Number Fields

by

Gabriel Phillips

A thesis submitted to the Graduate Faculty of
Auburn University
in partial fulfillment of the
requirements for the Degree of
Master of Science

Auburn, Alabama
May 6, 2017

Approved by

Ulrich Albrecht, Chair, Professor of Mathematics
Dean Hoffman, Professor of Mathematics
Peter Nylen, Professor of Mathematics

Abstract

This paper focuses on number fields and the number rings associated with a particular number field. This topic falls under the study of algebra, and in particular algebraic number theory. The motivation of this paper is to discuss the properties of these number fields in an effort to observe the prime ideal structure. The Dedekind property is most useful in the observation of the prime ideal structure. Along with discussing the structure of these number fields, we will also briefly talk about completions in a number field, which is from the area of topology.

Table of Contents

Section 1 - Introduction

The study of algebraic number theory focuses on number fields and their properties. A number field is a finite field extension over the field $\mathbb{Q}$ of rational numbers. These such number fields are of the form $\mathbb{Q}[\alpha]$ for some algebraic integer α. An algebraic integer is a complex number which is a root to some monic poynomial with integer coefficients.

Example 1.1: Since $\sqrt{2}$ is a root to the polynomial x^2 - 2, then it is an algebraic integer. We can define the number field $\mathbb{Q}[\sqrt{2}] = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$.

Proposition 1.2: Let d be a square free integer. The set of algebraic integers in the number field $\mathbb{Q}[\sqrt{d}]$ is

$$\{a + b\sqrt{d} \mid a, b \in \mathbb{Z}\} \text{ if } d \equiv 2 \text{ or } 3 \pmod 4$$

$$\{\tfrac{a+b\sqrt{d}}{2} \mid a, b \in \mathbb{Z}, a \equiv b \pmod 2\} \text{ if } d \equiv 1 \pmod 4$$

The result of Proposition 1.2 is that the algebraic integers in $\mathbb{Q}[\sqrt{d}]$ form a ring. Furthermore, this is true for any number field and it can be proven by showing that the sum of two algebraic numbers and the product of two algebraic numbers both yield an algebraic number. The following theorem will be useful in proving this.

Theorem 1.3: The following conditions are equivalent for $\alpha \in \mathbb{C}$:
(i) α is an algebraic integer;
(ii) The additive group of the ring $\mathbb{Z}[\alpha]$ is finitely generated;

(iii) α is a member of some subring of $\mathbb{C}$ having a finitely generated additive group;
(iv) $\alpha A \subset A$ for some finitely generated additive subgroup $A \subset \mathbb{C}$
(Marcus 15-16).

Corollary 1.4: If α and β are algebraic integers, then so are $\alpha + \beta$ and $\alpha\beta$.
Proof: By (ii) of Theorem 1.3, we know that $\mathbb{Z}[\alpha]$ and $\mathbb{Z}[\beta]$ both have finitely generated additive groups. Suppose $\alpha_1, \cdots, \alpha_m$ generate $\mathbb{Z}[\alpha]$, and $\beta_1, \cdots, \beta_n$ generate $\mathbb{Z}[\beta]$. The total of mn products of $\alpha_i\beta_i$ generate $\mathbb{Z}[\alpha, \beta]$. We can see that $\alpha + \beta$, $\alpha\beta \in \mathbb{Z}[\alpha, \beta]$, and by (iii) of Theorem 1.3, we have that they are algebraic integers. ■

From the same notion of the set of algebraic integers in any number field K, we can consider the set of algebraic integers of the complex field $\mathbb{C}$ which we will denote **A**. The set of algebraic integers **A** is a ring, and we will use this to define a number ring.

Definition 1.5: For any number field K, we shall say that the subring $\mathbf{A} \cap K$ of K is the number ring corresponding to K. An example of a number ring is $\mathbb{Z}[\sqrt{3}] = \{a + b\sqrt{3} \mid a, b \in \mathbb{Z}\}$.

Suppose we have a number field K with degree n over $\mathbb{Q}$. We have that K lies in $\mathbb{C}$, and there are exactly n $\mathbb{Q}$-linearly independent monomorphisms of K in $\mathbb{C}$, say $\sigma_1, \cdots, \sigma_n$. We can define two functions trace and norm on K. Then for each $\alpha \in K$, the trace of α on K is defined:

$$\mathrm{T}(\alpha) = \sigma_1(\alpha) + \cdots + \sigma_n(\alpha)$$

and the norm of α on K is defined:

$$\mathrm{N}(\alpha) = \sigma_1(\alpha)\cdots\sigma_n(\alpha)$$

From these definitions we have $\mathrm{T}(\alpha + \beta) = \mathrm{T}(\alpha) + \mathrm{T}(\beta)$ and $\mathrm{N}(\alpha\beta) = \mathrm{N}(\alpha)\mathrm{N}(\beta)$.

Proof: $\mathrm{T}(\alpha + \beta) = \sigma_1(\alpha + \beta) + \cdots + \sigma_n(\alpha + \beta)$

$$\begin{aligned} &= (\sigma_1(\alpha) + \sigma_1(\beta)) + \cdots + (\sigma_n(\alpha) + \sigma_n(\beta)) \\ &= (\sigma_1(\alpha) + \cdots + \sigma_n(\alpha)) + (\sigma_1(\beta) + \cdots + \sigma_n(\beta)) \\ &= \mathrm{T}(\alpha) + \mathrm{T}(\beta). \end{aligned}$$

$$\begin{aligned} \mathrm{N}(\alpha\beta) &= \sigma_1(\alpha\beta)\cdots\sigma_n(\alpha\beta) \\ &= (\sigma_1(\alpha)\sigma_1(\beta))\cdots(\sigma_n(\alpha)\sigma_n(\beta)) \\ &= (\sigma_1(\alpha)\cdots\sigma_n(\alpha))(\sigma_1(\beta)\cdots\sigma_n(\beta)) \\ &= \mathrm{N}(\alpha)\mathrm{N}(\beta). \end{aligned}$$

Suppose we have a number field K as before with K having degree n over $\mathbb{Q}$, and such that $\sigma_1, \cdots, \sigma_n$ are the n embeddings of K in $\mathbb{C}$. If we take any n elements $\alpha_1, \cdots, \alpha_n \in \mathrm{K}$, we can define the discriminant of $\alpha_1, \cdots, \alpha_n$ as follows:

$$\mathrm{disc}(\alpha_1, \cdots, \alpha_n) = |\sigma_i(\alpha_j)|^2$$

which is the square of the determinant of the matrix with $\sigma_i(\alpha_j)$ in the i^{th} row, j^{th} column. We can further define the discriminant using the trace function, that is:

$$\text{disc}(\alpha_1, \cdots, \alpha_n) = |\text{T}(\alpha_i \alpha_j)|.$$

We can now use the discriminant to determine the additive structure of R. Keeping in mind, we are dealing with the number field K having degree n over $\mathbb{Q}$ and let R be the ring of algebraic integers in K, as we have defined to be the number ring corresponding to K.

