APPENDIX B

Algebraic Systems

B.1 INTRODUCTION

This Appendix investigates some of the major algebraic systems in mathematics: semigroups, groups, rings, and fields. We also define the notion of a homomorphism and the notion of a quotient structure. We begin with the formal definition of an operation, and discuss various types of operations.

B.2 OPERATIONS

The reader is familiar with the operations of addition and multiplication of numbers, union and intersection of sets, and the composition of functions. These operations are denoted as follows:

$$a + b = c, \quad a \cdot b = c, \quad A \cup B = C, \quad A \cap B = C, \quad g \circ f = h.$$

In each situation, an element (c, C, or h) is assigned to an original pair of elements. We make this notion precise.

Definition B.1: Let S be a nonempty set. An *operation* on S is a function $*$ from $S \times S$ into S. In such a case, instead of $*(a, b)$, we usually write

$$a * b \quad \text{or sometimes} \quad ab$$

The set S and an operation $*$ on S is denoted by $(S, *)$ or simply S when the operation is understood.

Remark: An operation $*$ from $S \times S$ into S is sometimes called a *binary operation*. A *unary* operation is a function from S into S. For example, the absolute value $|n|$ of an integer n is a unary operation on $\mathbf{Z}$, and the complement A^C of a set A is a unary operation on the power set $P(X)$ of a set X. A *ternary* (3-ary) operation is a function from $S \times S \times S$ into S. More generally, an n-ary operation is a function from $S \times S \times \cdots \times S$ (n factors) into S. Unless otherwise stated, the word operation shall mean binary operation. We will also assume that our underlying set S is nonempty.

Suppose S is a finite set. Then an operation $*$ on S can be presented by its operation (multiplication) table where the entry in the row labeled a and the column labeled b is $a * b$.

Suppose S is a set with an operation $*$, and suppose A is a subset of S. Then A is said to be *closed under* $*$ if $a * b$ belongs to A for any elements a and b in A.

EXAMPLE B.1 Consider the set **N** of positive integers.

(a) Addition ($+$) and multiplication ($\times$) are operations on **N**. However, subtraction ($-$) and division ($/$) are not operations on **N** since the difference and the quotient of positive integers need not be positive integers. For example, $2 - 9$, and $7/3$ are not positive integers.

(b) Let A and B denote, respectively, the set of even and odd positive integers. Then A is closed under addition and multiplication since the sum and product of any even numbers are even. On the other hand, B is closed under multiplication but not addition since, for example, $3 + 5 = 8$ is even.

EXAMPLE B.2 Let $S = \{a, b, c, d\}$. The tables in Fig. B-1 define operations $*$ and $\cdot$ on S. Note that $*$ can be defined by the following operation where x and y are any elements of S:

$$x * y = x$$

$*$	a	b	c	d
a	a	a	a	a
b	b	b	b	b
c	c	c	c	c
d	d	d	d	d

(a)

$\cdot$	a	b	c	d
a	a	b	c	d
b	b	a	a	b
c	c	b	a	a
d	d	a	a	a

(b)

Fig. B-1

Next we list a number of important properties of our operations.

Associative Law:

An operation $*$ on a set S is said to be *associative* or to satisfy the *Associative Law* if, for any elements a, b, c in S, we have

$$(a * b) * c = a * (b * c)$$

Generally speaking, if an operation is not associative, then there may be many ways to form a product. For example, the following shows five ways to form the product *abcd*:

$$((ab)c)d, \quad (ab)(cd), \quad (a(bc))d, \quad a((bc)d), \quad a(b(cd))$$

If the operation is associative, then the following theorem (proved in Problem B.4) applies.

Theorem B.1: Suppose $*$ is an associative operation on a set S. Then any product $a_1 * a_2 * \cdots * a_n$ requires no parentheses, that is, all possible products are equal.

Commutative Law:

An operation $*$ on a set S is said to be *commutative* or satisfy the *Commutative Law* if, for any elements a, b in S,

$$a * b = b * a$$

EXAMPLE B.3

(a) Consider the set **Z** of integers. Addition and multiplication of integers are associative and commutative. On the other hand, subtraction is nonassociative. For example,

$$(8 - 4) - 3 = 1 \quad \text{but} \quad 8 - (4 - 3) = 7$$

Moreover, subtraction is not commutative since, for example, $3 - 7 \neq 7 - 3$.

(b) Consider the operation of matrix multiplication on the set M of n-square matrices. One can prove that matrix multiplication is associative. On the other hand, matrix multiplication is not commutative. For example,

$$\begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix}\begin{bmatrix} 5 & 6 \\ 0 & -2 \end{bmatrix} = \begin{bmatrix} 5 & 2 \\ 15 & 10 \end{bmatrix} \quad \text{but} \quad \begin{bmatrix} 5 & 6 \\ 0 & -2 \end{bmatrix}\begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix} = \begin{bmatrix} 23 & 34 \\ -6 & -8 \end{bmatrix}$$

Identity Element:

Consider an operation $*$ on a set S. An element e in S is called an *identity* element for $*$ if, for any element a in S,

$$a * e = e * a = a$$

More generally, an element e is called a *left identity* or a *right identity* according as $e * a = a$ or $a * e = a$ where a is any element in S. The following theorem applies.

Theorem B.2: Suppose e is a left identity and f is a right identity for an operation on a set S. Then $e = f$

The proof is very simple. Since e is a left identity, $ef = f$; but since f is a right identity, $ef = e$. Thus $e = f$. This theorem tells us, in particular, that an identity element is unique, and that if an operation has more than one left identity then it has no right identity, and vice versa.

Inverses:

Suppose an operation $*$ on a set S does have an identity element e. The *inverse* of an element a in S is an element b such that

$$a * b = b * a = e$$

If the operation is associative, then the inverse of a, if it exists, is unique (Problem B.2). Observe that if b is the inverse of a, then a is the inverse of b. Thus the inverse is a symmetric relation, and we can say that the elements a and b are inverses.

Notation: If the operation on S is denoted by $a * b$, $a \times b$, $a \cdot b$, or ab, then S is said to be written *multiplicatively* and the inverse of an element $a \in S$ is usually denoted by a^{-1}. Sometimes, when S is commutative, the operation is denoted by $+$ and then S is said to be written *additively*. In such a case, the identity element is usually denoted by 0 and it is called the *zero* element; and the inverse is denoted by $-a$ and it is called the *negative* of a.

EXAMPLE B.4 Consider the rational numbers $\mathbf{Q}$. Under addition, 0 is the identity element, and -3 and 3 are (additive) inverses since

$$(-3) + 3 = 3 + (-3) = 0$$

On the other hand, under multiplication, 1 is the identity element, and -3 and $-1/3$ are (multiplicative) inverses since

$$(-3)(-1/3) = (-1/3)(-3) = 1$$

Note 0 has no multiplicative inverse.

Cancellation Laws:

An operation $*$ on a set S is said to satisfy the *left cancellation law* or the *right cancellation law* according as:

$$a * b = a * c \text{ implies } b = c \quad \text{or} \quad b * a = c * a \text{ implies } b = c$$

Addition and subtraction of integers in $\mathbf{Z}$ and multiplication of nonzero integers in $\mathbf{Z}$ do satisfy both the left and right cancellation laws. On the other hand, matrix multiplication does not satisfy the cancellation laws. For example, suppose

$$A = \begin{bmatrix} 1 & 1 \\ 0 & 0 \end{bmatrix}, \quad B = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}, \quad C = \begin{bmatrix} 0 & -3 \\ 1 & 5 \end{bmatrix}, \quad D = \begin{bmatrix} 1 & 2 \\ 0 & 0 \end{bmatrix}$$

Then $AB = AC = D$, but $B \neq C$.

B.3 SEMIGROUPS

Let S be a nonempty set with an operation. Then S is called a *semigroup* if the operation is associative. If the operation also has an identity element, then S is called a *monoid*.

EXAMPLE B.5

(a) Consider the positive integers $\mathbf{N}$. Then $(\mathbf{N}, +)$ and $(\mathbf{N}, \times)$ are semigroups since addition and multiplication on $\mathbf{N}$ are associative. In particular, $(\mathbf{N}, \times)$ is a monoid since it has the identity element 1. However, $(\mathbf{N}, +)$ is not a monoid since addition in $\mathbf{N}$ has no zero element.

(b) Let S be a finite set, and let $F(S)$ be the collection of all functions $f\colon S \to S$ under the operation of composition of functions. Since the composition of functions is associative, $F(S)$ is a semigroup. In fact, $F(S)$ is a monoid since the identity function is an identity element for $F(S)$.

(c) Let $S = \{a, b, c, d\}$. The multiplication tables in Fig. B-1 define operations $*$ and $\cdot$ on S. Note that $*$ can be defined by the formula $x * y = x$ for any x and y in S. Hence

$$(x * y) * z = x * z = x \quad \text{and} \quad x * (y * z) = x * y = x$$

Therefore, $*$ is associative and hence $(S, *)$ is a semigroup. On the other hand, $\cdot$ is not associative since, for example,

$$(b \cdot c) \cdot c = a \cdot c = c \quad \text{but} \quad b \cdot (c \cdot c) = b \cdot a = b$$

Thus $(S, \cdot)$ is not a semigroup.

Free Semigroup, Free Monoid

Let A be a nonempty set. A *word* w on A is a finite sequence of its elements. For example, the following are words on $A = \{a, b, c\}$:

$$u = ababbbb = abab^4 \quad \text{and} \quad v = baccaaaa = bac^2a^4$$

(We write a^2 for aa, a^3 for aaa, and so on.) The *length* of a word w, denoted by $l(w)$, is the number of elements in w. Thus $l(u) = 7$ and $l(v) = 8$.

The concatenation of words u and v on a set A, written $u * v$ or uv, is the word obtained by writing down the elements of u followed by the elements of v. For example,

$$uv = (abab^4)(bac^2a^4) = abab^5c^2a^4$$

Now let $F = F(A)$ denote the collection of all words on A under the operation of concatenation. Clearly, for any words u, v, w, the words $(uv)w$ and $u(vw)$ are identical; they simply consist of the elements of u, v, w written down one after the other. Thus F is a semigroup; it is called the *free semigroup* on A, and the elements of A are called the *generators* of F.

The empty sequence, denoted by λ, is also considered as a word on A. However, we do not assume that λ belongs to the free semigroup $F = F(A)$. The set of all words on A including λ is frequently denoted by A^*. Thus A^* is a monoid under concatenation; it is called the *free monoid* on A.

Subsemigroups

Let A be a nonempty subset of a semigroup S. Then A is called a subsemigroup of S if A itself is a semigroup with respect to the operation on S. Since the elements of A are also elements of S, the Associative Law automatically holds for the elements of A. Therefore, A is a subsemigroup of S if and only if A is closed under the operation on S.

EXAMPLE B.6

(a) Let A and B denote, respectively, the set of even and odd positive integers. Then $(A, \times)$ and $(B, \times)$ are subsemigroups of $(\mathbf{N}, \times)$ since A and B are closed under multiplication. On the other hand, $(A, +)$ is a subsemigroup of $(\mathbf{N}, +)$ since A is closed under addition, but $(B, +)$ is not a subsemigroup of $(\mathbf{N}, +)$ since B is not closed under addition.

(b) Let F be the free semigroup on the set $A = \{a, b\}$. Let H consist of all even words, that is, words with even length. The concatenation of two such words is also even. Thus H is a subsemigroup of F.

Congruence Relations and Quotient Structures

Let S be a semigroup and let $\sim$ be an equivalence relation on S. Recall that the equivalence relation $\sim$ induces a partition of S into equivalence classes. Also, $[a]$ denotes the equivalence class containing the element $a \in S$, and that the collection of equivalence classes is denoted by $S/\sim$.

Suppose that the equivalence relation $\sim$ on S has the following property:

$$\boxed{\text{If } a \sim a' \text{ and } b \sim b', \text{ then } ab \sim a'b'.}$$

Then $\sim$ is called a *congruence relation* on S. Furthermore, we can now define an operation on the equivalence classes by

$$[a] * [b] = [a * b] \quad \text{or, simply,} \quad [a]\,[b] = [ab]$$

Furthermore, this operation on $S/\sim$ is associative; hence $S/\sim$ is a semigroup. We state this result formally.

Theorem B.3: Let $\sim$ be a congruence relation on a semigroup S. Then $S/\sim$, the equivalence classes under $\sim$, form a semigroup under the operation $[a]\,[b] = [ab]$.

This semigroup $S/\sim$ is called the quotient of S by $\sim$.

EXAMPLE B.7

(a) Let F be the free semigroup on a set A. Define $u \sim u'$ if u and u' have the same length. Then $\sim$ is an equivalence relation on F. Furthermore, suppose $u \sim u'$ and $v \sim v'$, say,

$$l(u) = l(u') = m \quad \text{and} \quad l(v) = l(v') = n$$

Then $l(uv) = l(u'v') = m + n$, and so $uv \sim u'v'$. Thus $\sim$ is a congruence relation on F.

(b) Consider the integers $\mathbf{Z}$ and a positive integer $m > 1$. Recall (Section 11.8) that we say that a is congruent to b modulo m, written

$$a \equiv b \pmod{m}$$

if m divides the difference $a - b$. Theorem 11.21 states that this relation is an equivalence relation on $\mathbf{Z}$. Furthermore, Theorem 11.22 tells us that if $a \equiv c \pmod{m}$ and $b \equiv d \pmod{m}$ then:

$$a + b \equiv c + d \pmod{m} \quad \text{and} \quad ab \equiv cd \pmod{m}$$

In other words, this relation is a congruence relation on $\mathbf{Z}$.

Homomorphism of Semigroups

Consider two semigroups $(S, *)$ and $(S', *')$. A function $f\colon S \to S'$ is called a *semigroup homomorphism* or, simply, a *homomorphism* if

$$f(a * b) = f(a) *' f(b) \quad \text{or, simply} \quad f(ab) = f(a)f(b)$$

Suppose f is also one-to-one and onto. Then f is called an *isomorphism* between S and S', and S and S′ are said to be *isomorphic* semigroups, written $S \cong S$.

EXAMPLE B.8

(a) Let M be the set of all 2×2 matrices with integer entries. The determinant of any matrix $A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$ is denoted and defined by $\det(A) = |A| = ad - bc$. One proves in Linear Algebra that the determinant is a *multiplicative function*, that is, for any matrices A and B,

$$\det(AB) = \det(A) \cdot \det(B)$$

Thus the determinant function is a semigroup homomorphism on $(M, \times)$, the matrices under matrix multiplication. On the other hand, the determinant function is not additive, that is, for some matrices,

$$\det(A + B) \neq \det(A) + \det(B)$$

Thus the determinant function is not a semigroup homomorphism on $(M, +)$.

(b) Figure B-2(a) gives the addition table for $\mathbf{Z_4}$, the integers modulo 4 under addition; and Fig. B-2(b) gives the multiplication table for $S = \{1, 3, 7, 9\}$ in $\mathbf{Z_{10}}$. (We note that S is a reduced residue system for the integers $\mathbf{Z}$ modulo 10.) Let $f\colon \mathbf{Z_4} \to S$ be defined by

$$f(0) = 1, \quad f(1) = 3, \quad f(2) = 9, \quad f(3) = 7$$

+	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

(a)

×	1	3	7	9
1	1	3	7	9
3	3	9	1	7
7	7	1	9	3
9	9	7	3	1

(b)

Fig. B-2

One can show that f is a homomorphism. Since f is also one-to-one and onto, f is an isomorphism. Thus $\mathbf{Z_4}$ and S are isomorphic semigroups.

