\mu_{i_0} \geqslant m_{i_0}$, and so $a_1^{\mu_1} \ldots\ldots a_n^{\mu_n} \in Q$.
Since $a_1^{\mu_1} \ldots\ldots a_n^{\mu_n}$ is a generator, $P^m \subseteq Q$.
(This argument shows, in fact, that any ideal contains a power of its radical in a noetherian ring.)
Conversely, suppose $P^m \subseteq Q$.
If P' is a prime belonging to Q , then $P^m \subseteq Q \subseteq P'$.
Then $P \subseteq P'$, for, if not, $\exists\, x \in P'$, $x \notin P$, implying

$x^m \in P'$, $x^m \notin P^m$.

By maximality, $P = P'$, so P is the only prime belonging to Q .

Thus Q is P-primary. □

Corollary If R is noetherian and has Krull dimension one, then $Q_1, \ldots, Q_n$ P-primary $\Rightarrow Q = \prod_{i=1}^{n} Q_i$ P-primary.

Proof: Each Q_i P-primary implies that, for each i , $\exists\, m_i$ such that $Q_i \supseteq P^{m_i}$. Put $m = \Sigma m_i$.

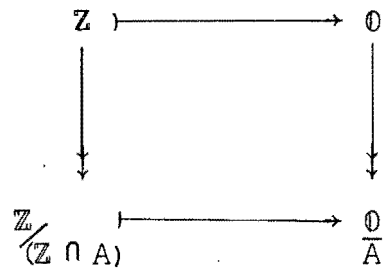
Then $Q = \Pi Q_i \supseteq P^m$, so Q is P-primary. □

Remark: In a ring of Krull dimension one it is sufficient that the associated primes be distinct for a decomposition (whether an intersection or a product) to be normal. For if $Q_i \supseteq \bigcap_{j \neq i} Q_j$ (resp. $\prod_{j \neq i} Q_j$) then $P_i \supseteq$ some Q_{j_0} , otherwise for each $j \neq i$ we can find $x_j \in Q_j$, $x_j \notin P_i$, hence $\Pi x_j \in \bigcap_{j \neq i} Q_j$ (resp. $\prod_{j \neq i} Q_j$) , but $\notin P_i$. So $P_i \supseteq P_{j_0}$, and by maximality $P_i = P_{j_0}$, a contradiction.

1.3 Defining the generalized Zeta function

The *norm* of an ideal A in an order $\mathbb{O}$, written Norm (A) , or just $N(A)$, is the index $\{\mathbb{O}:A\} = \#|\frac{\mathbb{O}}{A}|$.

We now show that $N(A)$ is always finite, by considering the diagram



Now $\mathbb{Z} \cap A = n\mathbb{Z}$ for some $n \in \mathbb{Z}$, so $\frac{\mathcal{O}}{A}$ is a finite extension of the finite ring $\mathbb{Z}/n\mathbb{Z}$, hence itself a finite ring.

The *Dedekind zeta function* of a numberfield K is defined as

$$\zeta_K(s) = \sum_{A \neq 0} \frac{1}{N(A)^s} \quad , \quad s \in \mathbb{C} \quad ,$$

the sum being taken over all nonzero ideals of $\mathcal{O}_K$.
If $K = \mathbb{Q}$, this is just the *Riemann zeta function*

$$\zeta(s) = \sum_{n \in \mathbb{N}} \frac{1}{n^s} \quad .$$

The most important properties of the Dedekind zeta function are the following :

(1) $\zeta_K(s)$ converges absolutely for $\mathrm{Re}(s) > 1$.

(2) $\zeta_K(s)$ may be written as a product

$$\prod_P (1 - \frac{1}{N(P)^s})^{-1} = \prod_P (1 + \frac{1}{N(P)^s} + \frac{1}{N(P)^{2s}} + \ldots) \quad ,$$

the product being taken over all prime ideals $P \neq 0$ of $\mathcal{O}_K$. This representation is called the *Euler Product Formula*.

(3) $\zeta_K(s)$ can be analytically continued as a meromorphic function to the whole s-plane.

(4) $\zeta_K(s)$ has a simple pole at $s = 1$, and the residue at $s = 1$ is given by

$$\lim_{\substack{s\to 1 \\ \mathrm{Re}(s)>1}} (s-1)\zeta_K(s) = \frac{2^{r_1+r_2}\,\pi^{r_2}\,R}{\mu\sqrt{|\Delta|}}\,h \quad ,$$

where (r_1, r_2) is the signature of K, μ the number of roots of unity in K, Δ the discriminant of K, R the regulator of K, and h the class number of K.

(5) The function

$$2^{-r_2 s}\,|\Delta|^{s/2}\,\pi^{-ns/2}\,\Gamma\left(\frac{s}{2}\right)^{r_1}\Gamma(s)^{r_2}\,\zeta_K(s) \quad ,$$

where $n = [K:\mathbb{Q}]$, and Γ is the gamma function, is invariant under the transformation $s \to 1 - s$.

This is called the *functional equation* for $\zeta_K(s)$.

There is also the famous *Riemann Hypothesis*: All non-trivial zeroes of $\zeta_K(s)$ have $\mathrm{Re}(s) = \frac{1}{2}$.

This is regarded by many as the most difficult and most important of all the unsolved problems of mathematics.

There are two obvious candidates for the definition of a generalized zeta function: a generalization of either the definition of $\zeta_K(s)$, or the Euler product formula for $\zeta_K(s)$. This question has previously been considered by Jenner, who chooses the latter because it coincides with the definition in the case of an affine scheme. (Jenner [2]). We attempt to show in the sequel (§1.6) that there are other reasons, perhaps more telling, for choosing the following definition for $\zeta_K(s)$, the zeta function of an arbitrary order $\mathcal{O}$ in a numberfield :

$$\zeta_{\mathcal{O}}(s) = \sum_{A \neq 0} \frac{1}{N(A)^s} \quad , \quad s \in \mathbb{C} \ ,$$

the sum being taken over all nonzero ideals of $\mathcal{O}$.

1.4 Convergence of $\zeta_{\mathcal{O}}(s)$

The generalized zeta function converges in the same region as the Dedekind zeta function.

In order to prove this result, we need to introduce certain concepts and prove some results about the norm of an ideal.

Lemma 5 If I , J are ideals in an order $\mathcal{O}$, then

$$N(I \cap J) \cdot N(I + J) = N(I) \cdot N(J) \ .$$

Proof: Consider first the short exact sequence

$$(A) \qquad \mathcal{O}/(I \cap J) \xrightarrow{\alpha} \mathcal{O}/I \oplus \mathcal{O}/J \xrightarrow{\beta} \mathcal{O}/(I + J) \ ,$$

which is obtained as follows :

The map $\mathcal{O} \to \mathcal{O}/I \oplus \mathcal{O}/J$ given by $x \to (x + I, x + J)$ ($(\bar{x}, \bar{x})$ for short) clearly has kernel $I \cap J$.

To see that coker (α) is isomorphic to $\mathcal{O}/(I + J)$, we show that

$$\mathcal{O} \longrightarrow \frac{(\mathcal{O}/I \oplus \mathcal{O}/J)}{\mathrm{Im}(\mathcal{O}/(I \cap J))} = \text{coker } (\alpha)$$

has kernel $I + J$. Now every element of $\mathcal{O}/I \oplus \mathcal{O}/J$ can be written as $(\bar{x},\bar{y}) = (\bar{x},\bar{x}) + (0,\bar{y}-\bar{x})$, so every coset of coker (α) contains a representative $(0,\bar{z})$, as $(\bar{x},\bar{x})$ belongs to $\mathrm{Im}(\mathcal{O}/(I \cap J))$. Mapping via $z \mapsto \overline{(0,\bar{z})}$ we see that $(0,\bar{z})$ is 0 in the quotient if and only if

$(0,\bar{z}) = (\bar{t},\bar{t})$ for some t, i.e. $t \in I$, $z - t \in J$, so $z \in I + J$.

Next consider the obvious short exact sequence

$$(B) \qquad \mathbb{O}/I \rightarrowtail \mathbb{O}/I \oplus \mathbb{O}/J \twoheadrightarrow \mathbb{O}/J \ .$$

Applying Lagrange's theorem on the orders of finite groups to (A) and (B) we obtain the result. □

Proposition 9 If I and J are comaximal ideals in an order $\mathbb{O}$, then $N(IJ) = N(I) \cdot N(J)$.

Proof: If I, J are comaximal, then $I + J = \mathbb{O}$, and $I \cap J = IJ$ (Lemma 3).

Since $N(\mathbb{O}) = 1$, the result follows by Lemma 5. □

Proposition 10 If I and J are any ideals in the maximal order $\mathbb{O}_K$, then $N(IJ) = N(I) \cdot N(J)$.

Proof: Every ideal of $\mathbb{O}_K$ can be written as a product of prime powers, with distinct primes giving comaximal factors; so by Proposition 9 it suffices to prove that $N(P^r) = N(P)^r$ for P prime.

Now consider the short exact sequence

$$P/P^r \rightarrowtail \mathbb{O}_K/P^r \twoheadrightarrow \left(\mathbb{O}_K/P^r\right)\Big/\left(P/P^r\right) \cong \mathbb{O}_K/P \ .$$

Thus we have, by Lagrange's theorem,

$$N(P^r) = N(P) \cdot \{P:P^r\} \ .$$

Next we obtain the sequence

$$P^2/P^r \longmapsto P/P^r \twoheadrightarrow P/P^2 \ .$$

Now every ideal in a Dedekind domain is generated by two elements (for example, see Zariski and Samuel [1]), and we may choose one of the generators of P to be in P^2. So P/P^2 is a one-dimensional vector space over the field $\mathbb{O}_K/P$, hence $\{P:P^2\} = N(P)$.

So we obtain $\{P:P^r\} = N(P) \ . \ \{P^2:P^r\}$.

Continuing in this manner we obtain the result. □

Let p be a rational prime. Then the ideal $p\mathbb{O}_K$ has a unique factorisation

$$p\mathbb{O}_K = P_1^{e_1} \ \ldots \ P_r^{e_r}$$

into a product of prime powers by the Dedekind theorem. It is clear that a prime P of $\mathbb{O}_K$ occurs among the P_i if and only if P lies above p, i.e. P divides p.

Each e_i is called the *ramification index* of P_i over p, written $e(P_i/p)$.

The *residue class degree* of P_i over p, written $f(P_i/p)$ is the index $\{\mathbb{O}_K/P_i : \mathbb{Z}/p\}$.

If $[K:\mathbb{Q}] = n$, we have the important relation (see, for example, Lang [2])

$$n = \sum_{i=1}^{r} e(P_i/p) \ . \ f(P_i/p) \ .$$

From this we deduce that a rational prime splits into at most n primes in a numberfield of degree n.

Proposition 11 Let m be any positive integer. Then the number of ideals of $\mathcal{O}_K$ with norm m is finite.

Proof: Let P be any $\mathcal{O}_K$-prime, and p the rational prime it divides. Then by definition of the norm and residue class degree, we must have $N(P) = p^{f(P/p)}$.
Let A be an $\mathcal{O}_K$-ideal satisfying $N(A) = m$, and suppose the factorisation of A is $A = P_1^{n_1} \dots P_r^{n_r}$.
Then $m = N(P_1)^{n_1} \dots N(P_r)^{n_r}$ (Proposition 10)
$= p_1^{n_1 f_1} \dots p_r^{n_r f_r}$, where $f_i = f(P_i/p)$.
Since $\mathbb{Z}$ is a unique factorization domain, the primes belonging to any other ideal with norm m must lie over the P_i.
For each i, the number of such primes is finite, and the result then follows easily. □

The convergence of $\zeta_{\mathcal{O}}(s)$ is proved using the convergence of $\zeta_K(s)$, so we prove the latter first.

Theorem 4 The Dedekind zeta function $\zeta_K(s)$ converges absolutely for $\mathrm{Re}(s) > 1$.

Proof (Goldstein [1]): We observe that it suffices to show that $\sum_{A \neq 0} \frac{1}{N(A)^s}$ converges for $s \in \mathbb{R}$, $s > 1$, since, for $s \in \mathbb{C}$, $|N(A)^s| = |N(A)|^{\mathrm{Re}(s)} = N(A)^{\mathrm{Re}(s)}$.
We show first that $\sum_P N(P)^{-s}$, the sum being taken over all primes P of $\mathcal{O}_K$, converges for $s > 1$.

For each prime P of $\mathcal{O}_K$, let p be the rational prime which P divides. There are at most n such P dividing p.

Then $N(P) = p^{f(P/p)} \geq p$, so

$$\sum_P N(P)^{-s} \leq n \sum_p p^{-s} ,$$

and the latter series converges for $s > 1$. (The latter sum is over all rational primes p.)

Using the fact that the infinite product $\prod_{n\in\mathbb{N}}(1 + u_n)$ converges absolutely if and only if $\sum_{n\in\mathbb{N}} u_n$ converges absolutely, we deduce immediately that the Euler product

$$\prod_{\text{all } P} (1 - N(P)^{-s})^{-1}$$

converges absolutely for $s > 1$.

Now let m be a positive integer, and $P_1, \ldots, P_r$ the primes of $\mathcal{O}_K$ with $N(P_i) \leq m$. (Proposition 11).

By unique factorization of $\mathcal{O}_K$-ideals into prime powers, we have

$$\begin{aligned}\prod_{i=1}^{r}(1 - N(P_i)^{-s})^{-1} &= \prod_{i=1}^{r}(1 + N(P_1)^{-s} + N(P_2)^{-2s} + \ldots) \quad (N(P_i)^{-s}<1) \\ &= \sum{}' N(A)^{-s} \\ &\geq \sum_{\substack{A:\ N(A)\leq m \\ A\neq 0}} N(A)^{-s} ,\end{aligned}$$

where $\sum'$ denotes the sum over all nonzero ideals A "generated" by $P_1, \ldots, P_r$. Clearly every term in the last series is in $\sum'$, hence the inequality.

