1967

A Study of Unique Factorization Domains

James D. Harris
College of William & Mary - Arts & Sciences

A STUDY OF UNIQUE FACTORIZATION DOMAINS

A Thesis

Presented to

The Faculty of the Department of Mathematics

The College of William and Mary in Virginia

In Partial Fulfillment

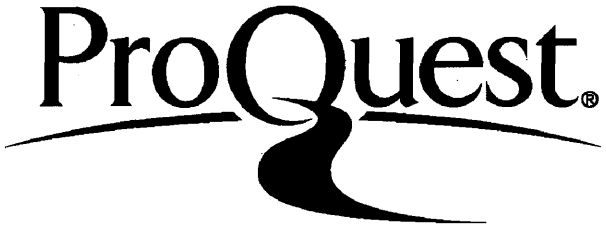
Of the Requirements for the Degree of

Master of Arts

By

James D. Harris

1967



APPROVAL SHEET

This thesis is submitted in partial fulfillment of

the requirements for the degree of

Master of Arts

James D. Harris

Author

Approved, May 1967

Thomas L. Reynolds

Thomas L. Reynolds, Ph.D.

Richard H. Prosl

R. H. Prosl, Ph.D.

George Rublein

G. T. Rublein, Ph.D.

ACKNOWLEDGMENTS

The author wishes to express his appreciation to Professor Thomas L. Reynolds for his guidance in the preparation of this work and to Professor G. T. Rublein and Professor R. H. Prosl for reading the manuscript and making several helpful suggestions.

TABLE OF CONTENTS

ABSTRACT

Theorems giving necessary and sufficient conditions under which an integral domain will be a unique factorization domain are given, and several results which follow from these theorems are proved.

A STUDY OF UNIQUE FACTORIZATION DOMAINS

INTRODUCTION

This paper presents a study of integral domains in which each element is uniquely expressible as a product of irreducible elements (unique except for unit factors and order of the elements). These integral domains are called unique factorization domains.

The reader is assumed to be reasonably familiar with the theory of rings and ideals. Such familiarity could be obtained from Introduction to Abstract Algebra, by Barnes, Modern Algebra, by Van der Waerden, or from almost any text on the subject.

Chapter I is concerned with theorems and definitions which are a necessary prerequisite for the following chapters. In chapter II, two theorems giving necessary and sufficient conditions for an integral domain to be a unique factorization domain are developed. Chapter III gives several applications of the theorems in chapter II.

CHAPTER I

PRELIMINARIES

In this paper, all rings are assumed to be commutative with unit.

To begin with, two theorems will be stated for later reference.

Definition: A ring, R, is said to satisfy the ascending chain condition for ideals if each strictly increasing sequence $A_1, A_2, \ldots$ of ideals of R has only a finite number of terms. That is, there is some n such that $A_1 \subset A_2 \subset \ldots \subset A_n$ and the sequence has no next element other than R.

Definition: A ring, R, satisfies the finite basis condition if every ideal in R has a finite basis. That is, every ideal in R is generated by a finite set of elements of R.

Definition: A ring, R, satisfies the maximal condition for ideals if in any nonempty set of ideals of R there exists an ideal maximal in the set. That is, there exists an ideal A in the set such that if B is an ideal of R and $B \supset A$ then $B = A$.

Theorem 1: In a ring, the ascending chain condition for ideals, the maximal condition for ideals and the finite basis condition are equivalent. [2, p. 113]

Definition: A partial ordering is a binary relation which is reflexive, transitive, and artisymmetric. A set on which a partial ordering, β, is defined is said to be partially ordered. Two elements are said to be comparable if $(a, b) \in \beta$ or $(b, a) \in \beta$. If $(a, b) \in \beta$, then b precedes a.

Definition: Let β be a partial ordering of the set M. Let A be a subset of M. "a" is called a minimal element of A if $x \in A$ and $(a, x) \in \beta$ implies that $x = a$. M is said to satisfy the minimum condition for elements if every nonempty subset of M has at least one minimal element.

Definition: Let β be a partial ordering of M. If every descending chain of elements of M $(a_1, a_2) \in \beta$, $(a_2, a_3) \in \beta$, . . ., $(a_n, a_{n+1}) \in \beta$, ... reaches a point where $a_n = a_{n+1} = \ldots$ then M is said to satisfy the descending chain condition for elements.

Definition: Let β be a partial ordering of M. M satisfies the inductive condition if a property E is possessed by all minimal elements of M and if from the validity of E for all elements strictly preceding some element a, we can deduce the validity of E for a, then all elements of M satisfy E.

Theorem 2: The inductive condition, the descending chain condition for elements, and the minimum condition for elements are equivalent. [3, p.23]

Definition: Two elements a, b of a ring R are said to be associates if $a = i \cdot b$ where i is a unit.

Now I wish to show that from the concept of associativity, a partial order can be found.

Theorem 3: In an integral domain, R, the relation of associativity is an equivalence relation.

Proof: Since we have assumed that R has an identity e, $a = e \cdot a$. If $a = \xi \cdot b$ where ξ is a unit, then $\xi^{-1} \cdot a = \xi^{-1} \cdot \xi \cdot b = b$. If $a = \xi_1 \cdot b$ and $b = \xi_2 \cdot c$ where ξ_1 and ξ_2 are units, then $a = \xi_1 \cdot (\xi_2 \cdot c) = (\xi_1 \cdot \xi_2) \cdot c$ and $\xi_1 \cdot \xi_2$ is a unit since $(\xi_1^{-1} \cdot \xi_2) \cdot (\xi_2^{-1} \cdot \xi_1) = e$.

Now this equivalence relation can be used to partition the integral doman R into classes of associated elements.

Let $\beta = \{(A, B) : A$ and B are classes of associated elements and an element $b \in B$ divides an element $a \in A\}$. If b divides a then $a = r \cdot b$, $r \in R$. If a' is any other element of A and b' is any other element of B, then $a = \xi_1 \cdot a'$ and $b = \xi_2 \cdot b'$ where ξ_1 and ξ_2 are units, thus $\xi_1 \cdot a' = r \cdot \xi_2 \cdot b'$ and $a' = \xi_1^{-1} \cdot \xi_2 \cdot r \cdot b'$. Therefore, if any element of A divides any element of B, then all elements of A divide all elements of B.

Theorem 4: If R is an integral domain, then β is a partial ordering of R.

Proof: $(A, A) \in \beta$ since $a = e \cdot a$, therefore β is reflexive. If $(A, B) \in \beta$ and $(B, A) \in \beta$ then if $a \in A$ and $b \in B$, $a = r \cdot b$ and $b = q \cdot a$ for some $r, q \in R$. Therefore, $a = r \cdot q \cdot a$, $e = r \cdot q$, and r and q are units which imply that $A = B$. Therefore, β is antisymmetric. If $(A, B) \in \beta$ and $(B, C) \in \beta$, then let $a \in A$, $b \in B$, and $c \in C$. There exist $r_1, r_2 \in R$ such that $a = r_1 \cdot b$, $b = r_2 \cdot c$, and $a = r_1 \cdot r_2 \cdot c$. Therefore, c divides a, which implies $(A, C) \in \beta$. Thus β is transitive.