(c) Let $\sim$ be a congruence relation on a semigroup S. Let $\phi\colon S \to S/\sim$ be the *natural mapping* from S into the factor semigroup $S/\sim$ defined by

$$\phi(a) = [a]$$

That is, each element a in S is assigned its equivalence class $[a]$. Then ϕ is a homomorphism since

$$\phi(ab) = [ab] = [a]\,[b] = \phi(a)\phi(b)$$

Fundamental Theorem of Semigroup Homomorphisms

Recall that the image of a function $f\colon S \to S'$, written $f(S)$ of Im f, consists of the images of the elements of S under f. Namely:

$$\text{Im } f = \{b \in S' \mid \text{there exists } a \in S \text{ for which } f(a) = b\}$$

The following theorem (proved in Problem B.5) is fundamental to semigroup theory.

Theorem B.4: Let $f : S \to S'$ be a semigroup homomorphism. Let $a \sim b$ if $f(a) = f(b)$. Then: (i) $\sim$ is a congruence relation on S. (ii) $S/\sim$ is isomorphic to $f(S)$.

EXAMPLE B.9

(a) Let F be the free semigroup on $A = \{a, b\}$. The function $f : F \to \mathbf{Z}$ defined by

$$f(u) = l(u)$$

is a homomorphism. Note $f(F) = \mathbf{N}$. Thus $F/\sim$ is isomorphic to $\mathbf{N}$.

(b) Let M be the set of 2×2 matrices with integer entries. Consider the determinant function det: $M \to \mathbf{Z}$. We note that the image of det is $\mathbf{Z}$. By Theorem B.4, $M/\sim$ is isomorphic to $\mathbf{Z}$.

Semigroup Products

Let $(S_1, *_1)$ and $(S_2, *_2)$ be semigroups. We form a new semigroup $S = S_1 \otimes S_2$, called the direct product of S_1 and S_2, as follows.

(1) The elements of S come from $S_1 \times S_2$, that is, are ordered pairs (a, b) where $a \in S_1$ and $b \in S_2$

(2) The operation $*$ in S is defined componentwise, that is,

$$(a, b) * (a', b') = (a *_1 a',\ b *_2 b') \quad \text{or simply} \quad (a, b)(a', b') = (aa', bb')$$

One can easily show (Problem B.3) that the above operation is associative.

B.4 GROUPS

Let G be a nonempty set with a binary operation (denoted by juxtaposition). Then G is called a *group* if the following axioms hold:

[$\mathbf{G_1}$] Associative Law: For any a, b, c in G, we have $(ab)c = a(bc)$.
[$\mathbf{G_2}$] Identity element: There exists an element e in G such that $ae = ea = a$ for every a in G.
[$\mathbf{G_3}$] Inverses: For each a in G, there exists an element a^{-1} in G (the *inverse* of a) such that

$$aa^{-1} = a^{-1}a = e$$

A group G is said to be *abelian* (or *commutative*) if $ab = ba$ for every $a, b \in G$, that is, if G satisfies the Commutative Law.

When the binary operation is denoted by juxtaposition as above, the group G is said to be written *multiplicatively*. Sometimes, when G is abelian, the binary operation is denoted by $+$ and G is said to be written *additively*. In such a case the identity element is denoted by 0 and it is called the *zero* element; and the inverse is denoted by $-a$ and it is called the *negative* of a.

The number of elements in a group G, denoted by $|G|$, is called the *order* of G. In particular, G is called a *finite group* if its order is finite.

Suppose A and B are subsets of a group G. Then we write:

$$AB = \{ab \mid a \in A,\ b \in B\} \quad \text{or} \quad A + B = \{a + b \mid a \in A,\ \ b \in B\}$$

EXAMPLE B.10

(a) The nonzero rational numbers $\mathbf{Q}\backslash\{0\}$ form an abelian group under multiplication. The number 1 is the identity element and q/p is the multiplicative inverse of the rational number p/q.

(b) Let S be the set of 2×2 matrices with rational entries under the operation of matrix multiplication. Then S is not a group since inverses do not always exist. However, let G be the subset of 2×2 matrices with a nonzero determinant. Then G is a group under matrix multiplication. The identity element is

$$I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \text{ and the inverse of } A = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \text{ is } A^{-1} = \begin{bmatrix} d/|A| & -b/|A| \\ -c/|A| & a/|A| \end{bmatrix}$$

This is an example of a nonabelian group since matrix multiplication is noncommutative.

(c) Recall that $\mathbf{Z}_m$ denotes the integers modulo m. $\mathbf{Z}_m$ is a group under addition, but it is not a group under multiplication. However, let $\mathbf{U}_m$ denote a reduced residue system modulo m which consists of those integers relatively prime to m. Then $\mathbf{U}_m$ is a group under multiplication (modulo m). Figure B-3 gives the multiplication table for $\mathbf{U}_{12} = \{1, 5, 7, 11\}$.

$\times$	1	5	7	11
1	1	5	7	11
5	5	1	11	7
7	7	11	1	5
11	11	7	5	1

Fig. B-3

	ε	σ_1	σ_2	σ_3	ϕ_1	ϕ_2
ε	ε	ϕ_1	σ_3	σ_3	ϕ_1	ϕ_2
σ_1	σ_1	ε	ϕ_1	ϕ_2	σ_2	σ_3
σ_2	σ_2	ϕ_2	ε	ϕ_1	σ_3	σ_1
σ_3	σ_3	ϕ_1	ϕ_2	ε	σ_1	σ_2
ϕ_1	ϕ_1	σ_3	σ_1	σ_2	ϕ_2	ε
ϕ_2	ϕ_2	σ_2	σ_3	σ_1	ε	ϕ_1

Fig. B-4

Symmetric Group S_n

A one-to-one mapping σ of the set $\{1, 2, \ldots, n\}$ onto itself is called a *permutation*. Such a permutation may be denoted as follows where $j_i = \sigma(i)$:

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & \cdots & n \\ j_1 & j_2 & j_3 & \cdots & j_n \end{pmatrix}$$

The set of all such permutations is denoted by S_n, and there are $n! = n(n-1) \cdot \ldots \cdot 2 \cdot 1$ of them. The composition and inverses of permutations in S_n belong to S_n, and the identity function ε belongs to S_n. Thus S_n forms a group under composition of functions called the *symmetric group of degree n*.

The symmetric group S_3 has $3! = 6$ elements as follows:

$$\varepsilon = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \quad \sigma_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, \quad \phi_1 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$$

$$\sigma_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \quad \sigma_3 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \quad \phi_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$$

The multiplication table of S_3 appears in Fig. B-4.

MAP(A), PERM(A), and AUT(A)

Let A be a nonempty set. The collection MAP(A) of all functions (mappings) $f: A \to A$ is a semigroup under composition of functions; it is not a group since some functions may have no inverses. However, the subsemigroup PERM(A) of all one-to-one correspondences of A with itself (called *permutations* of A) is a group under composition of functions.

Furthermore, suppose A contains some type of geometric or algebraic structure; for example, A may be the set of vertices of a graph, or A may be an ordered set or a semigroup. Then the set AUT(A) of all isomorphisms of A with itself (called *automorphisms* of A) is also a group under compositions of functions.

B.5 SUBGROUPS, NORMAL SUBGROUPS, AND HOMOMORPHISMS

Let H be a subset of a group G. Then H is called a *subgroup* of G if H itself is a group under the operation of G. Simple criteria to determine subgroups follow.

Proposition B.5: A subset H of a group G is a subgroup of G if:

(i) The identity element $e \in H$.
(ii) H is closed under the operation of G, i.e. if $a, b \in H$, then $ab \in H$.
(iii) H is closed under inverses, that is, if $a \in H$, then $a^{-1} \in H$.

Every group G has the subgroups $\{e\}$ and G itself. Any other subgroup of G is called a *nontrivial subgroup*.

Cosets

Suppose H is a subgroup of G and $a \in G$. Then the set

$$Ha = \{ha \mid h \in H\}$$

is called a *right coset* of H. (Analogously, aH is called a *left coset* of H.) We have the following important results (proved in Problems B.13 and B.15).

Theorem B.6: Let H be a subgroup of a group G. Then the right cosets Ha form a partition of G.

Theorem B.7 (Lagrange): Let H be a subgroup of a finite group G. Then the order of H divides the order of G.

The number of right cosets of H in G, called the index of H in G, is equal to the number of left cosets of H in G; and both numbers are equal to $|G|$ divided by $|H|$.

Normal Subgroups

The following definition applies.

Definition B.2: A subgroup H of G is a *normal* subgroup if $a^{-1}Ha \subseteq H$, for every $a \in G$, or, equivalently, if $aH = Ha$, i.e., if the right and left cosets coincide.

Note that every subgroup of an abelian group is normal.

The importance of normal subgroups comes from the following result (proved in Problem B.17).

Theorem B.8: Let H be a normal subgroup of a group G. Then the cosets of H form a group under coset multiplication:

$$(aH)(bH) = abH$$

This group is called the *quotient group* and is denoted by G/H.

Suppose the operation in G is addition or, in other words, G is written additively. Then the cosets of a subgroup H of G are of the form $a + H$. Moreover, if H is a normal subgroup of G, then the cosets form a group under coset addition, that is,

$$(a + H) + (b + H) = (a + b) + H$$

EXAMPLE B.11

(a) Consider the permutation group S_3 of degree 3 which is investigated above. The set $H = \{\varepsilon, \sigma_1\}$ is a subgroup of S_3. Its right and left cosets follow:

Right Cosets	**Left Cosets**
$H = \{\varepsilon, \sigma_1\}$	$H = \{\varepsilon, \sigma_1\}$
$H\phi_1 = \{\phi_1, \sigma_2\}$	$\phi_1 H = \{\phi_1, \sigma_3\}$
$H\phi_2 = \{\phi_2, \sigma_3\}$	$\phi_2 H = \{\phi_2, \sigma_2\}$

Observe that the right cosets and the left cosets are distinct; hence H is not a normal subgroup of S_3.

(b) Consider the group G of 2×2 matrices with rational entries and nonzero determinants. (See Example A.10.) Let H be the subset of G consisting of matrices whose upper-right entry is zero; that is, matrices of the form

$$\begin{bmatrix} a & 0 \\ c & d \end{bmatrix}$$

Then H is a subgroup of G since H is closed under multiplication and inverses and $I \in H$. However, H is not a normal subgroup since, for example, the following product does not belong to H:

$$\begin{bmatrix} 1 & 2 \\ 1 & 3 \end{bmatrix}^{-1} \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix} \begin{bmatrix} 1 & 2 \\ 1 & 3 \end{bmatrix} = \begin{bmatrix} -1 & -4 \\ 1 & 3 \end{bmatrix}$$

On the other hand, let K be the subset of G consisting of matrices with determinant 1. One can show that K is also a subgroup of G. Moreover, for any matrix X in G and any matrix A in K, we have

$$\det(X^{-1}AX) = 1$$

Hence $X^{-1}AX$ belongs to K, so K is a normal subgroup of G.

Integers Modulo *m*

Consider the group $\mathbf{Z}$ of integers under addition. Let H denote the multiples of 5, that is,

$$H = \{\ldots, -10, -5, 0, 5, 10, \ldots\}$$

Then H is a subgroup (necessarily normal) of $\mathbf{Z}$. The cosets of H in $\mathbf{Z}$ appear in Fig. B-5(a). By the above Theorem B.8, $\mathbf{Z}/H = \{0, 1, 2, 3, 4\}$ is a group under coset addition; its addition table appears in Fig. B-5(b).

This quotient group $\mathbf{Z}/H$ is referred to as the integers modulo 5 and it is frequently denoted by $\mathbf{Z_5}$. Analogously, for any positive integer n, there exists the quotient group $\mathbf{Z_n}$ called the *integers modulo n*.

$\bar{0} = 0 + H = H = \{..., -10, -5, 0, 5, 10, ...\}$
$\bar{1} = 1 + H = \{..., -9, -4, 1, 6, 11, ...\}$
$\bar{2} = 2 + H = \{..., -8, -3, 2, 7, 12, ...\}$
$\bar{3} = 3 + H = \{..., -7, -2, 3, 8, 13, ...\}$
$\bar{4} = 4 + H = \{..., -6, -1, 4, 9, 14, ...\}$

(a)

$+$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{0}$
$\bar{2}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{0}$	$\bar{1}$
$\bar{3}$	$\bar{3}$	$\bar{4}$	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{4}$	$\bar{4}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$

(b)

Fig. B-5

Cyclic Subgroups

Let G be any group and let a be any element of G. As usual, we define $a^0 = e$ and $a^{n+1} = a^n \cdot a$. Clearly, $a^m a^n = a^{m+n}$ and $(a^m)^n = a^{mn}$, for any integers m and n. Let S denote the set of all the powers of a; that is

$$S = \{\cdots, a^{-3},\ a^{-2},\ a^{-1},\ e,\ a,\ a^2,\ a^3,\ \cdots\}$$

Then S is a subgroup of G called the cyclic group generated by a. We denote this group by $gp(a)$.

Furthermore, suppose that the powers of a are not distinct, say $a^r = a^s$ with, say, $r > s$. Then $a^{r-s} = e$ where $r, s > 0$. The smallest positive integer m such that $a^m = e$ is called the *order* of a and it will be denoted by $|a|$. If $|a| = m$, then the cyclic subgroup $gp(a)$ has m elements as follows:

$$gp(a) = \{e, a, a^2, a^3, \ldots, a^{m-1}\}$$

Consider, for example, the element ϕ_1 in the symmetric group S_3 discussed above. Then:

$$\phi_1{}^1 = \phi_1, \quad \phi_1{}^2 = \phi_2, \quad \phi_1{}^3 = \phi_2 \cdot \phi_1 = e$$

Hence $|\phi_1| = 3$ and $gp(\phi_1) = \{e,\ \phi_1,\ \phi_2\}$. Observe that $|\phi_1|$ divides the order of S_3. This is true in general; that is, for any element a in a group G, $|a|$ equals the order of $gp(a)$ and hence $|a|$ divides $|G|$ by Lagrange's Theorem B.7. We also remark that a group G is said to be *cyclic* if it has an element a such that $G = gp(a)$.

Generating Sets, Generators

Consider any subset A of a group G. Let $gp(A)$ denote the set of all elements x in G such that x is equal to a product of elements where each element comes from the set $A \cup A^{-1}$ (where A^{-1} denotes the set of inverses of elements of A). That is,

$$gp(A) = \{x \in G \mid x = b_1 b_2 \ldots b_m \text{ where each } b_i \in A \cup A^{-1}\}$$

Then $gp(A)$ is a subgroup of G with *generating set* A. In particular, A is said to generate the group G if $G = gp(A)$, that is, if every g in G is a product of elements from $A \cup A^{-1}$. We say A is a *minimal set of generators* of G if A generates G and if no set with fewer elements than A generates G. For example, the permutations $a = \sigma_1$ and $b = \phi_1$ form a minimal set of generators of the symmetric group S_3 (Fig. B-4). Specifically,

$$e = a^2, \quad \sigma_1 = a, \quad \sigma_2 = ab, \quad \sigma_3 = ab^2, \quad \phi_1 = b, \quad \phi_2 = b^2$$

and S_3 is not cyclic so it cannot be generated by one element.