Letting $m \to \infty$, the RHS of the inequality becomes $\zeta_K(s)$, while the LHS becomes the Euler product, so the result follows by the convergence of the latter, which we have shown. □

Let R be a ring, K its quotient field.
A *fractional ideal* A of R is an R-submodule of K so that $rA \subseteq R$ for some nonzero $r \in K$.
Clearly every ideal is a fractional ideal. We sometimes refer to the former as an *integral* ideal when clarity is needed.

Theorem 5 The zeta function of an arbitrary order $\mathbb{O}$ in a numberfield K, $\zeta_{\mathbb{O}}(s)$, converges absolutely for $Re(s) > 1$.

Proof (Jenner [1]) : We define an equivalence relation on the fractional ideals of $\mathbb{O}$ by : $A \sim B$ iff $A = \lambda B$ for some nonzero $\lambda \in K$. The number of equivalence classes modulo this relation is finite. (See Theorem 3 §2.4)
Let $A_1, \ldots, A_n$ be a complete set of representatives of these classes, and we may assume the A_i are integral.
Since the index of A_i in $\mathbb{O}$ is finite for each i, we can find a nonzero integer c such that
$c\mathbb{O} \subseteq A_1 \cap \ldots \cap A_n$.
Let F denote the conductor of $\mathbb{O}$ in $\mathbb{O}_K$.
Then $cF = cF\mathbb{O} \subseteq A_i F \subseteq A_i \subseteq \mathbb{O} \subseteq \mathbb{O}_K$ for all i.
Now consider the map $\phi: A \to A\mathbb{O}_K$ from the integral ideals of $\mathbb{O}$ to those of $\mathbb{O}_K$. We wish to obtain some measure of the extent to which ϕ is not one-to-one.
Suppose $\phi(A) = \phi(A')$. Then there exist $\lambda \in K^*$, $1 \leq i_0 \leq n$, such that $\lambda A = A_{i_0}$.

Then $(cF^2 \subseteq) cF \subseteq A_{i_0} = \lambda A \subseteq \mathfrak{O}_K$.

Multiplying by $\mathfrak{O}_K$, we obtain

$$cF \subseteq \lambda A\mathfrak{O}_K \subseteq \mathfrak{O}_K \quad .$$

But $\lambda A\mathfrak{O}_K = \lambda A'\mathfrak{O}_K$, so

$$cF \subseteq \lambda A'\mathfrak{O}_K \subseteq \mathfrak{O}_K \quad .$$

Multiplying by F , we obtain

$$cF^2 \subseteq \lambda A'F \subseteq \lambda A' \subseteq \mathfrak{O}_K \quad .$$

So both λA and $\lambda A'$ are between cF^2 and $\mathfrak{O}_K$.

Now the index $\{\mathfrak{O}_K : cF^2\}$ is finite, and $\lambda A = \lambda A'$ if and only if $A = A'$ as $\lambda \neq 0$. This, together with Proposition 11, shows that there is an integer m so that the number of integral ideals of $\mathfrak{O}$ having the same image under ϕ is at most m .

Let N , N' denote the norm for ideals in $\mathfrak{O}_K$, $\mathfrak{O}$, respectively.

If A is an $\mathfrak{O}$-ideal, we have

$$\begin{aligned} N(A\mathfrak{O}_K) = \{\mathfrak{O}_K : A\mathfrak{O}_K\} &\leqslant \{\mathfrak{O}_K : A\} \\ &= \{\mathfrak{O}_K : \mathfrak{O}\} \cdot \{\mathfrak{O} : A\} \\ &= g \cdot N'(A) \ , \end{aligned}$$

where $g = \{\mathfrak{O}_K : \mathfrak{O}\}$ is finite as $\mathfrak{O}_K$, $\mathfrak{O}$ are lattices of the same dimension in K .

Thus $N'(A)^{-1} \leqslant g \cdot N(A\mathfrak{O}_K)^{-1}$.

Now consider the sum $\sum^* |N'(A)^{-s}|$, taken over all integral $\mathfrak{O}$-ideals A for which $A\mathfrak{O}_K$ is fixed.

The number of terms in the sum is $\leqslant m$, and so

$$\sum^* |N'(A)^{-s}| \leqslant m \cdot |g^s| \cdot |N(A\mathfrak{O}_K)^{-s}|$$

Now let A range over all $\mathfrak{O}$-ideals. Then

$$\sum_{\text{all } A\neq 0} |N'(A)^{-s}| \leq m \cdot |g^s| \cdot \sum_{B} |N(B)^{-s}| \quad ,$$

where the sum on the right is taken over all $\mathbb{O}_K$-ideals B which are images of nonzero $\mathbb{O}$-ideals under ϕ, and each such B is counted once.

But this sum is bounded by $\sum_{\text{All } B\neq 0} |N(B)^{-s}|$, i.e. $\zeta_K(s)$, which converges absolutely for $\mathrm{Re}(s) > 1$ by Theoren 4.

The result then follows. □

1.5 A generalised Euler Product Relation

We observe first that the representation of $\zeta_K(s)$ as the Euler product may be written, using the standard expansion of $(1 - x)^{-1}$ for $|x| < 1$, as follows :

$$\zeta_K(s) = \prod_{\substack{\text{all primes } P \\ \text{of } \mathbb{O}_K}} (1 + N(P)^{-s} + N(P)^{-2s} + \ldots)$$

Of course the representation of $\zeta_K(s)$ as the Euler product is intimately tied up with the factorization of $\mathbb{O}_K$-ideals into prime powers. It is the presence of non-prime power primaries in a nonmaximal order which indicates how the product formula may be generalised.

First we need a generalisation of Proposition 11 :

Proposition 12 Let m be any positive integer, $\mathbb{O}$ an order. Then the number of $\mathbb{O}$-ideals with norm m is finite.

Proof: Let A be an $\mathbb{O}$-ideal with $N(A) = m$.

Then $N(A\mathbb{O}_K) \leq g \cdot N(A) = gm$, as in the proof of Theorem 5.

Then Proposition 11, together with the fact that the mapping ϕ sends only finitely many distinct $\mathfrak{O}$-ideals to the same $\mathfrak{O}_K$-ideal, established in the proof of Theorem 5, proves the result. □

Theorem 6 The zeta function of an arbitrary order $\mathfrak{O}$ in a numberfield K has a representation as a product :

$$\zeta_{\mathfrak{O}}(s) = \prod_{\substack{\text{all primes } P \\ \text{of } \mathfrak{O}}} (1 + N(P)^{-s} + N(Q_1)^{-s} + N(Q_2)^{-s} + \ldots)$$

where the sum in each local P-factor is taken over all primaries Q_i belonging to the prime P .

Proof: Let N be any positive integer. By Proposition 12, there are finitely many primes $P_1, \ldots, P_r$ with norm $\leq N$. For each $P = P_i$, the series $(1 + N(P)^{-s} + N(Q_1)^{-s} + \ldots)$ is absolutely convergent, because $\zeta_{\mathfrak{O}}(s)$ is, for $Re(s) > 1$. Multiplying these together for all i , we obtain

$$F_N(s) = \prod_{P:N(P)\leq N} (1 + N(P)^{-s} + N(Q_1)^{-s} + \ldots)$$

Then $F_N(s)$ is just a sum of all terms $N(A)^{-s}$, where A runs through all products of primaries whose associated primes have norm $\leq N$ .. (The norm is multiplicative as distinct P_i are comaximal.)

So $F_N(s) = \sum' N(A)^{-s}$, taken over all $\mathfrak{O}$-ideals whose associated primes all have norm $\leq N$, by Theorem 3, and the Remark following it which shows that every product of primaries occurring in $F_N(s)$ is normal.

Now $\zeta_{\mathcal{O}}(s) = \sum_{A:N(A)>N} N(A)^{-s} + \sum_{A:N(A)\leq N} N(A)^{-s}$

$< \sum_{A:N(A)>N} N(A)^{-s} + \sum{}' N(A)^{-s}$, as in Theorem 4.

Thus $|\zeta_{\mathcal{O}}(s) - F_N(s)| = |\zeta_{\mathcal{O}}(s) - \sum{}' N(A)^{-s}|$

$< \sum_{A:N(A)>N} N(A)^{-s}$.

By convergence of $\zeta_{\mathcal{O}}(s)$ we must have $\sum_{A:N(A)>N} N(A)^{-s} \to 0$ as $N \to \infty$, and so we obtain the result. □

We now turn to illustrate how the zeta function for the maximal order of a numberfield differs from that for nonmaximal orders by considering the field $K = \mathbb{Q}(i)$.
But first we introduce and develop a concept which distinguishes the "good" from the "bad" ideals in a nonmaximal order, both because we need it for our example, and because of its importance in its own right.

Let $\mathcal{O}$ be a nonmaximal order, F its conductor in $\mathcal{O}_K$.
An ideal I of $\mathcal{O}$ (resp. $\mathcal{O}_K$) is called *regular* (resp. *regular with respect to* $\mathcal{O}$) if $I + F = \mathcal{O}$ (resp. $I + F = \mathcal{O}_K$).

If I is regular, then because $I \subseteq I + J$ and $I \subseteq I : J$ for any ideal J , both $I + J$ and $I : J$ will be regular. If I , J are regular, then so is IJ , and hence also $I \cap J$.
For I,J regular implies that there exist $a \in I$, $b \in J$, $f_1, f_2 \in F$ such that $a + f_1 = 1 = b + f_2$; then

$$1 = (a+f_1)(b+f_2) = ab + (af_2+bf_1+f_1f_2) \in IJ + F ,$$

and so $IJ + F = \mathcal{O}$ or $\mathcal{O}_K$, depending on whether I,J are $\mathcal{O}$- or $\mathcal{O}_K$-ideals.

We now give the main theorem on regular ideals, a result first proved by Dedekind. Our proof is essentially a modern adaptation of the one given in Hancock [2].

First we need a lemma, the so-called "Modular Law":

Lemma 5 If K, L, N are submodules of the R-module M and $K \supseteq L$, then $K \cap (L + N) = L + (K \cap N)$.

Proof: It is obvious $L + (K \cap N) \subseteq K \cap (L + N)$.
If $x \in K \cap (L + N)$, then $x = y + z$, $y \in L$, $z \in N$.
Then $z = x - y \in K$ as $x \in K$ and $y \in L \subseteq K$.
So $z \in K \cap N$, and hence $x \in L + (K \cap N)$. □

Theorem 7 There is a one-to-one correspondence between regular ideals I of $\mathbb{O}$ and regular ideals J of $\mathbb{O}_K$ under the correspondences

$$I \longmapsto I\mathbb{O}_K$$
$$J \longmapsto J \cap \mathbb{O} .$$

The correspondences preserve the operations of sum, intersection and product.
In addition, the norms of corresponding ideals in $\mathbb{O}$ and $\mathbb{O}_K$ are equal.

Proof: If I is a regular $\mathbb{O}$-ideal, i.e. $I + F = \mathbb{O}$, then $I\mathbb{O}_K + F\mathbb{O}_K = \mathbb{O}.\mathbb{O}_K$, i.e. $I\mathbb{O}_K + F = \mathbb{O}_K$, so $I\mathbb{O}_K$ is a regular $\mathbb{O}_K$-ideal.

If J is a regular $\mathbb{O}_K$-ideal, i.e. $J + \mathfrak{F} = \mathbb{O}_K$, then, since $\mathbb{O} \supseteq \mathfrak{F}$, we have, by Lemma 5,

$$(J \cap \mathbb{O}) + \mathfrak{F} = \mathbb{O} \cap (J + \mathfrak{F}) = \mathbb{O} \cap \mathbb{O}_K = \mathbb{O},$$

so that $J \cap \mathbb{O}$ is a regular $\mathbb{O}$-ideal.

We now show the correspondences are inverse.

If I is a regular $\mathbb{O}$-ideal, we want $I = I\mathbb{O}_K \cap \mathbb{O}$.

By Lemma 5, since $I\mathbb{O}_K \supseteq I$, we have

$$I + (I\mathbb{O}_K \cap \mathfrak{F}) = I\mathbb{O}_K \cap (I + \mathfrak{F}) = I\mathbb{O}_K \cap \mathbb{O}.$$

Since I is regular, $I\mathbb{O}_K$ and $\mathfrak{F}$ are comaximal, so, by Lemma 3, $I\mathbb{O}_K \cap \mathfrak{F} = I\mathbb{O}_K.\mathfrak{F}$. Thus

$$I\mathbb{O}_K \cap \mathbb{O} = I + I\mathbb{O}_K.\mathfrak{F} = I + I\mathfrak{F} = I(\mathbb{O} + \mathfrak{F}) = I.\mathbb{O} = I.$$

If J is a regular $\mathbb{O}_K$-ideal, we want $J = (J \cap \mathbb{O})\mathbb{O}_K$.

Clearly $(J \cap \mathbb{O})\mathbb{O}_K \subseteq J\mathbb{O}_K \subseteq J$, so we show $J \subset (J \cap \mathbb{O})\mathbb{O}_K$.

For brevity, put $I = J \cap \mathbb{O}$. Since J is regular, $I + \mathfrak{F} = \mathbb{O}$, so $I\mathbb{O}_K + \mathfrak{F} = \mathbb{O}_K$ as above, and hence

$$I\mathbb{O}_K.J + \mathfrak{F}.J = \mathbb{O}_K.J = J \quad \ldots\ldots \quad (1)$$

Now $\mathfrak{F}J \subseteq J$ and $\mathfrak{F}J \subseteq \mathfrak{F} \subseteq \mathbb{O}$, so $\mathfrak{F}J \subseteq J \cap \mathbb{O} = I$.

