Chapter 11 Groups and Rings

11.1 Introduction

$\oplus: A \times A \rightarrow A$

$\oplus$ *is a* ***function*** *from* $A \times A$ *to* A.

$^{\forall}a, {}^{\forall}b \in A, {}^{\exists 1}c = \oplus((a, b)) \in A.$

$\oplus$ *is called a* ***closed binary operation*** *on the set* A

$^{\forall}a, {}^{\forall}b \in A, {}^{\exists 1}c = a \oplus b \in A.$

($A, \oplus$*) is called an* ***algebraic system****, if*

$\oplus$ *is a* ***closed*** *binary operation*

$^{\forall}a, {}^{\forall}b \in A, {}^{\exists 1}a \oplus b \in A.$

$\oplus((a_1, a_2)) = \oplus(a_1, a_2)$ *or* $\oplus\, a_1\, a_2$ ***prefix notation***

$a_1 \oplus a_2$ ***infix notation***

$\oplus: A \times A \times A \rightarrow A$

ternaly operation

$\oplus: A \times \ldots \times A \rightarrow A$

n-ary operation

$+: N \times N \rightarrow N$

$3 + 2, + 3\ 2, +(3, 2)$

($N, +$*) is an algebraic system*

11.2 Groups

Let $\oplus: A \times A \to A$.
The operation $\oplus$ *is said to be* ***associative****, if*
$\forall a, b, c \in A, (a \oplus b) \oplus c = a \oplus (b \oplus c)$.

Let $(A, \oplus)$ *be an algebraic system. Then* $(A, \oplus)$ *is called a* ***semigroup****, if*
i) $\oplus$ *is* ***closed*** *and*
ii) $\oplus$ *is* ***associative****.*

Let $\oplus$ *is* ***associative****.*
$(a \oplus b) \oplus c = a \oplus (b \oplus c) = a \oplus b \oplus c$
$a \oplus b \oplus c \qquad \oplus a\ b\ c$

$a_1 \oplus \ldots \oplus a_n \qquad \oplus a_1 \ldots a_n \qquad a_1 \ldots a_n$
$a \oplus \ldots \oplus a \qquad \oplus a \ldots a \qquad a \ldots a \quad a^n$

binary operation $\to$ *n-ary operation*

Example $(N, +)$ *is a* ***semigroup*** $(+$ *is* ***associative****)*
$((a_0 + a_1) + a_2) \ldots + a_{n-1}) + a_n =$
$= a_0 + a_1 + a_2 \ldots + a_{n-1} + a_n =$
$= +_{r=0}^{n} a_r = \Sigma_{r=0}^{n} a_r = \sum_{r \in \{0,1,\ldots,n\}} a_r$.
$(\{a, b, \ldots, z\}^*, \cdot)$ *also is a* ***semigroup****.*

Let $(A, \oplus)$ be a algebraic system.

*$e_L \in A$ is a **left identity**, if $^{\forall}a \in A$, $e_L \oplus a = a$.*

*$e_R \in A$ is a **right identity**, if $^{\forall}a \in A$, $a \oplus e_R = a$.*

*$e \in A$ is an **identity**, if $^{\forall}a \in A$, $e \oplus a = a \oplus e = a$.*

*Let $\oplus$ be a binary operation. If there are both **left** and **right** identity, they are **same**.*

Proof

Let e_L be a left identity and e_R be a right identity.

$e_L \oplus e_R = e_R$ *e_L is left identity*

$e_L \oplus e_R = e_L$ *e_R is right identity.*

$\therefore e_L = e_R$.

identity

***neutralize** the operation*

$(N, +)$ 0

$(N, *)$ 1

$(V^*, \cdot)$ ε

(set of colored lights, combine two lights) white

*An algebraic system $(A, \oplus)$ is called a **monoid**, if*

*i) $\oplus$ is **closed**,*

*ii) $\oplus$ is **associative**, and*

*iii)there is an **identity** $e \in A$,*

*or $((A, \oplus, e)$ is called a **monoid**.*

Let $(A, \oplus)$ be a algebraic system with ***identity*** *e.*

$b \in A$ is a ***left inverse*** *of $a \in A$, if $b \oplus a = e$.*

$b \in A$ is a ***right inverse*** *of $a \in A$, if $a \oplus b = e$.*

$b \in A$ is an ***inverse*** *of $a \in A$, if $b \oplus a = a \oplus b = e$.*

inverse *of a*

cancels *the effect of the element a.*

An algebraic system $(A, \oplus)$ is called a ***group****, if*

i) $\oplus$ is ***closed****,*

ii) $\oplus$ is ***associative****,*

iii)there is an ***identity****, i.e.,*

$$^{\exists}e \in A, \text{ .э. } ^{\forall}a \in A, \ ^{\exists}e \oplus a = a \oplus e = e.$$

iv) every elements in A has ***inverse****, i.e.,*

$$^{\forall}a \in A, \ ^{\exists}a^{-1} \in A \text{ .э. } a \oplus a^{-1} = a^{-1} \oplus a = e.$$

Let $\oplus$ be ***associative****. Then* ***left inverse of*** *an elements is* ***also right inverse****.*

Proof *Let $a_L{}^{-1}$ be a left inverse of a*

and $a_L{}^{-1}{}_L{}^{-1}$ be a left inverse of $a_L{}^{-1}$. Then

$a_L{}^{-1}{}_L{}^{-1} \oplus a_L{}^{-1} \oplus a \oplus a_L{}^{-1}$

$= a_L{}^{-1}{}_L{}^{-1} \oplus ((a_L{}^{-1} \oplus a) \oplus a_L{}^{-1})$ *assoc.*