Homomorphisms

A mapping f from a group G into a group G' is called a homomorphism if, for every $a, b \in G$,

$$f(ab) = f(a) f(b)$$

In addition, if f is one-to-one and onto, then f is called an *isomorphism*; and G and G' are said to be *isomorphic*, written $G \cong G'$.

If $f : G \to G'$ is a homomorphism, then the kernel of f, written Ker f, is the set of elements whose image is the identity element e' of G'; that is,

$$\text{Ker } f = \{a \in G \mid f(a) = e'\}$$

Recall that the image of f, written $f(G)$ or Im f, consists of the images of the elements under f; that is,

$$\text{Im } f = \{b \in G' \mid \text{there exists } a \in G \text{ for which } f(a) = b\}\ .$$

The following theorem (proved in Problem B.19) is fundamental to group theory.

Theorem B.9: Suppose $f\colon G \to G'$ is a homomorphism with kernel K. Then K is a normal subgroup of G, and the quotient group G/K is isomorphic to $f(G)$.

EXAMPLE B.12

(a) Let G be the group of real numbers under addition, and let G' be the group of positive real numbers under multiplication. The mapping $f\colon G \to G'$ defined by $f(a) = 2^a$ is a homomorphism because

$$f(a+b) = 2^{a+b} = 2^a 2^b = f(a)f(b)$$

In fact, f is also one-to-one and onto; hence G and G' are isomorphic.

(b) Let a be any element in a group G. The function $f\colon \mathbf{Z} \to G$ defined by $f(n) = a^n$ is a homomorphism since

$$f(m+n) = a^{m+n} = a^m \cdot a^n = f(m) \cdot f(n)$$

The image of f is $gp(a)$, the cyclic subgroup generated by a. By Theorem B.9,

$$gp(a) \cong \mathbf{Z}/\mathbf{K}$$

where K is the kernel of f. If $K = \{0\}$, then $gp(a) = \mathbf{Z}$. On the other hand, if m is the order of a, then $K = \{\text{multiples of } m\}$, and so $gp(a) \cong \mathbf{Z}_m$. In other words, any cyclic group is isomorphic to either the integers $\mathbf{Z}$ under addition, or to $\mathbf{Z}_m$, the integers under addition modulo m.

B.6 RINGS, INTEGRAL DOMAINS, AND FIELDS

Let R be a nonempty set with two binary operations, an operation of addition (denoted by $+$) and an operation of multiplication (denoted by juxtaposition). Then R is called a *ring* if the following axioms are satisfied:

$[\mathbf{R_1}]$ For any $a, b, c \in R$, we have $(a+b)+c = a+(b+c)$.

$[\mathbf{R_2}]$ There exists an element $0 \in R$, called the *zero* element, such that, for every $a \in R$,

$$a + 0 = 0 + a = a.$$

$[\mathbf{R_3}]$ For each $a \in R$ there exists an element $-a \in R$, called the *negative* of a, such that

$$a + (-a) = (-a) + a = 0.$$

$[\mathbf{R_4}]$ For any $a, b \in R$, we have $a + b = b + a$.

$[\mathbf{R_5}]$ For any $a, b, c \in R$, we have $(ab)c = a(bc)$.

$[\mathbf{R_6}]$ For any $a, b, c \in R$, we have: (i) $a(b+c) = ab + ac$, and (ii) $(b+c)a = ba + ca$.

Observe that the axioms $[\mathbf{R_1}]$ through $[\mathbf{R_4}]$ may be summarized by saying that R is an abelian group under addition.

Subtraction is defined in R by $a - b = a + (-b)$.

One can prove (Problem B.21) that $a \cdot 0 = 0 \cdot a = 0$ for every $a \in R$.

A subset S of R is a *subring* of R if S itself is a ring under the operations in R. We note that S is a subring of R if: (i) $0 \in S$, and (ii) for any $a, b \in S$, we have $a - b \in S$ and $ab \in S$.

Special Kinds of Rings: Integral Domains and Fields

This subsection defines a number of different kinds of rings, including integral domains and fields.

R is called a *commutative ring* if $ab = ba$ for every $a, b \in R$.

R is called a *ring with an identity element 1* if the element 1 has the property that $a \cdot 1 = 1 \cdot a = a$ for every element $a \in R$. In such a case, an element $a \in R$ is called a *unit* if a has a multiplicative inverse, that is, an element a^{-1} in R such that $a \cdot a^{-1} = a^{-1} \cdot a = 1$.

R is called a *ring with zero divisors* if there exist nonzero elements $a, b \in R$ such that $ab = 0$. In such a case, a and b are called *zero divisors*.

Definition B.3: A commutative ring R is an *integral domain* if R has no zero divisors, that is, if $ab = 0$ implies $a = 0$ or $b = 0$.

Definition B.4: A commutative ring R with an identity element 1 (not equal to 0) is a field if every nonzero $a \in R$ is a unit, that is, has a multiplicative inverse.

A field is necessarily an integral domain; for if $ab = 0$ and $a \neq 0$, then

$$b = 1 \cdot b = a^{-1}ab = a^{-1} \cdot 0 = 0$$

We remark that a field may also be viewed as a commutative ring in which the nonzero elements form a group under multiplication.

EXAMPLE B.13

(a) The set $\mathbf{Z}$ of integers with the usual operations of addition and multiplication is the classical example of an integral domain (with an identity element). The units in $\mathbf{Z}$ are only 1 and -1, that is, no other element in $\mathbf{Z}$ has a multiplicative inverse.

(b) The set $\mathbf{Z}_m = \{0, 1, 2, \ldots, m-1\}$ under the operation of addition and multiplication modulo m is a ring; it is called the *ring of integers modulo m*. If m is a prime, then $\mathbf{Z}_m$ is a field. On the other hand, if m is not a prime then $\mathbf{Z}_m$ has zero divisors. For instance, in the ring $\mathbf{Z}_6$,

$$2 \cdot 3 = 0 \quad \text{but} \quad 2 \not\equiv 0 \pmod 6 \quad \text{and} \quad 3 \not\equiv 0 \pmod 6$$

(c) The rational numbers $\mathbf{Q}$ and the real numbers $\mathbf{R}$ each form a field with respect to the usual operations of addition and multiplication.

(d) Let M denote the set of 2×2 matrices with integer or real entries. Then M is a noncommutative ring with zero divisors under the operations of matrix addition and matrix multiplication. M does have an identity element, the identity matrix.

(e) Let R be any ring. Then the set $R[x]$ of all polynomials over R is a ring with respect to the usual operations of addition and multiplication of polynomials. Moreover, if R is an integral domain then $R[x]$ is also an integral domain.

Ideals

A subset J of a ring R is called an *ideal* in R if the following three properties hold:

(i) $0 \in J$.

(ii) For any $a, b \in J$, we have $a - b \in J$.

(iii) For any $r \in R$ and $a \in J$, we have $ra, ar \in J$.

Note first that J is a subring of R. Also, J is a subgroup (necessarily normal) of the additive group of R. Thus we can form the following collection of cosets which form a partition of R:

$$\{a + J \mid a \in R\}$$

The importance of ideals comes from the following theorem which is analogous to Theorem B.7 for normal subgroups.

Theorem B.10: Let J be an ideal in a ring R. Then the cosets $\{a + J \mid a \in R\}$ form a ring under the coset operations

$$(a + J) + (b + J) = a + b + J \quad \text{and} \quad (a + J)(b + J) = ab + J$$

This ring is denoted by R/J and is called the *quotient ring*.

Now let R be a commutative ring with an identity element 1. For any $a \in R$, the following set is an ideal:

$$(a) = \{ra \mid r \in R\} = aR$$

It is called the *principal ideal generated* by a. If every ideal in R is a principal ideal, then R is called a *principal ideal ring*. In particular, if R is also an integral domain, then R is called a *principal ideal domain* (PID).

EXAMPLE B.14

(a) Consider the ring $\mathbf{Z}$ of integers. Then every ideal J in $\mathbf{Z}$ is a principal ideal, that is, $J = (m) = m\mathbf{Z}$, for some integer m. Thus $\mathbf{Z}$ is a principal ideal domain (PID). The quotient ring $\mathbf{Z_m} = \mathbf{Z}/(m)$ is simply the ring of integers modulo m. Although $\mathbf{Z}$ is an integral domain (no zero divisors), the quotient ring $\mathbf{Z_m}$ may have zero divisors, e.g., 2 and 3 are zero divisors in $\mathbf{Z_6}$.

(b) Let R be any ring. Then $\{0\}$ and R are ideals. In particular, if R is a field, then $\{0\}$ and R are the only ideals.

(c) Let K be a field. Then the ring $K[x]$ of polynomials over K is a PID (principal ideal domain). On the other hand, the ring $K[x, y]$ of polynomials in two variables is not a PID.

Ring Homomorphisms

A mapping f from a ring R into a ring R' is called a *ring homomorphism* or, simply, *homomorphism* if, for every $a, b \in R$,

$$f(a + b) = f(a) + f(b), \quad f(ab) = f(a)f(b)$$

In addition, if f is one-to-one and onto, then f is called an *isomorphism*; and R and R' are said to be *isomorphic*, written $R \cong R'$.

Suppose $f: R \to R'$ is a homomorphism. Then the kernel of f, written Ker f, is the set of elements whose image is the zero element 0 of R'; that is,

$$\text{Ker } f = \{r \in R \mid f(r) = 0\}$$

The following theorem (analogous to Theorem B.9 for groups) is fundamental to ring theory.

Theorem B.11: Let $f: R \to R'$ be a ring homomorphism with kernel K. Then K is an ideal in R, and the quotient ring R/K is isomorphic to $f(R)$.

Divisibility in Integral Domains

Now let D be an integral domain. We say that b divides a in D if $a = bc$ for some $c \in D$. An element $u \in D$ is called a *unit* if u divides 1, i.e., if u has a multiplicative inverse. An element $b \in D$ is called an *associate* of $a \in D$ if $b = ua$ for some unit $u \in D$. A nonunit $p \in D$ is said to be *irreducible* if $p = ab$ implies a or b is a unit.

An integral domain D is called a *unique factorization domain* (UFD), if every nonunit $a \in D$ can be written uniquely (up to associates and order) as a product of irreducible elements.

EXAMPLE B.15

(a) The ring $\mathbf{Z}$ of integers is the classical example of a unique factorization domain. The units of $\mathbf{Z}$ are 1 and -1. The only associates of $n \in Z$ are n and $-n$. The irreducible elements of $\mathbf{Z}$ are the prime numbers.

(b) The set $D = \{a + b\sqrt{13} \mid a, b \text{ integers}\}$ is an integral domain. The units of D follow:

$$\pm 1, \quad 18 \pm 5\sqrt{13}, \quad -18 \pm 5\sqrt{13}$$

The elements 2, $3 - \sqrt{13}$ and $-3 - \sqrt{13}$ are irreducible in D. Observe that

$$4 = 2 \cdot 2 = (3 - \sqrt{13})(-3 - \sqrt{13})$$

Thus D is not a unique factorization domain. (See Problem B.97.)

B.7 POLYNOMIALS OVER A FIELD

This section investigates polynomials whose coefficients come from some integral domain or field K. In particular, we show that polynomials over a field K have many of the same properties as the integers.

Basic Definitions

Let K be an integral domain or a field. Formally, a polynomial f over K is an infinite sequence of elements from K in which all except a finite number of them are 0; that is,

$$f = (\ldots, 0, a_n, \ldots, a_1, a_0) \quad \text{or, equivalently,} \quad f(t) = a_n t^n + \cdots + a_1 t + a_0$$

where the symbol t is used as an indeterminate. The entry a_k is called the kth coefficient of f. If n is the largest integer for which $a \neq 0$, then we say that the degree of f is n, written $\deg(f) = n$. We also call a_n the leading coefficient of f. If $a_n = 1$, we call f a *monic* polynomial. On the other hand, if every coefficient of f is 0 then f is called the *zero* polynomial, written $f \equiv 0$. The degree of the zero polynomial is not defined.

Let $K[t]$ be the collection of all polynomials $f(t)$ over K. Consider the polynomials

$$f(t) = a_n t^n + \cdots + a_1 t + a_0 \quad \text{and} \quad g(t) = b_m t^m + \cdots + b_1 t + b_0$$

Then the sum $f + g$ is the polynomial obtained by adding corresponding coefficients; that is, if $m \leq n$, then

$$f(t) + g(t) = a_n t^n + \cdots + (a_m + b_m)t^m + \cdots + (a_1 + b_1)t + (a_0 + b_0)$$

Furthermore, the product of f and g is the polynomial

$$f(t)g(t) = (a_n b_m)t^{n+m} + \cdots + (a_1 b_0 + a_0 b_1)t + (a_0 b_0)$$

That is,

$$f(t)g(t) = c_{n+m}t^{n+m} + \cdots + c_1 t + c_0 \quad \text{where} \quad c_k = \sum_{i=0}^{k} a_i b_{k-i} = a_0 b_k + a_1 b_{k-1} + \cdots + a_k b_0$$

The set K of scalars is viewed as a subset of $K[t]$. Specifically, we identify the scalar $a_0 \in K$ with the polynomial

$$f(t) = a_0 \quad \text{or} \quad a_0 = (\cdots, 0, 0, a_0)$$

Then the operators of addition and scalar multiplication are preserved by this identification. Thus, the mapping $\psi\colon K \to K[t]$ defined by $\psi(a_0) = a_0$ is an isomorphism which embeds K into $K[t]$.

Theorem B.12: Let K be an integral domain. Then $K[t]$ under the operations of addition and multiplication of polynomials is a commutative ring with an identity element 1.

The following simple result has important consequences.

Lemma B.13: Suppose f and g are polynomials over an integral domain K. Then

$$\deg(fg) = \deg(f) + \deg(g).$$

The proof follows directly from the definition of the product of polynomials. Namely, suppose

$$f(t) = a_n t^n + \cdots + a_1 t + a_0 \quad \text{and} \quad g(t) = b_m t^m + \cdots + b_1 t + b_0$$

where $a_n \neq 0$ and $b_m \neq 0$. Thus $\deg(f) = n$ and $\deg(g) = m$. Then

$$f(t)g(t) = a_n b_m t^{n+m} + \text{ terms of lower degree}$$

Also, since K is an integral domain with no zero divisors, $a_n b_m \neq 0$. Thus

$$\deg(fg) = m + n = \deg(f) + \deg(g)$$

and the lemma is proved.

The following proposition lists many properties of our polynomials. (Recall that a polynomial g is said to *divide* a polynomial f if there exists a polynomial h such that $f(t) = g(t)h(t)$.)

Proposition B.14: Let K be an integral domain and let f and g be polynomials over K.

(i) $K[t]$ is an integral domain.

(ii) The units of $K[t]$ are the units in K.

(iii) If g divides f, then $\deg(g) \leq \deg(f)$ or $f \equiv 0$.

(iv) If g divides f and f divides g, then $f(t) = kg(t)$ where k is a unit in K.

