

University of Montana

ScholarWorks at University of Montana

Graduate Student Theses, Dissertations, &
Professional Papers

Graduate School

1971

Algebraic approach to number theory

Francis Thomas Hannick
The University of Montana

Follow this and additional works at: <https://scholarworks.umt.edu/etd>

Let us know how access to this document benefits you.

Recommended Citation

Hannick, Francis Thomas, "Algebraic approach to number theory" (1971). *Graduate Student Theses, Dissertations, & Professional Papers*. 8200.
<https://scholarworks.umt.edu/etd/8200>

This Thesis is brought to you for free and open access by the Graduate School at ScholarWorks at University of Montana. It has been accepted for inclusion in Graduate Student Theses, Dissertations, & Professional Papers by an authorized administrator of ScholarWorks at University of Montana. For more information, please contact scholarworks@mso.umt.edu.

AN ALGEBRAIC APPROACH TO NUMBER THEORY

By

Francis T. Hannick

B.S., St. Martin's College, 1966


Presented in partial fulfillment of the requirements for the degree of

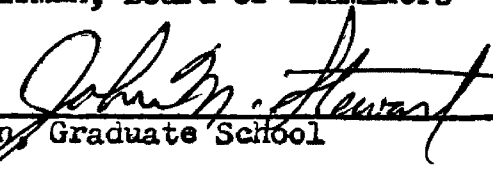
Master of Arts

UNIVERSITY OF MONTANA

1971

Approved by:


Chairman, Board of Examiners


Dean, Graduate School

Date Aug. 11, 1971

UMI Number: EP39001

All rights reserved

INFORMATION TO ALL USERS

The quality of this reproduction is dependent upon the quality of the copy submitted.

In the unlikely event that the author did not send a complete manuscript and there are missing pages, these will be noted. Also, if material had to be removed, a note will indicate the deletion.



UMI EP39001

Published by ProQuest LLC (2013). Copyright in the Dissertation held by the Author.

Microform Edition © ProQuest LLC.

All rights reserved. This work is protected against unauthorized copying under Title 17, United States Code



ProQuest LLC.
789 East Eisenhower Parkway
P.O. Box 1346
Ann Arbor, MI 48106 - 1346

ACKNOWLEDGEMENTS

I take this opportunity to express my gratitude to Professor Gloria Hewitt for her advice, guidance, and patience during the time this thesis was in preparation.

I wish to thank Professors Merle Manis, William Myers, and Randolph Jeppesen for their reading of the manuscript.

TABLE OF CONTENTS

| | Page |
|---|------|
| TABLE OF NOTATION | iv |
| LIST OF FIGURES | v |
| Chapter | |
| I. INTRODUCTION AND PRELIMINARIES | 1 |
| II. FACTORIZATION IN INTEGRAL DOMAINS | 3 |
| III. POLYNOMIAL RINGS AND FINITE FIELDS | 22 |
| IV. THE CHINESE REMAINDER THEOREM AND CONGRUENCES | 37 |
| LIST OF REFERENCES | 43 |

TABLE OF NOTATION

| | |
|-----------------|-----------------------------|
| \mathbb{Z} | the integers |
| \mathbb{N} | the natural numbers |
| \mathbb{Q} | the rational numbers |
| $A \subseteq B$ | A is contained in B |
| \subsetneq | proper containment |
| $R[x]$ | polynomials in x over R |
| R^* | field of quotients of R |

LIST OF FIGURES

| Figure | Page |
|--|------|
| 1. Relationship Between the Classes of Rings \mathcal{P} , \mathcal{N} , \mathcal{R} , and \mathcal{D} and the Class of Unique Factorization Domains | 15 |

CHAPTER I

INTRODUCTION AND PRELIMINARIES

This paper is divided into three parts. In the first, necessary and sufficient conditions are given for an element in an integral domain to admit a unique factorization into a product of irreducible elements. Rings in which every non-zero non-unit element admits such a factorization are called unique factorization domains (U.F.D.). In this first chapter, we consider the following special classes of rings: \mathcal{S} , the class of integral domains with identity; \mathcal{R} , the class of rings in \mathcal{S} which have the ascending chain condition (A.C.C.) on principal ideals; \mathcal{N} , the class of Noetherian rings in \mathcal{S} ; \mathcal{P} , the class of principal ideal domains (P.I.D.). It will be shown that the rings in \mathcal{P} are unique factorization domains. Rings in \mathcal{N} and \mathcal{R} have the property that every non-zero non-unit element admits a factorization into irreducibles, but this factorization is not necessarily unique. Finally, examples will be given to show that $\mathcal{P} \subset \mathcal{N} \subset \mathcal{R} \subset \mathcal{S}$.

The second section of the paper generalizes the notion of unique factorization domain to a polynomial ring over a unique factorization domain. We also generalize the Euler ϕ -function to integral domains, observing that $\phi(n)$ counts the number of units in $\mathbb{Z}/\langle n \rangle$. The final consideration of the chapter is finite fields. We characterize the structure of these fields, in that we show exactly how many elements they must possess and also that any two of them having the same number of elements are isomorphic.

The third section is a discussion of the Chinese Remainder

Theorem and congruences. The Chinese Remainder Theorem is seen to be a corollary of the major theorem of the section. Also, two special classes of rings, Bézout domains and Prüfer domains, are treated in some detail.

Throughout the paper, R is assumed to be an integral domain. An integral domain is a commutative ring with identity with no zero divisors. An ideal I of R is principal if there is a $a \in R$ such that $I = \{ra: r \in R\}$, denoted by $I = \langle a \rangle$. Note that since $1 \in R$, $\langle a \rangle$ is the smallest ideal of R containing a . R is a principal ideal domain if every ideal of R is principal. An ideal I of R is finitely generated if there are $a_1, a_2, \dots, a_n \in R$ such that $I = \left\{ \sum_{i=1}^n r_i a_i : r_i \in R \right\}$, denoted by $I = \langle a_1, a_2, \dots, a_n \rangle$. It is clear that a principal ideal of R is finitely generated, though we shall see later that the converse is false.

If A and B are sets, $\varphi: A \rightarrow B$, and if $C \subseteq A$, then $\varphi[C]$, the image of C under φ , is $\{\varphi(c): c \in C\}$. Also, if $D \subseteq B$, then $\varphi^{-1}[D]$, the inverse image of D , is $\{a \in A: \varphi(a) \in D\}$.

For $R \in \mathcal{S}$, I an ideal of R , and $a \in I$, we denote $I + a$ by \bar{a} . Also, if R has a finite number of elements, then we denote the number of elements of R by $|R|$. Finally, we denote the identity of R by 1_R , or, if no confusion will result, simply by 1 .

CHAPTER II

FACTORIZATION IN INTEGRAL DOMAINS

The main consideration of this chapter is the factorization of elements in an integral domain into products of irreducible elements.

Definition 1.1:

- 1) If $a, b \in R$, $a \neq 0$, then a divides b ($a|b$) if $\langle b \rangle \subseteq \langle a \rangle$.
- 2) $a \in R$ is a unit of R if there is $b \in R$ such that $ab = 1$.
(equivalently, $\langle a \rangle = \langle 1 \rangle$). We let $\mathcal{U}(R)$ denote the units of R .
- 3) $a, b \in R$ are associates ($a \sim b$) if there is $u \in \mathcal{U}(R)$ such that $a = ub$ (equivalently, $\langle a \rangle = \langle b \rangle$).
- 4) If $a, b \in R$, then a is a proper factor of b if $a|b$ and $a \not\sim b$ (equivalently, $\langle b \rangle \subsetneq \langle a \rangle$).
- 5) $a \in R$ is irreducible if $a \notin \mathcal{U}(R)$ and if $a = bc$, $b, c \in R$, then either $b \in \mathcal{U}(R)$ or $c \in \mathcal{U}(R)$.
- 6) $a \in R$ is prime if $a \neq 0$, $a \notin \mathcal{U}(R)$ and if $a|bc$, $b, c \in R$, then either $a|b$ or $a|c$.

Some results of the previous definition are given in the following.

Lemma 1.2:

- 1) If $a|b$ and $b|c$, then $a|c$.
- 2) $a|b$ iff $b = ac$ for some $c \in R$.
- 3) $a \in \mathcal{U}(R)$ iff $a^{-1} \in R$. It follows that $\mathcal{U}(R)$ is a group under multiplication.
- 4) \sim is an equivalence relation.

5) $a \sim b$ iff $a|b$ and $b|a$.

6) $a \in R$ is irreducible iff $a \notin \mathcal{U}(R)$ and $b|a$ implies $b \in \mathcal{U}(R)$ or $b \sim a$.

7) If $a \in R$ is prime, then $a|b_1 b_2 \dots b_n$ implies $a|b_i$ for some i .

8) if a is prime, then a is irreducible.

Proof: The proofs of properties (1) through (6) follow directly from Definition 1.1. The proof of property (8) also follows from the definition by using induction.

To show (8), we suppose $a = bc$, where $b, c \in R$. Then both $b|a$ and $c|a$. Now $\langle bc \rangle \subseteq \langle a \rangle$, so $a|bc$ and hence either $a|b$ or $a|c$. Thus either $a \sim b$ or $a \sim c$, and hence either $b \in \mathcal{U}(R)$ or $c \in \mathcal{U}(R)$. Also, since a is prime, note that $a \notin \mathcal{U}(R)$.

In general, the converse of Lemma 1.2 (8) is not true, as we see in the following example.

Example 1.3: Consider $Z[\sqrt{-5}] = \{a + b\sqrt{-5} : a, b \in Z\}$. Define $N(a + b\sqrt{-5}) = (a + b\sqrt{-5})(a - b\sqrt{-5}) = a^2 + 5b^2$. Then if $r, s \in Z[\sqrt{-5}]$, $N(rs) = N(r)N(s)$. Now $3 \in Z[\sqrt{-5}]$. If $3 = (a + b\sqrt{-5})(c + d\sqrt{-5})$, then $9 = N(3) = (a^2 + 5b^2)(c^2 + 5d^2)$, so $a^2 + 5b^2 \in \{1, 3, 9\}$. If $a^2 + 5b^2 = 1$, then $b = 0$ and $a = \pm 1$, so $a + b\sqrt{-5} = \pm 1$. If $a^2 + 5b^2 = 9$, then $c^2 + 5d^2 = 1$ and hence $c + d\sqrt{-5} = \pm 1$. Note that $a^2 + 5b^2 = 3$ has no solution in Z . Thus 3 is an irreducible element of $Z[\sqrt{-5}]$. Further, $3|(2 + \sqrt{-5})(2 - \sqrt{-5}) = 9$. Now if $2 + \sqrt{-5} = 3(a + b\sqrt{-5})$, then $3a = 2$ and $3b = 1$, a system having no solution in Z . Likewise, $2 - \sqrt{-5} = 3(c + d\sqrt{-5})$ leads to no solution. Thus $3 \nmid 2 + \sqrt{-5}$ and $3 \nmid 2 - \sqrt{-5}$, so 3 is not prime.

We now turn our attention to factorization in R .

Definition 1.4:

- 1) $a \in R$ admits a factorization into irreducible elements if there are irreducible elements $a_1, a_2, \dots, a_m \in R$ such that $a = a_1 a_2 \dots a_m$.
- 2) Such a factorization is unique if whenever $a = b_1 b_2 \dots b_n$ is also a factorization of a into irreducibles, then $m = n$ and for some rearrangement $b'_1 b'_2 \dots b'_m$ of $b_1 b_2 \dots b_m$, $a_i \sim b'_i$ for each i .
- 3) A ring R satisfying (1) and (2) for non-zero non-unit elements is called a unique factorization domain (U.F.D.).

Definition 1.5: A sequence of ideals $\{I_k\}_{k=0}^{\infty}$ is an increasing sequence if $I_k \subseteq I_{k+1}$ for $k \geq 0$.

Definition 1.6: R satisfies the ascending chain condition (A.C.C.) if, given an increasing sequence of ideals $\{I_k\}_{k=0}^{\infty}$ of R , there is $M \in \mathbb{Z}$, $M \geq 0$ such that $I_k = I_M$ for $k \geq M$.

The following theorem gives a sufficient condition for an element $a \in R$ to admit a factorization into a product of irreducibles.

Theorem 1.7: If $R \in \mathcal{R}$, then any non-zero non-unit element of R admits a factorization into irreducibles.

Proof: Suppose that $a \in R$, $a \neq 0$, $a \notin \mathcal{U}(R)$, and that a is not expressible as a product of irreducibles. Then a is not irreducible, so $a = a_1 b_1$, where both a_1 and b_1 are proper factors of a and not both a_1 and b_1 are expressible as a product of irreducibles. Choose c_1 to be one of a_1 and b_1 , where c_1 is not expressible as a product of irreducibles. Then c_1 is not irreducible, so $c_1 = a_2 b_2$, where both a_2 and b_2 are proper factors of c_1 and not both of a_2 and b_2 are expressible as a

product of irreducibles. Choose c_2 to be one of a_2 and b_2 , where c_2 is not expressible as a product of irreducibles. Now suppose that $c_0 = a$, c_1, c_2, \dots, c_{k-1} have each been defined so that c_j is a proper factor of c_{j-1} and so that c_{j-1} is not expressible as a product of irreducibles, $j = 1, 2, \dots, k-1$. Then c_{k-1} is not irreducible, so $c_{k-1} = a_k b_k$, where both a_k and b_k are proper factors of c_{k-1} and not both a_k and b_k are expressible as a product of irreducibles. Choose c_k to be one of a_k and b_k , where c_k is not expressible as a product of irreducibles. Thus by induction we have a sequence $c_0, c_1, c_2, \dots, c_k, \dots$ where each c_j is a proper factor of c_{j-1} , $j = 1, 2, \dots$. Further, $c_j \neq 0$ for $j = 0, 1, 2, \dots$. Thus $\langle c_0 \rangle \subsetneq \langle c_1 \rangle \subsetneq \dots \subsetneq \langle c_k \rangle \subsetneq \dots$, a contradiction.

We now point out a sufficient condition for elements of R to have a unique factorization into a product of irreducibles.

Lemma 1.8: If every irreducible element of R is prime, and if $a \in R$, $a \neq 0$, $a \notin \mathcal{U}(R)$ admits a factorization into irreducibles, then the factorization is unique.

