# ON FACTORIZATION IN NON-COMMUTATIVE DOMAINS

by

Hashim Ahmad Al-Tayyar

Submitted in Partial Fulfillment for the Requirements
of the Degree Master of Science
in the Mathematics Department of the
American University of Beirut
Beirut, Lebanon,
1967

In the Name of Allah

The Compassionate

The Merciful

To My Wife

For Her Patience and

Self-Sacrifice

# FACTORIZATION IN NON-COMMUTATIVE DOMAINS

Hashim Tayyar

ACKNOWLEDGEMENT

The writer wishes to express his deepest appreciation and gratitude to Professor David Singmaster, whose generous donation of time, supply of books, constructive comments and guidance, made this work to appear in this complete and clear manner.

The writer wishes also to express his best thanks to Miss Mona Jabbour for the very fine work she has done in typing the manuscripts.

ABSTRACT

Factorization theory in commutative domains is well-known. In this thesis, we extend this theory to non-commutative domains. Each of the basic concepts: divisor, prime, associate, common divisor, etc., principal ideal and unique factorization must be analyzed and appropriately generalized to the non-commutative case. The concept of being associated must be extended to the much more general concept of similarity. Using this, we can extend the ideal of unique factorization and establish that a principal ideal domain is a unique factorization domain, just as in the commutative case.

In Chapter I, we discuss the concept of associated elements both from one side and two sides. We also discuss units and divisibility from both sides and we give five definitions of a prime element and discuss the conditions which make some or all equivalent.

In Chapter II, we use modules and module-homomorphisms to define similarity between two elements. We give a definition of a prime element by means of the module notion. In the end of the Chapter, we prove the uniqueness of factorization, up to similar elements and up to the order, in a domain with properties weaker than the principal ideal property.

In Chapter III, we discuss principal ideal domain, PID, which we prove to be a unique factorization domain, UFD, in the previous sense.

Chapter IV deals mainly with the Hurwitz integral domain H, and the Lifschitz integral domain L. The first one is the maximal integral domain containing the second one. The second is the set of all quaternions with integral coefficients. We shall show that H is euclidean and hence a PID, and so a UFD.

TABLE OF CONTENTS

# CHAPTER I

## BASIC CONCEPTS

In this chapter, we shall state many definitions of a prime element in an integral domain (not necessarily commutative), and prove the equivalence of four of the definitions. We shall also define the norm and the relation of two elements being associated, and analyze both concepts.

### 1. Division in an Integral Domain

**Definition 1.1:** A ring $D$ (not necessarily commutative) with an identity $1 \neq 0$ is called an integral domain (domain, cancellation ring) iff it has no zero-divisors, i.e. $ab = 0$ implies $a = 0$ or $b = 0$ for any two elements $a$ and $b$ of $D$. Thus, in an integral domain D, the non-zero elements form a semigroup (a system consisting of a set $S$ and an associative binary operation in $S$) under multiplication, which will be denoted by $D^*$.

All our work will be in integral domains.

**Definition 1.2:** By writing $a \underset{R}{|} b$, $a$ is a right divisor of $b$, we mean that $\exists$ an element $c \in D$ such that $b = ca$. Similarly, by $a \underset{L}{|} b$, $a$ is a left divisor of $b$, we mean that $b = ac$ for some element $c \in D$.

**Proposition 1.1:** $a \underset{R}{|} b,\ b \underset{R}{|} c \Rightarrow a \underset{R}{|} c.$

Similarly $a \underset{L}{|} b,\ b \underset{L}{|} c \Rightarrow a \underset{L}{|} c.$

Proof:

Since $a \underset{R}{|} b$ then $b = ra$ for some $r \in D$ and, since $b \underset{R}{|} c$ then $c = sb$ for some $s \in D$. Hence $c = s.ra = sr.a = r'a$, where $sr = r' \in D$, that is $a \underset{R}{|} c$. The second assertion is proved similarly.

(Q.E.D.)

Proposition 1.2: $a \underset{R}{|} a$ and $a \underset{L}{|} a$ for any $a \in D$, since $a = 1.a = a.1$.

Proposition 1.3: Cancellation is valid, from right and from left, in any integral domain D, i.e. $ax = bx$, $x \neq 0$, implies $a = b$, similarly for $xa = xb$.

Definition 1.3: If $a \underset{R}{|} 1$ then a is called a right unit. Similarly if $a \underset{L}{|} 1$ then a is called a left unit.

Proposition 1.4: In an integral domain, a right unit a is necessarily a left unit, and conversely. Thus we refer to right (and so left) unit just as unit.

Proof:

Let $a \underset{R}{|} 1$. Then $1 = a'a$ for some $a' \in D$. So clearly a and $a'$ are both different from zero. Now $a'a \cdot a'a = 1.1 = 1 = a'a$. Thus by cancelling a from the right of both sides and $a'$ from the left of both sides, we have $aa' = 1$; that is $a \underset{L}{|} 1$ and hence a is a left unit.

Similarly we prove the converse.

(Q.E.D.)

We will denote $a'$ by $a^{-1}$, and so we have $a.a^{-1} = a^{-1}.a = 1$ in the integral domain D, if a is a unit.

## 2. Associated Elements

**Definition 2.1:** In an integral domain D, an element $b = u\,a\,v$, where u and v are units, is called an *associate* of a and is denoted by $b \sim a$.

If $v = 1$, i.e. $b = ua$ for some unit $u \in D$, then b is called a *right associate* of a and shall be denoted by $b \overset{R}{\sim} a$.

If $u = 1$, i.e. $b = av$ for some unit $v \in D$, then b is called a *left associate* of a and shall be denoted by $b \overset{L}{\sim} a$.

**Proposition 2.1:** $a \overset{R}{|} b$ and $b \overset{R}{|} a$ iff $a \overset{R}{\sim} b$. Similarly $a \overset{L}{|} b$ and $b \overset{L}{|} a$ iff $a \overset{L}{\sim} b$.

**Proof:**

Since $a \overset{R}{|} b$, then $b = ua$ for some $u \in D$.

Since $b \overset{R}{|} a$, then $a = vb$ for some $v \in D$.

Thus $a = v.ua = vu.a$, which means that $vu = 1$ and hence u and v are units. Thus $a \overset{R}{\sim} b$. Conversely, since $a \overset{R}{\sim} b$, then $a = vb$ for some unit $v \in D$. Hence $b \overset{R}{|} a$. But since u is a unit, it has an inverse $v^{-1}$ in D. So $v^{-1}a = b$, which means that $a \overset{R}{|} b$.

The proof for the second assertion is parallel to this.

**Theorem 2.1:** The relation $\sim$ defined in Definition (2.1) is an equivalence relation. (Q.E.D.)

**Proof:**

1. $a \sim a$ for any $a \in D$ since $a = 1.a.1$.

2. If $b \sim a$ then $a \sim b$, because $b = u\,a\,v$ for some units u and v. Thus $a = u^{-1}\,bv^{-1}$, and hence $a \sim b$.

3. If $b \sim a$, $a \sim d$ then $b \sim d$, because $b = u\,a\,v$, $a = u'\,d\,v'$ where $u,v,u'$ and $v'$ are units. Thus $b = uu'dvv' = u''\,dv''$; $u''$ and $v''$ are units recalling the well-known fact, that the units in any domain form a group under multiplication. Hence $b \sim d$, and so $\sim$ is reflexive, symmetric and associative; hence it is an equivalence relation.

(Q.E.D.)

More precisely, we have

Theorem 2.2: The relations $\overset{R}{\sim}$ and $\overset{L}{\sim}$ are both equivalence relations.

Proof:

1. $a \overset{R}{\sim} a$ for any $a \in D$ since $a = 1.a$.

2. If $b \overset{R}{\sim} a$ then $a \overset{R}{\sim} b$, because $b = ua$ for some unit $u \in D$. Hence $a = u^{-1}b$, and so $a \overset{R}{\sim} b$.

3. If $b \overset{R}{\sim} a$ and $a \overset{R}{\sim} d$ then $b \overset{R}{\sim} d$, because $b = ua$ and $a = vd$ for $u,v$ units in D. Thus $b = u\,v\,d = u'\,d$ where $u'$ is a unit, and hence $b \overset{R}{\sim} d$. Therefore $\overset{R}{\sim}$ is an equivalence relation.

The proof for $\overset{L}{\sim}$ is parallel to this one.

(Q.E.D.)

Proposition 2.2: If $b \overset{R}{\sim} a$ and $b = ca$, where $b \neq 0$ and hence $a \neq 0$, then $c$ is a unit.

Also $b = ac$ and $b \overset{L}{\sim} a$ imply that $c$ is a unit, provided $b$ and hence $a$ are different from zero.

Proof:

Since $b \overset{R}{\sim} a$, then $b = ua$ for a unit $u \in D$. But $b = ca$, thus $ua = ca$ and hence $c = u$, i.e. $c$ is a unit (by the cancellation of a).

The proof for the second assertion is parallel to this. (Q.E.D.)

Remark: An element a may be a right divisor of another element b without being a left divisor of b, and conversely. Also, an element a may be a right associate of another element b without being a left associate of b, and conversely. That is

$\overset{|}{}_{R}$ and $\overset{|}{}_{L}$ are generally different.

Also

$\overset{R}{\sim}$ and $\overset{L}{\sim}$ are generally different.

To show this, take the Lipschitz integral domain, which is denoted by L, and consists of all quaternions, $a_0 + a_1 i + a_2 j + a_3 k$, where $a_i$'s are rational integers (to be discussed thoroughly in Chapter 4).

Take $a = 2+i$, $b = (2+i)(1+j-k) = 2+i+3j-k$. So

$$(2+i) \overset{|}{}_{L} (2+i+3j-k).$$

Now suppose that $(2+i) \overset{|}{}_{R} (2+i+3j-k)$, so there exists an element $d = a_0 + a_1 i + a_2 j + a_3 k$ of L such that

$$2+i+3j-k = (a_0 + a_1 i + a_2 j + a_3 k)(2+i).$$

$$2+i+3j-k = (2a_0 - a_1) + (2a_1 + a_0) i + (2a_2) j + (2a_3 - a_2) k,$$

which implies that $3 = 2a_2$, i.e. $a_2$ is half an integer, which is impossible in L. Therefore, no element d of L gives $2+i+3j-k$ such that $d(2+i) = 2+i+3j-k$, i.e.

$$(2+i) \overset{\nmid}{}_{R} (2+i+3j-k).$$

We shall see later on that $a = 2 + i$ is prime in $L$.

By a similar way one shows that

$$(2 - i) \mid_{R} (2 - i + 3j - k)$$

but

$$(2 - i) \nmid_{L} (2 - i + 3j - k).$$

To show that $\overset{R}{\sim}$ and $\overset{L}{\sim}$ are different, take any special case of Corollary ( 4.2 ) of Chapter 4, using $a = 1+i+j$ and $u = \pm i$ or $\pm j$ or $\pm k$. Thus $au \neq va$ for any unit $v \in L$.

## 3. The Norm

Definition 3.1: A norm is a function defined on a domain $D$ into the set $Z^{+}$ of non-negative integers such that:

1. $N(x) = 0$ iff $x = 0$

2. $N(ab) = N(a) \cdot N(b)$

3. $N(u) = 1$ implies that $u$ is a unit.

If a norm exists on a domain, we call the domain a normed domain (or a domain with a norm).

From the above Definition we conclude several corollaries.

Corollary 3.1.1: $N(ab) \geq N(a)$ for any $a \neq 0$, $b \neq 0$. Also $N(ab) \geq N(b)$ for any $a \neq 0$, $b \neq 0$.

Proof:

$N(ab) = N(a) \cdot N(b)$. But any one of the right factors is greater or equal to 1 since neither $a$ nor $b$ is zero (Property 1). Therefore $N(ab) \geq N(a)$, and $N(ab) \geq N(b)$.

(Q.E.D.)

Corollary 3.1.2: $N(1) = 1$.

Proof: $N(a) = N(a.1) = N(a) \cdot N(1)$ for any $a \neq 0 \in D$. Therefore $N(1) = 1$.

(Q.E.D.)

More generally, we have

Corollary 3.1.3: If $u$ is a unit, then $N(u) = 1$.

Proof:

$N(u.u^{-1}) = N(1) = 1 \geq N(u)$. But $N(u) \geq 1$ since $u \neq 0$ (because $u$ is a unit so is a divisor of 1). Therefore $N(u) = 1$.

(Q.E.D.)

From property (3) and corollary (3.1.3), we have

Corollary 3.1.4: $N(u) = 1$ iff $u$ is a unit.

Proposition 3.1: $a \underset{R}{|} b$ and $N(a) = N(b)$ imply that $a \overset{R}{\sim} b$. Similarly $a \underset{L}{|} b$ and $N(a) = N(b)$ imply that $a \overset{L}{\sim} b$.

Proof:

If $a = 0$, then $b = 0$ and the proposition follows immediately.

If $a \neq 0$, then $b = ua$ for some $u \in D$, since $a \underset{R}{|} b$. But $N(b) = N(u) \cdot N(a) = N(a)$. Thus $N(u) = 1$ (by cancelling $N(a)$ which is different from zero since $a \neq 0$). Thus $u$ is a unit (by Corollary 3.1.4). Hence $a \overset{R}{\sim} b$.

The proof for the second assertion is parallel to this.

(Q.E.D.)

Remark 1: Two associated elements have the same norm. In particular $N(-a) = N(a)$ for any $a \in D$.

That is because, if $a \sim b$, then $a = u\, b\, v$, where $u$ and $v$ are units. Then $N(a) = N(u) \cdot N(b) \cdot N(v) = 1.N(b).1 = N(b)$. The

second assertion follows since - 1 is a unit in any domain.

Remark 2: The converse of remark (1) is not necessarily true.

For the proof, take the Lipschitz integral domain $L = \{a = a_0 + a_1 i + a_2 j + a_3 k \mid a_i$ is a rational integer for all $i\}$. The norm of $a$ in $L$ is defined as $N(a) = a_0^2 + a_1^2 + a_2^2 + a_3^2$. (See the Lipschitz integral domain in Chapter 4).

Take $a = 1 + 2i + 2j - 2k$. Thus $N(a) = 1 + 4 + 4 + 4 = 13$.

Take $b = 3i + 2j$. Thus $N(b) = 9 + 4 = 13$.

However, $a \not\sim b$ because no one of the eight units of $L$, $\{\pm 1, \pm i, \pm j, \pm k\}$, changes the number of terms of an element of $L$ ($b$ has two terms while $a$ has four).

4. Definitions of a Prime

We are giving here six definitions of a prime element in an integral domain: In the following definitions $p$ represents a non-zero, non-unit in an integral domain $D$.

Definition I: $p$ is prime iff $p = \pi_1 \pi_2$ implies that $\pi_1$ or $\pi_2$ is a unit.

Definition II R: $p$ is prime iff $p \underset{R}{|} ab$ implies that $p \underset{R}{|} a$ or $p \underset{R}{|} b$.

Definition II L: $p$ is prime iff $p \underset{L}{|} ab$ implies that $p \underset{L}{|} a$ or $p \underset{L}{|} b$.

Definition III: $p$ is prime iff $p = ab$ implies that $a$ is a left associate of $p$ or $b$ is a right associate of $p$.

Definition IV R: p is prime iff $c \underset{R}{|} p$ implies that c is a unit or a right associate of p.

Definition IV L: p is prime iff $c \underset{L}{|} p$ implies that c is a unit or a left associate of p.

Now let us first prove

Theorem 4.1: In any domain D, the four definition I, III, IVR and IV L are equivalent.

Proof:

I $\Rightarrow$ III : Assume I and let $p = ab$. Then a or b is a unit. If a is a unit, then b is a right associate of p (by Definition 2.1 of right associate). If b is the unit, then a is a left associate of p (by Definition 2.1 of left associate), and so Definition III follows.