$= a_L{}^{-1}{}_L{}^{-1} \oplus (e \oplus a_L{}^{-1})$ *left inv. of a*

$= a_L{}^{-1}{}_L{}^{-1} \oplus a_L{}^{-1}$ *e is identity*

$= e$ *left inv. of $a_L{}^{-1}$.*

$a_L{}^{-1}{}_L{}^{-1} \oplus a_L{}^{-1} \oplus a \oplus a_L{}^{-1}$

$= ((a_L{}^{-1}{}_L{}^{-1} \oplus a_L{}^{-1}) \oplus a) \oplus a_L{}^{-1}$ *assoc.*

$= (e \oplus a) \oplus a_L{}^{-1}$ *left inv. of* $a_L{}^{-1}$

$= a \oplus a_L{}^{-1}$ *e is identity*

$\therefore a \oplus a_L{}^{-1} = e$

$\therefore a_L{}^{-1}$ *is also the right inverse of a.*

Let $\oplus$ *be* ***associative****. Then the* ***inverse of*** *an elements is* ***unique****.*

Proof

Suppose both a^{-1} *and* $a^{-1}{}'$ *are two* ***inverses*** *of a.*

$a^{-1} \oplus a = e$ *and* $a^{-1}{}' \oplus a = e$

$\therefore (a^{-1} \oplus a) \oplus a^{-1} = (a^{-1}{}' \oplus a) \oplus a^{-1} = a^{-1}.$

$\therefore a^{-1} \oplus (a \oplus a^{-1}) = a^{-1}{}' \oplus (a \oplus a^{-1})$ *assoc.*

$\therefore a^{-1} \oplus e = a^{-1}{}' \oplus e$ *inv. of a*

$\therefore a^{-1} = a^{-1}{}'.$

We use a^{-1} *to denote the* ***unique inverse*** *of the a in a group.*

Let (A, $\oplus$*) be a group. Then*

$^{\forall}a \in A, {}^{\exists 1} a^{-1} \in A.$

Examples

(N, +, 0) is ***not*** *a* ***group****.*

but (I, +, 0) is a ***group****.*

*(I, *, 1) is a* ***monoid***

*(I, *, 1) is* ***not*** *a* ***group****.*

*but (Q, *, 1) is a* ***group****.*

(V^*, ·, ε) is ***not*** *a* ***group****.*

???

Since $\forall a \in G, \exists 1\, a^{-1} \in G$, *we may define* ***inverse*** *binary operation on G,*

$\oplus^{-1}: G \times G \to G$,

$a \oplus^{-1} b = a \oplus b^{-1}$.

We may say that $(G, \oplus, e, \oplus^{-1})$ *is a* ***group****,*

if $(G, \oplus)$ *is a group with* ***identity*** *e and* ***inverse*** *binary operation* $\oplus^{-1}$.

Cancelation *in the* ***group***

If $c \oplus a = c \oplus b$, *then* $a = b$. ***left cancelation***

$c \oplus a = c \oplus b$

$c^{-1} \oplus (c \oplus a) = c^{-1} \oplus (c \oplus b)$

$(c^{-1} \oplus c) \oplus a = (c^{-1} \oplus c) \oplus b$

$\therefore a = b$.

If $a \oplus c = b \oplus c$, *then* $a = b$. ***right cancelation***

If $a \neq b$, *then* $c \oplus a \neq c \oplus b$ *and* $a \oplus c \neq b \oplus c$.

Example For any integer n, $(Z_n, \oplus)$ is a finite ***group****.*

$Z_n = \{0, 1, \ldots n\text{-}1\}$

$a \oplus b = a + b$, *if* $a + b < n$

$= a + b - n$, *if* $a + b \geq n$.

group *of* ***integers modulo*** *n.*

Let $\oplus$ *be a binary operation on A. The operation is said to be* ***commutative****, if*

$^{\forall} a, b \in A, a \oplus b = b \oplus a$.

A group $(A, \oplus)$ *is called a* ***commutative*** *group or* ***abelian*** *group, if* $\oplus$ *is* ***commutative****.*

A group $(A, \oplus)$ *is said to be* ***finite****, if A is a finite set, and* ***infinite*** *if A is an infinite set.*

The ***size(cardinality)*** *of A is often referred to as the* ***order*** *of the* ***group*** $(A, \oplus)$.

closed ***algebraic system***

algebraic system of interest

associative ***semigroup***

n-ary operation, $a \oplus \ldots \oplus a = a^n$.

identity ***monoid***

unique *identity*

inverse ***group***

unique *inverse*

commutative ***abelian group****(commutative group)*

11.3 Subgroup

Let $(A, \oplus)$ be an algebraic system and $B \subseteq A$. Then
*$(B, \oplus)$ is called a **sub-**algebraic system of A.*
sub semigroup**, **submonoid**, **subgroup

subgroup

*1) $^{?}$**closed***	*$^{\forall} a, b \in B, a \oplus b \,^{?}\in B$*
*2) **associative***	*yes!*
*3) $^{?}$**identity** $\in B$*	*$e \,^{?}\in B$*
*4) $^{?}$**inverse** $\in B$*	*$^{\forall} a \in B, a^{-1} \,^{?}\in B$*

Theorem11.1 *Let $(A, \oplus)$ be a group and $B \subseteq A$. If B is a **finite**$^{(1)}$ set and $\oplus^{(2)}$ is a **closed** operation on B then $(B, \oplus)$ is a **subgroup** of $(A, \oplus)$.*

Proof *Let $a \in B$, then ($\oplus$ is associative and **closed**)*

$a = a^1 \in B, a \oplus a = a^2 \in B, \ldots, a^i \in B, \ldots (i > 0)$.

*Since B is **finite**, $a^n = a^m$ for some $n, m > 0, n < m$.*

$\therefore a^n = a^n \oplus a^{m-n}, m - n > 0$.

