

MODERN ALGEBRA ILLUSTRATED BY
NUMBER THEORETIC EXAMPLES

By

AUGUST WESLEY WALTMANN

Bachelor of Arts
Wartburg College
Waverly, Iowa
1964

Master of Arts
Kansas State University
Manhattan, Kansas
1966

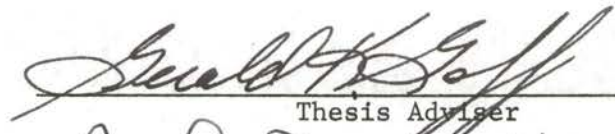
Submitted to the Faculty of the Graduate College
of the Oklahoma State University
in partial fulfillment of the requirements
for the Degree of
DOCTOR OF EDUCATION
May, 1969

OKLAHOMA
STATE UNIVERSITY
LIBRARY

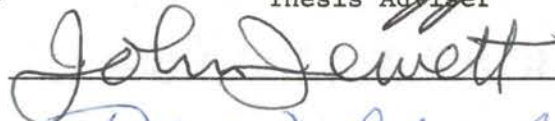
JAN 4 1971

MODERN ALGEBRA ILLUSTRATED BY
NUMBER THEORETIC EXAMPLES

Thesis Approved:



Thesis Adviser







Dean of the Graduate College

767457

ACKNOWLEDGMENTS

It is pertinent to express my appreciation to all who have helped me in the preparation and writing of this dissertation. Particular gratitude is due Dr. Gerald K. Goff, my dissertation adviser, who suggested the topic and assisted and encouraged me during the writing of this dissertation. Special thanks also go to Dr. John Jewett, my committee chairman, and to Dr. Robert Alciatore, a member of my advisory committee, for their cooperation throughout my study at Oklahoma State University.

Finally, I express my appreciation to my wife, Barbara, who served as my secretary, typist, and morale builder throughout my graduate study. Sincere thanks are due Barbara for converting my rough copy into the typed copy you are now reading.

TABLE OF CONTENTS

Chapter	Page
I. INTRODUCTION	1
Statement of the Problem	1
Approach Given the Problem	1
Content	3
Significance	3
II. GROUPS	5
Simple Properties of Groups	5
Subgroups	13
Cyclic Groups	17
Homomorphisms and Isomorphisms	20
Cosets	26
Invariant Subgroups	29
Quotient Groups	32
Products of Subgroups	35
Composition Series	36
Direct Products	43
III. RINGS AND IDEALS	47
Simple Properties of Rings	47
Subrings	57
Homomorphisms and Isomorphisms	58
Ideals	65
Prime Ideals and Maximal Ideals	70
Quotient Rings	72
Polynomial Rings	77
Euclidean Rings	85
Noetherian Rings	88
IV. INTEGRAL DOMAINS AND FIELDS	91
Integral Domains	91
Subdomains	96
Unique Factorization	97
Fields	102
Polynomials Over a Field	106
V. SUMMARY	111
SELECTED BIBLIOGRAPHY	113

CHAPTER I

INTRODUCTION

Statement of the Problem

Undergraduate mathematics curriculums usually offer at least one course in modern algebra. The Mathematical Association of America [7]¹ recommends that the training of teachers of mathematics at all levels from junior high school through college include at least one course in abstract algebra and more courses as the levels increase. In 1965 the Committee on the Undergraduate Program in Mathematics [6] included a course, Algebraic Structures, in the upper division of their recommendations for undergraduate mathematics. The topics suggested for this course are topics normally contained in courses called modern algebra.

Some students find modern algebra difficult. These students could possibly benefit from concrete examples which illustrate the abstract concepts. It is hoped that this dissertation will provide a source of such examples.

Approach Given the Problem

This dissertation is not meant to be a textbook but a body of reference material to supplement textbooks. It is hoped that this material

¹Numerals included in brackets [] will refer to references with corresponding numerals listed in the bibliography.

can be used for independent study as well as by teachers desiring a supply of examples to present to their students. Examples are offered that depend on systems developed in elementary number theory. This source seems appropriate since some students experience these and similar systems in junior and senior high school mathematics courses. A glance at the index of junior and senior high school textbooks such as those listed in the bibliography ([10], [20], [22], and [23]) reveals clock arithmetic and modular systems as well as other topics from elementary number theory. Previous experience with number theory is not, however, required to read and appreciate this dissertation. The author does not assume that students of undergraduate modern algebra have had a course in number theory.

This dissertation does not contain proofs of theorems or reiteration of lengthy discussions found in textbooks. Theorems and definitions are arranged in a logical sequence which could be adapted to courses in modern algebra. Definitions were selected on the basis of common usage and consistency with the theorems selected. The wording of definitions and theorems will sometimes be identical with that in one or more textbooks.

The author has surveyed several of the current undergraduate modern algebra textbooks ([2], [5], [9], [12], [14], [16], [17], and [24]) to determine a body of theorems common to the development in these texts. The Schaum's outline for modern algebra by Ayres [1] was also used to aid in selection of the theorems. From this body of theorems the author then selected some for which he could develop examples using elementary number theory. Examples are also given to help demonstrate the importance of careful reading of theorems, both the hypotheses and conclusions.

Content

This dissertation is restricted to material appropriate to an introductory undergraduate modern algebra course. Consideration is given only to the theory of groups, rings, ideals, integral domains, and fields. All examples are derived from elementary number theory and are limited in difficulty because of the background of students normally in such a course.

The author does assume the reader has had a course in college algebra or its equivalent in which he has become somewhat familiar with sets, mappings, functions, the absolute value function, the maximum or minimum of a set of real numbers, 2×2 matrices, properties of the set of integers, and other topics normally in such a course. A knowledge of modular systems from junior and senior high school mathematics courses or some other source is also assumed.

Some theorems that are quite common in textbooks for modern algebra are not included in this dissertation because of the limitation of topics considered and the limitations set on the source of examples. Chapter II is reserved for the discussion of groups. In Chapter III, consideration is extended to topics in the study of rings and ideals. Finally, in Chapter IV a limited coverage is given to integral domains and fields.

Significance

The primary contribution of this dissertation is the development of reference material for a first course in undergraduate modern algebra. Through the use of this material it is hoped that students will develop a greater appreciation and understanding of modern algebra. This dissertation relates topics from two fields of mathematics, modern algebra and

number theory. The author hopes that through this relationship, students will become interested in number theory and will want to continue their study of abstract algebra.

CHAPTER II

GROUPS

Simple Properties of Groups

A formal definition of a set and set operations shall not be given in this dissertation. A knowledge of sets, operations on sets, and set notations shall be assumed on the part of the reader.

A binary operation on a set S of mathematical objects is any rule $*$ that associates with each ordered pair $\langle a, b \rangle$ of elements (not necessarily distinct) of S a uniquely determined element, denoted $a*b$, which is in S . Some authors define a binary operation as a rule which associates with each ordered pair $\langle a, b \rangle$ of elements of a set S an element in a set T and say the set S is closed with respect to the binary operation $*$ if $T \subset S$. In this dissertation a binary operation $*$ on a set S shall always mean S is closed with respect to $*$. Furthermore, a binary operation shall be called simply an operation. Ordinary addition defined on the set of integers is an example of an operation but some rules defined on sets are not operations.

Example 1 Let I be the set of all integers and $*$ be ordinary division. Throughout this dissertation I will be used to represent the set of all integers. Then $*$ is not an operation on I since $3*0$ is not defined nor are quotients such as $3*2$ defined in I .

Example 2 Let S be the set of all odd integers and $*$ be

ordinary addition. Then $*$ is not an operation since $1*3$ is not in S .

Example 3 Let S be the set of all nonnegative integral powers of 5 and $*$ be the "common divisor." Then $*$ is not a binary operation since $5*25 = 1$ or 5 so that the rule $*$ does not determine a unique element of S .

A nonempty set of elements on which an operation is defined is called a groupoid. The notation $[G; *]$ will be used for a groupoid G under the operation $*$. When it is not necessary to refer to the operation, the groupoid $[G; *]$ shall be denoted by G .

If S is a groupoid with operation $*$ such that for arbitrary $a, b, c \in S$, $(a*b)*c = a*(b*c)$, then S is an associative groupoid or a semigroup. If the operation satisfies certain additional properties, then the system is known as a group.

Definition 2.1 A groupoid G with operation $*$ is said to form a group with respect to $*$ provided, for arbitrary $a, b, c \in G$, the following properties hold:

P_1 : $(a*b)*c = a*(b*c)$ (associative law)

P_2 : There exists $u \in G$ such that for each $a \in G$, $a*u = u*a = a$
(existence of identity element)

P_3 : For each $a \in G$ there exists $a^{-1} \in G$ such that $a*a^{-1} = a^{-1}*a = u$
(existence of inverses)

A groupoid satisfying P_1 of the definition of a group is a semigroup.

Notice that the identity element u , inferred in P_2 of the definition of a group G must satisfy both of the equations $a*u = a$ and $u*a = a$ for any element $a \in G$.

Let $[H; *]$ be a groupoid and $u' \in H$ such that $a * u' = a$ for every $a \in H$. Then u' is called a right identity for H . If $u'' \in H$ such that $u'' * a = a$ for every $a \in H$, then u'' is called a left identity for H . It is easy to show that if u' and u'' are right and left identities for H , respectively, then $u' = u''$ and H has an identity. Sometimes an element of a groupoid will be a right identity and not a left identity or vice versa.

Example 4 Consider the set E of even integers under the operation \circ defined by $a \circ b = (2 \cdot a) + b$ for any $a, b \in E$ where \cdot and $+$ are ordinary multiplication and addition of integers. The integer $0 \in E$ acts as a left identity, i.e., $0 \circ a = a$ for any $a \in E$, but not a right identity, i.e., $a \circ 0 = 2 \cdot a \neq a$, if $a \neq 0$. Hence, 0 is not an identity for $[E; \circ]$. Furthermore, 0 is the only left identity for $[E; \circ]$ since $a \circ b = (2 \cdot a) + b = b$ if and only if $a = 0$ so that $[E; \circ]$ has no identity.

In order to talk about the existence of inverses, a groupoid must have an identity element. This is true since the identity is one member of the equality conditions in P_3 of the definition of a group. Hence, if a groupoid has no identity element, it can have no inverses.

Example 5 The set of all positive multiples of 2 under the operation, multiplication, is an associative groupoid but not a group since no identity and, hence, no inverses exist in the set.

Let $[H; *]$ be a groupoid with identity u and $x \in H$ such that $a * x = u$ for $a \in H$. Then x is called a right inverse of a in H . Similarly, if $y * a = u$ for $y, a \in H$, then y is called a left inverse of a in H . If an

associative groupoid $[H; *]$ has a left inverse y and a right inverse x for some $a \in H$, then $x = y$ and a has an inverse in H .

For any element a in the groupoid $[E; \circ]$ of Example 4, $a \circ [2 \cdot (-a)] = [2 \cdot a] + [2 \cdot (-a)] = 0$. We noted earlier that 0 is a left identity in $[E; \circ]$. Hence, for any $a \in E$, $2 \cdot (-a) \in E$ operates similar to a right inverse of a even though $[E; \circ]$ has no identity. Also notice that $2 \cdot (-a)$ is not a left inverse for $a \in E$. The elements -2 and 6 operate similar to left inverses for 4 and -12 , respectively, in $[E; \circ]$ but no such elements exist in $[E; \circ]$ for 10 or -6 .

As mentioned before, a groupoid does not exist satisfying P_1 and P_3 but not P_2 of the definition of a group. However, groupoids satisfying P_1 and P_2 alone or P_2 and P_3 alone do exist.

Example 6 Let S be the set of all integers n of the form $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_r^{\alpha_r}$ where the p_i for $i = 1, 2, \dots, r$ are fixed distinct primes and the α_i for $i = 1, 2, \dots, r$ are equal to zero or one. Define the operation $*$ on S to be $n * m = (n, m)$, the greatest common divisor of n and m . Then $u = p_1^1 p_2^1 \dots p_r^1$ is an identity for S since $(u, n) = (n, u) = n$ for every $n \in S$. Hence, for the groupoid $[S; *]$, the largest element is an identity. $[S; *]$ is also an associative groupoid but no element of S except u has an inverse. $[S; *]$ is an example of a groupoid that satisfies P_1 and P_2 but not P_3 of the definition of a group.

Example 7 Let I_0^+ denote the set of all nonnegative integers and let $T = \{6^n : n \in I_0^+\}$. Define $*$ on T by $6^n * 6^m = 6^{|n-m|}$ for any $n, m \in I_0^+$. $[T; *]$ is a groupoid and 6^0 is an identity for $[T; *]$ since $6^0 * 6^n = 6^n * 6^0 = 6^n$ for any $n \in I_0^+$. Notice that $6^n * 6^n = 6^0$

for any $n \in \mathbb{I}_0^+$, i.e., each element in T is its own inverse. $[T; *]$ is not associative since, for example, $(6^3 * 6^8) * 6^{10} = 6^5 * 6^{10} = 6^5$ while $6^3 * (6^8 * 6^{10}) = 6^3 * 6^2 = 6^1$. Hence, $[T; *]$ is a groupoid that satisfies P_2 and P_3 but not P_1 of the definition of a group.

For purposes of simplicity, the notation of ordinary multiplication or addition will frequently be used to designate the operation in a group, i.e., $a * b$ will be written as ab or $a + b$. If multiplicative notation is used for the operation on a group G and $a \in G$, then a^n is the product having n factors of a for any positive integer n . The terminology of multiplication will sometimes be used in referring to $a * b$, i.e., a and b will be called "factors" and $a * b$ will be called the "product" of a and b . If additive notation is used for the operation on a group G , then $na = a + a + \dots + a$ (n summands of a).

The negative sign will also be used in a customary fashion, i.e., $a^{-n} = (a^{-1})^n$ and $-na = n(-a)$ where n is a positive integer and $-a$ is the inverse of a in additive notation. The letters u and z will represent the identity element in multiplicative and additive notation, respectively. For any $a \in G$ a group, $a^0 = u$ and $0a = z$ in the respective notations by definition.

Theorem 2.2 A group has only one identity element.

The set of integers under ordinary addition is a group, denoted $[I; +]$, whose only identity is 0 . A groupoid such that the identity element is unique is not necessarily a group.

Example 8 Let S be the set of all positive even integers and define $*$ on S by $a * b = [a, b]$, the least common multiple of a and b .

$[S; *]$ is an associative groupoid with 2 as the only identity. $[S; *]$ is not a group since only 2, which is its own inverse, has an inverse in S .

Theorem 2.3 A group has only one inverse associated with each element of the group.

The group $[I; +]$ of integers under addition serves as a simple example for this theorem since $-n$ is the unique additive inverse of n for any $n \in I$. A groupoid having a unique inverse for each of its elements is not always a group.

Example 9 Let I_0^+ be the set of all nonnegative integers. Consider I_0^+ under the operation $a * b = |a - b|$, the absolute value of $a - b$. Notice that 0 is the unique identity in $[I_0^+; *]$ and a is the unique inverse of a for each $a \in I_0^+$. $[I_0^+; *]$ is not a group under this operation since $(2 * 5) * 7 \neq 2 * (5 * 7)$.

Theorem 2.4 (Cancellation Law) Let $[G; *]$ be a group and $a, b, c \in G$. Then $a * b = a * c$ (also $b * a = c * a$) implies $b = c$.

While the group $[I; +]$ is again a simple example of this theorem, $[T; *]$ of Example 7 and also $[I_0^+; *]$ of Example 9 show that a groupoid which satisfies the Cancellation Law is not necessarily a group.

Theorem 2.5 Let a and b be elements of a group $[G; *]$. Then each of the equations $a * x = b$ and $y * a = b$ has a unique solution.

See $[T; *]$ of Example 7 or $[I_0^+; *]$ of Example 9 for an example of a groupoid which is not a group but has unique solutions to the equations in Theorem 2.5.

Theorem 2.6 For every element a of a group G , the inverse of the inverse of a is a , i.e., $(a^{-1})^{-1} = a$.

Again $[T; *]$ of Example 7 and $[I_0^+; *]$ of Example 9 provide examples of a groupoid G which is not a group but such that $(a^{-1})^{-1} = a$ for every $a \in G$.

Definition 2.7 A group G with operation $*$ is

- (i) An abelian (or commutative) group if for every $a, b \in G$, $a * b = b * a$.
- (ii) An additive group if $*$ is addition.
- (iii) A multiplicative group if $*$ is multiplication.
- (iv) An infinite group (or group of infinite order) if G contains infinitely many elements.
- (v) A finite group if G contains a finite number of elements.
- (vi) A group of order n if G contains exactly n elements.

The group of integers $[I; +]$ is an example of an infinite abelian additive group. A finite group is given in the following example.

Example 10 Let M be the set of all 2×2 nonsingular matrices over the integers modulo 2. Then $M = \{a, b, c, d, e, f\}$ where

$$\begin{array}{lll}
 a = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} & b = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} & c = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \\
 d = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} & e = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} & f = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}.
 \end{array}$$

The following Cayley square is a table for products of elements in M . In a Cayley square the product $x \cdot y$ is the entry common to the row labeled x and the column labeled y . For example, in the following Cayley square, $c \cdot d = e$.

•	a	b	c	d	e	f
a	a	b	c	d	e	f
b	b	a	e	f	c	d
c	c	f	a	e	d	b
d	d	e	f	a	b	c
e	e	d	b	c	f	a
f	f	c	d	b	a	e

M is a finite nonabelian multiplicative group of order 6 under ordinary matrix multiplication with operations in module 2 arithmetic. To see that M is nonabelian note that $b \cdot c \neq c \cdot b$. Denote the group M by $[M; \cdot]$.

Theorem 2.8 If G is a group, then for every $a, b \in G$,
 $(ab)^{-1} = b^{-1}a^{-1}$.

If $(ab)^{-1} = b^{-1}a^{-1}$ for every $a, b \in G$ a groupoid, this does not imply G is a group. For example, in $[I_0^+; *]$ of Example 9, $2*4 = |2-4| = 2$, $2^{-1} = 2$, $4^{-1} = 4$, and $4^{-1}*2^{-1} = |4^{-1}-2^{-1}| = |4-2| = 2$ so that $(2*4)^{-1} = 2 = 4^{-1}*2^{-1}$. Similar statements are true for any pair $a, b \in I_0^+$ but $[I_0^+; *]$ is not a group.

It is also important to note that Theorem 2.8 states that $(ab)^{-1} = b^{-1}a^{-1}$, not that $(ab)^{-1} = a^{-1}b^{-1}$. The group $[M; \cdot]$ of Example 10 can be used to demonstrate why this is so stated. Notice that $(c \cdot d)^{-1} = e^{-1} = f$ but $c^{-1} \cdot d^{-1} = c \cdot d = e$. Hence, $(c \cdot d)^{-1} \neq c^{-1} \cdot d^{-1}$ for this group but $(c \cdot d)^{-1} = d^{-1} \cdot c^{-1}$ since $d^{-1} \cdot c^{-1} = d \cdot c = f$.

Theorem 2.9 For any element a contained in a group G ,

- (i) $a^m a^n = a^{m+n}$ and
- (ii) $(a^m)^n = a^{mn}$, where $m, n \in I$, the set of integers.

The groupoids given in Example 7 and Example 9 satisfy both (i) and

(ii) of Theorem 2.9 but neither is a group.

Subgroups

Discussion has thus far covered some of the simple properties of groups and some examples related to these properties. Now some of the structural properties of groups will be considered.

Any nonempty subset G' of a group G with operation $*$ is called a subgroup of G if G' is itself a group with respect to $*$. If $G' = G$ or $G' = \{u\}$ where u is the identity of G , then G' is an improper subgroup of G ; if G' is any other subgroup of G , it will be called a proper subgroup of G . The subgroup $\{u\}$ is called the identity subgroup of G .

Consider the group $[I;+]$ of integers under addition. Then the set E of even integers under ordinary addition is a group and, hence, a proper subgroup of $[I;+]$ since $E \subset I$, $E \neq I$, $E \neq \{0\}$, and $[E;+]$ has the same operation as $[I;+]$. The set K of the first 8 nonnegative integers under addition modulo 8 is a group and $K \subset I$ but K is not a subgroup of $[I;+]$ since the operations are not the same.

Theorem 2.10 A nonempty subset G' of a group G is a subgroup of G if and only if

- (i) G' is closed with respect to the operation of G and
- (ii) G' contains the inverse of each of its elements.

Neither (i) nor (ii) of Theorem 2.10, above, is sufficient to know that a subset of a group is a subgroup. Consider the group $[I;+]$ and let G' be the set of all nonnegative integers. G' is closed with respect to $+$ but is not a subgroup of $[I;+]$ since -2 , the inverse of 2 , for example, is not in G' so that G' does not satisfy P_3 of the definition

of a group.

Example 11 Let $G = \{6^n : n \in I\}$ and consider \cdot , ordinary multiplication of integers, as the operation on G . Then $[G; \cdot]$ is a group and $G' = \{6^{2k+1} : k \in I\}$ is a proper subset of G such that every element in G' has an inverse in G' , i.e., for any $6^{2k+1} \in G'$, $(6^{2k+1})^{-1} = 6^{-2k-1} = 6^{2(-k-1)+1} \in G'$. However, G' is not a groupoid since G' is not closed with respect to multiplication, e.g., $6^3 \cdot 6^{-3} = 6^0 \notin G'$. Thus, G' is not a group and, hence, not a subgroup of G .

Any collection of characteristics which is both necessary and sufficient in order to identify a mathematical entity is called a characterization of this entity. Thus, any definition is a characterization but is not necessarily the only possible characterization for the entity defined. Theorem 2.10 gave one characterization of a subgroup. Another characterization of a subgroup is given in the following theorem.

Theorem 2.11 A nonempty subset G' of a group G is a subgroup of G if and only if for all $a, b \in G'$, $a^{-1}b \in G'$.

This characterization of a subgroup reduces the criterion for determining whether a subsystem of a group is a subgroup to checking special products. These products involve an element of the given subset with the inverse of some other element of the subset. By definition this inverse exists as an element of the group, but it is not necessary to assume that this inverse is in the subset of the group.

Subsets of another group will now be considered.

Example 12 Define $*$ on the set $S = \{0, 2, 3, 4, 5, 6\}$ by

$a*b = a+b-(a \cdot b)$ for any $a, b \in S$ where $+$, $-$, and \cdot are addition, subtraction, and multiplication, respectively, in modulo 7 arithmetic. S contains all the residue classes, modulo 7, except the one represented by 1 and $a*b = 1 \leftrightarrow a+b-ab \equiv 1 \pmod{7} \leftrightarrow a(1-b) \equiv 1-b \pmod{7} \leftrightarrow a \equiv 1 \pmod{7}$ but $a \not\equiv 1 \pmod{7}$ since $a \in S$. Hence, S is closed with respect to $*$ and $[S; *]$ is a groupoid. Straight forward calculations show that $[S; *]$ is associative, 0 is the identity, and 0, 2, 5, 6, 3, and 4 are, respectively, the inverses of 0, 2, 3, 4, 5, and 6. Thus, $[S; *]$ is, by definition, a group. By Theorem 2.11 the subset of even residue classes $S_1 = \{0, 2, 4, 6\}$ is not a subgroup of S since $2*4^{-1} = 2*6 = 3 \notin S_1$. By using Theorem 2.11 a subset of S containing 2 and 4 can be a subgroup of $[S; *]$ only if it contains 3. Theorem 2.11 can also be used to verify that $S_2 = \{0, 2\}$ and $S_3 = \{0, 4, 6\}$ are subgroups of $[S; *]$. $S_4 = \{0\}$ and S are, of course, the improper subgroups of $[S; *]$. The following theorem gives an interesting way to view the subgroups of S .

Theorem 2.12 Let a be an element of a group G . The set $G' = \{a^n : n \in I\}$ of all integral powers of a is a subgroup of G .

In the group $[S; *]$ of Example 12, $S_4 = \{0\} = \{0^n : n \in I\}$, $S_2 = \{0, 2\} = \{2^n : n \in I\}$, $S_3 = \{0, 4, 6\} = \{4^n : n \in I\} = \{6^n : n \in I\}$, and $S = \{0, 2, 3, 4, 5, 6\} = \{3^n : n \in I\} = \{5^n : n \in I\}$. It is interesting to note that in $[S; *]$ a^n , i.e., $a*a*\dots*a$ (n "factors" of a), is equal to $1-(1-a)^n$ in modulo 7 arithmetic, i.e., $1-(1-a)^n$ reduced to one of the least positive residue classes modulo 7.

Not all subgroups of a group are of the type given by Theorem 2.12. Examine the multiplication table of the group $[M; \cdot]$ of Example 10 to see

that $[M; \cdot]$ is not of this type. A group having a proper subgroup not of the type of Theorem 2.12 is given next.

Example 13 Let N be the set of all 2×2 matrices over the integers modulo 2. Then the set N under ordinary matrix addition, denoted by $+$, is a group in which the zero matrix is the identity and every element is its own inverse. Let $S = \{z, r, s, t\}$ where

$$z = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \quad r = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \quad s = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \quad t = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}.$$

Then $[S; +]$ is a proper subgroup of $[N; +]$ and $[S; +]$ is not of the type given by Theorem 2.12.