(v) If d and d' are monic polynomials such that d divides d' and d' divides d, then $d = d'$.

Euclidean Algorithm, Roots of Polynomials

This subsection discusses the roots of a polynomial $f(t)$, where we now assume the coefficients of $f(t)$ come from a field K. Recall that a scalar $a \in K$ is a *root* of a polynomial $f(t)$ if $f(a) = 0$. First we begin with an important theorem which is very similar to a corresponding theorem for the integers $\mathbf{Z}$.

Theorem B.15 (Euclidean Division Algorithm): Let $f(t)$ and $g(t)$ be polynomials over a field K with $g(t) \neq 0$. Then there exist polynomials $q(t)$ and $r(t)$ such that

$$f(t) = q(t)g(t) + r(t)$$

where either $r(t) \equiv 0$ or $\deg(r) < \deg(g)$.

The above theorem (proved in Problem B.30) formalizes the process known as "long division." The polynomial $q(t)$ is called the *quotient* and the polynomial $r(t)$ is called the *remainder* when $f(t)$ is divided by $g(t)$.

Corollary B.16 (Remainder Theorem): Suppose $f(t)$ is divided by $g(t) = t - a$. Then $f(a)$ is the remainder.

The proof follows from the Euclidean Algorithm. That is, dividing $f(t)$ by $t - a$ we get

$$f(t) = q(t)(t - a) + r(t)$$

where $\deg(r) < \deg(t - a) = 1$. Hence $r(t) = r$ is a scalar. Substituting $t = a$ in the equation for $f(t)$ yields

$$f(a) = q(a)(a - a) + r = q(t) \cdot 0 + r = r$$

Thus $f(a)$ is the remainder, as claimed.

Corollary B.16 also tells us that $f(a) = 0$ if and only if the remainder $r = r(t) \equiv 0$. Accordingly:

Corollary B.17 (Factor Theorem): The scalar $a \in K$ is a root of $f(t)$ if and only if $t - a$ is a factor of $f(t)$.

The next theorem (proved in Problem B.31) tells us the number of possible roots of a polynomial.

Theorem B.18: Suppose $f(t)$ is a polynomial over a field K, and $\deg(f) = n$. Then $f(t)$ has at most n roots.

The following theorem (proved in Problem B.32) is the main tool for finding rational roots of a polynomial with integer coefficients.

Theorem B.19: Suppose a rational number p/q (reduced to lowest terms) is a root of the polynomial

$$f(t) = a_n t^n + \cdots + a_1 t + a_0$$

where all the coefficients $a_n, \ldots, a_1, a_0$ are integers. Then p divides the constant term a_0 and q divides the leading coefficient a_n. In particular, if $c = p/q$ is an integer, then c divides the constant term a_0.

EXAMPLE B.16

(a) Suppose $f(t) = t^3 + t^2 - 8t + 4$. Assuming $f(t)$ has a rational root, find all the roots of $f(t)$.

Since the leading coefficient is 1, the rational roots of $f(t)$ must be integers from among ± 1, ± 2, ± 4. Note $f(1) \neq 0$ and $f(-1) \neq 0$. By synthetic division, or dividing by $t - 2$, we get

$$\begin{array}{r|rrrrrrr} 2 & 1 & + & 1 & - & 8 & + & 4 \\ & & & 2 & + & 6 & - & 4 \\ \hline & 1 & + & 3 & - & 2 & + & 0 \end{array}$$

Therefore $t = 2$ is a root and $f(t) = (t - 2)(t^2 + 3t - 2)$. Using the quadratic formula for $t^2 + 3t - 2 = 0$, we obtain the following three roots of $f(t)$:

$$t = 2, \quad t = (-3 + \sqrt{17})/2, \quad t = (-3 - \sqrt{17})/2$$

(b) Suppose $h(t) = t^4 - 2t^3 + 11t - 10$. Find all the real roots of $h(t)$ assuming there are two integer roots.

The integer roots must be among ± 1, ± 2, ± 5, ± 10. By synthetic division (or dividing by $t - 1$ and then $t + 2$) we get

$$\begin{array}{r|rrrrrrrrr} 1 & 1 & - & 2 & + & 0 & + & 11 & - & 10 \\ & & & 1 & - & 1 & - & 1 & + & 10 \\ \hline -2 & 1 & - & 1 & - & 1 & + & 10 & + & 0 \\ & & - & 2 & + & 6 & - & 10 & & \\ \hline & 1 & - & 3 & + & 5 & + & 0 & & \end{array}$$

Thus $t = 1$ and $t = -2$ are roots and $h(t) = (t-1)(t+2)(t^2-3t+5)$. The quadratic formula with $t^2 - 3t + 5$ tells us that there are no other real roots. That is, $t = 1$ and $t = -2$ are the only real roots of $h(t)$.

$K[t]$ as a PID and UFD

The following theorems (proved in Problems B.33 and B.34) apply.

Theorem B.20: The ring $K[t]$ of polynomials over a field K is a principal ideal domain (PID). That is, if J is an ideal in $K[t]$, then there exists a unique monic polynomial d which generates J, that is, every polynomial f in J is a multiple of d.

Theorem B.21: Let f and g be polynomials in $K[t]$, not both zero. Then there exists a unique monic polynomial d such that:

(i) d divides both f and g. (ii) If d' divides f and g, then d′ divides d.

The polynomial d in the above Theorem B.21 is called the *greatest common divisor* of f and g, written $d = gcd(f, g)$. If $d = 1$, then f and g are said to be *relatively prime*.

Corollary B.22: Let d be the greatest common divisor of f and g. Then there exist polynomials m and n such that $d = mf + ng$. In particular, if f and g are relatively prime, then there exist polynomials m and n such that $mf + ng = 1$.

A polynomial $p \in K[t]$ is said to be *irreducible* if p is not a scalar and if $p = fg$ implies f or g is a scalar. In other words, p is irreducible if its only divisors are its associates (scalar multiples). The following lemma (proved in Problem B.36) applies.

Lemma B.23: Suppose $p \in K[t]$ is irreducible. If p divides the product fg of polynomials f and g in $K[t]$, then p divides f or p divides g. More generally, if p divides the product $f_1 f_2 \cdots f_n$ of n polynomials, then p divides one of them.

The next theorem (proved in Problem B.37) states that the polynomials over a field form a *unique factorization domain* (UFD).

Theorem B.24 (Unique Factorization Theorem): Let f be a nonzero polynomial in $K[t]$. Then f can be written uniquely (except for order) as a product

$$f = kp_1 p_2 \cdots p_n$$

where $k \in K$ and the p's are monic irreducible polynomials in $K[t]$.

Fundamental Theorem of Algebra

The proof of the following theorem lies beyond the scope of this text.

Fundamental Theorem of Algebra: Any nonzero polynomial $f(t)$ over the complex field **C** has a root in **C**.

Thus $f(t)$ can be written uniquely (except for order) as a product

$$f(t) = k(t - r_1)(t - r_2) \cdots (t - r_n)$$

where k and the r_i are complex numbers and $\deg(f) = n$.

The above theorem is certainly not true for the real field **R**. For example, $f(t) = t^2 + 1$ is a polynomial over R, but $f(t)$ has no real root.

The following theorem (proved in Problem B.38) does apply.

Theorem B.25: Suppose $f(t)$ is a polynomial over the real field **R**, and suppose the complex number $z = a + bi$, $b \neq 0$, is a root of $f(t)$. Then the complex conjugate $\bar{z} = a - bi$ is also a root of $f(t)$. Hence the following is a factor of $f(t)$:

$$c(t) = (t - z)(t - \bar{z}) = t^2 - 2at + a^2 + b^2$$

The following theorem follows from Theorem B.25 and the Fundamental Theorem of Algebra.

Theorem B.26: Let $f(t)$ be a nonzero polynomial over the real field **R**. Then $f(t)$ can be written uniquely (except for order) as a product

$$f(t) = kp_1(t) p_2(t) \cdots p_n(t)$$

where $k \in \mathbf{R}$ and the $p_i(t)$ are real monic polynomials of degree 1 or 2.

EXAMPLE B.17 Let $f(t) = t^4 - 3t^3 + 6t^2 + 25t - 39$. Find all the roots of $f(t)$ given that $t = 2 + 3i$ is a root.

Since $2 + 3i$ is a root, then $2 - 3i$ is a root and $c(t) = t^2 - 4t + 13$ is a factor of $f(t)$. Dividing $f(t)$ by $c(t)$ we get

$$f(t) = (t^2 - 4t + 13)(t^2 + t - 3)$$

The quadratic formula with $t^2 + t - 3$ gives us the other roots of $f(t)$. That is, the four roots of $f(t)$ are as follows:

$$t = 2 + 3i, \quad t = 2 - 3i, \quad t = (-1 + \sqrt{13})/2, \quad t = (-1 - \sqrt{13})/2$$

Solved Problems

OPERATIONS AND SEMIGROUPS

B.1. Consider the set $\mathbf{Q}$ of rational numbers, and let $*$ be the operation on $\mathbf{Q}$ defined by

$$a * b = a + b - ab$$

(*a*) Find: (i) $3 * 4$; (ii) $2 * (-5)$; (iii) $7 * (1/2)$.

(*b*) Is $(\mathbf{Q}, *)$ a semigroup? Is it commutative?

(*c*) Find the identity element for $*$.

(*d*) Do any of the elements in $\mathbf{Q}$ have an inverse? What is it?

(*a*) (i) $3 * 4 = 3 + 4 - 3(4) = 3 + 4 - 12 = -5$
(ii) $2 * (-5) = 2 + (-5) + 2(-5) = 2 - 5 + 10 = 7$
(iii) $7 * (1/2) = 7 + (1/2) - 7(1/2) = 4$

(*b*) We have:

$$\begin{aligned}(a * b) * c &= (a + b - ab) * c = (a + b - ab) + c - (a + b - ab)c \\ &= a + b - ab + c - ac - bc + abc = a + b + c - ab - ac - bc + abc \\ a * (b * c) &= a * (b + c - bc) = a + (b + c - bc) - a(b + c - bc) \\ &= a + b + c - bc - ab - ac + abc\end{aligned}$$

Hence $*$ is associative and $(\mathbf{Q}, *)$ is a semigroup. Also

$$a * b = a + b - ab = b + a - ba = b * a$$

Hence $(\mathbf{Q}, *)$ is a commutative semigroup.

(*c*) An element e is an identity element if $a * e = a$ for every $a \in \mathbf{Q}$. Compute as follows:

$$a * e = a, \quad a + e - ae = a, \quad e - ea = 0, \quad e(1 - a) = 0, \quad e = 0$$

Accordingly, 0 is the identity element.

(*d*) In order for a to have an inverse x, we must have $a * x = 0$ since 0 is the identity element by Part (*c*). Compute as follows:

$$a * x = 0, \quad a + x - ax = 0, \quad a = ax - x, \quad a = x(a - l), \quad x = a/(a - l)$$

Thus if $a \neq 1$, then a has an inverse and it is $a/(a - 1)$.

B.2. Let S be a semigroup with identity e, and let b and b' be inverses of a. Show that $b = b'$, that is, that inverses are unique if they exist.

We have:

$$b * (a * b') = b * e = b \quad \text{and} \quad (b * a) * b' = e * b' = b'$$

Since S is associative, $(b * a) * b' = b * (a * b')$; hence $b = b'$.

B.3. Let $S = \mathbf{N} \times \mathbf{N}$. Let $*$ be the operation on S defined by $(a, b) * (a', b') = (aa', bb')$.

(a) Show that $*$ is associative. (Hence S is a semigroup.)

(b) Define $f: (S, *) \to (\mathbf{Q}, \times)$ by $f(a, b) = a/b$. Show that f is a homomorphism.

(c) Find the congruence relation $\sim$ in S determined by the homomorphism f, that is, where $x \sim y$ if $f(x) = f(y)$. (See Theorem B.4.)

(d) Describe $S/\sim$. Does $S/\sim$ have an identity element? Does it have inverses?

Suppose $x = (a, b)$, $y = (c, d)$, $z = (e, f)$.

(a) We have

$$(xy)z = (ac,\ bd) * (e,\ f) = [(ac)e, (bd)f]$$
$$x(yz) = (a,\ b) * (ce,\ df) = [a(ce), b(df)]$$

Since a, b, c, d, e, f, are positive integers, $(ac)e = a(ce)$ and $(bd)f = b(df)$. Thus $(xy)z = x(yz)$ and hence $*$ is associative. That is, $(S, *)$ is a semigroup.

(b) f is a homomorphism since

$$f(x * y) = f(ac,\ bd) = (ac)/(bd) = (a/b)(c/d) = f(x)f(y)$$

(c) Suppose $f(x) = f(y)$. Then $a/b = c/d$ and hence $ad = bc$. Thus f determines the congruence relation $\sim$ on S defined by $(a, b) \sim (c, d)$ if $ad = bc$.

(d) The image of f is $\mathbf{Q}^+$, the set of positive rational numbers. By Theorem B.3, $S/\sim$ is isomorphic to $\mathbf{Q}^+$. Thus $S/\sim$ does have an identity element, and every element has an inverse.

B.4. Prove Theorem B.1. Suppose $*$ is an associative operation on a set S. Then any product $a_1 * a_2 * \ldots * a_n$ requires no parenthesis, that is, all possible products are equal.

The proof is by induction on n. Since n is associative, the theorem holds for $n = 1, 2$, and 3. Suppose $n \geq 4$. We use the notation:

$$(a_1a_2, \cdots a_n) = (\cdots((a_1a_2)a_3)\cdots)a_n \quad \text{and} \quad [a_1a_2\cdots a_n] = \text{any product}$$

We show $[a_1a_2\cdots a_n] = (a_1a_2\cdots a_n)$ and so all such products will be equal. Since $[a_1a_2\cdots a_n]$ denotes some product, there exists an $r < n$ such that $[a_1a_2\cdots a_n] = [a_1a_2\cdots a_r]\,[a_{r+1}\cdots a_n]$. Therefore, by induction,

$$\begin{aligned}[a_1a_2\cdots a_n] &= [a_1a_2\cdots a_r]\,[a_{r+1}\cdots a_n] = [a_1a_2\cdots a_r](a_{r+1}\cdots a_n)\\ &= [a_1\cdots a_r]\,((a_{r+1}\cdots a_{n-1})a_n) = ([a_1\cdots a_r]\,(a_{r-1}\cdots a_{n-1}))a_n\\ &= [a_1\cdots a_{n-1}]a_n = (a_1\cdots a_{n-1})a_n = (a_1a_2\cdots a_n)\end{aligned}$$

Thus the theorem is proved.

B.5. Prove Theorem B.4: Let $f : S \to S'$ be a semigroup homomorphism. Let $a \sim b$ if $f(a) = f(b)$. Then: (i) $\sim$ is a congruence relation; (ii) $S/\sim$ is isomorphic to $f(S)$.

(i) First we show that $\sim$ is an equivalence relation. Since $f(a) = f(a)$, we have $a \sim a$.
If $a \sim b$, then $f(a) = f(b)$ or $f(b) = f(a)$; hence $b \sim a$. Lastly, if $a \sim b$ and $b \sim c$, then $f(a) = f(b)$ and $f(b) = f(c)$; hence $f(a) = f(c)$. Thus $a \sim c$. That is, $\sim$ is an equivalence relation. Suppose now $a \sim a'$ and $b \sim b'$. Then $f(a) = f(a')$ and $f(b) = f(b')$.