Thus $\mathfrak{F}J \subseteq I \subseteq I\mathbb{O}_K$. Putting this in (1), we obtain

$$J \subseteq I\mathbb{O}_K.J + I\mathbb{O}_K = I\mathbb{O}_K = (J \cap \mathbb{O})\mathbb{O}_K.$$

To see that the operations are preserved under the correspondences, it suffices to check each under just one correspondence as we have shown these to be inverse.

$AB \longmapsto (AB)\mathbb{O}_K = (A\mathbb{O}_K)(B\mathbb{O}_K)$, so multiplication is preserved;

$A + B \longmapsto (A + B)\mathbb{O}_K = A\mathbb{O}_K + B\mathbb{O}_K$, so addition is preserved;

$I \cap J \longmapsto (I \cap J) \cap \mathbb{O} = (I \cap \mathbb{O}) \cap (J \cap \mathbb{O})$, so intersection is preserved.

It remains to show the norm is preserved.

Let I be a regular $\mathbb{O}$-ideal.

Then $I\mathbb{O}_K + \mathbb{O} = I\mathbb{O}_K + I + F = I(\mathbb{O}_K + \mathbb{O}) + F = I\mathbb{O}_K + F = \mathbb{O}_K$.

This, together with a Noether isomorphism, gives

$$\mathbb{O}_K/I\mathbb{O}_K = (I\mathbb{O}_K + \mathbb{O})/I\mathbb{O}_K \cong \mathbb{O}/(I\mathbb{O}_K \cap \mathbb{O}) = \mathbb{O}/I \ .$$

So $N(I\mathbb{O}_K) = \overline{N}(I)$, where N = norm in $\mathbb{O}_K$, $\overline{N}$ = norm in $\mathbb{O}$. □

We deduce immediately from the theorem that there is, in fact, a one-to-one correspondence between the regular *primes* of $\mathbb{O}$ and the regular *primes* of $\mathbb{O}_K$.

If P is prime in $\mathbb{O}_K$, then clearly $P \cap \mathbb{O}$ is prime in $\mathbb{O}$.

If p is prime in $\mathbb{O}$, then $p\mathbb{O}_K$ is prime in $\mathbb{O}_K$, for, if not, there exists P' prime in $\mathbb{O}_K$ with $p\mathbb{O}_K \subsetneq P'$, with $p\mathbb{O}_K, P'$ regular. Then by the theorem, $p \subsetneq P' \cap \mathbb{O}$, which is impossible as p is maximal.

It also follows from the theorem that the regular ideals of $\mathbb{O}$ inherit all the good properties of ideals in $\mathbb{O}_K$, in particular, unique factorization into prime powers, and, as a consequence, the fact that, if P is a regular prime of $\mathbb{O}$, then all P-primaries are in fact powers of P .

We conclude this section with the

Example: In $K = \mathbb{Q}(i)$, the maximal order $\mathbb{O}_K = [1, i]$.

The rational primes behave as follows in $\mathbb{O}_K$:

2 ramifies i.e. $2\mathbb{O}_K = (1 + i)^2\mathbb{O}_K$;

the primes $4n + 1$ split e.g. $5\mathbb{O}_K = (1 + 2i)\mathbb{O}_K \cdot (1 - 2i)\mathbb{O}_K$;

the primes $4n + 3$ remain inert, e.g. $3\mathbb{O}_K$.

Now $N(1 + i) = 2$, $N(1 \pm 2i) = 5$, $N(3) = 9$, so the Dedekind zeta function is :

$$\zeta_K(s) = (1 + \frac{1}{2^s} + \frac{1}{4^s} + \ldots).\prod_{p \text{ inert}}(1 + \frac{1}{p^2} + \frac{1}{p^4} + \ldots).\prod_{p \text{ split}}(1 + \frac{1}{p} + \frac{1}{p^2} + \ldots)^2,$$

where p runs through the specified rational primes.
We now consider how $\zeta_K(s)$ differs from $\zeta_{\mathfrak{O}}(s)$ for some nonmaximal orders $\mathfrak{O}$ in K :

(i) $\mathfrak{O} = [1,2i]$ has conductor $\mathfrak{F} = [2,2i]$.
All primes of $\mathfrak{O}_K$, except $(1 + i)\mathfrak{O}_K$, are regular. The regular primes $\alpha\mathfrak{O}_K$ correspond to primes $\alpha\mathfrak{O}$ of $\mathfrak{O}$, and, since the norm is preserved and all primaries are powers of P , the local P-factors in $\zeta_{\mathfrak{O}}(s)$ are identical with the local $P\mathfrak{O}_K$-factors in $\zeta_K(s)$ for P regular. The prime $(1 + i)\mathfrak{O}_K$, however, corresponds to the prime $[2,2i] = \mathfrak{F}$ in $\mathfrak{O}$. The $\mathfrak{F}$-primaries, apart from powers of $\mathfrak{F}$, are $2\mathfrak{O}$, $2i\mathfrak{O}$, $[2 + 2i,4i]$ (Norm 4) , $(2 + 2i)\mathfrak{O}$, $(2 - 2i)\mathfrak{O}$ (Norm 8) , $4\mathfrak{O}$,$4i\mathfrak{O}$, $2[2 + 2i, 4i]$ (Norm 16) , etc.
Note that while $N(\mathfrak{F}) = 2$, $N(\mathfrak{F}^2) = 8$, as the norm is not always multiplicative in $\mathfrak{O}$. (cf. Proposition 12). So $\zeta_{\mathfrak{O}}(s)$ differs from $\zeta_K(s)$ in that the first factor is $(1 + \frac{1}{2^s} + \frac{3}{4^s} + \frac{3}{8^s} + \frac{3}{16^s} + \ldots)$.

(ii) $\mathfrak{O} = [1,3i]$ has conductor $\mathfrak{F} = [3,3i]$.
All primes of $\mathfrak{O}_K$, except $3\mathfrak{O}_K$, are regular. The regular inert primes remain principal in $\mathfrak{O}$ as in (i),

but the ramified and split primes do not : for example $(1 + 2i)\mathfrak{O}_K \cap \mathfrak{O} = [1 - 3i, 15i]$, and $(1 + i)\mathfrak{O}_K \cap \mathfrak{O} = [2, 1 + 3i]$. Of course the local factors for these primes are still the same as for $\zeta_K(s)$. The prime $3\mathfrak{O}_K$ corresponds to the prime $[3, 3i] = F$, and we have F-primaries which are not powers of F as in (i). So $\zeta_{\mathfrak{O}}(s)$ differs from $\zeta_K(s)$ in the local 3-factor, which is $(1 + \frac{1}{3^s} + \frac{3}{9^s} + \frac{3}{27^s} + \frac{3}{81^s} + \dots)$ by the same reasoning as in (i).

(iii) $\mathfrak{O} = [1, 4i]$ has conductor $F = [4, 4i]$.
Here the irregular prime $(1 + i)\mathfrak{O}_K$ corresponds to $P = [2, 4i]$ in $\mathfrak{O}$. F is not prime here, but P-primary. The P-primaries, apart from powers of P, are : $2\mathfrak{O}$, F , $[2 + 4i, 8i]$ (Norm 4), $[8, 4i]$, $[4 + 4i, 8i]$ (Norm 8) , $4\mathfrak{O}$, $4i\mathfrak{O}$, $[4 + 4i, 16i]$, $[4 + 8i, 16i]$, $[4 + 12i, 16i]$, $[8 + 4i, 8i]$ (Norm 16), etc., so the local 2-factor in $\zeta_{\mathfrak{O}}(s)$ is $(1 + \frac{1}{2^s} + \frac{3}{4^s} + \frac{3}{8^s} + \frac{7}{16^s} + \dots)$.

(iv) $\mathfrak{O} = [1, 5i]$ has conductor $[5, 5i]$.
Here $(1 + 2i)\mathfrak{O}_K$ and $(1 - 2i)\mathfrak{O}_K$ are irregular, and both correspond to the prime $[5, 5i] = F$ in $\mathfrak{O}$.
So the local 5-factor in $\zeta_{\mathfrak{O}}(s)$ is $(1 + \frac{1}{5^s} + \frac{3}{25^s} + \frac{3}{125^s} + \frac{3}{625^s} + \dots .)$, compared to $(1 + \frac{1}{5^s} + \frac{1}{25^s} + \dots)^2$ in $\zeta_K(s)$.

(v) $\mathbb{O} = [1, 6i]$ has conductor $[6, 6i]$.

Here both $(1 + i)\mathbb{O}_K$ and $3\mathbb{O}_K$ are irregular, and correspond to the primes $P_2 = [2, 6i]$ and $P_3 = [3,6i]$ in $\mathbb{O}$, respectively. F is not even primary here, in fact $F = P_2.P_3$.

The local 2- and 3-factors turn out to be

$$(1 + \frac{1}{2^s} + \frac{3}{4^s} + \frac{3}{8^s} + \frac{3}{16^s} + \dots) \text{ , and}$$

$$(1 + \frac{1}{3^s} + \frac{4}{9^s} + \frac{2}{27^s} + \frac{3}{81^s} + \dots) \text{ , respectively.}$$

The other factors are, of course, the same as in $\zeta_K(s)$.

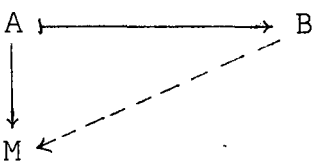
1.6 The Zeta function of an artinian injective module

We conclude this Chapter by discussing in outline a novel approach to the zeta function suggested by Dr K R Hughes. We shall relate this to our zeta function of a nonmaximal order, $\zeta_{\mathbb{O}}(s)$, in order to justify our particular choice of $\zeta_{\mathbb{O}}(s)$ (See §1.3).

The theory required for this discussion is quite substantial, so we shall merely state the main results and supply references for the proofs.

Let R be a ring, M an R-module.

M is said to be *injective* if the following diagram of R-modules and R-homomorphisms fills :



An R-module N is an *essential extension* of M if $M \subseteq N$ and for every nonzero submodule T of N $M \cap T \neq 0$.

Proposition 13: Every R-module M has an essential injective extension N which is unique up to isomorphism.

Proof: See Sharpe and Vamos [1].

We call N (in Proposition 1) the *injective envelope* of M, and write $N = E(M)$.

An R-module M is *indecomposable* if its only direct summands are 0 and M.

Proposition 14: Every injective module over a noetherian ring has a decomposition as a direct sum of indecomposable injective submodules.

Proof: See Matlis [1].

Theorem 8: Let R be a noetherian ring.. Then there is a 1-1 correspondence between the prime ideals of R and the indecomposable injective R-modules given by $P \leftrightarrow E(R/P)$, where P is a prime ideal of R.

Proof: See Matlis [1].

Let R be any ring, E an R-module, I an ideal of R, M a submodule of E.

The *annihilator of* I in E, written $\mathrm{Ann}_E(I)$ is the submodule of E given by $\{x \in E: xI = 0\}$.

The *annihilator of* M in R, written $\mathrm{Ann}_R(M)$ is the ideal of R given $\{x \in R: xM = 0\}$.

We say I (resp. M) is *closed* if $\mathrm{Ann}\,(\mathrm{Ann}\, I) = I$ (resp. $\mathrm{Ann}\,(\mathrm{Ann}\, M) = M$).

An injective R-module E is called an *injective cogenerator* of R if, for every R-module A, and every nonzero $a \in A$, there is an R-homomorphism $\phi: A \to E$ such that $\phi(a) \neq 0$.

Proposition 15: Let R be a ring, E an injective cogenerator of R. Then there is a 1-1 correspondence between the ideals I of R and the *closed* submodules M of E given by $I \longmapsto 0:_E I$, $M \longmapsto 0:_R M$.

Proof: See Sharpe and Vamos [1].

Recall that a nonzero R-module is simple if its only proper submodule is 0.

Let $\{S_i\}_{i \in I}$ be a family of representatives of the simple R-modules. Then $E(\oplus_{i \in I} E(S_i))$ is an injective cogenerator of R (Sharpe and Vamos [1], §2.4).

Now the simple modules of R are R/M, M a maximal ideal of R, and $E(\oplus A_i) = \oplus E(A_i)$ if R is noetherian (Sharpe

and Vamos [1], §4.1), so if we assume also that R has Krull dimension 1 , then it follows that $\bigoplus_{\text{all } P} E(R/P)$ is an injective cogenerator of R .

An *injective resolution* of an R-module M is an exact sequence $0 \longrightarrow M \longrightarrow I^0 \longrightarrow I^1 \longrightarrow \ldots$ where each I^i is injective. A *minimal* injective resolution of M is constructed by putting $I^0 = E(M)$, $I^1 = E(I^0/M)$, $I^2 = E(I^1/\mathrm{Im}(I^0))$ etc., and this is unique up to isomorphism. (Roberts [1] §1.2). The *injective dimension* of M (over R) , written $\mathrm{inj.dim.}_R M$, is equal to $\sup\{i: I^i \neq 0\}$.

A noetherian ring R is *Cohen-Macaulay* if every maximal ideal contains a regular element.
R is *Gorenstein* if it is Cohen-Macaulay and $\mathrm{inj.dim.}_R R < \infty$.

Proposition 16: A noetherian ring R is Gorentein if and only if the following holds :
If $0 \rightarrow R \rightarrow I^0 \rightarrow I^1 \rightarrow \ldots\ldots$ is a minimal injective resolution of R , then $I^j = \bigoplus_{P:\ \mathrm{ht}\ P=j} E(R/P)$, the sum being taken over all primes of R of height j .

Proof: See Bass [1].

Now let R be a Gorenstein domain of dimension 1 , and let Q be its quotient field.
Since R is a domain, $E(R) = Q$, and since $\dim R = 1$,

inj.dim. $R = 1$ also (Bass [1] §1).

So a minimal injective resolution for R is

$$0 \to R \to Q \to E(Q/R) \to 0 ,$$

and thus $E(Q/R) = Q/R$, i.e. Q/R is injective.