Let H_i for $i = 1, 2, \dots, n$ be subgroups of a group G . Then the intersection of these subgroups is the set of all elements in G common to all the subgroups H_i for $i = 1, 2, \dots, n$.

Theorem 2.13 If S is any set of subgroups of a group G , then the intersection of these subgroups is also a subgroup of G .

If some subgroups of a given group are known, then Theorem 2.13 furnishes a way of finding a different subgroup if the intersection, set wise, is a proper subset of the known subgroups. Considering, in various ways, intersections of the subgroups S_1, S_2, S_3 , and S_4 of the group $[S; *]$ given in Example 12 illustrates the validity of Theorem 2.13. On the other hand, if the intersection of a pair of subsets of a group is a known subgroup, this does not imply that either of the original subsets is a subgroup. If $S_1 = \{0, 2, 4, 6\}$ and $S_5 = \{1, 3, 4, 5, 6\}$, then $S_1 \cap S_5 = S_3 = \{0, 4, 6\}$. S_3 is a known subgroup of $[S; *]$ but neither S_1 nor S_5 is a subgroup of $[S; *]$.

Cyclic Groups

A group G is called a cyclic group if, for some $a \in G$, every $x \in G$ is of the form a^m , where m is some integer. The element a is then called a generator of G and G is said to be generated by a . Hence, the subgroups of the type given by Theorem 2.12 are all cyclic groups.

The order of an element a of a group G is the order of the cyclic subgroup of G generated by a .

A number system which is an important source of examples will now be defined.

Definition 2.14 Let m be any fixed integer greater than one and let $S = \{0, 1, 2, \dots, m-1\}$. The arithmetic of residue classes modulo m , or more briefly, m -arithmetic, is the arithmetic system defined on S such that when the operations of ordinary addition, subtraction, and multiplication are performed on S the result is replaced by its least nonnegative remainder on division by m .

The additive group in m -arithmetic will be denoted by $[A_m; +]$ and, if m is a prime, the multiplicative group of nonzero elements in m -arithmetic will be denoted $[A_m^\circ; \cdot]$. If m is not a prime, then the set of nonzero elements of A_m does not form a group under multiplication since the operation is not closed, i.e., if m is not a prime, then a product of the prime factors of m will always give 0 in m -arithmetic.

Diagrams are often convenient visual aids in presenting new concepts. Finite cyclic groups of small order can easily be represented in diagram form. Arrows will be used to indicate what each element becomes when multiplied by some fixed element of the group, where multiplication is the group operation.

Example 14 Let $A_8 = \{0,1,2,3,4,5,6,7\}$ and consider A_8 under addition in 8-arithmetic. $[A_8;+]$ is a cyclic group with identity 0 and the additive inverse of a equal to $8-a$ for every $a \in A_8$, $a \neq 0$. The element 0 is its own inverse. Associativity holds since ordinary addition of integers is associative. The addition diagrams for successively adding 1 to itself, 2 to itself, and 3 to itself in 8-arithmetic are given in Figures 1, 2, and 3, respectively.

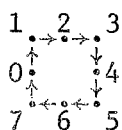


Figure 1

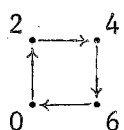


Figure 2

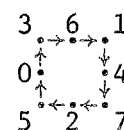


Figure 3

Figure 1 suggests that $[A_8;+]$ is a cyclic group and that 1 is a generator of the group. Figure 2 suggests that successively adding 2 to itself generates a cyclic subgroup of $[A_8;+]$ of order 4. Figure 3 shows that 3 is also a generator of $[A_8;+]$.

Theorem 2.15 An element a^m of a finite cyclic group G of order n is a generator of G if and only if $(n,m) = 1$, i.e., n and m are relatively prime.

Although the above theorem is stated as found in some texts, it is not entirely correct. The element a must be assumed to be a generator of G .

Example 15 Consider the additive group $[A_6;+]$ defined similar to $[A_8;+]$ in Example 14. In additive notation Theorem 2.15 would be: An element $m \cdot a$ of a finite cyclic group G of order n is a

generator of G if and only if $(n,m) = 1$. Notice that $1 \cdot 4 = 4 \in A_6$ with $(1,6) = 1$ but 4 is not a generator of A_6 as seen by Figure 4 below. Try all the elements of A_6 to verify that the only generators of A_6 are 1 and 5. Notice that $4 = 4 \cdot 1$ and $4 = 2 \cdot 5$ in A_6 . Also $(4,6) \neq 1$ and $(2,6) \neq 1$ so that 4 is not suppose to be a generator of A_6 by Theorem 2.15, assuming a of the theorem is a generator of the group.

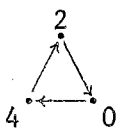


Figure 4

A peculiarity of cyclic groups is given in the following theorem.

Theorem 2.16 Every subgroup of a cyclic group is itself a cyclic group.

If every subgroup of a group is cyclic, then the group itself must be cyclic since any group is an improper subgroup of itself. However, if every proper subgroup of a group is cyclic, this does not imply the group itself is cyclic.

Example 16 Let $T = \{ \langle 0,0 \rangle, \langle 0,1 \rangle, \langle 1,0 \rangle, \langle 1,1 \rangle \}$. Then T is the set of all ordered pairs in 2-arithmetic and defined $*$ on T by element-wise addition in 2-arithmetic. Then $[T; *]$ is a group with $\langle 0,0 \rangle$ as identity and each element its own inverse.

$T_1 = \{ \langle 0,0 \rangle, \langle 0,1 \rangle \}$, $T_2 = \{ \langle 0,0 \rangle, \langle 1,0 \rangle \}$ and $T_3 = \{ \langle 0,0 \rangle, \langle 1,1 \rangle \}$ under $*$ are each proper cyclic subgroups of $[T; *]$ generated, respectively,

by $\langle 0,1 \rangle$, $\langle 1,0 \rangle$, and $\langle 1,1 \rangle$. T_1 , T_2 , and T_3 are the only proper subgroups of $[T; *]$ and each is cyclic but $[T; *]$ is not cyclic since no element of T generates T .

The group $[A_6; +]$ of Example 15 is cyclic with generators 1 and 5. The elements 2 and 4 generate $H_1 = \{0,2,4\}$; 3 generates $H_2 = \{0,3\}$; and 0 generates $H_3 = \{0\}$. A_6 , H_1 , H_2 , and H_3 are the only subgroups of $[A_6; +]$. Hence, each subgroup of the cyclic group $[A_6; +]$ is cyclic.

Homomorphisms and Isomorphisms

Certain types of mappings from one group into another provide a means of describing essential properties of groups and provide a way of recognizing when two seemingly different groups are mathematically the same.

Definition 2.17 Let G with binary operation $*$ and H with binary operation \circ be two groups. A (group) homomorphism of G into H is a mapping $\alpha: G \rightarrow H$ such that

- (i) Every $a \in G$ has a unique image $a\alpha \in H$.
- (ii) If $a, b \in G$, then $(a*b)\alpha = a\alpha \circ b\alpha$.

If the mapping α satisfies the additional condition that every $h \in H$ is an image of some $a \in G$, i.e., $h = a\alpha$, then α is a homomorphism of G onto H and H is called the homomorphic image of G under α . The set of all $a \in G$ such that $a\alpha \in H$ is called the preimage of H under the mapping α .

Condition (i) of Definition 2.17 is merely the condition most authors require of a correspondence between two sets in order for the correspondence to be called a mapping or function. Condition (ii) requires the mapping to be operation preserving. Both conditions are

necessary for a mapping to be a homomorphism. Some examples of correspondences between groups will now be considered.

Example 17 Let $[T; \cdot]$ be the group having 1 and -1 as its elements under the operation of ordinary multiplication and let $[A_4; +]$ be the additive group in 4-arithmetic. If α is the correspondence from T into A_4 such that $1\alpha = 0$, $-1\alpha = 1$, $-1\alpha = 2$, and $-1\alpha = 3$, then $(-1 \cdot 1)\alpha = -1\alpha = -1\alpha + 0 = (-1\alpha) + (1\alpha)$ so that for one choice of -1α , α is operation preserving. Similar conditions hold for other products in S . Also, α is onto $[A_4; +]$ but is not a homomorphism since (i) of the definition is not satisfied. If β is defined from T into A_4 such that $1\beta = 0$ and $-1\beta = 1$, then β satisfies (i) of the definition but $(-1 \cdot -1)\beta = 1\beta = 0$ while $(-1\beta) + (-1\beta) = 1 + 1 = 2$ so that β does not preserve operations and is not a homomorphism. If γ is defined from T into A_4 such that $1\gamma = 0$ and $-1\gamma = 2$ then γ is a homomorphism of T into A_4 .

Theorem 2.18 In any homomorphism between two groups G and G' , their identity elements correspond; and if $x \in G$ and $x' \in G'$ correspond, then their inverses also correspond.

All homomorphisms must satisfy Theorem 2.18 but maps may satisfy the conclusion of the theorem without being homomorphisms.

Example 18 Let $[A_3; +]$ be the additive group in 3-arithmetic and let $[S; *]$ be the group given in Example 12. If β is defined from A_3 into S by $0\beta = 0$, $1\beta = 3$, and $2\beta = 5$, then β is a mapping that satisfies the conclusion of Theorem 2.18 but β is not a homomorphism since, for example, $(2+2)\beta = 1\beta = 3$ while $(2\beta) * (2\beta) = 5 * 5 = 6$. If

α is defined from A_3 into S by $0\alpha = 0$, $1\alpha = 4$, and $2\alpha = 6$, then α is a homomorphism and satisfies Theorem 2.18. Note that the image of A_3 is the subgroup, S_3 , of $[S; *]$.

In Example 18, $[A_3; +]$ is cyclic and its homomorphic image $[S_3; *]$ is also cyclic. The next theorem establishes this fact formally.

Theorem 2.19 The homomorphic image of any cyclic group is cyclic.

If the image of a group G under a mapping is a cyclic group, this does not imply that G is cyclic.

Example 19 Let $[T; *]$ be the group given in Example 16 and $[A_2; +]$ be the additive group in 2-arithmetic. Define α from T onto A_2 by $\langle 0, 0 \rangle \alpha = \langle 0, 1 \rangle \alpha = 0$ and $\langle 1, 0 \rangle \alpha = \langle 1, 1 \rangle \alpha = 1$. Then A_2 is the homomorphic image of T under α and A_2 is cyclic but T is not cyclic as noted in Example 16.

If a map from one group into another is known to be a homomorphism and satisfies some additional conditions, then the map establishes additional relationships between the groups.

Definition 2.20 If α is a homomorphism of a group G onto a group H such that α is a one-to-one mapping, then α is said to be an isomorphism and G and H are said to be isomorphic.

The properties onto and one-to-one are both essential to an isomorphism. In Example 19 the homomorphism α is onto A_2 but is not one-to-one so that $[T; *]$ and $[A_2; +]$ are not isomorphic.

Example 20 Let $A_{10}^P = \{1, 3, 7, 9\}$, the set of all positive integers

less than 10 and relatively prime to 10. A_{10}^P under multiplication in 10-arithmetic is a cyclic group of order 4 with generators 3 and 7. Let $[A_8;+]$ be the additive group in 8-arithmetic. Define α from $[A_{10}^P; \cdot]$ into $[A_8;+]$ by $1\alpha = 0$, $3\alpha = 2$, $7\alpha = 6$, and $9\alpha = 4$. The mapping α is a one-to-one homomorphism of A_{10}^P into A_8 but is not an isomorphism between A_{10}^P and A_8 since α is not onto. However, α is an isomorphism between A_{10}^P and its image, the set $\{0,2,4,6\}$ which, under addition in 8-arithmetic, is a cyclic subgroup of $[A_8;+]$ of order 4 with generators 2 and 6.

Not all onto, one-to-one maps are isomorphisms.

Example 21. Let $[A_4;+]$ be the additive group in 4-arithmetic and define $A_8^P = \{1,3,5,7\}$ with operation \cdot , multiplication in 8-arithmetic. Then $[A_8^P; \cdot]$ is a group of order 4 and many one-to-one maps exist from A_4 onto A_8^P but none of these is a homomorphism and, hence, none are isomorphisms. $[A_8^P; \cdot]$ is a representation of the noncyclic group of order 4, sometimes called the Klein-4 group. $[A_8^P; \cdot]$ is isomorphic to $[T; *]$ of Example 16 under the mapping α defined by $1\alpha = \langle 0,0 \rangle$, $3\alpha = \langle 0,1 \rangle$, $5\alpha = \langle 1,0 \rangle$, and $7\alpha = \langle 1,1 \rangle$.

Notice that if a group G is isomorphic to a group H , then H is isomorphic to G . For example, if γ is defined from $[T; *]$ to $[A_8^P; \cdot]$ of Example 21 by $\langle 0,0 \rangle\gamma = 1$, $\langle 0,1 \rangle\gamma = 3$, $\langle 1,0 \rangle\gamma = 5$, and $\langle 1,1 \rangle\gamma = 7$, then γ is an isomorphism from T onto A_8^P where as α of Example 21 is an isomorphism from A_8^P onto T .

All cyclic groups are isomorphic to some arithmetic system based on the integers or some subset of the integers.

Theorem 2.21 (a) Every cyclic group of infinite order is isomorphic to the additive group I of integers. (b) Every cyclic group of finite order n is isomorphic to the additive group $I/(n)$ of integers modulo n .

Since the integers do not form a group under multiplication, examples of infinite order groups from this set must be subgroups of the additive group $[I; +]$. For any fixed integer $k \neq 0$, the set $K = \{a : a = ki \text{ for some } i \in I\}$ is an additive group of infinite order isomorphic to $[I; +]$ under the isomorphism $n\alpha = kn$ for every $n \in I$.

The group $[A_{10}^P; \cdot]$ of Example 20 is a cyclic group of order 4 and is isomorphic to the additive group $I/(4)$ under the isomorphism β defined by $1\beta = \bar{0}$, $3\beta = \bar{1}$, $7\beta = \bar{3}$, and $9\beta = \bar{2}$ where \bar{n} denotes the equivalence set modulo 4 containing n .

The additive group $I/(n)$ of integers modulo n is a cyclic group of order n , with generator the set $\bar{1}$ in n -arithmetic for every integer n greater than 1. In the case when $n = 1$, $I/(1)$ has only one residue class, $\bar{0}$, and $I/(1)$ is a group of order 1. Since $[I; +]$ is a group of infinite order which is also cyclic, cyclic groups of all orders exist.

A one-to-one mapping of a set A onto itself is called a permutation of the set A . The set S_n of $n!$ permutations of n symbols with product (composition) of maps as its operation is a group called the symmetric group on n symbols. Any subgroup of S_n is called a permutation group on n symbols. If A is the ordered set $\langle a, b, c, d \rangle$, then $\alpha = \begin{pmatrix} a & b & c & d \\ c & a & b & d \end{pmatrix}$ means the permutation of A which produces the ordered set $\langle c, a, b, d \rangle$. Similar notation is used for permutations of any finite ordered set.

Theorem 2.22 (Cayley) Every finite group of order n is isomorphic

to a permutation group on n symbols.

Permutation groups on n symbols do not have to be isomorphic to a group of order n since permutation groups on n symbols do not have to be of order n .

Example 22 Let $[A_8^D; \cdot]$ be the group defined in Example 21. A multiplication table for $[A_8^D; \cdot]$ is given in the Cayley square below.

\cdot	1	3	5	7
1	1	3	5	7
3	3	1	7	5
5	5	7	1	3
7	7	5	3	1

A permutation group of order 4 which is isomorphic to $[A_8^D; \cdot]$ is $[P; \circ]$ where \circ is ordinary map composition and $P = \{p_1, p_2, p_3, p_4\}$ where $p_1 = \begin{pmatrix} 1 & 3 & 5 & 7 \\ 1 & 3 & 5 & 7 \end{pmatrix}$, $p_2 = \begin{pmatrix} 1 & 3 & 5 & 7 \\ 3 & 1 & 7 & 5 \end{pmatrix}$, $p_3 = \begin{pmatrix} 1 & 3 & 5 & 7 \\ 5 & 7 & 1 & 3 \end{pmatrix}$, and $p_4 = \begin{pmatrix} 1 & 3 & 5 & 7 \\ 7 & 5 & 3 & 1 \end{pmatrix}$. Notice p_i is the i th column in the Cayley square for $[A_8^D; \cdot]$. A group constructed from the operation table of a group G , in a manner similar to the way $[P; \circ]$ was constructed, is sometimes called the right regular representation of G . The Cayley square for $[P; \circ]$ is given below. $[P; \circ]$ is a permutation group of the four symbols 1, 3, 5, and 7.

\circ	P ₁	P ₂	P ₃	P ₄
P ₁	P ₁	P ₂	P ₃	P ₄
P ₂	P ₂	P ₁	P ₄	P ₃
P ₃	P ₃	P ₄	P ₁	P ₂
P ₄	P ₄	P ₃	P ₂	P ₁

An isomorphism α from $[A_8^D; \cdot]$ onto $[P; \circ]$ is defined as follows;
 $1\alpha = p_1$, $3\alpha = p_2$, $5\alpha = p_3$, and $7\alpha = p_4$.

Cosets

Suppose H is a subgroup of a group $[G; *]$. Then for any $a \in G$, the set $aH = \{a * h : h \in H\}$ is called the left coset of H in G , generated by a . Similarly, $Ha = \{h * a : h \in H\}$ is called the right coset of H in G , generated by a . Attention will be given primarily to right cosets; similar results hold for left cosets. Notice that cosets of H in G are subsets of G whose elements can be represented in a special way.

Example 23 Let $[M; \cdot]$ be the group of nonsingular 2×2 matrices under multiplication as defined in Example 10. If $H = \{a, b\}$, then $[H; \cdot]$ is a subgroup of $[M; \cdot]$ and $cH = \{c, f\}$ since $c = c \cdot a$ and $f = c \cdot b$. Also the right coset $Hc = \{c, e\}$ since $c = a \cdot c$ and $e = b \cdot c$. Notice that $cH \neq Hc$, i.e., the elements of H do not commute under multiplication with c . By similar arguments, $aH = bH = Ha = Hb = H$, $dH = eH = \{d, e\}$, $fH = cH = \{f, c\}$, $Hc = He = \{c, e\}$, and $Hd = Hf = \{d, f\}$.

In Example 23 each coset of H in $[M; \cdot]$ has two elements and there are the same number, three, of left cosets as right cosets. Notice that three times two, the order of the subgroup H , equals the order of the group $[M; \cdot]$.

Theorem 2.23 (Lagrange) The order of each subgroup of a finite group G is a divisor of the order of G .

Example 24 Consider the additive group $[A_{12}; +]$.

$K = \{0, 1, 5, 6, 7, 11\}$ is a subset of A_{12} which has six elements and each of these elements has its inverse in K but K is not a subgroup of A_{12} since it is not closed. Thus, if the order of a subset K

divides the order of the group, this does not imply K is a subgroup of A_{12} . $H_0 = \{0\}$, $H_1 = \{0,6\}$, $H_2 = \{0,4,8\}$, $H_3 = \{0,3,6,9\}$, $H_4 = \{0,2,4,6,8,10\}$, and $H_5 = A_{12}$ are all the subgroups of $[A_{12};+]$. The order of $[A_{12};+]$ is 12 and H_0, H_1, H_2, H_3, H_4 , and H_5 are subgroups having, respectively, orders 1, 2, 3, 4, 6, and 12. Hence, there exists a subgroup of order n for every positive integer n that divides the order of A_{12} .

If a group G has order n and m is a positive integer divisor of n , then a subgroup of G of order m may, but does not always, exist. The author has not found an example from elementary number theory demonstrating this fact. The alternating group, A_4 , on four symbols is a group of order 12 with no subgroup of order 6 although subgroups of orders 1, 2, 3, 4, and 12 do exist. The alternating group on four symbols is defined and these facts stated by Dean [8] on page 58.

The order of an element of a finite group, like the order of a subgroup, must satisfy divisibility properties.

Theorem 2.24 If G is a finite group of order n , then the order of any element $a \in G$ is a divisor of n .

In the additive group $[A_{12};+]$, 0 is of order 1; 6 is of order 2; 4 and 8 are of order 3; 3, 6, and 9 are of order 4; 2 and 10 are of order 6; and 1, 5, 7, and 11 are of order 12. Every subgroup of A_{12} given in Example 24 contains the element 0 of order 1. The element 6 of order 2 is contained in H_1, H_3, H_4 , and H_5 of orders 2, 4, 6, and 12, respectively, but 6 is not contained in H_2 of order 3. The other elements of A_{12} are also seen to satisfy Theorem 2.24.

The alternating group on four symbols, A_4 , mentioned above has no

element of order 6 since it has no subgroup of order 6. Since A_4 is of order 12, it is seen that elements of every dividing order do not always exist in a group.

Notice, also, that there is no element of order n in any noncyclic group of order n . If the order of a group G is a prime, there must be an element in G of order n where n is the order of G .

Theorem 2.25 Every group of prime order is cyclic. Moreover, every element except the identity is a generator of the group.

The additive group $[A_{12};+]$ is cyclic with 1, 5, 7, and 11 as generators even though the order of A_{12} is 12, not a prime. Most of the elements of A_{12} do not, however, generate A_{12} but subgroups of A_{12} .

Example 25 The additive group $[A_5;+]$ is of prime order 5 with identity element 0. Using the diagram form introduced before Example 14, Figures 5, 6, 7, and 8, respectively, show that 1, 2, 3, and 4 are all generators of A_5 .

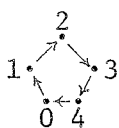


Figure 5

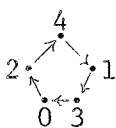


Figure 6

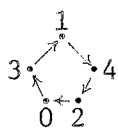


Figure 7

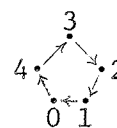


Figure 8

The order of an element of a finite group must be less than or equal to the order of the group by Theorem 2.24. The following is true of every element of a finite group.

Theorem 2.26 If G is a finite group of order n with identity u , then $a^n = u$ for each $a \in G$.

Notice that the theorem is stated in multiplicative notation. The number 2 is an element of the additive group $[A_6; +]$ of order 6 with identity 0, but $2^6 = 4 \neq 0$ in 6-arithmetic. For $[A_6; +]$ the theorem means that, for example, $2+2+2+2+2+2 = 6 \cdot 2 = 0$ and this is seen to be true in 6-arithmetic. Similar equalities hold for all the elements in A_6 .

If G is a finite group with identity u and $a^n = u$ for each $a \in G$, this does not imply G is of order n . Every element in the group $[A_8^P; \cdot]$ of Example 21 is of order 2, i.e., $a^2 = 1$ for every $a \in A_8^P$. $[A_8^P; \cdot]$ is not, however, of order 2 but of order 4.

Invariant Subgroups

A subgroup H of a group G is called an invariant (normal) subgroup of G and is said to be invariant in G if $gH = Hg$ for every $g \in G$.

A group may have some subgroups which are invariant and some which are not invariant. In Example 23 it was found that the subgroup $H = \{a, b\}$ is not an invariant subgroup of the group $[M; \cdot]$ since, for example, $dH \neq Hd$. The subgroup $K = \{a, e, f\}$ is an invariant subgroup of M since it satisfies the definition.

A characterization of an invariant subgroup is given in the following theorem.

Theorem 2.27 If H is a subgroup of a group G and if $g^{-1}hg \in H$ for all $g \in G$ and all $h \in H$, then H is an invariant subgroup of G .

Since Theorem 2.27 is a characterization, it furnishes another way to determine if a subgroup is invariant. For the subgroup H of $[M; \cdot]$ defined in Example 23, $c^{-1}bc = cbc = (cb)c = fc = d \notin H$ so that H is seen, independent of the definition, to not be an invariant subgroup of M .

Checking the special products given in Theorem 2.27 is not sufficient to determine if any given proper subset of a group is an invariant subgroup.

Example 26 Consider the additive group $[A_{10};+]$ and the subset $S = \{0,3,7\}$. The products $g^{-1} \cdot h \cdot g \in S$ for all $g \in A_{10}$ and all $h \in S$. For example, $(-8)+3+8 = 2+3+8 = (2+3)+8 = 5+8 = 3$ in 10-arithmetic and $3 \in S$. S even contains the identity of $[A_{10};+]$ and inverses for each of its elements but S is not an invariant subgroup of $[A_{10};+]$ since S is not closed and, hence, is not a subgroup of A_{10} , e.g., $3+3 = 6 \notin S$.

The property of a subgroup being invariant in a group G carries over to certain subgroups of G .

Theorem 2.28 If H is an invariant subgroup of a group G and if H is also a subgroup of a subgroup K of G , then H is an invariant subgroup of K .