*$e = a^{m-n}$ is an **identity** and in B.*

*Two cases for **inverse***

(1) If $m - n > 1$, $a^{m-n} = a \oplus a^{m-n-1} = e$.

*$a^{m-n-1}(m - n - 1 > 0)$ is the **inverse** of a and in B.*

(2) If $m - n = 1$, $a^1 = e$,

$\therefore a^{n+1} = a^n \oplus a^1 = a^n \oplus e = a^n = a$

$\therefore a = a \oplus a$.

*a is idendty and **inverse** of a and in $B = \{a\}$.*

11.4 Generators and Evaluation of Power

Let $(A, \oplus)$ be an algebraic system, and $B \subseteq A$.
Let $B_1 = B \cup \{a \oplus b \in A \mid a, b \in B\}$.

*B_1 is called the set **generated directly** by B.*

$B_2 = B_1 \cup \{a \oplus b \in A \mid a, b \in B_1\}$

…

$B_{i+1} = B_i \cup \{a \oplus b \in A \mid a, b \in B_i\}$

$B^* = B \cup B_1 \cup B_2 \cup \ldots$

$\therefore \forall c \in B^*, \exists a, b \in B^*$ *.э.* $a \oplus b = c$.

$\forall x \in B^*$, *x is said to be **generated** by B.*

$B^* \subseteq A$, *is called the set **generated** by B.*

$\therefore \forall a, b \in B^*, a \oplus b \in B^*$*.(**closed**)*

*$(B^*, \oplus)$ is called the **subsystem generated** by B.*

*If B^* is **finite** and $(A, \oplus)$ is a **group**,*

*$(B^*, \oplus)$ is the **subgroup**.(Theorem 11.1)*

If $B^* = A$, B is called
*a **generating set** or a **set of generators***
of the algebraic system $(A, \oplus)$.

*A group that has generating consisting of a **single** element is called as a **cyclic group**.*

Let $(A, \oplus)$ be a cyclic group with generating set $\{a\}$.
$A = \{a, a^2, a^3, \ldots\}$
$a^i \oplus a^j = a^j \oplus a^j = a^{i+j}$. ***associative***
$\therefore$ *Any **cyclic** group is **commutative** group*

Let B be a generating set of an algebraic system$(A, \oplus)$.
For $a \in A$, $^{\exists}r \geq 1$, and $a_r = a$.
$a_1\ a_2\ \ldots\ a_r$ ***generating sequence** for $a \in A$*
$^{\forall}i$.ə. $1 \leq i \leq r$, $a_i = a_j \oplus a_k$
where $a_j, a_k \in B$ or $(j < i)$ or $(k < i)$.

Example)
*$(V^*, \cdot, \varepsilon)$ is a **monoid generated** by V with identity ε.*
*$(N, +, 0)$ is an commutative **cyclic** group*
generated by $\{1\}$ with the identity 0.

Example)
Consider (I, +), B = {1}, and consider 9

2 3 4 5 6 7 8 9
2 3 4 5 9
2 3 5 8 9
addition chain

The shortest addition chain

***Method 1**. If $n = p \times q$.*

$p_1\ p_2\ \ldots p_{i-1}\ \ p$ *is an addition chain for p,*
$q_1\ q_2\ \ldots q_{j-1}\ \ q$ *is an addition chain for q,*
$q_1\ q_2\ \ldots q_{j-1}\ \ q\ \ qp_1\ \ qp_2\ \ \ldots\ \ qp_{i-1}\ \ qp$
addition chain for n=pq

45 = 5 × 9

5: 1, 2, 3, 5
9: 1, 2, 4, 8, 9
45: 1, 2, 4, 8, 9, 18, 27, 45 or
1, 2, 3, 5, 10, 20, 40, 45

Method 2

If n is even, determine addition chain for
n/2, n.
If n is odd, determine addition chain for
(n-1)/2, (n-1), n.

2 4 5 10 11 22 44 45

11.5 Coset and Lagrange's Theorem

Let $(A, \oplus)$ be a algebraic system, $a \in A$, and $H \subseteq A$. Then

***left coset of** H **with respect to** a, $a \oplus H$,*

$a \oplus H = \{a \oplus x \mid x \in H\}$

***right coset of** H **with respect to** a, $a \oplus H$,*

$H \oplus a = \{x \oplus a \mid x \in H\}$

***Theorem 11.2** Let $(G, \oplus)$ be a **group** and $(H, \oplus)$ be a **subgroup** of $(G, \oplus)$. Then*

$a \oplus H = b \oplus H$ *or* $a \oplus H \cap b \oplus H = \varnothing$.

***Proof** Assume $a \oplus H \cap b \oplus H \neq \varnothing$.*

$^{\exists}f \in a \oplus H \wedge f \in b \oplus H$.

$\therefore f = a \oplus h_1 = b \oplus h_2$ $(h_1, h_2 \in H)$

$\therefore a = b \oplus h_2 \oplus h_1^{-1}$ $(h_1^{-1} \in H$, *inverse of* $h_1)$

$^{\forall}x \in a \oplus H, {}^{\exists}h_3 \in H$.э. $x = a \oplus h_3$,

$x = b \oplus h_2 \oplus h_1^{-1} \oplus h_3, \therefore x \in b \oplus H$.

$\therefore a \oplus H \subseteq b \oplus H$.

Similar way, $a \oplus H \supseteq b \oplus H$.

$\therefore a \oplus H = b \oplus H$. *(But note that* $a \oplus h \neq b \oplus h$*)*

Furthermore, since $e \in H$,

$G = \cup_{a \in G} a \oplus H = \cup_{a \in G} H \oplus a$.

