Algebraic Structure

A non-empty set G equipped with one or more binary operations is said to be an algebraic structure. Suppose * is a binary operation on G. Then (G, *) is an algebraic structure. (N,*), (1, +), (1, -) are all the algebraic structure. Here, (R, +, .) is an algebraic structure equipped with two operations.

Binary Operation on A Set

Suppose **G** is a non-empty set. The **G X G = {(a,b) : a E G, b E G)}**. If **f : G X G → G** then **f** is called a binary operation on a set **G**. The image of the ordered pair **(a,b)** under the function **f** is denoted by **afb**.

A binary operation on asset **G** is sometimes also said to be the binary composition in the set **G**. If ***** is a binary composition in **G** then, **a * b E G, a, b E G**. Therefore **g** is closed with respect to the composition denoted by *****.

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:

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

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 × S into S. In such a case, instead of * (a, b), we usually write

a * b or sometimes 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 × 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 **Z**, and the complement AC of a set A is a unary operation on the power set P(X) of a set X. Aternary (3-ary) operation is a function from S ×S ×S into S. More generally, an n-ary operation is a function from S ×S×・・・×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 (×) 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 products 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 · 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*)

·	*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, (ab)(cd), (a(bc))d, a((bc)d), 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 $a_1 * a_2 * \ldots * a_n$ 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 non-associative. For example,

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

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 ×b, a . 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 **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 implies b = c or b * a = c * a implies b = c
Addition and subtraction of integers in **Z** and multiplication of nonzero integers in **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 ≠C.

HOMOMORPHISMS

Let $(G_1,*)$ and $(G_2,0)$ be two algebraic system where * and 0 both are binary operation. Then the mapping f: $G_1 \rightarrow G_2$ is said to be homomorphism from $(G_1,*)$ to $(G_2,0)$ such that for every a, b ∈ G, we have

$$f(a,b)=f(a).\ f(b)$$

ISOMORPHISM

Let $(G_1,*)$ and $(G_2,0)$ be two algebraic system where * and 0 both are binary operation. The system $(G_1,*)$ and $(G_2,0)$ are said to be isomorphic if there exist an isomorphic mapping f: $G_1 \rightarrow G_2$.

AUTOMORPHISM

Let $(G_1,*)$ and $(G_2,0)$ be two algebraic system where * and 0 both are binary operation on G_1 and G_2 respectively. Then an isomorphism from $(G_1,*)$ to $(G_2,0)$ is called an automorphism if $G_1=G_2$.

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 **N**. Then (**N**, +) and (**N**, ×) are semigroups since addition and multiplication on **N** are associative. In particular, (**N**, ×) is a monoid since it has the identity element 1. However, (**N**, +) is not a monoid since addition in **N** has no zero element.

(b) Let S be a finite set, and let F(S) be the collection of all functions f : S → 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 · on S. Note that * can be defined by the formula x * y = x for any x and y in S. Hence

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

Therefore, * is associative and hence (S, *) is a semigroup. On the other hand, ・ is notn associative since,for example,

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

Thus (S, ・) 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}:

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

(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 l, is also considered as a word on A. However, we do not assume that l belongs to the free semigroup F = F(A). The set of all words on A including l 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*, ×) and (*B*, ×) are subsemigroups of (**N**, ×) since *A* and *B* are closed under multiplication. On the other hand, (*A*, +) is a subsemigroup of (**N**, +) since *A* is closed under addition, but (*B*, +) is not a subsemigroup of (**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 ~ be an equivalence relation on S. Recall that the equivalence relation ~ 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 ~ on S has the following property:

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

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

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

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

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

EXAMPLE B.7

(a) Let F be the free semigroup on a set A. Define u ~ u' if u and u' have the same length. Then ~ is an equivalence relation on F. Furthermore, suppose u ~ u' and v ~ v', say, l(u) = l(u') = m and l(v) = l(v') = n
Then l(uv) = l(u'v') = m + n, and so uv ~ u'v'. Thus ~ is a congruence relation on F.

Homomorphism of Semigroups

Consider two semigroups (S, *) and (S`,*`). A function f : S → S` is called a semigroup homomorphism or, simply, a homomorphism if

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

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, ×), 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 **Z4**, the integers modulo 4 under addition; and Fig. B-2(b) gives the multiplication table for S = {1, 3, 7, 9} in **Z10**. (We note that S is a reduced residue system for the integers **Z** modulo 10.) Let f : **Z4** → S be defined by

f (0) = 1, f(1) = 3, f(2) = 9, 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 Z4 and S are isomorphic semigroups.

Fundamental Theorem of Semigroup Homomorphisms

Recall that the image of a function f : S → 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 → S` be a semigroup homomorphism. Let a ~ b if f (a) = f (b). Then: (i) ~ is a congruence relation on S. (ii) S/~ is isomorphic to f (S).

EXAMPLE B.9

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

f (u) = l(u)

is a homomorphism. Note f (F) = **N**. Thus F/~ is isomorphic to **N**.

(b) LetM be the set of 2×2 matrices with integer entries. Consider the determinant function det: M → **Z**. We note that the image of det is **Z**. By Theorem B.4, M/~ is isomorphic to **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 productof 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.

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:
[**G1**] Associative Law: For any a, b, c in G, we have (ab)c = a(bc).
[**G2**] Identity element: There exists an element e in G such that ae = ea = a for every a in G.
[**G3**] 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 ∈ G, that is, if G satisfies theCommutative 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 | a ∈ A, b ∈ B} or A + B = {a + b | a ∈ A, b ∈ B}

EXAMPLE B.10
(a) The nonzero rational numbers**Q**\{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 non-commutative.

(c) Recall that **Zm** denotes the integers modulo m. **Zm** is a group under addition, but it is not a group under multiplication. However, let **Um** denote a reduced residue system modulo m which consists of those integers relatively prime to m. Then **Um** is a group under multiplication (modulo m). Figure B-3 gives the multiplication table for **U12** = {1, 5, 7, 11}.

×	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

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.

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.

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,

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

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:

- [**R1**] For any a, b, c ∈ R, we have (a + b) + c = a + (b + c).
- [**R2**] There exists an element 0 ∈ R, called the zero element, such that, for every a ∈ R,
- a + 0 = 0 + a = a.
- [**R3**] For each a ∈ R there exists an element −a ∈ R, called the negative of a, such that
- a + (−a) = (−a) + a = 0.
- [**R4**] For any a, b ∈ R, we have a + b = b + a.
- [**R5**] For any a, b, c ∈ R, we have (ab)c = a(bc).
- [**R6**] For any a, b, c ∈ R, we have: (i) a(b + c) = ab + ac, and (ii) (b + c)a = ba + ca.

Observe that the axioms [**R1**] through [**R4**] 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 · 0 = 0 · a = 0 for every a ∈ 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 ∈ S, and (ii) for any a, b ∈ S, we have a − b ∈ S and ab ∈ 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 ∈ R.

R is called a ring with an identity element 1 if the element 1 has the property that a · 1 = 1 · a = a for every element a ∈ R. In such a case, an element a ∈ 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 ∈ 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 ∈ R is a unit, that is, has a multiplicative inverse.

A field is necessarily an integral domain; for if ab = 0 and a ≠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.

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 ∈ R,

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

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 $f : R \rightarrow R`$ 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 $f : R \rightarrow R`$ 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).