Moreover, since all primes of R have height 1 (R has dimension 1 and is a domain), we have, by Proposition 16

$$Q/R = \bigoplus_{\text{all } P} E(R/P) .$$

By our earlier remarks Q/R is thus an injective cogenerator of R , so by Proposition 15 we may deduce

Proposition 17: If R is a Gorenstein domain of Krull dimension 1 and Q is its quotient field, then there is a 1-1 correspondence between the ideals of R and the closed submodules of Q/R .

Theorem 9: Let R be a complete local ring with maximal ideal M , and put $E = E(R/M)$. Then there is a 1-1 correspondence between the ideals of R and the submodules of E .

Proof: See Sharpe and Vamos [1].

Now let R be a noetherian ring, P a prime ideal of R . Let $R_P\hat{}$ denote the completion of R in the P-adic topology. (Ideal-adic completions are discussed in detail in §2.2). Then there are obvious 1-1 correspondences between the

ideals of $R_P\hat{}$ and those of $R_{(P)}$, and between the latter and the P-primary ideals of R. We also know $E(R/P) \cong E(R_P\hat{}/PR_P\hat{})$, so, by Theorem 9, we have

Proposition 18: Let R be noetherian, P a prime ideal of R. Then there is a 1-1 correspondence between the submodules of $E(R/P)$ and the P-primary ideals of R.

A module is *artinian* if every descending chain of its submodules stabilizes.

Let R be a Gorenstein domain of dimension 1.

We define the *zeta function of an artinian injective module* E over R as follows :

$$\zeta_E(s) = \sum_{\substack{\text{all closed} \\ \text{submodules} \\ M \text{ of } E}} \frac{1}{\#|M|^s}, \quad s \in \mathbb{C} .$$

Since E is artinian it is a finite direct sum of indecomposable injective R-modules (Matlis [1] §4), so it suffices to observe that $\overline{\zeta}_E(s)$ is well-defined when E is an indecomposable injective.

We now show how this zeta function relates to our $\zeta_{\mathfrak{O}}(s)$. First we observe that a nonmaximal order $\mathfrak{O}$ of a numberfield is Gorenstein because it satisfies the criterion in Bass [1]

that all its localizations be subrings of discrete valuation rings.

Let P be a prime ideal of $\mathfrak{O}$. Then by Proposition 18 there is a 1-1 correspondence between the P-primary ideals Q of $\mathfrak{O}$ and the submodules of $E = E(\mathfrak{O}/P)$.

Moreover, we show that $\text{Norm } Q = \#|\mathfrak{O}/Q| = \#|0:_E Q|$, and it suffices to show the relation for $Q = P$, for we can then use a Jordan-Hölder argument to prove it for a general P-primary ideal Q.

Now clearly $\mathfrak{O}/P \subseteq 0:_E P$. But $0:_E P$ may be regarded as a vector space over a field $\mathfrak{O}/P$, and $\mathfrak{O}/P$ is a subspace of $0:_E P$. Thus $0:_E P = \mathfrak{O}/P \oplus S$, where S is an $\mathfrak{O}/P$-module Now S is also an $\mathfrak{O}$-module, and $\mathfrak{O}/P \cap S = 0$, so $S = 0$ as E is indecomposable. So in fact $\mathfrak{O}/P = 0:_E P$.

Thus $\overline{\zeta}_E(s)$ is precisely the local P-factor, $\zeta_{\mathfrak{O},P}(s)$, of $\zeta_{\mathfrak{O}}(s)$.

By Proposition 17 there is a 1-1 correspondence between the ideals I of $\mathfrak{O}$ and the closed submodules of $\mathfrak{Q}/\mathfrak{O}$.

We also deduce that $\text{Norm } I = \#|\mathfrak{O}/I| = \#|0:_{\mathfrak{Q}/\mathfrak{O}} I|$, using the normal decomposition of ideals in $\mathfrak{O}$, the above result for primary ideals, and the fact that $\mathfrak{Q}/\mathfrak{O} = \bigoplus_{\text{all } P} E(\mathfrak{O}/P)$.

So $\overline{\zeta}_{\mathfrak{Q}/\mathfrak{O}}(s)$ turns out to be the same as $\zeta_{\mathfrak{O}}(s)$.

The Euler Product relation $\zeta_{\mathfrak{O}}(s) = \prod_{\text{all } P} \zeta_{\mathfrak{O},P}(s)$ (§1.5)

then takes the following pleasing form, since $\mathfrak{Q}/\mathfrak{O} = \bigoplus_{\text{all } P} E(\mathfrak{O}/P)$:

$$\overline{\zeta}_{\bigoplus_{\text{all } P} E(\Phi/P)}(s) = \prod_{\text{all } P} \overline{\zeta}_{E(\Phi/P)}(s) \quad .$$

The relationship we have exhibited between $\overline{\zeta}_E(s)$ and $\zeta_\Phi(s)$ depends on having all P-primaries occurring in the local P-factor of $\zeta_\Phi(s)$, which would not be the case if we had chosen the alternative definition for $\zeta_\Phi(s)$. (See §1.3).

CHAPTER TWO

THE UNITS OF A NONMAXIMAL ORDER

In this Chapter we discuss the extension of some well-known results concerning the units of the maximal order of a numberfield K (usually just called the units of K) to an arbitrary order. We shall consider the classical Dirichlet Unit Theorem on the structure of the group of units, as well as the Class Group and Class Number, of arbitrary orders.

Before proceeding to discuss these topics per se, we need to develop some machinery, viz. the theory of ideles, as well as ideal-adic completions of semi-local rings.

2.1 The ideles of an algebraic numberfield

Let K be a numberfield of degree n.
By the *signature* of K we mean the ordered pair (r_1,r_2), where r_1 is the number of real embeddings, and r_2 is the number of non-conjugate complex embeddings, of K in its algebraic closure $\mathbb{C}$.

From Galois theory we know that $n = r_1 + 2r_2$.
To each of these embeddings σ of K we associate a valuation on K as follows :

$$|x|_\sigma = \begin{cases} |\sigma(x)| & \text{if } \sigma \text{ is real} \\ |\sigma(x)|^2 & \text{if } \sigma \text{ is complex.} \end{cases}$$

Now the non-archimedean valuations of K all come from prime ideals of $\mathfrak{O}_K$, called the *finite primes* of K ; and

corresponding to the $r_1 + r_2$ archimedean valuations defined above, we introduce $r_1 + r_2$ *infinite primes* of K.

For any prime P of K, finite or infinite, let $K_P\hat{}$ denote the completion of K in the P-adic topology (i.e. the metric topology induced by the valuation $|\ |_P$), and for P finite let $\mathfrak{O}_P\hat{}$ (resp. $P\hat{}$) denote the closure of $\mathfrak{O}_K$ (resp. P) in $K_P\hat{}$. (Observe that for P an infinite prime, $K_P\hat{}$ is just $\mathbb{R}$ or $\mathbb{C}$, depending on whether P is real or complex).

It is clear that $\mathfrak{O}_P\hat{}$ and $P\hat{}$ are complete, as they are closed subspaces of the complete metric space $K_P\hat{}$.

Proposition 1 $\mathfrak{O}_P\hat{}$ and $P\hat{}$ are open in $K_P\hat{}$.

Proof: (adapted from Goldstein [1]) :

We show first that $\mathfrak{O}_P\hat{} = \{x \in K_P\hat{} : |x|_P \leq 1\}$,

and $P\hat{} = \{x \in K_P\hat{} : |x|_P < 1\}$,

from which it follows immediately that $P\hat{}$ is open.

We know from the elementary theory of valuations that

$$\mathfrak{O}_{K(P)} = \{x \in K : |x|_P \leq 1\}$$

and $$P\mathfrak{O}_{K(P)} = \{x \in K : |x|_P < 1\}.$$

(We denote the P-adic valuations on K and $K_P\hat{}$ both by $|\ |_P$, as the former extends uniquely to the latter.)
It is clear that $\mathfrak{O}_P\hat{} \subseteq \{x \in K_P\hat{} : |x|_P \leq 1\}$, for $\mathfrak{O}_K \subseteq \{x \in K_P\hat{} : |x|_P \leq 1\}$, and the latter set is obviously closed.

For the reverse inclusion, it suffices to show that if $x \in K_P\hat{}$, $|x|_P \leq 1$, and $0 < \varepsilon < 1$ is given, we can find $z \in \mathbb{O}_K$ such that $|x-z|_P < \varepsilon$.

Now K is dense in $K_P\hat{}$, so $\exists\ y \in K$ such that $|x-y|_P < \varepsilon$.

Then $|y|_P = |x - (x-y)|_P \leq \max(|x|_P, |x-y|_P) \leq 1$.

By the Strong Approximation Theorem, $\exists\ z \in K$ such that $|y-z|_P < \varepsilon$, and $|z|_Q \leq 1$ for primes $Q \neq P$.

But then $|z|_P = |y - (y-z)|_P \leq \max(|y|_P, |y-z|_P) \leq 1$, so $|z|_Q \leq 1$ for *all* primes Q, and hence $z \in \mathbb{O}_K$.

Moreover, $|x-z|_P \leq \max(|x-y|_P, |y-z|_P) < \varepsilon$, as required.

The statement for $P\hat{}$ is proved similarly.

To see that $\mathbb{O}_P\hat{}$ is open, we merely have to observe that we can write $\mathbb{O}_P\hat{} = \{x \in K_P\hat{} : |x|_P < p\}$ $(p = \text{Norm } P)$ because $||_P$ is a *discrete* valuation, even when extended to $K_P\hat{}$. □

Remarks: It follows immediately from the proof of the Proposition that $\mathbb{O}_P\hat{}$ (resp. $P\hat{}$) may be regarded as the completion of $\mathbb{O}_{K(P)}$ (resp. $PO_{K(P)}$). Since $\mathbb{O}_P\hat{}$ is a discrete valuation ring, it also follows that all its ideals are powers of $P\hat{}$ and these are all open.

Now put $(K_P\hat{})^* = \{\text{units of } K_P\hat{}\}$

$(\mathbb{O}_P\hat{})^* = U_P = \{\text{units of } \mathbb{O}_P\hat{}\}$

The *ideles of the numberfield* K, written $\mathbb{J}_K$, are then defined as follows :

$$\mathbb{J}_K = \{(i_P) \in \prod_{\substack{\text{all primes} \\ P \text{ of } K}} (K_P\hat{})^* : i_P \in U_P \text{ for all but finitely many } P\}$$

We give $\mathbb{J}_K$ a group structure by defining multiplication coordinate-wise : $(ij)_P = i_P \circ j_P$,
and endow it with the topology which has, as basic open neighbourhoods of 1 , sets of the form

$$\prod_{\substack{\text{all primes} \\ P \text{ of } K}} O_P \ , \quad O_P \text{ open in } (K_P\hat{})^* \text{ for all } P \ ,$$

$O_P = U_P$ for all but finitely many P .
(It is clear that U_P is, in fact, open in $(K_P\hat{})^*$ because $\mathfrak{O}_P\hat{}$ is open in $K_P\hat{}$ as we have seen.)
We may regard K^* as a subgroup of $\mathbb{J}_K$ by identifying it with its embedding along the diagonal in $\mathbb{J}_K$, for if $x \in K^*$ then $x \in U_P$ for all but finitely many P (by the Product Formula), so $(x,x,\ldots) \in \mathbb{J}_K$.

We may also define the additive analogue of $\mathbb{J}_K$, the *ring of adeles* $\mathbb{A}_K$, by considering $K_P\hat{}$ and $\mathfrak{O}_P\hat{}$ instead of just their multiplicative subgroups.

We now prove some fundamental results concerning the ideles.

Proposition 2 U_P is compact and open in $(K_P\hat{})^*$.

Proof (Goldstein [1]) : We have seen that U_P is open, and to show it is compact in $(K_P\hat{})^*$, it suffices to show $\mathfrak{O}_P\hat{}$ is compact in $K_P\hat{}$.

Now a metric space is compact if it is complete and totally bounded, i.e. it can be covered by a finite number of sets having arbitrarily small diameter $\varepsilon < 0$. We know $\mathbb{O}_P\hat{}$ is complete, so it remains to show it is totally bounded. It is clear that diameter $(P\hat{})^s = p^{-s}$, so if we can show $\mathbb{O}_P\hat{}/(P\hat{})^s$ is finite, then by choosing s so that $p^{-s} < \varepsilon$, $\mathbb{O}_P\hat{}$ will be covered by the cosets of $(P\hat{})^s$ in $\mathbb{O}_P\hat{}$. We know $\mathbb{O}_K/P^s$ is finite (§1.3), and so it remains to observe that $\mathbb{O}_K/P^s \cong \mathbb{O}_P\hat{}/(P\hat{})^s$, which follows from the Chinese Remainder Theorem. □

Proposition 3 K^* is discrete in $\mathbb{J}_K$.

Proof (adapted from Goldstein [1]) : To show K^* is discrete it suffices to show that 1 is an isolated point of K^* , i.e. that there exists a neighbourhood of 1 in $\mathbb{J}_K$ which contains no other point from K^* .

Now put $N(\varepsilon) = \prod_{P \text{ finite}} U_P \times \prod_{P \text{ infinite}} O_P^\varepsilon$, where $0 < \varepsilon < 1$, and each O_P^ε is a disc around 1 in $K_P\hat{}$ ($= \mathbb{R}$ or $\mathbb{C}$) with radius ε .

Then $x \in K^* \cap N(\varepsilon)$ implies $x \in K^*$ and $x \in U_P$ for all finite P , and $x \in O_P^\varepsilon$ for all infinite P .

This means $x \in K^* \cap U_P$ for all finite P , so $x \in U_K$. (This is proved in detail later, in Proposition (a)). By choosing ε sufficiently small we can ensure that $x = 1$.

□

Definition: Given $x = (x_P) \in \mathbb{J}_K$, we define the *volume* of x as $\|x\| = \prod_{\substack{\text{all primes} \\ P}} |x_P|_P$.