$\therefore$ *If H is a* ***subgroup,***
$\{a \oplus H \mid a \in G\}$ *is a* ***partition*** *of G.*

Furthermore.
$^{\forall}a \in G, {}^{\forall}h_1 \neq h_2 \in H,$
$a \oplus h_1 \neq a \oplus h_2$. *(left cancelation)*
$\therefore |H| = |a \oplus H|$
$\therefore \{a \oplus H \mid a \in G\}$ *form a* ***partition*** *of G, and all blocks are of* ***same size****.*

$\therefore |G|$ = *(number of distinct left coset of H)* $\times |H|$

Example $G = \{0°, 60°, 120°, 180°, 240°, 300°\}$
subgroup $H_1 = \{0°, 180°\}$, $H_2 = \{0°, 120°, 240°\}$
$0° \oplus H_1 = \{0°, 180°\} = 180° \oplus H_1$
$60° \oplus H_1 = \{60°, 240°\} = 240° \oplus H_1$
$120° \oplus H_1 = \{120°, 300°\} = 300° \oplus H_1$
$P_1 = \{\{0°, 180°\}, \{60°, 240°\}, \{120°, 300°\}\}$
subgroup $H_2 = \{0°, 120°, 240°\}$
$0°\oplus H_2 = \{0°,120°,240°\} = 120°\oplus H_2 = 240°\oplus H_2$
$60°\oplus H_2=\{60°,180°,300°\}=180°\oplus H_2 = 300°\oplus H_2$
$P_2 = \{\{0°,120°,240°\}, \{60°,180°,300°\}\}$

Theorem 11.3(Lagrange) *The order of any subgroup of a* ***finite*** *group divides the order of the group.*

If the order of group is ***prime****,*
no nontrivial*(except {e} and A) subgroup.*
∴ It is a ***cyclic*** *group.*
Any singleton set except identity is
a generating set

11.8 Isomorphisms and Automorphisms

Let (A, ⊕) and (B, ⊗) be ***algebraic system****. Then (B, ⊗) is said to be* ***isomorphic*** *to (A, ⊕), if*

$^{\exists}f: A \rightarrow B$ *.ə. one-to-one onto*
$f(a \oplus b) = f(a) \otimes f(b)$
f: ***isomorphism***
(B, ⊗) is the ***isomorphic image*** *of (A, ⊕)*

Fig. 11.10, 11.11

automorphism

An ***isomorphism*** *f (****permutation****)*
from (A, ⊕) to (A, ⊕).

Example 11.4 (Z_p, ⊕) is a group of integer modulo p.

$Z_p = \{0, 1, \ldots p\text{-}1\}$
$a \oplus b = a + b$, *if* $a + b < p$
$= a + b - p$, *if* $a + b \geq p$.

Let $(G, \otimes)$ be a group of prime order p
Since any group of prime order is ***cyclic****,*
G can be represented as $a^0, a^1, \ldots, a^{p-1}$, $^\forall a \in G-\{e\}$
$a^n \otimes a^m = a^{n \oplus m}$.
$\therefore$ *$f(a^i) = i$ is the* ***isomorphism*** *from G to Z_p.*
$f(a^n \otimes a^m) = f(a^{n \oplus m}) = n \oplus m = f(a^n) \oplus f(a^m)$.

$\therefore$ *Any group of prime order p is* ***isomorphic*** *to $(Z_p, \oplus)$.*

11.9 Homomorphisms and Normal Subgroups

Let $(A, \oplus)$ and $(B, \otimes)$ be ***algebraic systems****. Then $(B, \otimes)$ is said to be* ***homomorphic*** *to $(A, \oplus)$ w.r.t. h, if*
$^\exists h: A \rightarrow B$ *.ə.* ***onto****$(|A| \geq |B|)$ and*
$h(a \oplus b) = h(a) \otimes h(b)$.
h: ***homomorphism*** *from $(A, \oplus)$ to $(B, \otimes)$.*
$(B, \otimes)$ is the ***homomorphic image*** *of $(A, \oplus)$ w.r.t. h.*
Fig. 11.12

Let $(A, \oplus)$ be an algebraic system and
R be an ***equivalence*** *relation on A.*
R is called the ***congruence relation*** *on A w.r.t $\oplus$,*
if (a_1, a_2) and $(b_1, b_2) \in R$ ***implies*** *that*
$(a_1 \oplus b_1, a_2 \oplus b_2) \in R$.
$[a]_R$: ***congruence*** *class.*
Fig. 11.13, 11.14

*Let $(A, \oplus)$ be an **algebraic system**, R be a **congruence** relation on A w.r.t $\oplus$, and $P_R = \{[a]_R \mid a \in A\}$.*
We define $[\oplus]_R: P_R \times P_R \rightarrow P_R$, as

$$[a]_R\ [\oplus]_R\ [b]_R = [a \oplus b]_R \text{ and}$$

$h: A \rightarrow P$.ə. $^{\forall}a \in [a]_R$, $h(a) = [a]_R$. Then

$$h(a \oplus b) = [a]_R\ [\oplus]_R\ [b]_R. \text{ Then}$$

*$\therefore$ $(P_R, [\oplus]_R)$ is a **homorphic** image of $(A, \oplus)$ w.r.t h.*

*Let $(B, \otimes)$ be a **homomorphic** image of $(A, \oplus)$ w.r.t. f. A **congruence** relation R on A w.r.t $\oplus$ is defined as*

$$R = \{(a, b) \in A \times A \mid f(a) = f(b)\}. \text{ Then}$$

*$(P_R, [\oplus]_R)$ and $(B, \otimes)$ are **isomorphic**.*

$$[a]_R\ [\oplus]_R\ [b]_R \leftrightarrow f(a) \otimes f(b).$$

homomorphism $\Leftrightarrow$ ***congruence*** *relation*

*$(A, \oplus)$ is a **refinement** of $(B, \otimes)$ w.r.t. f*
*homomorphic image $(B, \otimes)$ has **grosser** information.*