Since f is a homomorphism,

$$f(ab) = f(a)f(b) = f(a')\,f(b') = f(a'b')$$

Therefore $ab \sim a'b'$. That is, $\sim$ is a congruence relation.

(ii) Define $\Psi: S/\sim \to f(S)$ by $\Psi([a]) = f(a)$. We need to prove: (1) Ψ is well-defined, that is, $\Psi([a]) \in f(S)$, and if $[a] = [b]$ then $f([a]) = f([b])$. (2) Ψ is an isomorphism, that is, Ψ is a homomorphism, one-to-one and onto.

(1) *Proof that Ψ is well-defined*: We have $\Psi([a]) = f(a)$. Since $a \in S$, we have $f(a) \in f(S)$. Hence $\Psi([a]) \in f(S)$, as required. Now suppose $[a] = [b]$. Then $a \sim b$ and hence $f(a) = f(b)$. Thus

$$\Psi([a]) = f(a) = f(b) = \Psi([b])$$

That is, Ψ is well-defined.

(2) *Proof that Ψ is an isomorphism*: Since f is a homomorphism,

$$\Psi([a][b]) = \Psi[ab] = f(ab) = f(a)f(b) = \Psi([a])\Psi([b])$$

Hence Ψ is a homomorphism. Suppose $\Psi([a]) = \Psi([b])$. Then $f(a) = f(b)$, and so $a \sim b$. Thus $[a] = [b]$ and Ψ is one-to-one. Lastly, let $y \in f(S)$. Then, $f(a) = y$ for some $a \in S$. Hence $\Psi([a]) = f(a) = y$. Thus Ψ is onto $f(S)$. Accordingly, Ψ is an isomorphism.

GROUPS

B.6. Consider the group $G = \{1, 2, 3, 4, 5, 6\}$ under multiplication modulo 7.

(*a*) Find the multiplication table of G.
(*b*) Find $2^{-1}, 3^{-1}, 6^{-1}$.
(*c*) Find the orders and subgroups generated by 2 and 3.
(*d*) Is G cyclic?

(*a*) To find $a * b$ in G, find the remainder when the product ab is divided by 7.

For example, $5 \cdot 6 = 30$ which yields a remainder of 2 when divided by 7; hence $5 * 6 = 2$ in G. The multiplication table of G appears in Fig. B-6(*a*).

(*b*) Note first that 1 is the identity element of G. Recall that a^{-1} is that element of G such that $aa^{-1} = 1$. Hence $2^{-1} = 4$, $3^{-1} = 5$ and $6^{-1} = 6$.

(*c*) We have $2^1 = 2$, $2^2 = 4$, but $2^3 = 1$. Hence $|2| = 3$ and $gp(2) = \{1, 2, 4\}$. We have $3^1 = 3$, $3^2 = 2$, $3^3 = 6$, $3^4 = 4$, $3^5 = 5$, $3^6 = 1$. Hence $|3| = 6$ and $gp(3) = G$.

(*d*) G is cyclic since $G = gp(3)$.

*	1	2	3	4	5	6
1	1	2	3	4	5	6
2	2	4	6	1	3	5
3	3	6	2	5	1	4
4	4	1	5	2	6	3
5	5	3	1	6	4	2
6	6	5	4	3	2	1

(*a*)

*	1	2	4	7	8	11	13	14
1	1	2	4	7	8	11	13	14
2	2	4	8	14	1	7	11	13
4	4	8	1	13	2	14	7	11
7	7	14	13	4	11	2	1	8
8	8	1	2	11	4	13	14	7
11	11	7	14	2	13	1	8	4
13	13	11	7	1	14	8	4	2
14	14	13	11	8	7	4	2	1

(*b*)

Fig. B-6

B.7. Let G be a reduced residue system modulo 15, say, $G = \{1, 2, 4, 7, 8, 11, 13, 14\}$ (the set of integers between 1 and 15 which are coprime to 15). Then G is a group under multiplication modulo 15.

(*a*) Find the multiplication table of G.
(*b*) Find $2^{-1}, 7^{-1}, 11^{-1}$.
(*c*) Find the orders and subgroups generated by 2, 7, and 11.
(*d*) Is G cyclic?

(*a*) To find $a * b$ in G, find the remainder when the product ab is divided by 15. The multiplication table appears in Fig. B-6(*b*).

(*b*) The integers r and s are inverses if $r * s = 1$. Hence: $2^{-1} = 8$, $7^{-1} = 13$, $11^{-1} = 11$.

(*c*) We have $2^2 = 4$, $2^3 = 8$, $2^4 = 1$. Hence $|2| = 4$ and $\text{gp}(2) = \{1, 2, 4, 8\}$. Also, $7^2 = 4$, $7^3 = 4 * 7 = 13$, $7^4 = 13 * 7 = 1$. Hence $|7| = 4$ and $\text{gp}(7) = \{1, 4, 7, 13\}$. Lastly, $11^2 = 1$. Hence $|11| = 2$ and $\text{gp}(11) = \{1, 11\}$.

(*d*) No, since no element generates G.

B.8. Consider the symmetric group S_3 whose multiplication table is given in Fig. B-4.

(*a*) Find the order and the group generated by each element of S_3.

(*b*) Find the number and all subgroups of S_3.

(*c*) Let $A = \{\sigma_1, \sigma_2\}$ and $B = \{\phi_1, \phi_2\}$. Find AB, $\sigma_3 A$, and $A\sigma_3$.

(*d*) Let $H = gp(\sigma_1)$ and $K = gp(\sigma_2)$. Show that HK is not a subgroup of S_3.

(*e*) Is S_3 cyclic?

(*a*) There are six elements: (1) ε, (2) σ_1, (3) σ_2, (4) σ_3, (5) ϕ_1, (6) ϕ_2. Find the powers of each element x until $x^n = \varepsilon$. Then $|x| = n$, and $gp(x) = \{\varepsilon, x^1, x^2, \ldots, x^{n-1}\}$. Note $x^1 = x$, so we need only begin with $n = 2$ when $x \neq \varepsilon$.

(1) $\varepsilon^1 = \varepsilon$; so $|\varepsilon| = 1$ and $g(\varepsilon) = \{\varepsilon\}$.

(2) $\sigma_1^2 = \varepsilon$; hence $|\sigma_1| = 2$ and $gp(\sigma_1) = \{\varepsilon, \sigma_1\}$.

(3) $\sigma_2^2 = \varepsilon$; hence $|\sigma_2| = 2$ and $gp(\sigma_2) = \{\varepsilon, \sigma_2\}$.

(4) $\sigma_3^2 = \varepsilon$; hence $|\sigma_3| = 2$ and $gp(\sigma_3) = \{\varepsilon, \sigma_3\}$.

(5) $\phi_1^2 = \phi_2$, $\phi_1^3 = \phi_2\phi_1 = \varepsilon$; hence $|\phi_1| = 3$ and $gp(\phi_1) = \{\varepsilon, \phi_1, \phi_2\}$.

(6) $\phi_2^2 = \phi_1$, $\phi_2^3 = \phi_1\phi_2 = \varepsilon$; hence $|\phi_2| = 3$ and $gp(\phi_1) = \{\varepsilon, \phi_2, \phi_1\}$.

(*b*) First of all, $H_1 = \{\varepsilon\}$ and $H_2 = S_3$ are subgroups of S_3. Any other subgroup of S_3 must have order 2 or 3 since its order must divide $|S_3| = 6$. Since 2 and 3 are prime numbers, these subgroups must be cyclic (Problem B.61) and hence must appear in part (a). Thus the other subgroups of S_3 follow:

$$H_3 = \{\varepsilon, \sigma_1\}, \quad H_4 = \{\varepsilon, \sigma_2\}, \quad H_5 = \{\varepsilon, \sigma_3\}, \quad H_6 = \{\varepsilon, \phi_1, \phi_2\}$$

Accordingly, S_3 has six subgroups.

(*c*) Multiply each element of A by each element of B:

$$\sigma_1\phi_1 = \sigma_2, \quad \sigma_1\phi_2 = \sigma_3, \quad \sigma_3\phi_1 = \sigma_3, \quad \sigma_2\phi_2 = \sigma_1$$

Hence $\text{AB} = \{\sigma_1, \sigma_2, \sigma_3\}$.

Multiply σ_3 by each element of A:

$$\sigma_3\sigma_1 = \phi_1, \quad \sigma_3\sigma_2 = \phi_2, \quad \text{hence} \quad \sigma_3 A = \{\phi_1, \phi_2\}$$

Multiply each element of A by σ_3:

$$\sigma_1\sigma_3 = \phi_2, \quad \sigma_2\sigma_3 = \phi_1, \quad \text{hence} \quad A\sigma_3 = \{\phi_1, \phi_2\}$$

(*d*) $H = \{e, \sigma_1\}$, $K = \{e, \sigma_2\}$ and then $HK = \{e, \sigma_1, \sigma_2, \phi_1\}$, which is not a subgroup of S_3 since HK has four elements.

(*e*) S_3 is not cyclic since S_3 is not generated by any of its elements.

B.9. Let σ and τ be the following elements of the symmetric group S_6:

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 1 & 5 & 4 & 6 & 2 \end{pmatrix} \quad \text{and} \quad \tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 3 & 1 & 6 & 2 & 4 \end{pmatrix}$$

Find: $\tau\sigma$, $\sigma\tau$, σ^2, and σ^{-1}. (Since σ and τ are functions, $\tau\sigma$ means apply σ and then τ.)

Figure B-7 shows the effect on 1, 2, …, 6 of the composition of the permutations:

(a) σ and then τ; (b) τ and then σ; (c) σ and then σ, i.e. σ^2.

Thus:

$$\tau\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 5 & 2 & 6 & 4 & 3 \end{pmatrix}, \quad \sigma\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 5 & 3 & 2 & 1 & 4 \end{pmatrix}, \quad \sigma^2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 3 & 6 & 4 & 2 & 1 \end{pmatrix}$$

We obtain σ^{-1} by interchanging the top and bottom rows of σ and then rearranging:

$$\sigma^{-1} = \begin{pmatrix} 3 & 1 & 5 & 4 & 6 & 2 \\ 1 & 2 & 3 & 4 & 5 & 6 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 6 & 1 & 4 & 3 & 5 \end{pmatrix}$$

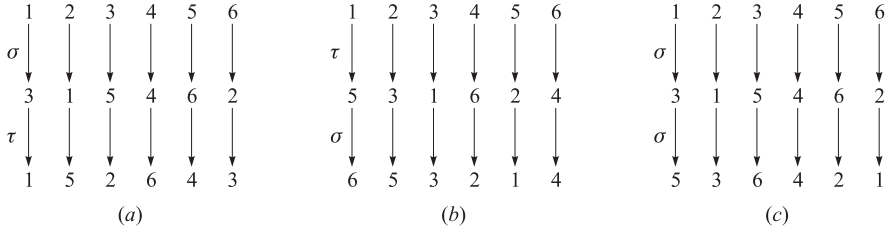


Fig. B-7

B.10. Let H and K be groups.

(a) Define the direct product $G = H \times K$ of H and K.

(b) What is the identity element and the order of $G = H \times K$?

(c) Describe and find the multiplication table of the group $G = \mathbf{Z_2} \times \mathbf{Z_2}$.

(a) Let $G = H \times K$, the Cartesian product of H and K, with the operation $*$ defined componentwise by

$$(h,\ k) * h',\ k' = (hh', kk')$$

Then G is a group (Problem B.68), called the *direct product* of H and K.

(b) The element $e = (e_H, e_K)$ is the identity element of G, and $|G| = |H| \cdot |K|$.

(c) Since $\mathbf{Z_2}$ has two elements, G has four elements. Let

$$e = (0, 0), \quad a = (1, 0), \quad b = (0, 1), \quad c = (1, 1)$$

The multiplication table of G appears in Fig. B-8(a). Note that G is abelian since the table is symmetric. Also, $a^2 = e$, $b^2 = e$, $c^2 = e$. Thus G is not cyclic, and hence $G \ncong \mathbf{Z_4}$.

B.11. Let S be the square in the plane $\mathbf{R^2}$ pictured in Fig. B-8(b), with its center at the origin 0. Note that the vertices of S are numbered counterclockwise from 1 to 4.

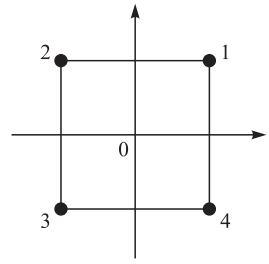
(a) Define the group G of symmetries of S.

(b) List the elements of G.

(c) Find a minimum set of generators of G.

$*$	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

(a)



(b)

Fig. B-8

(a) A symmetry σ of S is a rigid one-to-one correspondence between S and itself. (Here rigid means that distances between points do not change.) The group G of symmetries of S is the set of all symmetries of S under composition of mappings.

(b) There are eight symmetries as follows. For $\alpha = 0°, 90°, 180°, 270°$, let $\sigma(\alpha)$ be the symmetry obtained by rotating S about its center α degrees, and let $\tau(\alpha)$ be the symmetry obtained by reflecting S about the y-axis and then rotating S about its center α degrees. Note that any symmetry σ of S is completely determined by its effect on the vertices of S and hence σ can be represented as a permutation in S_4. Thus:

$$\sigma(0°) = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix}, \quad \sigma(90°) = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix},$$

$$\sigma(180°) = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 4 \end{pmatrix}, \quad \sigma(270°) = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{pmatrix}$$

$$\tau(0°) = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}, \quad \tau(90°) = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 1 & 4 \end{pmatrix},$$

$$\tau(180°) = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix}, \quad \tau(270°) = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 3 & 2 \end{pmatrix}$$

(c) Let $a = \sigma(90°)$ and $b = \tau(0°)$. Then a and b form a maximum set of generators of G. Specifically,

$$\sigma(0°) = a^4, \quad \sigma(90°) = a, \quad \sigma(180°) = a^2, \quad \sigma(270°) = a^3$$
$$\tau(0°) = b, \quad \tau(90°) = ba, \quad \tau(180°) = ba^2, \quad \tau(270°) = ba^3$$

and G is not cyclic so it is not generated by one element. (One can show that the relations $a^4 = e$, $b^2 = e$, and $bab = a^{-1}$ completely describe G.)

B.12. Let G be a group and let A be a nonempty set.

(a) Define the meaning of the statement "G acts on A."

(b) Define the stabilizer H_a of an element $a \in A$.

(c) Show that H_a is a subgroup of G.

(a) Let PERM(A) denote the group of all permutations of A. Let $\psi : G \to \text{PERM}(A)$ be any homomorphism. Then G is said to act on A where each element g in G defines a permutation $g : A \to A$ by

$$g(a) = (\psi(g))(a)$$

(Frequently, the permutation $g : A \to A$ is given directly and hence the homomorphism is implicitly defined.)

