Discrete Mathematics (ITPC-309)

Algebraic Structures - Part III

Dr. Sanga Chaki

Department of Information Technology

Dr. B. R. Ambedkar National Institute of Technology, Jalandhar

Contents

- Subgroups
- Direct product of groups
- Homomorphism
- Isomorphism of Groups
- Cyclic groups
- Rings
- Fields

Subgroup

1. A special subset of a group
2. If (G, •) is a group and H is a non-null proper subset of G, then H is said to be a subgroup of (G, •) if H is a group under the binary operation •
3. Example: let (G, •) = (Z_6, +) : what is Z_6 ? = {0, 1, 2, 3, 4 ,5} with + defined in modulo 6. Can you create the table for this?
4. If H = {0, 2, 4}, then H is a nonempty subset of Z_6
5. Can we show that (H, +) is a subgroup of (Z_6, +) ?
6. Hint: Given, the table for (H, +), **check for closure, associativity, identity and inverse.**

+	0	2	4
0	0	2	4
2	2	4	0
4	4	0	2

Subgroup - Properties

1. Every group G has {e} (identity) and G as subgroups, called trivial subgroups of G
2. All others are non-trivial or proper subgroups of G
3. Examples:
   a) **In the previous example**: In addition to H = {0, 2, 4}, K = {0, 3} is also a proper subgroup of (Z_6, +) – Can you prove this? Hint: Create the table for K and compare with Z_6
   b) What are the trivial subgroups of Z_6 ?
   c) The group (Z, +) is a subgroup of (Q, +) which is a subgroup of (R, +) for general addition. Z = Set of integers, Q = set of rational numbers, R = Set of real numbers. Hint: Prove that each of these form groups on their own. State that Z is a subset of Q is a subset of R.

Larger Groups from Smaller

1. Let (G, o) and (H, $*$) be two groups.
2. We can define the binary operation ♦ on G X H by

   (g_1, h_1) ♦ (g_2, h_2) = $(g_1 \text{ o } g_2, h_1 * h_2)$
3. Then (G X H, ♦) is a group and is called the **direct product** of G and H
4. Example: Are the below additions same? No

Consider the groups $(\mathbf{Z}_2, +)$, $(\mathbf{Z}_3, +)$. On $G = \mathbf{Z}_2 \times \mathbf{Z}_3$, define $(a_1, b_1) \cdot (a_2, b_2) = (a_1 + a_2, b_1 + b_2)$. Then G is a group of order 6 where the identity is (0, 0), and the inverse, for example, of the element (1, 2) is (1, 1).

5. Make the tables for both groups – remember to use modulo n
6. Make the table for G X H [6X6 table] – check for closure, associativity, identity, inverse.

Homomorphisms of Groups

1. If (G, $\circ$) and (H, $*$) are groups and there exists f: G → H, then f is called a group homomorphism if for all a, b $\in$ G, f(a $\circ$ b) = f(a) $*$ f(b)

2. Some properties of group homomorphisms: Let (G, $\circ$) and (H, $*$) are groups with respective identities e_G and e_{H}, if f: G → H is a homomorphism, then

a) $f(e_G) = e_H$.

b) $f(a^{-1}) = [f(a)]^{-1}$ for all $a \in G$.

c) $f(a^n) = [f(a)]^n$ for all $a \in G$ and all $n \in \mathbf{Z}$.

d) $f(S)$ is a subgroup of H for each subgroup S of G.

Isomorphism of Groups

1. If f:(G, o) → (H, $*$) is a homomorphism, we call f an isomorphism if it is one-to-one and onto. G and H are isomorphic groups.
2. Example 1:

Let $f:(\mathbf{R}^+, \cdot) \to (\mathbf{R}, +)$ where $f(x) = \log_{10}(x)$. This function is both one-to-one and onto. (Verify these properties.) For all $a, b \in \mathbf{R}^+$, $f(ab) = \log_{10}(ab) = \log_{10} a + \log_{10} b = f(a) + f(b)$. Therefore, f is an isomorphism and the group of positive real numbers under multiplication is abstractly the same as the group of all real numbers under addition. Here the function f translates a problem in the multiplication of real numbers (a somewhat difficult problem without a calculator) into a problem dealing with the addition of real numbers (an easier arithmetic consideration). This was a major reason behind the use of logarithms before the advent of calculators.