Example *$(I, \times)$, I: set of integers, $\times$: multiplication*

$(B, \otimes)$, $B = \{P, N, Z\}$

$\otimes: B \times B \rightarrow B$ (Figure 11.15)

$f: I \rightarrow B$ homomorphism from I to B w.r.t. $\times$

$$f(n) = \begin{cases} P, & \text{if } n > 0 \\ N, & \text{if } n < 0 \\ Z, & \text{if } n = 0. \end{cases}$$

We define ***congruence*** *relation on $R \subseteq I \times I$ as*

$$R = \{(0, 0)\} \cup \{(n, m) \mid n > 0, m > 0\} \cup \{(n, m) \mid n < 0, m < 0\}$$

$P_R = \{[0]_R, [1]_R, [-1]_R.\}$ *where*

$[0]_R = \{0\}$

$[1]_R = \{1, 2, \ldots\} = [2]_R = \ldots$

$[-1]_R = \{-1, -2, \ldots\} = [-2]_R = \ldots$

$[\otimes]_R: P_R \times P_R \rightarrow P_R$ *(isomor. to Figure 11.15)*

$(P_R, [\otimes]_R)$ *is* ***isomorphic*** *to $(B, \otimes)$ w.r.t. $i: P_R \leftrightarrow B$*

$i([0]_R) = Z$ $i([1]_R) = P$ $i([-1]_R) = N.$

$i^{-1}(Z) = [0]_R$ $i^{-1}(P) = [1]_R$ $i^{-1}(P) = [1]_R.$

Let H be a subgroup of G. H is said to be

*a **normal subgroup**, if* $^{\forall}a \in A, a \oplus H = H \oplus a$.

*If G is a **commutative** group,*

*any subgroup is **normal.***

***Theorem** Any distinct **cosets** of a **normal** subgroup H are **congruence** classes of group G.*

Proof

Let $a \oplus H$ *and* $b \oplus H$ *be two distinct normal cosets.*

To prove $(a \oplus H) \oplus (b \oplus H) \subseteq (a \oplus b) \oplus H$.

Fix $^{\forall}a_1 \in a \oplus H, ^{\forall}b_1 \in b \oplus H$.

$a_1 \oplus b_1 = (a \oplus h_1) \oplus (b \oplus h_2)$ *(def.)*

$= (a \oplus h_1) \oplus (h_3 \oplus b), h_3 \in H$ *(normal)*

$= a \oplus h_4 \oplus b\ , h_4 \in H$ *(asso., closed)*

$= a \oplus b \oplus h_5, h_5 \in H$ *(normal)*

$\therefore a_1 \oplus b_1 \in (a \oplus b) \oplus H$

$\therefore (a \oplus H) \oplus (b \oplus H) \subseteq (a \oplus b) \oplus H$.

We can prove $(a \oplus H) \oplus (b \oplus H) = (a \oplus b) \oplus H$.

We define $h: G \rightarrow P = \{[a \oplus H] \mid a \in G\}$ *as*

$^{\forall}a_1 \in a \oplus H, h(a_1) = [a \oplus H]$, *and*

$[\oplus]: P \times P \rightarrow P$

$[a \oplus H]\ [\oplus]\ [b \oplus H] = [(a \oplus b) \oplus H]$

*(P, [⊕]) is a **homomorphic** image of (G, ⊕) w.r.t. h, since h is **total** and **onto**.*

*Is exhausting all cosets of normal subgroup of $(G, \oplus)$ exhauste **all** homomorphic image of $(G, \oplus)$?*

Lemma *Let h be a **homomorphism** from $(G, \oplus, e)$ to $(P, \otimes, \varepsilon)$ and $I = \{a \in G \mid h(a) = \varepsilon\}$. Then $(I, \oplus, e)$ is a **normal subgroup** of $(G, \oplus)$.*

Proof *Consider the **congruence partion** on G.*

1. $^{\forall}a, b \in I, h(a \oplus b) = [a]\ [\oplus]\ [b] = [e]$
   $\therefore a \oplus b \in I$ ***closed***.
2. *Let $e \in G$ be the **identity**.*
   $^{\forall}a \in G, h(a \oplus e) = h(a) = h(a) \otimes h(e)$
   $\therefore \varepsilon = \varepsilon \otimes h(e) \qquad \varepsilon = h(e)$
   $\therefore e \in I.$ ***identity***
3. *Consider $a \in I$ and $a^{-1} \in G$.*
   $h(e) = h(a \oplus a^{-1}) = h(a) \otimes h(a^{-1})$
   $= \varepsilon \otimes h(a^{-1}) = \varepsilon$
   $\therefore \varepsilon = h(a^{-1}), a^{-1} \in I$ ***inverse***

$\therefore$ *$(I, \oplus)$ is a subgroup of $(G, \oplus)$. (G is **assocoative**)*

4. $^{\forall}a \in G, ^{\forall}i \in I.$
   $h(a \oplus i \oplus a^{-1}) = h(a) \otimes h(i) \otimes h(a^{-1})$
   $= h(a) \otimes \varepsilon \otimes h(a^{-1}) = h(a) \otimes h(a^{-1})$
   $= h(a \oplus a^{-1}) = h(e) = \varepsilon$
   $\therefore a \oplus i \oplus a^{-1} \in I$
   $\therefore {}^{\exists}i_1 \in I$.ə. $a \oplus i \oplus a^{-1} = i_1$.
   $\therefore a \oplus i = a \oplus i \oplus a^{-1} \oplus a = i_1 \oplus a.$

$\therefore\ a \oplus I = I \oplus a.$

$\therefore$ *(I, ⊕) is a* ***normal subgroup*** *of (G, ⊕).*

$\therefore\ (a \oplus I) \oplus (b \oplus I) = (a \oplus b) \oplus I.$

Furthermore,

If $a, b \in c \oplus I$ *for some* $c \in G$, *then* $h(a) = h(b)$.