Example 27 Let $[G;\cdot]$ be the group of all nonsingular 2×2 matrices over 3-arithmetic with matrix multiplication as the group operation. $[G;\cdot]$ is a group of order 48 with $[K;\cdot]$ as a subgroup of order 12 where K is the set of all upper-triangular matrices in G . Every element in the group K is nonsingular and has 0 as its lower left entry. If $H = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix} \right\}$, then $[H;\cdot]$ is a subgroup of $[K;\cdot]$ and $[G;\cdot]$. Notice that each matrix in H commutes under multiplication with every matrix in G so that $gH = Hg$ for every $g \in G$. Hence, H is an invariant subgroup of G . But, since $H \subset K \subset G$, $kH = Hk$ for every $k \in K$ and H is an invariant subgroup of K . The conclusion of Theorem 2.28 says nothing about whether K is an

invariant subgroup of G . In fact, K is not an invariant subgroup of G since, for example, if $g = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$, $k = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$, and $h = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}$, then $g \in G$, $k \in K$ and $k \cdot g = h \in Kg$ but $h \notin gK$.

Invariant subgroups arise naturally when considering homomorphisms between groups.

Theorem 2.29 Under any homomorphism of a group $[G; *]$ with identity element u into a group $[G'; \circ]$ with identity element u' , the subset S of all elements of G which are mapped onto u' is an invariant subgroup of G .

Thus, if α is a known homomorphism from a group G into a group G' , then the preimage of the identity of G' is an invariant subgroup of G . If, however, α is a map which maps an invariant subgroup of G onto the identity of G' , α is not necessarily a homomorphism.

Example 28 Let $[A_{10}; +]$ and $[A_5; +]$ be the additive groups in 10 and 5-arithmetic, respectively. Define α from A_5 into A_{10} by $\alpha a = 2a$ for each $a \in A_5$. α is a homomorphism from A_5 into A_{10} and the subgroup $\{0\}$ of A_5 is the preimage of the identity, 0, of A_{10} . $\{0\}$ is an invariant subgroup of A_5 . $H = \{0, 5\}$ is an invariant subgroup of $[A_{10}; +]$. If $0\beta = 5\beta = 0$ and $a\beta = 3$ for all $a \in A_{10}$ such that $a \neq 0$ and $a \neq 5$, then β is a mapping from A_{10} into A_5 and the preimage of the identity of A_5 is an invariant subgroup of $[A_{10}; +]$ but β is not a homomorphism since $(1+1)\beta = 2\beta = 3$ but $(1\beta)+(1\beta) = 3+3 = 1$ in A_5 .

The homomorphism of Theorem 2.29 from G into G' may be onto G' without changing the conclusion of the theorem. Define γ from $[A_{10}; +]$ onto

$[A_5; +]$ by $0\gamma = 5\gamma = 0$, $1\gamma = 6\gamma = 1$, $2\gamma = 7\gamma = 2$, $3\gamma = 8\gamma = 3$, and $4\gamma = 9\gamma = 4$. Then γ is an onto homomorphism and $\{0, 5\}$ is an invariant subgroup of A_{10} .

Quotient Groups

Definition 2.30 Let H be an invariant subgroup of a group G with binary operation $*$. The set, denoted G/H , consisting of all the (right) cosets of H in G , is called the set of cosets of H in G . Define the binary operation \circ on G/H by $(Ha)\circ(Hb) = \{(h_1*a)*(h_2*b) : h_1, h_2 \in H\}$ for all $Ha, Hb \in G/H$.

The subgroup H of Definition 2.30 must be invariant in order for \circ to be a binary operation.

Example 29 The subgroup $H = \{a, b\}$ of the group $[M; \cdot]$ of Example 10 is not an invariant subgroup of M . $(Hc)\circ(Hd) = \{a, b, c, e\} = S$ which is not a right coset of H in M so that \circ is not a binary operation on M/H . The subgroup $K = \{a, e, f\}$ is an invariant subgroup of M and \circ is a binary operation on M/K . In fact, M/K under \circ is a group with the following Cayley square.

\circ	K	Kb
K	K	Kb
Kb	Kb	K

This result generalizes as seen by the next theorem.

Theorem 2.31 The set G/H with binary operation \circ is a group (called a quotient group or a factor group) if H is an invariant subgroup of G .

It can be proved that if H is a subgroup of the group G , the product, \circ , of any two right cosets of H in G is again a right coset of H in G if and only if H is an invariant subgroup of G . Hence, if the set G/H is a group under the product, \circ , then H is an invariant subgroup of G . The set M/H of Example 29, under the product, \circ , is not a group while M/K under \circ is a group. Both H and K are subgroups of M but only K is an invariant subgroup of M .

The order of a quotient group of a finite group G depends on the order of G .

Theorem 2.32 If H , of order m , is an invariant subgroup of group G , of order n , then the quotient group G/H is of order n/m .

The order of the group M of Example 29 is 6, the order of K is 3, and the order of M/K is $2 = 6/3$. Another example of Theorem 2.32 is now given.

Example 30 Consider the additive group $[A_{12};+]$ and the invariant subgroup $[H;+]$ of $[A_{12};+]$ where $H = \{0,3,6,9\}$. The orders of A_{12} , H , and A_{12}/H are, respectively, 12, 4, and 3. For every divisor n of 12, there exists an invariant subgroup of A_{12} of order n and, hence, there also exists a quotient group of A_{12} of order n .

If m is a positive integer divisor of n , the order of a group G , this does not imply that G has a quotient group of order n/m . The only subgroups of order 2 of the group $[M;\cdot]$ of Example 10 are $H_1 = \{a,b\}$, $H_2 = \{a,c\}$, and $H_3 = \{a,d\}$ but none of these subgroups is an invariant subgroup of M since $H_i e \neq e H_i$ for $i = 1, 2, \text{ or } 3$. Hence, no quotient group of $[M;\cdot]$ exists of order $3 = 6/2$ although 2 divides 6, the order

of M .

If the quotient group of a group G is of finite order, this does not imply G is of finite order.

Example 31 Consider the subset $H = \{3n:n \in I\}$ of the integers I .

$[H;+]$ is an invariant subgroup of $[I;+]$ since $H+a = a+H$ (additive coset notation) for every $a \in I$. $I/H = \{H,H+1,H+2\}$ is a quotient group of I under the coset operation \circ defined by $(H+a)\circ(H+b) = H+c$ for $a,b,c \in \{0,1,2\}$ where c is equal to $a+b$ modulo 3. $[I/H;\circ]$ is a finite group of order 3 although $[I;+]$ is of infinite order.

Homomorphisms exist between a group and any of its quotient groups.

Theorem 2.33 If H is an invariant subgroup of group G , define the mapping α from G to G/H by $a\alpha = Ha$ for all $a \in G$. Then α is a homomorphism of G onto G/H .

For the groups $[I;+]$ and $[I/H;\circ]$ of Example 31, the mapping α defined in Theorem 2.33 may be described as follows: $a\alpha = H$ if $a = 3n$, $a\alpha = H+1$ if $a = 3n+1$, and $a\alpha = H+2$ if $a = 3n+2$ where n is any integer. Notice that α is a mapping from I onto I/H since $0\alpha = H$, $1\alpha = H+1$, and $2\alpha = H+2$. Straight forward calculations can be used to verify that α is a homomorphism, e.g., $[(3n+1)+(3m+2)]\alpha = [3(n+m)+3]\alpha = [3(n+m+1)]\alpha = H$ while $(3n+1)\alpha\circ(3m+2)\alpha = (H+1)\circ(H+2) = H$ so that $[(3n+1)+(3m+2)]\alpha = (3n+1)\alpha\circ(3m+2)\alpha$.

If the subgroup H in Theorem 2.33 is not invariant in the group G , then α of the theorem cannot be a homomorphism since G/H is not a group.

The structure of a particular quotient group is limited by the structure of the original group.

Theorem 2.34 Any quotient group of a cyclic group is cyclic.

The quotient group $[I/H;0]$ of $[I;+]$ given in Example 31 is cyclic of order 3 with generators $H+1$ and $H+2$. $[I;+]$ is cyclic with generators 1 and -1 .

A quotient group of a group G may be cyclic even though G is not cyclic. M/K of Example 29 is cyclic of order 2 with generator Kb even though $[M;\cdot]$ is not cyclic.

Products of Subgroups

Definition 2.35 Let H and K be two subgroups of a group G with binary operation $*$. The product of H and K is denoted HK where $HK = \{a \in G : a = h*k, h \in H, k \in K\}$.

Notice that the product of two subgroups H and K of a group G need not be a group, i.e., HK need not be a subgroup of G .

Example 32 The subgroups $H = \{a,b\}$ and $K = \{a,c\}$ of $[M;\cdot]$ of Example 10 are not invariant in M . $HK = \{a,b,c,e\}$ which is not a subgroup of M and, hence, is not a group. $KH = \{a,b,c,f\}$ is not a group either. The product of subgroups is not commutative since $HK \neq KH$. If L is the subgroup of $[M;\cdot]$ with elements $a, e, \text{ and } f$, then $HL = LH = M$ is a group. Notice L is invariant in M .

The product of two subgroups of a group G may be a proper subgroup of G as seen in the next example.

Example 33 Consider the subgroups $H = \{0,6\}$ and $K = \{0,4,8\}$ of the additive group $[A_{12};+]$ in 12-arithmetic. $HK = L = \{0,2,4,6,8,10\}$ and L of order 6 is a proper subgroup of $[A_{12};+]$ of order 12.

Notice that H , K , and L are all invariant subgroups of A_{12} .

Example 33 also serves as an example of the next theorem.

Theorem 2.36 If H and K are invariant subgroups of a group G , then HK is an invariant subgroup of G .

If H and K are subgroups of a group G such that HK is an invariant subgroup of G , this does not imply that both H and K are invariant subgroups of G . In Example 32 $HL = M$ which is obviously invariant in M but H is not invariant in M .

Composition Series

An invariant subgroup H of a group G is called a maximal invariant subgroup of G provided there exists no proper invariant subgroup K of G having H as a proper subgroup. The invariant subgroup K of $[M; \cdot]$ given in Example 29 is a maximal invariant subgroup of M since no proper subgroup of M properly contains K . The subgroup H given in the same example is maximal in M but is not a maximal invariant subgroup of M since it is not invariant in M .

Definition 2.37 Let G be a group with identity element u . A finite sequence of subgroups $G = H_0, H_1, \dots, H_r = \{u\}$ is called a composition series of G if each H_i is a maximal invariant subgroup of H_{i-1} for $i = 1, 2, \dots, r$. This composition series is said to have $r+1$ terms and be of length $r+1$. The groups $H_0/H_1, H_1/H_2, \dots, H_{r-1}/H_r$ are called the quotient groups of the composition series.

Example 34 The additive group $[A_4; +]$ in 4-arithmetic has a maximal invariant subgroup $K = \{0, 2\}$. The series $A_4 = H_0, K = H_1,$

$\{0\} = H_2$ is the only composition series of A_4 . A_4/K and K/H_2 are the quotient groups of the composition series.

Not every group has a composition series. The additive group $[I;+]$ of integers has the series of subgroups $I = H_0, H_1, H_2, \dots, H_i, \dots$ where $H_1 = \{2n:n \in I\}$, $H_2 = \{4n:n \in I\}$, and, in general $H_i = \{2^i n:n \in I\}$ for every nonnegative integer i . Each H_i is invariant in I and, hence, H_i is invariant in each H_j for $0 \leq j \leq i$. Furthermore, H_i is maximal in H_{i-1} for every positive integer i . But, $H_0, H_1, H_2, \dots, H_i, \dots$ is not a composition series since the series is not finite—in fact, no composition series exists for $[I;+]$. The quotient groups $H_0/H_1, H_1/H_2, \dots, H_{i-1}/H_i, \dots$ still exist and $H_{i-1}/H_i = \{H_i, H_i+2^{i-1}\}$ is a cyclic group of order 2 for every positive integer i .

Theorem 2.38 Every finite group has at least one composition series.

$[A_4;+]$ was seen, in Example 34, to have only one composition series. Some groups have more than one composition series.

Example 35 Consider the additive group $[A_{12};+]$ in 12-arithmetic. Let $H_0 = K_0 = A_{12}$, $H_1 = \{0,2,4,6,8,10\}$, $K_1 = \{0,3,6,9\}$, $H_2 = \{0,4,8\}$, $K_2 = \{0,6\}$, and $H_3 = K_3 = \{0\}$. Then the H_i and K_i are invariant subgroups of $[A_{12};+]$ for $i = 0, 1, 2, 3$. Furthermore, both H_0, H_1, H_2, H_3 and K_0, K_1, K_2, K_3 are composition series since the H_i and K_i satisfy the maximal invariant conditions of Definition 2.37. The series H_0, H_1, K_2, H_3 is another composition series for the group A_{12} . A_{12} has two distinct maximal invariant subgroups, H_1 and K_1 . H_1 also has two distinct maximal invariant subgroups, H_2 and K_2 .

Notice that all three composition series of the group $[A_{12};+]$ in Example 35 are of the same length, 4. Quotient groups of the composition series are also related as seen in the next theorem.

Theorem 2.39 (Jordan-Hölder) For any finite group with distinct composition series, all series have the same number of terms and the quotient groups of any two series can be put into one-to-one correspondence so that corresponding quotient groups are isomorphic.

Example 36 Each composition series given in Example 35 has three quotient groups associated with it. The quotient groups of the composition series H_0, H_1, H_2, H_3 are $H_0/H_1 = A_{12}/H_1$, H_1/H_2 , and H_2/H_3 . The composition series K_0, K_1, K_2, K_3 has the quotient groups $K_0/K_1 = A_{12}/K_1$, K_1/K_2 , and K_2/K_3 while the composition series H_0, H_1, K_2, H_3 has the quotient groups $H_0/H_1 = A_{12}/H_1$, H_1/K_2 , and K_2/H_3 . Many one-to-one correspondences exist between the quotient groups of any two of the given series. In fact, there may be more than one of these one-to-one correspondences such that the corresponding quotient groups are isomorphic. The quotient groups H_0/H_1 , H_1/H_2 , and H_2/H_3 are of orders 2, 2, and 3, respectively, while the quotient groups K_0/K_1 , K_1/K_2 and K_2/K_3 have orders 3, 2, and 2, respectively. Groups must be of the same order if they are isomorphic. For this example, the mapping α , which associates H_0/H_1 with K_1/K_2 , H_1/H_2 with K_2/K_3 , and H_2/H_3 with K_0/K_1 , is one correspondence which satisfies Theorem 2.39. H_0/H_1 is isomorphic to K_1/K_2 under the isomorphism α , defined from H_0/H_1 into K_1/K_2 by $H_1\alpha_1 = K_2$ and $(H_1+1)\alpha_1 = K_2+3$. The map α_2 defined by $H_2\alpha_2 = K_3$ and $(H_2+2)\alpha_2 = K_3+6$ is an isomorphism from H_1/H_2 into K_2/K_3 . Similarly, α_3 defined by

$H_3\alpha_3 = K_1$, $(H_3+4)\alpha_3 = H_1+1$, and $(H_3+8)\alpha_3 = K_1+2$ is an isomorphism from H_2/H_3 into K_0/K_1 . Another correspondence satisfying Theorem 2.39 for the quotient groups of the same two series is defined by the mapping β which associates H_0/H_1 with K_2/K_3 , H_1/H_2 with K_1/K_2 , and H_2/H_3 with K_0/K_1 . Similar correspondences can be established for the quotient groups of any two composition series of $[A_{12};+]$.

It was helpful in Example 36 to know the number of distinct cosets in each quotient group since isomorphic groups must be of the same order. The number of distinct (right) cosets of the subgroup H in the group G is called the index of H in G and is denoted by $[G:H]$. For the groups given in Example 35, $[A_{12}:H_1] = 2$, $[A_{12}:K_1] = 3$, and $[A_{12}:H_2] = 4$.

The next theorem gives, for a finite group G , a characterization of a subgroup of a quotient group of G , using the concept of the index of a group.

Theorem 2.40 Let H be an invariant subgroup of a finite group G . A set P of cosets of H is a subgroup of index t of G/H if and only if K , the set of group elements which belong to the cosets in P , is a subgroup of index t of G .

A set P of cosets of H , referred to in Theorem 2.40, is just a subset of the known group G/H . Hence, the theorem reduces the problem of recognizing subgroups of a quotient group to recognizing subgroups of an ordinary group.

Example 37 Consider the additive group $[A_{20};+]$ in 20-arithmetic and the quotient group A_{20}/H of A_{20} where the invariant subgroup $H = \{0,10\}$. $A_{20}/H = \{H, H+1, H+2, H+3, H+4, H+5, H+6, H+7, H+8, H+9\}$ is a

group of order 10. Each coset of H has two elements of A_{20} , e.g., $H+1 = \{1,11\}$ and $H+4 = \{4,14\}$. By Lagrange's theorem, Theorem 2.23, the order of a subgroup of A_{20} divides 20. Thus, a subset P of A_{20}/H may, by Theorem 2.40, be a subgroup of A_{20}/H only if P contains 1, 2, 5, or 10 cosets of H since then the set K of Theorem 2.40 would be of order 2, 4, 10, or 20 and these numbers are the only positive even divisors of 20, the order of A_{20} . The subset $S = \{H+2, H+8\}$ contains two cosets of H but is not a subgroup of A_{20}/H since $(H+2) \cup (H+8) = \{2,12\} \cup \{8,18\} = \{2,8,12,18\} = N$ does not contain the identity of A_{20} and is, hence, not a subgroup of A_{20} . The subset $T = \{H, H+2, H+4, H+6, H+8\}$ of A_{20}/H is a subgroup of index 2 of A_{20}/H since $M = \{0,2,4,6,8,10,12,14,16,18\} = H \cup (H+2) \cup (H+4) \cup (H+6) \cup (H+8)$ is a subgroup of index 2 of A_{20} .

A characterization of an invariant subgroup of a quotient group is given in the next theorem.

Theorem 2.41 Let G be a group of order $n = rpt$, K be a subgroup of order rp of G , and H be an invariant subgroup of order r of both K and G . Then K is an invariant subgroup of G if and only if K/H is an invariant subgroup of G/H .

The subgroup M of A_{20} , given in Example 37, is an invariant subgroup of order $2 \cdot 5 = 10$ of the group $[A_{20}; +]$ of order $2 \cdot 2 \cdot 5 = 20$. $H = \{0,10\}$ is an invariant subgroup of order 2 of both M and A_{20} . Hence, by Theorem 2.41, T of Example 37 is an invariant subgroup of A_{20}/H since $T = M/H$.

In Example 27 the group $[G; \cdot]$ is of order $48 = 2 \cdot 6 \cdot 8$, K is a subgroup of order $12 = 2 \cdot 6$ of G , and H is an invariant subgroup of order 2

of both K and G . It was found that K is not an invariant subgroup of G . Hence, without further investigation, it is known by Theorem 2.41 that the subgroup K/H of G/H is not invariant in G/H .

An interesting isomorphism involving a quotient group of a quotient group appears in the next theorem.

Theorem 2.42 Let H and K be invariant subgroups of G with H an invariant subgroup of K , and let $P = K/H$ and $S = G/H$. Then the quotient groups S/P and G/K are isomorphic.

Notice that S/P of Theorem 2.42 is $(G/H)/(K/H)$ and that S/P and G/K are representations of the same abstract group, i.e., S/P and G/K are isomorphic.

Example 38 The additive group $[A_8; +]$ in 8-arithmetic has invariant subgroups $H = \{0, 4\}$ and $K = \{0, 2, 4, 6\}$. H is also invariant in K so that A_8/H , K/H , and A_8/K are groups by Theorem 2.31. Since K is invariant in A_8 , Theorem 2.41 implies that K/H is invariant in A_8/H so that $(A_8/H)/(K/H)$ is also a group. $A_8/K = \{K, K+1\}$, $A_8/H = \{H, H+1, H+2, H+3\}$, and $K/H = \{H, H+2\}$. Hence, $(A_8/H)/(K/H) = \{(K/H), (K/H)+1\}$ and the mapping α from $(A_8/H)/(K/H)$ into A_8/K defined by $(K/H)\alpha = H$ and $[(K/H)+1]\alpha = H+2$ establishes the isomorphism asserted in Theorem 2.42.

A group G is said to be simple or a simple group if the only invariant subgroups of G are itself and the identity subgroup. Any group having no proper subgroups is, of course, simple, e.g., the additive group $[A_5; +]$ in 5-arithmetic is simple.

The author has not found an example from elementary number theory of

a simple group having proper subgroups. In some of the more advanced courses in modern algebra students are asked in a problem to prove that the alternating group A_n is simple if $n \geq 5$. Barnes [3] defines the alternating group A_n and states the above mentioned problem on page 45. The alternating group A_5 is a simple group of order 60. The permutation $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 1 & 4 & 3 & 5 \end{pmatrix}$ is an element of A_5 of order 2 and, hence, generates a proper subgroup of A_5 of order 2. Thus, the alternating group A_5 is a simple group having a proper subgroup.

A characterization of a simple quotient group is given in the next theorem.

Theorem 2.43 Let H be an invariant subgroup of group G . Then H is a maximal invariant subgroup of G if and only if G/H is simple.

Example 39 Consider the additive group $[A_{20};+]$ and its subgroups $H = \{0,2,4,6,8,10,12,14,16,18\}$ and $K = \{0,4,8,12,16\}$. By Theorem 2.43 A_{20}/H is simple while A_{20}/K is not simple since H is maximal invariant in A_{20} while K is invariant but not maximal invariant in A_{20} .

The next theorem establishes isomorphisms between special types of quotient groups.

Theorem 2.44 Let H and K be distinct maximal invariant subgroups of a group G . Then

- (i) $D = H \cap K$ is an invariant subgroup of G .
- (ii) H/D is isomorphic to G/K and K/D is isomorphic to G/H .

Example 40 Let G be the additive group $[A_{12};+]$ in 12-arithmetic

which has two distinct maximal invariant subgroups $H = \{0, 2, 4, 6, 8, 10\}$ and $K = \{0, 3, 6, 9\}$. Then $D = H \cap K = \{0, 6\}$ is an invariant subgroup of G and, hence, is an invariant subgroup of both of the subgroups H and K of G . Thus, H/D , G/K , K/D , and G/H are groups by Theorem 2.31 and are of orders 3, 3, 2, and 2, respectively, by Theorem 2.32. The mapping α defined from $H/D = \{D, D+2, D+4\}$ into $G/K = \{K, K+1, K+2\}$ by $D\alpha = K$, $(D+2)\alpha = K+1$, and $(D+4)\alpha = K+2$ establishes the isomorphism between H/D and G/K . If a mapping β is defined from $K/D = \{D, D+3\}$ into $G/H = \{H, H+1\}$ by $D\beta = H$ and $(D+3)\beta = H+1$, then β is an isomorphism between K/D and G/H .

Direct Products

Given a group G , other groups may be associated with G in a natural way. The study of subgroups and quotient groups provided ways of constructing new groups from the given group G . Another useful way of constructing new groups from a set of given groups will now be considered.

Definition 2.45 Let $[G; \circ]$ and $[H; \theta]$ be two groups and let $G \times H = \{ \langle g, h \rangle : g \in G, h \in H \}$. Define the binary operation $*$ on $G \times H$ by $\langle g, h \rangle * \langle g', h' \rangle = \langle g \circ g', h \theta h' \rangle$ for all $g, g' \in G$ and $h, h' \in H$.

The rule $*$ given in Definition 2.45 is indeed a binary operation if $[G; \circ]$ and $[H; \theta]$ are groups since $*$ is equivalent to the elementwise binary operations \circ and θ .

Theorem 2.46 If $[G; \circ]$ and $[H; \theta]$ are groups and if $G \times H$ with binary operation $*$ is defined as in Definition 2.45, then $[G \times H; *]$ is a group (called a direct product of G and H).

The group $[G \times H; *]$ is sometimes called an external direct product of the groups G and H to distinguish it from a similar construction called an internal direct product in which G and H are invariant subgroups of a known group. A variety of groups may be constructed in the form of direct products.

Example 41 Consider the additive group of integers $[I; +]$ and the group $[M; \cdot]$ of Example 10. Then Theorem 2.46 asserts that $[I \times M; *]$ is a group. The element $\langle 1, a \rangle$ is seen to be the identity and $\langle -n, x^{-1} \rangle$ is the inverse of $\langle n, x \rangle$ for each $n \in I$ and $x \in M$ where x^{-1} is the inverse of x in M (see the Cayley square given in Example 10). The operation $*$ is associative since $+$ and \cdot are associative in I and M , respectively. Notice that $I \times M$ is an infinite noncyclic nonabelian group since infinitely many different ordered pairs are in the set $I \times M$ and since, for example, $\langle 3, b \rangle * \langle 2, c \rangle = \langle 5, e \rangle$ while $\langle 2, c \rangle * \langle 3, b \rangle = \langle 5, f \rangle$ and $f \neq e$. $I \times M$ is noncyclic since no element of M generates M , i.e., M is not cyclic and, hence, no ordered pair in $I \times M$ can generate all of the group.

The direct product of two finite groups yields a finite group.

Example 42 Consider the group $[A_8^{\mathbb{P}}; \cdot]$ of positive integers less than 8 and relatively prime to 8 under multiplication in 8-arithmetic. $A_8^{\mathbb{P}} = \{1, 3, 5, 7\}$ is a noncyclic group of order 4. The group $[A_3; +]$ is a cyclic group of order 3. $[A_3 \times A_8^{\mathbb{P}}; *]$ is a noncyclic group of order 12 since 12 different elements exist in $A_3 \times A_8^{\mathbb{P}}$ and since each of the elements $\langle 0, 1 \rangle$, $\langle 0, 3 \rangle$, $\langle 0, 5 \rangle$, and $\langle 0, 7 \rangle$ is of order 1 while each of the other eight elements is of order 3.