III $\Rightarrow$ IV R : Assume III and let $c \underset{R}{|} p$, so $p = dc$ for some $d \neq 0 \in D$. Therefore, by Definition III, c is a right associate of p or d is a left associate of p. If c is a right associate of p then we are finished. If d is a left associate of p then c is a unit (Proposition 2.2) and so Definition IV R follows.

IV R $\Rightarrow$ IV L : Assume IV R and let $c \underset{L}{|} p$, so $p = cd$ for some $d \neq 0 \in D$ and so $d \underset{R}{|} p$. Therefore, by Definition IV R, d is a unit or a right associate of p. If d is a unit then p is a left associate of c, and hence, by symmetry, c is a left associate of p. If d is a right associate of p then c is a unit (by Proposition 2.2).

IV L $\Rightarrow$ I : Assume IV L and let $p = \pi_1 . \pi_2$ . Therefore, $\pi_1 \underset{L}{|} p$, and so $\pi_1$ is a unit or a left associate of p. If $\pi_1$ is a unit then we are done. If $\pi_1$ is a left associate of p then $\pi_2$ is a unit (by Proposition 2.2), and so definition I follows.

Hence, the four definitions I, III, IV R and IV L are equivalent. (Q.E.D.)

We shall always refer to Definition I whenever we speak about a prime element in a domain.

Theorem 4.2: In a normed domain D, if N(a) is a rational prime (integer), then a is prime in D.

Proof:

Let N(a) = p, where p is a rational prime. Suppose that a = bc, where neither b nor c is a unit. Then N(a) = N(b).N(c) = s.r for some positive integers s,r such that N(b)=s, N(c)=r. Now since neither b nor c is a unit, then both s and r are greater than 1 (by Corollary 3.1.4). Therefore, N(a) = p is not a rational prime, contrary to our assumption that p is a rational prime. Hence b or c is a unit, and a is prime (by Definition I of a prime element). (Q.E.D.)

Theorem 4.3: In a normed domain D, Definition II R implies Definition I of a prime element in D. The same thing is true for Definition II L.

Proof:

Assume II R and let $p = \pi_1 \pi_2$. Then $p \underset{R}{|} \pi_1 \pi_2$, because

$\pi_1 \pi_2 = 1.p.$ Therefore, $p \underset{R}{|} \pi_1$, or $p \underset{R}{|} \pi_2$ (by Definition II R). If $p \underset{R}{|} \pi_1$, then $\pi_1 = h\,p$ for some $h \neq 0 \in D$. $N(\pi_1) = N(h).N(p) \geq N(p)$. But $N(\pi_1) \leq N(p)$, since $p = \pi_1 \pi_2$. Therefore, $N(\pi_1) = N(p)$. Hence $N(\pi_2) = 1$, and so $\pi_2$ is a unit (by Corollary 3.1.4). Now if $p \underset{R}{|} \pi_2$, then by the same way we prove that $\pi_1$ is a unit. Thus $\pi_1$ or $\pi_2$ is a unit, which is the required result.

Definition II L implies Definition I similarly since $\pi_1 \pi_2 = p.1$, and so $p \underset{L}{|} \pi_1$ or $p \underset{L}{|} \pi_2$; hence $\pi_2$ or $\pi_1$ is a unit.

(Q.E.D.)

We shall see later on a case for which Definition I implies Definition II R and Definition II L.

## CHAPTER II

## NON-COMMUTATIVE UNIQUE FACTORIZATION DOMAINS

In this Chapter we generalize the notion of a commutative unique factorization domain. The generalization given here is due to P.M. Cohn,[Non-Commutative Unique Factorization Domains, Transaction-Amer. Math. Soc. Vol. 109(1963), pp. 313-331].

Cohn wrote his paper on advanced level, using many concepts without definitions. He also was not accurate in his Lemma which we shall use in the Chapter. However, we shall state all the required concepts and explanations. We shall define module and module-isomorphism. We shall also define ideals before defining the new concept of similarity which will be used in the case of non-commutative unique factorization domain.

### 1. Modules

Definition 1.1: M is an R-module if M is an additive abelian group and R is a ring such that for all $r \in R$ and for all $m \in M$, there exists a unique product $m.r \in M$, such that

1. $m(r + s) = mr + ms \quad r,s \in R;\ m,n \in M.$

2. $(m + n)r = mr + nr$

3. $m(rs) = (mr)s.$

Such a module is called a right module. Left modules are defined

similarly with multiplication from left by the elements of R.

If, moreover, there exists a multiplicative identity $1 \in R$ and $m.1 = m$ for all $m \in M$, we call M a unitary module (or unital as some people prefer to use).

From now on we deal exclusively with right modules, unless otherwise stated, and we refer to them simply as modules or R-modules. It is evident that what we say about these can be said about left modules.

Definition 1.2: Let M be an R-module. N is called a submodule of M if N is a subgroup of M closed under multiplication by elements of R(from right). Now if N is a submodule of M, then we can easily see that the factor group M/N can be turned into an R-module by defining

$$(m + N)r = mr + N.$$

Definition 1.3: It is immediate that this composition defines a module. We call this module the factor module (or difference module) of M relative to N.

Definition 1.4: If X is a subset of a module M, then the set (X), of elements of the form

$$n_1 x_1 + n_2 x_2 + \cdots\cdots + x_1 r_1 + x_2 r_2 + \cdots\cdots + x_s r_s$$

where the $n_i$'s are integers, the $r_i$'s are in R and the $x_i$'s are in X, is a submodule of M. Evidently $(X) \supseteq X$ and (X) is contained in every submodule of M that contains X. Hence we call (X) the submodule generated by X. If $(X) = M$, we say that X is a set of

generators for M. If there exists a finite set of generators for M, then we call M a finitely generated module and, if there exists a single generator then M is a cyclic module.

A simpler formula can be given in the special case of modules that are unitary. (X) can be written in the form $\sum_{\text{finite}} x_i r_i$ , where $r_i \in R$, $x_i \in X$ for all i.

Definition 1.5: Let M and M' be R-modules. A mapping $\phi$ of M into M' is called an R-homomorphism iff

1. $\phi$ is a group homomorphism of (M, +) into (M', +), that is $\phi(m_1 \pm m_2) = \phi(m_1) \pm \phi(m_2)$ for any $m_1$ and $m_2$ of M.

2. $\phi(mr) = \phi(m).r$ for all $m \in M$, $r \in R$.

The submodule $\{m \mid \phi(m) = 0\}$ is called the kernel of $\phi$, denoted by kern $\phi$.

If $\phi$ is one-to-one and onto, it is called an R-isomorphism. If $\phi$ is an isomorphism of M onto M' then M and M' are called isomorphic modules.

If $\phi$: $M \to M/N$ is defined by

$\phi(m) = m + N$, then $\phi$ is an R-module homomorphism (onto), with kern $\phi = N$.

If $\phi$: $M \to N$ is an R-module homomorphism, then $M/\text{kern } \phi \simeq \phi(M)$ as R-modules; by " $\simeq$ " we mean "isomorphic to".

## 2. Ideals: Right and Left

Definition 2.1: Take a ring R. A right ideal A of R is a subset of R such that

1. $a_1 - a_2$ is in A for any $a_1$, $a_2$ in A.

2. given any $a \in A$, any $r \in R$, then $a.r \in A$.

Similar definition is given for left ideals except that (2) now becomes

$2'$. given any $a \in A$, any $r \in R$, then $r.a \in A$.

Since every ring $R$ is an R-module, then we see easily that an ideal $A$ of $R$ is a submodule of $R$ and conversely, any submodule of $R$ is an ideal.

It is clear that the sum and the intersection of two right (left) ideals are right (left) ideals.

Definition 2.2: A right ideal $A$ is called a principal right ideal if there exists one element $a \in R$ such that $A = aR$, i.e. all the elements of $A$ are of the form $ar$ for some $r \in R$. We shall denote the principal right ideal generated by $a$ by $aR$ or $[a)$. Since all our rings are domains, and so have an identity 1, then $a \in A$.

Similar definition is given for principal left ideals exept that every element now is of the form $ra$ for some $r \in R$. We shall denote such ideals by $Ra$ or $(a]$.

$A$ is cyclic iff it is principal.

Now if $M$ is any cyclic R-module and $x$ is a generator of $M$, the correspondence between $a$ in $R$ and $xa$ in $M$ is an R-homomorphism. Thus in this case $M \simeq R/A$, where $A$ is the right ideal of elements $b$ such that $xb = 0$ (the kernel of homomorphism' which is called the annihilator or the order of $x$).

## 3. The (GCRD), (GCLD), (LCRM) and (LCLM)

Definition 3.1: An element $g$ of a domain $D$, is called a

greatest common right divisor (GCRD) of two elements b and c if g is a common right divisor of b and c (See Definition 1.2.), and, if any common right divisor of b and c is a right divisor of g.

A similar definition is given for the greatest common left divisor (GCLD).

Definition 3.2: If $b = ac$ for some $c \in D$, we call b a right multiple of a. Similarly if $b = ca$ for some $c \in D$, we call b a left multiple of a. It can be seen that b is a right multiple of a iff a is a left divisor of b.

Now if $b = ac = a'c'$ for some $c, c'$ in D, then b is called a common right multiple of a and $a'$. Similar definition is given for a common left multiple.

Definition 3.3: An element $\ell$ of D is called a least common right multiple (LCRM) of two elements b and c if $\ell$ is a common right multiple of b and c and, if any common right multiple of b and c is a right multiple of $\ell$ (or $\ell$ is a left divisor of such a common multiple).

Similar definition is given for a least common left multiple (LCLM).

Lemma 3.1: In an integral domain R, if a prime element p does not divide an element x from right (left), then the GCRD(GCLD) of x and p is 1.

Proof:

Suppose that there exists a common right divisor $d \neq 1$,

of $x$ and $p$. Then $p = cd$ for some $c \in R$. But $p$ is prime, thus $c$ or $d$ is a unit. Suppose that $c$ is a unit, then $c^{-1} p = c^{-1} cd = d$. But $x = rd$ for some $r \in R$, thus $x = r(c^{-1}p) = (rc^{-1})p$, a contradiction since $p \nmid_R x$. Therefore, $d$ should be a unit. But the GCRD of two elements is unique up to left unit factors; this can be seen directly from the definition. Thus we can agree to take the GCRD to be 1.

The proof for the left case is similar to this. (Q.E.D.)

Proposition 3.1: Let $R$ be a domain. If $aR$ and $bR$ are right ideals $\neq (0)$, then $aR \geqq bR$ iff $a \mid_L b$. Similarly, if $Ra$ and $Rb$ are left ideals $\neq (0)$, then $Ra \geqq Rb$ iff $a \mid_R b$.

Proof:

Assume $aR \geqq bR$. Then $b \in aR$, and hence $b = ax$ for some $x \in R$, i.e. $a \mid_L b$.

Conversely, if $a \mid_L b$ then $b = ax$ for some $x \in R$. Thus $br = ax.r = a(xr)$, i.e., any right multiple of $b$ is a right multiple of $a$, and hence $bR \leqq aR$.

The proof for the second assertion is similar to this. (Q.E.D.)

Proposition 3.2: $aR = bR$ iff $a \sim_L b$. Also $Ra = Rb$ iff $a \sim_R b$.

Proof:

Assume $aR = bR$. So $aR \geqq bR$ and hence $a \mid_L b$ (Proposition 3.1 above). Also $bR \geqq aR$, and hence $b \mid_L a$. Hence $a \sim_L b$ (Proposition 2.1 of Chapter 1).

Conversely, if $a \overset{L}{\sim} b$ then $a \underset{L}{|} b$ and $b \underset{L}{|} a$ (Proposition 2.1 of Chapter 1). Thus $aR \geqq bR$ and $bR \geqq aR$, which implies that $aR = bR$.

The proof for the second assertion is similar to this.

Proposition 3.3: An element m, of an integral domain D, is an (LCRM) of two elements a and b iff $aR \cap bR = mR$.

Proof:

Suppose that m is an (LCRM) of a and b. Then $mr = (as)r = ar' \in aR$ for some $s \in R$ and for any $r \in R$. Similarly $mr \in bR$, thus $mR \leqq aR \cap bR$. Also any element in $aR \cap bR$ is of the form $ar = br'$ for some r and $r'$ of R. But m is an (LCRM) of a and b, hence $aR \cap bR \leqq mR$, and hence $aR \cap bR = mR$.

Conversely, if $aR \cap bR = mR$, then $m.1 = m \in aR \cap bR$. Then m is a common right multiple of a and b. But any common right multiple of a and b is in $aR \cap bR = mR$, and so is a right multiple of m. Hence m is an (LCRM), by Definition (3.3). (Q.E.D.)

Proposition 3.4: In any domain R, if $aR + bR = dR$, then d is a (GCLD) of a and b; and d can be written in the form $d = ar + bs$ where $r,s \in D$.

Proof:

Since $aR + bR = dR$, and because R has an identity $1 \neq 0$, then $a = a.1 + b.0 = dr$ for some $r \in R$. Also $b = dr'$ for some $r' \in R$. Thus d is a common left divisor of a and b. Now suppose that $d'$ is any common left divisor of a and b. Then

$aR \leq d'R$ and $bR \leq d'R$ (by Proposition 3.1 above). Hence $aR + bR = dR \leq d'R$, and hence $d = d'r$ for some $r \in R$, i.e. $d'$ is a left divisor of $d$. So $d$ is a (GCLD) of $a$ and $b$ (by Definition 3.1).

In particular, if $aR + bR = R$, then the (GCLD) of $a$ and $b$ is a unit.

(Q.E.D.)

Remark: The converse of the above Proposition is not necessarily true even if $d$ is 1.

For the proof, take the domain $R = Z[x,y]$ of all polynomials in $x$ and $y$ over the ring of integers $Z$. R is a commutative unique factorization domain. Now the (GCLD) of $x$ and $y$ is 1. Yet $xR + yR \neq R = Z[x,y]$ since the left-hand side does not contain any polynomial of non-zero constant term. So we cannot find two elements $a,b$ of $R$ such that $ar + bs = 1$, since 1 is a non-zero constant polynomial.

Cohn assumed the equivalence of the two previous concepts in the statement of his Lemma, i.e. of 1 being a (GCLD) of two elements $a$ and $b$, and of being able to write a relation such as $ad' - bc' = 1$ for some $c'$, $d'$ in a domain $R$ (See the paper of Cohn which has been mentioned in the beginning of the Chapter). So we state below the Lemma of Cohn in its correct form, and give an amplification of his proof.

Definition 3.4: An $n \times n$ matrix over a domain $R$ is called unimodular if it is a unit in $R_n$, the ring of $n \times n$ matrices over $R$.

Lemma 3.2: [Cohn]:

Two elements $a$, $a'$ of an integral domain $R$ may be taken as the first row of a unimodular matrix over $R$ iff $a$ and $a'$ have an (LCRM), and such that there exist $c', d' \in R$ such that $ad' - a'c' = 1$.

More precisely, the conditions

(3.1) $m = ab' = a'b$, where $m$ is an (LCRM) of $a$ and $a'$,

and

(3.2) $ad' - a'c' = 1$, where $c'$ and $d'$ are in $R$,

are necessary and sufficient for the existence of $c$ and $d \in R$ such that the matrix

(3.3) $$A = \begin{bmatrix} a & a' \\ c & d \end{bmatrix}$$

is unimodular, with the inverse

(3.4) $$A' = \begin{bmatrix} d' & -b' \\ -c' & b \end{bmatrix}.$$

Proof:

Suppose that (3.1) and (3.2) hold. Then by (3.2), $ad'a - a'c'a = a$, i.e. $a(d'a - 1) = a'c'a$, hence there exists $c \in R$ such that

(3.5) $d'a - 1 = b'c$, $\quad c'a = bc$.