Since $a = c \oplus i$, $c = a \oplus i^{-1}$.

$\therefore\ ^{\exists} i \in I$.ə. $b = a \oplus i^{-1} \oplus i' = a \oplus i.$

$\therefore\ h(b) = h(a \oplus i) = h(a) \otimes h(i) = h(a) \otimes \varepsilon$

$\therefore\ h(a) = h(b)$

If $h(a) = h(b)$, *then* $^{\exists} c \in G$.ə. $a, b \in c \oplus I.$

$h(a^{-1} \oplus b) = h(a^{-1}) \otimes h(b) = h(a^{-1}) \otimes h(a)$

$= h(a^{-1} \oplus a) = h(e) = \varepsilon$

$\therefore\ ^{\exists} i \in I$.ə. $a^{-1} \oplus b = i.$

$\therefore\ a \oplus a^{-1} \oplus b = b = a \oplus i.$

$\therefore\ ^{\exists} c \in G$.ə. $a, b \in c \oplus I.$

$a \oplus I = I \oplus a = [a] = h(a)$

$h(a \oplus b) = [a] \otimes [b] = h(a) \otimes h(b)$

$\therefore$ *Every distinct* ***cosets*** *of the* ***normal*** *subgroup I is* ***all*** *of the* ***congruence*** *classes of G.*

homomorphic *images of G.*

Let $(G, \oplus, e)$ be a group and normal subgroup I.
We define congruence partiotion

$P = \{\{a \oplus I\} | \ a \in G\}$.

Furthermore since, $e \in I$, $a \in a \oplus I$,

we can write $h(a \oplus I) = [a]_R$.

$\therefore P = \{[a] | \ a \in G\}$.

We define ***homorphic*** *image of $(G, \oplus)$ as $(P, [\oplus])$*

w.r.t. $h: G \rightarrow P$.

$h(a \oplus b) = h(a)\ [\oplus]\ h(b) = [a]\ [\oplus]\ [b] = [a \oplus b]$

Example $(Z_6, \oplus) = (\{0, 1, 2, 3, 4, 5\}, \oplus)$

1. *normal subgroup* $I_1 = \{0, 2, 4\}$

$[0]_R = \{0, 2, 4\} = [2]_R = [4]_R$

$[1]_R = \{1, 3, 5\} = [3]_R = [6]_R$

$[0 \oplus 0] = [0]\ [\oplus]\ [0]$,

$[0 \oplus 1] = [0]\ [\oplus]\ [1]$,

…

2. *normal subgroup* $I_2 = \{0, 3\}$

$[0]_R = \{0, 3\} = [3]_R$

$[1]_R = \{1, 4\} = [4]_R$

$[2]_R = \{2, 5\} = [5]_R$

…

$(Z_2, \oplus)$ and $(Z_3, \oplus)$ are homomorphic images of $(Z_6, \oplus)$

11.6 Permutation Groups and Burnside's Theorem

$f: S \to S$

f is one-to-one (onto)

*f is called the **permutation** of the set S*

Example S = {a, b, c, d}. We write permutation f ≡ abcd ⇒ bdca, or bdca for short, if

f(a) = b, f(b) = d, f(c) = c, f(d) = a; or

f = {(a, b), (b, d), (c, c), (d, a)}

*For |S| = n, let A denote the set of all n! **permutations** of S. We define*

$\circ: A \times A \to A$

$\pi_1 \circ \pi_2 = \{(a, c) | (a, b) \in \pi_1, (b, c) \in \pi_2\}$

or $\pi_1 \circ \pi_2(a) = \pi_2(\pi_1(a))$

(reversed order in the text)

*$\circ$ is **closed**.*

*$\circ$ is **associative**.*

$(\pi_1 \circ \pi_2) \circ \pi_3 = \pi_1 \circ (\pi_2 \circ \pi_3)$

*$\pi_I = \{(a, a) | a \in S\}$ is the **identity** for $\circ$.*

*$\pi^{-1} = \{(b, a) | (a, b) \in \pi\}$ is the **inverse** of π.*

*$\therefore$ (A, $\circ$) is a **group**.*

*A **subgroup** of A is called the **permutation group** of S*

({abcd, bacd, abdc, badc}, $\circ$) is a per. group of S.

*Let $(G, \circ)$ be a **permutation** group of S ($G \subseteq A$).*
We define a binary relation R on S

$R = \{(a, b) | (a, b) \in \pi, \pi \in G\}$

*the binary relation **induced** by $(G, \circ)$.*

Example If $G = \{abcd, bacd, abdc, badc\}$,

$R = \{(a, a), (b, b), (c, c), (d, d),$
$(a, b), (b, a), (c, d), (d, c)\}$

*The binary relation R on S induced by **permutation** group $(G, \circ)$ is an **equivalence** relation.*

reflexive	$\pi_I \in G$.	***identity***
symmetric	*If* $\pi \in G, \pi^{-1} \in G$.	***inverse***
transitive	*If* $\pi_1, \pi_1 \in G, \pi_1 \circ \pi_2 \in G$.	***closed***

*What is the **index** of the equivalent relation?*

*$a \in S$ is said to be **invariant** under permutation $\pi \in G$, if $(a, a) \in \pi$, or **invariant**, otherwise.*

***Theorem 11.4(Burnside)** Let R be an **equivalence** relation on S induced by a **permutation** group $(G, \circ)$*

$|\{[s]_R | s \in S\}| = 1/|G| \sum_{\pi \in G} \psi(\pi)$

*where $\psi(\pi)$ is the number of **invariances** under the permutation π.*

***Example** If $G = \{abcd, bacd, abdc, badc\}$,*
$|\{[s]_R | s \in S\}| = |\{\{a, b\}, \{c, d\}\}| = 1/4(4+2+2+0) = 2$

Proof *For $s \in S$, $\eta(s)$ denotes the number of permutations in G under which s is* ***invariant****.*

$\sum_{\pi \in G} \psi(\pi) = \sum_{s \in S} \eta(s)$ $\quad 4+2+2+0=2+2+2+2$

Let $a, b \in S$ and $(a, b) \in R$.
How many permutations that maps a into b?