Cyclic groups can also be constructed in the form of a direct product.

Example 43 The direct product of the cyclic additive groups $[A_2;+]$ and $[A_3;+]$ in 2-arithmetic and 3-arithmetic, respectively, is a cyclic group of order 6 with generator $\langle 1,1 \rangle$. The group $[T;*]$ of Example 16 may be thought of as the direct product of $[A_2;+]$ with itself. T is noncyclic even though $[A_2;+]$ is cyclic.

Some quotient groups of a direct product of groups are of particular interest.

Theorem 2.47 Let G and H be two groups, $G \times H$ their direct product, and I_G and I_H the identity subgroups of G and H , respectively. Then the quotient group $(G \times H)/(G \times I_H)$ is isomorphic to $I_G \times H$, and the quotient group $(G \times H)/(I_G \times H)$ is isomorphic to $G \times I_H$.

Example 44 Let $G = A_3$ and $H = A_8^P$. Then the direct product $[A_3 \times A_8^P;*]$ of Example 42 may be denoted $[G \times H;*]$ and the identity subgroups are $I_G = \{0\}$ and $I_H = \{1\}$. $I_G \times H = \{\langle 0,1 \rangle, \langle 0,3 \rangle, \langle 0,5 \rangle, \langle 0,7 \rangle\}$ and $G \times I_H = \{\langle 0,1 \rangle, \langle 1,1 \rangle, \langle 2,1 \rangle\}$. Both $I_G \times H$ and $G \times I_H$ are invariant subgroups of $G \times H$ so that the quotient groups of Theorem 2.47 do exist. $(G \times H)/(G \times I_H) = \{G \times I_H, (G \times I_H) * \langle 0,3 \rangle, (G \times I_H) * \langle 0,5 \rangle, (G \times I_H) * \langle 0,7 \rangle\}$. $(G \times H)/(G \times I_H)$ is isomorphic to $I_G \times H$ under the isomorphism α defined from $I_G \times H$ into $(G \times H)/(G \times I_H)$ by $\langle 0,1 \rangle \alpha = G \times I_H$, $\langle 0,3 \rangle \alpha = (G \times I_H) * \langle 0,3 \rangle$, $\langle 0,5 \rangle \alpha = (G \times I_H) * \langle 0,5 \rangle$, and $\langle 0,7 \rangle \alpha = (G \times I_H) * \langle 0,7 \rangle$. If β is a mapping defined from $I_G \times H$ into H by $\langle 0,1 \rangle \beta = 1$, $\langle 0,3 \rangle \beta = 3$, $\langle 0,5 \rangle \beta = 5$, and $\langle 0,7 \rangle \beta = 7$, then β is an isomorphism from $I_G \times H$ into H . Hence, $G \times H$ contains a subgroup isomorphic to H . It can be proved that if K_1 ,

K_2 , and K_3 are groups and K_1 is isomorphic to K_2 and K_2 is isomorphic to K_3 , then K_1 is isomorphic to K_3 . Hence, $(G \times H)/(G \times I_H)$ is isomorphic to H . The isomorphism between $(G \times H)/I_G \times H$ and $G \times I_H$, asserted in Theorem 2.47, can be constructed in a manner similar to the construction of α above. An isomorphism between $(G \times H)/(I_G \times H)$ and G can also be established by arguments similar to those above.

CHAPTER III

RINGS AND IDEALS

Simple Properties of Rings

In this chapter an important algebraic system called a ring having two binary operations will be studied. The study of groups required the system to have only one binary operation. It will be seen that for some of the examples of groups given in Chapter II, an additional binary operation can be defined to qualify these examples as rings.

Definition 3.1 Let R be a nonempty set on which two binary operations (designated as addition and multiplication) have been defined. R is said to be a ring provided the following properties are satisfied

- (i) R is an additive abelian group.
- (ii) R is a multiplicative semigroup.
- (iii) For arbitrary elements $a, b, c \in R$, the following distributive laws hold: $a(b+c) = ab+ac$ and $(b+c)a = ba+ca$.

For simplicity, the usual notation of addition and multiplication of integers will be used in referring to the ring operations as is done in Definition 3.1. If addition and multiplication on the ring R are denoted by $+$ and \cdot , respectively, then the distributive laws would be $a \cdot (b+c) = (a \cdot b) + (a \cdot c)$ and $(b+c) \cdot a = (b \cdot a) + (c \cdot a)$, respectively. The notation $[R; +; \cdot]$ will be used to denote a set R with two binary operations, $+$ and \cdot , called addition and multiplication, respectively. The additive

identity of a ring R is called the zero of R and will be denoted by z .

From condition (i) of Definition 3.1, it is seen that it is impossible to define multiplication on a group $[G; *]$ so that G will be a ring if $*$ is not abelian. Hence, the nonabelian group $[M; \cdot]$ of Example 10 cannot be extended to a ring by defining a multiplication on M and using the original operation on M as addition. The original operation on M would qualify as multiplication on M . If addition on M is defined as ordinary matrix addition modulo 2, then M still is not a ring since, for example $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} + \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \notin M$.

Condition (ii) of Definition 3.1 requires that multiplication be an associative operation on the set R . Not all sets with two operations which satisfy (i) and (ii) of Definition 3.1 are rings.

Example 45 Consider the additive group of integers $[I; +]$ and define multiplication \circ on I by $m \circ n =$ least common multiple of m and n where $m, n \in I$. $[I; \circ]$ is a semigroup and $[I; +]$ is an abelian group but $[I; +; \circ]$ is not a ring since, for example, $2 \circ (3+4) = 2 \circ 7 = 14$ while $(2 \circ 3) + (2 \circ 4) = 6 + 4 = 10$ so that $2 \circ (3+4) \neq (2 \circ 3) + (2 \circ 4)$.

A set may have two operations that satisfy (ii) and (iii) of Definition 3.1 and still not be a ring.

Example 46 Consider the group $[M; \cdot]$ of Example 10. M is the set of all nonsingular 2×2 matrices over the integers modulo 2 with \cdot being ordinary matrix multiplication modulo 2. Consider this operation \cdot as addition on M and define a new multiplication on M by $x \circ y = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = a \in M$ for every $x, y \in M$. Then $[M; \circ]$ is a semigroup because M is associative and closed with respect to \circ .

Furthermore, $x \circ (y \cdot z) = a = a \cdot a = (x \circ y) \cdot (x \circ z)$ and $(y \cdot z) \circ x = a = a \cdot a = (y \circ x) \cdot (z \circ x)$ for arbitrary $x, y, z \in M$ so that both distributive laws hold. Hence, $[M; \cdot; \circ]$ satisfies (ii) and (iii) of the definition of a ring but is not a ring since $[M; \cdot]$ is a nonabelian group.

An example of an infinite set having two operations satisfying (ii) and (iii) of the definition of a ring but which is not a ring is the set I^+ of all positive integers under the usual operations of addition and multiplication of integers. $[I^+; +; \cdot]$ is not a ring since $[I^+; +]$ is not a group.

Other algebraic systems may lack a combination of a few of the properties required of a ring.

Example 47 Consider the additive abelian group $[A_2; +]$ in 2-
arithmetic and define multiplication \circ on A_2 by $a \circ b = 0 \in A_2$ for every $a, b \in A_2$ except the product $0 \circ 1$ in that order which is defined by $0 \circ 1 = 1$. Then $[A_2; +; \circ]$ satisfies the distributive law $a \circ (b + c) = (a \circ b) + (a \circ c)$ for every $a, b, c \in A_2$. $[A_2; \circ]$ is not a semigroup since \circ is not associative, e.g., $1 \circ (1 \circ 1) = 1 \circ (0) = 0$ but $(1 \circ 1) \circ 1 = 0 \circ 1 = 1$ so that $1 \circ (1 \circ 1) \neq (1 \circ 1) \circ 1$. Hence, $[A_2; +; \circ]$ is not a ring. Also, $[A_2; +; \circ]$ does not satisfy the second distributive law, e.g., $(1 + 1) \circ 1 = 0 \circ 1 = 1$ while $(1 \circ 1) + (1 \circ 1) = 0 + 0 = 0$ so that $(1 + 1) \circ 1 \neq (1 \circ 1) + (1 \circ 1)$.

The order of a ring R is the same as the order of the additive group R . Rings of finite as well as infinite order exist.

Example 48 The set of all even integers is a ring, denoted $[E; +; \cdot]$, of infinite order under the operations of ordinary addition

and multiplication of integers. The set of odd integers under the same operations is not a ring since addition is not closed.

Example 49 Consider the group $[A_8^P; \cdot]$ of all positive integers less than 8 and relatively prime to 8 under the operation of multiplication \cdot in 8-arithmetic. Consider \cdot as addition and define a new multiplication \circ on $A_8^P = \{1, 3, 5, 7\}$ by $a \circ b = 1$ for every $a, b \in A_8^P$. $[A_8^P; \cdot; \circ]$ is a finite ring of order 4.

A ring R is called a ring with unity or a ring with identity if there is a multiplicative identity, called the unity and denoted by u , in the ring, i.e., if there exists an element $u \in R$ such that $au = ua = a$ for every $a \in R$. Neither the ring $[E; +; \cdot]$ of Example 48 nor the ring $[A_8^P; \cdot; \circ]$ of Example 49 has a unity.

Example 50 Consider the set N of all 2×2 matrices over 2-arithmetic. Let $+$ and \cdot be, respectively, ordinary addition and multiplication of matrices in 2-arithmetic. Then $[N; +; \cdot]$ is a ring with unity $u = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$.

A ring R is called a commutative ring if multiplication in R is commutative, i.e., $ab = ba$ for every $a, b \in R$. $[E; +; \cdot]$ and $[A_8^P; \cdot; \circ]$ of Examples 48 and 49, respectively, are both commutative rings having no unity. $[N; +; \cdot]$ of Example 50 is a noncommutative ring with unity. Many commutative rings with unity exist. The set of integers I under ordinary addition and multiplication of integers is an infinite commutative ring with unity $u = 1$. An interesting finite commutative ring with unity is given next.

Example 51 Let $S = \{0,1,2,3,4,5,6,7,8,9\}$ and define $*$ and \circ , addition and multiplication, respectively, on S by $a*b = a+b-1$ and $a\circ b = a+b-ab$ where the indicated operations on the right side of each of the equations are performed in 10-arithmetic. Then $[S;*; \circ]$ is a commutative ring of order 10 with unity. The unity of S is $u = 0$ and the zero of S is $z = 1$.

Theorem 3.2 If a ring has a unity, it is unique.

The unity $u = 0$ of the ring $[S;*; \circ]$ of Example 51 is unique as is the unity $u = 1$ of the ring of integers $[I;+; \cdot]$. ($[I;+; \cdot]$ will always denote the ring of integers with the usual operations of addition and multiplication of integers.) An abelian group having an additional operation, multiplication, and having a unique unity need not be a ring.

Example 52 Consider the additive abelian group $[A_2;+]$ with multiplication \circ defined by the following Cayley square.

$$\begin{array}{c|cc} \circ & 0 & 1 \\ \hline 0 & 0 & 1 \\ 1 & 1 & 0 \end{array}$$

Then 0 is a unique unity for A_2 but $[A_2;+; \circ]$ is not a ring since the distributive laws are not satisfied, e.g., $1\circ(1+0) = 1\circ 1 = 0$ while $(1\circ 1)+(1\circ 0) = 0+1 = 1$ so that $1\circ(1+0) \neq (1\circ 1)+(1\circ 0)$.

A ring may have several elements which satisfy one of the equality conditions in the definition of a unity.

Example 53 Let T be the set of all 2×2 matrices of the form

$\begin{pmatrix} n & m \\ 0 & 0 \end{pmatrix}$ where $n, m \in I$, the set of integers. Define the operations on T to be ordinary matrix addition and multiplication. Then $[T; +; \cdot]$ is a ring and elements of the form $\begin{pmatrix} 1 & k \\ 0 & 0 \end{pmatrix}$ for every $k \in I$ satisfy the equation $\begin{pmatrix} 1 & k \\ 0 & 0 \end{pmatrix} \cdot \begin{pmatrix} n & m \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} n & m \\ 0 & 0 \end{pmatrix}$, i.e., $\begin{pmatrix} 1 & k \\ 0 & 0 \end{pmatrix}$ is a left unity for every $k \in I$. However, T has no unity.

If R is a ring with unity u , then an element $a \in R$ is said to have a multiplicative inverse in R if there exists an element $b \in R$ such that $ab = ba = u$. Then the element b is called the multiplicative inverse of a and b is denoted a^{-1} . The ring $[T; +; \cdot]$ of Example 53 had no unity so that no element of T has a multiplicative inverse.

Theorem 3.3 An element of a ring R with unity has at most one multiplicative inverse.

In the ring $[S; *; 0]$ of Example 51, the unique multiplicative inverses of 0, 2, 4, and 8 are, respectively, 0, 2, 8, and 4 while the other elements in S have no multiplicative inverses. In some rings every element except the zero has a multiplicative inverse.

Example 54 Consider the ring $[A_5; +; \cdot]$ with the usual operations in 5-arithmetic. Then the zero and unity of the ring $[A_5; +; \cdot]$ are $z = 0$ and $u = 1$, respectively. The multiplicative inverses of 1, 2, 3, and 4 are, respectively, 1, 3, 2, and 4.

No multiplicative inverse exists for the zero of ring R , even if the other elements of R do have multiplicative inverses. This fact is established by the next theorem.

Theorem 3.4 For each element a of a ring R with zero z ,
 $az = za = z$.

Any of the rings given in Examples 48 through 51 or 53 or 54 can be used to illustrate the validity of this theorem.

Since the product of zero with any other element of a ring always yields zero, no element multiplied by zero equals the unity so that no multiplicative inverse exists for zero. Using this special property of multiplication by zero, one may construct a ring given any abelian group $[G; +]$. Simply define multiplication \circ on G by $a \circ b = z$ for any $a, b \in G$ where z is the identity of the group G and let $+$ be considered as addition in the newly formed ring. The ring $[A_8^{\mathbb{P}}; \cdot; \circ]$ of Example 49 was constructed in this manner.

Not every abelian group having a second operation which satisfies Theorem 3.4 is a ring.

Example 55 Consider the additive abelian group $[A_4; +]$ and define multiplication \circ on A_4 by $a \circ a = 1$ for every $a \neq 0$, $a \in A_4$ and define all other products of two elements in A_4 to be 0. Then $[A_4; +; \circ]$ satisfies Theorem 3.4 but is not a ring since the distributive laws are not satisfied, e.g., $2 \circ (1+1) = 2 \circ 2 = 1$ while $(2 \circ 1) + (2 \circ 1) = 0 + 0 = 0$ so that $2 \circ (1+1) \neq (2 \circ 1) + (2 \circ 1)$.

An important relationship between multiplication and additive inverses is given next.

Theorem 3.5 If R is a ring, then $(-a)b = a(-b) = -ab$ and $(-a)(-b) = ab$ for every $a, b \in R$.

This theorem acknowledges that all rings have properties similar to

the "rules of signs" for multiplication of integers. The ring of even integers $[E;+;\cdot]$ of Example 48 is an infinite ring satisfying Theorem 3.5. Notice that the theorem is true for all rings, hence, for finite rings as well.

Example 56 Consider the ring $[A_6;+;\cdot]$ of integers

$A_6 = \{0,1,2,3,4,5\}$ with the usual operations in 6-arithmetic. A_6 is a ring of order 6. Additive inverses of 0, 1, 2, 3, 4, and 5 are 0, 5, 4, 3, 2, and 1, respectively. The equalities $(-2) \cdot 5 = 4 \cdot 5 = 2 = -4 = -(2 \cdot 5)$ and $(-4) \cdot (-3) = 2 \cdot 3 = 0 = 4 \cdot 3$ demonstrate Theorem 3.5. Of course, all such products of elements of A_6 satisfy the theorem.

Some sets having two operations satisfying the equalities in Theorem 3.5 are not rings.

Example 57 Consider the groupoid $[I_0^+;*\cdot]$ given in Example 9. If multiplication \circ is defined on I_0^+ as ordinary multiplication of integers, then all equalities of the form given in Theorem 3.5 hold for $[I_0^+;*\cdot;\circ]$. This is easily seen since every element in $[I_0^+;*\cdot]$ is its own additive inverse. $[I_0^+;*\cdot;\circ]$ is not a ring since $[I_0^+;*\cdot]$ is not a group.

The next two definitions establish some notation for future use in dealing with rings.

Definition 3.6 For an element a of a ring R and the integer n the scalar product $an = na$ is defined to be:

- (i) $a+a+\dots+a$, n summands of a if $n > 0$,
- (ii) z if $n = 0$ and where z denotes the zero of R ,

(iii) $(-a)+(-a)+\cdots+(-a)$, $|n|$ summands of $(-a)$ if $n < 0$.

Definition 3.7 For an element a of the ring R ,

- (i) $a^1 = a$,
- (ii) $a^{k+1} = a^k a$, for k any positive integer, and
- (iii) if a has a multiplicative inverse, $a^0 = u$ the unity of R and $a^{-k} = (a^{-1})^k$ for k any positive integer.

The notation introduced in the last two definitions is equivalent to that used in high school and college algebra for scalar products and powers of a variable x . In rings whose elements are not represented by integers, no confusion should occur. Confusion may occur in examples involving a ring whose elements are represented by integers.

Example 58 Consider the ring $[A_4; +; \cdot]$ with the usual operations in 4-arithmetic. Then $8 \cdot 2$ and $3 \cdot 4$ are clearly scalar products involving the scalars 8 and 4, respectively, since 8 and 4 are not in the set A_4 . On the other hand, $2 \cdot 3$ might mean a scalar product or a product of two elements in A_4 , but either interpretation yields the same result so that the misunderstanding is not critical. The exponent in the expression 2^8 and similar expressions must be considered as a scalar and the whole expression interrupted as given in Definition 3.7. Thus, $8 \notin A_4$ but $2^8 = 0$ in A_4 . Notice that 8 is congruent to 0 modulo 4 but 2^0 has not been defined since 2 has no inverse.

Several simple results of Definitions 3.6 and 3.7 are given in the next theorem.

Theorem 3.8 Let R be a ring, m and n be any integers, and h and

k be positive integers. Then, for any $a, b \in R$:

- (i) $n \cdot z = z$, the zero of R and $u^k = u$, the unity of R . The latter is valid only if R is a ring with unity.
- (ii) $n(a+b) = na+nb$ and $(ab)^k = a^k b^k$. The latter holds if and only if R is a commutative ring.
- (iii) $(m+n)a = ma+na$ and $a^{h+k} = a^h a^k$.
- (iv) $mn(a) = m(na)$ and $(a^h)^k = a^{hk}$.

Any of the rings given previously can be used to demonstrate the validity of the first equalities in (i) and (ii) and both of the equalities in (iii) and (iv) of Theorem 3.8. The second equality of (i) may be demonstrated by using the ring $[N;+;\cdot]$ of Example 50, $[S;*;o]$ of Example 51, $[A_5;+;\cdot]$ of Example 54, $[A_6;+;\cdot]$ of Example 56, or the ring of integers $[I;+;\cdot]$. The elements of the rings $[E;+;\cdot]$, $[A_8^D;*;o]$, $[S;*;o]$, $[A_5;+;\cdot]$, and $[A_6;+;\cdot]$ of Examples 48, 49, 51, 54, and 56, respectively, all satisfy the second equality of (ii) of Theorem 3.8 since each of these rings is commutative. Either the ring $[N;+;\cdot]$ of Example 50 or the ring $[T;+;\cdot]$ of Example 53 may be used to show that not all products of elements in a noncommutative ring satisfy the second equality in (ii) of Theorem 3.8. For example, with $k = 2$ in $[N;+;\cdot]$,

$$\left[\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \right]^2 = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}^2 = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \text{ while } \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}^2 \cdot \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}^2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

so that $\left[\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \right]^2 \neq \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}^2 \cdot \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}^2$.

A set with two binary operations satisfying one or even several of the equalities of Theorem 3.8 need not be a ring.

Example 59 The system $[I_0^+;+;\cdot]$ of nonnegative integers under the usual addition and multiplication of integers satisfies all the

equalities of Theorem 3.8 if the scalars are restricted to the set of positive integers. The second equality in each part of the theorem are always true. $[I_0^+; +; \cdot]$ is not a ring since $[I_0^+; +]$ is not a group, e.g., (-2) is not in I_0^+ .

Example 60 The system $[I_0^+; *; 0]$ of Example 57 satisfies all of the equalities of Theorem 3.8 except the first one in (iv). The equalities involving exponents are easy to verify since multiplication in the system is the usual multiplication of integers. The scalar product properties are harder to verify. For example, $n(a*b) = n|a-b| = |a-b|$ if n is odd and $n(a*b) = 0$ if n is even while $na*nb = a*b = |a-b|$ if n is odd and $na*nb = 0*0 = |0-0| = 0$ if n is even so that the equality, $n(a+b) = na+nb$, of (ii) is true for this system. Similar arguments can be used to verify the other parts of the theorem claimed to be true for this system. If m is even, n odd and $a \neq 0$, then $mn(a) = a$ while $m(na) = m(a) = 0$ so that $mn(a) \neq m(na)$. $[I_0^+; *; 0]$ is not a ring since $*$ is not associative.

Subrings

A nonempty subset S of a ring R is a subring of R if S itself is a ring with respect to the binary operations of R . Thus, the ring $[E; +; \cdot]$ of Example 48 is a subring of the ring of integers $[I; +; \cdot]$. Other subrings can be formed by taking all the multiples of any fixed integer under the operations of $[I; +; \cdot]$. $[I; +; \cdot]$ is, of course, a subring of itself.

It may be true that a ring S is not a subring of the ring R even though S is a subset of R . For example, the ring $[A_8^p; \cdot; 0]$ of Example 49 is a subset of the ring $[A_8; +; \cdot]$ with the usual operations in 8-arithmetic,

but A_8^p is not a subring of A_8 since the operations of A_8^p are not the operations of A_8 . If $T = \{0, 2, 4, 6\}$, then $[T; +; \cdot]$ with the operations of $[A_8; +; \cdot]$ is a subring of $[A_8; +; \cdot]$.

A useful characterization of a proper subring is given next.

Theorem 3.9 Let R be a ring and S be a proper subset of the set R . Then S is a subring of R if and only if

- (i) S is closed with respect to the ring operations, and
- (ii) for each $a \in S$, $-a \in S$.

The set S of all multiples of 6, say, under the operations of $[I; +; \cdot]$, is a subring of I . This is easy to verify using Theorem 3.9 since addition or multiplication of multiples of 6 always gives a multiple of 6 and, secondly, if $a = 6k$ is in the set S , then $-a = 6(-k)$ is also in S since $6(-k)$ is a multiple of 6.

The set $T = \{0, 1, 3, 5, 7, 9\}$ is a subset of the ring $[A_{10}; +; \cdot]$ with the usual operations in 10-arithmetic. The additive inverse of each element of T is in the set T but T is not a subring of A_{10} since T is not closed with respect to addition. T is closed with respect to multiplication. Examples satisfying some but not all of the other conditions of Theorem 3.9 may be constructed similarly.

Homomorphisms and Isomorphisms

The existence of certain types of mappings between groups yielded a wealth of information in Chapter II. Certain mappings between rings, similarly, provide much information.

Definition 3.10 Let $[R; +; \cdot]$ and $[S; *; \circ]$ be two rings. A mapping α from R into S is said to be a (ring) homomorphism if $(a+b)\alpha = a\alpha * b\alpha$ and

$(a \cdot b)\alpha = a\alpha \circ b\alpha$ for all $a, b \in R$. If the homomorphism α is a mapping from R onto S , then α is called a homomorphism of R onto S and S is called a homomorphic image of R and R is called the preimage of S under the mapping α .

The two equality conditions of Definition 3.10 require that a homomorphism preserve both of the operations of the ring R . Hence, a ring homomorphism is a group homomorphism between the underlying additive groups which also preserves multiplication.

Example 61 Consider the rings $[A_8^P; \cdot; \circ]$ and $[N; +; \cdot]$ of Examples 49 and 50, respectively. Define the mapping α from A_8^P into N by $1\alpha = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$, $3\alpha = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$, $5\alpha = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$, and $7\alpha = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$. α preserves the addition \cdot of A_8^P , e.g., $(3 \cdot 5)\alpha = 7\alpha = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$ while $3\alpha + 5\alpha = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} + \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 0 & 1 \end{pmatrix}$ so that $(3 \cdot 5)\alpha \neq 3\alpha + 5\alpha$. α does not preserve the multiplication \circ of A_8^P , e.g., $(3 \circ 7)\alpha = 1\alpha = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$ while $3\alpha \cdot 7\alpha = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$ so that $(3 \circ 7)\alpha \neq 3\alpha \cdot 7\alpha$. Hence, α is a group homomorphism between the underlying groups which is not a ring homomorphism.