That is because $m$ is an (LCRM) of $a$ and $a'$, thus the common right multiple of $a$ and $a'$, namely $a(d'a - 1) = a'c'a$, should be a right multiple of $m = ab'$. Thus $\exists\ c \in R$ such that

$a(d'a - 1) = ab'c$, and so (3.5). Also since $m = a'b$ then $a'.c'a = a'b.c$ which implies that $c'a = bc$ ($a' \neq 0$, because otherwise, $b' = 0$, and $a$ is a unit, and the problem is trivial since $c = c' = b' = 0$ and $d = a$, $d' = b = a^{-1}$ will do the job).

Similarly, $ad'a' - a'c'a' = a'$, i.e. $ad'a' = a'(c'a' + 1)$, which gives

(3.6) $\qquad d'a' = b'd,\ c'a' + 1 = bd$ for some $d \in R$,

because $ad'a' = a'(c'a' + 1)$ is a common right multiple of $a$ and $a'$, hence is a right multiple of $m = ab' = a'b$. So $\exists\ d \in R$ such that $ad'a' = md = ab'd$ and $a'(c'a' + 1) = md = a'bd$.

Now if we define $A, A'$ as in (3.3) and (3.4), then (3.5) and (3.6) just state that $A'A = I$

$$\text{because } A'A = \begin{bmatrix} d' & -b' \\ -c' & b \end{bmatrix} \cdot \begin{bmatrix} a & a' \\ c & d \end{bmatrix}$$

$$= \begin{bmatrix} d'a - b'c & d'a' - b'd \\ -c'a + bc & -c'a' + bd \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = I.$$

Hence $A'A.A' = A'$, and $AA' = I$ if $A'$ is not a left zero-divisor (because then $A'(AA' - I) = 0$ and hence $AA' = I$ since $A'$ is not a left zero-divisor). Thus, suppose that

$$A' \cdot \begin{bmatrix} x & x_1 \\ y & y_1 \end{bmatrix} = 0$$

$$\text{So } \begin{bmatrix} d'x - b'y & d'x_1 - b'y_1 \\ -c'x + by & -c'x_1 + by_1 \end{bmatrix} = 0\ ,$$

and so $d'x = b'y$, $c'x = by$, $d'x_1 = b'y_1$ and $c'x_1 = by_1$. We shall prove that the first two equalities are impossible, and certainly this is equivalent to the impossibility of the remaining two.

Now, by (3.2) we have

$x = 1.x = ad'x - a'c'x = ab'y - a'by = 0$, hence $x = 0$ and $by = b'y = 0$. Suppose that $y \neq 0$, then $b = b' = 0$ and hence, by (3.5 - 3.6), $d'a = 1$, $c'b' = -1$. It follows that $ad' = 1$, $a'c' = -1$, and so $ad' - a'c' = 2$, which contradicts (3.2). Hence $y = 0$ and so $A'$ is not a left zero-divisor. So $A'$ is an inverse of A.

Conversely, if A, given by (3.3), is unimodular with inverse $A'$ given by (3.4), then

$$AA' = \begin{bmatrix} a & a' \\ c & d \end{bmatrix} \cdot \begin{bmatrix} d' & -b' \\ -c' & b \end{bmatrix} = \begin{bmatrix} ad' - a'c' & a'b - ab' \\ cd' - dc' & db - cb' \end{bmatrix}$$

$$= \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} .$$

Hence $ad' - a'c' = 1$, and $ab' = a'b$. Now let $ab' = m$ and let $n \in aR \cap a'R$, say $n = ab_1 = a'a_1$. Put $da_1 - cb_1 = k$, then

$$A \cdot \begin{bmatrix} -b_1 \\ a_1 \end{bmatrix} = \begin{bmatrix} a'a_1 - ab_1 \\ da_1 - cb_1 \end{bmatrix} = \begin{bmatrix} 0 \\ k \end{bmatrix} \quad , \text{ hence}$$

$$\begin{bmatrix} -b_1 \\ a_1 \end{bmatrix} = A' \begin{bmatrix} 0 \\ k \end{bmatrix} = \begin{bmatrix} -b'k \\ bk \end{bmatrix} \quad ,$$

which shows that $n = mk$ (because $b_1 = b'k$, hence $n = ab_1 = ab'k = mk$

or $a_1 = bk$ which implies that $n = a'a_1 = a'bk = mk$), which means that m is an (LCRM) of a and a'.

(Q.E.D.)

Lemma 3.3: Any element similar to zero is, itself, zero.

Proof:

Suppose a is right similar to 0.

Thus $R/aR \simeq R/(0) = R$ as right R - module.

Thus $1 + aR \rightarrow C$ for some $c \in R$.

Now if $c = 0$, then $1 + aR = aR$, and hence $R/aR = (0)$ which is never isomorphic to the domain R(R has at least two elements 0,1). So $c \neq 0$. Now $a + aR = aR \rightarrow ca + (0) = ca$, hence $ca = 0$, and thus $a = 0$ since $c \neq 0$.

Similarly, we prove the Lemma for left similarity.

Lemma 3.4: An element a of the domain R is a unit iff $R/aR$ is the zero-module, and an element b is similar to a iff b is a unit.

Proof:

The first assertion is obvious since then $aR = R$.

If b is a unit then $R/bR$ is the zero-module, and hence is isomorphic to the zero-module $R/aR$.

Conversely, b is similar to the unit a implies that $R/bR = (0)$, and hence $bR = R$, which is true only if b is a unit.

(Q.E.D.)

Jacobson proved the following Proposition for principal ideal domains [See Jacobson, Theory of Ring pp. 33]. Cohn reproduced the same proof for any domain without explanations.

He, moreover, should have excluded the case of a or b being a unit [See the Proposition below], because if a = u, a unit, then a is similar to any non-zero element b since, by taking $d' = u^{-1}$, $a' = b' = 0$, then both (3.7) and (3.8) below are satisfied. However, as we have seen in Lemma 3.4, b should be a unit so as to be similar to a. Therefore, we state the Proposition in its corrected following way, and we give all the required explanations.

Proposition 3.5 Jacobson-Cohn : Two non-zero, non-unit elements a,b in an integral domain R are right similar iff $\exists$ $a'$, $b'$, $c'$, $d' \in R$ such that

(3.7) $$ad' - a'c' = 1$$

and

(3.8) $ab' = a'b$ is an (LCRM) of a and $a'$.

Proof:

Assume that $R/bR \simeq R/aR$ and in the isomorphism, let

(3.9) $$1 + bR \longrightarrow a' + aR.$$

Thus $(1 + bR)c$ corresponds to $(a' + aR)c$ for any $c \in R$. Since $0 \rightarrow 0$ in any R-isomorphism, $(1 + bR)b = b + bR = bR \rightarrow (a' + aR)b = a'b + aR = aR$. Hence $a'b \in aR$ and we have

(3.10) $a'b = ab'$ for some $b' \in R$.

Moreover,

(3.11) $a'a_1 = ab_1$ implies $a_1 \in bR$,

because $a_1 + bR \rightarrow a'a_1 + aR = aR$ since $a'a_1 = ab_1$ and hence is in aR; therefore $a_1 + bR = bR$ which implies that $a_1 \in bR$. From this we conclude that $a'b$ is an (LCRM) of a and $a'$ (because any common right multiple of a and $a'$ as $ab_1 = a'a_1$ is a right multiple of $a'b$ since $a_1 \in bR$). So (3.8) has been rstablished. Further, $a' + aR$ generates $R/aR$ since its corresponding coset $1 + bR$ generates $R/bR$. So $\exists\, c', d' \in R$ such that $ad' - a'c^- = 1$, which is the required equation (3.7).

Conversely, if (3.7) and (3.8) hold, then let $\emptyset: R/bR \longrightarrow R/aR$ be defined by $\emptyset(r + bR) = a'r + aR$ for any $r \in R$.

Suppose that $r_1 + bR = r_2 + bR$, then $r_1 - r_2 = b\,s \in bR$. Hence $a'(r_1 - r_2) = a'bs = ab's$ (by 3.8), and so is in aR. Hence $a'r_1 + aR = a'r_2 + aR$, and so $\emptyset$ is well-defined. The mapping $\emptyset$ is an R-homomorphism, because $\emptyset(r_1 + bR \pm (r_2 + bR))$ $= \emptyset(r_1 \pm r_2 + bR) = a'(r_1 \pm r_2) + aR = a'r_1 + aR \pm (a'r_2 + aR)$ $= \emptyset(r_1 + bR) \pm \emptyset(r_2 + bR)$; also $\emptyset((r_1 + bR))r_2) = \emptyset(r_1r_2 + bR)$ $= a'r_1r_2 + aR = (a'r_1 + aR)r_2$. The homomorphism $\emptyset$ is onto since by (3.7), $1 + aR = a'(-c') + ad' + aR = a'(-c) + aR$. Thus any element $r + aR$ of $R/aR$ is equal to $a'(-c'r) + aR$ which is an image of $-c'r + bR \in R/bR$. Finally, the homomorphism is one-to-one as it is shown below.

Let $a'r_1 + aR = a'r_2 + aR$. Then $a'r_1 - a'r_2$ $= a'(r_1 - r_2) \in aR$, i.e. $a'(r_1 - r_2) = ab_1$ for some $b_1 \in R$. But $a'(r_1 - r_2) = ab_1 = a'br$ for some $r \in R$, since $a'b = ab'$

is an (LCRM) of $a$ and $a'$ (by 3.8). Now $a' \neq 0$, because otherwise, $ad = 1$ which means that $a$ is a unit contrary to our assumption.

Hence, by cancelling $a'$ from both sides of the equality $a'(r_1 - r_2) = a' b r$, we have $r_1 - r_2 = br \in bR$. Hence $r_1 + bR = r_2 + bR$, which is the required condition for $\emptyset$ to be one-to-one. Hence $\emptyset$ is an isomorphism, and so $a$ is similar to $b$. (Q.E.D.)

Before stating Fitting's result of the equivalence of left and right similarity, let us state the following Lemma which is analogous to Cohn's Lemma (3.2) and has an analogous proof. However, we shall state it and its proof for completeness, and for the benefit of those studying matrices. We shall need it in proving Fitting's result completely.

Lemma 3.5: Two elements $a, a_1'$ of an integral domain $R$ may be taken as the first column of a unimodular matrix over $R$ iff $a$ and $a_1'$ have an (LCLM), and such that there exist $c_1', d_1' \in R$ such that $c_1' a_1' - d_1' a = 1$.

More precisely, the conditions

(3.12) $$m = b a_1' = b_1' a$$

where $m$ is an (LCLM) of $a$ and $a_1'$, and

(3.13) $$c_1' a_1' - d_1' a = 1,$$

where $c_1'$ and $d_1'$ are in $R$, are necessary and sufficient for the existence of $c_1$ and $d_1 \in R$ such that the matrix

(3.14) $$A_1 = \begin{bmatrix} a & c_1 \\ a_1' & d_1 \end{bmatrix}$$

is unimodular, with the inverse

(3.15) $$A_1' = \begin{bmatrix} -d_1' & c_1' \\ b_1' & -b \end{bmatrix} .$$

Proof:

Suppose that (3.12) and (3.13) hold. Then by (3.13), $ac_1'a_1' - ad_1'a = a$, i.e., $(ad_1' + 1)a = ac_1'a_1'$ which is a common left multiple of $a$ and $a_1'$. Hence $\exists\, c_1 \in R$ such that

(3.16) $$ad_1' + 1 = c_1b_1', \quad ac_1' = c_1b.$$

Similarly, $a_1'c_1'a_1' - a_1'd_1'a = a_1'$, i.e., $(a_1'c_1' - 1)a_1' = a_1'd_1'a$, which gives

(3.17) $$a_1'c_1' - 1 = d_1b, \quad a_1'd_1' = d_1b_1'$$

for some $d_1 \in R$. Now if we define $A$, $A'$ as in (3.14) and (3.15), then (3.16) and (3.17) just state that

$$A_1A_1' = \begin{bmatrix} a & c_1 \\ a_1' & d_1 \end{bmatrix} \cdot \begin{bmatrix} -d_1' & c_1' \\ b_1' & -b \end{bmatrix}$$

$$= \begin{bmatrix} -ad_1' + c_1b_1' & ac_1' - c_1b \\ -a_1'd_1' + d_1b_1' & a_1'c_1' - d_1b \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = I.$$

Hence $A_1' A_1 A_1' = A_1'$ and $A_1' A_1 = I$ if $A_1'$ is not a right zero-divisor. Thus, suppose that

$$\begin{bmatrix} x & y \\ x_1 & y_1 \end{bmatrix} \cdot \begin{bmatrix} -d_1' & c_1' \\ b_1' & -b_1 \end{bmatrix} = 0,$$

so

$$\begin{bmatrix} -xd_1' + yb_1' & xc_1' - yb \\ -x_1 d_1' + y_1 b_1' & x_1 c_1' - y_1 b \end{bmatrix} = 0,$$

and so $xd_1' = yb_1'$, $xc_1' = yb$, $x_1 d_1' = y_1 b_1'$ and $x_1 c_1' = y_1 b$. We shall prove that the first two equalities are impossible, which is equivalent to the impossibility of the remaining two.

By (3.13), we have

$$x = xc_1' a_1' - xd_1' a = yba_1' - yb_1' a = 0, \quad \text{hence } x = 0$$

and thus $yb = yb_1' = 0$. Now if $y \neq 0$, then $b_1' = b = 0$ and hence, by (3.16) - 3.17), $ad_1' = -1$, $a_1' c_1' = 1$. It follows that $d_1' a = -1$ and $c_1' a_1' = 1$ and so, $c_1' a_1' - d_1' a = 2$, contrary to (3.13). Hence $y = 0$ and so $A_1'$ is not a right zero-divisor.

Conversely, if $A_1$, given by (3.14), is unimodular with inverse $A_1'$ given by (3.15), then

$$A_1' A_1 = \begin{bmatrix} -d_1' & c_1' \\ b_1' & -b \end{bmatrix} \cdot \begin{bmatrix} a & c_1 \\ a_1' & d_1 \end{bmatrix}$$

$$= \begin{bmatrix} -d_1' a + c_1' a_1' & -d_1' c_1 + c_1' d_1 \\ b_1' a - b a_1' & b_1' c_1 - b d_1 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}.$$

Hence $c_1' a_1' - d_1' a = 1$ (which is the required 3.13), and $ba_1' = b_1' a$. Now let $ba_1' = b_1' a = m$ and let $n \in Ra \cap Ra_1'$, say $n = b_1 a_1' = a_1 a$. Put $a_1 c_1 - b_1 d_1 = k$, then

$$\begin{bmatrix} a_1 & -b_1 \end{bmatrix} \begin{bmatrix} a & c_1 \\ a_1' & d_1 \end{bmatrix} = \begin{bmatrix} a_1 a - b_1 a_1' & a_1 c_1 - b_1 d_1 \end{bmatrix}$$

$$= \begin{bmatrix} 0 & k \end{bmatrix}, \text{ hence}$$

$$\begin{bmatrix} a_1 & -b_1 \end{bmatrix} = \begin{bmatrix} 0 & k \end{bmatrix} \cdot A' = \begin{bmatrix} 0 & k \end{bmatrix} \begin{bmatrix} -d_1' & c_1' \\ b_1' & -b \end{bmatrix} = \begin{bmatrix} kb_1' - kb \end{bmatrix},$$

which shows that $n = km$ since $a_1 = kb_1'$, which means that $m = b_1' a = ba_1'$ is an (LCLM) of $a$ and $a_1'$.

(Q.E.D.)

Now we state a proposition which is analogous to Proposition (3.5). We shall omit the proof since it is directly parallel to the proof of Proposition (3.5).