$\exists \pi^a{}_b \in G$ *.ə.* $(a, b) \in \pi^a{}_b$, *since* $(a, b) \in R$.

i) Let $H_a = \{\pi | (a, a) \in \pi\}$. *Then* $|H_a| = \eta(a)$ *and*

consider $H_a \circ \pi^a{}_b = \{\pi | (a, b) \in \pi\}$.

$\forall \pi_1, \pi_2 \in H_a$, *If* $\pi_1 \circ \pi^a{}_b = \pi_2 \circ \pi^a{}_b$,

$\pi_1 = \pi_2$*(right cancellation).*

$\therefore |H_a \circ \pi^a{}_b| = |H_a| = \eta(a)$. $\quad (?(H_a, \circ)$ *is a group)*

ii) Suppose $\exists \pi \in G$ *.ə.* $(a, b) \in \pi$ *but* $\pi \notin H_a \circ \pi^a{}_b$.

$(a, a) \in \pi \circ (\pi^a{}_b)^{-1} \quad \therefore \pi \circ (\pi^a{}_b)^{-1} \in H_a$.

$\therefore \pi \circ ((\pi^a{}_b)^{-1} \circ \pi^a{}_b) = \pi \in H_a \circ \pi^a{}_b$ (***contradiction***).

$\therefore \exists$ *exactly* $\eta(a)$ *permutations that maps a into b*

Let $[a]_R \subseteq S$ *be an equivalence class.*

$\forall b \in [a]_R, \eta(a) = \eta(b)$.

$\sum_{b \in [a]_R} \eta(b) = |G|$.

$\therefore \sum_{s \in S} \eta(s) = |G| \times |\{[a]_R\}|$

Example 11.1, 11.2, 11.3.

11. 7 Codes and Group Codes

Coding problem

representing distinct message by distinct sequence of letters from a given alphabet

Assume the alphabet = {0, 1}

a sequence of alphabet ***word****(string)*

code *a collection of words to represents distinct message (language)*

a word in a code ***codeword****(sentence)*

A ***block code*** *a code consisting of words that are of the same length*

error correction

transmit error

Let A denote a set of all binary sequence of length n

$A = \{0, 1\}^n$ *and* $\oplus$ *be a binary operator on A .ə.*

If $x = a_1 \ldots a_n$, $y = b_1 \ldots b_n$,

$$(x \oplus y)_i = \begin{cases} 0, \text{ if } a_i = b_i \\ 1, \text{ if } a_i \neq b_i. \end{cases} \quad 1 \leq {}^{\forall} i \leq n,$$

$(A, \oplus)$ is a ***group***

$\oplus$ is ***associative***. *exclusive or*

$0^n \in A$ is the ***identity***.

$\forall x \in A$, x is the ***inverse*** *of x.*

$x \oplus x = 0^n$

$w(x)$ is the number of 1's in x. ***weight*** *of x*

$d(x, y) = w(x \oplus y)$ ***distance*** *between x and y*

number of different bits

$d(x, y) = d(y, x)$

$w(x \oplus y) = w(x \oplus z \oplus z \oplus y)$ $(z \oplus z = 0^n)$

$\leq w(x \oplus z) + w(z \oplus y)$ $(w(x \oplus y) \leq w(x) + w(y))$

$\therefore d(x, y) \leq d(x, z) + d(z, y), \forall z \in A.$

Let G be a block code.

the ***distance*** *of G*

minimum distance between any pair

of distinct codewords in G

Let $x_1, \ldots, x_n$ be codewords in G.

$P(x_i|y)$: probability that x_i is the transmitted word,

given that y is the received word.

If $P(x_k|y)$ is maximum, we conclude x_k is transmitted

maximum-likelihood decoding criterion

If $d(x_k|y)$ is minimum, we conclude x_k is transmitted

minimum-distance decoding criterion

Assume that the occurrences of errors in positions are independent and the probability of the error occurrence is p

$P(x_i|y) = (1-p)^{n-t}p^t$

$t = d(x_i, y)$

For $p < 1/2$, $P(x_i|y) > P(x_j|y)$, *if* $d(x_i, y) < d(x_j, y)$

minimum-distance decoding criterion
= maximum-likelihood decoding criterion

A group code of (minimum) distance 2t+1 can correct t or fewer errors
If no more than t errors has occurred

$d(x, y) \le t$

Consider another code word z

$d(x, z) \ge 2t+1$

$d(x, z) \le d(x, y) + d(y, z)$

$\therefore\ d(y, z) = d(z, y) \ge t+1$

$\therefore$ *We can select x as the transmitted word*

A subset G of A is called (binary) ***group code****,*
if (G, ⊕) is a subgroup of (A, ⊕)

Let $x \neq 0, x \in G$
$w(x) = d(x, 0)$
$\therefore\ w(x) \geq min_{y,z \in G}\ d(y, z)$
$min_{x \in G,\ x \neq 0}\ w(x) \geq min_{y,z \in G}\ d(y, z)$

Since $d(y, z) = w(y \oplus z)$ *and* $y \oplus z \in G$,
$d(y, z) \geq min_{x \in G,\ x \neq 0}\ w(x)$
$min_{y,z \in G}\ d(y, z) \geq min_{x \in G,\ x \neq 0}\ w(x)$
$\therefore\ min_{x \in G,\ x \neq 0}\ w(x) = min_{y,z \in G}\ d(y, z)$

Let G be a group code, and y be a received word
G ⊕ y are the distances between code words and the received word.