(This is well-defined as $|x_P|_P = 1$ for all but finitely many P by definition of $\mathbb{J}_K$.)

Now set $\mathbb{J}_K^\rho = \{x \in \mathbb{J}_K : \|x\| = \rho\}$, referred to as the *ideles of volume* ρ , for any $\rho > 0$.

It is clear that $K^* \subseteq \mathbb{J}_K^1$ from the Product Formula.

The next result requires the Density Lemma of Artin and Whaples. The proof of this Lemma is very lengthy and technical, so we shall state it without proof. (See Lang [2], for example, for a proof.)

Definition: Given $i \in \mathbb{J}_K$, put $\Pi(i) = \{(b_P) \in \mathbb{A}_K : |b_P|_P \leq |i_P|_P$ for all $P\}$, called the *parallelotope of size* i . Then set $M(i) = \#|K \cap \Pi(i)|$ (whether finite or not), where the intersection is taken in $\mathbb{A}_K$, obviously.

Density Lemma: Let K be a numberfield. Then ther exist positive constants C,D depending only on K so that, for all $i \in \mathbb{J}_K$, we have

$$C.\|i\| < M(i) \leq \max(1, D.\|i\|) .$$

Proposition 4: $\mathbb{J}_K^1 / K^*$ is compact.

Proof (Lang [2]) : Let $\psi: \mathbb{J}_K \to \mathbb{R}^+$ be the map $a \longmapsto \|a\|$. Since $\psi(K^*) = 1$, ψ is defined on $\mathbb{J}_K/K^*$, and the kernel

of this map is clearly $\mathbb{J}_K^1 / K^* = C^1$. For any real number $\rho > 0$, let $C^\rho = \psi^{-1}(\rho)$.

Then C^ρ is topologically isomorphic to C^1 .

In fact, putting $a^\rho = (a_P^\rho)$ with

$$a_P^\rho = \begin{cases} \rho^{1/n} & \text{for } P \text{ infinite} \\ 1 & \text{for } P \text{ finite} , \end{cases}$$

we see that $\psi(a^\rho) = \rho$ and $C^\rho = \rho C^1$.

It therefore suffices to show that C^ρ is compact for some $\rho > 0$.

Now let $F = 2/C$, where C is the constant in the Density Lemma. Then for $i \in \mathbb{J}_K^\rho$, $\rho > F$, we have, by the Density Lemma ,

$$M(i) > \|i\| . C > F.C = 2 .$$

Thus $\mathbb{I}(i) \cap K$ contains a nonzero point, i.e. $\exists\ \alpha^{-1} \in K^*$ such that $|\alpha^{-1}|_P \leq |i_P|_P$ for all P .

This implies that $|\alpha i_P|_P \geq 1$ for all P , and also that

$$|\alpha i_P|_P = \frac{\|\alpha i\|}{\prod_{Q \neq P} |\alpha i_Q|_Q} \leq \frac{\rho}{1} = \rho \quad \text{for all } P .$$

For P finite $|\ |_P$ is a discrete valuation, so $|\alpha i_P|_P$ must be a power of $NP = p$. So either $|\alpha i_P|_P = 1$ or $|\alpha i_P|_P \geq p$. In the latter case we have $NP = p \leq \rho$, and from Proposition 11 (Chapter 1) we see that only a finite number of P can satisfy this inequality.

Thus there exists a finite set of primes S such that

$$1 \leq |\alpha i_P|_P \leq \rho \quad \text{for } P \in S$$

$$|\alpha i_P|_P = 1 \quad \text{for } P \notin S .$$

Let X^ρ be the subset of $\mathbb{J}_K$ defined by these conditions.

Then $X^\rho = \prod_{P \in S} A_P \times \prod_{P \notin S} U_P$, where A_P is an annulus in $(K_P\hat{})^*$.

Each factor of X^ρ is compact, and so X^ρ is compact.

(Since the idelic topology on X^ρ is the same as the topology induced on it by the product topology on $\prod_{\text{all } P} (K_P\hat{})^*$.)

Now the image of the compact X^ρ under the continuous map $\mathbb{J}_K \longrightarrow \mathbb{J}_K/K^*$ is a compact subset of $\mathbb{J}_K/K^*$ containing C^ρ .

Since C^ρ is closed, it must be compact, as required. □

2.2 Ideal-adic completions of semi-local rings

In this section we shall prove only those results in the theory which we require for our purpose. The material is taken essentially from Nagata [1] (unless otherwise indicated), and any details omitted may be found there.

Let I be an ideal of a ring R , M an R-module.

We define a topology on M , called the I-*adic topology* on M , by taking as basic open neighbourhoods of 0 the sets $I^n M$, $n \geqslant 0$.

By regarding R as a module over itself we obtain the I-adic topology on R .

Definition: A ring R is said to be *semi-local* if it is noetherian and has only a finite number of maximal ideals.

The *Jacobson radical* of R is the intersection of the maximal ideals of R .

The *natural topology* on a semi-local ring R is the Jacobson radical-adic topology. It is easily shown that the natural topology on R is, in fact, given by a metric, and hence R has a unique (up to isomorphism) completion R^* in the natural topology.

Before proceeding further, we mention briefly the *principle of idealization* of a module: Let M be an R-module, and put $R' = R \oplus M$, a direct sum of R-modules.
Define a multiplication on R' by
$(r+m)(r'+m') = rr' + rm' + r'm$.
Then R' becomes a ring containing R and M , in which M is an *ideal* and $M^2 = 0$. The submodules of M are precisely the ideals of R' contained in M , and the structure of M as an R-module is substantially the same as that of M as an R'-module because $R'/M = R$ and $M^2 = 0$.

Nakayama's Lemma : Let R be a ring, I an ideal of R contained in all maximal ideals of R , M a finite R-module. Then $IM = M$ implies $M = 0$.

Proof (Lang [1]): Suppose M is generated by $m_1, \ldots, m_r$. Then $m_1 = a_1m_1 + \ldots + a_rm_r$, $a_i \in I$, by assumption. Hence $(1-a_1)m_1 = a_2m_2 + \ldots + a_rm_r$.

Now $1 - a_1$ is a unit of R for, if not, it would be contained in some maximal ideal P and since $a_1 \in P$ we would get the contradiction $1 \in P$.
Thus M can be generated by $n - 1$ elements. Proceeding inductively, we obtain the result. □

Lemma 1 (Artin-Rees) : Let M be a finite module over a noetherian ring R , N a submodule of M , I an ideal of R . Then there exists a positive integer r such that

$$I^n M \cap N = I^{n-r}(I^r M \cap N) \quad , \text{ for all } n > r .$$

Proof: Using the principle of idealization and the fact that $R \oplus M$ becomes a noetherian ring (Hilbert Basis Theorem), we may assume that M,N are ideals of R .
Let $a_1, \ldots, a_s$ be a basis for I , and $x_1, \ldots, x_s$ be indeterminates. Let S_n be the set of all homogeneous polynomials $f(x_i)$ of degree n in the x_i so that $f(a_1,\ldots,a_s) \in I^n M \cap N$.
Let $S = \bigcup_n S_n$ and let I be the ideal of $R[x_1, \ldots, x_s]$ generated by S . Since $R[x_1, \ldots, x_s]$ is noetherian by the Hilbert Basis Theorem, I is generated by a finite number of elements $f_1, \ldots, f_t$ in S .
Put $d_i = \deg f_i$, $r = \max\{d_i\}$.
For $n > r$, let $a \in I^n M \cap N$.
Since $a \in I^n$, $\exists\, f \in S_n$ such that $f(a_1, \ldots, a_s) = a$.
Since $f \in S$, $f = \sum g_i f_i$, $g_i \in R[x_1, \ldots, x_n]$.

Comparing degrees, we see that g_i must be homogeneous of degree $n - d_i$. Thus we have

$$a = f(a_1, \ldots, a_s) = \sum g_i(a_1, \ldots, a_s) f_i(a_1, \ldots, a_s)$$
$$\in \sum I^{n-d_i} (I^{d_i} M \cap N)$$
$$\subseteq I^{n-r}(I M \cap N) .$$

Thus $I^n M \cap N \subseteq I^{n-r}(I^r M \cap N)$ for $n > r$, and the reverse inclusion is obvious, giving the result. □

Corollary: Let I be an ideal of a noetherian ring R, M a finite R-module. Put $N = \bigcap_{n=0}^{\infty} I^n M$. Then $IN = N$.

Proof: By Lemma 1 $\exists\ r > 0$ such that

$$I^n M \cap N = I^{n-r}(I^r M \cap N) \quad \text{for} \quad n > r .$$

Then $N = \bigcap_{n>r} (N \cap I^n M) = \bigcap_{n>r} I^{n-r}(I^r M \cap N) \subseteq I^{n-r} N$, and clearly $I^{n-r} N \subseteq IN \subseteq N$, so we have $IN = N$, as required. □

Lemma 2: Let I be an ideal of a noetherian ring R, M an R-module, N a submodule of M. Then the I-adic topology on N coincides with the topology induced on N by the I-adic topology on M.

Proof: It is obvious that $I^n N \subseteq I^n M \cap N$.

Lemma 1 implies that

$$I^n M \cap N = I^{n-r}(I^r M \cap N) \subseteq I^{n-r} N \quad \text{for } n > \text{some } r .$$

This proves the assertion. □

Lemma 3: Let I be an ideal of a ring R, M an R-module with the I-adic topology, N a submodule of M. Then the closure of N, $\overline{N}$, is $\bigcap_{n=0}^{\infty} (N + I^n M)$.

Proof: Since each $N + I^n M$ is open, it is also closed. Hence $\overline{N} \subset N + I^n M$ for all n, and so $N \subseteq \bigcap_n (N + I^n M)$. Conversely, let $x \in \bigcap_n (N + I^n M)$. Then $x = b_n + a_n$, $b_n \in N$, $a_n \in I^n M$ for all n. So $x + I^n M$ meets N for all n. Since the sets $x + I^n M$ form a basis for the neighbourhoods of x, it follows that x must be in $\overline{N}$, proving the result. □

Lemma 4: An ideal J in a semi-local ring (with the natural topology) is closed.

Proof: Let m be the Jacobson radical of R. Putting $N = \bigcap_{n=0}^{\infty} m^n$ we see that $JN = N$ by the Corollary to Lemma 1. Using Nakayama's Lemma we deduce that $\cap m^n = N = 0$.

By Lemma 3, $\overline{J} = \cap(J + m^n)$

$= J$ because $\cap m^n = 0$.

So J is closed as asserted. □

Proposition 5: Let J be an ideal of a semi-local ring R with the natural topology, R^* the completion of R. Then the completion of J is JR^* and $JR^* \cap R = J$.

Proof: The first assertion follows immediately from Lemma 2. Now J is closed in R (by Lemma 4), and JR^* is its closure in R^*, so we must have $JR^* \cap R = J$ as required. □

We are now in a position to examine the main substance of this Chapter.

2.3 The Unit Theorem

The original classical geometric proof of the Unit Theorem is based on the Minkowski theory of lattices and is valid for all orders, as no distinction was drawn in the nineteenth century between maximal and nonmaximal orders. (See, for example, the proof in Borevich and Shafarevich [1]).
In his famous paper "On the rings of Valuation Vectors" of 1951, Iwasawa produced an elegant proof of the result using topological methods, but this applied to maximal orders only. We here attempt to generalize the version of Iwasawa's proof given in Goldstein [1] to cover nonmaximal orders.

Let $\mathbb{O}$ be any order of a numberfield K, P a prime of $\mathbb{O}_K$, and put $p = P \cap \mathbb{O}$. Clearly p is a prime of $\mathbb{O}$, for if $a,b \in \mathbb{O}$, $ab \in p = P \cap \mathbb{O}$, then $a \in P$ or $b \in P$, so $a \in p$ or $b \in p$. As usual, $\mathbb{O}_{K(P)}$ and $\mathbb{O}_{(p)}$ denote the localisations of $\mathbb{O}_K$ at P and $\mathbb{O}$ at p, respectively.

We shall use the following definitions and notation in the sequel :

$U_{\mathfrak{O}}$ = units of $\mathfrak{O}$

$W_{\mathfrak{O}}$ = roots of unity of $\mathfrak{O}$

$\overline{\mathfrak{O}^P}$ = closure of $\mathfrak{O}_{(P)}$ in $\mathfrak{O}_P\hat{}$

$$V_P = \begin{cases} \text{units of } \overline{\mathfrak{O}^P} \text{ , for } P \text{ finite} \\ \{x \in (K_P\hat{})^* : |X|_P = 1\} \text{ , for } P \text{ infinite.} \end{cases}$$

$$\mathbb{J}_{\mathfrak{O}}^{\infty} = \prod_{P \text{ finite}} V_P \times \prod_{P \text{ infinite}} (K_P\hat{})^*$$

$$\mathbb{J}_{\infty,1} = \{(x_P) \in \prod_{P \text{ infinite}} (K_P\hat{})^* : \prod_{P \text{ infinite}} |x_P|_P = 1\}$$

A crucial part will be played by two subgroups of $\mathbb{J}_K^1$ which we define as follows :

$$G = \mathbb{J}_{\mathfrak{O}}^{\infty} \cap \mathbb{J}_K^1 = \prod_{P \text{ finite}} V_P \times \mathbb{J}_{\infty,1} \quad .$$

$$G_0 = \prod_{\text{all } P} V_P \quad .$$

The proof of the Theorem depends essentially on the following three Propositions :

(a) $G \cap K^* = U_{\mathfrak{O}}$

(b) G is open in $\mathbb{J}_K^1$

(c) G_0 is compact.

When $\mathfrak{O}$ is maximal (a), (b), (c) follow easily, but for $\mathfrak{O}$ nonmaximal their proof requires some argument.
Each result is proved by a series of lemmas and propositions, many of which we have already discussed in the preceding two sections.