Proof: Suppose that $a = p_1 p_2 \dots p_m = q_1 q_2 \dots q_n$, where the p_i and q_j are irreducible elements of R , $1 \leq i \leq m$, $1 \leq j \leq n$. Since $q_1 q_2 \dots q_n \in \langle p_1 \rangle$, $\langle q_1 q_2 \dots q_n \rangle \subseteq \langle p_1 \rangle$ and hence there is $i \in \mathbb{Z}$, $1 \leq i \leq n$ such that $p_1 \mid q_i$. We suppose $i = 1$. Then $q_1 = u_1 p_1$, where $u_1 \in \mathcal{U}(R)$. Note that if $u \in \mathcal{U}(R)$ and q is irreducible, then uq is irreducible.

We now proceed by induction on m . If $m = 1$, then by the above argument, $1 = u_1 q_2 \dots q_n$. If $n > 1$, then $q_n \in \mathcal{U}(R)$, which is contrary to q_n being irreducible. Thus $n = 1$ and $p_1 \sim q_1$. Now assume that the theorem is true for products with less than m factors. Then, by the above

argument, $p_2 \cdots p_m = u_1 q_2 \cdots q_n$. By the induction hypothesis, $m - 1 = n - 1$, and for a suitable arrangement of factors, $p_i \sim q_i$ for $i \geq 2$ and $p_2 \sim u_1 q_2 \sim q_2$. Therefore $m = n$ and $p_i \sim q_i$ for all $i \geq 1$.

Theorem 1.7 and Lemma 1.8 tell us that R is a U.F.D. if $R \in \mathcal{R}$ and if every irreducible element of R is prime. We now show the converse to these results.

Theorem 1.9: If R is a U.F.D., then $R \in \mathcal{R}$ and every irreducible element of R is prime.

Proof: Let $\{\langle a_i \rangle\}_{i=0}^{\infty}$ be an increasing sequence of principal ideals. If $a_0 \in \mathcal{U}(R)$, then $\langle a_0 \rangle = \langle 1 \rangle$ and hence $\langle a_i \rangle = \langle 1 \rangle = \langle a_0 \rangle$ for all i . Now suppose that $a_0 \neq 0$, $a_0 \notin \mathcal{U}(R)$, and that $\langle a_0 \rangle \subsetneq \langle a_1 \rangle \subsetneq \cdots$, $a_i \in R$. Then for each i , $a_i \notin \mathcal{U}(R)$. Now $a_i = b_1^{(i)} b_2^{(i)} \cdots b_{m_i}^{(i)}$, where the $b_j^{(i)}$ are all irreducible. Further, there are irreducibles $c_1^{(i)}, c_2^{(i)}, \dots, c_{p_i}^{(i)} \in R$ such that $b_1^{(i-1)} b_2^{(i-1)} \cdots b_{m_i-1}^{(i-1)} = (b_1^{(i)} b_2^{(i)} \cdots b_{m_i}^{(i)}) (c_1^{(i)} c_2^{(i)} \cdots c_{p_i}^{(i)})$, as $a_i = 1 \cdot a_i$. By unique factorization, $m_i - 1 = m_i + p_i$ and hence $m_i < m_i - 1$, $i = 1, 2, \dots$. But there are only a finite number of positive integers between m_0 and 0, so there is a positive integer M such that $\langle a_i \rangle = \langle a_M \rangle$ for $i \geq M$, a contradiction.

Now suppose that $p \in R$, p is irreducible, and that $p \mid ab$, where $a, b \in R$. Then there is $c \in R$ such that $ab = pc$. Since $p \notin \mathcal{U}(R)$, we have that not both of a and b are units. Suppose that $a \notin \mathcal{U}(R)$. If $b \in \mathcal{U}(R)$, then $a = pcb^{-1}$, so $p \mid a$. If $b \notin \mathcal{U}(R)$, then $a = a_1 a_2 \cdots a_m$, $b = b_1 b_2 \cdots b_n$, where the a_i and b_j are irreducible, $1 \leq i \leq m$, $1 \leq j \leq n$. Now $(a_1 a_2 \cdots a_m)(b_1 b_2 \cdots b_n) = pc$, so either $p \sim a_i$ for some i or $p \sim b_j$ for some j . Without loss of generality, suppose that $p \sim a_1$. Then $p \mid a_1$ and hence $p \mid a$.

We now summarize the last three results.

Theorem 1.10: R is a U.F.D. iff $R \in \mathcal{R}$ and every irreducible element of R is prime.

In order that we might find other conditions equivalent to R being a U.F.D., we now introduce the notions of greatest common divisor (g.c.d.) and least common multiple (l.c.m.).

Definition 1.11:

- 1) If $a, b \in R$, then $d \in R$ is the greatest common divisor of a and b ($d \sim (a, b)$) if $d|a$ and $d|b$ and whenever $c|a$ and $c|b$, then $c|d$.
- 2) If $a, b \in R$, then $m \in R$ is the least common multiple of a and b ($m \sim [a, b]$) if $a|m$ and $b|m$ and whenever $a|n$ and $b|n$, then $m|n$.

Remark 1.12: We note that the definition can be generalized to the greatest common divisor and least common multiple of a non-empty subset T of R .

The usual generalization from the integers of the notions of g.c.d. and l.c.m. to an integral domain R is given in terms of the ideal structure of R . If I and J are ideals of R , then $\text{g.c.d.}(I, J) = I + J$ and $\text{l.c.m.}(I, J) = I \cap J$. Lemma 1.14 gives conditions under which these definitions coincide with Definition 1.11. Observe that $d \sim (a, b)$ iff $\langle d \rangle$ is the smallest principal ideal containing $\langle a \rangle + \langle b \rangle$. Also, $m \sim [a, b]$ iff $\langle m \rangle = \langle a \rangle \cap \langle b \rangle$.

The notion of elements being "relatively prime" differs in these two generalizations. For example, using Definition 1.11 in $\mathbb{Z}[x]$, the elements 2 and x have g.c.d.1, while $\langle 2 \rangle + \langle x \rangle \neq \langle 1 \rangle$, as is shown in

Example 1.30.

Remark 1.13: If $a, b \in R$ and if $d \sim (a, b)$, $c \sim (a, b)$, then $d \sim c$. If $(a, b) \sim u \in \mathcal{U}(R)$, then $(a, b) \sim 1$.

Lemma 1.14: If $a, b \in R$, then

1) $\langle a \rangle + \langle b \rangle = \langle d \rangle$ implies $d \sim (a, b)$ and

2) $d \sim (a, b)$ implies $\langle a \rangle + \langle b \rangle = \langle d \rangle$ iff $\langle a, b \rangle$ is principal.

Proof: 1) If $\langle a \rangle + \langle b \rangle = \langle d \rangle$, then $a = 1 \cdot a + 0 \cdot b \in \langle d \rangle$, so $d|a$.

Likewise, $d|b$. If $c|a$ and $c|b$, then $\langle a \rangle \subseteq \langle c \rangle$ and $\langle b \rangle \subseteq \langle c \rangle$. Hence $\langle a \rangle + \langle b \rangle \subseteq \langle c \rangle$, so $\langle d \rangle \subseteq \langle c \rangle$ and $c|d$.

2) If $d \sim (a, b)$ and if $\langle a \rangle + \langle b \rangle = \langle d \rangle$, then clearly $\langle a \rangle + \langle b \rangle$ is principal. On the other hand, if $\langle a, b \rangle$ is principal, then there is $t \in R$ such that $\langle a \rangle + \langle b \rangle = \langle t \rangle$. But then (1) implies $t \sim (a, b)$, so $t \sim d$.

Lemma 1.15: If $a, b \in R$, then $m \sim [a, b]$ iff $\langle m \rangle = \langle a \rangle \cap \langle b \rangle$.

Proof: If $\langle m \rangle = \langle a \rangle \cap \langle b \rangle$, then clearly $a|m$ and $b|m$. If there is $x \in R$ such that $a|x$ and $b|x$, then $x \in \langle a \rangle$ and $x \in \langle b \rangle$, so $x \in \langle m \rangle$ and hence $m|x$.

Conversely, if $m \sim [a, b]$, then $a|m$ and $b|m$, so $m \in \langle a \rangle \cap \langle b \rangle$ and hence $\langle m \rangle \subseteq \langle a \rangle \cap \langle b \rangle$. If $x \in \langle a \rangle \cap \langle b \rangle$, then $a|x$ and $b|x$, so $m|x$ and hence $x \in \langle m \rangle$. Thus $\langle a \rangle \cap \langle b \rangle \subseteq \langle m \rangle$.

Lemma 1.16: If R is a U.F.D., then every pair of elements of R not both zero have a greatest common divisor in R , and this element is unique, up to associates.

Proof: Let $a, b \in R$, where not both of a and b is zero. If $b = 0$, then $a|a$ and $a|b$. Further, if $c|a$ and $c|b$, then since $c|a$ we have $(a, b) \sim a$.

Suppose $a \neq 0$ and $b \neq 0$. If $a \in \mathcal{U}(R)$, then $a|b$ and hence as

above, $(a, b) \sim a$. Thus suppose that neither a nor b are units. Then $a = p_1^{f_1} p_2^{f_2} \dots p_n^{f_n}$, $b = p_1^{e_1} p_2^{e_2} \dots p_n^{e_n}$, where the p_i are distinct irreducibles in R and $0 \leq f_i$, $0 \leq e_i$ for $1 \leq i \leq n$. Let $g_i = \min(e_i, f_i)$, and let $d = p_1^{g_1} p_2^{g_2} \dots p_n^{g_n}$. $g_i \leq e_i$ and $g_i \leq f_i$ implies $d|a$ and $d|b$. If $x|a$ and $x|b$, and if $x = v p_1^{u_1} p_2^{u_2} \dots p_n^{u_n} p_{n+1}^{u_{n+1}} \dots p_s^{u_s}$, where $v \in \mathcal{U}(R)$, then $u_{n+1} = \dots = u_s = 0$ and $u_i \leq e_i$, $u_i \leq f_i$ for $1 \leq i \leq n$, as R is a U.F.D. But then $u_i \leq g_i$, so $x|d$. By Remark 1.13, (a, b) is unique.

Remark 1.17: More generally, if R is a U.F.D. and if S is a finite non-empty subset of R , then an easy proof by induction shows that the g.c.d. of S exists.

Lemma 1.18: If every pair of elements of R not both zero has a greatest common divisor, and if $a, b, c \in R$ are non-zero, then

- 1) $(a, (b, c)) \sim ((a, b), c) \sim \text{g.c.d.}\{a, b, c\}$,
- 2) $c(a, b) \sim (ca, cb)$,
- 3) if $(a, b) \sim 1$, $(a, c) \sim 1$, then $(a, bc) \sim 1$, and
- 4) if $a \in R$ is irreducible, then a is prime.

Proof: 1) Suppose $d \sim \text{g.c.d.}\{a, b, c\}$, $d_1 \sim (b, c)$, $d_2 \sim (a, b)$. Since $d|b$ and $d|c$, we have $d|d_1$. If $f|a$ and $f|d_1$, then $f|b$ and $f|c$, so $f|d$. Thus $d \sim (a, (b, c))$. Similarly, we obtain $d \sim ((a, b), c)$.

2) Since $c(a, b)|ca$ and $c(a, b)|cb$, we have $c(a, b)|(ca, cb)$. Thus there is $r \in R$ such that $(ca, cb) \sim rc(a, b)$. Now $rc(a, b)|ca$ and $rc(a, b)|cb$, so since $c \neq 0$ we have $r(a, b)|a$ and $r(a, b)|b$. Thus $r(a, b)|(a, b)$, and hence $r \in \mathcal{U}(R)$.

3) Since $(a, b) \sim 1$, note that $(a, c) \sim (a, (a, b)c)$. Thus, from properties (1) and (2), we have $1 \sim (a, c) \sim (a, (a, b)c) \sim (a, (ac, bc)) \sim ((a, ac), bc) \sim (a, bc)$.

4) Let $p \in R$, p irreducible, and suppose $p|ab$, where $a, b \in R$. Then either $(p, a) \sim p$ or $(p, a) \sim 1$ and either $(p, b) \sim p$ or $(p, b) \sim 1$. If $(p, a) \sim 1$ and $(p, b) \sim 1$, then $(p, ab) \sim 1$. However, $p|ab$, so $(p, ab) \sim p$ and hence $p \sim 1$, a contradiction.

Remark 1.19: Suppose finitely generated ideals of R are principal. If $a|c$, $b|c$, and $(a, b) \sim 1$, then $ab|c$.

Summarizing the results of Lemma 1.16 and Lemma 1.18 (4), we now have the following necessary and sufficient conditions for R to be a U.F.D.

Theorem 1.20: R is a U.F.D. iff $R \in \mathcal{R}$ and every pair of elements of R not both zero has a greatest common divisor in R .

We now consider an example of a ring in which an element admits a factorization into irreducibles which is not unique.

Example 1.21: Consider once more $Z[\sqrt{-5}] = \{a + b\sqrt{-5} : a, b \in Z\}$. In $Z[\sqrt{-5}]$, $9 = 3 \cdot 3 = (2 + \sqrt{-5})(2 - \sqrt{-5})$. Recall that 3 is an irreducible element of $Z[\sqrt{-5}]$. If $2 + \sqrt{-5} = (a + b\sqrt{-5})(c + d\sqrt{-5})$, then $9 = N(2 + \sqrt{-5}) = (a^2 + 5b^2)(c^2 + 5d^2)$, so $a^2 + 5b^2 \in \{1, 3, 9\}$. If $a^2 + 5b^2 = 1$, then $a + b\sqrt{-5} = \pm 1$, and if $a^2 + 5b^2 = 9$, then $c + d\sqrt{-5} = \pm 1$. Further, $a^2 + 5b^2 = 3$ has no solution in Z . Thus $2 + \sqrt{-5}$ is an irreducible element of $Z[\sqrt{-5}]$, and in exactly the same manner, so is $2 - \sqrt{-5}$. Now by Example 1.3, $3 \not\sim 2 + \sqrt{-5}$ and $3 \not\sim 2 - \sqrt{-5}$, so we have exhibited two different factorizations of 9 into a product of irreducible elements of $Z[\sqrt{-5}]$.

We now show that there are $a, b \in Z[\sqrt{-5}]$, $a \neq 0$, $b \neq 0$ such that (a, b) does not exist. In so doing, we will exhibit cases in which Lemma 1.18 (2) and (3) does not hold.