Theorem 5: If β is defined as above in the integral domain R, then the ascending chain condition for ideals implies the descending chain condition for elements.

Proof: Suppose we have the chain $(a_1, a_2) \in \beta$, $(a_2, a_3) \in \beta$, . . . where $a_1, a_2, \ldots \in R$. Each a_i generates an ideal (a_i) and $(a_i) \subseteq (a_{i+1})$, since if $x \in (a_i)$, then $x = b \cdot a_i$ for some $b \in R$. Then $(a_i, a_{i+1}) \in \beta$ implies $a_i = c \cdot a_{i+1}$ for some $c \in R$. Therefore, $x = b \cdot c \cdot a_{i+1}$ and $x \in (a_{i+1})$. Thus we have $(a_1) \subseteq (a_2)$

$\subseteq \cdots \subseteq (a_i) \subseteq (a_{i+1}) \subseteq \cdots$ by the ascending chain condition there exists n such that $(a_n) = (a_{n+1}) = \cdots$. Now $(a_n) = (a_{n+1})$ implies $a_n \in (a_{n+1})$ and $a_{n+1} \in (a_n)$. Therefore, a_n and a_{n+1} are associates and members of the same equivalence class. Therefore, R satisfies the descending chain condition for elements.

Example: Let $R_1, R_2, \ldots, R_n, \ldots$ be rings with unit. The direct product $S = R_1 \oplus R_2 \oplus \cdots \oplus R_n \oplus \cdots$ is the set of all infinite sequences $(a_1, a_2, a_3, \ldots)$, $a_i \in R_i$, $i = 1, 2, \ldots$. If $a = (a_1, a_2, a_3, \ldots)$, $b = (b_1, b_2, b_3, \ldots)$ $a + b = (a_1 + b_1, a_2 + b_2, a_3 + b_3, \ldots)$ and $a \cdot b = (a_1 \cdot b_1, a_2 \cdot b_2, a_3 \cdot b_3, \ldots)$. S is a ring.

Let

$$A_1 = (a_1, 0, 0, \ldots)$$

$$A_2 = (a_1, a_2, 0, 0, \ldots)$$

$$A_n = (a_1, a_2, \ldots, a_n, 0, 0, \ldots)$$

$A_1 = A_2 \cdot (1, 0, 0, \ldots)$, $A_n = A_{n+1} \cdot (1, 1, 1, \ldots, 1, 0, 0, \ldots)$ where the first n elements in the last term are 1. Therefore, $(A_1, A_2) \in \beta$, $(A_2, A_3) \in \beta, \ldots, (A_n, A_{n+1}) \in \beta, \ldots$ and there is no point where $A_m = A_{m+1} = \cdots$. Thus s does not satisfy the descending chain condition for elements, and by theorem 5 s does not satisfy the ascending chain condition for ideals. [4, p. 17]

CHAPTER II

NECESSARY AND SUFFICIENT CONDITIONS

Now the preliminary results will be used to aid in constructing theorems giving necessary and sufficient conditions for a ring to be a unique factorization domain.

Definition: An element of a ring is said to be irreducible if, whenever it is expressed as a product of two elements, one and only one of them is a unit.

Theorem 6: In a ring R satisfying the inductive condition every nonzero, nonunit element is expressible as a product of irreducible elements.

Proof: Let E be the property that an element is expressible as a product of irreducible elements. Clearly E is true for all minimal elements of R, since all minimal elements are irreducible.

Let x be a nonunit, nonzero element of R. Assume that E is satisfied for all proper divisors of x. Then $x = y \cdot z$ where y and z are proper divisors of x. By hypothesis, $y = y_1 \cdot y_2 \cdot \ldots y_n$, $z = z_1 \ z_2 \cdot \ldots z_m$ where $y_1, y_2, \ldots, y_n; z_1, \ldots, z_m$ are all irreducible. Therefore, $x = y_1 \ldots y_n \cdot z_1 \ldots z_m$.

The following is an example of an ring where every element is not necessarily expressible as a product of irreducible elements.

Example: In the example given on page six, let $R_1, R_2, \ldots$ be the integers, I. Then S is the set of all infinite sequences $(a_1, a_2, \ldots)$, $a_i \in I$ for all i.

Let p be a prime integer and $a = (p, p, p, \ldots)$. Assume that $a = B_1 \cdot B_2 \ldots B_m$ where $B_1, B_2, \ldots B_m$ are irreducible, and

$$B_1 = (b_{11}, b_{12}, b_{13}, \ldots)$$

$$B_2 = (b_{21}, b_{22}, b_{23}, \ldots)$$

$$\vdots$$

$$B_m = (b_{m1}, b_{m2}, b_{m3}, \ldots)$$

Thus $a = (b_{11} \cdot b_{21} \cdot b_{31} \ldots b_{m1}, b_{12} \cdot b_{22} \ldots b_{m2}, b_{13} \cdot b_{23} \ldots b_{m3}, \ldots)$ and $p = b_{11} \cdot b_{21} \ldots b_{m1}$, $p = b_{12} \cdot b_{22} \ldots b_{m2}$, $p = b_{13} \cdot b_{23} \ldots b_{m3}, \ldots$ but p is irreducible. Therefore, each factorization of p can contain only one nonunit element and that must be $\pm p$. Assume that $b_{11} = \pm p$. Since B_1 is irreducible, $b_{1i} = \pm 1$ $i \neq 1$. Therefore, $b_{12} \neq \pm p$ which implies $b_{22}, b_{32}, \ldots,$ or b_{m2} must equal $\pm p$. The B_i's can be ordered so that $b_{22} = \pm p$. Then since B_2 is irreducible $b_{2i} = \pm 1$ for $i \neq 2$. Now $b_{13} \neq \pm p$ and $b_{23} \neq \pm p$, thus by reordering if necessary, I can get $b_{33} = \pm p$ and $b_{3i} = \pm 1$ for $i \neq 3$. Continuing, I will eventually get $b_{ii} = \pm p$ $i \leq m$, $b_{ij} = \pm 1$, $i \leq m$, and $j \neq i$. But $p = b_{1(m+1)}\ b_{2(m+1)} \cdot \ldots b_{m(m+1)}$, thus $b_{j(m+1)} = \pm p$ for some $j \leq m$. Then

$$B_j = (b_{j1}, b_{j2}, \ldots, b_{jm}, b_{j(m+1)}, \ldots)$$

$$= (b_{j1}, b_{j2}, \ldots, b_{jm}, 1, 1, \ldots) \cdot (1, 1, \ldots, 1, b_{j(m+1)}, \ldots)$$

and neither of the right hand factors is a unit, contradicting the fact that B_j is irreducible. Thus a is not expressible as a product of irreducible elements of S.