Proposition 6: $\overline{\mathbb{O}^P} \cap K = \mathbb{O}_{(p)}$

Proof: It clearly suffices to show $\overline{\mathbb{O}^P} \cap K \subseteq \mathbb{O}_{(p)}$.
Let $a/b \in \overline{\mathbb{O}^P} \cap K$, $a,b \in \mathbb{O}$.
Then $a \in b\overline{\mathbb{O}^P} \cap \mathbb{O}_{(p)}$.
Now we can let $R = \mathbb{O}_{(p)}$, $R^* = \overline{\mathbb{O}^P}$ and $I = b\mathbb{O}_{(p)}$ and apply Proposition 5 to obtain $b\overline{\mathbb{O}^P} \cap \mathbb{O}_{(p)} = b\mathbb{O}_{(p)}$.
Thus $a \in b\mathbb{O}_{(p)}$, so $a/b \in \mathbb{O}_{(p)}$ as required. □

Corollary: $V_p \cap K^* = \mathbb{O}^*_{(p)}$

Proof: It suffices to show $V_p \cap K^* \subseteq \mathbb{O}^*_{(p)}$.
If $x \in V_p \cap K^*$, then $x \in \overline{\mathbb{O}^P} \cap K = \mathbb{O}_{(p)}$ by Proposition 6.
Now $x \in V_p \cap K^*$ means x is a unit of both $\overline{\mathbb{O}^P}$ and K, both of which are embedded in $K_p\hat{}$. So the inverse of x in $\overline{\mathbb{O}^P}$ and K must be the same thing - say y.
Then $xy = 1$ and $y \in \overline{\mathbb{O}^P} \cap K = \mathbb{O}_{(p)}$, so x is a unit of $\mathbb{O}_{(p)}$. □

Lemma 5: For any ring R, $\bigcap_{\substack{\text{all maximal} \\ \text{ideals } m}} R^*_{(m)} = R^*$.

Proof: Clearly $R^* \subseteq \cap R^*_{(m)}$.
If $r/s \in \cap R^*_{(m)}$, $r,s \in R$, then $r/s \in R^*_{(m)}$ for all m, so $r \notin m$, $s \notin m$ for all m.
Then r,s must be units of R, otherwise, for example, $sR \subseteq m$, and hence $s \in m$. This shows r/s is a unit of R, as required. □

Before proving (a), we need to observe that every prime p of $\mathcal{O}$ can be written as $p = P \cap \mathcal{O}$ for some prime P of $\mathcal{O}_K$. For $p\mathcal{O}_K$, although it may not be prime, is contained in some prime P of $\mathcal{O}_K$, and clearly $p \subseteq P \cap \mathcal{O}$, a prime of $\mathcal{O}$. By the dimension one condition, we must have $p = P \cap \mathcal{O}$.

We can now prove

Proposition (a): $G \cap K^* = U_{\mathcal{O}}$.

Proof: It is obvious that $U_{\mathcal{O}} \subseteq G \cap K^*$.

So let $(x,x,\ldots) \in G \cap K^*$ $(x \in K^*)$.

Then $x \in V_P \cap K^*$ for all finite P.

So $G \cap K^* \subseteq \bigcap_{\substack{\text{finite primes} \\ P \text{ of } \mathcal{O}_K}} (V_P \cap K^*)$

$= \bigcap_{\substack{\text{all primes} \\ P \text{ of } \mathcal{O}}} \mathcal{O}^*_{(p)}$ (by the Corollary to Proposition 6 and the observation following Lemma 5)

$= U_{\mathcal{O}}$ (by Lemma 5) □

In order to prove (b), it suffices to show that $\mathbb{J}^{\infty}_{\mathcal{O}}$ is open in $\mathbb{J}_K$. By definition of the topology on $\mathbb{J}_K$, we must therefore show that

(i) V_P is open for all P

(ii) $V_P = U_P$ for almost all (i.e. all but finitely many) P.

We shall in fact show that (ii) holds for P regular.

Lemma 6: Let A be a domain, A' its integral closure, $\mathfrak{F}$ the conductor of A in A', S a multiplicative set in A. Then we have the following :

(i) $A'_{(S)}$ is the integral closure of $A_{(S)}$, and hence $A_{(S)}$ is integrally closed if A is.

(ii) $A_{(S)}$ is integrally closed if $\mathfrak{F} \cap S \neq \phi$.

(iii) If A' is a finite A-module, then the conductor of $A_{(S)}$ in $A'_{(S)}$ is $\mathfrak{F}A_{(S)}$.

Proof (Zariski and Samuel [1]) : We show first that $A'_{(S)}$ is integrally closed.

Let $x \in K$, the quotient field of A, x integral over $A'_{(S)}$.

Then $x^n + a_{n-1}x^{n-1} + \ldots + a_0 = 0$, $a_i \in A'_{(S)}$.

Each $a_i = {}^{b'_i}\!/_{s_i}$, $b'_i \in A'$, $s_i \in S$. If s is a common multiple of the s_i, we see that $a_i = {}^{b_i}\!/_{s}$, $b_i \in A'$, $s \in S$.

Multiplying the equation by s^n we see that sx is integral over A', whence $sx = z \in A'$. Then $x = {}^{z}\!/_{s} \in A'_{(S)}$ as required. Now $A'_{(S)}$ is easily shown to be integral over $A_{(S)}$.

For if ${}^{r}\!/_{s} \in A'_{(S)}$, $r \in A'$, $s \in S$, then r is integral over A, so $r^n + a_{n-1}r^{n-1} + \ldots + a_0 = 0$, $a_i \in A$. Dividing this equation by s^n we see that ${}^{r}\!/_{s}$ is integral over $A_{(S)}$, thus proving (i).

If $\mathfrak{F} \cap S \neq \phi$, $\exists\ s \in \mathfrak{F} \cap S$, so $sA' \subseteq A$ and hence $A' \subseteq \frac{1}{s}A \subseteq A_{(S)}$.

Thus $A'_{(S)} \subseteq A_{(S)}$, so $A'_{(S)} = A_{(S)}$ and $A_{(S)}$ must be integrally closed by (i). This proves (ii).

If $f \in F$, then $fA' \subseteq A$, so $fA'_{(S)} \subseteq A_{(S)}$. This shows $FA'_{(S)}$ is contained in the condutor of $A_{(S)}$ in $A'_{(S)}$.

Now let d/s be in this conductor, $d \in A$, $s \in S$.

Then $\frac{d}{s}A'_{(S)} \subseteq A_{(S)}$, and so

$dA' = s.\frac{d}{s}A' \subseteq s.\frac{d}{s}A'_{(S)} \subseteq sA_{(S)} \subseteq A_{(S)}$.

Let A' be generated by $x_1, \ldots, x_n$ over A. Then $dx_i = y_i/s_i$, $y_i \in A$, $s_i \in S$ for all i. Let s' be a common multiple of the s_i. Then $dx_i = y'_i/s'$, $y'_i \in A$, $s \in S$, so $dA' \subseteq \frac{1}{s'}A$.

Thus $ds' \in F$, and $d/s = ds'/ss' \in FA_{(S)}$ as required for (iii). □

Proposition 7: Let P be a prime of $\mathbb{O}_K$, and $p = P \cap \mathbb{O}$. Put $S = \mathbb{O} - p$ $(= \mathbb{O} - P)$ and $S' = \mathbb{O}_K - P$.

Then $\mathbb{O}_{K(S)} = \mathbb{O}_{K(S')}$.

Proof: $\mathbb{O}_{K(S')}$ and $\mathbb{O}_{K(P)}$ obviously mean the same thing. We show first that $\mathbb{O}_{K(S)}$ is a discrete valuation ring. We recall that a local Dedekind domain is a discrete valuation ring. (See Cassels & Frolich [1], for example). $\mathbb{O}_{K(S)}$ is obviously local, and it is integrally closed by Lemma 6(ii). That it is noetherian and of Krull dimension one follows from the fact that the mapping $I \longmapsto I \cap R$ of ideals of the local ring $R_{(S)}$ to ideals of R is one-to-one. (See Zariski & Samuel [1], for example.)

Now clearly $\mathbb{O}_{K(S)} \subseteq \mathbb{O}_{K(S')}$. Suppose they are not equal. Using the well-known correspondence between {discrete valuation rings of K} and {primes of $\mathbb{O}_K$} , we see that there exists a prime $P_1 \neq P$ such that $\mathbb{O}_{K(S)} = \mathbb{O}_{K(P_1)}$. Then the valuations $|\ |_{P_1}$ and $|\ |_P$ are inequivalent. This means $\exists\ a \neq 0$ in K such that $|a|_{P_1} > 1$ and $|a|_P < 1$.

Now $|a|_P < 1 \Rightarrow |a^{-1}|_P < 1 \Rightarrow a^{-1} \in \mathbb{O}_{K(P)}$,

while $|a|_P < 1 \Rightarrow a \in P\mathbb{O}_{K(P)}$ $(\subseteq \mathbb{O}_{K(P)}) \Rightarrow a$ is a non-unit of $\mathbb{O}_{K(P)} \Rightarrow a^{-1} \notin \mathbb{O}_{K(P)}$.

This contradicts $\mathbb{O}_{K(P_1)} = \mathbb{O}_{K(S)} \subseteq \mathbb{O}_{K(S')} = \mathbb{O}_{K(P)}$, so the assertion is proved. □

We can now prove, using the notation of Proposition 7,

Proposition (b): G is open in $\mathbb{J}_K^1$.

Proof: If P is a regular prime of $\mathbb{O}_K$, then p is a regular prime of $\mathbb{O}$ by Theorem 7, Chapter 1.

Then $F \cap S \neq \phi$, so by Lemma 6(ii) $\mathbb{O}_{(p)}$ is integrally closed.

But Lemma 6(i) implies that $\mathbb{O}_{K(S)}$ is the integral closure of $\mathbb{O}_{(p)}$, so we must have $\mathbb{O}_{K(S)} = \mathbb{O}_{(p)}$.

Then $\mathbb{O}_{K(P)} = \mathbb{O}_{(p)}$ by Proposition 7.

It follows immediately that $V_P = U_P$ for all regular P , as claimed.

To show that V_P is open in $(K_P\hat{})^*$ for all P, it suffices to show that $\overline{\mathbb{O}^P}$ is open in $K_P\hat{}$ for all P. For this, it is enough to show that $\overline{\mathbb{O}^P}$ contains an open set, as it is a topological ring. We show, in fact, that $\overline{\mathbb{O}^P}$ contains some power of $P\hat{}$, open by Proposition 1.

For brevity, we write P_L for $P\mathbb{O}_{K(P)}$.

By Lemma 6(iii), the conductor of $\mathbb{O}_{(p)}$ in $\mathbb{O}_{K(P)}$, its integral closure, is $F\mathbb{O}_{(p)}$.

Now $F\mathbb{O}_{(p)}$ is an $\mathbb{O}_{K(P)}$-ideal, hence it is a power of P_L, say P_L^r, since $\mathbb{O}_{K(P)}$ is a discrete valuation ring.

Thus $P_L^r \subseteq \mathbb{O}_{(p)}$.

We recall (Remarks following Proposition 1) that $P\hat{}$ may be regarded as the completion of either P or P_L in $\mathbb{O}_P\hat{}$.

We therefore have

$$(P\hat{})^r = (P_L\hat{})^r = (P_L\mathbb{O}_P\hat{})^r = P_L^r\mathbb{O}_P\hat{} = (P_L^r)\hat{} \subseteq \overline{\mathbb{O}^P}, \text{ since}$$

$P_L^r \subseteq \mathbb{O}_{(p)}$. We have thus proved the result. □

Finally, we prove

Proposition (c): G_0 is compact.

Proof: For all P, V_P is open (Proposition (b)), hence closed, and it is contained in the compact U_P (Proposition 2), so is itself compact.

Then by Tychonoff's Theorem, $\prod_{\text{all } P} V_P$ is compact in $\prod_{\text{all } P} (K_P\hat{})^*$ with the product topology. But it is easily seen that the

topology induced on $\prod_{\text{all } P} V_P$ by the product topology on $\prod_{\text{all } P} (K_P\hat{})^*$ is the same as that induced by the topology on $\mathbb{J}_K$.

It thus follows that G_0 is a compact subspace of $\mathbb{J}_K$. □

Having proved Proposition (a), (b) and (c) we are now in a position to prove the main result.

Theorem 1 (Dirichlet Unit Theorem) : Let $\mathfrak{O}$ be any order in a numberfield K with signature (r_1, r_2) . Put $s = r_1 + r_2$. Then the following hold :

(i) $W_{\mathfrak{O}}$ is a finite group.

(ii) $V_{\mathfrak{O}} \cong U_{\mathfrak{O}}/W_{\mathfrak{O}}$ is a free abelian group of rank $s - 1$

(iii) $U_{\mathfrak{O}} = W_{\mathfrak{O}} \oplus V_{\mathfrak{O}}$.

Proof (adapted from Goldstein [1]): Assuming (i) and (ii) we can deduce that $U_{\mathfrak{O}}$ is finitely generated.
Since $W_{\mathfrak{O}}$ is clearly the torsion subgroup of $U_{\mathfrak{O}}$, (iii) then follows by the Fundamental Theorem on finitely generated abelian groups.
It thus remains to prove (i) and (ii).
By Proposition (a), $U_{\mathfrak{O}} = G \cap K^*$, and from this it follows easily that $W_{\mathfrak{O}} = G_0 \cap K^*$. Thus $V_{\mathfrak{O}} \cong (G \cap K^*)/(G_0 \cap K^*)$.
By Proposition (c), G_0 is compact in $\mathbb{J}_K$, and by Proposition 3 K^* is discrete in $\mathbb{J}_K$, so $G_0 \cap K^*$ is both discrete and compact, and hence finite.
This proves (i).