(b) The stabilizer H_a of $a \in A$ consists of all elements of G which "fix a," that is,

$$H_a = \{g \in G \mid g(a) = a\}$$

(*c*) Since $e(a) = a$, we have $e \in H_a$. Suppose $g, g' \in H_a$. Then $(gg')(a) = g(g'(a)) = g(a) = a$; hence $gg' \in H_a$. Also, $g^{-1}(a) = a$ since $g(a) = a$; hence $g^{-1} \in H_a$. Thus H_a is a subgroup of G.

B.13. Prove Theorem B.6: Let H be a subgroup of a group G. Then the right cosets Ha form a partition of G.

Since $e \in H$, we have $a = ea \in Ha$; hence every element belongs to a coset. Now suppose Ha and Hb are not disjoint. Say $c \in Ha \cap Hb$. The proof is complete if we show that $Ha = Hb$.

Since c belongs to both Ha and Hb, we have $c = h_1 a$ and $c = h_2 b$, where $h_1, h_2 \in H$. Then $h_1 a = h_2 b$, and so $a = h_1^{-1} h_2 b$. Let $x \in Ha$. Then

$$x = h_3 a = h_3 h_1^{-1} h_2 b$$

where $h_3 \in H$. Since H is a subgroup, $h_3 h_1^{-1} h_2 \in H$; hence $x \in Hb$. Since x was any element of Ha, we have $Ha \subseteq Hb$. Similarly, $Hb \subseteq Ha$. Both inclusions imply $Ha = Hb$, and the theorem is proved.

B.14. Let H be a finite subgroup of G. Show that H and any coset Ha have the same number of elements.

Let $H = \{h_1, h_2, \ldots, h_k\}$, where H has k elements. Then $Ha = \{h_1 a, h_2 a, \ldots, h_k a\}$.

However, $h_i a = h_j a$ implies $h_i = h_j$; hence the k elements listed in Ha are distinct. Thus H and Ha have the same number of elements.

B.15. Prove Theorem B.7 (Lagrange): Let H be a subgroup of a finite group G. Then the order of H divides the order of G.

Suppose H has r elements and there are s right cosets; say

$$Ha_1, Ha_2, \ldots, Ha_s$$

By Theorem B.6, the cosets partition G and by Problem B.14, each coset has r elements. Therefore G has rs elements, and so the order of H divides the order of G.

B.16. Prove: Every subgroup of a cyclic group G is cyclic.

Since G is cyclic, there is an element $a \in G$ such that $G = gp(a)$. Let H be a subgroup of G. If $H = \{e\}$, then $H = gp(e)$ and H is cyclic. Otherwise, H contains a nonzero power of a. Since H is a subgroup, it must be closed under inverses and so H contains positive powers of a. Let m be the smallest positive power of a such that a^m belongs to H. We claim that $b = a^m$ generates H. Let x be any other element of H; since x belongs to G we have $x = a^n$ for some integer n. Dividing n by m we get a quotient q and a remainder r, that is,

$$n = mq + r$$

where $0 \leq r < m$. Then

$$a^n = a^{mq+r} = a^{mq} \cdot a^r = b^q \cdot a^r \quad \text{so} \quad a^r = b^{-q} a^n$$

But $a^n, b \in H$. Since H is a subgroup, $b^{-q} a^n \in H$, which means $a^r \in H$. However, m is the smallest positive power of a belonging to H. Therefore, $r = 0$. Hence $x = a^n = b^q$. Thus b generates H, and H is cyclic.

B.17. Prove Theorem B.8: Let H be a normal subgroup of a group G. Then the cosets of H in G form a group under coset multiplication defined by $(aH)\,(bH) = abH$.

Coset multiplication is well-defined, since

$$(aH)(bH) = a(Hb)H = a(bH)H = ab(HH) = abH$$

(Here we have used the fact that H is normal, so $Hb = bH$, and, from Problem B.57, that $HH = H$.) Associativity of coset multiplication follows from the fact that associativity holds in G. H is the identity element of G/H, since

$$(aH)H = a(HH) = aH \quad \text{and} \quad H(aH) = (Ha)H = (aH)H = aH$$

Lastly, $a^{-1}H$ is the inverse of aH since

$$(a^{-1}H)(aH) = a^{-1}aHH = eH = H \quad \text{and} \quad (aH)(a^{-1}H) = aa^{-1}HH = eH = H$$

Thus G/H is a group under coset multiplication.

B.18. Suppose $F : G \to G'$ is a group homomorphism. Prove: (*a*) $f(e) = e'$; (*b*) $(fa^{-6}) = f(a)^{-1}$.

(*a*) Since $e = ee$ and f is a homomorphism, we have

$$f(e) = f(ee) = f(e)f(e)$$

Multiplying both sides by $f(e)^{-1}$ gives us our result.

(*b*) Using part (a) and that $aa^{-1} = a^{-1}a = e$, we have

$$e' = f(e) = f(aa^{-1}) = f(a)f(a^{-1}) \quad \text{and} \quad e' = f(e) = f(a^{-1}a) = f(a^{-1})f(a)$$

Hence $f(a^{-1})$ is the inverse of $f(a)$; that is, $f(a^{-1}) = f(a)^{-1}$.

B.19. Prove Theorem B.9: Let $f : G \to G'$ be a homomorphism with kernel K. Then K is a normal subgroup of G, and G/K is isomorphic to the image of f. (Compare with Problem B.5, the analogous theorem for semigroups.)

Proof that K is normal: By Problem B.18, $f(e) = e'$, so $e \in K$. Now suppose $a, b \in K$ and $g \in G$. Then $f(a) = e'$ and $f(b) = e'$. Hence

$$\begin{aligned} f(ab) &= f(a)f(b) = e'e' = e' \\ f(a^{-1}) &= f(a)^{-1} = e'^{-1} = e' \\ f(gag^{-1}) &= f(g)f(a)f(g^{-1}) = f(g)e'f(g)^{-1} = e' \end{aligned}$$

Hence ab, a^{-1}, and gag^{-1} belong to K, so K is a normal subgroup.

Proof that $G/K \cong H$, where H is the image of f: Let φ: $G/K \to H$ be defined by

$$\varphi(Ka) = f(a)$$

We show that φ is well-defined, i.e., if $Ka = Kb$ then $\varphi(Ka) = \varphi(Kb)$. Suppose $Ka = Kb$. Then $ab^{-1} \in K$ (Problem B.57). Then $f(ab^{-1}) = e'$, and so

$$f(a)f(b)^{-1} = f(a)f(b^{-1}) = f(ab^{-1}) = e'$$

Hence $f(a) = f(b)$, and so $\varphi(Ka) = \varphi(Kb)$. Thus φ is well-defined.

We next show that φ is a homomorphism:

$$\varphi(KaKb) = \varphi(Kab) = f(ab) = f(a)f(b) = \varphi(Ka)\varphi(Kb)$$

Thus φ is a homomorphism. We next show that φ is one-to-one. Suppose $\varphi(Ka) = \varphi(Kb)$. Then

$$f(a) = f(b) \quad \text{or} \quad f(a)f(b)^{-1} = e' \quad \text{or} \quad f(a)f(b^{-1}) = e' \quad \text{or} \quad f(ab^{-1}) = e'$$

Thus $ab^{-1} \in K$, and by Problem B.57 we have $Ka = Kb$. Thus φ is one-to-one. We next show that φ is onto. Let $h \in H$. Since H is the image of f, there exists $a \in G$ such that $f(a) = h$. Thus $\varphi(Ka) = f(a) = h$, and so φ is onto. Consequently $G/K \cong H$ and the theorem is proved.

RINGS, INTEGRAL DOMAINS, FIELDS

B.20. Consider the ring $\mathbf{Z_{10}} = \{0, 1, 2, \ldots, 9\}$ of integers modulo 10. (*a*) Find the units of $\mathbf{Z_{10}}$. (*b*) Find -3, -8, and 3^{-1}. (*c*) Let $f(x) = 2x^2 + 4x + 4$. Find the roots of $f(x)$ over $\mathbf{Z_{10}}$.

(*a*) By Problem B.78 those integers relatively prime to the modulus $m = 10$ are the units in $\mathbf{Z}_{10}$. Hence the units are 1, 3, 7, and 9.

(*b*) Recall that $-a$ in a ring R is the element such that $a+(-a) = (-a)+a = 0$. Hence $-3 = 7$ since $3+7 = 7+3 = 0$ in $\mathbf{Z_{10}}$. Similarly $-8 = 2$. Recall that a^{-1} in a ring R is the element such that $a \cdot a^{-1} = a^{-1} \cdot a = 1$. Hence $3^{-1} = 7$ since $3 \cdot 7 = 7 \cdot 3 = 1$ in $\mathbf{Z_{10}}$.

(*c*) Substitute each of the ten elements of $\mathbf{Z_{10}}$ into $f(x)$ to see which elements yield 0. We have:

$$f(0) = 4, \quad f(2) = 0, \quad f(4) = 2, \quad f(6) = 0, \quad f(8) = 4$$
$$f(1) = 0, \quad f(3) = 4, \quad f(5) = 4, \quad f(7) = 0, \quad f(9) = 2$$

Thus the roots are 1, 2, 6, and 7. (This example shows that a polynomial of degree n can have more than n roots over an arbitrary ring. This cannot happen if the ring is a field.)

B.21. Prove that in a ring R: (i) $a \cdot 0 = 0 \cdot a = 0$; (ii) $a(-b) = (-a)b = -ab$; (iii) $(-1)a = -a$ (when R has an identity element 1).

(i) Since $0 = 0 + 0$, we have

$$a \cdot 0 = a(0 + 0) = a \cdot 0 + a \cdot 0$$

Adding $-(a \cdot 0)$ to both sides yields $0 = a \cdot 0$. Similarly $0 \cdot a = 0$.

(ii) Using $b + (-b) = (-b) + b = 0$, we have

$$ab + a(-b) = a(b + (-b)) = a \cdot 0 = 0$$
$$a(-b) + ab = a((-b) + b) = a \cdot 0 = 0$$

Hence $a(-b)$ is the negative of ab; that is, $a(-b) = -ab$. Similarly, $(-a)b = -ab$.

(iii) We have

$$a + (-1)a = 1 \cdot a + (-1)a = (1 + (-1))a = 0 \cdot a = 0$$
$$(-1)a + a = (-1)a + 1 \cdot a = ((-1) + 1)a = 0 \cdot a = 0$$

Hence $(-1)a$ is the negative of a; that is, $(-1)a = -a$.

B.22. Let D be an integral domain. Show that if $ab = ac$ with $a \neq 0$ then $b = c$.

Since $ab = ac$, we have

$$ab - ac = 0 \quad \text{and so} \quad a(b - c) = 0$$

Since $a \neq 0$, we must have $b - c = 0$, since D has no zero divisors. Hence $b = c$.

B.23. Suppose J and K are ideals in a ring R. Prove that $J \cap K$ is an ideal in R.

Since J and K are ideals, $0 \in J$ and $0 \in K$. Hence $0 \in J \cap K$. Now let $a, b \in J \cap K$ and let $r \in R$. Then $a, b \in J$ and $a, b \in K$. Since J and K are ideals,

$$a - b, ra, ar \in J \quad \text{and} \quad a - b, ra, ar \in K$$

Hence $a - b, ra, ar \in J \cap K$. Therefore $J \cap K$ is an ideal.

B.24. Let J be an ideal in a ring R with an identity element 1. Prove: (*a*) If $1 \in J$ then $J = R$; (*b*) If any unit $u \in J$ then $J = R$.

(*a*) If $1 \in J$ then for any $r \in R$ we have $r \cdot 1 \in R$ or $r \in J$. Hence $J = R$.

(*b*) If $u \in J$ then $u^{-1} \cdot u \in J$ or $1 \in J$. Hence $J = R$ by part (a).

B.25. Prove: (*a*) A finite integral domain D is a field. (*b*) $\mathbf{Z_p}$ is a field where p is a prime number. (*c*) (Fermat) If p is prime, then $a^p \equiv a \pmod{p}$ for any integer a.

(*a*) Suppose D has n elements, say $D = \{a_1, a_2, \ldots, a_n\}$. Let a be any nonzero element of D. Consider the n elements

$$aa_1, aa_2, \ldots, a_n$$

Since $a \neq 0$, we have $aa_i = aa_k$ implies $a_i = a_k$ (Problem B.22). Thus the above n elements are distinct, and so they must be a rearrangement of the elements of D. One of them, say aa_k, must equal the identity element 1 of D; that is, $aa_k = 1$. Thus a_k is the inverse of a. Since a was any nonzero element of D, we have that D is a field.

(*b*) Recall $\mathbf{Z_p} = \{0, 1, 2, \ldots, p - 1\}$. We show that $\mathbf{Z_p}$ has no zero divisors. zero divisors. Suppose a $*b = 0$ in $\mathbf{Z_p}$; that is, 0 (mod p). Then p divides ab. Since p is prime, p divides a or p divides b. Thus $a \equiv 0 \pmod{p}$ or $b \equiv 0 \pmod{p}$; that is, $a = 0$ or $b = 0$ in $\mathbf{Z_p}$. Accordingly, $\mathbf{Z_p}$ has no zero divisors and hence $\mathbf{Z_p}$ is an integral domain. By part (a), $\mathbf{Z_p}$ is a field.

(*c*) If p divides a, then $a \equiv 0 \pmod{p}$ and so $a^p \equiv a \equiv 0 \pmod{p}$. Suppose p does not divide a, then a may be viewed as a nonzero element of $\mathbf{Z_p}$ is a field, its nonzero elements form a group G under multiplication of order $p - 1$. By Problem B.45, $a^{p-1} = 1$ in $\mathbf{Z_p}$.

In other words, $a^{p-1} \equiv 1 \pmod{p}$. Multiplying by a gives $a^p \equiv a \pmod{p}$, and the theorem is proved.

POLYNOMIALS OVER A FIELD

B.26. Suppose $f(t) = 2t^3 - 3t^2 - 6t - 2$. Find all the roots of $f(t)$ knowing that $f(t)$ has a rational root.

The rational roots of $f(t)$ must be among $\pm 1, \pm 2, \pm 1/2$. Testing each possible root, we get, by synthetic division (or dividing by $2t + 1$),

$$\begin{array}{r|l} -\frac{1}{2} & 2 - 3 - 6 - 2 \\ & \quad -1 + 2 + 2 \\ \hline & 2 - 4 - 4 + 0 \end{array}$$

Therefore $t = -1/2$ is a root and

$$f(t) = (t + 1/2)(2t^2 - 4t - 4) = (2t + 1)(t^2 - 2t - 2)$$

We can now use the quadratic formula on $t^2 - 2t - 2$ to obtain the following three roots of $f(t)$:

$$t = -1/2, \quad t = 1 + \sqrt{3}, \quad t = 1 - \sqrt{3}$$

B.27. Let $f(t) = t^4 - 3t^3 + 3t^2 + 3t - 20$. Find all the roots of $f(t)$ given that $t = 1 + 2i$ is a root.

Since $1 + 2i$ is a root, then $1 - 2i$ is a root and $c(t) = t^2 - 2t + 5$ is a factor of $f(t)$. Dividing $f(t)$ by $c(t)$ we get

$$f(t) = (t^2 - 2t + 5)(t^2 - t - 4)$$

The quadratic formula with $t^2 - t - 4$ gives us the other roots of $f(t)$. That is, the four roots of $f(t)$ follow:

$$t = 1 + 2i, \quad t = 1 - 2i, \quad t = (1 + \sqrt{17})/2, \quad t = (1 - \sqrt{17})/2$$

B.28. Let $K = \mathbf{Z_8}$. Find all roots of $f(t) = t^2 + 6t$.