Example 62 Consider the ring $[W; +; \cdot]$ of 2×2 matrices over 4-arithmic and the ring $[A_4; +; \cdot]$ with the usual operations in 4-arithmic. If α is defined from A_4 into W by $0\alpha = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$, $1\alpha = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$, $2\alpha = \begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix}$, and $3\alpha = \begin{pmatrix} 3 & 0 \\ 0 & 3 \end{pmatrix}$, then α is a homomorphism from the ring $[A_4; +; \cdot]$ into the ring $[W; +; \cdot]$ since both operations are

preserved by α . The set $M = \left\{ \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix}, \begin{pmatrix} 3 & 0 \\ 0 & 3 \end{pmatrix} \right\}$ is the homomorphic image of A_4 and A_4 is the preimage of M under α . Notice that both $[A_4; +; \cdot]$ and $[M; +; \cdot]$ are commutative rings.

Ring homomorphisms may be used to construct subrings of a known ring.

Theorem 3.11 Let α be a homomorphism of ring R into ring S . If S' is the homomorphic image of R in S , then S' is a subring of S .

By Theorem 3.11, $[M; +; \cdot]$ of Example 62 is known to be a subring of $[W; +; \cdot]$. Another subring of W can be constructed by defining a different map which satisfies the definition of a ring homomorphism.

Example 63 Consider the ring $[W; +; \cdot]$ of Example 62 and the ring

$[A_4; +; \cdot]$ with the usual operations in 4-arithmetic. Notice that

$\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$ is a unity for all elements of W of the form $\begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix}$ where

$a \in A_4$. Define β from A_4 into W so that the zeros correspond, i.e.,

$0\beta = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$. Since 1 is the unity of A_4 and is also a generator of

the additive group of A_4 , define $1\beta = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$. Now, since 2 is its

own additive inverse and has no multiplicative inverse, define the

image of 2 to be a similar acting element of the form $\begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix}$ in W ,

i.e., $2\beta = \begin{pmatrix} 2 & 0 \\ 0 & 0 \end{pmatrix}$. $1+2 = 3$ in A_4 so one must define $3\beta = \begin{pmatrix} 3 & 0 \\ 0 & 0 \end{pmatrix} =$

$\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} + \begin{pmatrix} 2 & 0 \\ 0 & 0 \end{pmatrix} = 1\beta + 2\beta$. β thus defined preserves both operations of

A_4 and is a ring homomorphism. Hence, by Theorem 3.11, the set

$P = \left\{ \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 2 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 3 & 0 \\ 0 & 0 \end{pmatrix} \right\}$ with the operations of $[W; +; \cdot]$ is a

subring of W . Notice that $[P;+;\cdot]$ has a unity but it is not the unity of W .

The image of a map from a ring R into a ring S might be a subring of S without the map being a homomorphism.

Example 64 Consider the rings $[A_2;+;\cdot]$ and $[A_{10};+;\cdot]$ with the usual operations in 2 and 10-arithmetic, respectively. If γ is defined from A_2 into A_{10} by $0\gamma = 5$ and $1\gamma = 0$, then the image of γ in A_{10} is the set $S = \{0,5\}$ which under the operations of $[A_{10};+;\cdot]$ is a subring of A_{10} . γ is not a homomorphism, however, since $(1+1)\gamma = 0\gamma = 5$ while $1\gamma+1\gamma = 0+0 = 0$ so that γ does not preserve addition.

Both of the subrings $[M;+;\cdot]$ and $[P;+;\cdot]$ of $[W;+;\cdot]$ given in Examples 62 and 63, respectively, are one-to-one with $[A_4;+;\cdot]$ under the homomorphisms of the respective examples. Homomorphisms of this special type are defined next.

Definition 3.12 If α is a homomorphism of ring R onto ring S such that α is a one-to-one mapping, then α is called an isomorphism. Rings R and S are said to be isomorphic if there exists an isomorphism of R onto S .

The homomorphism β in Example 63 is not an isomorphism from A_4 into W but it is an isomorphism from A_4 into the ring $[P;+;\cdot]$. The homomorphism of Example 62 is of a similar type. Some homomorphisms cannot be thought of as isomorphisms.

Example 65 Consider the rings $[A_{12};+;\cdot]$ and $[A_3;+;\cdot]$ with the

usual operations in 12 and 3-arithmetic, respectively. Then ϕ defined by $0\phi = 3\phi = 6\phi = 9\phi = 0$, $1\phi = 4\phi = 7\phi = 10\phi = 1$, and $2\phi = 5\phi = 8\phi = 11\phi = 2$ is a homomorphism of A_{12} onto A_3 . ϕ is not a one-to-one map from A_{12} into any subset of A_3 . Hence, ϕ cannot be thought of as an isomorphism between A_{12} and a subring of A_3 .

Isomorphisms exist for rings of infinite as well as finite order.

Example 66 Consider the ring of integers $[I;+;\cdot]$ and the ring $[S;+;\cdot]$ of all 2×2 matrices over the integers with the usual operations of addition and multiplication of matrices. The set $S' = \left\{ \begin{pmatrix} n & 2n \\ 0 & 0 \end{pmatrix} : n \in I \right\}$ under the operations of $[S;+;\cdot]$ is a subring of S . The mapping α defined by $n\alpha = \begin{pmatrix} n & 2n \\ 0 & 0 \end{pmatrix}$ for every $n \in I$ is an isomorphism from I into S' . Other isomorphisms between I and subrings of S can be established similarly.

Earlier it was noted that some rings have a unity while others do not have a unity. However, the next theorem asserts that every ring can be considered as isomorphically equivalent to a subring of a ring with unity.

Theorem 3.13 For any ring R , there exists a ring S with a unity such that a subring S' of S is isomorphic to R . (R is said to be imbedded in S .)

The ring of even integers $[E;+;\cdot]$ under ordinary addition and multiplication of integers is naturally imbedded in the ring of integers $[I;+;\cdot]$. The imbedding isomorphism is the identity map α defined from E into I by $a\alpha = a$ for each $a \in E$. Similarly, all rings with unity,

such as $[S; *; 0]$ of Example 51, are imbedded in themselves by the identity map.

If a ring R has no unity, it is not, in general, easy to find a ring S with unity in which R can be imbedded. Some proofs of Theorem 3.13 are of the constructive nature, i.e., some proofs consist of constructing the needed ring with unity. The construction technique is demonstrated in the next example.

Example 67 The ring $[A_8^P; \cdot; 0]$ of Example 49 has no unity. Let $[I; +]$ and $[A_8^P; \cdot]$ denote the additive abelian groups of the ring of integers $[I; +; \cdot]$ and the ring $[A_8^P; \cdot; 0]$, respectively. Then the direct product $A_8^P \times I = \{ \langle a, n \rangle : a \in A_8^P, n \in I \}$ under addition $*$ defined by $\langle a, n \rangle * \langle b, m \rangle = \langle a \cdot b, n+m \rangle$ for every $a, b \in A_8^P$ and $n, m \in I$ is an additive group by Theorem 2.46. Since addition in $A_8^P \times I$ is defined by elementwise additions in A_8^P and I and each of these additions is abelian, $A_8^P \times I$ is an abelian group. Now define multiplication θ on $A_8^P \times I$ by $\langle a, n \rangle \theta \langle b, m \rangle = \langle (a \circ b) \cdot ma \cdot nb, n \cdot m \rangle$ for every $a, b \in A_8^P$ and every $n, m \in I$. The operations indicated in the left component of the product are the operations in the ring $[A_8^P; \cdot; 0]$ with scalar products denoted by adjunction while the operation in the right component of the product is ordinary multiplication of integers. This multiplication on $A_8^P \times I$ is closed since $[A_8^P; \cdot; 0]$ and $[I; +; \cdot]$ are rings. Verifications that multiplication is associative and that the distributive laws hold are left to the reader. The element $\langle 1, 1 \rangle$ is a unity for $A_8^P \times I$ since $\langle 1, 1 \rangle \theta \langle a, n \rangle = \langle (1 \circ a) \cdot 1 \cdot a, 1 \cdot n \rangle = \langle 1 \cdot 1 \cdot a, 1 \cdot n \rangle = \langle a, n \rangle$ and, similarly, $\langle a, n \rangle \theta \langle 1, 1 \rangle = \langle a, n \rangle$. Hence, $[A_8^P \times I; *; \theta]$ is a ring with unity. $T = \{ \langle a, 0 \rangle : a \in A_8^P, 0 \in I \}$ can be shown to be a subring of $A_8^P \times I$. If the mapping α is defined from A_8^P into T by

$a\alpha = \langle a, 0 \rangle$ for every $a \in A_8^P$, then α is an isomorphism. Hence, $[A_8^P; \cdot; 0]$ has been imbedded in the ring $[A_8^P \times I; *; \theta]$ with unity.

Much work is involved to determine if a given mapping is a ring isomorphism. Some identifying properties of isomorphisms are given next.

Theorem 3.14 In any isomorphism α of a ring R onto a ring R' :

- (i) if z and z' are the zeros of R and R' , respectively, then $z\alpha = z'$.
- (ii) if $a\alpha = a'$, then $(-a)\alpha = -a'$.
- (iii) if u and u' are the unities of R and R' , respectively, then $u\alpha = u'$.
- (iv) if R is a commutative ring, then so is R' .

All of the ring isomorphisms given previously necessarily satisfy all four of the conclusions of Theorem 3.14. The isomorphism α of Example 67 satisfies (iii) of the theorem vacuously since neither the ring $[A_8^P; \cdot; 0]$ nor the ring $[T; *; \theta]$ has a unity.

Some one-to-one maps from a ring R onto a ring R' satisfy most or all of the conclusions of Theorem 3.14 but are not isomorphisms.

Example 68 The subset $H = \{0, 2, 4, 6, 8\}$ of the ring $[A_{10}; +; \cdot]$ with the usual operations in 10-arithmetic is a subring of A_{10} . Consider the map α from the ring $[A_5; +; \cdot]$ with the usual operations in 5-arithmetic onto the ring $[H; +; \cdot]$ defined by $0\alpha = 0$, $1\alpha = 2$, $2\alpha = 4$, $3\alpha = 6$, and $4\alpha = 8$. α satisfies (i), (ii), and (iv) of Theorem 3.14 but is not an isomorphism since α does not satisfy (iii), 2 is not a unity for H . In fact, H has no unity so that A_5 and H are not isomorphic.

Example 69 Consider the ring $[A_5; +; \cdot]$ with the usual operations in 5-arithmetic and the map α defined from A_5 into itself by $0\alpha = 0$,

$1\alpha = 1$, $2\alpha = 3$, $3\alpha = 2$, and $4\alpha = 4$. Then α is a one-to-one onto map and satisfies all four conclusions of Theorem 3.14 but α is not an isomorphism, e.g., $(3+3)\alpha = 1\alpha = 1$ while $3\alpha+3\alpha = 2+2 = 4$ so that addition is not preserved by α .

Ideals

In Chapter II the study of group homomorphisms and isomorphisms was closely related to a special class of subgroups known as invariant subgroups. The study of ring homomorphisms and isomorphisms is, similarly, closely related with a special class of subrings now to be defined.

Definition 3.15. A nonempty subset N of a ring R is called a left (right) ideal in R if N is a subgroup of the additive group of R and $rn \in N$ ($nr \in N$) for every $r \in R$ and every $n \in N$. A nonempty subset M of a ring R is called an ideal (two-sided ideal) in R if M is both a left and a right ideal in R .

Any left, right, or two-sided ideal N in a ring R is a subring of R by Theorem 3.9 since N is closed with respect to both operations and additive inverses for every element of N are in N since N is a subgroup of the additive group of R . If N is a left ideal in a commutative ring R , then N is a two-sided ideal since the condition $rn \in N$ for every $r \in R$ and every $n \in N$ implies $nr = rn \in N$. Similar statements are true for right ideals so that only noncommutative rings have right or left ideals which are not two-sided ideals.

Example 70 The subring $H = \{0, 2, 4, 6, 8\}$ of the ring $[A_{10}; +; \cdot]$ with the usual operations in 10-arithmetic is an ideal, two-sided ideal, in the commutative ring A_{10} .

Example 71 Let $[R;+;\cdot]$ be the ring of 2×2 matrices over 3-arithmetic under matrix addition and multiplication in 3-arithmetic. Let

$$B = \left\{ \begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix} : a, b \in A_3 \right\}, \quad C = \left\{ \begin{pmatrix} a & 0 \\ b & 0 \end{pmatrix} : a, b \in A_3 \right\}, \quad \text{and } D =$$

$$\left\{ \begin{pmatrix} a & 0 \\ b & c \end{pmatrix} : a, b, c \in A_3 \right\}. \quad \text{Theorem 3.9 can be used to verify that } B, C,$$

and D are subrings of $[R;+;\cdot]$. B is a right ideal in R since

$$\begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix} \cdot \begin{pmatrix} c & d \\ e & f \end{pmatrix} = \begin{pmatrix} (ac+be) & (ad+bf) \\ 0 & 0 \end{pmatrix} \in B \text{ for every } a, b, c, d, e, f \in A_3. \quad B$$

is not a left ideal in R , e.g., $\begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} \cdot \begin{pmatrix} 2 & 2 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 2 & 2 \\ 2 & 2 \end{pmatrix} \notin B$. Similarly,

C can be shown to be a left ideal but not a right ideal in R and D

can be shown to be a subring of R but neither a left nor a right ideal in R .

Let R be a ring with zero z and N an ideal in R . Then N is a proper ideal in R if $N \neq \{z\}$, and $N \neq R$. The ideal H in Example 70 is a proper ideal in the ring $[A_{10};+;\cdot]$.

A special type of ideal may be constructed using the next theorem.

Theorem 3.16 If a is an arbitrary element of a commutative ring R with unity, then $A = \{ar : r \in R\}$ is an ideal in R . Furthermore, if M is an ideal in R and $a \in M$, then $A \subset M$.

Theorem 3.16 applies to both finite and infinite rings and implies that A is the smallest ideal containing a .

Example 72 The ring of integers $[I;+;\cdot]$ is a commutative ring with unity of infinite order. $A = \{2n : n \in I\}$, $B = \{3n : n \in I\}$, $C = \{4n : n \in I\}$, $D = \{5n : n \in I\}$, and $E = \{6n : n \in I\}$ are all ideals in I . Since $6 \in A$ and $6 \in B$, $E \subset A$ and $E \subset B$. Similarly, $C \subset A$

since $4 \in A$. No other nontrivial subset relations can be established between these five ideals. Notice that $10 \in A \cap D$ but that $A \not\subset D$ since $2 \notin D$ and $D \not\subset A$ since $5 \notin A$.

Example 73 The ring $[A_{12}; +; \cdot]$ with the usual operations in 12-arithmetic is a commutative ring with unity of finite order 12. $A = \{2n : n \in A_{12}\}$, $B = \{3n : n \in A_{12}\}$, $C = \{4n : n \in A_{12}\}$, $D = \{5n : n \in A_{12}\}$, and $E = \{6n : n \in A_{12}\}$ are all ideals in A_{12} . In fact, $A = \{0, 2, 4, 6, 8, 10\}$, $B = \{0, 3, 6, 9\}$, $C = \{0, 4, 8\}$, $D = A_{12}$, and $E = \{0, 6\}$. Notice that $E \subset B \subset D$, $E \subset A \subset D$, and $C \subset A \subset D$, as would be expected if Theorem 3.16 were used.

If the ring R of Theorem 3.16 has no unity, then the ideal A need not contain a .

Example 74 Consider the ring $[A_8^P; \cdot; 0]$ of Example 49. $\{1 \cdot r : r \in A_8^P\} = \{3 \cdot r : r \in A_8^P\} = \{5 \cdot r : r \in A_8^P\} = \{7 \cdot r : r \in A_8^P\} = \{1\} = A$. There is only one ideal of the type given in Theorem 3.16. A_8^P is a commutative ring but it has no unity. Notice that 3, 5, and 7 are not contained in A . $B = \{1, 3\}$, $C = \{1, 5\}$, and $D = \{1, 7\}$ are the only proper subrings of A_8^P and each of these is an ideal since each is closed with respect to multiplication \circ but elements of A_8^P . The other ideal in this ring is A_8^P itself. Theorem 3.16 is easily verified for all possible cases for this example.

The ring R in Theorem 3.16 must be commutative to be assured that A is a two-sided ideal. In the ring $[R; +; \cdot]$ of Example 71, each element of the right ideal B is equal to at least one product of the form

$\begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix} \cdot \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ where $a, b, c, d \in A_3$. Hence, B is of the form given in Theorem

3.16 but B is not a left ideal and, hence, not an ideal.

The operation of set intersection is closed with respect to ideals of a given ring.

Theorem 3.17. The intersection of any collection of ideals in a ring is an ideal in the ring.

All the ideals of the ring $[A_8^p; +; \cdot]$ are given in Example 74. It is clear that the intersection of any collection of these ideals in A_8^p is an ideal. If the intersection of a collection of sets is an ideal, this does not imply that each set is an ideal, even if some of the sets intersected are known to be ideals.

Example 75 Consider the ring $[A_{12}; +; \cdot]$ with the usual operations in 12-arithmetic. If $B = \{0, 2, 6, 10\}$ and $C = \{0, 4, 6, 8\}$, then $B \cap C = \{0, 6\} = D$ and D is an ideal in A_{12} but neither B nor C is an ideal since neither is closed under addition. The subset $E = \{0, 4, 8\}$ is an ideal in A_{12} and $E \cap C = E$ so that $E \cap C$ is an ideal even though C is not an ideal. Other ideals in A_{12} are $F = \{0\}$ and A_{12} , the trivial ideals, as well as $G = \{0, 2, 4, 6, 8, 10\}$ and $H = \{0, 3, 6, 9\}$. Intersections of any of the ideals in A_{12} always yields one of these ideals.

The intersection of all ideals (right ideals) in a ring R which contain a given nonempty set K of elements of R is called the ideal (right ideal) generated by K . If K is a singleton set $\{a\}$, then the ideal in R generated by the element a of R is called the principal ideal generated by a and is denoted by (a) .

If the ring R has no unity, then the principal ideal generated by an

element $a \in R$ might not contain a as seen in Example 74, e.g., $(3) = \{1\} = A$ but $3 \notin A$. If the ring has a unity, then the principal ideal generated by an element $a \in R$ must contain a .

Example 76 In Example 75, the ideal generated by the set $\{0,8\}$ is $A_{12} \cap G \cap E = E$, the ideal generated by the set $\{0,3\}$ is $A_{12} \cap H = H$, and the ideal generated by the set $\{3,4,8\}$ is A_{12} since no other ideal in A_{12} contains this set. All the ideals in A_{12} are seen to be principal ideals since $F = (0)$, $D = (6)$, $E = (4) = (8)$, $H = (3) = (9)$, $G = (2) = (10)$, and $A_{12} = (1) = (5) = (7) = (11)$ and each of these principal ideals contains each of its generators.

In Example 71, the right ideal B in the ring $[R;+;\cdot]$ is the principal right ideal generated by the matrix $\begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix}$. Other matrices in B also generate B . The right ideal generated by the set of matrices

$\left\{ \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 2 & 0 \\ 0 & 0 \end{pmatrix} \right\}$ is also B .

If every ideal in a commutative ring R is a principal ideal, then R is called a principal ideal ring. In Example 76 it was noted that all the ideals in A_{12} are principal ideals so that $[A_{12};+;\cdot]$ is a finite principal ideal ring.

Theorem 3.18 The ring $[I;+;\cdot]$ of integers is a principal ideal ring.

The ring of integers has only one finite ideal, $(0) = \{0\}$. Every other ideal has two generators, i.e., if the ideal $N = (n)$, then $-n$ is also a generator of N . It is interesting to notice that the intersection

of any collection of ideals in $[I;+;\cdot]$ is a principal ideal generated by the least common multiple of the positive generators of the ideals in the collection, e.g., $(2) \cap (3) \cap (4) \cap (6) = (12)$.

Prime Ideals and Maximal Ideals

If N is an ideal in a commutative ring R such that $ab \in N$ only if $a \in N$ or $b \in N$, then N is called a prime ideal in R . The ideal $B = \{1,3\}$ in the commutative ring $[A_8^P;+;\cdot]$ given in Example 74 is not a prime ideal since any product of two elements of A_8^P equals $1 \in B$, e.g., $5 \cdot 7 = 1 \in B$ but $5 \notin B$ and $7 \notin B$. Similarly, every ideal in A_8^P can be shown to not be a prime ideal except A_8^P itself. Rings may have some proper ideals which are prime and some which are not prime.

Example 77 The ring $[A_{20};+;\cdot]$ with the usual operations in 20-arithmetical is a principal ideal ring with ideals $J = \{0\}$, $K = \{0,10\}$, $L = \{0,5,10,15\}$, $M = \{0,4,8,12,16\}$, $N = \{0,2,4,6,8,10,12,14,16,18\}$, and A_{20} itself with generators 0, 10, 5, 4, 2, and 1, respectively. N and L are proper prime ideals. K and M are proper ideals but are not prime since $2 \cdot 5 = 10 \in K$ and $2 \cdot 6 = 12 \in M$ while the factors are not elements of the respective ideals.

A ring having no proper ideals is called a simple ring. Thus, $[A_{11};+;\cdot]$ with the usual operations in 11-arithmetical is a simple ring since no subgroup of the additive group $[A_{11};+]$ exists by Theorem 2.23. In Example 77, $[A_{20};+;\cdot]$ was found to have several proper ideals so that A_{20} is not simple.

An ideal N in a ring R is called a maximal ideal if $N \neq R$ and if $N \subset M \subset R$ implies $N = M$ or $M = R$ for any ideal M in R . The ideals N and

L of $[A_{20}; +; \cdot]$ given in Example 77 are maximal ideals. Since $K \subset L$ and $M \subset N$, K and M are not maximal ideals in A_{20} . Recall that N and L are also prime ideals. This observation is formalized in the next theorem.

Theorem 3.19 Any maximal ideal in a commutative ring with unity is a prime ideal.

The ideals G and H in the ring $[A_{12}; +; \cdot]$ of Example 75 are maximal ideals. Since A_{12} is a commutative ring, G and H must also be prime ideals.

In a commutative ring without a unity, a maximal ideal need not be a prime ideal.

Example 78 The ideal C in the ring $[A_8^{\mathbb{P}}; \cdot; 0]$ of Example 74 is a maximal ideal but it is not a prime ideal since $3 \cdot 7 = 1 \in C$ while $3 \notin C$ and $7 \notin C$. The ideals B and D of the same example are similarly seen to be maximal but not prime ideals in $A_8^{\mathbb{P}}$.

Not all prime ideals in a commutative ring with unity are maximal.

Example 79 Consider the two rings $[A_3; +; \cdot]$ and $[A_4; +; \cdot]$ with the usual operations in 3 and 4-arithmetic, respectively. Let $A_3 \times A_4 = \{ \langle a, b \rangle : a \in A_3, b \in A_4 \}$. By Theorem 2.46, $[A_3 \times A_4; *]$ is an additive group if $*$ is defined by $\langle a, b \rangle * \langle a', b' \rangle = \langle a + a', b + b' \rangle$ for every $a, a' \in A_3$ and for every $b, b' \in A_4$. $[A_3 \times A_4; *]$ is an abelian group since addition in A_3 and A_4 is abelian. If multiplication \circ is defined on $A_3 \times A_4$ by $\langle a, b \rangle \circ \langle a', b' \rangle = \langle a \cdot b, a' \cdot b' \rangle$ for every $a, a' \in A_3$ and for every $b, b' \in A_4$ where the multiplications indicated on the right side of the equation are in the respective rings, then multiplication is closed in $A_3 \times A_4$ since multiplication is closed in the

respective rings. It is easy to verify that $[A_3 \times A_4; *; 0]$ thus defined is a commutative ring with unity element $\langle 1, 1 \rangle$. The subsets $N = \{\langle 0, 0 \rangle, \langle 0, 2 \rangle, \langle 1, 0 \rangle, \langle 1, 2 \rangle, \langle 2, 0 \rangle, \langle 2, 2 \rangle\}$ and $M = \{\langle 0, 0 \rangle, \langle 0, 2 \rangle\}$ are proper prime ideals in $A_3 \times A_4$ but M is obviously not a maximal ideal in $A_3 \times A_4$ since M is properly contained in the N . Hence, $[A_3 \times A_4; *; 0]$ is a commutative ring with unity which has a prime ideal which is not a maximal ideal.

The next theorem gives an easy way to identify prime ideals in the ring of integers $[I; +; \cdot]$.

Theorem 3.20 In the ring of integers $[I; +; \cdot]$, a proper ideal $J = \{mr : r, m \in I, \text{ fixed } m \neq 0\}$ is a prime ideal if and only if m is a prime integer.

Recall that by Theorem 3.18, all ideals in $[I; +; \cdot]$ are principal ideals. Hence, if the generator of an ideal in I can be identified, it is easy to determine if the ideal is a prime ideal. Notice that in Theorem 3.20, $J = (m)$. Thus, (2), (3), (5), (7), and (11) are prime ideals while (4), (6), (8), (9), and (10) are not prime ideals. If $m = 0$, then $(m) = (0) = \{0\}$ which is also a prime ideal in I . (1) is obviously a prime ideal since $(1) = I$.