Proposition 3.6: Two non-zero, non-unit elements $a,b$ of an integral domain $R$ are left similar iff $\exists\ a_1', b_1', c_1', d_1' \in R$ such that

(3.18) $$c_1' a_1' - d_1' a = 1$$

and,

(3.19) $$b a_1' = b_1' a$$

is an (LCLM) of $a$ and $a'$.

We can now prove Fitting's Corollary completely. Actually, Fitting's Corollary follows from a more general result of his [Über den Zusammenhang zwischen dem Begrieff der Gleichartigkeit

zweier Ideals und dem Äquivalenzbegriff der Elementarteilertheorie, Math. Ann. 112(1936), 572-582 ]. However, Cohn proved it very briefly by using his Lemma (3.2) and Proposition (3.5). [ See Cohn's paper pages (316-317) ].

Corollary (3.5.1) [FITTING]: Two elements a,b in an integral domain R are right similar iff they are left similar.

Proof:

This is trivial if one of the elements (and hence the other) is zero or a unit [See Lemmas (3.3) and (3.4)]. Now suppose that both a and b are non-zero, non-unit, elements. Hence, by combining Lemma (3.2) and Proposition (3.5), we see that a and b are right similar iff $\exists$ a', c, d, b', c', d' such that the matrices A, $A^{*}$ given by (3.3) and (3.4) are mutually inverse. Also, by combining Lemma (3.5) and Proposition (3.6), we see that a and b are left similar iff $\exists$ $a_1'$, $c_1$, $d_1$, $b_1'$, $c_1'$, $d_1'$ such that the matrices $A_1$, $A_1'$ given by (3.14) and (3.15) are mutually inverse. But the existence of the first six elements in R with the first condition mentioned above is equivalent to the existence of the second six elements under their corresponding condition; we take

$$a_1' = -c,\ c_1 = a',\ d_1 = -d,\ b_1' = -c',\ c_1' = b',\ d_1' = -d'.$$

Hence the Corollary follows.

(Q.E.D.)

As we shall be dealing exclusively with integral domains, we may omit the reference to left or right and simply speak of similar elements.

Corollary 3.5.2: An element of an integral domain is similar to any of its associates.

Proof:

Let $a \sim b$, then $b = u\,a\,v$, where $u$ and $v$ are units. Thus $a$ is an (LCRM) of $a$ and $u^{-1}$ and so $a.v = u^{-1} \cdot u\,a\,v = u^{-1}b$ is also an (LCRM) of $a$ and $u^{-1}$ (Apply the definition to see that the (LCRM) of two elements, of a domain, is unique up to unit right factor). Hence, to apply the two conditions (3.7) and (3.8) mentioned in Proposition (3.5), we take $a' = u^{-1}$. Also we take $c' = -u$ and $d' = 0$. Hence equation (3.7) is satisfied and hence $a$ and $b$ are right (and thus left) similar.

(Q.E.D.)

Definition 3.5: An R-module is called strictly cyclic if it has one generator and one defining relation (which is not redundant).

Proposition 3.7: A strictly cyclic R-module (with $R$ an integral domain) is one of the form $R/aR$, $a$ is a non-zero, non-unit element of $R$.

Proof:

Let $\bar{R}$ be a strictly cyclic R-module. Then $\bar{R} = mR$ for some $m \neq 0$, and with the defining relation $ma = 0$, $a \neq 0$. Define the R-homomorphism

$$\phi : \bar{R} = mR \longrightarrow R/aR$$

by the relation

$$\phi(mr) = r + aR \quad \text{for any} \quad r \in R.$$

Now, if $mr_1 = mr_2$, then $m(r_1 - r_2) = 0$, and $r_1 - r_2 \in aR$, since

otherwise we have another defining relation. Hence $r_1 + aR = \phi(mr_1) = r_2 + aR = \phi(mr_2)$. So $\phi$ is well-defined. It can be seen directly that $\phi$ is an R-homomorphism onto. Now if $r_1 + aR = r_2 + aR$, then $r_1 - r_2 = a\,r \in aR$, and hence $m(r_1 - r_2) = m\,a\,r = 0$ since $ma = 0$. Hence $mr_1 = mr_2$, and so $\phi$ is an R-isomorphism. Hence $\bar{R}$ is of the form $R/aR$. Now $a \neq 0$, since otherwise $\bar{R} = R$, which has no defining relation. Also, if a is a unit, then $\bar{R} = (0)$, which has no non-redundant defining relation.

Conversely, if $\bar{R}$ is of the form $R/aR$, where a is a non-zero, non-unit, element of R, then it is cyclic since it is generated by $1 + aR$. Moreover, it has exactly one non-redundant defining relation, namely, $(1 + aR)a = aR = (0)$.

Lemma 3.6: If $R > S > \{0\}$, where by $>$ we mean strictly greater, and if $R/S$ is strictly cyclic, then S is of the form bR, where b is a non-zero, non-unit of R.

Proof:

Since $R/S$ is strictly cyclic, then it has a unique defining relation, say, $(1 + S)b = S$. Hence bR is contained in the annihilator of $R/S$.

If $\phi: R \to R/S$ is the canonical homomorphism defined by $\phi(r) = r + S = (1 + S)r$ for all $r \in R$, then Kern $\phi = S$ = annihilator of $R/S \geq bR$. If $\exists\, x \in S \sim bR$, then $(1 + S)x = S$ is a non-redundant second defining relation. So $S = bR$ where $b \neq 0$, b is non-unit, because otherwise either $S = 0$ or $R = S$ which are both contrary to our assumption.

(Q.E.D.)

Proposition 3.8: A non-unit, non-zero, element a of an integral domain R is prime iff $\bar{R} = R/aR$ has no submodules $\bar{S}$ other than zero or itself such that $\bar{R}/\bar{S}$ is strictly cyclic.

Proof:

Suppose a is not prime. Then $a = bc \in bR$, where neither b nor c is a unit, and $R \supset bR \supset aR$. So $\bar{R} = R/aR \supset \bar{S} = bR/aR \supset \{0\}$, and we have the submodule $\bar{S}$ of $\bar{R}$ which is non-zero, and $\neq \bar{R}$ since b is not a unit. Moreover, $\bar{R}/\bar{S} \simeq R/bR$ is strictly cyclic [see Proposition 3.7]. Hence, $\bar{R}$ has no submodule $\bar{S}$ other than zero or itself such that $\bar{R}/\bar{S}$ is strictly cyclic implies a is prime.

Conversely, let $\bar{R}$ has a submodule $\bar{S} \neq 0$, such that $\bar{R}/\bar{S}$ is strictly cyclic. Then $\bar{R} = R/aR \supset \bar{S} \supset \{0\}$. Let S be the unique submodule of R, such that $S/aR = \bar{S}$. Then $R \supset S \supset aR$. Also, $\bar{R}/\bar{S} = R/aR/S/aR \simeq R/S$. Since $\bar{R}/\bar{S}$ is strictly cyclic, then $R/S$ is strictly cyclic, and $S = bR$ for some non-zero, non-unit element of R [Lemma 3.6]. Hence $bR = S \supset aR$, and $a = bc$ for some non-zero, non-unit c of R. Hence a is not prime. (Q.E.D.)

Definition 3.6: Let $a,b \in R$ and consider any factorizations of a and b

$$a = a_1 a_2 \cdots a_r,$$

$$b = b_1 b_2 \cdots b_s.$$

These factorizations are said to be isomorphic if $r = s$ and there is a permutation $\pi$ of $(1,\ldots,r)$ such that $a_i$ is similar to $b_{i'}$,

where $i^t$ is the result of $\pi$ on $i$.

Proposition 3.9: Let a,b be non-zero elements of an integral domain R, which are similar. Then any factorization of a gives rise to an isomorphic factorization of b.

Proof:

Let $a = a_1 a_2$ be any factorization into two elements of a.

Then

$$aR \leqq a_1 R \leqq R, \qquad \text{since } a_1 \underset{L}{|} a.$$

Hence,

$$0 \leqq a_1R/aR \leqq R/aR.$$

Now,

$$R/aR \simeq R/bR$$

since a and b are similar. If we denote the isomorphism by $\phi$, then $\phi$ maps $a_1R/aR$ onto a submodule $\bar{B}$, $0 \leqq \bar{B} \leqq R/bR$, which corresponds to submodule B, $bR \leqq B \leqq R$, and $\bar{B} = B/bR$.

Now

$$R/B \simeq R/bR/\bar{B} \overset{\phi}{\simeq} R/aR/a_1R/aR \simeq R/a_1R$$

which is strictly cyclic, or, if $a_1$ is a unit, is (0). Then $B = b_1R$ by Lemma 3.6, or else $B = R = 1 \cdot R$ (if $a_1$ is a unit), so we have

$$a_1R/aR \overset{\phi}{\simeq} b_1R/bR.$$

Now if $\psi : R/a_2R \to a_1R/aR$ is defined by

$$\psi(r + a_2R) = a_1r + aR$$

for all $r \in R$, then $\psi$ defines an R-isomorphism. For the proof, let $r_1 + a_2R = r_2 + a_2R$, then $r_1 - r_2 \in a_2R$. Hence $a_1(r_1 - r_2) \in aR = a_1a_2R$. Hence $a_1r_1 - a_1r_2 \in aR$, and $a_1r_1 + aR = a_1r_2 + aR$. Hence $\psi$ is well -

defined. The proof for $\Psi$ to be an R-homomorphism onto is direct. Now to prove the one-to-one property, let $a_1r_1 + aR = a_1r_2 + aR$. Then $a_1(r_1 - r_2) = ar \in aR$ for some $r \in R$. Hence $a_1(r_1 - r_2) = a_1 a_2 r$, and thus $r_1 - r_2 = a_2 r \in a_2R$. Hence $\Psi$ is an R-isomorphism.

Now, we have the following figure

$$R/a_2R \overset{\Psi}{\simeq} a_1R/aR \overset{\phi}{\simeq} b_1R/bR \overset{\Psi'}{\simeq} R/b_2R$$

where $\Psi'$ is an isomorphism similar to $\Psi$, and $b_2$ is an element of R such that $b = b_1 b_2$ since $bR \subseteq b_1R$. Hence $a_2$ is similar to $b_2$, by the isomorphism. Now, since $R/a_1R \simeq R/aR/a_1R/aR$ and $R/b_1R \simeq R/bR/b_1R/bR$, by the second isomorphic theorem, then

$$R/a_1R \simeq R/aR/a_1R/aR \overset{\phi}{\simeq} R/bR/b_1R/bR \simeq R/b_1R.$$

Hence $R/a_1R \simeq R/b_1R$, and $a_1$ is similar to $b_1$. Hence the proposition is true for two factors, and by induction it is true for any finite number of factors.

(Q.E.D.)

Now we can state Cohn's basic definition of a unique factorization domain (UFD), which is a generalization of the definition of a commutative UFD.

4. Definition of a Unique Factorization Domain

Definition 4.1: A (UFD) is an integral domain R such that every non-unit of $R^*(= R - \{0\})$ has a factorization into primes, and any two prime factorizations of a given element are isomorphic.

The first natural thing to do is to show that this definition

reduces to the three conditions of a commutative UFD given below.

Definition 4.2: A commutative UFD is a commutative domain satisfying the three conditions:

A1: Every element of R which is neither zero nor a unit is a product of primes.

A2: Any two prime factorizations of a given element have the same number of factors.

A3: The primes occurring in any factorization of x, any non-zero, non-unit of R, are completely determined by x except for their order and for multiplication by units (i.e. up to order and associates).

Theorem 4.1: A commutative integral domain R is a UFD iff it satisfies A1 - 3 in Definition 4.2.

Proof:

Suppose that R is a UFD (of Definition 4.1). A1 and A2 follow directly from the Definition. So, we need to prove that if

$$a = a_1 a_2 \dots a_r,$$

and

$$a = b_1 b_2 \dots b_r,$$

are two prime factorizations of any non-unit a of $R^*$, then $a_i \sim b_j$ for some j between 1 and r and for all i. Now $j = i'$ where $i'$ is the result of the permutation $(1,\dots,r)$ assumed in Definition (3.6), where $a_i$ is similar to $b_j$. Call $a_i = c$, $b_j = d$. So the theorem reduces to proving that

(4.1) $$R/cR \simeq R/dR$$

holds iff $c \sim d$ ($c$ and $d$ are associated).

If $c \sim d$, then $c$ is similar to $d$, and $R/cR \simeq R/dR$ (by Corollary 3.5.2)

If, conversely, $R/cR \simeq R/dR$, then $d + cR = (1 + cR)d \to (d' + dR)d$ for some $d' \in R$. But $(d' + dR)d = d'd + dR = dd' + dR = dR$. Hence $d \in cR$, and so $dR \subseteq cR$. By symmetry $cR \subseteq dR$, and hence $cR = dR$, which implies that $c \sim d$.

(Q.E.D.)

In the proof we have just proved

Corollary 4.1: In a commutative domain, two elements are similar iff they are associated.

As an example of a non-commutative UFD we mention non-commutative principal ideal domains, which will be discussed later on in Chapter III. These include in particular the ring of integral quaternions which will be discussed in Chapter IV, and the skew polynomial rings studied by Ore [Theory of non-commutative polynomials. Ann. of Math. (2) 34 (1933), 480-508].

## 5. The Refinement

Definition 5.1: Given two factorizations of the same element $a$, say

(5.1) $$a = a_1 a_2 \cdots a_r,$$

(5.2) $$a = b_1 b_2 \cdots b_s,$$

we say that (5.2) is a refinment of (5.1) if it is obtained from (5.1) by replacing each $a_i$ by some factorization of itself.

A factorization is said to proper if no factor is a unit. Now, if two factorizations of $a$ are isomorphic, then by absorbing

the units into their neighbours we obtain two proper factorizations of a which are still isomorphic (recall Lemma 3.4). Now we note that in a UFD,R, any two factorizations of an element of R have isomorphic refinements. We need only decompose each non-unit occuring in the two factorizations into primes; the refinements so obtained are then isomorphic, provided we insert an appropriate number of unit factors so as to get the same number of factors in the two factorizations.

As a converse we have.

Theorem 5.1 [Cohn]: Let R be an integral domain such that any two factorizations of an element of R have isomorphic refinements. Then any two prime factorizations of a given element of R are isomorphic, and if a is an element of R possessing a prime factorization, then any proper factorization of a has a refinement with prime factors. In particular, if every non-unit of R has at least one prime factorization, then R is a UFD.

Proof:

Let

$$a = p_1 p_2 \cdots p_r, \tag{5.1}$$

$$a = q_1 q_2 \cdots q_s, \tag{5.2}$$

be two prime factorizations of a. By hypothesis these have isomorphic refinements. But in any factorization of $p_i$ or $q_j$, all but one of the factors must be units (since it is prime). Since all units are similar among themselves, but not similar to any prime [Lemma 3.4], we may disregard them. Hence $r = s$ and

for some permutation $\pi$, $p_i$ is similar to an associate of $q_{\pi(i)}$. Now by Corollary (3.5.2), $p_i$ is similar to $q_{\pi(i)}$. Further, if $a$ has a prime factorization with $r$ factors, then no factorization of $a$ can have more than $r$ non-unit factors, from which it follows that any proper factorization of $a$ has a refinement with prime factors. The last assertion is an immediate consequence of this fact.

(Q.E.D.)

for some permutation $\pi$, $p_i$ is similar to an associate of $q_{\pi(i)}$. Now by Corollary (3.5.2), $p_i$ is similar to $q_{\pi(i)}$. Further, if a has a prime factorization with r factors, then no factorization of a can have more than r non-unit factors, from which it follows that any proper factorization of a has a refinement with prime factors. The last assertion is an immediate consequence of this fact.