Definition 1.6: A free abelian group of finite rank n is a group which is the direct sum of n subgroups, each isomorphic to $\mathbb{Z}$.

Theorem 1.7: Let $\{\alpha_1, \cdots, \alpha_n\}$ be a basis for K over $\mathbb{Q}$ consisting entirely of algebraic integers, and let $\text{d} = \text{disc}(\alpha_1, \cdots, \alpha_n)$. Then every $\alpha \in \text{R}$, where R is the ring of algebraic integers in K, can be expressed in the form

$$\alpha = \frac{m_1\alpha_1 + \cdots + m_n\alpha_n}{d}$$

with all $\text{m}_j \in \mathbb{Z}$ and all m_j^2 divisible by d (Marcus 29).

Theorem 1.7 says that R is contained in the free abelian group

$$\tfrac{1}{d}\text{A} = \mathbb{Z}\tfrac{\alpha 1}{d} \oplus \cdots \oplus \mathbb{Z}\tfrac{\alpha n}{d}.$$

Therefore, R has rank n, and R is contained in a free abelian group of rank n. This implies the following corollary.

Corollary 1.8: R is a free abelian group of rank n.

Section 2 - Localization

When dealing with number fields, it is useful to look at the localization of a ring R at some prime ideal P. We will start this discussion by defining a multiplicative subset of a ring. All rings are assumed to be commutative with identity.

Definition 2.1: Let A be a ring. A multiplicative subset, S of A, is a subset containing 1 such that, whenever x, y $\in$ S, then xy $\in$ S. We shall assume 0 is not contained in S.

Suppose S is the multiplicative subset containing all nonzero elements of the ring A. The set K = $S^{-1}A$ is the quotient field of A. We shall define the set K to be the set of quotients $\frac{x}{s}$ with x $\in$ A and s $\in$ S. From this definition it is obvious that A has a canonical inclusion in its field of quotients K.

Definition 2.2: An R-module of a ring R is an additive abelian group A together with a function R $\times$ A $\rightarrow$ A such that for all r, s $\in$ R and
a, b $\in$ A:
(i) r(a+b) = ra + rb;
(ii) (r+s)a = ra + sa;
(iii) (rs)a = r(sa);
(iv) If 1 is the identity of R, then 1a = a for all a $\in$ A. If R is a division ring, then a unitary R-module is called a vector space.

Consider a ring A. If M is an A-module contained in some field L (con-

taining A), then $S^{-1}M$ denotes the set of elements $\frac{v}{s}$ with v ∈ M and s ∈ S. We are actually speaking of equivalence classes by $\frac{v}{s}$. That is, $\frac{v}{s} \sim \frac{w}{t}$ if and only if vt = ws. Then $S^{-1}M$ is an $S^{-1}A$-module. We can sometimes consider the case with M a ring containing A as a subring.

Definition 2.3: A proper ideal P of a ring R is said to be a prime ideal if for any ideals A, B in R, then AB ⊂ P implies A ⊂ P or B ⊂ P.

Let P be a prime ideal of a ring A, then P ≠ A by definition. The complement of P in A, denoted A - P, is a multiplicative subset of A. If we let A - P = S, we can denote $S^{-1}A$ by A_P.

Definition 2.4: A maximal ideal of a ring R is a proper ideal M of R, M ≠ R, such that for any other ideal N of R with M ⊂ N ⊂ R, then either N = M or N = R.

Definition 2.5: A local ring R is a ring which has a unique maximal ideal. In the case of such a local ring R with maximal ideal M, for any element x ∈ R with x ∉ M, then x is a unit. Thus the maximal ideal M of a local ring R is the set of non-units of R.

Example 2.6: If p is a prime and n a positive integer, then $\mathbb{Z}_{p^n}$ is a local ring with a unique maximal ideal p$\mathbb{Z}$.

Notice the ring A_P as defined earlier is a local ring. Its maximal ideal M_P

consists of the quotients $\frac{x}{s}$, with x ∈ P and s ∈ A - P (s in A but not in P).

Theorem 2.7: If R is a commutative ring, then the following conditions are equivalent:

(i) R is a local ring;

(ii) all non-unit, non-zero elements of R are contained in some ideal M ≠ R;

(iii) the non-unit elements of R form an ideal.

Proof: (i) $\Longrightarrow$ (ii) If a ∈ R is a nonunit, then aR ≠ R (where aR denotes the ideal generated by a). **Remark:** Every ideal in a ring with identity is contained in some maximal ideal, thus the unique maximal ideal of a local ring R must contain every ideal of R. Therefore, aR is contained in the unique maximal ideal of R. (ii) $\Longrightarrow$ (iii) and (iii) $\Longrightarrow$ (i) follow from the fact that if I is an ideal of R and a ∈ I, then aR ⊂ I. Consequently, I ≠ R if and only if I consists only of nonunits. ■

Observe that $M_P \cap A = P$. The inclusion ⊃ is clear. Conversely, if $y \in M_P \cap A$ with $y = \frac{x}{s}$ for x ∈ P and s ∈ S, then x = sy ∈ P and s ∉ P. Hence y ∈ P.

Let A be a ring and S a multiplicative subset of A. Consider B an ideal of $S^{-1}A$. Then, $B = S^{-1}(B \cap A)$. The inclusion ⊃ is clear. Conversely, let x ∈ B. Write $x = \frac{a}{s}$ for some a ∈ A and s ∈ S. Then sx ∈ B ∩ A, so $x \in S^{-1}(B \cap A)$.

Section 3 - Integral Closure

Definition 3.1: Let A be a ring and L some field containing A. We shall say for some element $x \in L$, that x is integral over A if either one of the following two conditions holds:

(i) There exists a finitely generated non-zero A-module $M \subset L$ such that $xM \subset M$.

(ii) The element x satisfies some equation

$$x^n + a_{n-1}x^{n-1} + \cdots + a_0 = 0$$

with coefficients $a_i \in A$. Such an equation is called an integral equation. Another way to state this second condition is, that x is a root to some monic polynomial f(x) in A[x], that is, $f(x) = 0$.

The previous two conditions are actually equivalent. Assume (i), that is, there exists $M = \langle v_1, \cdots, v_n \rangle$ such that $xM \subset M$ and $M \neq 0$. Then

$$\begin{aligned} xv_1 &= a_{11}v_1 + \cdots + a_{1n}v_n \\ &\vdots \\ xv_n &= a_{n1}v_1 + \cdots + a_{nn}v_n \end{aligned}$$

with coefficients a_{ij} in A. Transposing $xv_1, \cdots, xv_n$ to the right hand side of these equations we can conclude that the determinant is equal to 0. This gives us an integral equation for x over A. Conversely, assuming (ii), the module M generated by $1, x, \cdots, x^{n-1}$ is mapped into itself by the element x so $xM \subset M$.

Proposition 3.2: Let A be a ring, K its quotient field, and x algebraic

over K. Then there exists an element $c \neq 0$ of A such that cx is integral over A.