Quotient Rings

Knowing an ideal in a ring enables one to construct another ring by defining an additional operation on an additive quotient group.

Definition 3.21 Any ideal N in a ring R is an invariant subgroup of the additive abelian group R so that the additive quotient group

$R/N = \{N+a : a \in R\}$ is the set of all distinct cosets of N in R . Addition on R/N is defined by $(N+a)+(N+b) = N+(a+b)$ for any $a, b \in R$. Multiplication may be defined on R/N by $(N+a) \cdot (N+b) = N+ab$ for any $a, b \in R$.

Theorem 3.22 If N is an ideal in a ring R and if addition and multiplication are defined as in Definition 3.21, then the quotient group R/N is a ring (called a quotient ring) with respect to these binary operations.

Notice that multiplication and addition in a quotient ring of a ring R are defined in terms of the operations in R .

Example 80 $[N; \cdot; \circ]$ is an ideal in the ring $[A_8^P; \cdot; \circ]$ of Example 49, where $N = \{1, 3\}$. Keep in mind that the operations \cdot and \circ are called addition and multiplication, respectively, on A_8^P . Consequently, the operations defined in Definition 3.21 for a quotient ring of A_8^P would have to be symbolized accordingly. Hence, $A_8^P/N = \{N, N \cdot 5\}$ where $N \cdot 5 = \{5, 7\} = N \cdot 7$. Tables I and II below give the Cayley squares for the operations of addition and multiplication, respectively, in A_8^P/N .

+	N	N·5
N	N	N·5
N·5	N·5	N

TABLE I

·	N	N·5
N	N	N
N·5	N	N

TABLE II

Notice that the product of any two elements in A_8^P/N gives N because the product of any two elements in A_8^P gives 1. Hence, the unique product property of A_8^P is inherited by A_8^P/N .

If N in Theorem 3.22 is a subring which is not an ideal in the ring R , then the conclusion of the theorem is not valid.

Example 81 The right ideal $B = \left\{ \begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix} : a, b \in A_3 \right\}$ in the ring

$[R; +; \cdot]$ of 2×2 matrices over 3-arithmetics is a subring of R which is not an ideal in R (see Example 71). B is of order 9 and R is of order 81 so that R/B is an additive quotient group of order 9 by Theorem 2.32. R/B consists of nine cosets, each representable in the form $B + \begin{pmatrix} 0 & 0 \\ a & b \end{pmatrix}$ where $a, b \in A_3$. Notice that the coset $B + \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$ can

also be represented by $B + \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ since $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \in \left[B + \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} \right]$. Also,

$$\begin{pmatrix} 0 & 0 \\ 2 & 2 \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 2 & 2 \end{pmatrix} \in \left[B + \begin{pmatrix} 0 & 0 \\ 2 & 2 \end{pmatrix} \right] \text{ while } \begin{pmatrix} 0 & 0 \\ 2 & 2 \end{pmatrix} \cdot \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 2 \end{pmatrix} \in \left[B + \begin{pmatrix} 0 & 0 \\ 0 & 2 \end{pmatrix} \right].$$

Since $B + \begin{pmatrix} 0 & 0 \\ 0 & 2 \end{pmatrix}$ and $B + \begin{pmatrix} 0 & 0 \\ 2 & 2 \end{pmatrix}$ are distinct cosets in R/B , the product of the cosets $B + \begin{pmatrix} 0 & 0 \\ 2 & 2 \end{pmatrix}$ and $B + \begin{pmatrix} 0 & 0 \\ 1 & 1 \end{pmatrix}$, as defined in Definition 3.21, is not well defined, i.e., the product depends on the choice of representatives. Hence, this definition of product does not define a binary operation on R/B so that R/B is not a ring. Recall that B is a right ideal in R but not a two-sided ideal in R .

Some homomorphisms between rings and quotient rings are closely related to certain ideals. If α is a homomorphism of a ring R into a ring S and if z is the zero of S , then the set $z\alpha^{-1} = \{a \in R : \alpha a = z\}$ is called the kernel of the homomorphism α .

Theorem 3.23 Let N be an ideal in a ring R and let α be a mapping of R onto R/N such that $a\alpha = N+a$ for every $a \in R$. Then α is a (ring) homomorphism with kernel N .

The mapping α in Theorem 3.23 is called the natural homomorphism of R onto R/N . The natural homomorphism from the ring A_8^P onto A_8^P/N of Example 80 is defined by the equations $1\alpha = 3\alpha = N$ and $5\alpha = 7\alpha = N \cdot 5$. From Table I it is seen that N is the zero of A_8^P/N and, hence, by the way α is defined, N is the kernel of α . Straight forward verification that α preserves both addition and multiplication shows that α is indeed a homomorphism, e.g., $(1 \cdot 3)\alpha = 3\alpha = N = N+N = 1\alpha+3\alpha$ and $(5 \cdot 7)\alpha = 1\alpha = N = (N \cdot 5) \cdot (N \cdot 5) = (5\alpha) \cdot (7\alpha)$.

Consider another example of Theorem 3.23.

Example 82 The ring $[A_{20}; +; \cdot]$ with the usual operations in 20-arithmetic has many ideals and, hence, many corresponding natural homomorphisms can be constructed. The subset $M = \{0, 5, 10, 15\}$ is an ideal in A_{20} so that A_{20}/M with the operations given in Definition 3.21 is a quotient ring. Define the mapping β by $0\beta = 5\beta = 10\beta = 15\beta = M$, $1\beta = 6\beta = 11\beta = 16\beta = M+1$, $2\beta = 7\beta = 12\beta = 17\beta = M+2$, $3\beta = 8\beta = 13\beta = 18\beta = M+3$, and $4\beta = 9\beta = 14\beta = 19\beta = M+4$. Straight forward calculations show that β preserves both of the operations of A_{20} . Hence, β is a homomorphism and by the way β is defined, the kernel of β is M .

If N is a subring of a ring R , then the mapping defined in Theorem 3.23 need not be a ring homomorphism.

Example 83 Consider the subring B of the ring R and the corresponding quotient group R/B given in Example 81. Define the mapping α from R onto R/B by $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \alpha = B + \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ for every $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in R$. Then α preserves addition, e.g., $\left[\begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix} + \begin{pmatrix} 0 & 2 \\ 2 & 0 \end{pmatrix} \right] \alpha = \begin{pmatrix} 1 & 2 \\ 1 & 1 \end{pmatrix} \alpha = B + \begin{pmatrix} 0 & 0 \\ 1 & 1 \end{pmatrix}$ and

$$\begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix} \alpha + \begin{pmatrix} 0 & 2 \\ 2 & 0 \end{pmatrix} \alpha = \left[B + \begin{pmatrix} 0 & 0 \\ 2 & 1 \end{pmatrix} \right] + \left[B + \begin{pmatrix} 0 & 0 \\ 2 & 0 \end{pmatrix} \right] = B + \left[\begin{pmatrix} 0 & 0 \\ 2 & 1 \end{pmatrix} + \begin{pmatrix} 0 & 0 \\ 2 & 0 \end{pmatrix} \right] = B + \begin{pmatrix} 0 & 0 \\ 1 & 1 \end{pmatrix} \text{ so}$$

that $\left[\begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix} + \begin{pmatrix} 0 & 2 \\ 2 & 0 \end{pmatrix} \right] \alpha = \begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix} \alpha + \begin{pmatrix} 0 & 2 \\ 2 & 0 \end{pmatrix} \alpha$. But, α does not preserve

multiplication, e.g., $\left[\begin{pmatrix} 2 & 0 \\ 2 & 2 \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 \\ 1 & 0 \end{pmatrix} \right] \alpha = \begin{pmatrix} 2 & 0 \\ 1 & 0 \end{pmatrix} \alpha = B + \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}$ while

$$\begin{pmatrix} 2 & 0 \\ 2 & 2 \end{pmatrix} \alpha \cdot \begin{pmatrix} 1 & 0 \\ 1 & 0 \end{pmatrix} \alpha = \left[B + \begin{pmatrix} 0 & 0 \\ 2 & 2 \end{pmatrix} \right] \cdot \left[B + \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} \right] = B + \left[\begin{pmatrix} 0 & 0 \\ 2 & 2 \end{pmatrix} \cdot \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} \right] = B + \begin{pmatrix} 0 & 0 \\ 2 & 0 \end{pmatrix} \text{ so}$$

that $\left[\begin{pmatrix} 2 & 0 \\ 2 & 2 \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 \\ 1 & 0 \end{pmatrix} \right] \alpha \neq \begin{pmatrix} 2 & 0 \\ 2 & 2 \end{pmatrix} \alpha \cdot \begin{pmatrix} 1 & 0 \\ 1 & 0 \end{pmatrix} \alpha$. Hence, α is a group homomor-

phism between the additive groups R and R/B but α is not a ring homomorphism. This is not surprising since in Example 81 it was found that R/B is not a ring.

Theorem 3.23 and the next theorem are sometimes combined as one theorem and called the fundamental homomorphism theorem for rings.

Theorem 3.24 Let α be a homomorphic mapping of a ring R onto a ring R' with kernel N . Then N is an ideal in R and the ring R/N is isomorphic to R' .

Many of the examples in this dissertation have been developed using m -arithmetic systems. Theorem 3.24 can be used to show that $[A_m; +; \cdot]$ with the usual operations in m -arithmetic is isomorphic to the quotient ring $I/(m)$, where $[I; +; \cdot]$ is the ring of integers and (m) is the principal ideal generated by the integer m .

Example 84 Consider the ring of integers $[I; +; \cdot]$ and the ring $[A_{10}; +; \cdot]$ with the usual operations in 10-arithmetic. For any integer $n \in I$, $n = 10q + r$ where $q, r \in I$ and $0 \leq r < 10$. Define α from I onto A_{10} by $n\alpha = r$, where n has the representation just given, for any $n \in I$. Then α can be shown to be a homomorphism and α maps I

onto A_{10} since each element in A_{10} has at least one preimage, i.e., $0\alpha = 0$, $1\alpha = 1$, $2\alpha = 2, \dots, 8\alpha = 8$, and $9\alpha = 9$. The zero of A_{10} is 0 so that the kernel of α is the set $\{10n : n \in I\} = N$. Theorem 3.24 asserts that N is an ideal. In fact, N is recognized as the principal ideal generated by 10, (10) . The cosets in the quotient ring $I/(10)$ can all be represented in the form $(10)+n$ where $n = 0, 1, 2, \dots, 9$. The isomorphism asserted in Theorem 3.24 is the mapping β from $I/(10)$ into A_{10} defined by $[(10)+n]\beta = n$ for every $n = 0, 1, 2, \dots, 9$.

The fact that the kernel N of a mapping α from a ring R onto a ring R' is an ideal in R does not imply that α is a homomorphism or that R/N is isomorphic to R' .

Example 85 Consider the rings $[A_{12}; +; \cdot]$ and $[A_4; +; \cdot]$ with the usual operations in 12 and 4-arithmetic, respectively. The subset $N = \{0, 6\}$ is an ideal in A_{12} . Define α from A_{12} onto A_4 by $0\alpha = 6\alpha = 0$, $1\alpha = 1$, $2\alpha = 2$, and $3\alpha = 4\alpha = 5\alpha = 7\alpha = 8\alpha = 9\alpha = 10\alpha = 11\alpha = 3$. Then the kernel of α is the ideal N in A_{12} . α is not a homomorphism since α does not preserve the operations of A_{12} , e.g., $(2+5)\alpha = 7\alpha = 3$ while $2\alpha+5\alpha = 2+3 = 1$ so that $(2+5)\alpha \neq 2\alpha+5\alpha$. A_{12}/N is not isomorphic to A_4 , either, since A_{12}/N is of order 6 while A_4 is of order 4.

Polynomial Rings

Polynomials in one variable with real numbers as coefficients are dealt with extensively in elementary algebra. Many of the results derived for these polynomials are special cases of more general theorems now to

be considered.

Definition 3.25 Let R be a ring and let x , called an indeterminate, be any symbol not representing an element of R . A polynomial in x over R is any expression of the form $f(x) = a_0x^0 + a_1x^1 + a_2x^2 + \dots = \sum a_k x^k$, $a_k \in R$ in which only a finite number of the a_k 's, called coefficients, are different from z , the zero of R .

Two polynomials, $f(x) = \sum a_k x^k$ and $g(x) = \sum b_k x^k$, in x over the ring R will be called equal, denoted $f(x) = g(x)$, provided $a_k = b_k$ for all values of k . If $f(x) = \sum a_k x^k$ is written without using the summation symbol, then only the powers of x having nonzero coefficients will be written explicitly. All powers of x not present in such an expansion of $f(x)$ implicitly have z as coefficient where z is the zero of R .

Example 86 Consider the ring $[A_8; +; \cdot]$ with the usual operations in 8-arithmetic. $f(x) = 7x^0 + 2x^1 + 3x^5$ and $g(x) = 7x^0 + 2x^1 + 4x^5$ are polynomials in x over A_8 since each has only a finite number of coefficients different from 0, the zero of A_8 . $f(x)$ and $g(x)$ are not equal since the coefficients of x^5 are not the same. $h(x) = 7x^0 + 0x^1 + 2x^1 + 0x^2 + 0x^3 + 0x^4 + 3x^5 + \sum_{i=6}^{\infty} 0x^i$ is also a polynomial in x over A_8 since only a finite number of the coefficients are different from 0. It is clear that $f(x) = h(x)$ and that the way $f(x)$ is written is simpler and, hence, the preferred way of writing this polynomial.

Some polynomials may be written identically but not be equal because the coefficients are from different rings.

Example 87 $f(x) = 2x^0 + 1x^8$, where $1, 2 \in I$, is a polynomial over

the ring of integers $[I; +; \cdot]$. $g(x) = 2x^0 + 1x^8$, where $1, 2 \in A_3$, is a polynomial over the ring $[A_3; +; \cdot]$ with the usual operations in 3-arithmetics. $f(x)$ and $g(x)$ are written identically but are not equal in the sense defined above since the coefficients are elements of different rings.

Definition 3.26 Let $R[x]$ denote the set of all polynomials in x over the ring R . Define addition $+$ and multiplication \cdot on $R[x]$ by $f(x) + g(x) = \sum (a_k + b_k)x^k$ and $f(x) \cdot g(x) = \sum c_k x^k$, where $f(x) = \sum a_k x^k$ and $g(x) = \sum b_k x^k$ are elements of $R[x]$ and where $c_k = \sum_{i=0}^k a_i b_{k-i}$.

Theorem 3.27 The set of all polynomials, $R[x]$, in x over the ring R is a ring with respect to the addition and multiplication defined in Definition 3.26. This ring is called a ring of polynomials in x over R or, briefly, a polynomial ring.

Theorem 3.27 establishes that addition and multiplication as defined on $R[x]$ are binary operations. These operations obviously depend on the operations in the ring R .

Example 88 Let $A_8^P[x]$ represent the ring of polynomials in x over the ring $[A_8^P; \cdot; 0]$ of Example 49. The zero of $A_8^P[x]$ is the polynomial $f(x) = \sum 1x$ since 1 is the zero of $[A_8^P; \cdot; 0]$. Recalling that each element in A_8^P is its own additive inverse allows one to recognize that every polynomial in $A_8^P[x]$ is also self inverse under addition. Multiplication of polynomials in $A_8^P[x]$ always yields the polynomial, $f(x) = \sum 1x$, since products in A_8^P always yield 1 and 1 added to itself any number of times is 1 in A_8^P . The ring $[A_8^P; \cdot; 0]$ is a commutative ring and, hence, so is the ring $A_8^P[x]$. $[A_8^P; \cdot; 0]$

has no unity and neither does $A_8^P[x]$.

Not all the properties of a ring R are inherited by the ring of polynomials $R[x]$. For example, the ring $[A_8^P; \cdot; 0]$ is a finite ring of order 4 while the polynomial ring $A_8^P[x]$ is of infinite order. In fact, all polynomial rings are of infinite order. The next theorem states one property which is always inherited by a polynomial ring.

Theorem 3.28 Let R be a ring and let x be an indeterminant. Then $R[x]$ is a commutative ring if and only if R is a commutative ring.

In Example 88 it was noted that both $[A_8^P; \cdot; 0]$ and $A_8^P[x]$ are commutative rings. The ring $[R; +; \cdot]$ of Example 71 is noncommutative. One can show that $R[x]$ for this ring R is noncommutative by computing the product of $\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}x$ and $\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}x$ in both orders. On the other hand, $[A_6; +; \cdot]$ with the usual operations in 6-arithmetics is a commutative ring and so is the ring $A_6[x]$ of polynomials in x over A_6 .

Some definitions made for the study of polynomials over the real numbers in elementary algebra are special cases of definitions associated with the study of polynomial rings. If R is a ring and $f(x) \in R[x]$, where $f(x) = \sum_k a_k x^k$, then the degree of $f(x)$ is n and a_n is the leading coefficient of $f(x)$ if $a_n \neq z$, the zero of R , while $a_k = z$ for all $k > n$. The polynomial $\sum_k z x^k \in R[x]$ is called the zero polynomial of $R[x]$. If the ring R has a unity u , then any polynomial $f(x)$ of degree m over R with leading coefficient u is called monic.

The degree of each of the polynomials $f(x)$, $g(x)$, and $h(x)$ in Example 86 is 5 and their respective leading coefficients are 3, 4, and 3. The polynomial $f(x)$ of Example 87 is of degree 8 and has leading

coefficient 1, the unity of the ring $[I; +; \cdot]$, and, hence, $f(x)$ is monic. The zero polynomial of the ring $A_8^p[x]$ of Example 88 is $\Sigma 1x^k$ while the zero polynomial of the ring $A_8[x]$ of Example 86 is $\Sigma 0x^k$.

A result similar to the Division Algorithm for the ring of integers can be established for a ring of polynomials over a ring with unity. The terminology used will be analogous to that associated with the Division Algorithm for the ring of integers. One may say that one polynomial is divided by another obtaining a quotient and remainder, etc.

Theorem 3.29 (Division Algorithm) Let R be a commutative ring with unity u , $f(x) = \Sigma a_k x^k \in R[x]$ be either the zero polynomial or a polynomial of degree m , and $g(x) = \Sigma b_k x^k \in R[x]$ be a monic polynomial of degree n . Then there exist unique polynomials $q(x), r(x) \in R[x]$ with $r(x)$ either the zero polynomial or of degree less than n such that $f(x) = [q(x) \cdot g(x)] + r(x)$.

Example 89 The commutative ring $[A_{10}; +; \cdot]$ with the usual operations in 10-arithmetic has a unity, 1. Hence, Theorem 3.29 applies to the ring of polynomials $A_{10}[x]$. The zero polynomial of $A_{10}[x]$ is $\Sigma 0x^k$. Let $f(x) = 2x^0 + 1x^1 + 2x^2 + 3x^4$ and $g(x) = 7x^0 + 1x^2$. Since $g(x)$ is monic, Theorem 3.29 implies that unique polynomials $q(x)$ and $r(x)$ exist such that $f(x) = [q(x) \cdot g(x)] + r(x)$ where $r(x) = \Sigma 0x^k$ or the degree of $r(x)$ is less than 2, the degree of $g(x)$. Simple division shows that $q(x) = 1x^0 + 3x^2$ and $r(x) = 5x^0 + 1x^1$. Notice the degree of $r(x)$ is 1 which is less than 2. If $h(x) = 3x^0 + 1x^1$, then $f(x) = [s(x) \cdot h(x)] + t(x)$ where $s(x) = 4x^0 + 9x^1 + 1x^2 + 3x^3$ and $t(x) = \Sigma 0x^k$.

The polynomial $g(x)$ in Theorem 3.29 must be monic in order for unique polynomials $q(x)$ and $r(x)$ to exist satisfying the given conditions.

Example 90 Consider the polynomials over the ring $[A_{12}; +; \cdot]$ with the usual operations in 12-arithmetic. Then $A_{12}[x]$ is a commutative ring with unity. The zero polynomial is $\sum 0x^k$. If $f(x) = 4x^0 + 2x^4$ and $g(x) = 8x^0 + 2x^1$, then $f(x) = [h(x) \cdot g(x)] + \sum 0x^k$ where $h(x) = 2x^0 + 4x^1 + 2x^2 + 1x^3$ and $f(x) = [k(x) \cdot g(x)] + \sum 0x^k$ where $k(x) = 2x^0 + 4x^1 + 2x^2 + 7x^3$. Hence, the representation of $f(x)$ in the form $f(x) = [q(x) \cdot g(x)] + r(x)$ is not unique where $r(x)$ is the zero polynomial or is of degree less than 1, the degree of $g(x)$.

The ring R in Theorem 3.29 must have a unity.

Example 91 The commutative ring $[A_8^p; \cdot; 0]$ of Example 49 has no unity. Hence, there are no monic polynomials in $A_8^p[x]$. Still for any $f(x), g(x) \in A_8^p$, there exist $q(x), r(x) \in A_8^p$ such that $f(x) = [q(x) \cdot g(x)] + r(x)$. Any polynomial in $A_8^p[x]$ can be used for $q(x)$ but $r(x)$ will be unique, $r(x) = f(x)$. Hence, $r(x)$ may, but need not be, the zero polynomial or have degree less than $g(x)$.

If R is a ring with unity, then for $f(x)$ and $g(x)$ as given in Theorem 3.29, there exists unique polynomials $q_R(x), r_R(x), q_L(x), r_L(x) \in R[x]$ with $r_R(x)$ and $r_L(x)$ either the zero polynomial or of degree less than the degree of $g(x)$ such that $f(x) = [q_R(x) \cdot g(x)] + r_R(x)$ and $f(x) = [g(x) \cdot q_L(x)] + r_L(x)$. Thus, Theorem 3.29 is a special case of this fact when R is commutative so that $q_R(x) \cdot g(x) = g(x) \cdot q_L(x)$ and, hence, $q_R(x) = q_L(x)$ and $r_R(x) = r_L(x)$.

Example 92 Consider the noncommutative ring of 2×2 matrices over 2-arithmetic. Let the ring be denoted $[N; +; \cdot]$ where $+$ and \cdot are, respectively, ordinary addition and multiplication of matrices in

2-arithmetic. The unity of N is $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$. The ring of polynomials $N[x]$ is also noncommutative by Theorem 3.28. Let

$f(x) = \begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix}x^0 + \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}x^3$ and $g(x)$ be the monic polynomial

$\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}x^0 + \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}x^1$. Then $q_R(x) = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}x^2$, $r_R(x) = \begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix}x^0$,

$q_L(x) = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}x^0 + \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}x^1 + \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}x^2$, and $r_L(x) = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}x^0$ are unique

polynomials such that $f(x) = [q_R(x) \cdot g(x)] + r_R(x)$ and

$f(x) = [g(x) \cdot q_L(x)] + r_L(x)$ where the degree of $r_R(x)$ and of $r_L(x)$ is 0 which is less than 1, the degree of $g(x)$. Notice that $q_R(x) \neq q_L(x)$ and $r_R(x) \neq r_L(x)$.

In algebra, students learn that if a product of two real numbers is zero, then at least one of the factors must be zero. Similarly, products which equal the zero of a ring are important in ring theory. Let R be a ring with zero z . An element $a \neq z$ of R is called a divisor of zero or a zero divisor if there exists an element $b \neq z$ of R such that $ab = z$ or $ba = z$. Of course, if R is commutative, then $ab = z$ if and only if $ba = z$.

Example 93 The ring $[A_{10}; +; \cdot]$ with the usual operations in 10-arithmetic is a commutative ring with zero element 0. Since $2 \cdot 5 = 0$, $4 \cdot 5 = 0$, $6 \cdot 5 = 0$, and $8 \cdot 5 = 0$, the elements 2, 4, 5, 6, and 8 are all divisors of zero in A_{10} . 1, 3, 7, and 9 are not divisors of zero since a product of two elements of A_{10} , one of which is 1, 3, 7, or 9, will equal 0 only if 0 is the other factor.

Many elements in the noncommutative ring $[N; +; \cdot]$ of Example 92 are divisors of zero. Since $\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \cdot \begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$ and $\begin{pmatrix} 1 & 0 \\ 1 & 0 \end{pmatrix} \cdot \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$,

the zero of N , each of the elements $\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$, $\begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix}$, $\begin{pmatrix} 1 & 0 \\ 1 & 0 \end{pmatrix}$ and $\begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$ is a divisor of zero.

Theorem 3.30 If R be a commutative ring without divisors of zero, then $R[x]$ is also free of divisors of zero.

The property of being free of divisors of zero is thus seen to be another property of a ring R inherited by $R[x]$. Hence, since the ring $[A_7; +; \cdot]$ with the usual operations in 7-arithmetic has no divisors of zero, one knows that the polynomial ring $A_7[x]$ also has no divisors of zero. It is, of course, easier to determine if there are divisors of zero in A_7 than it is in $A_7[x]$ since A_7 is of finite order while $A_7[x]$ is of infinite order.