Isomorphism of Groups

1. Example 2:

Let G be the group of complex numbers $\{1, -1, i, -i\}$ under multiplication. Table 16.6 shows the multiplication table for this group. With $H = (\mathbf{Z}_4, +)$, consider $f: G \to H$ defined by

$$f(1) = [0] \qquad f(-1) = [2] \qquad f(i) = [1] \qquad f(-i) = [3].$$

Then $f((i)(-i)) = f(1) = [0] = [1] + [3] = f(i) + f(-i)$, and $f((-1)(-i)) = f(i) = [1] = [2] + [3] = f(-1) + f(-i)$.

Table 16.6

$\cdot$	1	-1	i	$-i$
1	1	-1	i	$-i$
-1	-1	1	$-i$	i
i	i	$-i$	-1	1
$-i$	$-i$	i	1	-1

1. We can check for all possible cases and prove that the function is isomorphic.

Isomorphism of Groups

1. Also, in the group G: $i^1 = i$, $i^2 = -1$, $i^3 = -i$, and $i^4 = 1$
2. So, every element of G is a power of i (or – i), and we say that **i generates G**.
3. This is denoted by G = <i>
4. This is also true for G = <- i> → Exercise: Verify this.
5. This leads us to the definition of a cyclic group.

Cyclic Groups

A group G is called *cyclic* if there is an element $x \in G$ such that for each $a \in G$, $a = x^n$ for some $n \in \mathbf{Z}$.

1. In case of addition, multiples are used in place of powers.

2. Example 1:

The group $H = (\mathbf{Z}_4, +)$ is cyclic. Here the operation is addition, so we have multiples instead of powers. We find that both [1] and [3] generate H. For the case of [3], we have $1 \cdot [3] = [3]$, $2 \cdot [3]$ $(= [3] + [3]) = [2]$, $3 \cdot [3] = [1]$, and $4 \cdot [3] = [0]$. Hence $H = \langle [3] \rangle = \langle [1] \rangle$.

Cyclic Groups

A group G is called *cyclic* if there is an element $x \in G$ such that for each $a \in G$, $a = x^n$ for some $n \in \mathbf{Z}$.

1. Example 2: Consider the multiplicative group $U_9 = \{1, 2, 4, 5, 7, 8\}$

   Here we find that $2^1 = 2$, $2^2 = 4$, $2^3 = 8$, $2^4 = 7$, $2^5 = 5$, $2^6 = 1$.

   (considering modulo multiplication)

   so U_9 is

   a cyclic group of order 6 and $U_9 = \langle 2 \rangle$. It is also true that $U_9 = \langle 5 \rangle$ because $5^1 = 5$, $5^2 = 7$, $5^3 = 8$, $5^4 = 4$, $5^5 = 2$, $5^6 = 1$.

2. Exercise: Which elements in U_9 generate U_9 under the binary operation of multiplication modulo 9?

Cyclic Groups – Some Theorems

1. Theorem 1:

   Let G be a cyclic group.

   a) If $|G|$ is infinite, then G is isomorphic to $(\mathbf{Z}, +)$.

   b) If $|G| = n$, where $n > 1$, then G is isomorphic to $(\mathbf{Z}_n, +)$.

2. Theorem 2:

   Every subgroup of a cyclic group is cyclic.

Ring

1. A ring, denoted as R = <{…}, +, •>, is an algebraic structure with two closed binary operations.
2. The first operation must satisfy all five properties required for an abelian/commutative group.
3. The second operation must satisfy only the first two and must be distributed over the first operation.
4. So, what does this actually mean?

Rings

1. (R, +, •) is a ring if for all a, b, c $\in$ R, the following conditions are satisfied:

a)	$a + b = b + a$	Commutative Law of +
b)	$a + (b + c) = (a + b) + c$	Associative Law of +
c)	There exists $z \in R$ such that $a + z = z + a = a$ for every $a \in R$.	Existence of an identity for +
d)	For each $a \in R$ there is an element $b \in R$ with $a + b = b + a = z$.	Existence of inverses under +
e)	$a \cdot (b \cdot c) = (a \cdot b) \cdot c$	Associative Law of •
f)	$a \cdot (b + c) = a \cdot b + a \cdot c$ $(b + c) \cdot a = b \cdot a + c \cdot a$	Distributive Laws of • over +

2. A **commutative ring** is a ring in which the commutative property is also satisfied for the second the operation.

Rings

1. Example 1:

Under the (closed) binary operations of ordinary addition and multiplication, we find that **Z**, **Q**, **R**, and **C** are rings. In all of these rings the additive identity z is the integer 0, and the additive inverse of each number x is the familiar $-x$.