(Q.E.D.)

## CHAPTER III

## NON-COMMUTATIVE PRINCIPAL IDEAL DOMAINS

In this chapter, we give the definition and basic properties of non-commutative principal ideal domains (PID). We define the prime ideal in both commutative and non-commutative PID's, and state the relation between the two definitions. In the remaining part of the chapter, we prove the uniqueness of factorization in PID's in detail. The proof relates to N. Jacobson, [The Theory of Rings, Chapter (3), Amer, Math. Soc. 1943]. However, we modify it in such a way as to let us continue with Cohn's line of the previous chapter and make use of the last theorem of the chapter. We give the required lemmas, theorems, propositions and explanations which make things complete.

### 1. Definition of a PID, and Basic Properties.

Definition 1.1: An integral domain D is called a PID if every right ideal of it is principal, and every left ideal of it is principal.

Proposition 1.1: In a PID, R, any two non-zero elements $a$ and $b$ have a (GCLD), which can be written in the form $ap+bq$, and an (LCRM), determined to within unit right factors. They, similarly, have a (GCRD), which can be written in the form $pa+qb$, and an (LCLM), determined to within unit left factors.

Proof:

Consider the ideal $aR+bR$ of elements $ax+by$, $x$ and $y$

arbitrary in R. This is the smallest ideal containing aR and bR, and is principal since R is a PID. So $aR + bR = dR$ for some $d \in R$. Then $d = ap + bq$ for some p and q of R (R has an identity 1). Now d is a (GCLD) of a and b (by Proposition (3.4) of Chapter II). Now if $d' = du$ is another (GCLD) of a and b, then $d'R = dR = aR + bR$. Hence d is determined to within unit right factor.

Now write $a = da_1$, $b = db_1$. Then $a(1 - pa_1) = a - apa_1 = da_1 - apa_1 = bqa_1$ and similarly, $b(1 - qb_1) = db_1 - bqb_1 = apb_1$. Since either p or q (or both) $\neq 0$, this proves that the intersection $aR \cap bR = mR \neq 0$. Hence m is an (LCRM) of a and b (by Proposition (3.3) of Chapter II). Also, m is determined to within unit right factor, as it has been proved for d.

The proof for (GCRD) and (LCLM) is parallel to the above one.

(Q.E.D.)

Definition 1.2: For a family $\mathcal{F}$ of ideals, we say that an ideal A of $\mathcal{F}$ is maximal in $\mathcal{F}$ if no ideal of $\mathcal{F}$ contains A properly. Thus an ideal B of $\mathcal{F}$ is not maximal only if there exists an ideal A of $\mathcal{F}$ such that $A \supsetneq B$.

It is known that in a PID, the following two equivalent conditions are satisfied (See N. Jacobson, Lectures in Abstract Algebra, Vol. 1 pp. 168-170).

C1: Ascending Chain Condition (a.c.c.): If $A_1 \subseteq A_2 \subseteq A_3 \subseteq \cdots$ is an increasing sequence of submodules, then there exists an integer N such that $A_N = A_{N+1} = \cdots$. This can also be phrased as: Every

strictly ascending chain $A_1 < A_2 < \ldots$ of left ideals of R is finite; the same is true for right ideals.

C2: Maximum Condition (M.C.): Any non-vacuous collection of submodules contains a maximal member.

Proposition 1.2 (Jacobson): Let R be a PID. Any descending chain of right (left) ideals having an intersection $\neq 0$ contains only a finite number of distinct ideals. This property is called the weak descending chain condition(wd.c.c.); actually the (d.c.c.) may be defined in a similar way to that of the (a.c.c.)

Proof: Suppose that $a_1R \geqq a_2R \geqq \ldots$ is a descending chain and that all the $a_iR$ contain a fixed element $b \neq 0$. Then $b = a_i b_i$, $a_i = a_{i-1} c_{i-1}$, $b_i$ and $c_{i-1}$ are in R. Hence $b = a_{i-1}(c_{i-1}b_i)$ $= a_{i-1} b_{i-1}$ for $b_{i-1}$ in R. It follows that $b_{i-1} = c_{i-1} b_i$ and $Rb_1 \leqq Rb_2 \leqq \ldots$ so that $Rb_N = Rb_{N+1} = \ldots$ for N sufficiently large (by the a.c.c.). Thus $c_N$, $c_{N+1}$, ... are units (See Proposition 3.2 of Chapter III). Hence $a_NR = a_{N+1}R = \ldots$ .

The proof for the left ideals is similar.

(Q.E.D.)

2. Prime Ideals

Definition 2.1: An ideal P in the domain R is called a prime ideal iff $CD \subset P$ implies $C \subset P$ or $D \subset P$ for any two ideals C, D of R. By CD we mean the ideal consisting of all finite sums $\sum c_i d_i$, for $c_i \in C$ and $d_i \in D$. Certainly, $CD \subset C \cap D$.

If R is commutative, the definition is equivalent to the element-wise definition.

Definition 2.1': An ideal P of a domain R is called a

prime ideal iff $bc \in P$ implies $b \in P$ or $c \in P$, for any two elements $b,c$ of $R$.

Proposition 2.1: In any domain $R$, the element-wise Definition (2.1)' implies Definition (2.1).

Proof:

Suppose $P$ is not prime according to Definition (2.1). Then $\exists$ two ideals $C$ and $D$ such that $CD \subset P$ but $P \not\supset C$ and $P \not\supset D$. Thus $\exists\ c \in C \sim P$, $d \in D \sim P$; by $C \sim P$, we mean simply those elements of $C$ which do not belong to $P$, and similarly for $D \sim P$. Thus $cd \in CD \subset P$. However, $c \notin P$ and $d \notin P$. Thus $P$ is not prime according to Definition (2.1)'. Hence Definition (2.1)' implies Definition (2.1).

(Q.E.D.)

Proposition 2.2: In a commutative domain $R$, Definition (2.1) implies Definition (2.1'), and hence, the two definitions are equivalent.

Proof:

If the ideal $P$ does not satisfy Definition (2.1'), then there exist $c$ and $d$ not in $P$ but with $cd \in P$. Thus, if $(c)$, is the principal ideal generated by $c$, then $(c) \not\subset P$; and $(d) \not\subset P$. However, since $cd \in P$, then $cp.dq = cd\,pq \in P$ for any $p,q$ of $R$. Thus $\sum c_i\, d_i \in P$, where $c_i = cp_i \in (c)$, $d_i = dq_i \in (d)$ for some $p_i$ and $q_i \in R$; that is $(c)(d) \subset P$. Thus $P$ is not prime according to Definition (2.1). Thus Definition (2.1) implies Definition (2.1').

Now, combining this Proposition with the previous one, we

see the equivalence of the two definitions (2.1) and (2.1') in the case of commutativity.

(Q.E.D.)

For our work in non-commutative domains, we will mean by a prime ideal one which satisfies the weaker Definition (2.1).

Lemma 2.1: Let R be any domain. If p is an irreducible element in the sense that $p \mid_R ab$ implies $p \mid_R a$ or $p \mid_R b$ (Definition IIR pp. 8), then the principal left ideal $(p]$ is prime. Similarly, if $p \mid_L ab$ implies $p \mid_L a$ or $p \mid_L b$, then $[p)$ is prime.

Proof:

Let $cd \in (p]$ ; c and d are any two elements of R. Then $cd = hp$ for some $h \in R$, and so $p \mid_R cd$. Therefore $p \mid_R c$ or $p \mid_R d$; that is $c \in (p]$ or $d \in (p]$. Hence $(p]$ is prime in the sense of Definition (2.1'). Thus $(p]$ is prime ideal (Proposition 2.1).

(Q.E.D.)

3. Factorization in PID

Definition 3.1: A module M is called simple if it is not trivial and has no submodules other than zero or itself.

Definition 3.2: Let R be a ring and let $R_1, R_2, \ldots, R_n$ be R-submodules such that $R_i$ is a submodule of $R_{i-1}$, then $R = R_0 \supseteq R_1 \supseteq R_2 \supseteq \ldots \supseteq R_n$ is called a chain from R to $R_n$. The quotients $R_{i-1} / R_i$ for all $i = 1,2,\ldots,n$ are called the quotients of the chain. If the chain is of the form $R \supset R_1 \supset R_2 \supset \ldots \supset R_n \supset 0$, where $\supset$ means strictly greater, we say that it is proper chain. And if $R_{i-1} / R_i$ has no proper submodule for all $i = 1,2,\ldots,n+1$, i.e. $R_{i-1} / R_i$ is a simple module, we call the chain a composition chain

or a composition series. We shall also say that the chain $R \supset R_1 \supset \dots \supset R_n$ has no proper refinement to mean the same thing.

Theorem 3.1: Let R be a PID. Two non-zero, non-unit elements a, b of R are right similar iff $\exists$ a', b' $\in$ R such that the GCLD of a' and a, (a', a) is 1, and the LCRM of a' and a is a', $a = ab' = a'b = m$.

Proof:

This reduces to Proposition (3.5) of Chapter (2) if we show that 1 is the GCLD of a' and a iff $\exists$ d', c' $\in$ R such that $ad' - a'c' = 1$. Now the necessity follows from Proposition (1.1). Conversely, if $ad' - a'c' = 1$, then $aR + a'R = R$ and hence $1 = (a', a)$ by Proposition 3.4 of Chapter (2).

(Q.E.D.)

Lemma 3.1: In a PID every element has a left prime factor.

Proof:

Let a be any non-zero, non-unit, of R, our domain. If a is prime, we are done. If not, $a = a_1b_1$, where $a_1, b_1$ are non-units, non-zero. If $a_1$ is a prime, we are done. If not, $a_1 = a_2b_2$. So $a = a_2b_2b_1$, and so on. This gives $aR \subset a_1R \subset a_2R \subset \dots$ by Proposition (3.1) of Chapter (2) . Since the chain must be finite (by the a.c.c.), then the factorization must cease with $a_i$ prime at some i.

(Q.E.D.)

Theorem 3.2: In a PID, every element has a prime factorization.

Proof:

Let a be any non-zero, non-unit, of R, our domain. Then $a = p_1 b_1$, $p_1$ prime (by Lemma 3.1). Also $b_1 = p_2 b_2$, $p_2$ prime. Hence $a = p_1 p_2 b_2$, and so on. If any $b_i$ is a prime, we are done. If not, we have $Rb_1 < Rb_2 < \ldots$ with no termination, which is impossible (by the a.c.c.). Hence $b_N$ is prime for some finite N, and $a = p_1 p_2 p_3 \ldots p_N b_N$, where all $p_i$ and $b_N$ are prime. (Q.E.D.)

Now to show that a PID is a UFD, we only establish the refinement property of the hypothesis of Cohn's result (Theorem (5.1) of Chapter (2)). However, before that, we rephrase Theorem (3.2) above in the language of submodules and composition series.

In view of the proof of Proposition (3.9) of Chapter (2), we have that a factorization of $a = a_1 a_2 \ldots a_n$ corresponds to a chain of R-submodules between R and aR, $R \geqq a_1 R \geqq a_1 a_2 R \geqq \ldots \geqq aR$, such that the quotients of the chain are strictly cyclic, and conversely, a sequence $R \geqq R_1 \geqq R_2 \geqq \ldots \geqq aR$ with strictly cyclic quotients gives a factorization $a = b_1 b_2 \ldots b_n$.

A prime factorization corresponds to a proper chain with strictly cyclic quotients : $Q_1 = R/a_1 R$, $Q_2 = a_1 R/a_1 a_2 R$, ..., $Q_n = a_1 a_2 \ldots a_{n-1} R/aR$, where $Q_i$ has no non-trivial submodules S such that $Q_i/S$ is strictly cyclic.

Lemma 3.2: Since we are in a PID, any chain $R \geqq R_1 \geqq R_2 \geqq \ldots \geqq R_n \geqq aR$ has strictly cyclic quotients, and the chain may be written

$$R \geqq b_1R \geqq b_2R \geqq \dots \geqq b_nR \geqq aR$$

Proof:

$R_i = b_iR$ (by the fact of PID). Since $b_iR \geqq b_{i+1}R$, then $\exists\ c_i \in R$ such that $b_{i+1} = b_ic_i$, and so $b_nc_n = a$.

$Q_1 = R/R_1 = R/b_1R$ is strictly cyclic, $Q_2 = R_1/R_2 = b_1R/b_2R$ $= b_1R/b_1c_1R \simeq R/c_1R$ ... etc. So $Q_i \simeq R/c_{i-1}R$ is strictly cyclic

(Q.E.D.)

Lemma 3.3: Let R be a PID. If Q is a cyclic R-module, then Q has no non-trivial submodules S such that Q/S is strictly cyclic iff Q has no non-trivial submodules S.

Proof:

The sufficiency is trivial. For the necessity proof, let $Q = qR$ for some $q \in Q$, and suppose $\exists$ a submodule S such that $Q > S > 0$. Take the homomorphism

$$\phi: R \longrightarrow qR = Q, \quad \text{defined by}$$

$$\phi(r) = qr \quad \text{for all } r \in R.$$

It is direct that $\phi$ is an R-homomorphism.

Now $\phi^{-1}(S)$ is a submodule $S'$ of R, which equals bR for some $b \in R$ since R is a PID. So $\phi(\phi^{-1}(S)) = S = \{qs \mid s \in S'\} = \{qbr \mid r \in R\}$ $= qbr = (qb)R$ which is cyclic. Hence $S = cR < Q = qR$, where $c = qb$. Now $Q/S = qR/cR = qR/qbR \simeq R/bR$ is strictly cyclic, contrary to assumption. Hence we are done.

(Q.E.D.)

Hence we have now for a PID, the following correspondences.

| | | |
|---|---|---|
| | factorizations | chains from R to aR |
| proper | " | proper chains " |
| prime | " | composition series " . |

Hence the existence of a prime factorization is equivalent to the existence of a composition series. We have already seen that we have a prime factorization. However, we give an alternate approach by showing the existence of a composition series.

Theorem 3.3: A ring R has a composition series if it satisfies both chain conditions.

Proof:

If $R = (0)$, we are done. If not, consider the family $\mathcal{F}$ of proper submodules of R. This has a maximal member $R_1$, by the maximum condition, which is equivalent to the a.c.c. Hence there is no submodule R' such that $R \supset R' \supset R_1$ and so $R / R_1$ is simple. Similarly $R_1$ contains a submodule $R_2$ such that $R_1 / R_2$ is simple, provided $R_1 \neq (0)$, and so on.

Now, if any $R_i$ is (0), we are done. If not, then we have $R \supset R_1 \supset R_2 \supset \cdots \supset \cdots$, contrary to the d.c.c. So some $R_i$ must be zero, and we have a composition series.

Corollary 3.3.1: Let R satisfy the (a.c.c.) and the (d.c.c.). Then for any non-zero element $a \in R$, then R/aR satisfies both chain conditions, and hence R / aR has a composition series, which gives rise to the composition series

$$R \supset R_1 \supset \cdots \supset aR.$$

Since any PID satisfies the (a.c.c.) and (w.d.c.c.), we have the following direct.

Corollary 3.3.2.: Any PID R has a composition series from R to aR for any $a \neq 0$.

We can now state the main and last theorem of the Chapter.

Theorem 3.4: Any PID is a UFD.

Proof:

Refering to Theorem (5.1) of Chapter (2), we need only to show that any two factorisations of an element of R have isomorphic refinements. But in a PID this is equivalent to asserting that the corresponding chains of R-submodules have isomorphic refinements; the previous notion is used in the usual sense of schreier [See Lang, Algebra, Chapter 4]. Now, since the corresponding chains of R-submodules do have isomorphic refinements, by the Schreier refinement theorem [op. cit], then the theorem follows.

(Q.E.D.)