Here $\mathbf{Z_8} = \{0, 1, 2, \ldots, 7\}$. Substitute each element of $\mathbf{Z_8}$ into $f(t)$ to obtain:

$$f(0) = 0, \quad f(2) = 0, \quad f(4) = 0, \quad f(6) = 0$$

Then $f(t)$ has four roots, $t = 0, 2, 4, 6$. (Theorem B.21 does not hold here since K is not a field.)

B.29. Suppose $f(t)$ is a real polynomial with odd degree n. Show that $f(t)$ has a real root.

The complex (nonreal) roots come in pairs. Since $f(t)$ has an odd number n of roots (counting multiplicity), $f(t)$ must have at least one real root.

B.30. Prove Theorem B.15 (Euclidean Division Algorithm): Let $f(t)$ and $g(t)$ be polynomials over a field K with $g(t) \neq 0$. Then there exist polynomials $q(t)$ and $r(t)$ such that

$$f(t) = q(t)g(t) + r(t)$$

where either $r(t) \equiv 0$ or $\deg(r) < \deg(g)$.

If $f(t) = 0$ or if $\deg(f) < \deg(g)$, then we have the required representation $f(t) = 0g(t) + f(t)$. Now suppose $\deg(f) \geq \deg(g)$, say

$$f(t) = a_n t^n + \cdots + a_1 t + a_0 \quad \text{and} \quad g(t) = b_m t^m + \cdots + b_1 t + b_0$$

where $a_n, b_m \neq 0$ and $n > m$. We form the polynomial

$$f_1(t) = f(t) - \frac{a_n}{b_m} t^{n-m} g(t) \tag{1}$$

(This is the first subtraction step in "long division.") Then $\deg(f_1) < \deg(f)$. By induction, there exist polynomials $q_1(t)$ and $r(t)$ such that $f_1(t) = q_1(t)g(t) + r(t)$ where either $r(t) \equiv 0$ or $\deg(r) < \deg(g)$. Substituting this into (1) and solving for $f(t)$, we get

$$f(t) = \left[q_1(t) + \frac{a_n}{b_m} t^{n-m}\right] g(t) + r(t)$$

which is the desired representation.

B.31. Prove Theorem B.18: Suppose $f(t)$ is a polynomial over a field K, and $\deg(f) = n$. Then $f(t)$ has at most n roots.

The proof is by induction on n. If $n = 1$, then $f(t) = at + b$ and $f(t)$ has the unique root $t = -b/a$. Suppose $n > 1$. If $f(t)$ has no roots, then the theorem is true. Suppose $a \in K$ is a root of $f(t)$. Then

$$f(t) = (t - a)g(t) \tag{1}$$

where $\deg(g) = n - 1$. We claim that any other root of $f(t)$ must also be a root of g(t).

Suppose $b \neq a$ is another root of $f(t)$. Substituting $t = b$ in (1) yields $0 = f(b) = (b - a)g(b)$.

Since K has no zero divisors and $b - a \neq 0$, we must have $g(b) = 0$. By induction, $g(t)$ has at most $n - 1$ roots. Thus $f(t)$ has at most $n - 1$ roots other than a. Thus $f(t)$ has at most n roots.

B.32. Prove Theorem B.19: Suppose a rational number p/q (reduced to lowest terms) is a root of the polynomial

$$f(t) = a_n t^n + \cdots + a_1 t + a_0$$

where all the coefficients $a_n, \ldots, a_1, a_0$ are integers. Then p divides the constant term a_0 and q divides the leading coefficients a_n. In particular, if $c = p/q$ is an integer, then c divides the constant term a_0.

Substitute $t = p/q$ into $f(t) = 0$ to obtain $a_n(p/q)^n + \cdots + a_1(p/q) + a_0 = 0$. Multiply both sides of the equation by q^n to obtain

$$a_n p^n + a_{n-1} p^{n-1} q + a_{n-2} p^{n-2} q^2 + \cdots + a_1 p q^{n-1} + a_0 q^n = 0 \tag{1}$$

Since p divides all of the first n terms of (1), p must divide the last term $a_0 q^n$. Assuming p and q are relatively prime, p divides a_0. Similarly, q divides the last n terms of (1), hence q divides the first term $a_n p^n$. Since p and q are relatively prime, q divides a_n.

B.33. Prove Theorem B.20: The ring $K[t]$ of polynomials over a field K is a principal ideal domain (PID). If J is an ideal in $K[t]$, then there exists a unique monic polynomial d which generates J, that is, every polynomial f in J is a multiple of d.

Let d be a polynomial of lowest degree in J. Since we can multiply d by a nonzero scalar and still remain in J, we can assume without loss in generality that d is a monic polynomial (leading coefficient equal 1). Now suppose $f \in J$. By the division algorithm there exist polynomials q and r such that $f = qd + r$ where either $r \equiv 0$ or $\deg(r) < \deg(d)$. Now $f, d \in J$ implies $qd \in J$ and hence $r = f - qd \in J$. But d is a polynomial of lowest degree in J. Accordingly, $r \equiv 0$ and $f = qd$, that is, d divides f. It remains to show that d is unique. If d' is another monic polynomial which generates J, then d divides d' and d' divides d. This implies that $d = d'$, because d and d' are monic. Thus the theorem is proved.

B.34. Prove Theorem B.21: Let f and g be polynomials in $K[t]$, not both the zero polynomial. Then there exists a unique monic polynomial d such that: (i) d divides both f and g. (ii) If d' divides f and g, then d' divides d.

The set $I = \{mf + ng \mid m, n \in K[t]\}$ is an ideal. Let d be the monic polynomial which generates I. Note $f, g \in I$; hence d divides f and g. Now suppose d' divides f and g. Let J be the ideal generated by d'. Then $f, g \in J$ and hence $I \subseteq J$. Accordingly, $d \in J$ and so d' divides d as claimed. It remains to show that d is unique. If d_1 is another (monic) greatest common divisor of f and g, then d divides d_1 and d_1 divides d. This implies that $d = d_1$ because d and d_1 are monic. Thus the theorem is proved.

B.35. Prove Corollary B.22: Let d be the greatest common divisor of f and g. Then there exist polynomials m and n such that $d = mf + ng$. In particular, if f and g are relatively prime, then there exist polynomials m and n such that $mf + ng = 1$.

From the proof of Theorem B.21 in Problem B.34, the greatest common divisor d generates the ideal $I = \{mf + ng \mid m, n \in K[t]\}$. Thus there exist polynomials m and n such that $d = mf + ng$.

B.36. Prove Lemma B.23: Suppose $p \in K[t]$ is irreducible. If p divides the product fg of polynomials $f, g \in K[t]$, then p divides f or p divides g. More generally, if p divides the product $f_1 f_2 \cdots f_n$ of n polynomials, then p divides one of them.

Suppose p divides fg but not f. Since p is irreducible, the polynomials f and p must then be relatively prime. Thus there exist polynomials $m, n \in K[t]$ such that $mf + np = 1$. Multiplying this equation by g, we obtain $mfg + npg = g$. But p divides fg and so p divides mfg. Also, p divides npg. Therefore, p divides the sum $g = mfg + npg$.

Now suppose p divides $f_1 f_2 \cdots f_n$. If p divides f_1, then we are through. If not, then by the above result p divides the product $f_2 \cdots f_n$. By induction on n, p divides one of the polynomials in the product $f_2 \cdots f_n$. Thus the lemma is proved.

B.37. Prove Theorem B.24 (Unique Factorization Theorem): Let f be a nonzero polynomial in $K[t]$. Then f can be written uniquely (except for order) as a product $f = kp_1 p_2 \cdots p_n$ where $k \in K$ and the p's are monic irreducible polynomials in $K[t]$.

We prove the existence of such a product first. If f is irreducible or if $f \in K$, then such a product clearly exists. On the other hand, suppose $f = gh$ where g and h are nonscalars. Then g and h have degrees less than that of f. By induction, we can assume $g = k_1 g_1 g_2 \cdots g_r$ and $h = k_2 h_1 h_2 \cdots h_s$ where $k_1, k_2 \in K$ and the g_i and h_j are monic irreducible polynomials. Accordingly, our desired representation follows:

$$f = (k_1 k_2) g_1 g_2 \cdots g_r h_1 h_2 \cdots h_s$$

We next prove uniqueness (except for order) of such a product for f. Suppose

$$f = kp_1 p_2 \ldots p_n = k' q_1 q_2 \ldots q_m \quad \text{where} \quad k, k' \in K$$

and the $p_1, \ldots, p_n, q_1, \ldots, q_m$ are monic irreducible polynomials. Now p_1 divides $k'q_1 \ldots q_m$. Since p_1 is irreducible it must divide one of the q's by Lemma B.23. Say p_1 divides q_1. Since p_1 and q_1 are both irreducible and monic, $p_1 = q_1$. Accordingly, $kp_2 \ldots p_n = k' q_2 \ldots q_m$. By induction, we have that $n = m$ and $p_2 = q_2, \ldots, p_n = q_m$ for some rearrangement of the q's. We also have that $k = k'$. Thus the theorem is proved.

B.38. Prove Theorem B.25: Suppose $f(t)$ is a polynomial over the real field R, and suppose the complex number $z = a + bi$, $b \neq 0$, is a root of $f(t)$. Then the complex conjugate $\bar{z} = a - bi$ is also a root of $f(t)$. Hence the following is a factor of $f(t)$:

$$c(t) = (t - z)(t - \bar{z}) = t^2 - 2at + a^2 + b^2$$

Dividing $f(t)$ by $c(t)$ where $\deg(c) = 2$, there exist $q(t)$ and real numbers M and N such that

$$f(t) = c(t)q(t) + Mt + N \tag{1}$$

Since $z = a + bi$ is a root of $f(t)$ and $c(t)$, we have, by substituting $t = a + bi$ in (1),

$$f(z) = c(z)q(z) + M(z) + n \quad \text{or} \quad 0 = 0q(z) + M(z) + N \quad \text{or} \quad M(a + bi) + N = 0$$

Thus $Ma + N = 0$ and $Mb = 0$. Since $b \neq 0$, we must have $M = 0$. Then $0 + N = 0$ or $N = 0$. Accordingly, $f(t) = c(t)q(t)$ and $\bar{z} = a - bi$ is a root of $f(t)$.

Supplementary Problems

OPERATIONS AND SEMIGROUPS

B.39. Consider the set **N** of positive integers, and let $*$ denote least common multiple (lcm) operation on N.

(a) Find $4 * 6$, $3 * 5$, $9 * 18$, $1 * 6$.

(b) Is $(\mathbf{N}, *)$ a semigroup? Is it commutative?

(c) Find the identity element of $*$.

(d) Which elements in N, if any, have inverses and what are they?

B.40. Let $*$ be the operation on the set **R** of real numbers defined by $a * b = a + b + 2ab$.

(a) Find $2 * 3$, $3 * (-5)$, and $7 * (1/2)$. (b) Is $(\mathbf{R}, *)$ a semigroup? Is it commutative?

(c) Find the identity element of $*$. (d) Which elements have inverses and what are they?

B.41. Let A be a nonempty set with the operation $*$ defined by $a * b = a$, and assume A has more than one element.

(a) Is A a semigroup? (c) Does A have an identity element?

(b) Is A commutative? (d) Which elements, if any, have inverses and what are they?

B.42. Let $A = \{a, b\}$. (a) Find the number of operations on A. (b) Exhibit one which is neither associative nor commutative.

B.43. For each of the following sets, state which are closed under: (a) multiplication; (b) addition.

$$A = \{0, l\}, \quad B = \{1, 2\}, \quad C = \{x \mid x \text{ is prime}\}, \quad D = \{2, 4, 8, \ldots\} = \{x \mid x = 2^n\}.$$

B.44. Let $A = \{\ldots, -9, -6, -3, 0, 3, 6, 9, \ldots\}$, the multiples of 3. Is A closed under:

(a) addition; (b) multiplication; (c) subtraction; (d) division (except by 0)?

B.45. Find a set A of three integers which is closed under: (a) multiplication; (b) addition.

B.46. Let S be an infinite set. Let A be the collection of finite subsets of S and let B be the collection of infinite subsets of S

(a) Is A closed under: (i) union; (ii) intersection; (iii) complements?

(b) Is B closed under: (i) union; (ii) intersection; (iii) complements?

B.47. Let $S = \mathbf{Q} \times \mathbf{Q}$, the set of ordered pairs of rational numbers, with the operation $*$ defined by

$$(a, b) * (x, y) = (ax, ay + b)$$

(a) Find $(3, 4) * (1, 2)$ and $(-1, 3) * (5, 2)$. (c) Find the identity element of S.

(b) Is S a semigroup? Is it commutative? (d) Which elements, if any, have inverses and what are they?

B.48. Let $S = \mathbf{N} \times N$, the set of ordered pairs of positive integers, with the operation $*$ defined by

$$(a, b) * (c, d) = (ad + bc, bd)$$

(a) Find $(3, 4) * (1, 5)$ and $(2, 1) * (4, 7)$.

(b) Show that $*$ is associative. (Hence that S is a semigroup.)

(c) Define $f : (S, *) \to (\mathbf{Q}, +)$ by $f(a, b) = a/b$. Show that f is a homomorphism.

(d) Find the congruence relation $\sim$ in S determined by the homomorphism f, that is, $x \sim y$ if $f(x) = f(y)$.

(e) Describe $S/\sim$. Does $S/\sim$ have an identity element? Does it have inverses?

B.49. Let $S = \mathbf{N} \times \mathbf{N}$. Let $*$ be the operation on S defined by

$$(a, b) * (a', b') = (a + a', b + b')$$

(a) Find $(3, 4) * (1, 5)$ and $(2, 1) * (4, 7)$.

(b) Show that $*$ is associative. (Hence that S is a semigroup.)

(c) Define $f: (S, *) \to (\mathbf{Z}, +)$ by $f(a, b) = a - b$. Show that f is a homomorphism.

(d) Find the congruence relation $\sim$ in S determined by the homomorphism f.

(e) Describe $S/\sim$. Does $S/\sim$ have an identity element? Does it have inverses?

GROUPS

B.50. Consider $\mathbf{Z}_{20} = \{0, 1, 2, \ldots, 19\}$ under addition modulo 20. Let H be the subgroup generated by 5. (a) Find the elements and order of H. (b) Find the cosets of H in $\mathbf{Z}_{20}$.

B.51. Consider $G = \{1, 5, 7, 11\}$ under multiplication modulo 12. (a) Find the order of each element. (b) Is G cyclic? (c) Find all subgroups of G.

B.52. Consider $G = \{1, 5, 7, 11, 13, 17\}$ under multiplication modulo 18. (a) Construct the multiplication table of G. (b) Find 5^{-1}, 7^{-1}, and 17^{-1}. (c) Find the order and group generated by: (i) 5; (ii) 13; (d) Is G cyclic?

B.53. Consider the symmetric group S_4. Let $\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 2 & 1 \end{pmatrix}$ and $\beta = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 3 & 1 \end{pmatrix}$.