By the argument used above, it is easy to show that $9 \in \mathbb{Z}[\sqrt{-5}]$ factors as $9 = 3 \cdot 3 = (-3)(-3) = (2 + \sqrt{-5})(2 - \sqrt{-5}) = (-2 - \sqrt{-5})(-2 + \sqrt{-5})$. Thus the possible values of $(9, 3(2 + \sqrt{-5}))$ are 1, 3, and $2 + \sqrt{-5}$. However, $3 \nmid 2 + \sqrt{-5}$ and $2 + \sqrt{-5} \nmid 3$, as we have already seen, so $(9, 3(2 + \sqrt{-5}))$ does not exist.

Now since $2 + \sqrt{-5}$ is irreducible, $(3, 2 + \sqrt{-5}) \sim 1$. However, $(3 \cdot 3, 3(2 + \sqrt{-5}))$ does not exist. Also, $(3, 2 + \sqrt{-5}) \sim 1$ and $(3, 2 - \sqrt{-5}) \sim 1$, but $(3, (2 + \sqrt{-5})(2 - \sqrt{-5})) \sim 3$.

We now turn our attention to some special classes of rings, first considering \mathcal{P} , the class of principal ideal domains. Recall that $R \in \mathcal{P}$ if every ideal of R is principal.

Lemma 1.22: If $R \in \mathcal{P}$, $a \in R$, then the following statements are equivalent.

- 1) a is irreducible.
- 2) $\langle a \rangle$ is a non-zero maximal ideal
- 3) $R/\langle a \rangle$ is a field.
- 4) $R/\langle a \rangle \in \mathcal{F}$.
- 5) $\langle a \rangle$ is a proper prime ideal.
- 6) a is prime.

Proof: (1) implies (2): If a is irreducible, then $a \neq 0$ and hence $\langle a \rangle \neq \langle 0 \rangle$. We suppose that there is $b \in R$ such that $\langle a \rangle \subsetneq \langle b \rangle \subseteq R$. Then $b \mid a$, so either $b \in \mathcal{U}(R)$ or $a \sim b$ by Lemma 1.2 (6). Hence either $\langle b \rangle = \langle 1 \rangle = R$ or $\langle a \rangle = \langle b \rangle$. Further, $a \notin \mathcal{U}(R)$, so $\langle a \rangle \neq R$.

(2) implies (3): Note that $R/\langle a \rangle$ is commutative and has an identity $\bar{1} = \langle a \rangle + 1$, as R has these properties. If $\bar{b} \in R/\langle a \rangle$, $\bar{b} \neq \bar{0}$, then $b \notin \langle a \rangle$ and hence $\langle a \rangle + \langle b \rangle = \langle 1 \rangle$, as $\langle a \rangle$ is maximal. Thus there are

$r, s \in R$ such that $1 = ra + sb$, so $\bar{s} \cdot \bar{b} = \bar{1}$.

(3) implies (4): If $R/\langle a \rangle$ is a field, then in particular $R/\langle a \rangle \in \mathcal{B}$.

(4) implies (5): Let us suppose that $c, d \in R$, $cd \in \langle a \rangle$. Then we have that $\overline{cd} = \bar{c} \cdot \bar{d} = \bar{0}$, and since $R/\langle a \rangle \in \mathcal{B}$, either $\bar{c} = \bar{0}$ or $\bar{d} = \bar{0}$. But then either $c \in \langle a \rangle$ or $d \in \langle a \rangle$. Furthermore, $\langle a \rangle \neq R$, since $\bar{1} \in R/\langle a \rangle$.

(5) implies (6): We suppose that $c, d \in R$ and that $a | cd$. Then $cd \in \langle a \rangle$, and since $\langle a \rangle$ is prime, either $c \in \langle a \rangle$ or $d \in \langle a \rangle$. Thus either $a | c$ or $a | d$. Moreover, $a \notin \mathcal{U}(R)$, as $\langle a \rangle \neq R$.

(6) implies (1): This result follows from Lemma 1.2 (8).

If $R \in \mathcal{P}$, then from Lemma 1.14 we note that every pair of elements of R , not both of which are zero, has a greatest common divisor. The following lemma, which shows that $\mathcal{P} \subseteq \mathcal{R}$, will enable us to say that R is a U.F.D.

Lemma 1.23: If $R \in \mathcal{P}$, then $R \in \mathcal{R}$.

Proof: Let $\{I_k\}_{k=0}^{\infty}$ be an increasing sequence of ideals of R , and let $I = \bigcup_{k=0}^{\infty} I_k$. Note that $I \neq \emptyset$, as $0 \in I_1 \subseteq I$. If $a, b \in I$, then there are $p, q \in \mathbb{Z}$ such that $a \in I_p$ and $b \in I_q$. Letting $r = \max(p, q)$, we have $a, b \in I_r$, so $a - b \in I_r \subseteq I$. If $r \in R$, $s \in I$, then there is $p \in \mathbb{Z}$ such that $s \in I_p$, so $rs \in I_p \subseteq I$. Thus I is an ideal of R , and hence there is $d \in R$ such that $I = \langle d \rangle$. Now $d \in I_t$ for some t , so $I = \langle d \rangle \subseteq I_t \subseteq I_j \subseteq I$ for all $j \geq t$. Therefore $I_j = I_t$ for $j \geq t$.

Theorem 1.24: If $R \in \mathcal{P}$, then R is a U.F.D.

Proof: Theorem 1.10, Lemma 1.22, and Lemma 1.23.

Let us now consider \mathcal{N} , the class of Noetherian rings, and some

conditions which are equivalent to Noetherian.

Definition 1.25: A ring R is Noetherian if the A.C.C. holds in R .

Definition 1.26: R satisfies the maximal condition if, for any non-empty set \mathcal{J} of ideals of R , there is $I \in \mathcal{J}$ such that if $J \in \mathcal{J}$ and $I \subseteq J$, then $I = J$. I is called a maximal element of \mathcal{J} .

Theorem 1.27: The following are equivalent.

- 1) R is Noetherian.
- 2) R satisfies the maximal condition.
- 3) Every ideal of R is finitely generated.

Proof: (1) implies (2): Suppose \mathcal{J} is a non-empty set of ideals of R , and suppose that no member of \mathcal{J} is maximal. Since \mathcal{J} is non-empty, there is $I_0 \in \mathcal{J}$. I_0 is not maximal, so there is $I_1 \in \mathcal{J}$ such that $I_0 \subsetneq I_1$. I_1 is not maximal, so there is $I_2 \in \mathcal{J}$ such that $I_1 \subsetneq I_2$. Suppose I_0, I_1, \dots, I_k have been defined so that $I_m \subsetneq I_{m+1}$, where I_m is not maximal, $0 \leq m \leq k-1$. Then I_k is not maximal, so there is $I_{k+1} \in \mathcal{J}$ such that $I_k \subsetneq I_{k+1}$. Hence we have a sequence $\{I_k\}_{k=0}^{\infty}$ such that $I_0 \subsetneq I_1 \subsetneq \dots \subsetneq I_k \subsetneq \dots$, a contradiction.

(2) implies (3): Suppose I is an ideal of R , and let \mathcal{J} be the set of all finitely generated ideals contained in I . $\langle 0 \rangle \in \mathcal{J}$, so $\mathcal{J} \neq \emptyset$. Let $I^* = \langle a_1, a_2, \dots, a_n \rangle$ be a maximal ideal in \mathcal{J} . Note that $I^* \subseteq I$. If $I^* \neq I$, then there is $a \in I$ such that $a \notin I^*$. Now $I^* + \langle a \rangle = \langle a_1, a_2, \dots, a_n, a \rangle \in \mathcal{J}$, and $I^* \subsetneq I^* + \langle a \rangle$. However, $a \in I^* + \langle a \rangle$ and $a \notin I^*$, so $I^* \neq I^* + \langle a \rangle$, a contradiction, so $I = I^*$.

(3) implies (1): Suppose $\{I_k\}_{k=0}^{\infty}$ is an increasing sequence of ideals of R . Letting $I = \bigcup_{k=0}^{\infty} I_k$, I is an ideal of R . By hypothesis, there are $a_1, a_2, \dots, a_n \in R$ such that $I = \langle a_1, a_2, \dots, a_n \rangle$. Moreover,

since $a_i \in I$ for each i , $1 \leq i \leq n$, there is $m_i \in \mathbb{Z}$ such that $a_i \in I_{m_i}$. Let $m = \max(m_1, m_2, \dots, m_n)$. Then $a_i \in I_m$ for each i , $1 \leq i \leq n$, so $I \subseteq I_m$. Thus $I_k \subseteq I_m \subseteq I_k$ for $k \geq m$, and hence $I_k = I_m$ for $k \geq m$.

If $R \in \mathcal{P}$, then note that by Lemma 1.23, $R \in \mathcal{N}$ and hence $\mathcal{P} \subseteq \mathcal{N}$. Further, if $R \in \mathcal{N}$, then R certainly has the A.C.C. on principal ideals, so $R \in \mathcal{R}$ and hence $\mathcal{N} \subseteq \mathcal{R}$. Theorem 1.24 tells us that if R is a P.I.D., then R is a U.F.D. Finally, if R is a U.F.D., then from Theorem 1.20 we have that $R \in \mathcal{R}$. This situation is clearly described in the following diagram.

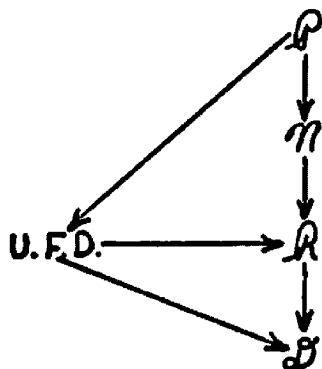


Figure 1

Relationship between the Classes of Rings
 \mathcal{P} , \mathcal{N} , \mathcal{R} , and \mathcal{D} and the Class of
 Unique Factorization Domains

We end this chapter with examples which show that the arrows in Figure 1 cannot be reversed nor can other arrows be added. We shall first show that $\mathcal{P} \subsetneq \mathcal{N}$. In so doing, we shall need to prove the Hilbert Basis Theorem, and to this end we first prove a lemma.

Lemma 1.28: Suppose \mathcal{A} is an ideal of $R[x]$, $i \in \mathbb{Z}$, $i \geq 0$, and let $\mathcal{L}_i(\mathcal{A}) = \{r \in R: r = 0 \text{ or } r \text{ is the leading coefficient of } p(x) \in \mathcal{A}, \deg p(x) = i\}$. Then $\{\mathcal{L}_i(\mathcal{A})\}_{i=0}^{\infty}$ is an increasing sequence of ideals of

R , and if \mathcal{B} is an ideal of $R[x]$ such that $\mathcal{A} \subseteq \mathcal{B}$ and $\mathcal{J}_i(\mathcal{A}) = \mathcal{J}_i(\mathcal{B})$, $i = 0, 1, 2, \dots$, then $\mathcal{A} = \mathcal{B}$.

Proof: $0 \in R$, so $0 \in \mathcal{J}_i(\mathcal{A})$ and hence $\mathcal{J}_i(\mathcal{A}) \neq \emptyset$. Suppose $r, s \in \mathcal{J}_i(\mathcal{A})$. If one or both of r and s is zero, it is clear that $r - s \in \mathcal{J}_i(\mathcal{A})$. If $r \neq 0, s \neq 0$, then there are $p(x), q(x) \in \mathcal{A}$ such that $p(x) = a_0 + \dots + a_{i-1}x^{i-1} + rx^i, q(x) = b_0 + \dots + b_{i-1}x^{i-1} + sx^i$. Now $p(x) - q(x) = (a_0 - b_0) + \dots + (a_{i-1} - b_{i-1})x^{i-1} + (r - s)x^i$, so $r - s \in \mathcal{J}_i(\mathcal{A})$. If $r \in \mathcal{J}_i(\mathcal{A}), m \in R$, and if $r = 0$, then $rm \in \mathcal{J}_i(\mathcal{A})$. If $r \neq 0$, then there is $p(x) \in \mathcal{A}, p(x) = a_0 + \dots + a_{i-1}x^{i-1} + rx^i$, and $m \cdot p(x) = ma_0 + \dots + ma_{i-1}x^{i-1} + mrx^i \in \mathcal{A}$, so $rm \in \mathcal{J}_i(\mathcal{A})$. Thus we have that $\mathcal{J}_i(\mathcal{A})$ is an ideal of R .

Now suppose $r \in \mathcal{J}_i(\mathcal{A})$. If $r = 0$, then $r \in \mathcal{J}_{i+1}(\mathcal{A})$. If $r \neq 0$, then there is $p(x) \in \mathcal{A}$ such that $p(x) = a_0 + \dots + a_{i-1}x^{i-1} + rx^i$. But $x \in R[x]$, so $x \cdot p(x) = a_0x + \dots + a_{i-1}x^i + rx^{i+1} \in \mathcal{A}$, and hence $r \in \mathcal{J}_{i+1}(\mathcal{A})$. Thus $\mathcal{J}_i(\mathcal{A}) \subseteq \mathcal{J}_{i+1}(\mathcal{A})$, so $\{\mathcal{J}_i(\mathcal{A})\}_{i=0}^{\infty}$ is an increasing sequence of ideals.

Now suppose \mathcal{B} is an ideal of $R[x]$, $\mathcal{A} \subseteq \mathcal{B}$, $\mathcal{J}_i(\mathcal{A}) = \mathcal{J}_i(\mathcal{B})$ for all i , and suppose $g(x) \in \mathcal{B}, g(x) \neq 0, \deg g(x) = i$. Then $g(x) = a_0 + \dots + a_{i-1}x^{i-1} + a_ix^i$, and since $a_i \in \mathcal{J}_i(\mathcal{B}), a_i \in \mathcal{J}_i(\mathcal{A})$. Then there is $f_i(x) \in \mathcal{A}$ such that $f_i(x) = b_0 + \dots + b_{i-1}x^{i-1} + a_ix^i$. Note that either $g(x) - f_i(x) = 0$ or $\deg(g(x) - f_i(x)) \leq i - 1$. If $g(x) - f_i(x) \neq 0$, then since $f_i(x) \in \mathcal{B}, g(x) - f_i(x) \in \mathcal{B}$. Now if $a_{i-1} - b_{i-1} = 0$, define $f_{i+1}(x) = 0$; otherwise define $f_{i+1}(x) = c_0 + \dots + c_{i-2}x^{i-2} + (a_{i-1} - b_{i-1})x^{i-1} \in \mathcal{A}$. Thus either $f_{i+1}(x) = 0$ or $\deg f_{i+1}(x) = i - 1$. Moreover, either $g(x) - f_i(x) - f_{i+1}(x) = 0$ or $\deg(g(x) - f_i(x) - f_{i+1}(x)) \leq i - 2$. By induction, we obtain

a sequence $\{f_i + f_j(x)\}$, $0 \leq j \leq i$, $f_i + f_j(x) \in \mathcal{A}$, such that each $f_i + f_j(x)$ is either 0 or of degree $i - j$ and such that $g(x) - f_i(x) - f_{i+1}(x) - \dots - f_{i+j}(x) = 0$ or $\deg(g(x) - f_i(x) - \dots - f_{i+j}(x)) \leq i - j - 1$, $0 \leq j \leq i - 1$. If $g(x) - f_i(x) - \dots - f_{2i-1}(x) \neq 0$, then $\deg(g(x) - f_i(x) - \dots - f_{2i-1}(x)) = 0$. But then $g(x) - f_i(x) - \dots - f_{2i-1}(x) - f_{2i}(x) = 0$, and so $g(x) = f_i(x) + f_{i+1}(x) + \dots + f_{i+k}(x)$, where $0 \leq k \leq i$. Thus $g(x) \in \mathcal{A}$, so $\mathcal{A} \subseteq \mathcal{B}$.