Definition: A Noetherian ring is a ring which satisfies the maximum conditon for ideals.

Theorem 7: In a Noetherian integral domain, R, every element is expressible as a product of irreducible elements.

Proof: By theorem 1, R satisfies the ascending chain condition for ideals, and thus, by theorem 5, R satisfies the descending chain condition for elements. Then, by theorem 2, R satisfies the inductive condition, and theorem 6 gives the result.

Definition: A prime element is an element x of an integral domain R such that if x divides $a \cdot b$, then x divides a, or x divides b.

The following two lemmas will prove useful in the proof of the next theorem.

Lemma 1: Let R be an integral domain in which any two elements have a greatest common divisor. Let a and b belong to R, then define $M_{ab} = \{m \in R: m = r \cdot a$ and $m = s \cdot b$ and the greatest common divisor of r and s is $1\}$. M_{ab} has only one class of associated elements.

Proof: Assume that M_{ab} contains two elements, m_1 and m_2. $m_1 = r_1 \cdot a$, $m_1 = s_1 \cdot b$, $m_2 = r_2 \cdot a$, and $m_2 = s_2 \cdot b$ where the greatest common divisor of r_1 and s_1 is 1 and the greatest common divisor of r_2 and s_2 is 1. m_1 and m_2 have a greatest common divisor, say d. a divides m_1 and m_2, and b divides m_1 and m_2. Therefore, $d = q_1 \cdot a$ and $d = q_2 \cdot b$ for some q_1 and q_2 belonging to R. q_1 and q_2 have a greatest common divisor, say d_2. $q_1 = r_3 \cdot d_2$ and $q_2 = s_3 \cdot d_2$, where r_3 and s_3 belong to R. Thus, $d = r_3 \cdot d_2 \cdot a$ and $d = s_3 \cdot d_2 \cdot b$. r_3 and s_3 have a greatest common divisor d_3. $r_3 = r_4 \cdot d_3$ and $s_3 = s_4 \cdot d_3$, where r_4 and s_4 belong to R. $q_1 = r_4 \cdot d_3 \cdot d_2$ and $q_2 = s_4 \cdot d_3 \cdot d_2$. $d_3 \cdot d_2$ divides both q_1 and q_2 and thus must divide d_2. Therefore, d_3

must be a unit. Let $m' = s_3 \cdot b = r_3 \cdot a$. The greatest common divisor of s_3 and r_3 is 1, so m' is in M_{ab}. Thus, $d = d_2 \cdot m'$ and d is a multiple of an element of M_{ab}. We had m_1 as a multiple of d, therefore m_1 is a multiple of m', say $m_1 = r \cdot m'$ where r belongs to R.

$r_1 \cdot a = r \cdot m' = r \cdot r_3 \cdot a$ and $s_1 \cdot b = r \cdot m' = r \cdot s_3 \cdot b$, therefore, $r_1 = r \cdot r_3$ and $s_1 = r \cdot s_3$, which implies r divides r_1 and s_1. But since the greatest common divisor of r_1 and s_1 is 1, r must be a unit. Thus m_1 and m' are associates. Likewise, m_2 and m' are associates. Thus m_1 and m_2 are associated.

Lemma 2: Let R be an integral domain in which any two elements have a least common multiple. If a and b are any two elements belonging to R and $m = a \cdot b$, then the greatest common divisor of a and b is m/n where n is the least common multiple of a and b.

Proof: Suppose c divides a and b, then $a = p \cdot c$ and $b = q \cdot c$ where $p, q \in R$. Since n is the least common multiple of a and b, $n = r \cdot a$ and $n = s \cdot b$ where $r, s \in R$. m is a multiple of n, say $m = u \cdot n$. c and u have a least common multiple, say d. $d = r_1 \cdot c$ and $d = s_1 \cdot u$ where $r_1, s_1 \in R$. a is a multiple of u since $n \cdot u = m$, $s \cdot b \cdot u = a \cdot b$ which implies $s \cdot u = a$. Since a is also a multiple of c, a must be a multiple of d, say $a = r_2 \cdot d$. Now b is a multiple of c and $r \cdot a \cdot u = a \cdot b$ implies $b = r \cdot u$. Thus, b is a multiple of u. Therefore, b is a multiple of d, say $b = s_2 \cdot d$. $r_2 \cdot d = a = u \cdot s$ and $r_2 \cdot s_1 \cdot u = u \cdot s$; therefore, $r_2 \cdot s_1 = s$. Likewise, $s_2 \cdot d = u \cdot r$ implies $s_2 \cdot s_1 \cdot u = u \cdot r$ and $s_2 \cdot s_1 = r$. Thus, $n = s_2 \cdot s_1 \cdot a$ and $n = r_2 \cdot s_1 \cdot b$.

Let $n' = s_2 \cdot a = r_2 \cdot b$. $n = s_1 \cdot n'$ implies s_1 is a unit, otherwise n would not be the least common multiple of a and b.

Therefore, d and u are associates. u is then a multiple of c. It then follows that u is the greatest common divisor of a and b.

Theorem 8: Any two elements of an integral domain R have a greatest common divisor if and only if any two elements have a least common multiple.

Proof: (only if) Let a and b belong to R, and let c be a multiple of both a and b, say $c = x \cdot a$ and $c = y \cdot b$. Let M be as in lemma 1. If c is a multiple of some $m \in M$, then m is the least common multiple of a and b, since all elements in m are associated.

x and y have a greatest common divisor, say d. $x = r \cdot d$ and $y = s \cdot d$ where $r, s \in R$. $c = r \cdot d \cdot a$ and $c = s \cdot d \cdot b$. Now r and s have a greatest common divisor d_2. $r = r_2 \cdot d_2$ and $s = s_2 \cdot d_2$ where $r_2, s_2 \in R$. Thus, $x = r_2 \cdot d_2 \cdot d$ and $y = s_2 \cdot d_2 \cdot d$. Since d is the greatest common divisor of x and y, d_2 must equal 1. Therefore, $c = r \cdot d \cdot a = s \cdot d \cdot b$, and $m = r \cdot a = s \cdot b \in M$.

(If) This follows immediately from lemma 2.

Theorem 9: Suppose R is an integral domain. Any two elements of R have a least common multiple if and only if the intersection of any two principal ideals is principal; and furthermore, $(a) \cap (b) = (c)$ if and only if c is the least common multiple of a and b.

Proof: (only if) Let A and B be two principal ideals, say $A = (a)$, $B = (b)$, where $a, b \in R$. a and b have a least common multiple, say m. If $x \in (a) \cap (b)$ then x is a multiple of both a and b, and thus a multiple of m. Therefore, $x \in (m)$ and $(a) \cap (b) \subset (m)$. If $x \in (m)$ then x is a multiple of m. Now m is a multiple of both a and b; therefore, x is a multiple of both a and b. Therefore, $x \in (a)$ and $x \in (b)$. Thus, $x \in (a) \cap (b)$ and $(a) \cap (b) = (m)$.