We have promised in the end of Chapter (1) to give a case for which Definition I of a prime element implies Definitions IIR and IIL. We decided that this is the best place to fulfil our promise in.

## 4. Duo Rings and Ore Rings

Definition 4.1: A ring is called due if every one-sided ideal of the ring is a two-sided ideal - and hence every right ideal is a left ideal - (see Amer. Math. Monthly, Volume 74 (January 1967), pp. 95-96).

Definition 4.2: A ring is said to be an Ore domain if it

is an integral domain and any pair of non-zero right ideals and left ideals has a non-zero intersection.

We state here a Lemma by F. L. Sandomierski and V.C. Cateforis, [op. cit].

Lemma 4.1: An integral domain R, which is duo ring, is an Ore ring.

Proof:

Let I and J be left (right), hence two-sided, non-zero ideals of R. Then $0 \neq IJ \subseteq I \cap J$.

Now we state our two theorems.

Theorem 4.1: In a PID, R which is a duo ring, hence an Ore ring, pR = Rp for any prime p.

Proof:

Let p be any prime element in R.

Since R is a duo ring. Hence Rp = I, where I is a right ideal. But R is a PID, hence I = qR for some $q \in R$. Now, since Rp = qR, p = qr for some $r \in R$. Hence q or r is a unit since p is prime. If q is a unit, then Rp = R, which implies that p is a unit [Proposition 3.2 of Chapter (2)], contrary to assumption. Hence r should be a unit and qR = pR [by Proposition (3.2) of Chapter (2)]. So Rp = pR.

(Q.E.D.)

Theorem 4.2: In a PID, R which is a duo ring, Definition I of a prime element implies Definitions IIR and IIL.

Proof:

Let p be any prime element (of Definition I), and

let $p \underset{R}{|} ab$. Then $ab = hp$ for some $h \in R$. Suppose $p \underset{R}{\nmid} a$, hence the GCRD of a and p is 1(by Lemma 3.1 of Chapter (2)), and hence $\exists$ u, v $\in$ R such that $ua + vp = 1$ (by Proposition (1.1)) since R is a PID). So $uab + vpb = b$. Now, since $pR = Rp$ (by Theorem (4.2)), $pb = cp$ for some $c \in R$. Also since $uab = uhp$, hence $uhp + vcp = b$, from which we conclude that $p \underset{R}{|} b$.

The proof for Definition IIL is done similarly.

(Q.E.D.)

# CHAPTER IV

## THE QUATERNIONS

In this chapter we shall discuss the quaternions, which were invented by Sir William Rowan Hamilton. Two integral domains of the rational quaternions shall be discussed. The first is the Lifschitz integral domain which shall be designated by L. The second is the Hurwitz integral domain which shall be designated by H. We have found that not every right associate of a non-zero, non-unit, element of L is a left associate. We have studied this case and gave our theorem for the cases of right and left associates being equal. The integral domain H is a non-commutative Euclidean domain, as we shall prove, and hence is a PID, from which the uniqueness factorization follows.

### 1. Definition and Some Basic Properties

Let $F$ be a field, and let $\mathfrak{D}$ be the set of all numbers

$$\alpha = a_0 + a_1 i + a_2 j + a_3 k, \qquad a_i \in F,$$

where it is understood that the numbers i,j,k are commutative with $F$, and that all associative and distributive laws hold. Furthermore, 1,i,j,k are linearly independent with respect to $F$. The coefficients $a_0$, $a_1$, $a_2$, $a_3$ are called the coordinates of $\alpha$. Define 1 to be the unit element of multiplication and define

(1.1) $\quad i^2 = j^2 = k^2 = -1, \quad ij = -ji = k, \quad jk = -kj = i, \quad ki = -ik = j.$

Definition 1.1: With properties above, $\alpha$ is called a quaternion, and if $\mathfrak{F}$ is the field of rational numbers, $\mathfrak{D}$ is called the rational quaternions, and so on.

Definition 1.2: Define $\bar{\alpha} = 2a_0 - \alpha = a_0 - a_1 i - a_2 j - a_3 k$ to be the conjugate of $\alpha$.

It is clear that the conjugate of $\bar{\alpha}$ is $\alpha$, and that the conjugate of a sum equals the sum of the conjugates.

Now if $\beta = b_0 + b_1 i + b_2 j + b_3 k$, it follows from (1.1) that

$$\alpha\beta = (a_0b_0 - a_1b_1 - a_2b_2 - a_3b_3) + (a_0b_1 + a_1b_0 + a_2b_3 - a_3b_2)i + (a_0b_2 - a_1b_3 + a_2b_0 + a_3b_1)j + (a_0b_3 + a_1b_2 - a_2b_j + a_3b_0)k. \tag{1.2}$$

We can see by multiplication that

$$\overline{\alpha\beta} = \bar{\beta}\cdot\bar{\alpha}. \tag{1.3}$$

Definition 1.3: A biunique correspondence of a ring with itself which is an automorphism with respect to addition but such that

$$\alpha \longleftrightarrow \alpha', \quad \beta \longleftrightarrow \beta' \quad \text{imply} \quad \alpha\beta \longleftrightarrow \beta'\alpha',$$

is called an anti-automorphism.

We have so just proved

Theorem 1.1: The correspondence $\alpha \longleftrightarrow \bar{\alpha}$ is an anti-automorphism of $\mathfrak{D}$.

**Definition 1.4:** The number $\alpha\bar{\alpha} = \bar{\alpha}\alpha = a_0^2 + a_1^2 + a_2^2 + a_3^2$ is in $\mathbb{F}$, and is called the norm of $\alpha$, denoted by $N(\alpha)$. Hence we have

$$N(\alpha) = \alpha.\bar{\alpha} = \bar{\alpha}.\alpha$$

for any $\alpha \in \mathfrak{D}$.

**Theorem 1.2:** $N(\alpha\beta) = N(\alpha).N(\beta)$ for any $\alpha$, $\beta$ of $\mathfrak{D}$.

**Proof:**

Immediate, since $N(\alpha\beta) = \alpha\beta.\overline{\alpha\beta} = \alpha\beta.\bar{\beta}\bar{\alpha} = \alpha.N(\beta).\bar{\alpha}$ $= N(\alpha).N(\beta)$.

(Q.E.D.)

**Theorem 1.3:** $N(\alpha+\beta) = N(\alpha) + N(\beta) + 2(a_0b_0 + a_1b_1 + a_2b_2 + a_3b_3)$, where the $a_i$'s, $b_i$'s are the coefficients of $\alpha$ and $\beta$ respectively.

**Proof:**

$$N(\alpha+\beta) = (\alpha+\beta)(\overline{\alpha+\beta}) = (\alpha+\beta)(\bar{\alpha}+\bar{\beta}) = \alpha\bar{\alpha} + \beta\bar{\alpha} + \alpha\bar{\beta} + \beta\bar{\beta} = N(\alpha) + N(\beta) + \alpha\bar{\beta} + \beta\bar{\alpha}.$$

But $\alpha\bar{\beta} = \bar{\alpha}\bar{\beta} = \overline{\beta\bar{\alpha}}$, and so $\alpha\bar{\beta} + \beta\bar{\alpha} = 2c_0$, where

$$\alpha\bar{\beta} = c_0 + c_1i + c_2j + c_3k.$$

Now, $c_0 = a_0b_0 + a_1b_1 + a_2b_2 + a_3b_3$ [See 1.2]. Hence, the theorem follows.

(Q.E.D.)

**Corollary 1.3:** If the corresponding coordinates of $\alpha$ and $\beta$ have the same sign, i.e. sign $a_i$ = sign $b_i$ for $i = 0,1,2,3$, then

$$N(\alpha+\beta) \leq N(\alpha) + N(\beta).$$

Proof:

This follows directly, since then, $2(a_0b_0 + a_1b_1 + a_2b_2 + a_3b_3) \geq 0$.

(Q.E.D.)

Theorem 1.4: Every quaternion $\alpha$ satisfies the quadratic equation

(1.4) $$x^2 - 2a_0x + N(\alpha) = 0,$$

which is called the principal equation of $\alpha$. The conjugate $\bar{\alpha}$ satisfies the same equation.

Proof:

The equation (1.4) may be written

(1.5) $$x^2 - (\alpha + \bar{\alpha})x + \alpha.\bar{\alpha} = 0,$$

which is satisfied by $\alpha$ recalling that $\alpha\bar{\alpha} = \bar{\alpha}\alpha$.

The equation (1.5) is satisfied also by $\bar{\alpha}$.

(Q.E.D.)

Definition 1.5: The middle coefficient of equations (1.4 - 1.5) $= T(\alpha) = T(\bar{\alpha}) = \alpha + \bar{\alpha} = 2a_0$ is called the trace of $\alpha$.

Theorem 1.5: If $N(\alpha) \neq 0$, then $\alpha$ has an inverse $\alpha^{-1}$ in $\mathfrak{D}$ such that $\alpha.\alpha^{-1} = \alpha^{-1}.\alpha = 1$.

Proof:

If $N(\alpha) \neq 0$, then $\bar{\alpha}/N(\alpha)$ is such a number.

(Q.E.D.)

2. Formally Real Field

Definition 2.1: A field is called formally real if the equation

(1.6) $$x_1^2 + x_2^2 + \cdots + x_n^2 = 0$$

implies that

$$x_1 = x_2 = \cdots = x_n = 0$$

for every finite n and every set of x's in the field. Evidently, the real field and all its subfields are formally real.

Theorem 2.1: A field $\mathcal{F}$ is formally real iff -1 is not a sum of squares of elements of $\mathcal{F}$.

Proof:

Let $\mathcal{F}$ be formally real, and suppose that -1 is a sum of squres. By moving -1 to the side of squares we will have a sum of square (one of them is 1 which is a square element of $\mathcal{F}$ ) equals zero, while at least one of them is different from zero, contrary to assumption.

Conversely, suppose that -1 is not a sum of squares of $\mathcal{F}$. If $\mathcal{F}$ is formally real, then we are done, If not, then there exist non-zero elements

$$a_0, a_1, \ldots, a_n$$

such that

$$a_0^2 + a_1^2 + \cdots + a_n^2 = 0.$$

Now, $a_n^2$ has an inverse $(a_n^2)^{-1} = a_n^{-2} = (a_n^{-1})^2$ which is a square. So

$$(a_n^{-1})^2 a_0^2 + (a_n^{-1})^2 a_1^2 + \cdots + 1 = 0,$$

and hence -1 is a sum of squares, contradiction. Hence $\mathcal{F}$ is formally real.

(Q.E.D.)

Theorem 2.2: If $\mathfrak{F}$ is formally real, then the principal equation over $\mathfrak{F}$: $x^2 - 2a_0x + N(\alpha) = 0$ is either irreducible or the square of $x - a_0 = 0$.

Proof:

Suppose

$$x^2 - 2a_0x + N(\alpha) = 0$$

reduces to

$$(x - c)(x - d) = 0.$$

Then

$$c + d = 2a_0,$$

and

$$cd = a_0^2 + a_1^2 + a_2^2 + a_3^2 .$$

Hence

$$c^2 + 2cd + d^2 - 4cd = 4a_0^2 - 4(a_0^2 + a_1^2 + a_2^2 + a_3^2).$$

So

$$(c - d)^2 = -4(a_1^2 + a_2^2 + a_3^2),$$

and hence

$$(c - d)^2 + 4a_1^2 + 4a_2^2 + 4a_3^2 = 0.$$

Now, since $\mathfrak{F}$ is formally real, then $(c-d)^2 = 0$, and hence $c = d$; moreover, $a_1 = a_2 = a_3 = 0$, and hence $\alpha = a_0$. Hence the equation reduces to $(x - a_0)^2 = 0$. Hence the principal equation is either irreducible or else it is the square of $x - a_0 = 0$. (Q.E.D.)

Theorem 2.3: If $\mathfrak{D}$ is over a formally real field $\mathfrak{F}$, and if $N(\alpha) = 0$, then $\alpha = 0$.

Proof:

$$N(\alpha) = a_0^2 + a_1^2 + a_2^2 + a_3^2 = 0.$$

But $\mathfrak{F}$ is formally real. Hence $a_0 = a_1 = a_2 = a_3 = 0$, and so $\alpha = 0$. (Q.E.D.)

Corollary 2.3.1: If $\mathfrak{D}$ is over a formally real field, then every element of $\mathfrak{D}$ except 0 has an inverse.

Proof:

If $\alpha$ is any non-zero element of $\mathfrak{D}$, then $N(\alpha) \neq 0$ [by Theorem 2.3]. Hence $\alpha$ has an inverse [by Theorem 1.5]. (Q.E.D.)

Corollary 2.3.2: The rational quaternions Q form a non-commutative field (skew-field or division ring).

Proof:

Q is a ring with identity $1 \neq 0$. Moreover, every $\alpha \neq 0 \in Q$ has an inverse, since the rationals Ra form a formally real field [See Corollary 2.3.1]. Hence Q is a non-commutative field. (Q.E.D.)

3. Integral Quaternions

Definition 3.1: Let Q be the rational quaternions, that is, the set of all numbers $\alpha = a_0 + a_1 i + a_2 j + a_3 k$, where $a_i \in Ra$. A quaternion is called integral if it satisfies some equation of integral type, i.e. of the form

$$x^n + a_1 x^{n-1} + \cdots + a_0 = 0, \quad a_i \in Z,$$

the ring of integers.

Form now on whenever we speak about quaternions we mean rational quaternions.

Before proving the following Theorem, let us state the following well-known Lemmas.

Lemma 3.1: If m(x) is a polynomial of degree n with coefficients in a field F, irreducible in F and, if $\alpha$ is a root

of the equation $m(x) = 0$ and of another equation $f(x) = 0$ over F, then $m(x) \mid f(x)$.

For the proof see for example, MacDuffee, [An introduction to Abstract Algebra, (1966), pp. 91].

Lemma 3.2 Gauss' Lemma : If $f(x)$ is a polynomial with rational integral coefficients, the leading coefficient being 1, and if $f(x) = g(x).\ h(x)$, where $g(x)$ and $h(x)$ have rational coefficients, the leading coefficient being 1, then all the coefficients of $g(x)$ and $h(x)$ are rational integers.

Proof:

See the previous reference page 105.

Theorem 3.1: The quaternion $\alpha$ is integral iff both $T(\alpha)$ and $N(\alpha)$ are rational integers.

Proof:

Let $\alpha$ satisfies the equation $f(x) = 0$ of integral type. Now since $\alpha$ satisfies its principal equation (1.4), hence $\alpha$ satisfies an irreducible equation $m(x) = 0$ which is either linear or quadratic [Theorem (2.2)]. Hence, by Lemma (3.1), $m(x) \mid f(x)$. But, by Lemma (3.2), if $f(x)$ factors, then the factors can be so chosen as to be of integral type. Hence $m(x)$ is of integral type. Now if $\alpha$ is not rational, then $m(x) = 0$ is the principal equation of $\alpha$. If $\alpha$ is rational, $[m(x)]^2 = 0$ is the principal equation. In either case, both $T(\alpha)$ and $N(\alpha)$ are rational integers.

If, conversely, both $T(\alpha)$ and $N(\alpha)$ are rational integers, then $\alpha$ satisfies an equation, namely, its principal equation [See Theorem (1.4)], which is of integral type. Hence $\alpha$ is

integral [by Definition (3.1)] .

(Q.E.D.)

Definition 3.2: An integral domain of Q, the rational quaternions, is a set of integral numbers of Q which is a ring with unit element, and which contains four linearly independent numbers. This last restriction is to exclude integral domains such as $\{a + bi\}$ where a and b are rational integers, which are properly integral domains of a subalgebra of Q.

The set of all integral numbers of an algebraic field forms an integral domain. Unfortunately, the set of all integral quaternions is not an integral domain. To show that the set of all integral quaternions is not closed we mention .