Recall that in the ring $[A_8^p; \cdot; 0]$ of Example 49 every element except 1, the zero of A_8^p , is a divisor of zero. Similarly, every element except $\sum 1x^k$, the zero of $A_8^p[x]$ is a divisor of zero in the ring $A_8^p[x]$. Some polynomial rings have both zero divisors and elements other than the zero polynomial which are not zero divisors.

Example 94 In Example 93 it was found that 2, 4, 5, 6, and 8 are zero divisors in the ring $[A_{10}; +; \cdot]$ while 1, 3, 5, 7, and 9 are nonzero elements of A_{10} which are not zero divisors. The polynomials $4x^5$, $5x^3$, $2x^0+6x^8$, and $5x^0+5x^2$ are divisors of zero in $A_{10}[x]$ since $4x^5 \cdot 5x^3 = \sum 0x^k$ and $(2x^0+6x^8) \cdot (5x^0+5x^2) = \sum 0x^k$, the zero polynomial in $A_{10}[x]$. One can easily show that $f(x) = 7x^0+2x^5$ and $g(x) = 6x^3+9x^8$ are nonzero polynomials in $A_{10}[x]$ which are not divisors of zero. $g(x)$ is not a divisor of zero since any nonzero polynomial of degree n multiplied by $g(x)$ will yield a polynomial

with a nonzero coefficient of x^{n+8} since 9 is not a divisor of zero in A_{10} . A similar type of argument can be used to show that $f(x)$ is not a divisor of zero.

Euclidean Rings

Definition 3.31 Let R be a commutative ring. If it is possible to define a (valuation) mapping θ on the set of nonzero elements of R into the nonnegative integers such that:

- (i) for $a, b \in R$, $(ab)\theta \geq a\theta$ if $ab \neq z$, the zero of R , and
- (ii) for every $a \in R$ and $b \neq z \in R$, there exist elements $q, r \in R$ such that $a = bq + r$ where either $r = z$ or $r\theta < b\theta$,

then R is called a Euclidean ring.

The ring of integers $[I; +; \cdot]$ is a Euclidean ring since the absolute value function is a mapping from I into the nonnegative integers satisfying all the properties of Definition 3.31. Other Euclidean rings have different valuation maps.

Example 95 The ring of polynomials $A_5[x]$ over the ring $[A_5; +; \cdot]$ with the usual operations in 5-arithmetic is a Euclidean ring. The valuation mapping θ on the nonzero elements of $A_5[x]$ is the mapping that assigns to each nonzero polynomial $f(x)$ in $A_5[x]$ the integer corresponding to its degree, i.e., $[f(x)]\theta = n$ if the degree of $f(x)$ is n .

If a polynomial ring has zero divisors then the degree map will not serve as a valuation map.

Example 96 Consider the polynomial ring $A_{10}[x]$ over the ring

$[A_{10}; +; \cdot]$ with the usual operations in 10-arithmetic. Let θ be defined from the nonzero elements of $A_{10}[x]$ into the nonnegative integers by $[f(x)]\theta = n$ if n is the degree of $f(x)$. θ is not a valuation map for $A_{10}[x]$ since $(7x^0+5x^1) \cdot (2x^0) = 4x^0 \neq \sum 0x^k$, the zero polynomial, but $(4x^0)\theta = 0 < 1 = (7x^0+5x^1)\theta$ so that (i) of Definition 3.31 is not satisfied.

Finite Euclidean rings also exist. Any finite ring in which every nonzero element has a multiplicative inverse can be shown to be a Euclidean ring by a technique similar to that used in the next example.

Example 97 The finite ring $[A_7; +; \cdot]$ with the usual operations in 7-arithmetic is a ring in which every nonzero element has a multiplicative inverse. If a map α is defined from the nonzero elements of A_7 into $[I; +; \cdot]$ by $a\alpha = 0$ for every $a \neq 0 \in A_7$, then α is a valuation map for A_7 . Part (i) of Definition 3.31 is satisfied by α since $(ab)\alpha = 0 = a\alpha$ if $ab \neq 0$. Part (ii) of Definition 3.31 is also satisfied since $r = 0$ in all cases for the ring A_7 . Hence, $[A_7; +; \cdot]$ is a finite Euclidean ring.

Every ring $[A_m; +; \cdot]$ with the usual operations in m -arithmetic, where m is an integer greater than 1, is a Euclidean ring. If m is not a prime, then the valuation map for the Euclidean ring A_m can be established in a manner similar to the next example.

Example 98 Consider the ring $[A_6; +; \cdot]$ with the usual operations in 6-arithmetic. One can show that a map similar to that defined in Example 97 does not work for A_6 since (ii) of Definition 3.31 is not satisfied. Recall that the order of an element $a \in A_6$ is the

order of the additive subgroup of A_6 which is generated by a .

Hence, 0 is of order 1; 1 and 5 are of order 6; 2 and 4 are of order 3; and 3 is of order 2. Define the map β from the nonzero elements of A_6 into the nonnegative integers by $1\beta = 5\beta = 1$, $2\beta = 4\beta = 2$, and $3\beta = 3$. Notice that $a\beta = \frac{6}{n_a}$ for each $a \neq 0 \in A_6$ where n_a denotes the order of the element $a \in A_6$. One can show that β is a valuation map for the Euclidean ring $[A_6; +; \cdot]$, e.g., $(3 \cdot 5)\beta = 3\beta = 3 > 1 = 5\beta$ and $2 = (5 \cdot 4) + 0$ in A_6 so that $q = 4$ and $r = 0$.

The next two theorems establish some properties that all Euclidean rings possess.

Theorem 3.32 Every Euclidean ring is a principal ideal ring.

Theorem 3.33 Every Euclidean ring has a unity.

Example 99 As mentioned above, the ring of integers $[I; +; \cdot]$ is a Euclidean ring with the absolute value function as its valuation map. Theorem 3.18 established that $[I; +; \cdot]$ is a principal ideal ring. Notice also that 1 is the unity for I . Hence, $[I; +; \cdot]$ satisfies both Theorem 3.32 and Theorem 3.33.

The Euclidean ring $[A_7; +; \cdot]$ of Example 97 has 1 as its unity. Since the only ideals in A_7 are the ideals $(0) = \{0\}$ and $(1) = A_7$, A_7 is seen to satisfy Theorem 3.32 and Theorem 3.33.

In Example 98 the ring $[A_6; +; \cdot]$ was found to be Euclidean. Since an ideal is a subring and since every subring of A_6 is generated by a single element of A_6 , A_6 is seen to be a principal ideal ring. The unity of A_6 is 1.

Theorem 3.32 is particularly valuable when considering the ring $A_5[x]$ of Example 95. It would be difficult to establish directly that $A_5[x]$ is a principal ideal ring since an infinite number of ideals exist in the ring, i.e., $(1x^n)$ is an ideal for each nonnegative integer n and $(1x^n) \neq (1x^m)$ if $n \neq m$. By Example 95, $A_5[x]$ is a Euclidean ring so that Theorem 3.32 can be used to easily establish that $A_5[x]$ is a principal ideal ring.

Rings do exist satisfying the conclusion of Theorem 3.32 or Theorem 3.33 but which are not Euclidean rings. The ring of all even integers under ordinary addition and multiplication of integers is a principal ideal ring but is not a Euclidean ring since it has no unity. The ring of 2×2 matrices over \mathbb{Z}_2 -arithmetic is a ring with unity $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ but is not a Euclidean ring since the ring is not commutative.

Noetherian Rings

Some properties of the set of all ideals in a ring R are of interest. A ring R is said to satisfy the ascending chain condition for ideals if every sequence of ideals N_1, N_2, N_3, \dots in R , such that $N_1 \subset N_2 \subset N_3 \subset \dots$, has only a finite number of distinct terms.

If R is a commutative ring in which every ideal in R is generated by a finite number of elements of R , then R has the basis property. A commutative ring which has the basis property is called a Noetherian ring. Notice that, contrary to some definitions, a Noetherian ring does not necessarily have a unity. Noetherian rings can be characterized in terms of the ascending chain condition.

Theorem 3.34 In any commutative ring R the following conditions

are equivalent:

- (i) R is a Noetherian ring.
- (ii) R satisfies the ascending chain condition for ideals.
- (iii) Every nonempty set of ideals in R contains at least one maximal ideal, i.e., one ideal which is not contained in any other proper ideal in the set.

The ring of integers $[I; +; \cdot]$ is a Noetherian ring with unity 1. Subrings of I such as $E = \{2n : n \in I\}$ and $S = \{6n : n \in I\}$ are also Noetherian rings but have no unity. Since, by Theorem 3.18, I is a principal ideal ring, I is easily seen to be Noetherian and, hence, to satisfy (ii) and (iii) of Theorem 3.34. Since E and S are subrings of I , they must also be Noetherian. Similarly, the finite ring $[A_8; +; \cdot]$ with the usual operations in 8-arithmetic and its subrings can be shown to be Noetherian and, hence, satisfy (ii) and (iii) of Theorem 3.34.

Theorem 3.35 (Hilbert Basis Theorem) If R is any Noetherian ring with unity, then so is the ring of polynomials $R[x]$.

The ring of integers $[I; +; \cdot]$ with unity 1 is Noetherian. Thus, $I[x]$ is also Noetherian and satisfies the ascending chain condition and maximal condition of Theorem 3.34. The unity of $I[x]$ is $1x^0$.

If R is a Noetherian ring but has no unity, then $R[x]$ has no unity either.

Example 100 The ring $[A_{12}; +; \cdot]$ with the usual operations in 12-arithmetic is a Noetherian ring with unity. $T = \{0, 2, 4, 6, 8, 10\}$ under the operations of $[A_{12}; +; \cdot]$ is a Noetherian ring without unity. $T[x]$ is a Noetherian ring since it is a subring of $A_{12}[x]$ which is

Noetherian by Theorem 3.35. However, $T[x]$ has no unity since $1x^0$, the unity of $A_{12}[x]$, is not in $T[x]$.

CHAPTER IV

INTEGRAL DOMAINS AND FIELDS

Integral Domains

Many algebraic structures have two operations, called addition and multiplication. A ring is a nonempty set R having two operations, addition and multiplication, such that R is an additive abelian group, R is a multiplicative semigroup, and two distributive laws relating addition and multiplication hold for elements of R . Different types of rings such as commutative rings and rings with unity are obtained, as in Chapter III, by imposing various conditions on the multiplicative semigroup of a ring. Rings satisfying more than one condition on their multiplicative semigroups are considered in this chapter.

Topics are not considered as extensively in this chapter as in previous chapters. Examples in this chapter illustrate the content of the definitions and theorems as stated. Systems developed in this and previous chapters can be used to show what happens if some of the hypotheses of a theorem are ignored.

Definition 4.1 A commutative ring with unity which has no divisors of zero is called an integral domain.

Notice that the existence of a unity is asserted in this definition of an integral domain; a few authors do not require an integral domain to have a unity. Thus, the ring of integers $[I; +; \cdot]$ is an integral

domain but the subring $[E;+;\cdot]$ of even integers is not an integral domain since E does not contain the unity 1 of I .

Finite integral domains also exist. The ring $[A_7;+;\cdot]$ with the usual operations in 7-arithmetic is an integral domain while the ring $[A_6;+;\cdot]$ with the usual operations in 6-arithmetic is not an integral domain since A_6 contains divisors of zero, i.e., $2 \cdot 3 = 0$ but $2 \neq 0$ and $3 \neq 0$.

Theorem 4.2 A commutative ring R with unity is an integral domain if and only if each equation $ab = ac$ and $ba = ca$ implies $b = c$, for a in R but not the zero of R and for arbitrary $b, c \in R$.

Theorem 4.2 is a characterization of an integral domain. Hence, the integral domains $[I;+;\cdot]$ and $[A_7;+;\cdot]$ mentioned above satisfy the only if part of the theorem. The only if part of the theorem can be used to show that a given commutative ring with unity is not an integral domain.

Example 101 The ring $[A_{12};+;\cdot]$ with the usual operations in 12-arithmetic is a commutative ring with unity. By Theorem 4.2, since $2 \cdot 3 = 6 = 2 \cdot 9$ while $3 \neq 9$, A_{12} is not an integral domain.

A characterization of when a quotient ring is an integral domain is given next.

Theorem 4.3 Let N be a proper ideal in a commutative ring R with unity. Then the quotient ring R/N is an integral domain if and only if N is a prime ideal in R .

Example 102 The ring of integers $[I;+;\cdot]$ is an integral domain with ideals $N = \{3n:n \in I\}$ and $M = \{8n:n \in I\}$. By Theorem 3.20, N

is a prime ideal while M is not a prime ideal since 3 is a prime while 8 is not a prime. Hence, by Theorem 4.3, I/N is an integral domain while I/M is not an integral domain. Notice that I/M is a commutative ring with unity but I/M has divisors of zero, e.g., $(M+4) \cdot (M+2) = M$ which is the zero of I/M while $M+4 \neq M$ and $M+2 \neq M$.

The ring R in Theorem 4.3 does not have to be an integral domain as was the case in Example 102.

Example 103. Consider the commutative ring $[A_{12}; +; \cdot]$ with the usual operations in 12-arithmetic. The ideals A_{12} , (2) , (3) , and (0) are the only prime ideals in A_{12} . (4) and (6) are the only ideals in A_{12} which are not prime. A_{12} and (0) are improper ideals in A_{12} . $A_{12}/(2)$ and $A_{12}/(3)$ are, by Theorem 4.3, integral domains while $A_{12}/(4)$ and $A_{12}/(6)$ are not integral domains. The quotient ring $A_{12}/(4)$ is a commutative ring with unity $(4)+1$ but is not an integral domain since $[(4)+2] \cdot [(4)+2] = (4)+0 = (4)$, which is the zero of $A_{12}/(4)$ while neither factor of the product is equal to (4) . Similar statements are true for $A_{12}/(6)$.

If N is an improper ideal in the ring R , then the double implication of Theorem 4.3 is not true. In Example 103 the ideal (0) is a prime ideal but $A_{12}/(0)$ is not an integral domain since $A_{12}/(0)$ is isomorphic to A_{12} which has divisors of zero.

An integral domain D may have multiplicative inverses for only a few of its elements. If an element a of an integral domain D has a multiplicative inverse in D , then a is called a unit. An element b of an integral domain D is called an associate of $a \in D$ if $b = ca$ for some unit $c \in D$.

Example 104 The integral domain of integers $[I;+;\cdot]$ has only two unit elements, 1 and -1. Hence, an element $b \in I$ is an associate of $a \in I$ if and only if $b = a$ or $b = -a$, the additive inverse of a .

Every element except zero in the integral domain $[A_7;+;\cdot]$ with the usual operations in 7-arithmetic has a multiplicative inverse in A_7 . Hence, all six nonzero elements of A_7 are units. Also, every nonzero element of A_7 is an associate of each of the other nonzero elements while 0 is an associate of itself.

An element a of an integral domain D is called a divisor of $b \in D$ if there exists an element $c \in D$ such that $b = ac$. If a is a divisor of b , then a divides b and this relationship is denoted a/b . A nonzero element a of an integral domain D is called a trivial divisor of $b \in D$ if a is a unit or an associate of b . Notice that in the integral domain $[A_7;+;\cdot]$ mentioned above, every nonzero element of A_7 is a trivial divisor of every element of A_7 including 0 since each nonzero element is a unit. Since 0 does not divide any element of A_7 , A_7 has no nontrivial divisors.

Nontrivial divisors of elements in $[I;+;\cdot]$ of Example 104 do exist. For example, 2 is a nontrivial divisor of every even integer except 2 and -2.

A nonzero, nonunit element b of an integral domain D having only trivial divisors is called a prime (irreducible element) of D . No element in A_7 is a prime since every nonzero element is a unit. On the other hand, an infinite number of elements in the integral domain $[I;+;\cdot]$ of integers are prime; e.g., 2, 3, 5, and 7. Notice that by this definition of prime, -2, -3, -5, and -7 are also primes.

Theorem 4.4 Let D be an integral domain which is also a Euclidean ring with valuation mapping θ . Then, for $a \neq z$, $b \neq z$ elements of D with zero z , $(ab)\theta = a\theta$ if and only if b is a unit of D .

The integral domain $[A_7; +; \cdot]$ with the usual operations in 7-arithmetic is a Euclidean ring under the valuation map α defined in Example 97. Since $a\alpha = 0$ for any $a \neq 0 \in A_7$ and since $ab = 0 \in A_7$ for $a, b \in A_7$ only if $a = 0$ or $b = 0$, $(ab)\alpha = a\alpha$ for all $a \neq 0$, $b \neq 0$. Hence, Theorem 4.4 implies that all the nonzero elements of A_7 are units, which is true as noted previously.

The integral domain of integers $[I; +; \cdot]$ has the absolute value function as its valuation mapping. Since $|nm| = |n| \cdot |m| = |n|$ for $n, m \in I$ only if $|m| = 1$, it follows from Theorem 4.4 that the only units of I are 1 and -1.

If D of Theorem 4.4 is a Euclidean ring which is not an integral domain, then the double implication of the theorem is not valid.

Example 105 Let $T = \{ \langle a, b \rangle : a, b \in A_2 \}$ where A_2 denotes the ring $[A_2; +; \cdot]$ with the usual operations in 2-arithmetic. T is thus the set of all ordered pairs of elements in A_2 . If addition and multiplication, respectively, are defined on T by $\langle a, b \rangle + \langle c, d \rangle = \langle a+c, b+d \rangle$ and $\langle a, b \rangle \cdot \langle c, d \rangle = \langle a \cdot c, b \cdot d \rangle$ for any $a, b, c, d \in A_2$ where the operations on the right side of each equation are those of A_2 , then T is a commutative ring with unity $\langle 1, 1 \rangle$. Define β from the nonzero elements of T into the nonnegative integers by $\langle 1, 1 \rangle \beta = 0$ and $\langle 1, 0 \rangle \beta = \langle 0, 1 \rangle \beta = 1$. Then T is a Euclidean ring with valuation map β . Notice that $(\langle 1, 0 \rangle \cdot \langle 1, 0 \rangle) \beta = \langle 1, 0 \rangle \beta$ even though $\langle 1, 0 \rangle$ is not a unit in T , i.e., $\langle 1, 0 \rangle$ has no multiplicative inverse in T .

T, however, is not an integral domain since T has zero divisors, e.g., $\langle 1,0 \rangle \cdot \langle 0,1 \rangle = \langle 0,0 \rangle$ while $\langle 1,0 \rangle \neq \langle 0,0 \rangle$ and $\langle 0,1 \rangle \neq \langle 0,0 \rangle$.

Subdomains

A subset H of an integral domain D, which is itself an integral domain with respect to the binary ring operations of D, is called a subdomain of D.

Theorem 4.5 If D is an integral domain with unity u, the subset $H = \{nu : n \in I\}$ is contained in every subdomain of D.

The integral domains $[I; +; \cdot]$ and $[A_7; +; \cdot]$ mentioned previously have no proper subdomains. For each of these integral domains, the subset $H = \{nu : n \in I\}$ is the whole integral domain so that these integral domains trivially satisfy Theorem 4.5. A nontrivial example of Theorem 4.5 is given next.

Example 106 Consider the set S of all 2X2 matrices over the integers

of the form $\begin{pmatrix} a & b \\ 5b & a \end{pmatrix}$ where $a, b \in I$, the integral domain of integers.

One can show that the set S under the usual matrix addition + and multiplication \cdot is an integral domain with unity $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$. The

only proper subdomain of S is the domain T consisting of all matrices

of the form $\begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix}$ where $a \in I$. Notice that $T = \left\{ n \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} : n \in I \right\}$

= H of Theorem 4.5. Since $T = H$ and T is a subdomain of S, S satisfies Theorem 4.5.

The result of repeatedly adding an element of an integral domain to itself helps classify integral domains. Let R be a ring with zero z and

suppose there exists a positive integer n such that $na = z$ for every $a \in R$. Then the smallest positive integer n such that $na = z$ for every $a \in R$ is called the characteristic of R . If no such integer exists, then R is said to have characteristic zero. (If no such integer exists, some authors say that R has characteristic infinity.) The characteristic of an integral domain D is the characteristic of the ring D .

Theorem 4.6 The characteristic of an integral domain is either zero or a positive prime integer.

Both of the integral domains $[I;+;\cdot]$ of integers and $[S;+;\cdot]$ of Example 106 have characteristic zero. The characteristic of the integral domain $[A_7;+;\cdot]$ with the usual operations in 7-arithmetic is 7, which is a prime.

Unique Factorization

Definition 4.7 Let D be an integral domain and $a \in D$ be any nonzero element of D which is not a unit. If $a = a_1 a_2 \cdots a_m = b_1 b_2 \cdots b_n$, where the a_i and b_j are prime elements of D , implies that $n = m$ and each a_i , $1 \leq i \leq m$ is an associate of some b_j , $1 \leq j \leq n$ and conversely each b_j is an associate of some a_i , then we say the unique factorization theorem holds in D or D has unique factorization.

The unique factorization theorem does not hold for all integral domains.

Example 107 Consider the integral domain $[S;+;\cdot]$ of Example 106.

Notice that $\begin{pmatrix} 4 & 0 \\ 0 & 4 \end{pmatrix} = \begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix} \cdot \begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix}$ and $\begin{pmatrix} 4 & 0 \\ 0 & 4 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 5 & 1 \end{pmatrix} \cdot \begin{pmatrix} -1 & 1 \\ 5 & -1 \end{pmatrix}$. It can

be shown that each of $\begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix}$, $\begin{pmatrix} 1 & 1 \\ 5 & 1 \end{pmatrix}$, and $\begin{pmatrix} -1 & 1 \\ 5 & -1 \end{pmatrix}$ is a prime in

$[S;+;\cdot]$ and that $\begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix}$ is not an associate of $\begin{pmatrix} 1 & 1 \\ 5 & 1 \end{pmatrix}$ or $\begin{pmatrix} -1 & 1 \\ 5 & -1 \end{pmatrix}$.

These facts are proved by Steward [21] on page 284. Hence, the integral domain $[S;+;\cdot]$ does not have unique factorization.

The work involved in determining, by use of the definition, if the unique factorization theorem holds for a particular integral domain could be lengthy. The next theorem is helpful when it applies.

Theorem 4.8 Let D be an integral domain which is also a Euclidean ring. Then the unique factorization theorem holds in D .

The integral domain $[I;+;\cdot]$ of integers is a Euclidean ring with the absolute value function as its valuation mapping. Hence, $[I;+;\cdot]$ must have unique factorization by Theorem 4.8. In high school algebra students are taught that the unique factorization theorem holds in I .

The integral domain $[A_7;+;\cdot]$ with the usual operations in 7-arithmetic is also a Euclidean ring under the valuation mapping $av = 0$ for every $a \neq 0 \in A_7$. Hence, A_7 has unique factorization. Notice that A_7 has no prime elements so A_7 vacuously satisfies Definition 4.7.

Equality or inequality can be established between principal ideals in an integral domain by use of the next theorem.

Theorem 4.9 Let $J = (z)$ and $K = (z)$ be principal ideals in an integral domain D with zero z . Then $J = K$ if and only if their generators are associate elements in D .

This theorem can be used to compare all ideals not equal to (0) in the integral domain $[I;+;\cdot]$ of integers since all ideals in I are

principal ideals by Theorem 3.18. Since $18 = 9 \cdot 2$ and neither 9 nor 2 is a unit in I , Theorem 4.9 asserts that $(18) \neq (9)$ and $(18) \neq (2)$. On the other hand, since $6 = 6 \cdot (-1)$ and -1 is a unit in I , $(6) = (-6)$. Theorem 4.9 is more valuable when applying it to less familiar integral domains.

Example 108. Consider the integral domain $[S; +; \cdot]$ of Example 106.

Since $\begin{pmatrix} 2 & 1 \\ 5 & 2 \end{pmatrix} \cdot \begin{pmatrix} -2 & 1 \\ 5 & -2 \end{pmatrix} = \begin{pmatrix} -2 & 1 \\ 5 & -2 \end{pmatrix} \cdot \begin{pmatrix} 2 & 1 \\ 5 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$, the unity of S , $\begin{pmatrix} -2 & 1 \\ 5 & -2 \end{pmatrix}$

is a unit in S . $\begin{pmatrix} 1 & 1 \\ 5 & 1 \end{pmatrix}$ is not a unit in S since it has no multipli-

cative inverse in S . Notice that $\begin{pmatrix} -2 & 1 \\ 5 & -2 \end{pmatrix} \cdot \begin{pmatrix} 1 & 1 \\ 5 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 5 & 1 \end{pmatrix} \cdot \begin{pmatrix} -2 & 1 \\ 5 & -2 \end{pmatrix} =$

$\begin{pmatrix} 3 & -1 \\ -5 & 3 \end{pmatrix}$. Hence, by Theorem 4.9 the principal ideals generated by

$\begin{pmatrix} 1 & 1 \\ 5 & 1 \end{pmatrix}$ and $\begin{pmatrix} 3 & -1 \\ -5 & 3 \end{pmatrix}$ are equal while neither of these ideals is equal

to the principal ideal generated by $\begin{pmatrix} -2 & 1 \\ 5 & -2 \end{pmatrix}$.