With this result, it is easy to prove the Hilbert Basis Theorem.

Theorem 1.29: If $R \in \mathcal{N}$, then $R[x] \in \mathcal{N}$ (and by induction, $R[x_1, x_2, \dots, x_n] \in \mathcal{N}$).

Proof: Let us suppose that $\{a_s\}_{s=0}^\infty$ is an increasing sequence of ideals of $R[x]$. We consider the double sequence $\{\mathcal{L}_i(a_j)\}$ of ideals of R . If i is fixed, then for $r \in \mathcal{L}_i(a_j)$ there is $p(x) = a_0 + \dots + a_{i-1}x^{i-1} + rx^i \in a_j \subseteq a_{j+1}$, so $r \in \mathcal{L}_i(a_{j+1})$ and hence $\{\mathcal{L}_i(a_j)\}$ is increasing. If j is fixed, then $\{\mathcal{L}_i(a_j)\}$ is increasing by Lemma 1.28. R is Noetherian, so let $\mathcal{L}_p(a_q)$ be a maximal element of the double sequence $\{\mathcal{L}_i(a_j)\}$. Note that $\mathcal{L}_p(a_0) \subseteq \mathcal{L}_p(a_1) \subseteq \dots \subseteq \mathcal{L}_p(a_{q-1}) \subseteq \mathcal{L}_p(a_q) \subseteq \dots$, so $\mathcal{L}_p(a_j) = \mathcal{L}_p(a_q)$ for $j \geq q$. But $\mathcal{L}_p(a_j) \subseteq \mathcal{L}_i(a_j)$ for $i \geq p$, so $\mathcal{L}_p(a_q) \subseteq \mathcal{L}_i(a_j)$ for $i \geq p$, $j \geq q$. Then by the maximality of $\mathcal{L}_p(a_q)$, $\mathcal{L}_p(a_q) = \mathcal{L}_i(a_j)$ for $i \geq p$, $j \geq q$.

Case (1): Suppose $i \geq p$. Then $\mathcal{L}_i(a_q) = \mathcal{L}_p(a_q)$. However, $\mathcal{L}_p(a_q) = \mathcal{L}_i(a_j)$ for $j \geq q$, so $\mathcal{L}_i(a_j) = \mathcal{L}_i(a_q)$ for $j \geq q$.

Case (2): Suppose $0 \leq i < p$. Then there is $n(i) \in \mathbb{Z}$ such that $\mathcal{L}_i(a_j) = \mathcal{L}_i(a_{n(i)})$ for $j \geq n(i)$, as R is Noetherian.

Now let $M = \max(n(0), n(1), \dots, n(p-1), q)$. Then for $i \in \mathbb{Z}$,

$i \geq 0$, we have $\mathcal{L}_i(a_j) = \mathcal{L}_i(a_M)$ for $j \geq M$. But then by Lemma 1.28, $a_j = a_M$ for $j \geq M$.

Example 1.30: Let us note that since $Z \in \mathcal{N}$, we have $Z[x] \in \mathcal{N}$ by the Hilbert Basis Theorem. However, consider $\langle x, 2 \rangle$, and suppose that there is $p(x) \in Z[x]$ such that $\langle x, 2 \rangle = \langle p(x) \rangle$. Let us recall that $\langle x, 2 \rangle = \{x \cdot m(x) + 2n(x) : m(x), n(x) \in Z[x]\}$. $2 \in \langle x, 2 \rangle$, so there is $q(x) \in Z[x]$ such that $p(x)q(x) = 2$. Thus $\deg p(x) = \deg q(x) = 0$, so $p(x) = m$, $q(x) = n$, where $m, n \in Z$. But then $mn = 2$, so $m = 2$ or $m = 1$. If $m = 2$, then $\langle x, 2 \rangle = \langle 2 \rangle$, so $x \in \langle 2 \rangle$. Then there is $q(x) \in Z[x]$ such that $x = 2q(x)$, so $2q_1 = 1$, where $q_1 \in Z$, a contradiction. If $m = 1$, then $\langle x, 2 \rangle = \langle 1 \rangle$, so $1 \in \langle x, 2 \rangle$ and hence there are $m(x), n(x) \in Z[x]$ such that $1 = x \cdot m(x) + 2n(x)$. But then $2n_0 = 1$, where $n_0 \in Z$, a contradiction. Thus $\langle x, 2 \rangle$ is not principal, and hence $Z[x] \notin \mathcal{P}$.

We shall now exhibit a ring R which has the A.C.C. on principal ideals yet which is not Noetherian. It will follow that the A.C.C. holding on principal ideals of a ring does not imply that it holds on arbitrary increasing sequences of the ring.

Example 1.31: Suppose F is a field and consider $F[x_1, x_2, \dots, x_n, \dots]$. Let $X = \{x_1, x_2, \dots, x_n, \dots\}$. Since $F \in \mathcal{S}$, we have $F[X] \in \mathcal{S}$, $F[X]$ being the union of integral domains. Note that $F[X] = \bigcup \{F[Y] : Y \text{ is a finite subset of } X\}$. Now let $\{\langle f_i \rangle : i = 1, 2, \dots\}$ be an increasing sequence of principal ideals, where $f_1 \neq 0$. For each p , choose Y_p such that $f_p \in F[Y_p]$ and such that Y_p is minimal. Let $x \in Y_p$. Write $f_p = U(T)x + V(T')$, where $x \notin T'$. By the minimality of Y_p , $U(T) \neq 0$. Now $f_p \mid f_1$, so there is $g_p \in F[X]$ such that $f_1 = g_p \cdot f_p$. We write $g_p = U'(S)x + V'(S')$, where $x \notin S'$. Then $f_1 = U'(S)U(T)x^2$

$+ U'(S)V(T')x + V'(S')U(T)x + V'(S')V(T') = 0$. Since $g_p \neq 0$, we have either $U'(S) \neq 0$ or $V'(S') \neq 0$. But then $x \in Y_1$, and hence $Y_p \subseteq Y_1$.

Thus $F[Y_p] \subseteq F[Y_1]$ for each p , and so $f_p \in F[Y_1]$ for each p . But by the Hilbert Basis Theorem, $F[Y_1]$ is Noetherian, so there is $M \in \mathbb{N}$ such that whenever $n \geq M$, $\langle f_n \rangle = \langle f_M \rangle$. Thus $F[X]$ has the A.C.C. on principal ideals, so $F[X] \in \mathcal{R}$.

However, note that $\langle x_1 \rangle \subsetneq \langle x_1, x_2 \rangle \subsetneq \dots \subsetneq \langle x_1, x_2, \dots, x_n \rangle \subsetneq \dots$. For if $f \in \langle x_1, x_2, \dots, x_k \rangle$, then $f = f_1x_1 + \dots + f_kx_k + 0 \cdot x_{k+1} \in \langle x_1, x_2, \dots, x_k, x_{k+1} \rangle$. Moreover, $x_{k+1} = 0 \cdot x_1 + \dots + 0 \cdot x_k + 1 \cdot x_{k+1} \in \langle x_1, x_2, \dots, x_k, x_{k+1} \rangle$, but $x_{k+1} \notin \langle x_1, x_2, \dots, x_k \rangle$. Thus we have $F[X] \notin \mathcal{N}$.

In Chapter II, we shall show that if R is a U.F.D., then so is $R[x]$. Using this fact, we observe that $F[X]$ is a U.F.D., so no arrow can be drawn from U.F.D. to \mathcal{N} .

Before considering our next example, we remind the reader of some of the concepts of extension fields. If F and K are fields, then K is an extension of F if K contains a subfield which is isomorphic to F . We shall write $F \hookrightarrow K$. Note that K is then a vector space over F , so we denote the dimension of K over F by $[K : F]$. K is a finite extension of F if $[K : F] < \infty$. An element $a \in K$ is algebraic over F if there are elements $b_0, b_1, \dots, b_n \in F$, not all zero, such that $b_0 + b_1a + \dots + b_na^n = 0$. Otherwise, a is transcendental over F . K is an algebraic extension of F if every element of K is algebraic over F . A basic result is that if K is an extension of F , then the set of all algebraic elements of K over F is a subfield of K . We shall use this result in the construction of our next example, which illustrates a ring R without

the A.C.C. on principal ideals. We assume it is known that the natural logarithm base, e , is transcendental over Q .

Lemma 1.32: $e^{m/n}$ is transcendental over Q , where $m, n \in \mathbb{Z}$, $m > 0$, $n \neq 0$.

Proof: If $n \in \mathbb{Z}$, $n \neq 0$, and if $e^{1/n}$ is algebraic over Q , then $(e^{1/n})^n = e$ is algebraic over Q . Hence $e^{1/n}$ is transcendental over Q . If $e^{m/n}$ is algebraic over Q , then there are $a_0, a_1, \dots, a_k \in Q$ not all zero such that $a_0 + a_1(e^{1/n})^m + a_2(e^{1/n})^{2m} + \dots + a_k(e^{1/n})^{km} = 0$, a contradiction.

Lemma 1.33: If $r_1, r_2, \dots, r_n \in Q$, then $\{e^{r_1}, e^{r_2}, \dots, e^{r_n}\}$ is independent over Q .

Proof: Suppose there are $a_1, a_2, \dots, a_n \in Q$ such that $a_1 e^{r_1} + a_2 e^{r_2} + \dots + a_n e^{r_n} = 0$. Then $a_1 e^{p_1/q} + a_2 e^{p_2/q} + \dots + a_n e^{p_n/q} = 0$, where q is a common denominator for r_1, r_2, \dots, r_n . Thus $a_1 (e^{1/q})^{p_1} + a_2 (e^{1/q})^{p_2} + \dots + a_n (e^{1/q})^{p_n} = 0$, and by Lemma 1.32, $a_1 = a_2 = \dots = a_n = 0$.

Example 1.34: Consider $\prod_{i=0}^{\infty} e^{10^{-i}} = (e)(e^{10^{-1}})(e^{10^{-2}}) \dots (e^{10^{-k}}) \dots = e^{1 + 10^{-1} + 10^{-2} + \dots + 10^{-k} + \dots} = e^{10/9}$. Further, let us consider $Q[Y]$, where $Y = \{e^{10^{-i}} : i = 0, 1, 2, \dots\} \cup \{(e^{10/9})/(\prod_{k=0}^n e^{10^{-k}}) : n = 1, 2, \dots\} \cup \{e^{10/9}\}$. We note that $Q[Y]$ is an integral domain with 1. Now $p_i = (e^{10/9})/(\prod_{k=0}^{i-1} e^{10^{-k}}) \in Q[Y]$, and $p_i = (p_{i+1})(e^{10^{-i}})$, $i = 1, 2, \dots$. Thus $p_{i+1} | p_i$, and hence $\langle p_i \rangle \subseteq \langle p_{i+1} \rangle$, $i = 1, 2, \dots$. If there is $g \in Q[Y]$ such that $p_{i+1} = g \cdot p_i$, then $g \cdot e^{10^{-i}} = 1$. Now $g = \sum_{\text{finite}} \alpha (k_1, \dots, k_n) e^{k_1 e^{10^{-1}} + \dots + k_n e^{10^{-n}} + 10^{-i}}$, $-1 = 0$, a contradiction by Lemma 1.33. Thus $p_{i+1} \notin \langle p_i \rangle$, $i = 1, 2, \dots$, and so $\langle p_1 \rangle \subsetneq \langle p_2 \rangle \subsetneq \dots \subsetneq \langle p_k \rangle \subsetneq \dots$. Hence $Q[Y] \nsubseteq R$.

Next we exhibit a ring R which is Noetherian yet which is not a U.F.D. Referring to Figure 1, this will tell us that no arrow can be drawn from \mathcal{N} to U.F.D., and hence none from either \mathcal{R} or \mathcal{B} to U.F.D.

Example 1.35: Recalling that $Z[x] \in \mathcal{N}$, we define $\psi: Z[x] \rightarrow Z[\sqrt{-5}]$ by $\psi(p(x)) = p(\sqrt{-5})$. It is clear that ψ is an onto homomorphism. Now if I is an ideal of $Z[\sqrt{-5}]$, then $\psi^{-1}[I]$ is an ideal of $Z[x]$, and since $Z[x] \in \mathcal{N}$, there are $a_1, a_2, \dots, a_n \in Z[x]$ such that $\psi^{-1}[I] = \langle a_1, a_2, \dots, a_n \rangle$. Since ψ is onto, $I = \psi[\psi^{-1}[I]] = \langle \psi(a_1), \psi(a_2), \dots, \psi(a_n) \rangle$, so $Z[\sqrt{-5}] \in \mathcal{N}$. We have seen in Example 1.21, however, that factorization in $Z[\sqrt{-5}]$ is not unique, so $Z[\sqrt{-5}]$ is not a U.F.D.

Finally, we consider an example of a ring R which is a U.F.D. but not a P.I.D. We know that Z is a U.F.D., as $Z \in \mathcal{P}$, so by our earlier remark $Z[x]$ is a U.F.D. However, in Example 1.30, we showed that $Z[x] \notin \mathcal{P}$. Thus we have that the arrow from \mathcal{P} to U.F.D. cannot be reversed, and hence we have considered all possibilities.

CHAPTER III

POLYNOMIAL RINGS AND FINITE FIELDS

This chapter is primarily concerned with finite fields and polynomial rings over fields.