2. Example 2:

Let $M_2(\mathbf{Z})$ denote the set of all 2×2 matrices with integer entries. [The sets $M_2(\mathbf{Q})$, $M_2(\mathbf{R})$, and $M_2(\mathbf{C})$ are defined similarly.] In $M_2(\mathbf{Z})$ two matrices are equal if their corresponding entries are equal in **Z**.

Here we define $+$ and $\cdot$ by

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} + \begin{bmatrix} e & f \\ g & h \end{bmatrix} = \begin{bmatrix} a+e & b+f \\ c+g & d+h \end{bmatrix}, \qquad \begin{bmatrix} a & b \\ c & d \end{bmatrix}\begin{bmatrix} e & f \\ g & h \end{bmatrix} = \begin{bmatrix} ae+bg & af+bh \\ ce+dg & cf+dh \end{bmatrix}.$$

Under these (closed) binary operations, $M_2(\mathbf{Z})$ is a ring. Here $z = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$ and the additive inverse of $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$ is $\begin{bmatrix} -a & -b \\ -c & -d \end{bmatrix}$.

Rings – Examples

1. Example 1: For infinite ring

Consider the set **Z** together with the binary operations of $\oplus$ and $\odot$, which are defined by

$$x \oplus y = x + y - 1, \qquad x \odot y = x + y - xy.$$

Consequently, here we find, for instance, that $3 \oplus 7 = 3 + 7 - 1 = 9$ and $3 \odot 7 = 3 + 7 - 3 \cdot 7 = -11$.

2. Are these operations closed in Z?
   - Since ordinary + and . are closed in Z, the new operations are also closed.
3. Prove that Z with these operations form a ring. Hint: Check all the properties of a ring are satisfied or not for both operations.
4. Check if it forms a commutative ring

Rings – Examples

1. Is the first operation commutative?

   First, since ordinary addition is a commutative binary operation for $\mathbf{Z}$, we find that for all $x, y \in \mathbf{Z}$,

   $$x \oplus y = x + y - 1 = y + x - 1 = y \oplus x.$$

   So the binary operation $\oplus$ is also commutative for $\mathbf{Z}$.

2. Does additive identity exist for the first operation?

   we need to find an integer z such

   that $a \oplus z = z \oplus a = a$, for every a in $\mathbf{Z}$. Therefore, we must solve the equation $a + z - 1 = a$, which leads us to $z = 1$. Hence the *nonzero* integer 1 is the *zero* element (or additive identity) for $\oplus$.

Rings – Examples

1. Does inverse exist for the first operation? Yes

- What about additive inverses? At this point if we are given an (arbitrary) integer a, we want to know if there is an integer b such that $a \oplus b = b \oplus a = z$. From part (2) above and the definition of $\oplus$ this says that the integer b must satisfy $a + b - 1 = 1$, and it follows that $b = 2 - a$. So, for instance, the additive inverse of 7 is $2 - 7 = -5$ and the additive inverse for -42 is $2 - (-42) = 44$. After all, in the case of 7 we find that $7 \oplus (-5) = 7 + (-5) - 1 = 7 - 5 - 1 = 1$, where 1 is the additive identity. [*Note*: Since we showed in part (1) that $\oplus$ is commutative, we also know that $(-5) \oplus 7 = 1$.]

2. Complete the discussion for the other necessary properties.

Rings – Examples

1. Example 2: Finite rings: Show that R is a commutative ring.

   Let $\mathcal{U} = \{1, 2\}$ and $R = \mathcal{P}(\mathcal{U})$. Define $+$ and $\cdot$ on the elements of R by

$$A + B = A \triangle B = \{x \mid x \in A \text{ or } x \in B, \text{ but not both}\}$$

$$A \cdot B = A \cap B = \text{the intersection of sets } A,\ B \subseteq \mathcal{U}.$$