(If) Suppose $a, b \in R$, then $(a) \cap (b) = (c)$ for some $c \in R$. $c \in (a)$

and $c \in (b)$. Suppose m is a multiple of both a and b, say $m = r \cdot a$ and $m = s \cdot b$, where $r, s \in R$. Therefore, $m \in (a)$ and $m \in (b)$ which implies $m \in (a) \cap (b) = (c)$ and thus m is a multiple of c. Thus c is the least common multiple of a and b. This concludes theorem 9.

The following is an example of an integral domain where the intersection of two principal ideals is not necessarily principal.

Example: Let R be the ring of elements of the form $\alpha = a + b \cdot i\sqrt{3}$ where a and b are integers. Define $N(\alpha) = a^2 + 3b^2$. If $\alpha = a + b \cdot i\sqrt{3}$ and $\beta = c + d \cdot i\sqrt{3}$,

$$\begin{aligned} N(\alpha \cdot \beta) &= N(ac - 3bd + i\sqrt{3}\,(ad + bc)) \\ &= a^2 c^2 + 9b^2 d^2 - 6acbd + 3a^2 d^2 + 3b^2 c^2 + 6abcd \\ &= a^2 c^2 + 3a^2 d^2 + 3b^2 c^2 + 9b^2 d^2 \\ &= (a^2 + 3b^2) \cdot (c^2 + 3d^2) = N(\alpha) \cdot N(\beta) \end{aligned}$$

Now $N(1) = 1$, and if $N(a + bi\sqrt{3}) = 1$ then $a^2 + 3b^2 = 1$ which implies $a = \pm 1$ and $b = 0$.

Consider $(1 + i\sqrt{3}) \cap (1 - i\sqrt{3})$ if this ideal is principal say $(1 + i\sqrt{3}) \cap (1 - i\sqrt{3}) = (c)$ then by theorem 9 c is the least common multiple of $1 + i\sqrt{3}$ and $1 - i\sqrt{3}$. Now 4 is a multiple of $1 + i\sqrt{3}$ and $1 - i\sqrt{3}$ therefore 4 is a multiple of c.

$$\begin{aligned} 4 = r \cdot c &= (r_1 + i\, r_2\, \sqrt{3})\,(c_1 + i\, c_2\, \sqrt{3}) \\ \therefore N(4) &= N(r_1 + i\, r_2\, \sqrt{3})\, N(c_1 + i\, c_2\, \sqrt{3}) \\ 16 &= (r_1^2 + 3\, r_2^2)\,(c_1^2 + 3c_2^2) \end{aligned}$$

$$16 = 16 \cdot 1 = 8 \cdot 2 = 4 \cdot 4$$

If $N(r) = 1$ then $r = 1$ and 4 is the least common multiple of

$1 + i\sqrt{3}$ and $1 - i\sqrt{3}$. $N(c)$ cannot be 1 because $N(c) \geq N(1 + i\sqrt{3}) = 4$. There are no integers a,b such that $a^2 + 3b^2 = r$ therefore neither $N(r)$ nor $N(c)$ can equal 2. If $N(c) = 4$ then $c = \pm 1 \pm i\sqrt{3}$ or $c = 2$. 2 and $\pm 1 \pm i\sqrt{3}$ are irreducible, since if $2 = \alpha \cdot \beta$ then $N(2) = N(\alpha) \cdot N(\beta)$, that is, $4 = N(\alpha)N(\beta)$. Either $N(\alpha) = 4$, $N(\beta) = 1$ or $N(\alpha) = 2$, $N(\beta) = 2$. If $N(\beta) = 1$ then $\beta = 1$ which means $\alpha = 2$, and we have a trivial factorization. $N(\alpha)$ cannot be 2 so 2 is irreducible. Now if $\pm 1 \pm i\sqrt{3} = \alpha\beta$ then $4 = N(\alpha) \cdot N(\beta)$, and by the same reasoning $\pm 1 \pm i\sqrt{3}$ is irreducible.

If 4 is the least common multiple of $1 + i\sqrt{3}$ and $1 - i\sqrt{3}$ then $-2 - 2i\sqrt{3}$ is a multiple of 4, since $-2 - 2i\sqrt{3} = -2(1 + i\sqrt{3}) = (1 - i\sqrt{3})^2$.

Say

$$-2 - 2i\sqrt{3} = r \cdot 4$$

$$-1 - i\sqrt{3} = r \cdot 2$$

$$1 + i\sqrt{3} = -2 \cdot r.$$

$1 + i\sqrt{3}$ is irreducible, so $-2 - 2i\sqrt{3}$ cannot be a multiple of 4 and 4 cannot be the least common multiple of $1 + i\sqrt{3}$ and $1 - i\sqrt{3}$.

c cannot be $\pm 1 \pm i\sqrt{3}$ or 2 because all of these elements are irreducible and therefore cannot be multiples of $1 + i\sqrt{3}$ and $1 - i\sqrt{3}$.

No other possibilities exist, so no such c exists and this implies that $(1 + i\sqrt{3}) \cap (1 - i\sqrt{3})$ is not principal.

In the next three lemmas the greatest common divisor of a and b will be denoted by (a,b).

Lemma 1: If a, b, and c are members of the integral domain R, then (ac,bc) and (a,b) · c are associates.

Proof: (a,b) divides a and b, thus (a,b) · c divides a · c and b · c and therefore (a · c, b · c), say (a · c, b · c) = (a,b) · c · r where r ∈ R. Thus a · c = (a · c, b · c) · s = (a,b) · c · r · s where s ∈ R. Therefore a = (a,b) · r · s. Likewise b · c = (a · c, b · c) · t = (a,b) · c · r · t where t ∈ R. Therefore b = (a,b) · r · t and (a,b) · r divides both a and b. Thus (a,b) · r divides (a,b) which implies r is a unit. Therefore (a · c, b · c) and (a,b) · c are associates.

Lemma 2: If a, b, c are members of the integral domain R then ((a,b), c) and (a, (b,c)) are associates.

Proof: ((a,b), c) divides (a,b) and c and thus a, b, and c. Therefore ((a,b), c) divides a and (b,c) which implies ((a,b),c) divides (a, (b,c)). Likewise (a, (b,c)) divides ((a,b),c), and the two are associates.

Lemma 3: If a, b, and c are members of the integral domain R and if (a,b) = 1 and (a,c) = 1 then (a,bc) = 1.

Proof: Obviously (a, a · c) = a. By lemma 1 (a,b) · c = r (a · c, b · c) for some unit r and thus c = r(a · c, b · c). Now by lemma 2 (a,b · c) = ((a, a · c), b · c) = s(a, (a · c, b · c)) where s is a unit. Therefore (a, b · c) = s(a, r^{-1} · c). Now (a, r^{-1} · c) = (a,c) since r^{-1} is a unit, therefore (a, bc) = s · (a,c) = s. Since any element associated with s also defines the greatest common divisor of a and b · c, (a, b · c) = s^{-1} · s = 1.