(a) Find $\alpha\beta$, $\beta\alpha$, α^2, α^{-1}. (b) Find the orders of α, β, and $\alpha\beta$.

B.54. Prove the following results for a group G.

(a) The identity element e is unique.

(b) Each a in G has a unique inverse a^{-1}.

(c) $(a^{-1})^{-1} = a$, $(ab)^{-1} = b^{-1}a^{-1}$, and, more generally, $(a_r a_2 \ldots a_n) = a_n^{-1} \ldots a_2^{-1} a_1^{-1}$.

(d) $ab = ac$ implies $b = c$, and $ba = ca$ implies $b = c$.

(e) For any integers r and s, we have $a^r a^s = a^{r+s}$, $(a^r)^s = a^{rs}$.

(f) G is abelian if and only if $(ab)^2 = a^2 b^2$ for all $a, b \in G$.

B.55. Let H be a subgroup of G. Prove: (a) $H = Ha$ if and only if $a \in H$. (b) $Ha = Hb$ if and only if $ab^{-1} \in H$, (c) $HH = H$.

B.56. Prove Proposition B.5: *A* subset H of a group G is a subgroup of G if: (i) $e \in H$, (ii) for all $a, b \in H$, we have $ab, a^{-1} \in H$.

B.57. Let G be a group. Prove:

(a) The intersection of any number of subgroups of G is a subgroup of G.

(b) For any $A \subseteq G$, $gp(A)$ is equal to the intersection of all subgroups of G containing A.

(c) The intersection of any number of normal subgroups of G is a normal subgroup of G.

B.58. Suppose G is an abelian group. Show that any factor group G/H is also abelian.

B.59. Suppose $|G| = p$, where p is a prime. Prove: (a) G has no subgroups except G and $\{e\}$. (b) G is cyclic and every element $a \neq e$ generates G.

B.60. Show that $G = \{1, -1, i, -i\}$ is a group under multiplication, and show that $G \cong \mathbf{Z_4}$ by giving an explicit isomorphism $f: G \to \mathbf{Z_4}$.

B.61. Let H be a subgroup of G with only two right cosets. Show that H is normal.

B.62. Let $S = \mathbf{R^2}$, the Cartesian plane. Find the stabilizer H_a of $a = (1, 0)$ in S where G is the following group acting on S:

(a) $G = \mathbf{Z} \times \mathbf{Z}$ and G acts on S by $g(x, y) = (x + m, y + n)$ where $g = (m, n)$. That is, each element g in G is a translation of S.

(b) $G = (\mathbf{R}, +)$ and G acts on S by $g(x, y) = (x\cos g - y\sin g, x\sin g + y\cos g)$. That is, each element in G rotates S about the origin by an angle g.

B.63. Let S be the regular polygon with n sides, and let G be the group of symmetries of S.

(a) Find the order of G.

(b) Show that G is generated by two elements a and b such that $a^n = e$, $b^2 = e$, and $b^{-1}ab = a^{-1}$. (G is called the *dihedral group*.)

B.64. Suppose a group G acts on a set S, say by the homomorphism $\psi: \to \mathrm{PERM}(S)$.

(a) Prove that, for any $s \in S$: (i) $e(s) = s$, and (ii) $(gg')(s) = g(g'(s))$ where $g, g' \in G$.

(b) The orbit G_s of any $s \in S$ is defined by $G_s = \{g(s) \mid g \in G\}$. Show that the orbits form a partition of S.

(c) Show that $|G_s| =$ the number of cosets of the stabilizer H_s of s in G. (Recall $H_s = \{g \in G \mid g(s) \in s\}$.)

B.65. Let G be an abelian group and let n be a fixed positive integer. Show that the function $f: G \to G$ defined by $f(a) = a^n$ is a homomorphism.

B.66. Let G be the multiplicative group of complex numbers z such that $|z| = 1$, and let $\mathbf{R}$ be the additive group of real numbers. Prove $G \cong \mathbf{R}/\mathbf{Z}$.

B.67. Suppose H and N are subgroups of G with N normal. Show that: (a) HN is a subgroup of G. (b) $H \cap N$ is a normal subgroup of H. (c) $H/(H \cap N) \cong HN/N$.

B.68. Let H and K be groups. Let G be the product set $H \times K$ with the operation

$$(h, k) * (h', k') = (hh', kk').$$

(a) Show that G is a group (called the *direct product* of H and K).

(b) Let $H' = H \times \{e\}$. Show that: (i) $H' \cong H$; (ii) H' is a normal subgroup of G; (iii) $G/H' \cong K$.

RINGS

B.69. Consider the ring $\mathbf{Z}_{12} = \{0, 1, \ldots, 11\}$ of integers modulo 12. (a) Find the units of $\mathbf{Z}_{12}$. (b) Find the roots of $f(x) = x^2 + 4x + 4$ over $\mathbf{Z}_{12}$. (c) Find the associates of 2.

B.70. Consider the ring $\mathbf{Z}_{30} = \{0, 1, \ldots, 29\}$ of integers modulo 30.

(a) Find -2, -7, and -11. (b) Find: 7^{-1}, 11^{-1}, and 26^{-1}.

B.71. Show that in a ring R: (a) $(-a)(-b) = ab$; (b) $(-1)(-1) = 1$, if R has an identity element 1.

B.72. Suppose $a^2 = a$ for every $a \in R$. (Such a ring is called a *Boolean* ring). Prove that R is commutative.

B.73. Let R be a ring with an identity element 1. We make R into another ring R' by defining:

$$a \oplus b = a + b + 1 \quad \text{and} \quad a * b = ab + a + b$$

(a) Verify that R' is a ring. (b) Determine the 0-element and the 1-element of R'.

B.74. Let G be any (additive) abelian group. Define a multiplication in G by $a * b = 0$ for every $a, b \in G$. Show that this makes G into a ring.

B.75. Let J and K be ideals in a ring R. Prove that $J + K$ nd $J \cap K$ are also ideals.

B.76. Let R be a ring with unity 1. Show that $(a) = \{ra \mid r \in R\}$ is the smallest ideal containing a.

B.77. Show that R and $\{0\}$ are ideals of any ring R.

B.78. Prove: (a) The units of a ring R form a group under multiplication. (b) The units in $\mathbf{Z}_m$ are those integers which are relatively prime to m.

B.79. For any positive integer m, verify that $m\mathbf{Z} = \{\text{rm} \mid r \in \mathbf{Z}\}$ is a ring. Show that $2\mathbf{Z}$ and $3\mathbf{Z}$ are not isomorphic.

B.80. Prove Theorem B.10: Let J be an ideal in a ring R. Then the cosets $\{a + J \mid a \in R\}$ form a ring under the coset operations $(a + J) + (b + J) = a + b + J$ and $(a + J)(b + J) = ab + J$.

B.81. Prove Theorem B.11: Let $f: R \to R'$ be a ring homomorphism with kernel K. Then K is an ideal in R, and the quotient ring R/K is isomorphic to $f(R)$.

B.82. Let J be an ideal in a ring R. Consider the (canonical) mapping $f: R \to R/J$ defined by $f(a) = a + J$. Show that: (a) f is a ring homomorphism; (b) f is an onto mapping.

B.83. Suppose J is an ideal in a ring R. Show that: (a) If R is commutative, then R/J is commutative. (b) If R has a unity element 1 and $1 \notin J$, then $1 + R$ is a unity element for R/J.

INTEGRAL DOMAINS AND FIELDS

B.84. Prove that if $x^2 = 1$ in an integral domain D, then $x = -1$ or $x = 1$.

B.85. Let $R \neq \{0\}$ be a finite commutative ring with no zero divisors. Show that R is an integral domain, that is, that R has an identity element 1.

B.86. Prove that $F = \{a + b\sqrt{2} \mid a, b \text{ rational}\}$ is a field.

B.87. Prove that $F = \{a + b\sqrt{2} \mid a, b \text{ integers}\}$ is an integral domain but not a field.

B.88. A complex number $a + bi$ where a, b are integers is called a *Gaussian integer*. Show that the set G of Gaussian integers is an integral domain. Also show that the units are ± 1, $\pm i$.

B.89. Let R be an integral domain and let J be an ideal in R. Prove that the factor ring R/J is an integral domain if and only if J is a prime ideal. (An ideal J is *prime* if $J \neq R$ and if $ab \in J$ implies $a \in J$ or $b \in J$.)

B.90. Let R be a commutative ring with unity element 1, and let J be an ideal in R. Prove that the factor ring R/J is a field if and only if J is a maximal ideal. (An ideal J is maximal if $J \neq R$ and no ideal K lies strictly between J and R, that is, if $J \subseteq K \subseteq R$ then $J = K$ or $K = R$.)

B.91. Let D be the ring of real 2×2 matrices of the form $\begin{bmatrix} a & -b \\ b & a \end{bmatrix}$. Show that D is isomorphic to the complex field C, when D is a field.

B.92. Show that the only ideal in a field K is $\{0\}$ or K itself.

B.93. Suppose $f: K \to K'$ is a homomorphism from a field K to a field K'. Show that f is an *embedding*; that is, f is one-to-one. (We assume $f(1) \neq 0$.)

B.94. Consider the integral domain $D = \{a + b\sqrt{13} \mid a, b \text{ integers}\}$. (See Example B.15(*b*).) If $\alpha = a + \sqrt{13}$, we define $N(\alpha) = a^2 - 13b^2$. Prove:

(i) $N(\alpha\beta) = N(\alpha)N(\beta)$.

(ii) α is a unit if and only if $N(\alpha) = +1$.

(iii) Among the units of D are ± 1, $18 \pm 5\sqrt{13}$; and $-18 \pm 5\sqrt{13}$.

(iv) The numbers 2, $3 - \sqrt{13}$ and $-3 - \sqrt{13}$ are irreducible.

POLYNOMIALS OVER A FIELD

B.95. Find the roots of $f(t)$ assuming $f(t)$ has an integer root: (a) $f(t) = t^3 - 2t^2 - 6t - 3$; (b) $f(t) = t^3 - t^2 - 11t - 10$; (c) $f(t) = t^3 + 2t^2 - 13t - 6$.

B.96. Find the roots of $f(t)$ assuming $f(t)$ has a rational root: (a) $f(t) = 2t^3 - 3t^2 - 16t - 7$; (b) $f(t) = 2t^3 - t^2 - 9t + 9$.

B.97. Find the roots of $f(t) = t^4 - 5t^3 + 16t^2 - 9t - 13$, given that $t = 2 + 3i$ is a root.

B.98. Find the roots of $f(t) = t^4 - t^3 - 5t^2 + 12t - 10$, given that $t = 1 - i$ is a root.

B.99. For any scalar $a \in K$, define the *evaluation map* $\psi_a\colon K[t] \to K$ by $\psi_a(f(t)) = f(a)$. Show that ψ_a is a ring homomorphism.

B.100. Prove: (a) Proposition B.14. (b) Theorem B.26.

Answers to Supplementary Problems

B.39. (a) 12, 15, 18, 6; (b) Yes, yes; (c) 1; (d) Only 1 and it is its own inverse.

B.40. (a) 17, -32, 29/2; (b) Yes, yes; (c) Zero; (d) If $a \neq 1/2$, then a has an inverse which is $-a/(1 + 2a)$.

B.41. (a) Yes; (b) No; (c) No; (d) It is meaningless to talk about inverses when no identity element exists.

B.42. (a) Sixteen, since there are two choices, a or b, for each of the four products aa, ab, ba, and bb. (b) Let $aa = b$, $ab = a$, $ba = b$, $bb = a$. Then $ab \neq ba$. Also, $(aa)b = bb = a$, but $a(ab)\ as = b$.

B.43. (a) A, D; (b) none.

B.44. (a) Yes; (b) yes; (c) yes; (d) no.

B.45. (a) $\{1, -1, 0\}$; (b) There is no set.

B.46. (a) Yes, yes, no; (b) Yes, no, no.

B.47. (a) (3, 10), $(-5, 1)$; (b) yes, no; (c) (1, 0); (d) The element (a, b) has an inverse if $a \neq 0$, and its inverse is $(1/a, -b/a)$.

B.48. (a) (19, 20), (18, 7). (d) $(a, b) \sim (c, d)$ if $ad = bc$. (e) $S/\sim$ is isomorphic to the positive rational numbers under addition. Thus $S/\sim$ has no identity element and no inverses.

B.49. (a) (4, 9), (6, 8); (d) $(a, b) \sim (c, d)$ if $a + d = b + c$. (e) $S/\sim$ is isomorphic $\mathbf{Z}$ since every integer is the difference of two positive integers. Thus $S/\sim$ has an identity element, and every element has an inverse.

B.50. (a) $H = l\{0, 5, 10, 15\}$ and $|H| = 4$. (b) H, $1 + H = \{1, 6, 11, 16\}$, $2 + H = \{2, 7, 12, 17\}$, $3 + H = \{3, 8, 13, 18\}$, $4 + H = \{4, 9, 14, 19\}$.

B.51. (a) $x^2 = 1$ if $x \neq 1$. (b) No. (c) $\{1\}$, $\{1, 5\}$, $\{1, 7\}$, $\{1, 11\}$, G.

B.52. (a) See Fig. B-9(*a*). (b) 11, 13, 17; (c) (i) $|\%| = 6$, $gp(5) = G$; (ii) $|13| = 3$, $gp(13) = \{1, 7, 13\}$; (d) Yes, since $G = gp(5)$.

B.53. (a) See Fig. B-9(*b*). (b) 4, 3, 4.

$\times$	1	5	7	11	13	17
1	1	5	7	11	13	17
5	5	7	17	1	11	13
7	7	17	13	5	1	11
11	11	1	5	13	17	7
13	13	11	1	17	7	5
17	17	13	11	7	5	1

(*a*)

$$\alpha\beta = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 4 & 2 \end{pmatrix}, \quad \beta\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{pmatrix}$$

$$\alpha^2 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}, \quad \alpha^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 1 & 2 \end{pmatrix}$$

(*b*)

Fig. B-9

B.60. $f(1) = 0$, $f(i) = 1$, $f(-1) = 2$, $f(-i) = 3$

B.62. (a) $\{(0, 0)\}$, (b) $\{2\pi r \mid r \in Z\}$.

B.69. (a) 1, 5, 7, 11; (b) 4, 10; (c) $\{2, 10\}$.

B.70. (a) 28, 23, 19; (b) 13, 11, 26^{-1} does not exist since 26 is not a unit.

B.72. Show $-a = a$ using $a + a = (a + a)^2$. Then show $ab = -ba$ by $(a + b) = (a + b)^2$.

B.73. (b) $-1 =$ 0−element, $0 =$ 1−element.

B.91. Show f is an isomorphism where $f\left(\begin{bmatrix} a & -b \\ b & a \end{bmatrix}\right) = a + bi$.

B.93. *Hint*: Use Problem B.92.

B.95. (a) -1, $(3 \pm \sqrt{21})/2$; (b) -2, $(3 \pm \sqrt{29})/2$; (c) 3, $(-5 \pm \sqrt{17})/2$

B.96. (a) $-1/2$, $1 \pm 2\sqrt{2}$; (b) 3/2, $(-1 \pm \sqrt{13})/2$

B.97. 2 ± 3i, $(1 \pm \sqrt{5})/2$

B.98. $1 \pm$ i, $(-1 \pm \sqrt{21})/2$