Proof: There exists an equation

$$a_n x^n + \cdots + a_0 = 0$$

with $a_i \in A$ and $a_n \neq 0$. Multiply this equation by a_n^{n-1}. Then

$$(a_n x)^n + \cdots + a_0 a_n^{n-1} = 0$$

is an integral equation for $a_n x$ over A. ■

Let B be a ring containing A. We will call B integral over A if every element of B is integral over A.

Proposition 3.3: If B is integral over A and finitely generated as an A-algebra, then B is a finitely generated A-module.

Proof: Use induction on the number of ring generators, and we may assume that $B = A[x]$ for some element x integral over A. We have already seen that our assertion is true for this case. ■

Proposition 3.4: Let $A \subset B \subset C$ be rings. If B is integral over A and C is integral over B, then C is integral over A.

Proof: Let $x \in C$, so x satisfies some integral equation

$$x^n + b_{n-1} x^{n-1} + \cdots + b_0 = 0$$

with $b_i \in B$. Let $B_1 = A[b_0, \cdots, b_{n-1}]$. Then B_1 is a finitely generated A-module by Proposition 3.3, and $B_1[x]$ is a finitely generated B_1-module,

whence it is a finitely generated A-module. Since multiplication by x maps $B_1[x]$ into itself, it follows that x is integral over A. ■

Proposition 3.5: Let A ⊂ B be rings such that B integral over A. Let σ be a homomorphism of B. Then σ(B) is integral over σ(A).
Proof: All we need to do is apply σ to some integral equation satisfied by any element x ∈ B. This will be an integral equation for σ(x) over σ(A). ■

Proposition 3.6: Let R be a ring contained in a field L. Let $\overline{R}$ be the set of elements of L which are integral over R. Then $\overline{R}$ is a ring which we call the integral closure of R in L.
Proof: Let x, y ∈ $\overline{R}$, and let M, N be two finitely generated R-modules such that xM ⊂ M and yN ⊂ N. Then MN is finitely generated, and it is mapped into itself by multiplication with x ± y and xy. ■

Let K be a field and f ∈ K[x] an irreducible polynomial. The polynomial f is said to be separable if in some splitting field of f over K, every root of f is a simple root. If F is an extension field of K, and every element of F is separable over K, then F is said to be a separable extension of K.

Corollary 3.7: Let A be a ring, K its quotient field, and L a finite separable extension of K. Let x be an element of L which is integral over A. Then the norm and trace of x from L to K are integral over A, and so are the coefficients of the irreducible polynomial satisfied by x over K.
Proof: For each isomorphism σ of L over K, σ(x) is integral over A. Since

the norm is the product of σ(x) over all such σ, and the trace is the sum of σ(x) over all such σ, it follows they are integral over A. Similarly, the coefficients of the irreducible polynomial are obtained from elementary symmetric functions of σ(x), and are therefore integral over A. ■

Definition 3.8: A ring R is integrally closed in a field L if R = $\overline{R}$. We say that R is integrally closed if it is integrally closed in its quotient field.

Let A be a ring, M an A-module and B a nonempty subset of A. B is called a submodule of M provided that B is an additive subgroup of M and rb $\in$ B for all r $\in$ A, b $\in$ B. A submodule of a vector space over a division ring is called a subspace.

A module M is said to satisfy the ascending chain condition (ACC) on submodules if for every chain $A_1 \subset A_2 \subset A_3 \subset \cdots$ of submodules of M, there is an integer n such that $A_i = A_n$ for all i $\geq$ n.

Definition 3.9: A ring A is called Noetherian if it satisfies the ascending chain condition on ideals.

If M and N are modules over a ring A, then $\mathbf{Hom_A(M,N)}$ is the set of all A-module homomorphisms f: M $\rightarrow$ N. If A = $\mathbb{Z}$ we write Hom(M,N) in place of Hom_A(M,N). Hom_A(M,N) is an abelian group under addition and this addition is distributive with respect to composition of functions.

Definition 3.10: If M is a right A-module, the dual M^* of M is the left A-module $\mathrm{Hom}_A(M,A)$. Similarly, if N is a left A-module, the dual N^* of N is the right A-module $\mathrm{Hom}_A(N,A)$.

Theorem 3.11: Let R be a ring with identity. The following conditions on a unitary R-module F are equivalent:
(i) F has a nonempty basis;
(ii) F is the internal direct sum of a family of cyclic R-modules, each of which is isomorphic as a left R-module to R;
(iii) F is R-module isomorphic to a direct sum of copies of the left R-module R;
(iv) there exists a nonempty set X and a function ι: $X \to F$ with the following property: given any unitary R-module A and function f: $X \to A$, there exists a unique R-module homomorphism $\overline{f}$: $F \to A$ such that $\overline{f}\iota = f$. In other words, F is a free object in the category of unitary R-modules.

A unitary F module over a ring R with identity which satisfies the equivalent conditions of the previous Theroem is called a free R-module on the set X.

If F is a free left A-module such that X is a basis for F, and if X is finite, then F^* is a free right A-module with basis $\{f_x \mid x \in X\}$, which is called the dual basis.

Definition 3.12: The kernel of a homomorphism of rings f: $R \to S$ is its kernel as a map of additive groups, that is, $\mathrm{Ker}\ f = \{r \in R \mid f(r) = 0\}$.

Proposition 3.13: Let A be a Noetherian ring, integrally closed. Let L be a finite separable extension of its quotient field K. Then the integral closure of A in L is finitely generated over A.

Proof: Let $w_1, \cdots, w_n$ be a linear basis of L over K. After multiplying each w_i by a suitable element of A, we may assume that the w_i are integral over A. The trace Tr from L to K is a K-linear map of L into K, and it is non-degenerate, that is, there exists an element $x \in L$ such that $Tr(x) \neq 0$. If α is a non-zero element of L, then the function $Tr(\alpha x)$ on L is an element of the dual space of L as K-vector space, and induces a homomorphism of L into its dual space. Since the kernel is trivial, it follows that L is isomorphic to its dual under the bilinear form $(x,y) \longmapsto Tr(xy)$. Let $w_1', \cdots, w_n'$ be the dual basis of $w_1, \cdots, w_n$, so that $Tr(w_i' w_j) = \delta_{ij}$. Let $c \neq 0$ be an element of A such that cw_i' is integral over A. Let $z \in L$ be integral over A. Then zcw_i' is integral over A, and so is $Tr(zcw_i')$ for each i. If we write

$$z = b_1 w_1 + \cdots + b_n w_n$$

with coefficients $b_i \in K$, then $Tr(zcw_i') = cb_i$, and $cb_i \in A$ because A is integrally closed. Hence z is contained in

$$Ac^{-1}w_1 + \cdots + Ac^{-1}w_n.$$

Since z was selected arbitrarily in the integral closure of A in L, it follows that the integral closure is contained in a finitely generated A-module, and thus our proof is finished. ■

Recall that an integral domain R is a commutative ring with identity such

that for any elements a, b $\in$ R whenever ab = 0, either a = 0 or b = 0. A unique factorization domain, or UFD, is an integral domain in which every element can be uniquely factored into a product of prime elements. Also a principal ideal ring (domain) is a ring in which every ideal is principal, that is, an ideal which is generated by a single element x.