Theorem 10: If a greatest common divisor exists for any pair of elements a, b ∈ R then every irreducible element of the integral domain R will be prime.

Proof: Let p be an irreducible element, and assume p is not prime. Then there exist $a, b \in R$ such that $a \cdot b \in (p)$ and $a \notin (p)$, $b \notin (p)$, thus $(p, a) = 1$ and $(p, b) = 1$. Therefore by lemma 3 $(p, a \cdot b) = 1$, but p divides $a \cdot b$. This is a contradiction, therefore p is prime. [4, p. 73]

Theorem 11: An integral domain R will be a unique factorization domain if and only if it satisfies condition (α) and either condition β_1, β_2, β_3, or β_4.

(α) R satisfies the minimum condition for elements.

(β_1) any two nonzero elements have a greatest common divisor.

(β_2) any two nonzero elements have a least common multiple.

(β_3) the intersection of any two principal ideals is principal.

(β_4) every irreducible element of R is prime.

Proof: β_1, β_2, and β_3 are equivalent thus it is sufficient to prove the theorem for β_1 and β_4.

First I will prove that if R is a unique factorization domain, then α and β_1 are satisfied. If $a \in R$ then $a = P_1 P_2 \ldots P_n$ where $P_1, P_2, \ldots P_n$ are irreducible. Every strictly decreasing chain of elements starting with a can obviously have at most n elements. Thus the descending chain condition is satisfied, which implies that α is satisfied. Let $a, b \in R$ and let $P_1, P_2, \ldots, P_n$ be irreducible elements such that every irreducible divisor of both a and b is associated with some P_i, and every P_i is associated with an irreducible divisor of either a or b. Therefore $a = \xi_1 P_1^{K_1} P_2^{K_2} \ldots P_n^{K_n}$ and $b = \xi_2 P_1^{L_1} P_2^{L_2} \ldots P_n^{L_n}$ where ξ_1 and ξ_2 are units and any number of K_i's and L_i's can be zero. Any divisor, a_1, of a can be written $a_1 = \xi_1^1 P_1^{i_1} P_2^{i_2} \ldots P_n^{i_n}$ with $0 \leq i_1 \leq K_i$, and any

divisor, b_1, of b can be written $b_1 = \xi_2^1 P_1^{j_1} P_2^{j_2} \ldots P_n^{j_n}$ with $0 \leq j_1 \leq L_i$. Thus $(a, b) = P_1^{m_1} P_2^{m_2} \ldots P_n^{m_n}$ where $m_i = \min (K_i, L_i)$, $i = 1, \ldots, n$. Thus R satisfies condition β_1.

By theorem 10 R satisfies condition β_4.

Thus it remains to be proved that if R satisfies conditions α and β_4 then R is a unique factorization domain. By theorem 6 we get that every nonunit, nonzero element of R is expressible as a product of irreducible elements. Every minimal element in R is irreducible and every irreducible element trivially satisfies the uniqueness property. Therefore the set of all minimal elements in R satisfies the property that they are uniquely expressible as a product of irreducible elements, call this property E. Assume E is true for all proper divisors of an element a, that is, for all b such that $(a, b) \in \beta$ and $(b, a) \notin \beta$. Now $a = b \cdot c$ where b and c are proper divisors of a. $b = \xi_1 P_1 P_2 \ldots P_n$ and $c = \xi_2 P_{n+1} P_{n+2} \ldots P_m$, where ξ_1 and ξ_2 are units and $P_1, \ldots, P_m$ are irreducible.

$a = \xi P_1 P_2 \ldots P_m$ where $\xi = \xi_1 \cdot \xi_2$. Assume that $a = \eta q_1 q_2 \ldots q_i$ where $q_1, \ldots, q_i$ are irreducible and η is a unit. Therefore $\xi P_1 P_2 \ldots P_m = \eta q_1 q_2 \ldots q_i$. Now $q_1, q_2, \ldots, q_i$ are prime. $\xi \cdot \eta^{-1} \cdot P_1 \cdot P_2 \ldots P_m = q_1 \cdot q_2 \ldots q_i$ therefore q_1 divides $(\xi \cdot \eta^{-1} P_1) \cdot P_2 \ldots P_n$ and q_1 divides either $(\xi \cdot \eta^{-1} P_1)$, $P_2, \ldots,$ or P_n. Assume that q_1 divides P_1. If not, then renumber so that it does. But P_1 is irreducible, therefore P_1 and q_1 are associates and $\xi \cdot \eta^{-1} \cdot P_1 = \xi' \cdot q_1$ where ξ' is a unit. Therefore $\xi' \cdot q_1 \cdot P_2 \ldots P_m = q_1 \cdot q_2 \ldots q_i$ which implies that $\xi' \cdot P_2 \ldots P_m = q_2 \ldots q_i$, but the left and right sides of this equation are both proper divisors of a, and by the inductive assumption each

P_i is associated with some q_j and vice versa. But then the two factorizations of a are associated. Therefore R is a unique factorization domain. [5, p. 75]

The following is an example of a ring satisfying condition α of theorem 11 which is not a unique factorization domain.

Example: Using the example used previously of the ring, R, of elements of the form $a + i\,b\sqrt{3}$ we see immediately that R is not a unique factorization domain since $4 = 2 \cdot 2 = (1 + i\sqrt{3})(1 - i\sqrt{3})$.

It is interesting to note that R satisfies condition (α) of theorem 11. If $\alpha_1, \alpha_2, \ldots$ is a decreasing sequence of elements of R say $\alpha_1 = r_1\ \alpha_2$, $\alpha_2 = r_2\ \alpha_3$, $\ldots$ then $N(\alpha_1) = N(r_1)\ N(\alpha_2)$, $N(\alpha_2) = N(r_1)\ N(\alpha_3)$, $\ldots$. $N(\alpha_1), N(\alpha_2), \ldots$ is a decreasing sequence of integers and since the integers satisfy the descending chain condition there must be an n such that $N(\alpha_n) = N(\alpha_{n+1}) = \ldots$. Then $N(r_n) = 1$, $N(r_{n+1}) = 1, \ldots$ and $r_n = 1$, $r_{n+1} = 1, \ldots$ which implies $\alpha_n = \alpha_{n+1} = \ldots$. R satisfies the descending chain condition, and by theorem 2 R satisfies condition α.

Definition: A prime ideal P of a ring R is of height r if there is a chain of prime ideals P_i such that $P \supset P_1 \supset P_2 \supset \ldots \supset P_r$ but there is no such chain with more terms. If there is no such r, we say that R is of infinite height. The height of a prime ideal in a Noetherian integral domain is finite. [6, p. 26]

Theorem 12: Let R be an integral domain satisfying condition α of theorem 11, then every prime ideal of R contains an irreducible element.