Example:

Let $\alpha = i$, which is integral since it satisfies the equation $x^2 + 1 = 0$.

Let $\beta = \frac{3}{5} i + \frac{4}{5} j$ which is also integral since it satisfies the same equation.

However, $\alpha + \beta = \frac{8}{5} i + \frac{4}{5} j$ is not an integral quaternion since $N(\alpha + \beta) = \frac{16}{5}$ which is not a rational integer [see Theorem(3.1)].

Two particular integral domains of quaternions have received much attention and are of interest, therefore, to us. The first is the Lifschitz integral domain, which shall be denoted by L, and which consists of all quaternions

$$\alpha = a_0 + a_1 i + a_2 j + a_3 k,$$

where the $a_i$'s range over all rational integers.

It is evident that $T(\alpha)$ and $N(\alpha)$ are rational integers, so that every number of this set is integral. It is also clear that the set is closed under addition, subtraction and multiplication. So that it forms a ring. Since L contains 1,i,j and k, it is of dimension 4. Hence L is an integral domain of Q [See Definition 3.2].

The second integral domain is the Hurwitz integral domain which shall be discussed after the first one.

4. The Lifschitz Integral Domain

Theorem 4.1: If $\alpha$ is an element of L, then $N(\alpha)$ defined in Definition (1.4) satisfies Definition (3.1) of Chapter (1) of the norm.

Proof:

$N(\alpha) = a_0^2 + a_1^2 + a_2^2 + a_3^2$ is a non-negative integer since all a's are rational integers. Also, since $\alpha$ is a rational quaternion, hence $N(\alpha) = 0$ iff $\alpha = 0$ [See Theorem (2.3)]. Moreover, $N(\alpha\beta) = N(\alpha).N(\beta)$ for any $\alpha, \beta \in \mathcal{L}$ [by Theorem (1.2)]. Finally, if $u \in L$, and $N(u) = 1$, then since $N(u) = u.\bar{u} = 1$, hence $u^{-1} = \bar{u} \in \mathcal{L}$ and so u is a unit in $\mathcal{L}$. Hence $N(\alpha)$ satisfies Definition (3.1) of Chapter (1).

(Q.E.D.)

From the above Theorem, all the Corollaries (3.1.1-3.1.4), and Proposition (3.1), of Chapter (1) are satisfied for $N(\alpha)$. We shall just mention them for completeness.

Corollary 4.1.1: $N(\alpha\beta) \geq N(\alpha)$, $N(\alpha\beta) \geq N(\beta)$, for any $\alpha \neq 0$, $\beta \neq 0$ of $\mathcal{L}$.

Corollary 4.1.2: $N(u) = 1$ iff $u$ is a unit.

Corollary 4.1.3: The units of $\mathfrak{L}$ are, precisely, the eight numbers $\pm 1, \pm i, \pm j, \pm k$.

Proof:

Let $u$ be any unit of $\mathfrak{L}$. Then $N(u) = a_0^2 + a_1^2 + a_2^2 + a_3^2 = 1$. But since every $a_i$ is an integer, then the only solutions of the equation are those which make $a_i = \pm 1$, $a_j = 0$ for any $j \neq i$. That is $u = \pm 1$ or $\pm i$ or $\pm j$ or $\pm k$.

(Q.E.D.)

Corollary 4.1.4: $\alpha \underset{R}{|} \beta$ and $N(\alpha) = N(\beta)$ imply $\alpha \overset{R}{\sim} \beta$. Similarly $\alpha \underset{L}{|} \beta$ and $N(\alpha) = N(\beta)$ imply $\alpha \overset{L}{\sim} \beta$.

Corollary 4.1.5: Two associated elements have the same norm.

Also, since $\mathfrak{L}$ is a normal domain, we have the following Corollary which follows from Theorem (4.2) of Chapter (2).

Corollary 4.1.6: If $N(\alpha)$ is a rational prime (integer), then $\alpha$ is prime in $\mathfrak{L}$.

Theorem 4.2: Let $\alpha \in \mathfrak{L}$. Then there is a right associate, other than $\pm\alpha$, which is a left associate iff

1. $\alpha$ has two or fewer terms.

2. $\alpha$ has four terms such that two coordinates are equal absolutely and the remaining two are equal absolutely.

In this situation, there are at least four right associates which are left associates.

Further, every right associate is a left associate iff

1. $\alpha$ has only one term.

2. $\alpha$ has two terms with coordinates equal absolutely.

3. $\alpha$ has four terms with equal coordinates absolutely.

Proof:

If $\alpha = 0$, we are done, because every right associate in this case is a left associate.

The proof for $\alpha \neq 0$ depends on finding the eight right associates of $\alpha = a_0 + a_1 i + a_2 j + a_3 k$, $a_i \in Z$, and the eight left associates of it, then equating any one of the first eight with any one of the second eight to find the required conditions. Nevertheless, we need not to take all the 64 equations, but rather 32 equations since the eight right associates (as the left ones also) are 4 different ones, and four others different from the previous ones by the sign only. So we take the positive four left associates of $\alpha$, namely, $\alpha$, $i\alpha$, $j\alpha$ and $k\alpha$, and combine them with the eight right associates. Moreover, $\pm\alpha \neq u\alpha$ and $\pm\alpha \neq \alpha v$ unless $u = v = \pm 1$ because $\mathfrak{L}$ is an integral domain. So, we actually need to equate expressions (2 - 4) from below with expressions (5 - 10) each, which makes 18 equations only and that is the minimum number of equations that we need.

(1) ... $\alpha = a_0 + a_1 i + a_2 j + a_3 k$ (5) ... $\alpha i = a_0 i - a_1 - a_2 k + a_3 j$

(2) ... $i\alpha = a_0 i - a_1 - a_2 - a_3 j$ (6) ... $-\alpha i = -a_0 i + a_1 + a_2 k - a_3 j$

(3) ... $j\alpha = a_0 j - a_1 k - a_2 + a_3 i$ (7) ... $\alpha j = a_0 j + a_1 k - a_2 - a_3 i$

(4) ... $k\alpha = a_0 k + a_1 j - a_2 i - a_3$ (8) ... $-\alpha j = -a_0 j - a_1 k + a_2 + a_3 i$

(9) $\ldots \alpha k = a_0 k - a_1 j + a_2 i - a_3$

(10) $\ldots -\alpha k = -a_0 k + a_1 j - a_2 i + a_3.$

By equating coordinates, we see that

(1.1) $i\alpha = \alpha i \Leftrightarrow a_2 = -a_2,\ a_3 = -a_3 \Leftrightarrow \boxed{a_2 = a_3 = 0}$

(1.2) $i\alpha = -\alpha i \Leftrightarrow a_0 = -a_0,\ a_1 = -a_1 \Leftrightarrow \boxed{a_0 = a_1 = 0}$

(1.3) $i\alpha = \alpha j \Leftrightarrow \boxed{a_0 = -a_3,\ a_1 = a_2}$

(1.4) $i\alpha = -\alpha j \Leftrightarrow \boxed{a_0 = a_3,\ a_1 = -a_2}$

(1.5) $i\alpha = \alpha k \Leftrightarrow \boxed{a_0 = a_2,\ a_1 = a_3}$

(1.6) $i\alpha = -\alpha k \Leftrightarrow \boxed{a_0 = -a_2,\ a_1 = -a_3}$

(2.1) $j\alpha = \alpha i \Leftrightarrow \boxed{a_0 = a_3,\ a_1 = a_2}$

(2.2) $j\alpha = -\alpha i \Leftrightarrow \boxed{a_0 = -a_3,\ a_1 = -a_2}$

(2.3) $j\alpha = \alpha j \Leftrightarrow a_1 = -a_1,\ a_3 = -a_3 \Leftrightarrow \boxed{a_1 = a_3 = 0}$

(2.4) $j\alpha = -\alpha j \Leftrightarrow a_0 = -a_0,\ a_2 = -a_2 \Leftrightarrow \boxed{a_0 = a_2 = 0}$

(2.5) $j\alpha = \alpha k \Leftrightarrow \boxed{a_0 = -a_1,\ a_2 = a_3}$

(2.6) $j\alpha = -\alpha k \Leftrightarrow \boxed{a_0 = a_1,\ a_2 = -a_3}$

(3.1) $k\alpha = \alpha i \Leftrightarrow \boxed{a_0 = -a_2,\ a_1 = a_3}$

(3.2) $k\alpha = -\alpha i \Leftrightarrow \boxed{a_0 = a_2,\ a_1 = -a_3}$

(3.3) $k\alpha = \alpha j \Leftrightarrow \boxed{a_0 = a_1,\ a_2 = a_3}$

(3.4) $k\alpha = -\alpha j \Leftrightarrow \boxed{a_0 = -a_1,\ a_2 = -a_3}$

(3.5) $k\alpha = \alpha k \Leftrightarrow a_1 = -a_1,\ a_2 = -a_2 \Leftrightarrow \boxed{a_1 = a_2 = 0}$

(3.6) $k\alpha = -\alpha k \Leftrightarrow a_0 = -a_0,\ a_3 = -a_3 \Leftrightarrow \boxed{a_0 = a_3 = 0}$ .

It is clear that the six conditions in the small rectangles mean that $\alpha$ should be of two or less terms. The twelve big rectangles prove the second case of the first part of the theorem.

Further, if $\alpha$ has one term, it is clear that every right associate is a left associate since the rational integers $a_i$ commute with all elements (and in particular with the units) of $\mathfrak{L}$. So actually $u\alpha = \pm \alpha u$ for any $u$, a unit, and any $\alpha$, an element of $\mathfrak{L}$ of one term. If $\alpha$ has two terms with equal coefficients absolutely, then for the case of $a_2 = a_3 = 0$, $a_0 = \pm a_1$, the equations (1.1), (2.5), (2.6), (3.3) and (3.4) all are satisfied, which means that every left associate is a right associate in such a case. The same thing is true for the case of $a_0 = a_1 = 0$ and $a_2 = \pm a_3$, by taking the equations (1.2), (2.5), (2.6), (3.3) and (3.4). One can check all the cases of $a_i = a_j = 0$, $a_r = \pm a_s$, where i,j,r and s may take the values 0,1,2 and 3 such that they are different from one another.

Finally, if all $a_i \neq 0$, we must combine one equation from each group of four large rectangles, so as to have all the left associates $i\alpha$, $j\alpha$, $k\alpha$. For example, taking (1.3) determines that we must take (2.5) or (2.6). Taking (1.3) and (2.5) then

determines (3.1) and determines $\alpha = a_0 - a_0 i - a_0 j - a_0 k$. Taking (1.3) and (2.6) determines (3.2) and determines $\alpha = a_0 + a_0 i + a_0 j - a_0 k$. Similarly we get a total of eight combinations giving all possible $\alpha = a_0 \pm a_0 i \pm a_0 j \pm a_0 k$.

(Q.E.D.)

Corollary 4.2: If $\alpha$ is of three terms, then $\alpha u = v \alpha \iff u = v = \pm 1$.

Proof:

From all the eighteen above conditions, no case of having one zero coordinate has arisen.

(Q.E.D.)

## 5. The Hurwitz Integral Domain (H)

5.1. Derivation of H. Recalling Definition (3.2), we try to find a maximal integral domain which contains $\mathcal{L}$, hence H contains i, j, k, and therefore, contains $i\alpha$, $j\alpha$, $k\alpha$ for any $\alpha = a_0 + a_1 i + a_2 j + a_3 k$ of H. Now $T(\alpha) = 2a_0$, $N(\alpha) = a_0^2 + a_1^2 + a_3^2 + a_3^2$, must be rational integers [Theorem 3.1]. But $T(i\alpha) = -2a_1$, $T(j\alpha) = -2a_2$ and $T(k\alpha) = 2a_3$. Hence, the doubles of $a_0$, $a_1$, $a_2$ and $a_3$ must be rational integers. Now let $2a_i = a_i'$, and so $\alpha$ may be written

$$\alpha = \tfrac{1}{2}(a_0' + a_1' i + a_2' j + a_3' k) \tag{5.1}$$

where the a' s are rational integers. Then

$$N(\alpha) = \tfrac{1}{4}(a_0'^2 + a_1'^2 + a_2'^2 + a_3'^2). \tag{5.2}$$

Since $N(\alpha)$ should be a rational integer, we must have

$$(5.3) \qquad a_0'^2 + a_1'^2 + a_2'^2 + a_3'^2 \equiv 0 \pmod 4.$$

But every square $n^2$ is congruent to 0 or 1 module 4 according as n is even or odd. Hence, $a_0'$, $a_1'$, $a_2'$, $a_3'$ are either all even or all odd rational integers.

Definition 5.1: H is the set of all rational quaternions $\alpha = a_0 + a_1 i + a_2 j + a_3 k$, where $a_i$'s are either all integers or all halves of odd integers.

Theorem 5.1: The set H is an integral domain.

Proof:

We have shown that H consists of integral quaternions. To show that it is closed under addition and subtraction, consider

$$\alpha = \tfrac{1}{2}(a_0' + a_1' i + a_2' j + a_3' k),$$

$$\beta = \tfrac{1}{2}(b_0' + b_1' i + b_2' j + b_3' k)$$

where the a' s are all even or all odd rational integers, and likewise the b' s are. If the a' s and b' s are all even or all odd, the sums and differences, $a_i' \pm b_i'$ are all even. If the a' s are all even and the b' s are all odd, or vice versa, then $a_i' \pm b_i'$ are all odd. Hence $\alpha \pm \beta$ is in H.

To show that H is closed under multiplication, let

$$\alpha\beta = \gamma = \tfrac{1}{2}(c_0' + c_1' i + c_2' j + c_3' k).$$

From (1.2), we have

$$c_0' = \tfrac{1}{2}(a_0'b_0' - a_1'b_1' - a_2'b_2' - a_3'b_3'),$$

$$c'_1 = \tfrac{1}{2}(a'_0b'_1 + a'_1b'_0 + a'_2b'_3 - a'_3b'_2),$$

$$c'_2 = \tfrac{1}{2}(a'_0b'_2 - a'_1b'_3 + a'_2b'_0 + a'_3b'_1),$$

$$c'_3 = \tfrac{1}{2}(a'_0b'_3 + a'_1b'_2 - a'_2b'_1 + a'_3b'_0).$$

If the $a'$ s are even, or $b'$ s are even, each of the $c'$ s is an integer. If all the $a'$ s and all the $b'$ s are odd, each expression in parantheses is the sum of four odd integers, which is even, so again the $c'$ s are integers. Now $N(\gamma) = N(\alpha) \cdot N(\beta)$, so $N(\gamma)$ is a rational integer. Hence $c'^2_0 + c'^2_1 + c'^2_2 + c'^2_3 \equiv 0 \pmod 4$. So that either all the $c'$ s are even or all are odd, which shows that $\gamma \in H$.

Other conditions are direct from Q, the quotient field of H. Hence H is an integral domain in Q, and is the unique maximal integral domain which contains $\mathcal{L}$, by its derivation.

(Q.E.D.)

Theorem 5.2: If $\alpha$ is an element of H, then $N(\alpha)$ defined in Definition (1.4) satisfies Definition (3.1) of Chapter (1) of the norm.

Proof:

The same proof of Theorem 4.1 exactly.

(Q.E.D.)

As in the case of Theorem (4.1), the following corollaries are immediate.

Corollary 5.2.1: $N(\alpha\beta) \geqq N(\alpha)$, $N(\alpha\beta) \geqq N(\beta)$, for any $\alpha \neq 0$, $\beta \neq 0$, of H.

Corollary 5.2.2: $N(u) = 1$ iff u is a unit.

Corollary 5.2.3: The units of H are, precisely, the twenty four numbers $\pm 1$, $\pm i$, $\pm j$, $\pm k$, $\frac{1}{2}(\pm 1 \pm i \pm j \pm k)$.