Proposition 3.14: If A is a unique factorization domain, then A is integrally closed.

Proof: Suppose there is a quotient $\frac{a}{b}$ with a, b $\in$ A which is integral over A, and a prime element p in A which divides b but not a. For some n $\geq$ 1, we have

$$(\tfrac{a}{b})^n + a_{n-1}(\tfrac{a}{b})^{n-1} + \cdots + a_0 = 0,$$

whence

$$a^n + a_{n-1}ba^{n-1} + \cdots + a_0b^n = 0.$$

Since p divides b, it must divide a^n, and hence p divides a which is a contradiction. ■

Let A be a left module over an integral domain R and for each a $\in$ A let $O_a = \{r \in R \mid ra = 0\}$. Moreover, $A_t = \{a \in A \mid O_a \neq 0\}$ is a submodule of A called the torsion submodule of A. Furthermore, A is a torsion module if $A = A_t$, and A is torsion-free if $A_t = 0$.

Theorem 3.15: Let A be a principal ideal ring, and L a finite separable extension of its quotient field, of degree n. Let B be the integral closure of

A in L. Then B is a free module of rank n over A.

Proof: As a module over A, the integral closure is torsion-free, and by the general theory of principal ideal rings, any torsion-free finitely generated module is in fact a free module. It is obvious that the rank is equal to the degree [L:K]. ■

Proposition 3.16: Let A be a subring of a ring B, integral over A. Let S be a multiplicative subset of A. Then $S^{-1}B$ is integral over $S^{-1}A$. If A is integrally closed, then $S^{-1}A$ is integrally closed.

Proof: If $x \in B$ and $s \in S$, and if M is a finitely generated A-module such that $xM \subset M$, then $S^{-1}M$ is a finitely generated $S^{-1}A$-module which is mapped into itself by $s^{-1}x$, so that $s^{-1}x$ is integral over $S^{-1}A$. As to the second assertion, let x be integral over $S^{-1}A$, with x in the quotient field of A. We have that

$$x^n + \frac{b_{n-1}}{s_{n-1}}x^{n-1} + \cdots + \frac{b_0}{s_0} = 0,$$

$b_i \in A$ and $s_i \in S$. Thus there exists an element $s \in S$ such that sx is integral over A, and hence lies in A. This proves that x lies in $S^{-1}A$. ■

Corollary 3.17: If B is the integral closure of A in some field extension L of the quotient field of A, then $S^{-1}B$ is the integral closure of $S^{-1}A$ in L.

Section 4 - Dedekind Rings

We will define a Dedekind ring (domain) in efforts to further inspect how we may view number rings. A good reason for inspecting these Dedekind rings is that a number ring is always Dedekind. Let's now give some definitions and theorems.

Definition 4.1: A **Dedekind domain** is an integral domain R in which every proper ideal is the product of a finite number of prime ideals.

Definition 4.2: A **fractional ideal** is a nonzero submodule I of K such that $aI \subset R$ for some nonzero $a \in R$.

Example: Every nonzero finitely generated R-submodule I of K is a fractional ideal of R. For if I is generated by $b_1, \cdots, b_n \in K$, then

$$I = Rb_1 + \cdots + Rb_n$$

and for each i, $b_i = \frac{c_i}{a_i}$ with $0 \neq a_i, c_i \in R$. Let $a = a_1 a_2 \cdots a_n$. Then $a \neq 0$ and

$$aI = Ra_2 \cdots a_n c_1 + \cdots + Ra_1 \cdots a_{n-1} c_n \subset R.$$

Definition 4.3: A **discrete valuation ring** is a principal ideal domain that has exactly one nonzero prime ideal.

Lemma 4.4: Let $I, I_1, I_2, \cdots, I_n$ be ideals in an integral domain R.
(i) The ideal $I_1 I_2 \cdots I_n$ is invertible if and only if each I_j is invertible.

(ii) If $P_1 \cdots P_m = I = Q_1 \cdots Q_n$, where the P_i and Q_j are prime ideals in R and every P_i is invertible, then m = n and after indexing $P_i = Q_i$ for each i = 1, $\cdots$, m (Hungerford 402).

Theorem 4.5: If R is a Dedekind domain, then every nonzero prime ideal of R is invertible and maximal (Hungerford 402-403).

Theorem 4.6: Every invertible fractional ideal of an integral domain R with quotient field K is a finitely generated R-module (Hungerford 403).

Theorem 4.7: A module A satisfies the ascending chain condition on submodules if and only if every submodule of A is finitely generated. In particular, a commutative ring R is Noetherian if and only if every ideal R is finitely generated.

Proof: ($\Longrightarrow$) If B is a submodule of A, let S be the set of all finitely generated submodules of B. Since S is nonempty because $0 \in S$, S contains a maximal element C. C is finitely generated by $c_1 c_2 \cdots c_n$. For each $b \in B$ let D_b be the submodule of B generated by b, $c_1 c_2 \cdots c_n$. Then $D_b \in S$ and $C \subset D_b$. Since C is maximal, $D_b = C$ for every $b \in B$, whence $b \in D_b = C$ for every $b \in B$ and $B \subset C$. Since $C \subset B$ by construction, B = C and thus B is finitely generated.

($\Longleftarrow$) Given a chain of submodules $A_1 \subset A_2 \subset A_3 \subset \cdots$, it is easy to verify that $\cup A_i$ is also a submodule of A and therefore finitely generated, say by $a_1, \cdots, a_k$. Since each a_i is an element of some A_i, there is an index n such that $a_i \in A_n$ for i = 1, 2, $\cdots$, k. Consequently, $\cup A_i \subset A_n$, whence $A_i = A_n$

for i $\geq$ n. ■

Theorem 4.8: Let S be an extension ring of R and s $\in$ S. Then the following conditions are equivalent.

(i) s is integral over R;

(ii) R[s] is a finitely generated R-module;

(iii) there is a subring T of S containing 1 and R[s] which is finitely generated as an R-module;

(iv) there is an R[s]-submodule B of S which is finitely generated as an R-module and whose annihilator in R[s] is zero.

Proof: (i) $\Longrightarrow$ (ii): Suppose s is a root to the monic polynomial f $\in$ R[x] of degree n. We claim that $1_R = s^0$, s, s^2, $\cdots$, s^{n-1} generate R[s] as an R-module. Every element of R[s] is of the form g(s) for some g $\in$ R[x]. By the division algorithm, g(x) = f(x)q(x) + r(x) with r $<$ deg f. Therefore,

g(s) = f(s)q(s) + r(s) = 0 + r(s) = r(s). Hence, g(s) is an R-linear combination of 1_R, s, s^2, $\cdots$, s^m with m = deg r $<$ deg f = n.

(ii) $\Longrightarrow$ (iii): This is trivial if we let T = R[s].