Proof: Let P be a prime ideal in R, then P contains a set of minimal elements, select one of these, say p. If $p = a \cdot b$ where a and b are not units, then either a or b is a member of P since P is prime.

Then $(p, a) \in \beta$ and p is not minimal in P. This is a contradiction. Therefore p is irreducible.

Theorem 13: Let R be an integral domain satisfying condition α of theorem 11. If every irreducible element of R is prime, then every prime ideal P of height 1 in R is principal.

Proof: Assume that there exists a nonprincipal prime ideal of height 1, say P. P contains an irreducible element p. Let $x \in (p)$ then $x = y \cdot p$ for some $y \in R$. $p \in P$ implies $y \cdot p \in P$ and $(p) \subset P$. $(p) \neq P$ by assumption. Therefore $P \supset (p) \supset (0)$ and P is of height 2. This is a contradiction. Thus P is principal.

Definition: An isolated prime ideal of an ideal P is a prime ideal which contains P but does not contain any other prime ideal which contains P.

The following is an example of a nonisolated prime ideal.

Example: Let I be the ring of integers. The ideal (x, y) is a prime ideal in $I[x, y]$. (x, y) consists of all elements of $I[x, y]$ with zero constant terms. $a \cdot b \in (x, y)$ implies the constant term of $a \cdot b$ is zero which implies the constant term of either a or b is zero. Thus (x, y) is prime.

(x) is prime since if a product of two elements has x as a factor then at least one of the elements must have x as a factor.

$(2x) \subset (x) \subset (x, y)$, which shows then (x, y) is not an isolated prime of $(2x)$.

Theorem 14: In a Noetherian integral domain every ideal, s, has a set of isolated primes, $P_1, P_2, \ldots, P_n$ and $s \subset P_1 \cap P_2 \cap \ldots \cap P_n$.

Proof: The theorem follows immediately from corollary 3.49.1 in Introduction to Abstract Algebra by Barnes.

Theorem 15: Let R be a Noetherian integral domain, if every prime ideal P of height 1 is principal then every irreducible element is prime.

Proof: Let p be an irreducible element. (p) has a set of isolated prime ideals $P_1, P_2, \ldots, P_n$ and $(p) \subset P_1 \cap P_2 \cap \ldots \cap P_n$. Therefore $(p) \subset P_i$ $i = 1, n$. Now there does not exist a prime ideal M such that $(p) \subset M \subset P_i$ since P_i is an isolated prime of (p).

Assume there exists a prime ideal M such that $(0) \subset M \subset (p)$. Now M can be assumed to be of height 1 for if it is not then there exists a prime ideal N such that N is of height 1 and $(0) \subset N \subset M$, and we can replace M by N. By assumption M is principal and $M = (m)$ for some $m \in R$. Therefore $(0) \subset (m) \subset (P)$ and $m = rp$ where $r \in R$. Assume $r \notin (m)$ then since $m \in (m)$ and (m) is prime $p \in (m)$. Thus if $x \in (p)$ then $x = sp$ for some $s \in R$ and $x \in (m)$. Therefore $(p) = (m)$ and p is prime.

If $r \in (m)$ then $r = r_2 m$ for some $r_2 \in R$, thus $m = r_2 m p$. Therefore $1 = r_2 p$ and p is a unit. This is a contradiction, therefore $r \notin (m)$, and as shown above, p is prime.

If no such prime ideal M exists, then P_i is of height 1. Therefore $P_i = (p_i)$ for some $p_i \in R$ and $(p) \subset (p_i)$ and $p = q \cdot p_i$ where $q \in R$. But p is irreducible, q is a unit and $(p) = (p_i)$. Thus p_i is prime.

The following is immediate from theorems 13 and 15.

Theorem 16: Let R be a Noetherian integral domain. Then every prime ideal P of height 1 is principal if and only if every irreducible element is prime.

Theorem 17: A Noetherian integral domain will be a unique factorization domain if and only if it satisfies one of the following: (β_1), (β_2), (β_3), (β_4), or (β_5), where (β_1), (β_2), (β_3), and (β_4) are as in theorem 11, and (β_5) is: "every prime ideal of height 1 is principal." [6, p. 1]

Proof: (only if) this follows immediately from theorems 11 and 16.

(If) Since R is Noetherian it satisfies condition α by theorem 6. The result then follows immediately from theorems 11 and 16.

CHAPTER III

APPLICATIONS

Theorem 18: Every principal ideal domain is a unique factorization domain.

Proof: If R is a principal ideal domain then every ideal in R is principal, that is, every ideal in R has a basis consisting of one element. Therefore by theorem 1, R is Noetherian.

The intersection of any two principal ideals is an ideal and thus principal. Therefore by theorem 17, R is a Unique Factorization Domain.

Theorem 19: Let A be an integral domain satisfying condition (α) of theorem 11. Let x and y be products of prime elements and $a, b \in A$. Then $(a \cdot y) \bigcap (b \cdot x)$ is principal if and only if $(a) \bigcap (b)$ is principal. [7, p. 3]

Proof: First assume $y = 1$ and x is prime. Let n be the largest power of x which divides a. If no such n exists then $a, \frac{a}{x}, \frac{a}{x^2}, \ldots$ forms a nonending strictly decreasing sequence of elements, which contradicts the fact that A satisfies condition (α). Likewise let m be the largest integer such that x^m divides b. Thus $a = p \cdot x^n$ and $b = q \cdot x^m$ for some $P, q \in A$.

Suppose $n \leq m$. If $(a) \bigcap (b)$ is principal then $(a) \bigcap (b) = (c)$ where c is the least common multiple of a and b.

Let y be a multiple of both a and bx, say $y = r \cdot a$ and $y = s \cdot b \cdot x$ where $r, s \in A$. Thus $\frac{y}{x^{n+1}} = s \cdot q \cdot x^{m-n}$, and

$\frac{y}{x^{n+1}} = \frac{r \cdot a}{x^{n+1}} = \frac{r \cdot p}{x^{n+1}} \frac{\cdot x^n}{} = \frac{r \cdot p}{x}$. But x is prime which implies x divides r or x divides p. Assume that x does not divide p then x divides r, $\frac{y}{x^{n+1}} = \frac{r}{x} p$ and $\frac{y}{x} = \frac{r}{x} p x^n = \frac{r}{x} \cdot a$. Thus $\frac{y}{x}$ is a multiple of a, which implies $\frac{y}{x}$ is a multiple of c and y is a multiple of cx. Therefore cx is the least common multiple of a and bx and $(a) \bigcap (bx) = (cx)$.

Now if x does divide p then $p = l \cdot x$ for some $l \in A$. Thus $a = l \cdot x \cdot x^n = l \cdot x^{n+1}$, but n was the largest power of x which divides a. Thus x does not divide p.