Proof:

The first eight are from $\mathfrak{L}$ which is included in H. Moreover, if $\alpha = \frac{1}{2}(a_0' + a_1'i + a_2'j + a_3'k)$ is a unit, then $N(\alpha) = \frac{1}{4}(a_0'^2 + a_1'^2 + a_2'^2 + a_3'^2) = 1$, which is possible only in these two cases:

1. If all $a_i$'s are odd then $a_0'^2 + a_1'^2 + a_2'^2 + a_3'^2 = 4$ iff $a_i' = \pm 1$ for all i, which gives the last sixteen units.

2. If all $a_i$'s are even then $a_i' = \pm 2$ for some i while $a_j' = 0$ for all $j \neq i$. This gives the first eight.

(Q.E.D.)

Also, since H is a normed domain, we have the following Corollary which follows from Theorem (4.2) of Chapter (2).

Corollary 5.2.4: If $N(\alpha)$ is a rational prime (integer), then $\alpha$ is prime in H.

Theorem 5.3: If $\beta \neq 0$ and $\alpha$ are two numbers of H, there exist numbers k and $\rho$ in H such that

$$\alpha = k\beta + \rho \quad , N(\rho) < N(\beta).$$

There is also, by symmetry, $k'$ and $\rho'$ such that

$$\alpha = \beta k' + \rho' \quad , N(\rho') < N(\beta).$$

Proof:

$$\frac{\alpha}{\beta} = \frac{\alpha \cdot \bar{\beta}}{N(\beta)} = s + ti + uj + vk,$$

where s,t,u and v are rationals. Choose $s'$, $t'$, $u'$ and $v'$ rational

integers such that $|s - s'| \leqq \frac{1}{2}$, $|t - t'| \leqq \frac{1}{2}$, $|u - u'| \leqq \frac{1}{2}$, $|v - v'| \leqq \frac{1}{2}$. Now, there are two cases:

If at least one of the inequalities is strict i.e. $\lneqq$, take $k = s' + t'i + u'j + v'k$, and take $\rho = \alpha - k\beta$. Then $N(\rho) = N(\alpha - k\beta)$, and writing $k = \left( \frac{\alpha}{\beta} + k - \frac{\alpha}{\beta} \right)$, $N(\rho) = N(\alpha - \alpha - (k - \frac{\alpha}{\beta})\beta) = N(\frac{\alpha}{\beta} - k) \cdot N(\beta)$. But $N(\frac{\alpha}{\beta} - k) = N[(s - s') + (t - t')i + (u - u')j + (v - v')k]$ $= (s - s')^2 + (t - t')^2 + (u - u')^2 + (v - v')^2 < \frac{1}{4} + \frac{1}{4} + \frac{1}{4} + \frac{1}{4} = 1$. Hence $N(\rho) < N(\beta)$.

If, however, all the inequalities are equalities, then s,t,u and v are all halves of integers and so $\frac{\alpha \bar{\beta}}{N(\beta)}$ is an element of H. So, in this cases take $k = \frac{\alpha \bar{\beta}}{N(\beta)} = \frac{\alpha}{\beta}$, and so $\rho = 0$.

(Q.E.D.)

Theorem 5.4: There exist a euclidean algorithm for finding a GCRD (and a GCLD) of two quaternions $\alpha$, $\beta$ of H.

Proof:

This theorem follows from the previous one. If $\beta \neq 0$, $\alpha \neq 0$, then $\exists$ $k_1$, $\rho_1$ in H such that

$$\alpha = k_1 \beta + \rho_1 , \quad N(\rho_1) < N(\beta).$$

Also, if $\rho_1 \neq 0$, then $\exists$ $k_2$, $\rho_2$ in H such that

$$\beta = k_2 \rho_1 + \rho_2 , \quad N(\rho_2) < N(\rho_1).$$

If $\rho_2 \neq 0$, then $\exists$ $k_3$, $\rho_3$ in H such that

$$\rho_1 = k_3 \rho_2 + \rho_3, \quad N(\rho_3) < N(\rho_2),$$

and so on. Since the norms form a descending positive integers, they should end with $\rho_n = 0$ for some n, and we have

$$\rho_{n-2} = k_n \rho_{n-1} + \rho_n = k_n \rho_{n-1} .$$

So $\rho_{n-1}$ is a right divisor of $\rho_{n-2}$, hence is a right divisor of $\rho_{n-3} = k_{n-1} \rho_{n-2} + \rho_{n-1}$, and so on. Hence $\rho_{n-1}$ is a common right divisor of $\alpha$ and $\beta$, since it is a right divisor of $\rho_{n-1}, \rho_{n-2}, \cdots, \rho_2, \rho_1$. But since any other common right divisor of $\alpha, \beta$ is a right divisor of $\rho_1$, and hence of $\rho_2, \rho_3, \cdots, \rho_{n-1}$, then $\rho_{n-1}$ is a GCRD of $\alpha$ and $\beta$. (Q.E.D.)

Hence we have the following direct.

Corollary 5.4.1: H is a non-commutative euclidean domain.

Corollary 5.4.2: H is a PID.

Proof:

Let $A \neq (0)$ be any left ideal in H. Take the element $\alpha \neq 0 \in A$ whose norm, which will be a positive integer since $\alpha \neq 0$, is the least. So $0 < N(\alpha) \leq N(\beta)$ for any $\beta \in A$. If it is possible to have an element $\beta \in A$ which is not a left multiple of $\alpha$, then $\beta = k\alpha + \rho$, where $k, \rho \in A$ and $0 < N(\rho) < N(\alpha)$, by Theorem (5.3). But $N(\alpha) \leq N(\rho)$ by its choice, hence we get a contradiction. Hence every element in A is a left multiple of $\alpha$, and so $A = (\alpha]$. Similarly, we prove that every right ideal is a principal one. Hence H is a PID. (Q.E.D)

From the previous Chapter, we have

Corollary 5.4.3: H is a UFD.

Theorem 5.5: If $\alpha$ is of integral type (i.e. all its coordinates are rational integers) and $\beta = m$, a positive rational integer, then a necessary and sufficient condition that the GCRD of $\alpha$, $\beta$, written $(\alpha, \beta)_R$, is 1 is that $(N\alpha, N\beta) = 1$, or (what is the same thing) that $(N\alpha, m) = 1$.

Proof:

Suppose that $(\alpha, \beta)_R = 1$, then $\exists$ u, v $\in$ H such that $u\alpha + v\beta = 1$ (by Proposition (1.1) of Chapter (3) since H is a PID). Hence $N(u\alpha) = N(1 - v\beta) = (1 - v\beta)(\overline{1 - v\beta})$ $= (1 - mv)(1 - m\bar{v}) = 1 - mv - m\bar{v} + m^2N(v) = N(u) \cdot N(\alpha)$. Now since $(N\alpha, m)$ divides every term in the equation except 1, hence $(N\alpha, m) = 1$. Since $N(\beta) = m^2$, the two forms of the condition are equivalent.

Conversely, if $(N\alpha, m) = 1$, then $(\alpha, m)_R = (\alpha, \beta)_R = 1$. (Q.E.D.)

Theorem 5.6: If $\alpha \in$ H, then one at least of its associates has integral coordinates (i.e. is of integral type).

Proof:

If the coordinates of $\alpha$ are not integral, then we can choose the signs so that

$$\alpha = (b_0 + b_1 i + b_2 j + b_3 k) + \tfrac{1}{2}(\pm 1 \pm i \pm j \pm k) = \beta + \gamma,$$

say, where $b_i$ are even integers. Hence any associate of $\beta$ has integral coordinates so as to have its norm, which equals the norm of $\beta$, a multiple of four. Also $\gamma\bar{\gamma}$, which is an associate of $\gamma$ since $\bar{\gamma}$ (and $\gamma$ itself) is a unit, equals 1. Hence $\alpha\bar{\gamma}$,

which is an associate of $\alpha$ , has integral coordinates.

(Q.E.D.)

The following Lemma is known in Number Theory.

Lemma (Lagrange's Theorem): Every positive integer is the sum of four squares.

For the proof see Hardy and Wright, [An Introduction to the Theory of Numbers, Chapter XX, 1960].

As an application to this Lemma, we have

Theorem 5.7: A rational integer p cannot be a prime quaternion (by a quaternion we mean here an element of H).

Proof:

If p is zero or $\pm$ 1, it is clear, because then it is zero or a unit which is in either case not a prime.

If p is any positive integer different from 1, then $p = a_0^2 + a_1^2 + a_2^2 + a_3^2$, where not all $a_i$ are zero (by the preceding Lemma). Then $p = \alpha \cdot \bar{\alpha}$ , where $\alpha = a_0 + a_1 i + a_2 j + a_3 k$. Now $\alpha$ is not a unit, because then $p = 1$, contrary to assumption. Hence, $\bar{\alpha}$ is also not a unit, and so p is not a prime quaternion.

Now if $p = -q$, where q is positive integer $\neq 1$, then $q = \beta \cdot \bar{\beta}$ as above, where $\beta$ and $\bar{\beta}$ are non-units. Hence $p = -\beta \cdot \bar{\beta}$ or $\beta(-\bar{\beta})$, and p is not a prime quaternion.

Theorem 5.8: An element $\pi$ of H is prime iff $N(\pi)$ is a prime integer.

Proof:

If $N(\pi)$ is a prime integer, then $\pi$ is prime (by Corollary (5.2.4)).

Suppose $\pi$ is prime and $p \mid N(\pi)$, where $p$ is a rational prime integer. $(\pi, p)_R = \pi'$, a non-unit (by Theorem (5.5) since $\pi$ can be taken to be of integral type by taking any of its associates by Theorem 5.6).

Since $\pi$ is prime, $\pi'$ is an associate of $\pi$, and $N(\pi') = N(\pi)$. Also $p = \lambda\pi'$, where $\lambda \in H$, and $p^2 = N(\lambda) \cdot N(\pi') = N(\lambda) \cdot N(\pi)$, so that $N(\lambda)$ is 1 or $p$. Now, if $N(\lambda)$ were 1, $p$ would be an associate of $\pi'$ and $\pi$, and so a prime quaternion, which we have seen to be impossible. Hence $N(\pi) = p$, a rational prime.

(Q.E.D.)

Now after we have characterized the prime elements of $H$, which is a UFD as we have seen, we can proceed further than before.

We give here the following Theorem from MacDuffee[6].

Theorem 5.9: Let $\alpha \in H$ be not divisible by a rational prime, and let

$$N(\alpha) = p_1 p_2 \cdots p_n ,$$

where the rational primes $p_i$ are arranged in any fixed order. Then

$$\alpha = \pi_1 \cdot \pi_2 \cdots \pi_n , \quad N(\pi_i) = p_i$$

where the $\pi$'s are prime quaternions. Moreover $\pi$'s are unique except for unit factors.

Proof:

Let $p$ be any one of the $p_i$, and consider the ideal $(p, \alpha] = (\pi]$ for some $\pi$ (by PID property). So $p = k\pi$, $\alpha = \lambda\pi$

for $k, \lambda \in H$; and $N(p) = p^2 = N(k) \cdot N(\pi)$, so that $N(\pi) = 1$ or $p$ or $p^2$.

Now if $N(\pi) = p^2$, then $k$ is a unit and $p \mid \pi$, hence $p \mid \alpha$, contrary to assumption. If $N(\pi) = 1$, then $\pi$ is a unit and $(p, \alpha] = H$. Hence $1 = up + v\alpha$, for $u, v \in H$. Then $v\alpha = 1 - up$, so $N(v\alpha) = (1 - up)(1 - \bar{u}p) = 1 - pT(u) + p^2N(u)$. But $u \in H$, so $T(u)$ and $N(u)$ are rational integers. Hence $N(v\alpha) = N(v) \cdot N(\alpha) \equiv 1 \pmod{p}$. But this is impossible, since $N(\alpha) \equiv 0 \pmod{p}$. Thus $N(\pi) = p$.

Now take $p = p_n$, and denote a corresponding $\pi$ by $\pi_n$. Then

$$\alpha = \alpha_1 \pi_n, \quad N(\alpha_1) = p_1 p_2 \cdots p_{n-1}, \quad N(\pi_n) = p_n.$$

As before, we find a $\pi_{n-1}$ such that

$$\alpha_1 = \alpha_2 \pi_{n-1}, \quad N(\alpha_2) = p_1 p_2 \cdots p_{n-2}, \quad N(\pi_{n-1}) = p_{n-1}.$$

Continuing, we have

$$\alpha = \pi_1 \pi_2 \cdots \pi_n, \quad N(\pi_i) = p_i.$$

Now, suppose that

$$\alpha = \pi_1 \pi_2 \cdots \pi_n = t_1 t_2 \cdots t_n, \quad N(\pi_i) = N(t_i) = p_i.$$

Hence $\pi_n$ is a GCRD of $\alpha$ and $p_n$, since $(p_n, \alpha] = (\pi_n]$. Since $t_n$ is also a common right divisor of $\alpha$ and $p_n$, $t_n$ is a right divisor of $\pi_n$. Let

$$\pi_n = u_{n-1} t_n, \quad N(\pi_n) = N(u_{n-1}) \cdot N(t_n).$$

But $N(\pi_n) = N(t_n) \neq 0$ so that $N(u_{n-1}) = 1$ and $u_{n-1}$ is a unit. Then

$$t_n = \overline{u_{n-1}} \cdot \pi_n, \quad \text{where } \overline{u_{n-1}}$$

is a unit. Thus

$$\alpha_1 = \pi_1 \pi_2 \cdots \pi_{n-1} = t_1 t_2 \cdots t_{n-1} \overline{u_{n-1}}.$$

If $n > 2$, we proceed as before to show that

$$t_{n-1} \overline{u_{n-1}} = \overline{u_{n-2}} \pi_{n-1},$$

or

$$t_{n-1} = \overline{u_{n-2}} \pi_{n-1} u_{n-1}, \quad N(u_{n-1}) = 1.$$

We continue until we have

$$\alpha = \pi_1 \pi_2 \cdots \pi_n = \pi_1 u_1 \cdot \bar{u}_1 \pi_2 u_2 \cdot \cdots \cdot \bar{u}_{n-3} \pi_{n-2} u_{n-2}$$

$$\cdot \bar{u}_{n-2} \pi_{n-1} u_{n-1} \cdot \bar{u}_{n-1} \pi_n.$$

Hence the factorization is unique except for unit factors. (Q.E.D.)

It seems that is is true that in H, two prime elements are similar iff they have the same norm. Unfortunately, we had no time to work on this. However, we leave it to a paper in the future.

REFERENCES


Books

1. Hardy and Wright, An Introduction to the Theory of Numbers, Oxford Univ. Press, Oxford, 1960.

2. N. Jacobson, Lectures in Abstract Algebra, Volumes 1 and 2, Van Nostrand Company, Princeton, N.J., 1964.

3. N. Jacobson, Theory of Rings, Amer. Math. Soc., N.Y., 1943.

4. A.G. Kurosh, General Algebra, Chelsea Publishing Company, N.Y., 1963.

5. Serge Lang, Algebra, Addison-Wesley Publishing Company, Reading, Mass., 1965.

6. C. C. MacDuffee, An Introduction to Abstract Algebra, Dover Publication Inc., N.Y., 1966.

7. Zariski and Samuel, Commutative Algebra, Vol. 1, Van Nostrand Company, Princeton, N.J., 1965.

Papers

1. P. M. Cohn, Non-Commutative Unique Factorization Domains, Transactions, Amer. Math. Soc., Vol. 109 (1963), pp. 313-331.

2. F. L. Sandomierski and V. C. Cateforis, Subdirect Sums of Ore Domains, Amer. Math. Monthly, Vol. 74, January 1967, pp. 95.