Lemma 2.1: An element $a \in R$ is irreducible (or a unit) in $R[x]$ iff it is irreducible (or a unit) in R .

Proof: Suppose first that $a \in \mathcal{U}(R[x])$. Then there is $b(x) \in R[x]$ such that $a \cdot b(x) = 1$, and since $\deg b(x) = 0$, $b(x) \in R$ and hence $a \in \mathcal{U}(R)$.

On the other hand, if $a \in \mathcal{U}(R)$, then there is $c \in R$ such that $a \cdot c = 1$, and since $a, c \in R[x]$, $a \in \mathcal{U}(R[x])$.

Now if a is irreducible in $R[x]$, and if $a = pq$, where $p, q \in R$, then since $p, q \in R[x]$, either $p \in \mathcal{U}(R[x])$ or $q \in \mathcal{U}(R[x])$. Thus either $p \in \mathcal{U}(R)$ or $q \in \mathcal{U}(R)$, so a is irreducible in R .

Conversely, if a is irreducible in R , and if $a = r(x)s(x)$, where $r(x), s(x) \in R[x]$, then since $\deg r(x) = \deg s(x) = 0$, we have $r(x), s(x) \in R$. But then either $r(x) \in \mathcal{U}(R)$ or $s(x) \in \mathcal{U}(R)$, so either $r(x) \in \mathcal{U}(R[x])$ or $s(x) \in \mathcal{U}(R[x])$, and hence a is irreducible in $R[x]$.

In the following definition, we shall assume that (a, b) exists whenever $a, b \in R$ are not both zero.

Definition 2.2: $p(x) = a_0 + a_1x + \dots + a_nx^n \in R[x]$ is primitive if $(a_0, a_1, \dots, a_n) \in \mathcal{U}(R)$.

Remark 2.3: If $p(x) = a_0 + a_1x + \dots + a_nx^n \in R[x]$, then we can write $p(x) = d \cdot q(x)$, where $d \in R$ and $q(x)$ is primitive. Note that $d \sim (a_0, a_1, \dots, a_n)$. d is called the content of $p(x)$ and is denoted

by $c(p)$. Note further that $p(x)$ is primitive iff $c(p) \in \mathcal{U}(R)$.

Theorem 2.4: R is a U.F.D. iff $R[x]$ is a U.F.D.

Proof: We first suppose that $R[x]$ is a U.F.D. and that $a \in R$ is a non-zero non-unit. Then $a \in R[x]$ and $a \notin \mathcal{U}(R[x])$, so there are $p_1(x), p_2(x), \dots, p_n(x) \in R[x]$, $p_i(x)$ irreducible for $1 \leq i \leq n$, such that $a = p_1(x)p_2(x)\dots p_n(x)$. But $\deg p_i(x) = 0$, so $p_i(x)$ is irreducible in R for $1 \leq i \leq n$. Now each factorization of a in R is also a factorization in $R[x]$, a U.F.D., so the factorization is unique.

Conversely, suppose R is a U.F.D. and let $p(x) \in R[x]$, $p(x) \notin \mathcal{U}(R[x])$. We induct on $\deg p(x)$. If $\deg p(x) = 0$, then $p(x)$ factors uniquely as a product of irreducibles in R , as R is a U.F.D., and so likewise in $R[x]$. Now let us suppose that every non-unit polynomial of $R[x]$ of degree less than n can be factored uniquely as a product of irreducibles in $R[x]$. Let $\deg p(x) = n$, and write $p(x) = c(p)q(x)$, where $q(x)$ is primitive. $c(p) \in R$, so either $c(p) \in \mathcal{U}(R[x])$ or $c(p)$ can be factored uniquely as a product of irreducibles in $R[x]$. If $q(x)$ is irreducible, we are through. Otherwise, $q(x) = r(x)s(x)$, where $r(x), s(x) \notin \mathcal{U}(R[x])$ and where $\deg r(x) < n$, $\deg s(x) < n$, the latter since $q(x)$ is primitive. But then both $r(x)$ and $s(x)$ can be factored uniquely as a product of irreducibles in $R[x]$, and hence so can $q(x)$.

Remark 2.5: Since \mathbb{Z} is a U.F.D., we have that $\mathbb{Z}[x]$ is a U.F.D.

We now turn our attention to the generalization of the Euler ϕ -function.

Definition 2.6: For $n \in \mathbb{N}$, let $\phi(1) = 1$ and let $\phi(n)$ denote the number of positive integers less than n and relatively prime to n for $n > 1$. $\phi(n)$ is called the Euler ϕ -function. We shall let $\mathcal{P}(R)$ stand

for the number of units in R .

Remark 2.7: If $R = \sum_{k=1}^m \oplus A_k$, then $f \in \mathcal{U}(R)$ iff $f = (u_1, u_2, \dots, u_m)$, where $u_i \in \mathcal{U}(A_i)$ for $1 \leq i \leq m$. Thus $\bar{\rho}(R) = \prod_{k=1}^m \bar{\rho}(A_k)$ whenever each A_k has finitely many units.

Theorem 2.8: If every finitely generated ideal of R is principal, and if $p \in R$, where $p = q_1^{e_1} q_2^{e_2} \dots q_m^{e_m}$ is a factorization of p into irreducibles, then $R/p \simeq \sum_{k=1}^m \oplus R/\langle q_k^{e_k} \rangle$.

Proof: We define $\psi: R/\langle p \rangle \rightarrow \sum_{k=1}^m \oplus R/\langle q_k^{e_k} \rangle$ by $\psi(\langle p \rangle + r) = (\langle q_1^{e_1} \rangle + r, \langle q_2^{e_2} \rangle + r, \dots, \langle q_m^{e_m} \rangle + r)$. If $\langle p \rangle + r_1 = \langle p \rangle + r_2$, then $r_1 - r_2 \in \langle q_k^{e_k} \rangle$ for $1 \leq k \leq m$, so $\psi(\langle p \rangle + r_1) = \psi(\langle p \rangle + r_2)$ and hence ψ is well-defined.

Now $\psi[(\langle p \rangle + r_1) + (\langle p \rangle + r_2)] = \psi[\langle p \rangle + (r_1 + r_2)] = (\langle q_1^{e_1} \rangle + (r_1 + r_2), \dots, \langle q_m^{e_m} \rangle + (r_1 + r_2)) = (\langle q_1^{e_1} \rangle + r_1, \dots, \langle q_m^{e_m} \rangle + r_1) + (\langle q_1^{e_1} \rangle + r_2, \dots, \langle q_m^{e_m} \rangle + r_2) = \psi(\langle p \rangle + r_1) + \psi(\langle p \rangle + r_2)$. Likewise, $\psi[(\langle p \rangle + r_1)(\langle p \rangle + r_2)] = \psi(\langle p \rangle + r_1) \psi(\langle p \rangle + r_2)$, so ψ is a ring homomorphism.

If $\psi(\langle p \rangle + r_1) = \psi(\langle p \rangle + r_2)$, then $r_1 - r_2 \in \langle q_k^{e_k} \rangle$ for $1 \leq k \leq m$ and hence $r_1 - r_2 \in \langle p \rangle$ by Remark 1.19, since $(q_i^{e_i}, q_j^{e_j}) \sim 1$ for $i \neq j$. But then $\langle p \rangle + r_1 = \langle p \rangle + r_2$, so ψ is one-to-one.

We now show that ψ is onto. Let $\alpha_i = (\langle q_1^{e_1} \rangle + 0, \dots, \langle q_{i-1}^{e_{i-1}} \rangle + 0, \langle q_i^{e_i} \rangle + r_i, \langle q_{i+1}^{e_{i+1}} \rangle + 0, \dots, \langle q_m^{e_m} \rangle + 0)$, and let $s_i = \prod_{j \neq i} q_j^{e_j}$. $(s_i, q_i^{e_i}) \sim 1$, so there are $a, b \in R$ such that $as_i = r_i - bq_i^{e_i}$. We let $r'_i = as_i$. Then $\psi(r'_i) = \alpha_i$. Now suppose $\alpha = (\langle q_1^{e_1} \rangle + r_1, \langle q_2^{e_2} \rangle + r_2, \dots, \langle q_m^{e_m} \rangle + r_m) \in \sum_{k=1}^m \oplus R/\langle q_k^{e_k} \rangle$. Note that $\alpha = \sum_{i=1}^m \alpha_i$. Then letting $r = \sum_{i=1}^m r'_i$, we have $\psi(\bar{r}) = \sum_{i=1}^m \psi(r'_i) = \sum_{i=1}^m \alpha_i = \alpha$.

Our first use for this theorem will be in computing $\bar{\phi}(Z/\langle n \rangle)$, where $n > 1$.

Lemma 2.9: Let p be a prime integer. Then $\phi(p^k) = p^k - p^{k-1}$ for $k \geq 1$.

Proof: If $(n, p^k) \sim d \neq 1$, then since $d | p^k$, we have $d = p^m$, where $0 < m \leq k$. But then $p^m | n$, so $p | n$. Conversely, if $p | n$, then $(n, p^k) \sim 1$. Thus $0 \leq n < p^k$ and $(n, p^k) \sim 1$ iff $n = qp$, where $q = 0, 1, \dots, p^k - 1 - 1$, and there are $p^k - 1$ such representations for n .

Theorem 2.10: $\bar{\phi}(Z/\langle n \rangle) = \phi(n)$ for $n > 1$.

Proof: If $\bar{p} \in \mathcal{U}(Z/\langle n \rangle)$, then there is $\bar{q} \in Z/\langle n \rangle$ such that $p\bar{q} \equiv 1 \pmod{n}$, so $n | p\bar{q} - 1$. Thus there is $r \in Z$ such that $p\bar{q} - nr = 1$. If $(p, n) \sim d$, then there are $a, b \in Z$ such that $p = da$, $n = db$, and hence $daq - dbr = d(aq - br) = 1$, so $d = 1$.

On the other hand, if $(p, n) \sim 1$, then there are $a, b \in Z$ such that $ap + bn = 1$, so $ap \equiv 1 \pmod{n}$ and hence $\bar{p} \in \mathcal{U}(Z/\langle n \rangle)$. Note that only values of p for which $0 < p < n$ need to be considered. Thus $\bar{\phi}(Z/\langle n \rangle) = \phi(n)$.

Corollary 2.11: If $n = \prod_{k=1}^m p_k^{e_k}$, where p_k is prime for $1 \leq k \leq m$, then $\bar{\phi}(Z/\langle n \rangle) = \prod_{k=1}^m p_k^{e_k} - 1(p_k - 1)$.

Proof: $Z/\langle n \rangle \cong \sum_{k=1}^m \oplus Z/\langle p_k^{e_k} \rangle$, so $\bar{\phi}(Z/\langle n \rangle) = \prod_{k=1}^m \bar{\phi}(Z/\langle p_k^{e_k} \rangle) = \prod_{k=1}^m \phi(p_k^{e_k})$.

Theorem 2.8 also gives us the well-known fact that $\phi(n)$ is a multiplicative function.

Corollary 2.12: If $a, b \in N$, $(a, b) \sim 1$, then $\phi(ab) = \phi(a)\phi(b)$.

Proof: Suppose $a = \prod_{k=1}^m p_k^{e_k}$ and $b = \prod_{k=m+1}^n p_k^{e_k}$ are factorizations of a and b into products of powers of primes. We note that $p_i \neq p_j$ for

$$\begin{aligned}
i \neq j, \text{ where } 1 \leq i \leq n, 1 \leq j \leq n. \text{ Now } \phi(ab) &= \bar{\phi}(Z/\langle \prod_{k=1}^n p_k^{e_k} \rangle) \\
&= \bar{\phi}(\sum_{k=1}^n \theta Z/\langle p_k^{e_k} \rangle) = \prod_{k=1}^n \bar{\phi}(Z/\langle p_k^{e_k} \rangle) = \prod_{k=1}^n \bar{\phi}(Z/\langle p_k^{e_k} \rangle) \prod_{k=n+1}^n \bar{\phi}(Z/\langle p_k^{e_k} \rangle) \\
&= \bar{\phi}(\sum_{k=1}^n \theta Z/\langle p_k^{e_k} \rangle) \bar{\phi}(\sum_{k=n+1}^n \theta Z/\langle p_k^{e_k} \rangle) = \bar{\phi}(Z/\langle \prod_{k=1}^n p_k^{e_k} \rangle) \bar{\phi}(Z/\langle \prod_{k=n+1}^n p_k^{e_k} \rangle) \\
&= \bar{\phi}(Z/\langle a \rangle) \bar{\phi}(Z/\langle b \rangle) = \phi(a)\phi(b).
\end{aligned}$$

We now suppose that $h: R \rightarrow S$ is a ring homomorphism, where $R, S \in \mathcal{S}$. Then if $x \in \mathcal{U}(R)$ and h is not the zero map, it follows that $h(x) \in \mathcal{U}(S)$, as $h(1)$ is the identity for S . The converse, however, is false, as we shall see in the following example.

Example 2.13: Let $R = \mathbb{Z}$, $S = \mathbb{Z}/\langle 5 \rangle$, and let $\pi: \mathbb{Z} \rightarrow \mathbb{Z}/\langle 5 \rangle$ be the natural map. Then $4 \in \mathcal{U}(\mathbb{Z}/\langle 5 \rangle)$, but $4 \notin \mathcal{U}(\mathbb{Z})$.

On the other hand, the following are cases in which the converse is true.

Example 2.14: Consider $\mathbb{Z} \xrightarrow{\pi} \mathbb{Z}/\langle p^n \rangle = R \xrightarrow{\bar{\pi}} R/A$, where π and $\bar{\pi}$ are the natural maps, p is a prime integer, and $A = \langle \langle p^n \rangle + p \rangle$. Since $\bar{\pi}$ is not the zero map, we clearly have $\bar{\pi}(\bar{x}) \in \mathcal{U}(R/A)$ if $\bar{x} \in \mathcal{U}(R)$. If $\bar{\pi}(\bar{x}) \in \mathcal{U}(R/A)$, then using the onto-ness of $\bar{\pi}$, there is $\bar{y} \in R$ such that $\bar{\pi}(\bar{x})\bar{\pi}(\bar{y}) = \bar{\pi}(1)$. Thus $A + \overline{xy} = \bar{\pi}(1) = A + \bar{1}$, so $\overline{xy - 1} \in A$. But then there is $a \in \mathbb{Z}$ such that $\langle p^n \rangle + (xy - 1) = \langle p^n \rangle + ap$, and hence there is $b \in \mathbb{Z}$ such that $xy - 1 - ap = bp^n$. Thus $p \nmid x$, so $(x, p^n) \sim 1$. Now there are $r, s \in \mathbb{Z}$ such that $rx + sp^n = 1$, so $\bar{x} \cdot \bar{r} = \bar{1}$ and $\bar{x} \in \mathcal{U}(R)$. Thus we have shown that $\bar{x} \in \mathcal{U}(R)$ iff $\bar{\pi}(\bar{x}) \in \mathcal{U}(R/A)$.