Let $n > m$ and assume $(a) \bigcap (b)$ is principal, c is again the least common multiple of a and b and $(a) \bigcap (b) = (c)$. Assume y is a multiple of a and bx then y is a multiple of c. $c = u \cdot a$ and $c = v \cdot b$ for some $u, v \in A$. Thus $u \cdot p \cdot x^n = c = v \cdot b = v \cdot q \cdot x^m$ which implies $v \cdot q = u \cdot p \cdot x^{n-m} = u \cdot p \cdot x^{n-m-1} \cdot x$ since if $n - m > 0$ then $n - m \geq 1$. x divides either v or q. If x divides q then $q = p \cdot x$ for some $p \in A$ and $b = p \cdot x \cdot x^m = p \cdot x^{m+1}$, but m was the largest integer such that x^m divides b. Therefore x does not divide q which implies x divides v. $v = l \cdot x$ for some $l \in A$. $c = v \cdot b = l \cdot x \cdot b$. Therefore c is a multiple of $x \cdot b$ and c is the least common multiple of a and xb. Thus $(a) \bigcap (x \cdot b) = (c)$.

(Only if) Assume $(a) \bigcap (b \cdot x)$ is principal. $(a) \bigcap (b \cdot x) = (d)$ where by theorem 9, d is the least common multiple of a and $b \cdot x$. Suppose $n \leq m$. Since $d \in (b \cdot x)$, then $d = r \cdot b \cdot x$ for some $r \in A$.

Suppose y is a multiple of both a and b, $y = u \cdot a$ and $y = v \cdot b$ for some $u, v \in A$. $y \cdot x$ is a multiple of both a and $b \cdot x$ thus $y \cdot x$ is a multiple of d and y is a multiple of $\frac{d}{x}$.

d is a multiple of a, say $d = a \cdot w$ where $w \in A$. Thus $p \cdot x^n \cdot w = a \cdot w = d = r \cdot b \cdot x = r \cdot q \cdot x^m \cdot x$. $p \cdot w = r \cdot q \cdot x^{m-n} \cdot x$ and x must divide p or w. If x divides p, say $p = P' x$ where $P' \in A$, then $a = P' \cdot x^{n+1}$ which contradicts the fact that n is the largest integer such that x^n divides a. Thus x does not divide p which implies x must divide w, say $w = x \cdot w'$ for $w' \in A$. $d = a \cdot x \cdot w'$ and $\frac{d}{x}$ is a multiple of a. Thus $\frac{d}{x}$ is the least common multiple of a and b and $(a) \bigcap (b) = \left(\frac{d}{x}\right)$. Suppose $n > m$ and let y be a multiple of both a and b, say $y = u \cdot a$ and $y = v \cdot b$ where $u, v \in A$. $v \cdot q \cdot x^m = v \cdot b = y = u \cdot a = u \cdot p \cdot x^n$ thus $v \cdot q = u \cdot p \cdot x^{n-m} = u \cdot p \cdot x^{n-m-1} \cdot x$. x divides either v or q and x cannot divide q since x^m is the highest power of x which divides b. Therefore x divides v, say $v = v' \cdot x$ where $v' \in A$. Then $y = v' \cdot x \cdot b$ and y is a multiple of both a and $b \cdot x$ which implies y is a multiple of d. Thus d is the least common multiple of a and b and by theorem 9 $(a) \bigcap (b) = (d)$.

Now if x and y are prime, $(a) \bigcap (b \cdot x)$ is principal and $(ay) \bigcap (b)$ is principal, thus $(a \cdot y) \bigcap (b \cdot x) = ((a \cdot y) \bigcap (b) \bigcap (b \cdot x) \bigcap (a))$ is principal. The theorem follows by induction on the number of prime factors in x and y.

Definition: Let R be an integral domain and S a subset of R which is closed under the operation of multiplication and $0 \notin S$, then $Rs = \{a/s \;\; a \in R \text{ and } s \in S\}$

Definition: If R is a ring and B is a subset of R and if $r \in R$ then $Br = \{b \cdot r : b \in B\}$

Theorem 20: Let A be an integral domain satisfying condition (α) of theorem 11, and let S be the multiplicative system generated by any

family of prime elements $\{x_i : i \in R$ where R is an indexing set$\}$.

If A_s is a unique factorization domain then so is A. [7, p. 3]

Proof: By theorem 11 this theorem will follow if I can show that the intersection of any two principal ideals is principal. For any $y \in A$ let $V_i(y)$ be the largest integer n such that x_i^n divides y. This integer n is finite since A satisfies condition (α). Furthermore any element $a' \in A$ can be written in the form $a' = a \prod_{i \in R} x_i^{V_i(a')}$ where a is not a multiple of x_i for any $i \in R$. Almost all $V_i(a')$ are zero since A satisfies condition (α). Theorem 19 shows that $(a') \cap (b')$ is principal if and only if $(a) \cap (b)$ is principal where $b' = b \prod_{i \in p} x_i^{V_i(b')}$. Now $A_s = \{a/s : a \in R, s \in S\}$ I first want to show that $A_s\, a \cap A = Aa$. Let $u \in A_s\, a \cap A$ then $u \in A_s\, a$ and $u \in A$ which implies $u = a \cdot d/s$ for some $s \in S$ and $d \in A$. Thus $a \cdot \frac{d}{s} \in A$. No divisor of s divides a therefore every divisor of s divides d and s divides d which implies that $a \cdot \frac{d}{s} \in Aa$ and $u \in Aa$. Thus $A_s\, a \cap A \subset Aa$. Let $u \in Aa$ then $u = a \cdot d$ for some $d \in A$. Let $s \in S$, $d \cdot s \in A$ then $\frac{d \cdot s}{s} \in A_s$. Therefore $a \cdot \frac{d \cdot s}{s} \in A_s\, a$ and $A_s\, a \cap A = Aa$. Likewise $A_s\, b \cap A = A_b$. Since A_s is a unique factorization domain $A_s\, a \cap A_s\, b$ is a principal ideal, say $A_s\, a \cap A_s\, b = A_s\, c$, where $c \in A_s$. $A\, a \cap A\, b = (A_s\, a \cap A) \cap (A_s\, b \cap A) = A \cap (A_s\, a \cap A_s\, b) = A \cap A_s\, c$. $c \in A_s$ implies $c = c' \cdot \prod_i x_i^{V_i(c)} / s$ where $s \in S$ and c' is not a multiple of any x_i. I want to show that $A_s\, c = A_s\, c'$. Let $y \in A_s\, c$ then $y = \frac{d}{s_1} \cdot \frac{c'}{s} \cdot \prod_i x_i^{V_i(c)}$ where $d \in A$. Therefore $y = \frac{d \prod_i x_i^{V_i(c)}}{s_1 \cdot s} \cdot c'$ and $y \in A_s\, c'$. If $y \in A_s\, c'$ then $y = \frac{d}{s_1} c'$ where $d \in A$, $s_1 \in S$. Thus $y = \frac{d}{s_1} \frac{s}{s} c' = \frac{ds}{s_1 \prod_i x_i^{V_i(c)}} \cdot \frac{c'}{s} \cdot \prod_i x_i^{V_i(c)} = \frac{d \cdot s}{s_1 \prod_i x_i^{V_i(c)}} \cdot c$, $S_1 \prod_i x_i^{V_i(c)} \in S$ and $y \in A_s\, c$. Therefore $A_s\, c = A_s\, c'$