(iii) $\Longrightarrow$ (iv): Let B be the subring T. Since R $\subset$ R[s] $\subset$ T, B is an R[s]-module that is finitely generated as an R-module by (iii). Moreover, $1_s \in$ B, uB = 0 for any u $\in$ S implies that u = u1_s = 0; that is, the annihilator of B in R[s] is 0.

(iv) $\Longrightarrow$ (i): Let B be generated over R by b_1, $\cdots$, b_n. We have that B is an R[s]-module $sb_i \in$ B for each i. Therefore, there exists $r_{ij} \in$ R such that

$$sb_1 = r_{11}b_1 + \cdots + r_{1n}b_n$$

$$\vdots$$

$$sb_n = r_{n1}b_1 + \cdots + r_{nn}b_n.$$

Consequently,

$$(r_{11} - s)b_1 + r_{12}b_2 + \cdots + r_{1n}b_n = 0$$
$$r_{21}b_1 + (r_{22} - s)b_2 + \cdots + r_{2n}b_n = 0$$
$$\vdots$$
$$r_{n1}b_1 + r_{n2}b_2 + \cdots + (r_{nn} - s)b_n = 0.$$

Let M be the n x n matrix (r_{ij}) and let $d \in R[s]$ be the determinant of the matrix $M - sI_n$. Then $db_i = 0$ for all i. Since B is generated by the b_i, $dB = 0$. Since the annihilator of B in R[s] is 0 by (iv), we must have $d = 0$. If f is the polynomial $|M - xI_n|$ in R[x], then one of f, -f is monic and

$$\pm f(s) = \pm |M - sI_n| = \pm d = 0.$$

Therefore, s is integral over R. ■

Theorem 4.9: In a nonzero ring R with identity maximal ideals always exist. In fact every ideal I in R ($I \neq R$) is contained in a maximal ideal.

Proof: Since 0 is an ideal and $0 \neq R$, it suffices to prove the second statement. We will use an application of Zorn's Lemma. If A is a ideal in R such that $A \neq R$, then let S be the set of all ideals B in R such that $A \subset B \neq R$. S is nonempty since $A \in S$. Partially order S using set theoretic inclusion; that is, $B_1 \leq B_2 \Leftrightarrow B_1 \subset B_2$. To apply Zorn's Lemma, we must show that every chain $C = \{C_i \mid i \in I\}$ of ideals in S has an upper bound in S. Let $C = \cup_{i \in I} C_i$. We claim that C is a ideal. If a, b ∈ C, then for some i, j ∈ I,

a $\in C_i$ and b $\in C_j$. Since C is a chain, either $C_i \subset C_j$ or $C_j \subset C_i$, say the latter. Hence, a, b $\in C_i$. Since C_i is a ideal, a - b $\in C_i$ and ra $\in C_i$ for all r $\in$ R. Therefore, a, b $\in$ C implies a - b and ra $\in C_i \subset$ C. Consequently, C is a ideal. Since A $\subset C_i$ for all i, A $\subset \cup C_i$ = C. Each $C_i \in$ S, $C_i \neq$ R for all i $\in$ I. Consequently, $1_R \notin C_i$ for every i, whence $1_R \in \cup C_i$ = C. Therefore, C $\neq$ R and hence, C $\in$ S. Clearly C is an upper bound of the chain C. Thus the hypotheses of Zorn's Lemma are satisfied and hence S contains a maximal element. But a maximal element of S is obviously a maximal ideal in R that contains A. ■

Theorem 4.10: If R is commutative, then every maximal ideal M in R is prime.

Proof: Suppose ab $\in$ M but a $\notin$ M and b $\notin$ M. Then each ideal M + aR and M + bR properly contains M. By maximality M + aR = R = M + bR. Since R is commutative and ab $\in$ M, (aR)(bR) $\subset$ (ab)R $\subset$ M. Therefore,

$$R = R^2 = (M + aR)(M + bR) \subset M^2 + (aR)M + M(bR) + (aR)(bR) \subset M.$$

This contradicts the fact that M $\neq$ R since M is maximal. Therefore, a $\in$ M or b $\in$ M, and so M is prime. ■

Theorem 4.11: Let T be a multiplicative subset of an integral domain R such that 0 $\notin$ T. If R is integrally closed, then $T^{-1}R$ is an integrally closed integral domain.

Proof: Observe that $T^{-1}R$ is an integral domain and R may be identified as a subring of $T^{-1}R$. Extending this, the quotient filed Q(R) of R may be

considered as a subfield of the quotient field $Q(T^{-1}R)$ of $T^{-1}R$. It is clear that $Q(R) = Q(T^{-1}R)$. Let $u \in Q(T^{-1}R)$ be integral over $T^{-1}R$, then for some $r_i \in R$ and $s_i \in T$

$$u^n + \frac{r_{n-1}}{s_{n-1}}u^{n-1} + \cdots + \frac{r_1}{s_1}u + \frac{r_0}{s_0} = 0.$$

Multiply through this equation by s^n, where $s = s_0 s_1 \cdots s_{n-1} \in T$. We can conclude that su is integral over R. Since $su \in Q(T^{-1}R) = Q(R)$ and R is integrally closed, $su \in R$. Therefore, $u = \frac{su}{s} \in T^{-1}R$, whence $T^{-1}R$ is integrally closed. ■

Lemma 4.12: Let S be a multiplicative subset of a commutative ring R with identity and let I be an ideal in R.
(i) $I \subset \phi s^{-1}(S^{-1}I)$.
(ii) If $I = \phi s^{-1}(J)$ for some ideal J in $S^{-1}R$, then $S^{-1}I = J$. In other words every ideal in $S^{-1}R$ is of the form $S^{-1}I$ for some ideal I in R.
(iii) If P is a prime ideal in R and $S \cap P = \varnothing$, then $S^{-1}P$ is a prime ideal in $S^{-1}R$ and $\phi s^{-1}(S^{-1}P) = P$ (Hungerford 146).

Remark: There is a one-to-one correspondence between the set U of prime ideals of a ring R which are disjoint from S and the set V of prime ideals of $S^{-1}R$, given by $P \mapsto S^{-1}P$.

Theorem 4.13: Let P be a prime ideal in a commutative ring R with identity.
(i) there is a one-to-one correspondence between the set of prime ideals of R

which are contained in P and the set of prime ideals of R_p, given by
$Q \mapsto Q_p$;
(ii) the ideal P_p in R_p is the unique maximal ideal of R_p.

Proof: Since the prime ideals of R contained in P are precisely those which are disjoint from S = R - P, (i) is an immediate consequence of the remark preceding the theorem. If M is a maximal ideal of R_P, then M is prime, whence $M = Q_P$ for some prime ideal Q of R with $Q \subset P$. But $Q \subset P$ implies $Q_P \subset P_P$. Since $P_P \neq R_P$, we must have $Q_P = P_P$. Therefore, P_P is the unique maximal ideal in R_P. ■

Theorem 4.14: If S is a set, $a \in S$ and for each $n \in \mathbb{N}$, f_n: $S \to S$ is a function ϕ: $\mathbb{N} \to S$ such that $\phi(0) = a$ and $\phi(n + 1) = f_n(\phi(n))$ for every $n \in \mathbb{N}$ (Hungerford 10-11).