Example 2.15: For $R \in \mathcal{S}$, we let A be the ideal of nilpotent elements of R , $\pi: R \rightarrow R/A$ be the natural map. Since π is not the zero map, $x \in \mathcal{U}(R)$ implies $\pi(x) \in \mathcal{U}(R/A)$. If $\pi(x) \in \mathcal{U}(R/A)$, then there is $\pi(y) \in R/A$ such that $\pi(x)\pi(y) = \pi(1)$. Thus $xy - 1 \in A$, so there is $a \in A$ such that $xy - 1 = a$. Also, there is $n \in \mathbb{Z}$ such that $a^n = 0$, so

$(xy - 1)^n = 0$. But $R \in \mathcal{D}$, so $xy - 1 = 0$ and hence $x \in \mathcal{U}(R)$. Therefore $x \in \mathcal{U}(R)$ iff $\pi(x) \in \mathcal{U}(R/A)$.

Example 2.16: We consider once again $Z \xrightarrow{\pi} Z/\langle p^n \rangle = R \xrightarrow{\bar{\pi}} R/A$, where $A = \langle \langle p^n \rangle + p \rangle$, π and $\bar{\pi}$ are the natural maps, and p is a prime integer. Note that $\psi = \bar{\pi} \circ \pi$ is a homomorphism of Z onto R/A , where \circ is the composition of $\bar{\pi}$ and π . If $a \in \ker \psi$, then $A = \bar{\pi}(\pi(a)) = \bar{\pi}(\bar{a}) = A + \bar{a}$, so $\bar{a} \in A$. Thus there is $b \in Z$ such that $a - bp \in \langle p^n \rangle$. But then $p|a$, so $a \in \langle p \rangle$.

Conversely, if $a \in \langle p \rangle$, then $\bar{a} = \langle p^n \rangle + a \in A$, so $\bar{\pi}(\bar{a}) = A$ and hence $a \in \ker \psi$.

Therefore we have $Z/\langle p \rangle \cong R/A$, so $\bar{\phi}(R/A) = \phi(p) = p - 1$.

For finite rings R , the next result will give us the relationship between $\bar{\phi}(R)$ and the number of units in a factor ring of R .

Theorem 2.17: If R is finite and A an ideal of R such that $\pi(x) \in \mathcal{U}(R/A)$ iff $x \in \mathcal{U}(R)$, where $\pi: R \rightarrow R/A$ is the natural homomorphism, then $\bar{\phi}(R) = |A| \bar{\phi}(R/A)$.

Proof: For each $\pi(x) \in \mathcal{U}(R/A)$, there are $|A|$ elements $y \in R$ such that $\pi(x) = \pi(y)$. Hence there are $|A|$ distinct elements of $\mathcal{U}(R)$ which map onto a given element $\pi(x) \in \mathcal{U}(R/A)$, as $\pi[\mathcal{U}(R)] = \mathcal{U}(R/A)$. Thus $\bar{\phi}(R) = |A| \bar{\phi}(R/A)$.

Remark 2.18: In Example 2.16, this result may also be obtained by the following argument. Recall that $\bar{\phi}(R/A) = p - 1$. Also, $R = Z/\langle p^n \rangle$, so $\bar{\phi}(R) = \phi(p^n) = p^n - p^{n-1}$. Now $A = \langle \langle p^n \rangle + p \rangle = \{ \langle p^n \rangle + p, \langle p^n \rangle + 2p, \dots, \langle p^n \rangle + (p^{n-1} - 1)p, \langle p^n \rangle + p^{n-1} \cdot p \}$, so $|A| = p^{n-1}$. Since $p^n - p^{n-1} = p^{n-1}(p - 1)$, $\bar{\phi}(R) = |A| \bar{\phi}(R/A)$.

We now suppose that F is a finite field with $|F| = m$ and we com-

pute $\bar{\phi}(F[x]/\langle p(x) \rangle)$, where $p(x) \in F[x]$. If $p(x) = 0$, then $F[x]/\langle p(x) \rangle \simeq F[x]$ and hence $\bar{\phi}(F[x]/\langle p(x) \rangle) = m - 1$. Further, if $p(x) \in \mathcal{U}(F[x])$, Then $F[x]/\langle p(x) \rangle \simeq \{0\}$, so $\bar{\phi}(F[x]/\langle p(x) \rangle) = 0$. Thus in the following we shall suppose that $p(x) \neq 0$ and $p(x) \notin \mathcal{U}(F[x])$.

Lemma 2.19: If $p(x) \in F[x]$, then $\mathcal{U}(F[x]/\langle p(x) \rangle) = \{\overline{g(x)} \in F[x]/\langle p(x) \rangle : (g(x), p(x)) \sim 1\}$.

Proof: Let $S = \{\overline{g(x)} \in F[x]/\langle p(x) \rangle : (g(x), p(x)) \sim 1\}$. If $\overline{g(x)} \in S$, then there are $m(x), n(x) \in F[x]$ such that $g(x)m(x) + p(x)n(x) = 1$, since $F[x] \in \mathcal{P}$. Thus $\overline{g(x)m(x)} = \bar{1}$, so $\overline{g(x)} \in \mathcal{U}(F[x]/\langle p(x) \rangle)$.

Conversely, if $\overline{g(x)} \in \mathcal{U}(F[x]/\langle p(x) \rangle)$, then there is $h(x) \in F[x]/\langle p(x) \rangle$ such that $\overline{g(x)h(x)} = \bar{1}$, so $g(x)h(x) - 1 \in \langle p(x) \rangle$. But then there is $q(x) \in F[x]$ such that $g(x)h(x) + p(x)q(x) = 1$, so $(g(x), p(x)) \sim 1$ and hence $g(x) \in S$.

Definition 2.20: For $p(x) \in F[x]$, $p(x) \neq 0$, and $p(x) \notin \mathcal{U}(F[x])$, define $\phi(p(x)) = \bar{\phi}(F[x]/\langle p(x) \rangle)$.

Theorem 2.21: If $p(x) \in F[x]$, $p(x) \neq 0$, and $p(x) \notin \mathcal{U}(F[x])$, then $\phi(p(x))$ is the number of elements $g(x) \in F[x]$ such that $(g(x), p(x)) \sim 1$ and $0 \leq \deg g(x) < \deg p(x)$.

Proof: If $\overline{g(x)} \in F[x]/\langle p(x) \rangle$, then we may assume that $0 \leq \deg g(x) < \deg p(x)$. The result is now immediate by Lemma 2.19.

Lemma 2.22: If $p(x) \in F[x]$ is irreducible and $\deg p(x) = n$, then $\phi(p(x)) = m^n - 1$.

Proof: There are m^n choices for $g(x) \in F[x]$ such that $0 \leq \deg g(x) < \deg p(x)$ or $g(x) = 0$, and if $(g(x), p(x)) \sim 1$, then $g(x) \neq 0$.

Lemma 2.23: If $q(x) \in F[x]$ is irreducible, $p(x) = q(x)^k$ for $k \in \mathbb{N}$, and if $\deg p(x) = n$, then $\phi(p(x)) = m^n - m^{n(k-1)}/k$.

Proof: If $(g(x), q(x)^k) \sim h(x)$, where $\deg h(x) > 0$, then since $F[x] \in \mathcal{P}$ and hence is a U.F.D., $h(x) \sim q(x)^s$, $1 \leq s \leq k$. But then $q(x) | g(x)$, so there is $r(x) \in F[x]$ such that $g(x) = q(x)r(x)$. On the other hand, if $g(x) = q(x)r(x)$, then $(g(x), q(x)^k) \sim 1$.

Now let us consider $\{g(x) \in F[x]: 0 \leq \deg g(x) < n \text{ or } g(x) = 0, (g(x), q(x)^k) \sim 1\}$. There are m^n choices for $g(x)$ satisfying $0 \leq \deg g(x) < \deg p(x)$ or $g(x) = 0$. For $g(x) = q(x)r(x)$, it follows that either $r(x) = 0$ or $\deg r(x) = \deg g(x) - \deg q(x) \leq (n-1) - n/k = (kn - k - n)/k$. Thus there are $m^{\lfloor (kn - k - n)/k \rfloor + 1} = m^{n(k-1)/k}$ choices for $r(x)$, and hence for $g(x)$, such that $(g(x), q(x)^k) \sim 1$. But then $\phi(p(x)) = m^n - m^{n(k-1)/k}$.

Corollary 2.24: If $p(x) \in F[x]$, $p(x) \neq 0$, $p(x) \notin \mathcal{U}(F[x])$, then $\bar{\phi}(F[x]/\langle p(x) \rangle) = \prod_{k=1}^n (m^{e_k \deg q_k(x)} - m^{(e_k - 1) \deg q_k(x)})$, where $p(x) = \prod_{k=1}^n q_k(x)^{e_k}$ is the factorization of $p(x)$ into a product of powers of irreducibles.

Proof: Since $F[x]/\langle p(x) \rangle \cong \sum_{k=1}^n \oplus F[x]/\langle q_k(x)^{e_k} \rangle$ by Theorem 2.8, we have by Remark 2.7 that $\bar{\phi}(F[x]/\langle p(x) \rangle) = \prod_{k=1}^n \bar{\phi}(F[x]/\langle q_k(x)^{e_k} \rangle)$. Thus $\bar{\phi}(F[x]/\langle p(x) \rangle) = \prod_{k=1}^n \phi(q_k(x)^{e_k}) = \prod_{k=1}^n (m^{e_k \deg q_k(x)} - m^{e_k \deg q_k(x)(e_k - 1)/e_k}) = \prod_{k=1}^n (m^{e_k \deg q_k(x)} - m^{(e_k - 1) \deg q_k(x)})$.

Remark 2.25: If $p(x), q(x) \in F[x]$, $p(x) \neq 0$, $p(x) \notin \mathcal{U}(F[x])$, $q(x) \neq 0$, and $q(x) \notin \mathcal{U}(F[x])$, and if $(p(x), q(x)) \sim 1$, then by Theorem 2.8 it is clear that $\phi(p(x)q(x)) = \phi(p(x))\phi(q(x))$.

We now summarize the results about $\mathcal{U}(F[x]/\langle p(x) \rangle)$.

Theorem 2.26: Suppose F is a finite field with $|F| = m$, and suppose $p(x) \in F[x]$.

1) If $p(x) = 0$, then $\bar{\phi}(F[x]/\langle p(x) \rangle) = m - 1$.

- 2) If $\deg p(x) = 0$, then $\bar{\phi}(F[x]/\langle p(x) \rangle) = 0$.
- 3) If $\deg p(x) > 0$, then $\bar{\phi}(F[x]/\langle p(x) \rangle) = \prod_{k=1}^n (m^{e_k \deg q_k(x)} - m^{(e_k - 1) \deg q_k(x)})$, where $p(x) = \prod_{k=1}^n q_k(x)^{e_k}$ is the factorization of $p(x)$ into a product of powers of irreducibles.

We conclude this chapter by characterizing the finite fields.

In so doing, we introduce the notion of prime field. Throughout the discussion, the symbol P is used to denote the prime field of F . Though we assume that the reader has a basic understanding of the elements of Galois theory, we recall at this time some of the ideas we will be using. If F is a field and $f(x) \in F[x]$, then a finite extension E of F is a splitting field for $f(x)$ over F if $f(x)$ has all its roots in E but in no proper subfield of E . We state, without proof, the uniqueness theorem for splitting fields.

Theorem 2.27: If F and F' are fields such that $F \cong F'$, then τ extends to an isomorphism $F[x] \xrightarrow{\tau^*} F'[x]$. If $f(x) \in F[x]$, and if E is the splitting field of $f(x)$ over F , E' is the splitting field of $\tau^*(f(x))$ over F' , then $E \cong E'$.

Definition 2.28: A prime field is a field having no proper subfields.

It is clear from the definition that a prime field is minimal. Given a field F , one can ask if F possesses a minimal subfield.

Theorem 2.29: Every field F contains a unique prime field P , namely $P = \bigcap \{G: G \text{ is a subfield of } F\}$.

An essential concept in our discussion of fields is that of characteristic.

Definition 2.30: If F is a field, then F is of characteristic

zero if $n \in \mathbb{Z}$, $n \cdot 1_F = 0$ implies $n = 0$. If for some $n \in \mathbb{N}$, $n \cdot 1_F = 0$, then F is of finite characteristic. In this case, the characteristic of F is the least positive integer such that $n \cdot 1_F = 0$. We denote the characteristic of F by $\chi(F)$.

Remark 2.31: If $\chi(F) = n$, then $n \cdot a = 0$ for every $a \in F$.

Further, $\chi(F)$ is either 0 or a prime number p .

Lemma 2.32: $\chi(F) = p$ iff $P \cong \mathbb{Z}/\langle p \rangle$.

Proof: Suppose $\chi(F) = p$. $G = \{n \cdot 1_F : n \in \mathbb{Z}\} \subseteq P$, and clearly G is a ring with 1. We define $\psi : \mathbb{Z} \rightarrow G$ by $\psi(n) = n \cdot 1_F$. ψ is an onto ring homomorphism, and $n \cdot 1_F = 0$ iff $n \in \langle p \rangle$, so $\ker \psi = \langle p \rangle$ and hence $G \cong \mathbb{Z}/\langle p \rangle$. Now $\langle p \rangle$ is a maximal ideal of \mathbb{Z} , so G is a field and hence $\mathbb{Z}/\langle p \rangle \cong G = P$.

On the other hand, suppose $P \cong \mathbb{Z}/\langle p \rangle$. $1 \in P$, and $\sigma(p \cdot 1) = p \cdot \bar{1} = \bar{0} = \sigma(0)$, so $p \cdot 1 = 0$. If $q \cdot 1 = 0$ for $q \in \mathbb{Z}$, then $\sigma(q \cdot 1) = q \sigma(1) = q(\langle p \rangle + 1) = \langle p \rangle + q = \bar{0}$, so $q \in \langle p \rangle$ and hence $\chi(F) = p$.

Theorem 2.33: If $\chi(F) = p$ and $[F : P] = n$, then $|F| = p^n$.