2. The tables for these operations are as below:

$+ (\triangle)$	$\emptyset$	$\{1\}$	$\{2\}$	$\mathcal{U}$
$\emptyset$	$\emptyset$	$\{1\}$	$\{2\}$	$\mathcal{U}$
$\{1\}$	$\{1\}$	$\emptyset$	$\mathcal{U}$	$\{2\}$
$\{2\}$	$\{2\}$	$\mathcal{U}$	$\emptyset$	$\{1\}$
$\mathcal{U}$	$\mathcal{U}$	$\{2\}$	$\{1\}$	$\emptyset$

(a)

$\cdot (\cap)$	$\emptyset$	$\{1\}$	$\{2\}$	$\mathcal{U}$
$\emptyset$	$\emptyset$	$\emptyset$	$\emptyset$	$\emptyset$
$\{1\}$	$\emptyset$	$\{1\}$	$\emptyset$	$\{1\}$
$\{2\}$	$\emptyset$	$\emptyset$	$\{2\}$	$\{2\}$
$\mathcal{U}$	$\emptyset$	$\{1\}$	$\{2\}$	$\mathcal{U}$

(b)

3. Hint: Null set is the identity, and for each $x \in R$, the inverse is x itself.

Rings - Properties

1. Property 1: z is the additive identity

Let $(R, +, \cdot)$ be a ring.

a) If $ab = ba$ for all $a, b \in R$, then R is called a *commutative* ring.

b) The ring R is said to have no *proper divisors of zero* if for all $a, b \in R$, $ab = z \Rightarrow a = z$ or $b = z$.

c) If an element $u \in R$ is such that $u \neq z$ and $au = ua = a$ for all $a \in R$, we call u a *unity*, or *multiplicative identity*, of R. Here R is called a *ring with unity*.

Rings – Properties - Fields

1. Property 2

   Let R be a ring with unity u. If $a \in R$ and there exists $b \in R$ such that $ab = ba = u$, then b is called a *multiplicative inverse* of a and a is called a *unit* of R. (The element b is also a unit of R.)

2. Property 3:

   Let R be a commutative ring with unity. Then

   a) R is called an *integral domain* if R has no proper divisors of zero.

   b) R is called a *field* if every nonzero element of R is a unit.

Rings - Properties

1. Property 4

In any ring $(R, +, \cdot)$,

a) the zero element z is unique, and

b) the additive inverse of each ring element is unique.

2. Property 5:

The Cancellation Laws of Addition. For all $a, b, c \in R$,

a) $a + b = a + c \Rightarrow b = c$, and

b) $b + a = c + a \Rightarrow b = c$.

Rings - Properties

1. Property 6

   For any ring $(R, +, \cdot)$ and any $a \in R$, we have $az = za = z$.

2. Property 7:

   Given a ring $(R, +, \cdot)$, for all $a, b \in R$,

   a) $-(-a) = a$,

   b) $a(-b) = (-a)b = -(ab)$, and

   c) $(-a)(-b) = ab$.

3. Property 8

   For a ring $(R, +, \cdot)$,

   a) if R has a unity, then it is unique, and

   b) if R has a unity, and x is a unit of R, then the multiplicative inverse of x is unique.

Rings - Properties

1. Property 9

Let $(R, +, \cdot)$ be a commutative ring with unity. Then R is an integral domain if and only if, for all $a, b, c \in R$ where $a \neq z$, $ab = ac \Rightarrow b = c$. (Hence, a commutative ring with unity that satisfies the *cancellation law of multiplication* is an integral domain.)

Proof: If R is an integral domain and $x, y \in R$, then $xy = z \Rightarrow x = z$ or $y = z$. Now if $ab = ac$, then $ab - ac = a(b - c) = z$, and because $a \neq z$, it follows that $b - c = z$ or $b = c$. Conversely, if R is commutative with unity and R satisfies multiplicative cancellation, then let $a, b \in R$ with $ab = z$. If $a = z$, we are finished. If not, as $az = z$, we can write $ab = az$ and conclude that $b = z$. So there are no proper divisors of zero and R is an integral domain.

Rings - Properties

1. Property 10

If $(F, +, \cdot)$ is a field, then it is an integral domain.

Proof: Let $a, b \in F$ with $ab = z$. If $a = z$, we are finished. If not, a has a multiplicative inverse a^{-1} because F is a field. Then

$$ab = z \Rightarrow a^{-1}(ab) = a^{-1}z \Rightarrow (a^{-1}a)b = a^{-1}z \Rightarrow ub = z \Rightarrow b = z.$$

Hence F has no proper divisors of zero and is an integral domain.