Let e_y *be the one of the word of the smallest weight in* $G \oplus y$
$e_y = x \oplus y, x \in G$
$\therefore\ e_y \oplus y$ *is the transmitted word*

11.10 Rings, Itegral domains, and Fields

*The operation ⊗ is **distributes** over ⊕, if*

$a \otimes (b \oplus c) = (a \otimes b) \oplus (a \otimes c)$

*Let (A, ⊕, ⊗) be an algebraic system with two operators. (A, ⊕, ⊗) is called a **ring**, if*

1. *(A, ⊕) is an **abelian group***
2. *(A, ⊗) is a **semigroup***
3. *The operation ⊗ is **distributive** over ⊕.*

Example: Consider $(Z_n, \oplus, \otimes)$ where

$Z_n = \{0, 1, \ldots, n-1\}$

$a \oplus b = a + b$, *if* $a + b < n$

$= a + b - n$, *if* $a + b \geq n$.

$a \otimes b$ = *the remainder of ab divided by n*

1. *$(Z_n, \oplus)$ is an **abelian group***
2. *$(Z_n, \otimes)$ is closed and associative(**semigroup**)*
3. *⊗ distributes over ⊕*

$\therefore$ *$(Z_n, \oplus, \otimes)$ is a **ring**.*

*⊕: **addition** operation of the ring*

$a \oplus b$: ***sum*** *of a and b*

*⊗: **multiplication** operation of the ring*

$a \otimes b$: ***multiplication*** *of a and b*

Let $(A, \oplus, \otimes)$ is a ***ring*** *with* ***additive identity*** *0.*

$^{\forall}a \in A, 0 \otimes a = (0 \oplus 0) \otimes a = (0 \otimes a) \oplus (0 \otimes a)$

$\therefore 0 \otimes a = a \otimes 0 = 0.$

0: ***zero****.*

-a: ***additive inverse***

$a \oplus^{-1} b = a \oplus (-b) = a - b$

$(A, \oplus, \otimes)$ is called an ***integral domain****, if*

1. *$(A, \oplus)$ is an* ***abelian group****.*
2. *$(A, \otimes)$ is* ***commutative semigroup****, and*
   If $c \neq 0$ and $c \otimes a = c \otimes b$, then $a = b$
   where 0 is the ***additive identity****.*
3. *The operation $\otimes$ is* ***distributive*** *over $\oplus$.*

Example *Consider I is set of integers, and + and $\times$ are normal addition and multiplication on integers.*

$(I, +, \times)$ is the ***integral domain***

$(A, \oplus, \otimes)$ is called a ***field****, if*

1. *$(A, \oplus)$ is an* ***abelian group****.*
2. *$(A-\{0\}, \otimes)$ is an* ***abelian group****.*
3. *The operation $\otimes$ is* ***distributive*** *over $\oplus$.*

$(A-\{0\}, \otimes)$ is a ***group***

1: ***multiplicative identity***

a^{-1}: ***multiplicative inverse*** *of a*

$\otimes^{-1}$: ***multiplication*** *of a and*
multiplicative inverse *of b*
$a \otimes^{-1} b = a \otimes 1/b = a/b$

Example)
(Q, +, ×) is the field
Q is the set of ***rational*** *numbers, and*
+ and × are normal addition and multiplication
(R, +, ×) is the field
R is the set of ***real*** *numbers,*
(C, +, ×) is the field
C is the set of ***complex*** *numbers*

We have studied operations in the ***field*** *of*
rational, ***real***, *and* ***complex*** *numbers.*
Substruction is not really an ***independent*** *operation*
but it is the ***addition*** *of the* ***additive inverse***.
Division is the ***multiplication*** *of*
the ***multiplcative inverse***.

Consider $(Z_n, \oplus, \otimes)$

$a \otimes b$ = *the remainder of* ab *divided by* n.

$(Z_n, \oplus)$ *is an abelian group, and* $\otimes$ *is commutative*

$(Z_n\text{-}\{0\}, \otimes)$ *is an abelian group iff* n *is prime.*

If n *is not prime,* $n = ab$ *for some* $a, b \in Z_n - \{0\}$,

But $a \otimes b = 0$ ***not closed***

If n *is prime,*

$^{\forall}a, b \in Z_n\text{-}\{0\}, a \otimes b \neq 0 \therefore a \otimes b \in Z_n\text{-}\{0\}.$

$\otimes$ *is* ***associative*** *and* ***commutative***

1 *is the* ***identity*** *of* $\otimes$.

$^{\forall}a, b \neq c \in Z_n\text{-}\{0\}, a \otimes b \neq a \otimes c$

assume $a \otimes b = a \otimes c$

$ab = kn + r, ac = ln + r$

$a(b\text{-}c) = (k\text{-}l)n$ *(assume* $b > c, \therefore k > l$*)*

Since $a, b\text{-}c < n$, *and* n *is* ***prime***

$a(b\text{-}c) \neq (k\text{-}l)n.$

$\therefore a \otimes b \neq a \otimes c$

$\therefore {}^{\forall}a \in Z_n\text{-}\{0\}, {}^{\exists}b \in Z_n\text{-}\{0\}$ *.ə.* $a \otimes b = 1.$

$^{\exists}1/a = b.$

$\therefore (Z_n\text{-}\{0\}, \oplus, \otimes)$ *is a* ***field****.*

field of integers modulus n