Proof: Since $P \cong \mathbb{Z}/\langle p \rangle$, $[F : \mathbb{Z}/\langle p \rangle] = n$ and so $|F| = p^n$.

Remark 2.34: $\chi(F) = 0$ iff $P \cong \mathbb{Q}$.

Proof: If $P \cong \mathbb{Q}$, $n \in \mathbb{Z}$, and if $n \cdot 1_F = 0$, then $n \cdot (1_F) = n \cdot 1_{\mathbb{Q}} = 0$, so $n = 0$ and $\chi(F) = 0$.

Conversely, if $\chi(F) = 0$, then $G = \{n \cdot 1_F : n \in \mathbb{Z}\} \subseteq P$. Let us define $\sigma : \mathbb{Z} \rightarrow G$ by $\sigma(n) = n \cdot 1_F$. σ is a ring homomorphism and $\ker \sigma = \langle 0 \rangle$, so $G \cong \mathbb{Z}/\langle 0 \rangle \cong \mathbb{Z}$. Now P contains the multiplicative inverse of every non-zero element of G , so P contains a subfield G' such that $G' \cong \mathbb{Q}$. But $G' \subseteq P \subseteq F$, so $G' = P$ and hence $P \cong \mathbb{Q}$.

We now turn our attention to the multiplicative structure of F .

The result we need concerns finite multiplicative subgroups of F , and to this end we prove some preliminary remarks.

Lemma 2.35: If G is a finite abelian group, p a prime number, and if $p \mid o(G)$, then G has an element of order p .

Proof: The proof is by induction on the order of G . If $o(G) = 1$, the result is vacuously true. Let us suppose the result is true for all finite abelian groups of order less than $o(G)$. Let $x \in G$, $x \neq 1$. If there is $m \in \mathbb{Z}$ such that $o(x) = pm$, then $o(x^m) = p$ and we are through. Now suppose $o(x) = t$, where $(p, t) \sim 1$. Then $\langle x \rangle$ is a normal subgroup of G of order t , so $G/\langle x \rangle$ is an abelian group of order $o(G)/t < o(G)$. Further, since $(p, t) \sim 1$ and $p \mid o(G)$, we have $p \mid o(G)/t$, so there is $\bar{y} \in G/\langle x \rangle$ such that $o(\bar{y}) = p$. Now consider $\pi: G \rightarrow G/\langle x \rangle$, where π is the natural map. Then $\bar{y}^{o(y)} = y^{o(y)}\langle x \rangle = \langle x \rangle$, so $p \mid o(y)$. Thus there is $k \in \mathbb{Z}$ such that $o(y) = pk$, and hence $o(y^k) = p$.

Remark 2.36: Suppose G is an abelian group, $x, y \in G$ are of finite order, and suppose $\langle x \rangle \cap \langle y \rangle = \{1\}$. Then $o(xy) = \text{l.c.m. } \{o(x), o(y)\}$ (may be extended by induction).

Proof: Let $t = \text{l.c.m. } \{o(x), o(y)\}$. Then $o(x) \mid t$ and $o(y) \mid t$, so $(xy)^t = x^t y^t = 1 \cdot 1 = 1$. If $(xy)^s = 1$, then $x^s = y^{-s} \in \langle x \rangle \cap \langle y \rangle$, so $x^s = y^s = 1$ and hence $o(x) \mid s$, $o(y) \mid s$. But then $t \mid s$, so $o(xy) = t$.

Theorem 2.37: Let F be a field, G a finite multiplicative subgroup of F . Then G is cyclic.

Proof: We suppose that $o(G) = n = p_1^{s_1} p_2^{s_2} \dots p_k^{s_k}$, where p_i is prime for $1 \leq i \leq k$. Note that for each i , $1 \leq i \leq k$, G has an element of order p_i . Choose, for each i , an element $a_i \in G$ such that $o(a_i) = p_i^{t_i}$, where t_i is maximal. Note that $x^{p_i^{t_i}} - 1$ has at most $p_i^{t_i}$

roots in F ; in fact, $\langle a_i \rangle$ is the solution set for the polynomial.

If $t_i < s_i$, then $p_i | o(G/\langle a_i \rangle) = o(G)/o(\langle a_i \rangle)$, so there is $\bar{b} \in G/\langle a_i \rangle$ such that $o(\bar{b}) = p_i$, where $\bar{b} = \langle a_i \rangle + b$, $b \in G$. Now $b \notin \langle a_i \rangle$, as otherwise $\bar{b} = \bar{1}$. But $b^{p_i} \in \langle a_i \rangle$, since $(\bar{b})^{p_i} = \bar{1}$, so $o(b^{p_i}) | o(\langle a_i \rangle) = p_i^{t_i}$ and hence $o(b^{p_i}) = p_i^{r_i}$, where $r_i \leq t_i$. Thus $(b^{p_i})^{p_i^{r_i}} = b^{p_i^{r_i+1}} = 1$, and r_i is the least such element, so $o(b) = p_i^{r_i+1}$. By the maximality of t_i , $r_i + 1 \leq t_i$, so $b^{p_i^{t_i}} = (b^{p_i^{r_i+1}})^{p_i^{t_i-r_i-1}} = 1$, and hence $b \in \langle a_i \rangle$, a contradiction. Therefore $t_i = s_i$, and hence $o(a_i) = p_i^{s_i}$, $1 \leq i \leq k$. Now suppose $c \in \langle a_i \rangle \cap \langle a_j \rangle$, where $i \neq j$. Then $o(c) | p_i^{s_i}$ and $o(c) | p_j^{s_j}$, so $o(c) = 1$ and hence $c = 1$, as $(p_i^{s_i}, p_j^{s_j}) \sim 1$. Thus $\langle a_i \rangle \cap \langle a_j \rangle = \{1\}$ for $i \neq j$. Now let $d = a_1 a_2 \cdots a_k$. Then by Remark 2.36, $o(d) = \prod_{k=1}^n o(a_i) = n$, so $G = \langle d \rangle$.

Corollary 2.38: If $|F| = p^n$, then $F - \{0\}$ is cyclic of order $p^n - 1$.

Proof: $F - \{0\}$ is a finite multiplicative subgroup of F .

A special application of the previous theorem is illustrated by considering the roots of $x^n - 1$.

Theorem 2.39: Suppose $F \subseteq E$, and let $G_E = \{a \in E: a^n = 1\}$.

Then (G_E, \cdot) is a cyclic group and $o(G_E) = r$, where $r | n$.

Proof: Clearly $G_E \neq \emptyset$ and $G_E \subseteq E$. If $a_1, a_2 \in G_E$, then since $a_1^n - 1 = 0 = a_2^n - 1$, $a_1^n = a_2^n$. Now $(a_1 a_2)^n - 1 = a_1^n a_2^n - 1 = (a_1^n - 1)(a_2^n + 1) - a_1^n + a_2^n = 0$, so $a_1 a_2 \in G_E$. Also, if $a \in G_E$, then $(a^{-1})^n - 1 = (a^n)^{-1} - 1 = 1^{-1} - 1 = 0$, so $a^{-1} \in G_E$. Thus G_E is a group.

Now $x^n - 1$ has at most n roots in E and hence in G_E , so $o(G_E) \leq n$. Thus G_E is a finite multiplicative subgroup of E and hence

(G_E, \cdot) is cyclic. Suppose $o(G_E) = r = p_1^{s_1} p_2^{s_2} \dots p_k^{s_k}$. Recall that for each i , there exists an element $a_i \in G_E$ such that $o(a_i) = p_i^{s_i}$. But $a_i^n = 1$, so $p_i^{s_i} | n$, $1 \leq i \leq k$. Further, $(p_i^{s_i}, p_j^{s_j}) \sim 1$ for $i \neq j$, so $r | n$.

The next question which arises concerns the multiplicity of the roots of $x^n - 1 \in F[x]$. The answer lies in the characteristic of F , as will be seen in the following lemma and theorem.

Lemma 2.40: Suppose $f(x) \in F[x]$. Then $f(x)$ has multiple roots iff there is $a \in E$ such that $f(a) = f'(a) = 0$, where $F \hookrightarrow E$.

Proof: If a is a multiple root of $f(x)$, then there is $g(x) \in E[x]$ such that $f(x) = (x - a)^2 g(x)$. Now $f'(x) = 2(x - a)g(x) + (x - a)^2 g'(x)$, and clearly $f(a) = f'(a) = 0$.

Conversely, if $f(a) = f'(a) = 0$, then there is $g(x) \in E[x]$ such that $f(x) = (x - a)g(x)$. Then $f'(x) = (x - a)g'(x) + g(x)$, so $g(a) = 0$ and hence $(x - a)^2 | f(x)$.

Theorem 2.41: Suppose $\chi(F) = p$, and let E be the splitting field of $x^n - 1$. Then $p \nmid n$ iff the roots of $x^n - 1$ are distinct.

Proof: If $x^n - 1$ has no multiple roots, then by the above lemma $p \nmid n$.

On the other hand, suppose that $p \nmid n$ and that $x^n - 1$ has a double root. Then there is $a \in E$, $a \neq 0$, such that $na^{n-1} - 1 = 0$. Thus $n \cdot 1 = 0$, so $p | n$, a contradiction.

From our experience in group theory, we know that there need not be any relation between the structures of two groups of the same order. However, when considering fields, this is not the case. In fact, we show that finite fields which have the same number of elements are

isomorphic. First, however, we need some preliminary results.

Lemma 2.42: If $|F| = p^n$, then $x^{p^n} - x \in F[x]$ has exactly p^n roots in F , and $x^{p^n} - x = \prod_{a \in F} (x - a)$.

Proof: Note that $x^{p^n} - x$ has at most p^n roots in F . But if $a \in F - \{0\}$, then $a^{p^n} - 1 = 1$, so $a^{p^n} = a$ and hence $x^{p^n} - x$ has exactly p^n roots in F . Moreover, $x^{p^n} - x = \prod_{a \in F} (x - a)$.

Corollary 2.43: Suppose $|F| = p^n$, and let P be the prime field of F . Then F is the splitting field of $x^{p^n} - x$ over P .

Proof: It is clear that $x^{p^n} - x \in P[x]$ and that $x^{p^n} - x$ splits over F . Further, if $x^{p^n} - x$ splits over G , then G contains F , so F is the splitting field of $x^{p^n} - x$ over P .

Theorem 2.44: If $|F| = |K|$, then $F \cong K$.

Proof: We suppose $|F| = p^n = |K|$. Now $p^n \cdot 1_F = 0$, so $p \cdot 1_F = 0$, as F is a field. But p is prime, so $\chi(F) = p$. Therefore $\chi(F) = \chi(K) = p$.

Now F is the splitting field of $x^{p^n} - x$ over its prime field P_F , and K is the splitting field of $x^{p^n} - x$ over its prime field P_K . By Lemma 2.32, $P_F \cong P_K$. Now τ extends to an isomorphism $P_F[x] \xrightarrow{\tau^*} P_K[x]$, and $\tau^*(x^{p^n} - x) = x^{p^n} - x$. Thus by the uniqueness theorem for splitting fields, $F \cong K$.

The final result of the chapter shows the existence of a finite field of any prime power order. Further, by the last theorem, this field is unique.

Theorem 2.45: If p is prime, $n \in \mathbb{N}$, then there is a unique (up to isomorphism) field with p^n elements.

Proof: Consider $x^{p^n} - x \in \mathbb{Z}/\langle p \rangle[x]$. Since $\chi(\mathbb{Z}/\langle p \rangle) = p$,

$(x^{p^n} - x)' = p^n x^{p^n - 1} - 1 = -1$, and hence by Lemma 2.40 the roots of $x^{p^n} - x$ are distinct.

Now let K be the splitting field of $x^{p^n} - x$, and let $F = \{a \in K: a^{p^n} = a\}$. Note that F has p^n elements. If $a, b \in F$, then $(a - b)^{p^n} = a^{p^n} - b^{p^n}$, since $\chi(K) = p$. But $a^{p^n} = a$ and $b^{p^n} = b$, so $a - b \in F$. Also, $(ab)^{p^n} = a^{p^n} b^{p^n} = ab$, so $ab \in F$. Finally, if $a \in F$, $a \neq 0$, then $(a^{-1})^{p^n} = (a^{p^n})^{-1} = a^{-1}$, so $a^{-1} \in F$. Thus F is a field, and $|F| = p^n$.

We conclude this chapter with some examples of finite fields.

Example 2.46: If $n \in \mathbb{N}$ is prime, then $\mathbb{Z}/\langle n \rangle$ is a field with n elements.

Example 2.47: Consider $F = \mathbb{Z}_p$, the field of integers modulo p , where p is prime, $p \neq 2$. Notice that $(p - n)^2 \equiv n^2 \pmod{p}$ for $1 \leq n \leq p$. Thus there is a $a \in \mathbb{Z}_p$ such that $x^2 \not\equiv a \pmod{p}$ for each $x \in \mathbb{Z}_p$. But then $x^2 - a \in \mathbb{Z}_p[x]$ is irreducible over \mathbb{Z}_p , so $\mathbb{Z}_p[x]/\langle x^2 - a \rangle$ is a field with p^2 elements.

CHAPTER IV

THE CHINESE REMAINDER THEOREM

AND CONGRUENCES

Initially, R is assumed to be a commutative ring with 1. Consider the system $\{A_k, a_k\}_{k=1}^n$, where A_k is an ideal of R and $a_k \in R$ for $1 \leq k \leq n$. This system is said to be solvable if there is $t \in R$ such that $t \equiv a_k \pmod{A_k}$, that is, $t - a_k \in A_k$, for $1 \leq k \leq n$, and t is called a solution to the system.

Note that if t is a solution to $\{A_k, a_k\}_{k=1}^n$, then $t - a_k \in A_k$ for $1 \leq k \leq n$ and hence $a_i - a_j \in A_i + A_j$ for $1 \leq i \leq n$, $1 \leq j \leq n$. Systems $\{A_k, a_k\}_{k=1}^n$ which meet this latter requirement for solution are called Chinese Remainder (CR) sequences. Rings in which every CR sequence is solvable are called solvable arithmetic rings. In the following, conditions are given for rings R to be arithmetical, and further conditions are given for rings $R \in \mathcal{D}$ to be arithmetical. Arithmetic domains are better known as Prüfer domains. The first result is especially important, in that it yields the standard Chinese Remainder Theorem as an easy corollary.