and $c' \in A$. Now I need to show that $A \cap A_s c' = A c'$. Let $y \in A \cap A_s c'$ then $y \in A$ and $y \in A_s c'$. $y = \frac{d}{s} \cdot c'$ for some $d \in A$, $s \in S$ which implies $\frac{d}{s} \cdot c' \in A$. Now each prime divisor of s divides either d or c', but c' is not divisible by x_i for all $i \in R$. Therefore each prime divisor of s divides d. Thus s divides d. Hence $y \in A c'$. Now let $y \in A c'$, then $y = a c'$ for some $a \in A$. $y = a \cdot \frac{s}{s} \cdot c'$ and $y \in A_s c'$. Therefore $A \cap A_s c' = A c'$ and $Aa \cap Ab = A c'$. Thus $Aa \cap Ab$ is principal.

Theorem 21: If R is a unique factorization domain then the polynomial ring $R[x]$ is a unique factorization domain.

Proof: If p is prime in R then it is also prime in $R[x]$.

Let $s = R - \langle 0 \rangle$ then $R_s = K$ where K is the quotient field of R. Therefore $K[x]$ is a principal ideal domain since the ring of polynomials over a field is always a principal ideal domain. Therefore by theorem 18 $K[x] = R_s[x]$ is a unique factorization domain. Now I need to show that $R_s[x] = R[x]_s$. Let $p \in R[x]_s$, then $p = \left(\sum_i a_i x^i \right) / s$ where $s \in S$ and $a_i \in R$. Thus $p = \sum_i \frac{a_i}{s} x^i$ which implies $p \in R_s[x]$. If $p \in R_s[x]$ then $p = \sum_i \frac{a_i}{s_i} x^i$, $\frac{1}{s_i} a_i x^i \in R[x]_s$. Therefore $R[x]_s = R_s[x]$, and by theorem 20 $R[x]$ is a unique factorization domain.

Corollary: If R is a unique factorization then $R[x_1, x_2, \ldots, x_n]$ is a unique factorization domain.

Proof: This result follows from the previous theorem by induction.

The following is an example which shows that not every unique factorization domain is a principal ideal domain.

Example: Let I be the ring of integers. I is a principal ideal domain and thus a unique factorization domain. But $I[x]$ which by theorem 21 is a unique factorization domain is not a principal ideal domain.

Consider the ideal generated by the elements 2 and x say $(2,x)$. $(2,x) \neq I[x]$ since no polynomial with an odd constant term is in the ideal. Furthermore if $(y) = (2,x)$ then since $2 \in (2,x)$ $2 \in (y)$ and $2 = py$ for some $p \in I[x]$. But then either $p = 1$ and $y = 2$, $p = -1$ and $y = -2$, $p = 2$ and $y = 1$, or $p = -2$ and $y = -1$. If $y = \pm 1$ then $(y) = I[x]$ contradicting the fact that $(y) = I[x]$. If $y = \pm 2$ then $x \in (2,x)$ and $x \notin (y)$ contradicting the fact that $(y) = (2,x)$. Therefore no such y can exist and $(2,x)$ is not principal.

Definition: Let A be a subring of the ring R, an element $a \in R$ is said to be integral over A if there exist elements $c_0, c_1, c_2, \ldots, c_{n-1}$ belonging to A such that $a^n + c_{n-1} \cdot a^{n-1} \ldots + c_1 \cdot a' + c_0 = 0$. That is a is the root of a monic polynomial over R.

Definition: Let R be an integral domain and let K be the field of quotients of R. R is said to be a normal ring if every element of K which is integral over R belongs to R.

The following is an example of a ring which is not normal.

Example: Again let R be the ring of elements of the form $a + i\, b \sqrt{3}$ where a and b are integers.

$x^2 + x + 1$ is a monic polynomial with coefficients in R. The roots are $-\frac{1}{2} \pm \frac{1}{2} i \sqrt{3}$. The roots are in the quotient field of R, but they are not in R.

Theorem 22: Every unique factorization domain is a normal ring.

Proof: Let R be a unique factorization domain with quotient field K. Suppose there is an element $x \in K$ which is integral over R and not in R. Then $x = a/b$ where $a, b \in R$. We can assume that a and b have no irreducible factors in common since common irreducible factors could be removed without changing x. There exist $c_0, c_1, c_2, \ldots, c_{n-1} \in R$ such that $\frac{a}{b}^n + c_{n-1} \frac{a}{b}^{n-1} + \ldots + c_1 \frac{a}{b} + c_0 = 0$. Thus $a^n + c_{n-1} a^{n-1} b + \ldots + c_1 a b^{n-1} + c_0 b^n = 0$. Thus $a^n \in (b)$. If p is an irreducible divisor of b then $a^n \in (p)$, but since p is irreducible and R is a unique factorization domain p is prime, and thus (p) is a prime ideal. Therefore $a \in (p)$. This is a contradiction. Thus $x \in R$. [6, p. 43]

This theorem essentially says that if a monic polynomial with coefficients in R does not have a root in R then it will not have a root in the quotient field of R.

BIBLIOGRAPHY

1. Auslander, M.; and Buchsbaum, D. A.: "Unique Factorization in Regular Local Rings." Proc. Nat. Acad. Sci., U.S.A., Vol. 45 (1959), pp. 733 - 734.

2. Barnes, W. E.: Introduction to Abstract Algebra. D. C. Heath and Co., Boston, 1963.

3. Kurosh, A. G.: Lectures in General Algebra. Pergamon Press, Oxford, 1965.

4. McCoy, N. H.: The Theorey of Rings. Macmillan, New York, 1964.

5. Nagata, M.: "A General Theory of Algebraic Geometry Over Dedekind Rings II." Am. J. Math., Vol. 80 (1958), pp. 382 - 420.

6. Nagata, M.: Local Rings. Wiley, New York (1962).

7. Samuel, P.: "On Unique Factorization Domains." Illinois J. Math., Vol. 5 (1961), pp. 1 - 17.

8. Van der Waerden, B. L.: Modern Algebra Vol. I. Frederick Ungar Publishing Co., New York, 1949.

VITA

James Dean Harris

Born in Coffeyville, Kansas, February 9, 1943. Graduated from Field Kindley High School in that city, June 1961; A.B., Kansas University, February 1964. Employed at the National Aeronautics and Space Administration's Langley Research Center since July 1964.

In September 1965, the author entered the College of William and Mary as a graduate student majoring in mathematics.