Now $G \cap K^*$ is also discrete, and $G_0 \cap K^*$ is finite, so $(G \cap K^*)/(G_0 \cap K^*)$ is discrete.

By a Noether isomorphism we have

$$(G \cap K^*)/(G_0 \cap K^*) \cong G_0(G \cap K^*)/G_0 ,$$

so $G_0(G \cap K^*)/G_0$ is discrete.

Now consider the continuous homomorphism $\mathbb{J}_K^1 \twoheadrightarrow \mathbb{J}_K^1/K^*$.

By Proposition (b) G is open in $\mathbb{J}_K'$, so it is closed, and hence its image GK^*/K^* under this homomorphism is also closed. Since J_K^1/K^* is compact by Proposition 4, it follows that GK^*/K^* is also compact.

Next consider the continuous homomorphism $GK^*/K^* \twoheadrightarrow GK^*/G_0K^*$. GK^*/K^* is compact, so its image GK^*/G_0K^* is also compact.

By applying Noether isomorphisms, we then have

$$\begin{aligned} GK^*/G_0K^* = GG_0K^*/G_0K^* &\cong G/(G \cap G_0K^*) \\ &= G/(GG_0 \cap G_0K^*) \\ &= G/G_0(G \cap K^*) \\ &\cong \left(G/G_0\right)\Big/\left(G_0(G \cap K^*)/G_0\right) , \end{aligned}$$

so the last quotient is compact.

We have thus seen that $G_0(G \cap K^*)/G_0$ is a discrete subgroup of G/G_0, whose quotient by this subgroup is compact.

Let S_∞ be the set of infinite primes of K, and let $S_\infty' = S_\infty - \{P_0\}$, where P_0 is some fixed infinite prime.

Define a map $f: G \to \mathbb{R}^{S-1}$ by

$$(x_P) \longrightarrow (\log |x_P|_P) \quad P \in S_\infty' .$$

Kerf obviously has V_P at all finite coordinates P (f does not depend on these), as well as at those P in S_∞'; but the P_0'th coordinate is also V_P because if $|x_P|_P = 1$ for

$P \in S'_\infty$ then $|x_{P_0}|_{P_0} = 1$ by definition of G.

So $\operatorname{Ker} f = G_0$.

It is obvious that f is onto, and hence $G/G_0 \cong \mathbb{R}^{s-1}$.

So we have shown that $G_0(G \cap K^*)/G_0$, which is isomorphic to $V_\mathfrak{O}$, is a discrete subgroup of $\mathbb{R}^{s-1}$, whose quotient by this subgroup is compact.

The result then follows from

Lemma 8: Let H be a discrete subgroup of $\mathbb{R}^m$ so that R^m/H is compact. Then H is free abelian of rank m.

Proof (Goldstein [1]): Let E be the $\mathbb{R}$-vector space generated by H. Then we have the exact sequence of continuous maps $R^m/H \to R^m/E \to 0$.

Hence R^m/E is compact and an $\mathbb{R}$-vector space, and so must be 0, i.e. $E = \mathbb{R}^m$. Thus H generates the whole of R^m.

Let $\{x_1, \ldots, x_m\} \subseteq H$ be a basis for $\mathbb{R}^m$, and let H_1 be the free $\mathbb{Z}$-module generated by the x_i.

Then $H_1 \subseteq H$ and the group H/H_1 is a closed subgroup of the compact group R^m/H, and hence compact. But it is also discrete (because H is), and so H/H_1 is finite.

Since H_1 and H/H_1 are both finitely generated, we must have H finitely generated. But H is also torsion free (it is a subgroup of the torsion free $\mathbb{R}^m$), so it must be free.

Suppose H is free abelian of rank r. Since E spans $\mathbb{R}^m$ we have $r \geq m$.

Assume $r > m$. Let $\{e_1, \ldots, e_r\}$ be a set of free $\mathbb{Z}$-generators of H and let there be an $\mathbb{R}$-linear dependence relation of the form

$$e_1 = \sum_{i=2}^{r} a_i e_i \quad , \quad a_i \in \mathbb{R} \ .$$

Let $\varepsilon > 0$ be given. Then there exists an integer N such that the Na_i are all within ε of an integer. Then Ne_1 is the sum of a $\mathbb{Z}$-linear combination of $e_2, \ldots, e_r$ and an $\mathbb{R}$-linear combination of the same with coefficients $\leqslant \varepsilon$ in absolute value. By choosing ε sufficiently small we can ensure that the latter combination is zero, so that

$$Ne_1 = \sum_{i=2}^{r} M_i e_i \quad , \quad M_i \in \mathbb{Z} \ .$$

This contradicts the choice of the e_i as a free $\mathbb{Z}$-basis, hence $r = m$ as required. □

2.4 The Divisor Class Group and Class Number

Let $\mathbb{O}$ be any order in a numberfield K.
A fractional ideal A of $\mathbb{O}$ (defined in Section 1.4) is said to be *invertible* if there exists a fractional ideal B of $\mathbb{O}$ such that $AB = \mathbb{O}$.
All nonzero ideals of the maximal order $\mathbb{O}_K$ are invertible, so the set $I^*(\mathbb{O}_K)$ of all nonzero (fractional) ideals of $\mathbb{O}_K$ forms a multiplicative group.
The nonzero principal ideals $P(\mathbb{O}_K)$ form a subgroup of $I(\mathbb{O}_K)$.
The (divisor) *class group of* K is then defined to be

$$Cl(\mathbb{O}_K) = I^*(\mathbb{O}_K) / P(\mathbb{O}_K) \quad .$$

It is a fundamental result of number theory that the order of $Cl(\mathbb{O}_K)$, denoted by h , is finite. (For example, see Borevich & Shafarevich [1]).

In this section we generalize the notion of the divisor class group to an arbitrary order, and relate the usual class number to the class number for a nonmaximal order.
Our discussion is largely a modification of the treatment of the function field case given in Hayes [1].
We use the following notation :

$I(\mathbb{O})$ = the monoid of fractional ideals of $\mathbb{O}$.
$I^*(\mathbb{O})$ = the group of invertible ideals of $\mathbb{O}$.
$P(\mathbb{O})$ ($\subseteq I^*(\mathbb{O})$) = the group of nonzero principal ideals of $\mathbb{O}$.
$K(\mathbb{O}) = \{I \in I(\mathbb{O}) : I\mathbb{O}_K = \mathbb{O}_K\}$.
$K^*(\mathbb{O})$ = the invertible ideals of $K(\mathbb{O})$.

The *class group of* $\mathbb{O}$ is defined as follows :

$$Cl(\mathbb{O}) = I^*(\mathbb{O}) / P(\mathbb{O}) \quad .$$

We denote $\#|Cl(\mathbb{O})|$ by $h(\mathbb{O})$, and call this the *class number of* $\mathbb{O}$.

We also let $M_F(\mathbb{O})$ (respectively $M_F(\mathbb{O}_K)$) denote the monoid of regular ideals of $\mathbb{O}$ (respectively $\mathbb{O}_K$), and

recall that there is a 1-1 correspondence between $M_F(\mathbb{O})$ and $M_F(\mathbb{O}_K)$ given by $I \longmapsto I\mathbb{O}_K$, $J \longmapsto J \cap \mathbb{O}$. (Theorem 7, Chapter 1).

Proposition 8: If $I \in M_F(\mathbb{O})$, then I is invertible..

Proof: We show first that, if $I,J \in M_F(\mathbb{O})$, $I \subseteq J$, then $\exists\ I' \in M_F(\mathbb{O})$ such that $I = JI'$.
For then $I\mathbb{O}_K \subseteq J\mathbb{O}_K$, and, since $\mathbb{O}_K$ is Dedekind, $\exists\ \tilde{I} \in M_F(\mathbb{O}_K)$ such that $I\mathbb{O}_K = J\mathbb{O}_K.\tilde{I}$.
Put $I' = \tilde{I} \cap \mathbb{O}$. Since products are preserved by the correspondence in Theorem 7, Chapter 1, we have $I = JI'$, with $I' \in M_F(\mathbb{O})$.
Now $I \in M_F(\mathbb{O}) \Rightarrow \exists\ x \in I$, $y \in F$ such that $x + y = 1$.
Clearly $x\mathbb{O} + F \subseteq \mathbb{O}$, and also $\mathbb{O} \subseteq x\mathbb{O} + y\mathbb{O} \subseteq x\mathbb{O} + F$, so that $x\mathbb{O} + F = \mathbb{O}$. Thus $x\mathbb{O} \in M_F(\mathbb{O})$, and $x\mathbb{O} \subseteq I$, so, by what we proved first, $\exists\ I' \in M_F(\mathbb{O})$ such that $II' = x\mathbb{O}$.
Clearly then $x^{-1}I'$ is the inverse of I . □

Lemma 8: Every class of $Cl(\mathbb{O}_K)$ has a representative which is regular.

Proof: Let $C \in Cl(\mathbb{O}_K)$, I an integral representative of C .
Let $P_1, \ldots, P_r$ be the primes common to I and F .
Suppose $I = P_1^{n_1} \ldots P_r^{n_r} J$, with J prime to F .

For each i, let π_i be a parameter for P_i, and let

$$I' = \pi^{-n_1} \ldots\ldots \pi_r^{-n_r} . I .$$

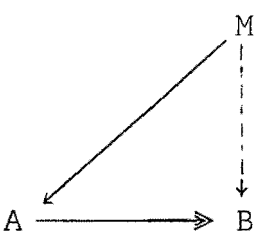
Since I is integral, $\operatorname{ord}_P I \geq 0$ for all P, and hence $\operatorname{ord}_P I' \geq 0$ for all P and $\operatorname{ord}_{P_i} I' = 0$ for all i. Thus I' is prime to F, i.e. regular, and I' clearly also represents C. □

Before proceeding to establish the main result in this section, we need to discuss some module and ring theory which is essential for that purpose. We shall omit most of the proofs of the required results.

Let M be a module over a ring R.

M is said to be *invertible* if $\exists$ an R-module M' such that $MM' = R$.

M is *projective* if the following diagram of R-modules and R-linear homomorphisms fills :



Proposition 9: If M is an invertible module over a local ring R, then M is projective.

Proof: See Bourbaki [1].

Proposition 10: If M is a projective module over a local ring R, then M is free.

Proof: See Kaplansky [1].

A module M over a ring R is *faithful* if $a \in R$, $aM = 0$ implies $a = 0$.

Proposition 11: Let A be a faithful finite algebra over R, a finite direct sum of local rings. Then every invertible submodule of A has the form Ru, where u is a unit of A.

Proof (Hayes [1]): We first prove the result for R a local ring.

Let m be the maximal ideal of R, M an invertible submodule of A. By Proposition 9, M is projective and hence, by Proposition 10, it is free over R.

Let $u_1, \ldots, u_s$ be a basis for M over R, and assume $s \geqslant 2$.

Let M' be the inverse of M. Then $\exists\, x \in M'$ which does not map each u_i in m, for otherwise $MM' \neq R$.

Assume $xu_1 = r_1 \notin m$. Put $xu_2 = r_2$.

Then $x(r_2u_1 - r_1u_2) = 0$ gives a nonzero linear relation between u_1 and u_2 as r_1 and x are invertible in A.

So $M' = Ru_1$, u_1 necessarily a unit of A.

Now suppose $R = \bigoplus_{i=1}^{n} R_i$, each R_i local, M an invertible submodule of A.

Then $M \cong M \otimes_R R = M \otimes (\oplus R_i)$

$= \oplus (M \otimes R_i)$

Put $M_i = M \otimes R_i$. Then $M = \oplus M_i$, and similarly $A = \oplus A_i$.
Since M is invertible, $\exists\ M'$ such that $M \otimes M' \cong R$, and
$M'_i = M' \otimes R_i$ is the inverse of M_i in R_i for each i ,
because

$$M_i \otimes M'_i = (M \otimes R_i) \otimes (M' \otimes R_i)$$
$$= (M \otimes M_i) \otimes R_i$$
$$= R \otimes R_i = R_i \ .$$

By the local case, for each i $\exists\ u_i \in A_i$ such that
$M_i = u_i R_i$.
Then $M = \oplus M_i = \oplus R_i u_i = Ru$, where $u = (u_1, \ldots, u_n)$.
This proves the general case. □

A ring is called *primary* if it contains exactly one prime ideal.
A primary ring which is also noetherian is clearly local.
A ring is *artinian* if every descending chain of its ideals stabilizes.

Proposition 12: An artinian ring is uniquely decomposable as a finite direct sum of noetherian primary rings.

Proof: See Zariski & Samuel [1].

An element $u \in \mathbb{O}_K$ is said to be *prime to* $\mathfrak{F}$ if
$u\mathbb{O}_K + \mathfrak{F} = \mathbb{O}_K$.

This is clearly equivalent to saying that the image of u under the mapping $\mathbb{O}_K \twoheadrightarrow \mathbb{O}_K/F$ is a unit.

Proposition 13 : (a) $I \in K(\mathbb{O}) \Rightarrow \mathbb{O}_K \supseteq I \supseteq F$.

(b) $K(\mathbb{O})$ is a finite monoid.

(c) $I \in K(\mathbb{O})$ is invertible $\iff I = u\mathbb{O} + F$, where $u \in \mathbb{O}_K$ is prime to F .

Proof (adapted from Hayes [1]) :

(a) If $I\mathbb{O}_K = \mathbb{O}_K$, then clearly $I \subseteq \mathbb{O}_K$ and $F = F\mathbb{O}_K = FI\mathbb{O}_K = FI \subseteq I$.

(b) From (a) we see that elements of $K(\mathbb{O})$ correspond one-to-one with the $\mathbb{O}$-submodules of the ring $\mathbb{O}_K/F$, which is finite (Section 1.3). So $K(\mathbb{O})$ must be finite.