Theorem 3.1: Let $\{A_k\}_{k=1}^\infty$ be a sequence of ideals of R . Then every CR sequence $\{A_k, a_k\}$ is solvable iff $\bigcap_{k=1}^n (A_k + A_{n+1}) = (\bigcap_{k=1}^n A_k) + A_{n+1}$ for each $n \in \mathbb{N}$.

Proof: We first suppose that every CR sequence is solvable. If $n \in \mathbb{N}$, then clearly $(\bigcap_{k=1}^n A_k) + A_{n+1} \subseteq \bigcap_{k=1}^n (A_k + A_{n+1})$. If $d \in \bigcap_{k=1}^n (A_k + A_{n+1})$, then $d \in A_k + A_{n+1}$ for $1 \leq k \leq n$. Consider $\{A_k, b_k\}_{k=1}^n$,

where $b_k = d$ for $1 \leq k \leq n$ and $b_{n+1} = 0$. $b_k - b_j = 0$ or $b_{n+1} - b_j = d$, so $b_k - b_j \in A_k + A_j$ for $1 \leq j \leq n+1$, $1 \leq k \leq n+1$. Thus $\{A_k, b_k\}$ is a CR sequence, so there is $t \in R$ such that $t - d \in A_k$ for $1 \leq k \leq n$ and $t = t - 0 \in A_{n+1}$. Let $x = d - t$. Then $x \in A_i$ for $1 \leq i \leq n$. But $d = x + t$, so $d \in (\bigcap_{k=1}^n A_k) + A_{n+1}$. Therefore $\bigcap_{k=1}^n (A_k + A_{n+1}) \subseteq (\bigcap_{k=1}^n A_k) + A_{n+1}$, and hence equality follows.

The proof of the converse is by induction. For a CR sequence $\{A_1, a_1\}$, we choose $t = a_1$ and t is a solution. Now suppose that any CR sequence of $k-1$ ideals is solvable, and let $S = \{A_i, a_i\}_{i=1}^k$ be a CR sequence. By hypothesis, there is $t' \in R$ such that $t' - a_i \in A_i$ for $1 \leq i \leq k-1$, and since $a_i - a_k \in A_i + A_k$ for $1 \leq i \leq k$, we have $t' - a_k \in A_i + A_i + A_k = A_i + A_k$ for $1 \leq i \leq k-1$. Thus $t' - a_k \in \bigcap_{i=1}^{k-1} (A_i + A_k) = (\bigcap_{i=1}^{k-1} A_i) + A_k$, so $t' - a_k = x + y$, where $x \in \bigcap_{i=1}^{k-1} A_i$ and $y \in A_k$. Let $t = t' - x = a_k + y$. Then $t - a_i = t' - a_i - x \in A_i + A_i = A_i$ for $1 \leq i \leq k-1$ and $t - a_k = y \in A_k$. Thus t is a solution to $\{A_i, a_i\}_{i=1}^k$.

Corollary 3.2 (Standard Chinese Remainder Theorem): If $A = \{A_k\}_{k=1}^\infty$ is a sequence of ideals of R such that $A_k + A_j = R$ for $k \neq j$, then for any sequence $\{a_k\} \subseteq R$ and for any n , the system $\{A_k, a_k\}_{k=1}^n$ is a solvable CR sequence.

Proof: Since $a_k - a_j \in R$, $a_k - a_j \in A_k + A_j$ for $1 \leq k \leq n$, $1 \leq j \leq n$, $\{A_k, a_k\}_{k=1}^n$ is a CR sequence. For $n \in \mathbb{N}$, we now show that $(\bigcap_{k=1}^n A_k) + A_{n+1} = R$.

Since $1 \in A_k + A_{n+1}$ for $1 \leq k \leq n$, $1 = a_k + a_{n+1}^{(k)}$, where $a_{n+1}^{(k)} \in A_{n+1}$ and $a_k \in A_k$, $1 \leq k \leq n$. Now $\prod_{k=1}^n (a_k + a_{n+1}^{(k)}) = \prod_{k=1}^n a_k + a_{n+1}$, where $\prod_{k=1}^n a_k \in \bigcap_{k=1}^n A_k$ and $a_{n+1} \in A_{n+1}$. Thus $1 \in (\bigcap_{k=1}^n A_k) + A_{n+1}$.

$+ A_{n+1}$, so $(\bigcap_{k=1}^n A_k) + A_{n+1} = R$. But $\bigcap_{k=1}^n (A_k + A_{n+1}) = R$, so by Theorem 3.1, $\{A_k, a_k\}_{k=1}^n$ is solvable.

Example 3.3 (Chinese Remainder Theorem for the integers): If $p_1, p_2, \dots, p_k \in \mathbb{Z}$ with $(p_i, p_j) \sim 1$ for $i \neq j$ and if $x_1, x_2, \dots, x_k \in \mathbb{Z}$, then by Corollary 3.2 there is $n \in \mathbb{Z}$ such that $n \equiv x_i \pmod{p_i}$ for $1 \leq i \leq k$.

The following corollaries of Theorem 3.1 give elementary formulations of the definition of an arithmetic ring. These results will be used later in this chapter.

Corollary 3.4: R is arithmetical iff for all ideals A, B, C of R , $(A + C) \cap (B + C) = (A \cap B) + C$.

Proof: Suppose R is arithmetical, and let A, B, C be ideals of R . Since every CR sequence is solvable, Theorem 3.1 implies that $(A + C) \cap (B + C) = (A \cap B) + C$.

Conversely, we show by induction that for all n , $\bigcap_{k=1}^n (A_k + A_j) = (\bigcap_{k=1}^n A_k) + A_j$, where $\{A_k\}$ is a sequence of ideals of R . The result is clear for $n = 1$. Suppose $\bigcap_{k=1}^n (A_k + A_j) = (\bigcap_{k=1}^n A_k) + A_j$. Then $\bigcap_{k=1}^{n+1} (A_k + A_j) = [\bigcap_{k=1}^n (A_k + A_j)] \cap (A_{n+1} + A_j) = [(\bigcap_{k=1}^n A_k) + A_j] \cap (A_{n+1} + A_j) = [(\bigcap_{k=1}^n A_k) \cap A_{n+1}] + A_j = (\bigcap_{k=1}^{n+1} A_k) + A_j$. Since j is arbitrary, we have in particular that $\bigcap_{k=1}^n (A_k + A_{n+1}) = (\bigcap_{k=1}^n A_k) + A_{n+1}$, so by Theorem 3.1, R is arithmetical.

Corollary 3.5: R is arithmetical iff for all ideals A, B, C of R , $(A \cap C) + (B \cap C) = (A + B) \cap C$.

Proof: Suppose R is arithmetical, and let A, B, C be ideals of R . For all ideals X, Y, Z of R , $(X + Z) \cap (Y + Z) = (X + Y) \cap Z$. Choosing $X = A$, $Y = C$, $Z = B \cap C$, then $(A \cap C) + (B \cap C) = [A + (B \cap C)] \cap C$.

$$\begin{aligned} \cap [C + (B \cap C)] &= (A + B) \cap (A + C) \cap [(C + B) \cap C] = (A + B) \cap (A + C) \\ \cap C &= (A + B) \cap C. \end{aligned}$$

On the other hand, suppose A, B, C are ideals of R and note that for all ideals X, Y, Z of R , $(X \cap Z) + (Y \cap Z) = (X + Y) \cap Z$. If we let $X = A, Y = C, Z = B + C$, then $(A + C) \cap (B + C) = [A \cap (B + C)] + [C \cap (B + C)] = (A \cap B) + (A \cap C) + [(C \cap B) + C] = (A \cap B) + (A \cap C) + C = (A \cap B) + C$, so R is arithmetical by Corollary 3.4.

Next to be considered are some special integral domains, Bézout domains and Prüfer domains. Important relationships will be noted between these domains and the concept of arithmetical domain.

Definition 3.6: An integral domain D is a Bézout domain if $\langle a, b \rangle$ is principal for all $a, b \in D$.

Remark 3.7: If $R \in \mathcal{S}$, $a, b \in R$, and if $\langle a, b \rangle = \langle d \rangle = \langle 0 \rangle$, then $a = a'd, b = b'd$ implies $(a', b') \sim 1$ and $a'b = b'a \in \langle a \rangle \cap \langle b \rangle$.

Proof: If $k|a'$ and $k|b'$, then there are $r, s \in R$ such that $a' = rk$ and $b' = sk$, so $a = rkd$ and $b = skd$. Now there are $m, n \in R$ such that $d = ma + nb$, so $d = (mr + ns)kd$. But then $k|d$, so $k \sim 1$.

Moreover, $a'bd = ab = ab'd$, so $a'b = ab'$. Thus clearly $a'b = ab' \in \langle a \rangle \cap \langle b \rangle$.

Theorem 3.8: Bézout domains are arithmetical.

Proof: Suppose R is a Bézout domain, and suppose A, B , and C are ideals of R . It is clear that $(A \cap B) + C \subseteq (A + C) \cap (B + C)$. If $x \in (A + C) \cap (B + C)$, then $x = a + c_1 = b + c_2$, where $a \in A, b \in B, c_1, c_2 \in C$. Now there is $d \in R$ such that $\langle a, b \rangle = \langle d \rangle$. If $d = 0$, then $a = b = 0$, so $x \in C \subseteq (A \cap B) + C$ and the proof is finished. We now suppose that $d \neq 0$. Then there are $a', b' \in R$ such that $a = a'd, b = b'd$,

and since $(a', b') \sim 1$, there are $u, v \in R$ such that $a'u + b'v = 1$. Then $x = x \cdot 1 = xua' + xvb' = (b + c_2)ua' + (a + c_1)vb' = (bua' + avb') + (c_2ua' + c_1vb')$. Since $ba' = ab' \in A \cap B$, $bua' + avb' \in A \cap B$. Also, $c_1, c_2 \in C$, so $c_2ua' + c_1vb' \in C$. Therefore $x \in (A \cap B) + C$, so we have $(A + C) \cap (B + C) = (A \cap B) + C$, and hence R is arithmetical.

Corollary 3.9: Every P.I.D. is arithmetical.

Proof: Every P.I.D. is a Bézout domain.

Definition 3.10: A ring $R \in \mathcal{B}$ is a Prüfer domain if for all $a, b \in R$ not both zero there exist $u, v \in R^*$ such that $au, bu, av, bv \in R$ and $au + bv = 1$.

Theorem 3.11: Every Prüfer domain is arithmetical.

Proof: Suppose R is a Prüfer domain, and suppose A, B , and C are ideals of R . It is clear that $(A \cap B) + C \subseteq (A + C) \cap (B + C)$, so suppose $x \in (A + C) \cap (B + C)$. Then there are $a \in A, b \in B, c_1, c_2 \in C$ such that $x = a + c_1 = b + c_2$. If $a = b = 0$, then $x \in C \subseteq (A \cap B) + C$, and the proof is finished. Thus we suppose that not both of a and b are zero. Then there are $u, v \in R^*$ such that $au, bu, av, bv \in R$ and $au + bv = 1$. Thus $x = x \cdot 1 = xau + xbv = bau + c_2au + abv + c_1bv = (abv + bau) + (c_2au + c_1bv)$. Now $au, bv \in R$, so $c_2au + c_1bv \in C$. Also, $bv, bu \in R$, so $abv, bau \in A$ and hence $abv + bau \in A$. Finally, $av, au \in R$, so $abv, bau \in B$ and hence $abv + bau \in B$. Therefore $x \in (A \cap B) + C$, and so $(A + C) \cap (B + C) = (A \cap B) + C$ and hence R is arithmetical.

In fact, the converse to Theorem 3.11 is also true. Once this has been shown, it will follow that the concepts of Prüfer domain and arithmetical domain are equivalent. This result is proved in the next theorem.

Theorem 3.12: A ring $R \in \mathcal{V}$ is an arithmetical domain iff R is a Prüfer domain.

Proof: The sufficiency has been proved in Theorem 3.11. We now show the necessity. Suppose $a, b \in R$ and $a \neq 0$. If $a + b = 0$, then $u = 1/a, v = 0 \in R^*$, and $au + bv = 1$. Further, $au, bu, av, bv \in R$.

Suppose now that $a + b \neq 0$. Since $a + b \in (\langle a \rangle + \langle b \rangle) \cap \langle a + b \rangle$, it follows from Corollary 3.5 that $a + b \in (\langle a \rangle \cap \langle a + b \rangle) + (\langle b \rangle \cap \langle a + b \rangle)$. Thus $a + b = x + y$, where $x \in \langle a \rangle \cap \langle a + b \rangle$ and $y \in \langle b \rangle \cap \langle a + b \rangle$. Then there are $x_1, x_2, y_1, y_2 \in R$ such that $x = ax_1 = (a + b)x_2, y = by_1 = (a + b)y_2$. Now $1 = (a + b)/(a + b) = x/(a + b) + y/(a + b) = ax_1/(a + b) + by_1/(a + b)$. Letting $u = x_1/(a + b), v = y_1/(a + b)$, it is clear that $au + bv = 1$, where $u, v \in R^*$. Also, note that $au = ax_2/a = x_2 \in R$. If $b = 0$, then clearly $bv \in R$. If $b \neq 0$, then $bv = by_2/b = y_2 \in R$. If $y_1 = 0$, then it is clear that $av \in R$. Thus we suppose $y_1 \neq 0$. If $b = 0$, then $a = x + y$, and $av = y_1(x + y)/(a + b) = y_1 \in R$. If $b \neq 0$, then $y_2 \neq 0$, so $avy_2 = bv(y_1 - y_2) = y_2(y_1 - y_2)$ and hence $av = y_1 - y_2 \in R$. Also, if $x_1 = 0$, then $bu \in R$, so we suppose $x_1 \neq 0$. If $b = 0$, then $bu \in R$. Otherwise, since $a \neq 0$ we have $x_2 \neq 0$. But then $bux_2 = au(x_1 - x_2) = x_2(x_1 - x_2)$, so $bu = x_1 - x_2 \in R$. Therefore R is Prüfer.

LIST OF REFERENCES

- Herstein, I.N. Topics in Algebra. Waltham, Massachusetts: Blaisdell Publishing Company, 1964.
- Leveque, William J. Elementary Theory of Numbers. Reading, Massachusetts, Addison-Wesley Publishing Company, Inc., 1962.
- Rotman, Joseph J. The Theory of Groups: An Introduction. Boston: Allyn and Bacon, Inc., 1965.
- Zariski, O. and Samuel, P. Commutative Algebra, Vol. I. Princeton: Van Nostrand Co., 1958.