Lemma 4.15: If R is a Noetherian, integrally closed integral domain and R has a unique nonzero prime ideal P, then R is a discrete valuation ring (Hungerford 404-405).

Theorem 4.16: (Dedekind's Theorem) The following conditions on an integral domain R are equivalent:
(i) R is a Dedekind domain;
(ii) every proper ideal in R is uniquely a product of a finite number of prime ideals;
(iii) every nonzero ideal in R is invertible;
(iv) every fractional ideal of R is invertible;

(v) R is Noetherian, integrally closed, and every nonzero prime ideal is maximal;

(vi) R is Noetherian and for every nonzero prime ideal P of R, the localization R_p of R at P is a discrete valuation ring.

Proof: (i) $\Longrightarrow$ (ii) and (ii) $\Longrightarrow$ (iii) follow immediately from Lemma 4.4 and Theorem 4.5.

(iii) $\Longrightarrow$ (iv) Trivial since every fractional ideal is a nonzero ideal.

(iv) $\Longrightarrow$ (v) Every ideal of R is invertible and hence finitely generated by Theroem 4.6. Since each of these ideals of R is finitely generated then they are necessarily Noetherian by Theorem 4.7. Let K be the quotient field of R. If $u \in K$ is integral over R, then R[u] is a finitely generated R-submodule of K by Theorem 4.8. Our example following immediately after Definition 4.2 shows that R[u] is a fractional ideal of R. Therefore, R[u] is invertible by our assumption (iv). Thus since R[u]R[u] = R[u], then $R[u] = RR[u] = (R[u]^{-1}R[u])R[u] = R[u]^{-1}R[u] = R$, whence $u \in R$. Therefore R is integrally closed. Finally if P is a nonzero prime ideal in R, then there is a maximal ideal M of R that contains P by Theorem 4.9. M is invertible by assumption. Consequently $M^{-1}P$ is a fractional ideal of R with $M^{-1}P \subset M^{-1}M = R$, whence $M^{-1}P$ is an ideal in R. Since $M(M^{-1}P) = RP = P$ and P is prime, either $M \subset P$ or $M^{-1}P \subset P$. But if $M^{-1}P \subset P$, then $R \subset M^{-1} = M^{-1}R = M^{-1}PP^{-1} \subset PP^{-1} \subset R$, so $M^{-1} = R$. Thus $R = MM^{-1} = MR = M$, which contradicts the fact that M is maximal. Therefore $M \subset P$ and hence $M = P$. Therefore P is maximal.

(v) $\Longrightarrow$ (vi) R_p is an integrally closed integral domain by Theorem 4.11. By Lemma 4.12 every ideal in R_p is of the form $I_p = \{i/s \mid i \in I, s \notin P\}$,

where I is an ideal of R. Since every ideal of R is finitely generated by (v) and by Theorem 4.7. It follows that every ideal of R_p is finitely generated. Therefore R_p is Noetherian by Theorem 4.7. By Theorem 4.13 every nonzero prime ideal of R_p is of the form I_p, where I is a nonzero prime ideal of R that is contained in P. Since every nonzero prime ideal of R is maximal by (v), P_p must be the unique nonzero prime ideal in R_p. Therefore R_p is a discrete valuation ring by Lemma 4.15.

(vi) $\Longrightarrow$ (i) Note that every nonzero ideal I is invertible by (iii). For each ideal I of R choose a maximal ideal M_I of R such that $I \subset M_I \subset R$ ($M_I \neq R$) by Theorem 4.9, and using the Axiom of Choice. If I = R, let $M_R = R$. Then IM_I^{-1} is a fractional ideal of R with $IM_I^{-1} \subset M_I M_I^{-1} \subset R$. Therefore IM_I^{-1} is an ideal of R that clearly contains I. Also if I is proper then $I \subset IM_I^{-1}$ (not equal). Let S be the set of all ideals of R and define a function f: $S \to S$ by $I \mapsto IM_I^{-1}$. Given a proper ideal J, there exists by the Recursion Theorem 4.14 a function ϕ: $\mathbb{N} \to S$ such that $\phi(0) = J$ and $\phi(n + 1) = f(\phi(n))$. If we denote $\phi(n)$ by J_n and M_{J_n} by M_n, then we have an ascending chain of ideals $J = J_0 \subsetneq J_1 \subsetneq J_2 \subsetneq \cdots$ such that $J = J_0$ and $J_{n+1} = f(J_n) = J_n M_n^{-1}$. Since R is Noetherian and J is a proper ideal, there is a least integer k such that

$$J = J_0 \subsetneq J_1 \subsetneq \cdots \subsetneq J_{k-1} \subsetneq J_k = J_{k+1}.$$

Thus $J_k = J_{k+1} = f(J_k) = J_k M_k^{-1}$. This can occur only if $J_k = R$. Consequently $R = J_k = f(J_{k-1}) = J_{k-1} M_{k-1}^{-1}$, so

$$J_{k-1} = J_{k-1}R = J_{k-1}M_{k-1}^{-1}M_{k-1} = RM_{k-1} = M_{k-1}.$$

Since $M_{k-1} = J_{k-1} \subsetneq J_k = R$, we have M_{k-1} is a maximal ideal. Then minimality of k insures that each of $M_0, \cdots, M_{k-2}$ is also maximal. It is easy

to verify that

$$\mathrm{M}_{k-1} = \mathrm{J}_{k-1} = \mathrm{J}_{k-2}\mathrm{M}_{k-2}^{-1} = \mathrm{J}_{k-3}\mathrm{M}_{k-3}^{-1}\mathrm{M}_{k-2}^{-1} = \cdots = \mathrm{J}\mathrm{M}_0^{-1}\mathrm{M}_1^{-1}\cdots\mathrm{M}_{k-2}^{-1}.$$

Consequently since each M_i is invertible,

$$\mathrm{M}_{k-1}(\mathrm{M}_0\cdots\mathrm{M}_{k-2}) = \mathrm{J}\mathrm{M}_0^{-1}\cdots\mathrm{M}_{k-2}^{-1}(\mathrm{M}_0\cdots\mathrm{M}_{k-2}) = \mathrm{J}.$$

Thus J is the product of maximal ideals, hence prime ideals. Therefore R is Dedekind. This concludes the proof. ■

Ideals in Dedekind rings can be generated by two elements, in which case we say the ideals are 2 generated. Furthermore, one of these elements can be taken arbitrarily. Let I be an ideal in a Dedekind ring. If there is some non-zero $\alpha \in \mathrm{I}$, then we can find $\beta \in \mathrm{I}$ such that $\mathrm{I} = \alpha\mathrm{R} + \beta\mathrm{R}$. When ideals are generated by two elements with one element taken arbitrarily, we say that the ideals are $1\frac{1}{2}$ generated.

Section 5 - Prime Ideals

In the following theorems and definitions, we will be discussing those such rings that are commutative. But since the focus of this paper is on number fields and number rings, we need not define these rings to be necessarily commutative in this section because that property follows from the fact they are number rings. This is because our definition of a number ring defines the elements thereof to be in the intersection of the set of algebraic integers **A** along with any number field K in which we are taking into consideration. Thus, these elements are complex numbers, which are commutative.