(c) Suppose $I \in K(\mathbb{O})$ is invertible with inverse I' . Then $I'\mathbb{O}_K = I'I\mathbb{O}_K = \mathbb{O}\mathbb{O}_K = \mathbb{O}_K$, and so $I' \in K(\mathbb{O})$ also. Then the image of I under the map $\mathbb{O}_K \twoheadrightarrow \mathbb{O}_K/F$ is also invertible. $\mathbb{O}_K/F$ is clearly a finite algebra over $\mathbb{O}_K/F$, which is finite and hence artinian.
By Proposition 12 therefore, it satisfies the conditions of Proposition 11, and thus $(I + F)/F = \bar{u} \cdot \mathbb{O}/F$, where $\bar{u}$ is a unit of $\mathbb{O}_K/F$, i.e. $I = u\mathbb{O} + F$, where $u \in \mathbb{O}_K$ is prime to F . This gives (c). □

Theorem 2: Let $\mathbb{O}$ be an order of K with conductor F . Then $Cl(\mathbb{O})$ is finite and, in fact,

$$h(\mathfrak{O}) = h.\frac{\Phi_{\mathfrak{O}_K}(F)}{\Phi_{\mathfrak{O}}(F).\ \{U_K : U_{\mathfrak{O}}\}} ,$$

where $\Phi_{\mathfrak{O}}(F)$ (resp. $\Phi_{\mathfrak{O}_K}(F)$) is the number of units of $\mathfrak{O}/F$ (resp. $\mathfrak{O}_K/F$), and $\{U_K : U_{\mathfrak{O}}\}$ is the index of the group of units of $\mathfrak{O}$ in the group of units of $\mathfrak{O}_K$.

Proof (adapted from Hayes [1]): Define ψ: $Cl(\mathfrak{O}) \to Cl(\mathfrak{O}_K)$ by $[A] \longmapsto [A\mathfrak{O}_K]$, where $A \in I^*(\mathfrak{O})$.

Let $[B] \in Cl(\mathfrak{O}_K)$, where, by Lemma 8, we can assume that B is regular. Hence $B \cap \mathfrak{O}$ is regular; by Proposition 8 $[B \cap \mathfrak{O}]$ belongs to $Cl(\mathfrak{O})$, and clearly $[B \cap \mathfrak{O}] \to [B]$. This shows ψ is surjective.

We now examine $\operatorname{Ker} \psi$.

Let A be a representative of a given class in $\operatorname{Ker} \psi$. This means $A\mathfrak{O}_K$ is principal, i.e. $A\mathfrak{O}_K = x\mathfrak{O}_K$, for some $x \in K$.

So $x^{-1}A\mathfrak{O}_K = \mathfrak{O}_K$, i.e. $x^{-1}A \in K(\mathfrak{O})$ and $x^{-1}A$ is invertible because A is. Therefore $x^{-1}A \in K^*(\mathfrak{O})$.

Thus every class of $\operatorname{Ker} \psi$ has a representative from $K^*(\mathfrak{O})$. Since $K(\mathfrak{O})$ is finite (Proposition 13(b)), we must have $\operatorname{Ker} \psi$ finite, and $h(\mathfrak{O}) = h.\#|\operatorname{Ker} \psi|$ finite as h is finite too.

We next determine $\#|\operatorname{Ker} \psi|$.

We have seen that every class of $\operatorname{Ker} \psi$ has a representative from $K^*(\mathfrak{O})$.

Two elements $A, B \in K^*(\mathfrak{O})$ belong to the same class of $\operatorname{Ker} \psi$

iff $A = xB$, $x \in K$. But then $\mathfrak{O}_K = A\mathfrak{O}_K = xB\mathfrak{O}_K = x\mathfrak{O}_K$, i.e. x is a unit of $\mathfrak{O}_K$.

So $\operatorname{Ker} \psi = {}^{K^*(\mathfrak{O})}/_{\sim}$, where $A \sim B$ iff $A = xB$, $x \in U_K$, i.e. $\operatorname{Ker} \psi = {}^{K^*(\mathfrak{O})}/_{G}$, where $G = \{x\mathfrak{O}: x \in U_K\}$.

Thus we have $\#|K^*(\mathfrak{O})| = \#|\operatorname{Ker} \psi| \cdot \#|G|$.

Now $x\mathfrak{O} = x'\mathfrak{O}$, $x,x' \in U_K$ iff $x = x'\varepsilon$, $\varepsilon \in U_{\mathfrak{O}}$.

So $\#|G| = \#|{}^{U_K}/_{U_{\mathfrak{O}}}| = \{U_K: U_{\mathfrak{O}}\}$, and this is finite because $U_K, U_{\mathfrak{O}}$ are finitely generated groups with free part of the same rank. (Theorem 1.)

So $\#|K^*(\mathfrak{O})| = \{U_K: U_{\mathfrak{O}}\} \cdot \#|\operatorname{Ker} \psi|$.

It remains to compute $\#|K^*(\mathfrak{O})|$.

From Proposition 13(c) we have seen that a one-to-one correspondence exists between elements of $K^*(\mathfrak{O})$ and $\{u\mathfrak{O}: u \in \left({}^{\mathfrak{O}_K}/_{F}\right)^*\}$.

Now $u\mathfrak{O} = u'\mathfrak{O}$ iff $u = u'\varepsilon$, $\varepsilon \in \left({}^{\mathfrak{O}}/_{F}\right)^*$.

This gives the relation

$$\#|K^*(\mathfrak{O})| = \frac{\#|\left({}^{\mathfrak{O}_K}/_{F}\right)^*|}{\#|\left({}^{\mathfrak{O}}/_{F}\right)^*|} ,$$

which proves the assertion. □

We are now in a position to prove a result which we cited earlier (in Theorem 5, Chapter 1).

Let $A(\mathfrak{O})$ be the set of *arithmetically equivalent* classes of $I(\mathfrak{O})$, i.e. $A \sim B$ iff $A = xB$ for some $x \in K$. Then $Cl(\mathfrak{O})$ operates on $A(\mathfrak{O})$ in a natural way.

Theorem 3: $A(\mathbb{O})$ is finite.

Proof: Let $[A] \in A(\mathbb{O})$. Then the orbit of $[A]$ under $Cl(\mathbb{O})$ is $\{[IA] : [I] \in Cl(\mathbb{O})\}$.

Now $A \in I(\mathbb{O})$, so $A\mathbb{O}_K \in I(\mathbb{O}_K)$ and since ψ (defined in Theorem 2) is onto there exists $B \in I^*(\mathbb{O})$ such that $[B\mathbb{O}_K] = [A\mathbb{O}_K]$.

Then $\exists\ x \in K$ such that $xA\mathbb{O}_K = B\mathbb{O}_K$, i.e. $xAB'\mathbb{O}_K = \mathbb{O}_K$, where B' is the inverse of B .

So $xAB' \in K(\mathbb{O})$ and $[xAB']$ is in the orbit of $[A]$ under $Cl(\mathbb{O})$.

Thus the orbit of each $[A]$ in $A(\mathbb{O})$ contains a class $[A']$ $A' \in K(\mathbb{O})$, and since the latter is finite (Proposition 13(b)), $A(\mathbb{O})$ must also be finite. □

CONCLUDING REMARKS

We have shown in the first Chapter that generalising the zeta function in terms of the primary decomposition of ideals in a nonmaximal order is a meaningful way of approaching the subject.

All the invariants of K, except the Class Number h, which occur in the formula for $\mathrm{Res}_{s=1}\zeta_K(s)$ (Section 1.4) are generalised to nonmaximal orders in Borevich and Shaferivich [1], and we have shown, in Chapter Two, how h can be generalised.

A challenging question which suggests itself is, therefore, whether one can express the residue at $s = 1$ of our generalised zeta function in terms of these generalised invariants.

REFERENCES

H Bass [1] On the ubiquity of Gorenstein rings.
Mathematische Zeitschrift **82**(1963) pp 8-28.

Z I Borevich and I R Shafarevich [1] Number Theory.
Academic Press, New York and London (1966).

N Bourbaki [1] Elements of Mathematics.
Commutative Algebra
Hermann, Paris & Addison-Wesley, Reading Mass.
(1972).

J W S Cassels and I Frohlich (eds) [1] Algebraic Number Theory.
Thompson, Washington DC (1967).

H Cohn [1] A Classical Invitation to Algebraic Numbers and Class Fields.
Springer, New York, Heidelberg, Berlin (1978).

A Devinatz Advanced Calculus.
Holt, Rinehart and Winston, New York (1968).

L J Goldstein [1] Analytic Number Theory.
Prentice Hall, Englewood Cliffs NJ (1971).

H Hancock Foundations of the Theory of Algebraic Numbers.

[1] Vol.I Introduction to the General Theory.

[2] Vol.II The General Theory.

Dover, New York (1964).

D R Hayes [1] Explicit Class Field Theory in Global Function Fields.
Studies in Algebra and Number Theory.
Advances in Mathematics Supplementary Studies
Vol.6 (1979)

K Iwasawa On the Rings of Valuation Vectors.
Annals of Mathematics Vol.**57** (1953) pp.331-356.

W E Jenner [1] Zeta Functions of nonmaximal orders in rational semisimple algebras.
Duke Mathematical Journal Vol.**30** (1963) pp.541-543.

[2] On zeta functions of number fields.
Duke Mathematical Journal Vol.**36** (1969) pp.669-671.

I Kaplansky [1] Projective Modules.
Annals of Mathematics Vol.**68** (1958) pp.372-377.

J L Kelley [1] General Topology.
Van Nostrand, Toronto, New York, London, (1955).

S Lang [1] Algebra
Addison-Wesley, Reading, Mass. (1974).

[2] Algebraic Number Theory.
Addison-Wesley, Reading, Mass., Menlo Park Calif., London, Don Mills Ontario (1970).

E Matlis [1] Injective modules over noetherian rings.
Pacific Journal of Mathematics 8(1958) pp 511-528.

[2] 1-Dimensional Cohen-Macaulay rings.
Lecture Notes in Mathematics 327
Springer, Berlin, Heidelberg, New York (1973).

H Matsumura [1] Commutative Algebra.
W A Benjamin, New York (1970).

M Nagata [1] Local Rings.
Interscience Tracts in Pure and Applied Mathematics No.13.
Interscience, New York and London (1962).

W Narkiewicz [1] Elementary and Analytic Theory of Numbers.
Mathematical Monographs Vol.57
PWN-Polish Scientific Publishers, Warsaw (1974).

D G Northcott [1] Ideal Theory.
Cambridge Tracts in Mathematics and Mathematical Physics No.42
Cambridge Univ. Press, Cambridge (1953).

P Roberts [1] Homological invariants of modules over commutative rings.
Univ. of Montreal Press, Montreal (1980).

D W Sharpe and P Vamos [1] Injective modules.
Cambridge Univ. Press, Cambridge (1972).

E Weiss [1] Algebraic Number Theory.
Chelsea, New York (1963).

O Zariski and P Samuel Commutative Algebra.
[1] Vol.I
[2] Vol.II
Van Nostrand, Princeton N J (1960).

Other Works Consulted :

E Artin and J Whaples Axiomatic characterisation of fields by the Product Formula for Valuations.
Bulletin of the American Mathematical Society 51 (1945) pp 469-492.

C T Benson and B T Weber Computing units in certain orders of algebraic integers.
Journal of Number Theory 5 (1973) pp 99-107.

L Bernstein The Jacobi-Perron Algorithm. Its Theory and Applications.
Lecture Notes in Mathematics 207
Springer, Berlin, Heidelberg, New York (1971).

D A Buchsbaum Lectures on Regular Local Rings in Category Theory, Homology Theory and their Applications I.
Springer, Berlin, Heidelberg, New York (1969).

H S Butts and G Pall Ideals not prime to the conductor in quadratic orders.
Acta Arithmetica 21 (1972) pp 261-270.

C W Curtis and I Reiner Representation Theory of Finite Groups and Associative Algebras.
Pure and Applied Mathematics Vol.XI.
Interscience, New York, London (1962).

B N Delone and D K Faddeev The theory of irrationalities of the third degree.
Translations of Mathematical Monographs Vol.10.
American Mathematical Society, Providence Rhode Island (1964).

E C Dade, O Taussky and H Zassenhaus On the theory of orders, in particular on the semigroup of ideal classes and genera of an order in an algebraic number field.
Mathematische Annalen 148(1962) pp 31-64.

D Falk On the invertibility of ideals in orders.
Journal of Number Theory 8 (1976) pp 308-312.

D Gorenstein An arithmetic theory of adjoint plane curves.
Transactions of the American Mathematical Society 72 (1952) pp 414-436.

D Kirby Artinian modules and Hilbert polynomials.
The Quarterly Journal of Mathematics, Oxford Second Series Vol. 24(1973) pp 47-57.

P J C Lamont Factorization and arithmetic functions for orders in composition algebras.
Glasgow Journal of Mathematics **14**(1973) pp 86-95.

H-W Leopoldt Zur Arithmetik in abelschen Zahlkörpern.
Journal fur die Reine und Angewandte Mathematik
Vol. **209** (1962) pp 54-71.

I Niven and H S Zuckerman An Introduction to the theory of Numbers.
Wiley, New York, London, Sydney (1966).

D G Northcott Injective envelopes and Inverse polynomials.
Journal of the London Mathematical Society (2)
8 (1974) pp 290-296.

I Reiner Class Groups and Picard Groups of Group Rings and Orders.
Regional Conference Series in Mathematics No.26
American Mathematical Society, Providence Rhode Island (1976).

P Roquette Über den Surgularitätsgrad von Teilringen in Funktionen korpern.
Mathematische Zeitschrift **77** (1961) pp 228-240.

R Y Sharp The Cousin complex for a module over a noetherian commutative ring.
Mathematische Zeitschrift **112** (1969) pp 340-356.

R G Swan K-Theory of Finite Groups and Orders.
Notes by E Graham Evans.
Springer, Berlin, Heidelberg, New York (1970).