A familiar division property of the integral domain $[I; +; \cdot]$ of integers is generalized to any integral domain by the next theorem.

Theorem 4.10 Let a , b , and p be elements in an integral domain D which is also a principal ideal ring. If p is a prime element in D such that $p|ab$, then $p|a$ or $p|b$.

Example 109 Since the integral domain $[A_5; +; \cdot]$ with the usual operations in 5-arithmetic is a commutative ring without divisors of zero, $A_5[x]$ is also free of divisors of zero by Theorem 3.30. Since $A_5[x]$ also has a unity, $1x^0$, and is commutative by Theorem 3.28, $A_5[x]$ is an integral domain. The only divisors of $3x^0+2x^1$ are units or associates of $3x^0+2x^1$ so that $3x^0+2x^1$ is a prime in

$A_5[x]$. $3x^0+2x^1$ divides the product $4x^0+3x^1+3x^2 = (2x^0+1x^1) \cdot (2x^0+3x^1)$, in fact, $3x^0+2x^1 = 4(2x^0+3x^1)$ so that $3x^0+2x^1$ divides one of the factors. The polynomial $4x^0+3x^1$ does not divide $4x^0+3x^1+3x^2$ since $4x^0+3x^1$, $2x^0+1x^1$, and $2x^0+3x^1$ are each primes in $A_5[x]$ and since $4x^0+3x^1$ does not divide either of these other primes.

Prime elements and prime ideals are related by the next theorem.

Theorem 4.11 If the unique factorization theorem holds in an integral domain D , then every prime element in D generates a prime ideal.

This theorem applies to the integral domain $[I; +; \cdot]$ of integers but Theorem 3.18 and Theorem 3.20 together imply even a stronger result. All ideals in I are principal and an ideal in I is prime if and only if its generator is a prime in I .

The integral domain $A_5[x]$ of Example 109 is a Euclidean ring under the degree mapping (see Example 95). By Theorem 4.8, $A_5[x]$ has unique factorization. Hence, the prime $2x^0+1x^1$ generates a prime ideal in $A_5[x]$. Notice that the ideal generated by $4x^0$ is also a prime ideal in $A_5[x]$ although $(4x^0) \cdot (4x^0) = 1x^0$, the unity of $A_5[x]$, so that $4x^0$ is a unit, not a prime in $A_5[x]$.

The greatest common divisor concept for the ring of integers can be generalized for any Euclidean ring.

Definition 4.9 Let R be a Euclidean ring with valuation mapping θ . Let $a, b, c \in R$ such that $b \neq z$, the zero of R . Then $d \in R$ is called a greatest common divisor of a and b if:

- (i) d/a and d/b and
- (ii) whenever c/a and c/b , then $c\theta \leq d\theta$.

Example 110 Consider the Euclidean ring $[T;+;\cdot]$ of Example 105.

$\langle 1,0 \rangle$ is the greatest common divisor of $\langle 1,0 \rangle$ and $\langle 1,1 \rangle$ since $\langle 1,0 \rangle$ and $\langle 1,1 \rangle$ are the only common divisors in this case and $\langle 1,1 \rangle \beta = 0 < 1 = \langle 1,0 \rangle \beta$. Similarly, the greatest common divisor of $\langle 0,1 \rangle$ and $\langle 1,1 \rangle$ is $\langle 0,1 \rangle$. For the pair of elements $\langle 0,1 \rangle$ and $\langle 1,0 \rangle$ and the pair of elements $\langle 1,1 \rangle$ and $\langle 0,0 \rangle$, $\langle 1,1 \rangle$ is the only common divisor so that $\langle 1,1 \rangle$ is the greatest common divisor. $\langle 1,0 \rangle$ and $\langle 0,1 \rangle$ are each greatest common divisors of the pair of elements $\langle 1,1 \rangle$ and $\langle 1,1 \rangle$ so that a greatest common divisor is not unique.

A greatest common divisor d of two elements $a, b \in R$, where R is a Euclidean ring, can always be written as a linear combination of a and b as in the next theorem. This property of a greatest common divisor is often stated when R is an integral domain as well as a Euclidean ring.

Theorem 4.10 Let D be an integral domain which is also a Euclidean ring and let $a \in D$ and nonzero $b \in D$. Let d be a greatest common divisor of a and b . Then there exist elements $x, y \in D$ such that $d = ax + by$.

As stated in the paragraph before this theorem, D need only be a Euclidean ring in order for a greatest common divisor to have the representation given in the theorem. One can show that a greatest common divisor of two elements of the Euclidean ring $[T;+;\cdot]$ of Example 105 can always be represented in the form given in Theorem 4.10 even though $[T;+;\cdot]$ is not an integral domain. The theorem is, of course, valid if the additional hypothesis is satisfied.

Example 111 $A_5[x]$ is an integral domain by Example 109 and is a Euclidean ring under the degree mapping by Example 95. Hence,

$A_5[x]$ satisfies the hypothesis for D of Theorem 4.10. $2x^0+3x^1$ is a greatest common divisor of the polynomials $f(x) = 2x^0+3x^1+4x^2+1x^3$ and $g(x) = 3x^1+2x^2$. One representation of $2x^0+3x^1$ satisfying Theorem 4.10 is the following: $2x^0+3x^1 = [(2x^0+3x^1+4x^2+1x^3) \cdot 1x^0] + [(3x^1+2x^2) \cdot 2x^1]$. A monic greatest common divisor of $f(x)$ and $g(x)$ is $4x^0+1x^1$ and $4x^0+1x^1 = [(2x^0+3x^1+4x^2+1x^3) \cdot 2x^0] + [(3x^1+2x^2) \cdot 1x^1]$.

Fields

Definition 4.11. A ring whose nonzero elements form an abelian multiplicative group is called a field.

The ring $[I; +; \cdot]$ of integers is not a field since the multiplicative inverse of any integer other than 1 and -1 does not exist in I .

If the nonzero elements of a ring R form a multiplicative group, then R is called a division ring or shew field. Notice that a division ring is a field only if multiplication is commutative. Hence, a field is a special type of division ring.

Example 112. The ring $[A_3; +; \cdot]$ with the usual operations in 3-arithmetic is a field. Each nonzero element of A_3 is its own multiplicative inverse and multiplication is commutative. Notice that A_3 is also a division ring.

Theorem 4.12. A field is necessarily an integral domain.

This theorem formally acknowledges that a field is a special integral domain. Some of the examples of integral domains given previously are fields.

The characteristic of a field F is the characteristic of the ring F . Since every field is an integral domain, Theorem 4.6 can be stated in terms of a field.

Theorem 4.13 The characteristic of a field is either zero or a positive prime integer.

The characteristic of the field $[A_3; +; \cdot]$ of Example 112 is the prime integer 3.

In grade school arithmetic students study the set Q of all numbers of the form $\frac{a}{b}$ where $a, b \in I$, the set of integers, and $b \neq 0$. Addition $+$ and multiplication \cdot on Q are defined by $\frac{a}{b} + \frac{c}{d} = \frac{(a \cdot d) + (b \cdot c)}{b \cdot d}$ and $\frac{a}{b} \cdot \frac{c}{d} = \frac{a \cdot c}{b \cdot d}$, respectively, for $\frac{a}{b}, \frac{c}{d} \in Q$ where $+$ and \cdot on the right side of each equation are ordinary addition and multiplication, respectively, in the ring $[I; +; \cdot]$ of integers. The set Q under these two operations is a field known as the field of rational numbers. Q has characteristic zero.

As mentioned above, some of the examples of integral domains given previously are fields. The next theorem provides an easy way to recognize which of those examples of integral domains are fields; none of those examples of integral domains which are of infinite order are fields.

Theorem 4.14 Every integral domain having a finite number of elements is a field.

Example 113 Let T be the set of all 2×2 matrices of the form

$$\begin{pmatrix} a & b \\ 2b & a \end{pmatrix} \text{ where } a \text{ and } b \text{ are elements of the field } [A_3; +; \cdot] \text{ of Example}$$

112. If addition $+$ and multiplication \cdot are defined on T as the usual matrix addition and multiplication in 3-arithmetic, then it

can be shown that $[T;+;\cdot]$ is an integral domain. Since the order of T is 9, Theorem 4.14 can be used to prove that $[T;+;\cdot]$ is a field. Hence, use of the theorem avoids the work of finding the multiplicative inverses of each of the elements of T .

The following theorem gives another interesting result relating integral domains and fields.

Theorem 4.15 For any integral domain D , there exists a field F such that a subset F' of F is isomorphic to D . (D is said to be imbedded in F .)

The integral domain of integers $[I;+;\cdot]$ can be imbedded in the field Q of rational numbers by the mapping θ from I into Q defined by $n\theta = \frac{n}{1} \in Q$ for every $n \in I$.

The next example illustrates that any finite integral domain D can be imbedded in D itself which is known to be a field by Theorem 4.14. The example also gives a more interesting imbedding map.

Example 114 The integral domain $[A_3;+;\cdot]$ with the usual operations in 3-arithmetic can be imbedded in the field $[A_3;+;\cdot]$ by the identity mapping α ; i.e., $a\alpha = a$ for every $a \in A_3$. The integral domain $[A_3;+;\cdot]$ can also be imbedded in the field $[T;+;\cdot]$ of Example 113. Define the mapping β from A_3 into T by $a\beta = \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix}$ for every $a \in A_3$. Then β is the imbedding map for A_3 in T .

Any subset S of a field F , which is itself a field with respect to the binary operations of F , is called a subfield of F . Thus, the field $[T;+;\cdot]$ of Example 113 has three subfields, namely $U = \left\{ \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \in T \right\}$,

$V = \left\{ \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} : a \in A_3 \right\}$, and T itself.

A subfield F' of a field F is called a proper subfield of F if $F' \neq F$ and $F' \neq \{z\}$, the field consisting of the zero of F only. If a field F has no proper subfields, then F is called a prime field. Thus, $V = \left\{ \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} : a \in A_3 \right\}$ is a proper subfield of $[T; +; \cdot]$ of Example 113 and T is not a prime field. The field $[A_3; +; \cdot]$ of Example 112 is a prime field.

Theorem 4.16 Let F be a prime field. If F has characteristic zero, then F is isomorphic to the field Q of rational numbers. If the characteristic of F is the prime p , then F is isomorphic to $I/(p)$, where I is the ring of integers.

The next example illustrates the second half of Theorem 4.16.

Example 115 Consider the field $[A_5; +; \cdot]$ with the usual operations in 5-arithmetic. If the distinct cosets of $I/(5)$ are represented by $(5)+0$, $(5)+1$, $(5)+2$, $(5)+3$, and $(5)+4$, where $[I; +; \cdot]$ is the ring of integers, then the mapping α defined from A_5 into $I/(5)$ by $\alpha a = (5)+a$ for each $a \in A_5$ is an isomorphism between A_5 and $I/(5)$.

A result for maximal ideals, similar to that stated in Theorem 4.3 for prime ideals, is given next.

Theorem 4.17 If N is an ideal in a commutative ring R with unity, then the quotient ring R/N is a field if and only if N is a maximal ideal in R .

In Example 102, N is a maximal ideal in I while M is not a maximal ideal. Hence, I/N is a field while I/M is not a field. The rings

$A_{12}/(2)$ and $A_{12}/(3)$, in Example 103, are fields since (2) and (3) are maximal ideals in A_{12} . Hence, the quotient rings in Example 103 which are integral domains are also fields but, recalling Theorem 4.14, this is not surprising.

Polynomials Over a Field

In this section ideas introduced in Chapter III for polynomials in an indeterminant x over a ring R are extended to polynomials over a field F .

The reader should review the definitions, theorems, and notation introduced for the study of polynomial rings in Chapter III.

Definition 4.18 A mapping α from a ring R into R is called a polynomial function if there is a polynomial $f(x) = \sum a_k x^k$ (only a finite number of the a_k are nonzero in R) in the polynomial ring $R[x]$ such that, for any $b \in R$, $b\alpha = a_0 b^0 + a_1 b^1 + a_2 b^2 + \dots = \sum a_k b^k$ ($+$ denotes addition in R and $a_k b^k$ means $a_k \cdot b^k$ where \cdot denotes multiplication in R).

Every polynomial $g(x)$ in the polynomial ring $R[x]$ can be associated with a polynomial function from the ring R into R . The polynomial function which is associated with the polynomial $g(x) \in R[x]$ will be denoted g . Hence, the polynomial function f from the ring R into R is the mapping defined by $f(b) = a_0 b^0 + a_1 b^1 + a_2 b^2 + \dots = \sum a_k b^k$ for each $b \in R$ where $f(x) = \sum a_k x^k \in R[x]$.

Some customary simplifying notations will be used in referring to polynomials over a field F . In particular, $a_0 x^0$ will be denoted a_0 , $a_1 x^1$ will be denoted $a_1 x$, and if u is the unity of F , then $u x^k$ will be denoted x^k . Also, $ax - b$ will denote $(-b) + ax$ where $-b$ is the additive

inverse of b in F .

Theorem 4.19 (Remainder Theorem) Let F be a field and let $b \in F$. If $f(x), (x-b) \in F[x]$, the remainder when $f(x)$ is divided by $x-b$ is $f(b)$.

Example 116 Let $f(x) = 2+3x^2+4x^3$ and $x-2$ be polynomials in $A_5[x]$ where $[A_5; +; \cdot]$ is the field with the usual operations in 5-arithmetic. Then $x-2 = 3+x$ and $f(x) = [(2+x+4x^2) \cdot (x-2)]+1$, i.e., the remainder when $f(x)$ is divided by $x-2$ is 1. $f(2) = 2+[3 \cdot (2)^2]+[4 \cdot (2)^3] = 2+2+2 = 1$ so that $f(2) = 1$ is the remainder when $f(x)$ is divided by $x-2$.

If F is a field and $f(x), g(x), h(x) \in F[x]$ such that $f(x) = g(x) \cdot h(x)$, then $g(x)$ (also $h(x)$) is a factor of $f(x)$. If a is an element of F such that $f(a) = z$, the zero of F , then a is called a zero of $f(x)$. Hence, common terminology is employed for polynomials over any field.

Theorem 4.20 (Factor Theorem) Let F be a field. If $f(x) \in F[x]$ and $b \in F$, then $x-b$ is a factor of $f(x)$ if and only if b is a zero of $f(x)$.

In Example 116, $x-2$ was found to not be a factor of $f(x)$ since the remainder is $1 = f(2) \neq 0$ when $f(x)$ is divided by $x-2$. Theorem 4.20 can be used to find all factors of degree 1 of any polynomial.

Example 117 For the polynomial $f(x) = 2+3x^2+4x^3 \in A_5[x]$ discussed in Example 116, $f(0) = 2$, $f(1) = 4$, $f(2) = 1$, $f(3) = 2$, and $f(4) = 1$ so that $f(a) \neq 0$ for any $a \in A_5$. Hence, $f(x)$ has no zeros and no factors of degree one. Notice that checking whether $1+2x$, for example, is a factor of $f(x)$ is equivalent to checking if $x-2$ is a

factor since $3(1+2x) = 3+x = (-2)+x = x-2$ in $A_5[x]$.

$g(x) = 4+2x+x^2+x^3+4x^4 \in A_5[x]$ has one zero, 3, since $g(3) = 0$ and $g(x) = f(x) \cdot (2+x)$.

Theorem 4.21 Let F be a field and $f(x) \in F[x]$ have degree $n > 0$ and leading coefficient a . If $b_1, b_2, \dots, b_n \in F$ are n distinct zeros of $f(x)$, then $f(x) = a(x-b_1)(x-b_2)\cdots(x-b_n)$.

$f(x)$ in Example 117 is of degree 3 but has no zeros so that $f(x)$ cannot be represented in the form of Theorem 4.21. An example of when this theorem applies is given next.

Example 118 Consider $A_{11}[x]$ where $[A_{11}; +; \cdot]$ is the field with usual operations in 11-arithmetic. Let $f(x) = 2x+9x^2+10x^3+3x^4$. $f(x)$ is of degree 4 with leading coefficient 3. $f(0) = 0$, $f(7) = 0$, $f(9) = 0$, and $f(10) = 0$ so that 0, 7, 9, and 10 are 4 distinct zeros of $f(x)$. Hence, $f(x) = 3(x-0)(x-7)(x-9)(x-10)$.

In Example 118, $f(x)$ was of degree 4 and had 4 distinct zeros. Two examples of polynomials which have fewer distinct zeros than their degrees are given in Example 117. The next theorem sets a maximum for the number of distinct zeros of a polynomial.

Theorem 4.22 Let F be a field. Every polynomial $f(x) \in F[x]$ of degree $n > 0$ has at most n distinct zeros in F .

Example 119 The polynomial $h(x) = 2+5x^3 \in A_{11}[x]$ of Example 118 has at most 3 distinct zeros. However, $h(a) \neq 0$ for any $a \in A_{11}$ except $a = 5$. Hence, 5 is the only zero. Also $k(x) = 10x+x^2$ has at most 2 zeros and since $k(0) = k(1) = 0$, Theorem 4.22 implies

that no other distinct zeros exist for $k(x)$.

If F is a finite field, then a limit, other than the one given in Theorem 4.22, exists for the number of distinct zeros of a polynomial. For example, any polynomial in $A_3[x]$, where $[A_3; +; \cdot]$ is the field with usual operations in 3-arithmetic, has at most 3 distinct zeros since only 3 distinct elements exist in A_3 .

The last theorem considered in this dissertation is particularly interesting because it points up a difference between the study of polynomials over a finite field and the study of polynomials over the real number field studied in college algebra.

Theorem 4.23 Let $f(x)$ and $g(x)$ be polynomials over a field F with the property that $f(a) = g(a)$ for every $a \in F$. If the number of elements in F exceeds the degrees of both $f(x)$ and $g(x)$, then necessarily $f(x) = g(x)$.

If $f(a) = g(a)$ for every real number a , where $f(x)$ and $g(x)$ are two polynomials over the real field, then $f(x) = g(x)$ which means that the coefficients of corresponding powers of x are identical. This is not the case for finite fields.

Example 120 Let $f(x) = 2x$ and $g(x) = 2x^5$ be two polynomials in $A_5[x]$ where $[A_5; +; \cdot]$ is the field with the usual operations in 5-arithmetic. The polynomial $f(x) \neq g(x)$ since corresponding coefficients are not identical. Notice, however, that $f(a) = g(a)$ for every $a \in A_5$ so that the polynomial functions f and g describe the same mapping from A_5 into A_5 . Theorem 4.23 does not imply that $f(x) = g(x)$ since the degree of $g(x)$ is 5 which is the same as the

number of elements in A_5 . Using Theorem 4.23, one is assured that if $h(x) \in A_5[x]$, the degree of $h(x)$ is less than 5, and $h(a) = f(a)$ for every $a \in A_5$, then $f(x) = h(x)$, i.e., $h(x) = 2x$.

CHAPTER V

SUMMARY

In this dissertation, topics in modern algebra were illustrated using number theoretic systems. The number theoretic systems used in examples are discussed in current junior and senior high school mathematics courses. However, if the reader is not knowledgeable of these systems, little time is necessary to develop an understanding sufficient to appreciate the examples. It is hoped that these examples will deepen the reader's understanding and appreciation of modern algebra.

Consideration was given to the theory of groups, rings, ideals, integral domains, and fields. In Chapter I the procedure used by the author, the content of the dissertation, and its significance were discussed. In Chapter II groups, subgroups, and homomorphisms and isomorphisms between groups were considered. Rings, subrings, ring homomorphisms and isomorphisms, ideals, and special types of rings were investigated in Chapter III. In Chapter IV integral domains, subdomains, and fields were considered. Throughout the dissertation, reference was made to previously presented definitions, theorems, and examples to avoid repetition as well as to recognize the relationships between the topics discussed.

The techniques and systems used in this dissertation could be employed to illustrate topics which were excluded but which are found in textbooks for introductory modern algebra as well as topics included in

additional modern algebra courses.

An approach similar to that used by the author might be employed to develop reference material for other mathematics courses such as geometry and analysis courses. Elementary number theory seems to be particularly useful as a source of examples. Barnett [4] expressed his interest in the theory of numbers when he quoted from the essay "A Mathematician's Apology" by G. H. Hardy:

"The elementary theory of numbers should be one of the very best subjects for early mathematical instruction. It demands very little previous knowledge; its subject matter is tangible and familiar; the processes of reasoning which it employs are simple, general and few; and it is unique among the mathematical sciences in its appeal to natural human curiosity. A month's intelligent instruction in the theory of numbers ought to be twice as instructive, twice as useful, and at least ten times as entertaining as the same amount of Calculus for Engineers."

The author has undoubtedly benefited from the experience of writing this dissertation. It is hoped that others will benefit from reading it.

SELECTED BIBLIOGRAPHY

- [1] Ayres, Frank Jr. Schaum's Outline of Theory and Problems of Modern Algebra. New York: Schaum Publishing Company, 1965.
- [2] Ball, Richard W. Principals of Abstract Algebra. New York: Holt, Rinehart and Winston, 1963.
- [3] Barnes, Wilfred E. Introduction to Abstract Algebra. Boston: D. C. Heath and Company, 1963.
- [4] Barnett, I. A. "The Theory of Numbers as a Required Course in the College Curriculum for Majors." The American Mathematical Monthly, Vol. 73 (November, 1966), 1002-4.
- [5] Birkhoff, Garrett, and Saunders MacLane. A Survey of Modern Algebra, 3rd ed. New York: MacMillan Company, 1965.
- [6] Committee on the Undergraduate Program in Mathematics. A General Curriculum in Mathematics for Colleges. Buffalo: Mathematical Association of America, January, 1965.
- [7] Committee on the Undergraduate Program in Mathematics. Recommendations for the Training of Teachers of Mathematics, Revised. Buffalo: Mathematical Association of America, December, 1966.
- [8] Dean, Richard A. Elements of Abstract Algebra. New York: John Wiley and Sons, Inc., 1966.
- [9] Deskins, W. E. Abstract Algebra. New York: MacMillan Company, 1964.
- [10] Dolciani, Mary P., Simon L. Berman, and Julius Freilich. Modern Algebra-Structure and Method Book 1. Ed. Albert E. Meder, Jr. Boston: Houghton Mifflin Company, 1965.
- [11] Dynkin, E. B., and V. A. Uspenskii. Problems in the Theory of Numbers. Boston: D. C. Heath and Company, 1963.
- [12] Herstein, I. N. Topics in Algebra. New York: Blaisdell Publishing Company, 1964.
- [13] Horyna, Sharon K. "A Dictionary of Rings" (unpub. M.S. report, Oklahoma State University, 1966).
- [14] McCoy, Neal H. Introduction to Modern Algebra. Boston: Allyn and Bacon, Inc., 1960.

- [15] McCoy, Neal H. The Theory of Rings. New York: MacMillan Company, 1964.
- [16] Miller, Kenneth S. Elements of Modern Abstract Algebra. New York: Harper and Row Publishers, Inc., 1958.
- [17] Moore, John T. Elements of Abstract Algebra. New York: MacMillan Company, 1962.
- [18] Moore, John T. Elements of Abstract Algebra, 2nd ed. New York: MacMillan Company, 1967.
- [19] Polites, George W. An Introduction to the Theory of Groups. Scranton: International Textbook Company, 1968.
- [20] Rosskopf, Myron F., Robert L. Morton, Joseph R. Hooten, and Harry Sitomer. Modern Mathematics for Junior High School Book 2. Morristown: Silver Burdett Company, 1961.
- [21] Stewart, B. M. Theory of Numbers, 2nd ed. New York: MacMillan Company, 1964.
- [22] VanEugen, Henry, Maurice L. Hartung, Harold C. Trimble, Emil J. Berger, and Ray W. Cleveland. Seeing Through Mathematics Book 1. Chicago: Scott, Foresman and Company, 1962.
- [23] VanEugen, Henry, Maurice L. Hartung, Harold C. Trimble, Emil J. Berger, and Ray W. Cleveland. Seeing Through Mathematics Book 2. Chicago: Scott, Foresman and Company, 1964.
- [24] Whitesitt, J. Eldon. Principles of Modern Algebra. Reading: Addison-Wesley Publishing Company, Inc., 1964.

VITA

August Wesley Waltmann

Candidate for the Degree of

Doctor of Education

Dissertation: MODERN ALGEBRA ILLUSTRATED BY NUMBER THEORETIC EXAMPLES

Major Field: Higher Education Minor Field: Mathematics

Biographical:

Personal Data: Born in Cedar Falls, Iowa, February 22, 1942, the son of Leo H. and Alma L. Waltmann.

Education: Graduated from Hudson High School, Hudson, Iowa, in May, 1960; received the Bachelor of Arts degree from Wartburg College, Waverly, Iowa, in May, 1964, with a major in Mathematics; received the Master of Arts degree from Kansas State University, Manhattan, Kansas, in June, 1966, with a major in Mathematics; completed requirements for the Doctor of Education degree at Oklahoma State University in May, 1969.

Professional Experience: Taught as a graduate assistant in Mathematics at Kansas State University, 1964-66; taught as a graduate assistant in Mathematics at Oklahoma State University, 1966-69.

Professional Organizations: Member of the Mathematical Association of America, Pi Mu Epsilon, and Phi Delta Kappa.