Let P be a prime ideal of a ring A and let S = A - P. If B is a ring containing A, we denote by B_P the ring $S^{-1}B$. Let B be a ring containing a ring A. Let P be a prime ideal of A and P′ be a prime ideal of B. We say that P′ **lies above** P if $P' \cap A = P$ and we write P′ | P. In this case, the injection
$A \to B$ induces an injection of the factor rings $A/P \to B/P'$, and we have a commutative diagram:

$$\begin{array}{ccc} B & \to & B/P' \\ \uparrow & & \uparrow \\ A & \to & A/P \end{array}$$

in which the horizontal arrows are canonical homomorphisms, and the vertical arrows indicate inclusions. If B is integral over A, then B/P′ is integral over A/P by Proposition 3.5 in section 3.

Nakayama's Lemma: Let A be a ring, B an ideal contained in all maximal

ideals of A, and M a finitely generated A-module. If BM = M, then M = 0.

Proof: Induction on the number of generators of M. Say M is generated by $w_1, \cdots, w_m$. There exists an expression

$$w_1 = a_1 w_1 + \cdots + a_m w_m$$

with $a_i \in B$. Hence

$$(1\text{-}a_1)w_1 = a_2 w_2 + \cdots + a_m w_m.$$

If $1\text{-}a_1$ is not a unit in A, then it is contained in a maximal ideal N. Since $a_1 \in N$ by hypothesis, we have a contradiction. Hence $1\text{-}a_1$ is a unit, and dividing by it shows that M can be generated by m-1 elements, thereby concluding our proof. ■

Proposition 5.1: Let A be a ring, P a prime ideal, and B a ring containing A and integral over A. Then $PB \neq B$, and there exists a prime ideal P' of B lying above P.

Proof: We know that B_P is integral over A_P, and that A_P is a local ring with maximal ideal M_P. Since we have $PB_P = PA_PB = PA_PB_P = M_PB_P$, it will suffice to prove our first assertion when A is a local ring. In that case, if PB = B, then 1 has an expression as a finite linear combination of elements of B with coefficients in P,

$$1 = a_1 b_1 + \cdots + a_n b_n$$

with $a_i \in P$ and $b_i \in B$. Let $B_0 = A[b_1, \cdots, b_n]$. Then $PB_0 = B_0$ and B_0 is a finite A-module by Proposition 3.3. Hence $B_0 = 0$, which is a contradiction.

To prove our second Assertion, we go back to the original notation, and note the following commutative diagram:

$$\begin{array}{ccc} B & \to & B_P \\ \uparrow & & \uparrow \\ A & \to & A_P \end{array}$$

with all arrows inclusions here. We have just proved that $M_P B_P \neq B_P$. Hence $M_P B_P$ is contained in a maximal ideal M of B_P, and $M \cap B_P$ therefore contains M_P. Since M_P is maximal, it follows that $M_P = M \cap A_P$. Let $P' = M \cap B$. Then P' is a prime ideal of B, and taking intersections with A going both ways around our diagram shows that $M \cap A = P$, so that $P' \cap A = P$, which is what needs to be shown. ■

Remark: Let B be integral over A, and let N be an ideal of B, $N \neq 0$. Then $N \cap A \neq 0$. Let $b \neq 0 \in N$. Then b satisfies an equation

$$b^n + a_{n-1}b^{n-1} + \cdots + a_0 = 0$$

with $a_i \in A$, and $a_0 \neq 0$. But a_0 lies in $N \cap A$.

Proposition 5.2: Let A be a subring of B, and assume B is integral over A. Let P' be a prime ideal of B lying over a prime ideal P of A. Then P' is maximal if and only if P is maximal.

Proof: Assume P is maximal in A. Then A/P is a field. We are reduced to proving that a ring which is integral over a field is a field. If K is a field and x is integral over K, then it is standard from elementary field theory that the ring K[x] is itself a field, so x is invertible in the ring. Conversely,

assume that P′ is maximal in B. Then B/P′ is a field, which is integral over the ring A/P. If A/P is not a field, it has a non-zero maximal ideal M. By Proposition 5.1, there exists a maximal ideal N of B/P′ lying above M, which is a contradiction. ■

When an extension is given explicitly by a generating element, then we can describe the primes lying above a given prime more explicitly.

Let A be integrally closed in its quotient field K, and let E be a finite extension of K. Let B be the integral closure of A in E. Assume that B = A[α] for some element α, and let f(X) be the irreducible polynomial of α over K. Let M be a maximal ideal of A. We have a canonical homomorphism
A $\to$ A/M = $\overline{A}$, which extends to the polynomial ring, namely

$$\mathrm{g(X)} = \sum_{i=1}^{m} \mathrm{c}_i \mathrm{X}^i \longmapsto \sum_{i=1}^{m} \overline{c_i} \mathrm{X}^i = \overline{g}(\mathrm{X}),$$

where $\overline{c}$ denotes the residue class mod M of an element c $\in$ A.

Proposition 5.3: We will contend that there is a natural bijection between the prime ideals P′ of B lying above P and the irreducible factors $\overline{P}$(X) of $\overline{f}$(X) having leading coefficient 1. This bijection is such that a prime P′ of B lying above P corresponds to $\overline{P}$ if and only if P′ is the kernel of the homomorphism A[α] $\to$ $\overline{A}$[$\overline{\alpha}$] where $\overline{\alpha}$ is a root of $\overline{P}$.
Proof: Let P′ lie above P. Then the canonical homomorphism B $\to$ B/P′ sends α on a root of $\overline{f}$ which is conjugate to a root of some irreducible factor of $\overline{f}$. Furthermore, two roots of $\overline{f}$ are conjugate over $\overline{A}$ if and only if they

are roots of the same irreducible factors of $\overline{f}$. Finally, let z be a root of $\overline{P}$ in some algebraic closure of $\overline{A}$. The map $g(\alpha) \mapsto \overline{g}(z)$ for $g(X) \in A[X]$ is a well-defined map, because if $g(\alpha) = 0$ then $g(X) = f(X)h(X)$ for some $h(X) \in A[X]$, whence $\overline{g}(z) = 0$ also. Being well-defined, our map is obviously a homomorphism, and since z is a root of an irreducible polynomial over $\overline{A}$, it follows that its kernel is a prime ideal in B, thus proving our contention. ■

Remark 1: The assumption that P is maximal can be weakened to P prime by localizing.

Remark 2: In dealing with extensions of number fields, the assumption $B = A[\alpha]$ is not always satisfied, but it is true that $B_P = A_P[\alpha]$ for all but a finite number of P, so that the previous discussion holds almost always locally.

Definition 5.4: Let I be an ideal in a ring R. The **radical (or nilradical)** of I is the ideal I intersect P, where the intersection is taken over all prime ideals P in R such that P contains I. The radical is denoted Rad I, and if the set of prime ideals containing I is empty, then Rad I is R itself.

Remark: If R has identity, then every ideal I, not equal R, is contained in a maximal ideal M. Since $M \neq R$ and M is necessarily prime, then $\text{Rad } I \neq R$.

Example 5.5: In an integral domain R, the zero ideal is prime. Hence, $\text{Rad } 0 = 0$. In the ring of integers $\mathbb{Z}$, $\text{Rad } (12) = (2) \cap (3) = (6)$ and

Rad (4) = (2) = Rad (32).

Theorem 5.6: If I is an ideal in a commutative ring R, then
Rad I = $\{r \in R \mid r^n \in I, \text{ for some } n > 0\}$.
Proof: If Rad I = R, then $\{r \in R \mid r^n \in I\} \subset$ Rad I. Assume Rad I $\neq$ R. If $r^n \in I$ and P is any prime ideal containing I, then $r^n \in P$ whence $r \in P$. Thus $\{r \in R \mid r^n \in I\} \subset$ Rad I. Conversely, if $t \in R$ and $t^n \notin I$ for all $n > 0$, then $S = \{t^n + x \mid n \in \mathbb{N}^*; x \in I\}$ is a multiplicative set such that
$S \cap I = \emptyset$. There is a prime ideal P disjoint from S that contains I. By construction, $t \in P$ and hence $t \in$ Rad I. Thus $t \notin \{r \in R \mid r^n \in I\}$ implies $t \notin$ Rad I, whence Rad I $\subset \{r \in R \mid r^n \in I\}$. ■

Definition 5.7: An ideal Q $\neq$ R in a ring R is primary if for any a, b $\in$ R: ab $\in$ Q and a $\notin$ Q implies $b^n \in$ Q for some $n > 0$.

Example 5.8: Every prime ideal is primary by definition. If p is a prime integer and $n \geq 2$, then $(p)^n = (p^n)$ is a primary ideal in $\mathbb{Z}$ which is not prime. In general, a power P^n of a prime ideal P need not be primary.

Theorem 5.9: If Q is a primary ideal in a ring R, then Rad Q is a prime ideal.
Proof: Suppose ab $\in$ Rad Q and a $\notin$ Rad Q. Then $a^n b^n = (ab)^n \in$ Q for some n. Since a $\notin$ Rad Q, $a^n \notin$ Q. Since Q is primary, there is an integer $m > 0$ such that $(b^n)^m \in$ Q, whence b $\in$ Rad Q. Therefore, Rad Q is prime. ■

Theorem 5.10: Let Q and P be ideals in a ring R. Then Q is primary for P if and only if:

(i) $Q \subset P \subset \text{Rad } Q$;

(ii) if $ab \in Q$ and $a \notin Q$, then $b \in P$ (Hungerford 381).

Theorem 5.11: If $Q_1, Q_2, \cdots, Q_n$ are primary ideals in a commutative ring R, all of which are primary for the prime ideal P, then $\cap_{i=1}^{n} Q_i$ is also a primary ideal belonging to P (Hungerford 381).

Definition 5.12: An ideal I in a ring R has a **primary decomposition** if $I = Q_1 \cap Q_2 \cap \cdots \cap Q_n$ with each Q_i primary. If no Q_i contains $Q_1 \cap \cdots \cap Q_{i-1} \cap Q_{i+1} \cap \cdots \cap Q_n$ and the radicals of the Q_i are all distinct, then the primary decomposition is said to be **reduced (or irredundant)**.

Section 6 - Completions

In this section we will define a completion, and we will look at a couple of the properties that go along with completions. We will not prove any of these theorems since it is dealing with the study of topology and this paper is meant to focus on the study of algebraic number theory. However, we make mention of the notion of a completion because it is useful in the discussion of number fields and number rings. First, we will define an absolute value.

Definition 6.1: Let K be a field. An **absolute value** on K is a real valued function $x \mapsto |x|_v$ on K satisfying the following three properties:
(i) $|x|_v \geqq 0$ (= 0 if and only if x = 0);
(ii) for all x, y $\in$ K we have $|xy|_v = |x|_v|y|_v$;
(iii) $|x + y|_v \leqq |x|_v + |y|_v$.
If instead of property (iii) we have the stronger condition:
(iv) $|x + y|_v \leqq \max(|x|_v, |y|_v)$,
then we shall say that it is a **valuation**.

An absolute value || defines a distance (x, y) $\mapsto$ |x - y|, and thus defines a topology on the field. If two absolute values define the same topology they are called dependent. If they do not define the same topology they are called independent.

Definition 6.2: Let K be a field. We say the K is **complete** if every cauchy sequence in K converges, that is, there is a limit to every cauchy sequence.

Proposition 6.3: There exists a pair (K_v, i) consisting of a field K_v which is complete under an absolute value, and an embedding i: $K \to K_v$ such that the absolute value on K is induced by that of K_v, and such that iK is dense in K_v. If (K_v, i$\prime$) is another such pair, then there exists a unique isomorphism σ: $K_v \to K_v'$ that preserves the absolute values (Lang, Algebra 468-469).

In the introduction of this paper we saw the term norm, but here we will re-introduce the term with some conditions.

Definiton 6.4: Let K be a field with a non-trivial absolute value, and E be a vector space over K. We define a **norm** on E by a function $\phi \to |\phi|$ of E into the real numbers, satisfying the following conditions:
(i) $|\phi| \geq 0$ for all $\phi \in$ E, and $= 0$ if and only if $\phi = 0$;
(ii) For all x $\in$ K and $\phi \in$ E we have $|x\phi| = |x||\phi|$;
(iii) If ϕ, $\phi\prime \in$ E, then $|\phi + \phi\prime| \leq |\phi| + |\phi\prime|$.
Two norms $||_1$ and $||_2$ are said to be **equivalent** if there exist numbers c_1, c_2 greater than zero such that for all $\phi \in$ E we have: $c_1|\phi|_1 \leq |\phi|_2 \leq c_2|\phi|_1$

Proposition 6.5: Let K be a complete field under a non-trivial absolute value, and let E be a finite-dimensional vector space over K. Then any two norms on E are equivalent (Lang, Algebra 470).

Proposition 6.6: Let K be complete with respect to a non-trivial absolute value. Let α be algebraic over K, and let N be the norm from K(α) to

K. Let n = [K(α): K]. Then $|\alpha| = |N(\alpha)|^{1/n}$.

The notion of completion is used widely in the field of mathematics. The most relative example to any field of mathematics is forming the real numbers from the rational numbers by ordering. Other examples of completions are the p-adic absolute values, and the Banach space used in analysis and topology. The Banach space is a complete normed vector space.

Reference

T. Hungerford, *Algebra*, GTM 73, Springer-Verlag, New York, 1974.

S. Lang, *Algebra*, third edition, GTM 211, Springer-Verlag, New York, 2002.

S. Lang, *Algebraic Number Theory*, second edition, GTM 110, Springer-Verlag, New York, 1994.

D. Marcus, *Number Fields*, Universitext, Springer-Verlag, New York, 1977.