Algebra

李錦州

January 9, 2022

Contents

Chapter 1

Groups

1.1 Binary Operations

Definition 1.1

A **binary operator** (二元運算) $*$ on a set S is a function mapping form $S \times S$ into S ($* : S \times S \to S$). Each $(a, b) \in S \times S$, will denote the element $*(a, b)$ of S is $a * b$.

Example 1.1

Addition $(+)$ is a binary operator on $\mathbb{R}$. Mapping $\mathbb{R} \times \mathbb{R} \to \mathbb{R}$. Each $(a, b) \in \mathbb{R} \times \mathbb{R}$, $+(a, b) = a + b$.

Definition 1.2

Let $*$ be a binary operator on S. Define S is **closed under** $*$, if $\forall a, b \in S$, then $a * b \in S$.

Example 1.2

$\mathbb{Z}_{<0}$ is **not** closed under $\times$. Since $-1, -2 \in \mathbb{Z}_{<0}$, and $(-1) \times (-2) = 2 \notin \mathbb{Z}_{<0}$.

1.2 Groups

Definition 1.3

Suppose a set G is closed under a binary operator $*$. Define $(G, *)$ is a **group** if it satisfy the following axioms.

(G1) $\forall a, b, c \in G$, $(a * b) * c = a * (b * c)$. (Is called associativity (結合律).)

(G2) $\exists e \in G$ such that $\forall x \in G$, $x * e = e * x = x$. (e is called identity element (單位元素).)

(G3) $\forall a \in G$, $\exists a' \in G$ such that $a * a' = a' * a = e$. (a' is inverse (反元素) of a.)

Definition 1.4

A group $(G,*)$ is abelian (阿貝爾群, or commutative groups 可交換群) if $\forall a,b \in G$, $a*b=b*a$. (滿足交換律)

Example 1.3 Let $G=\{M \in M_{n\times n}(\mathbb{R}) | M \text{ is invertible}\}$, prove that $(G,\cdot)$ is a non-abelian group.

(G0) $\forall A,B \in G$, $\exists A^{-1},B^{-1}$ such that $AA^{-1}=BB^{-1}=I_n$, Then

$$(AB)(B^{-1}A^{-1})=A(BB^{-1})A^{-1}=AI_nA^{-1}=I_n.$$

Thus AB is invertible, so $AB \in G$. Hence G is closed under $\cdot$.

(G1) $\forall A,B,C \in G$, $A(BC)=(AB)C$.

(G2) $\exists I_n \in G$, $\forall A \in G$ such that $AI_n=I_nA=A$.

(G3) $\forall A \in G$, $\exists A^{-1}$ such that $AA^{-1}=A^{-1}A=I_n$. Hence G is a group.

(Abelian) Let $A=\begin{bmatrix}1 & 1\\ 0 & 1\end{bmatrix}$, $B=\begin{bmatrix}1 & 2\\ 3 & 4\end{bmatrix}$, then $AB=\begin{bmatrix}4 & 6\\ 3 & 4\end{bmatrix} \neq \begin{bmatrix}1 & 3\\ 3 & 7\end{bmatrix}=BA$. Hence G is a non-abelian group.

Theorem 1.1

If $(G,*)$ is a group, then $\forall a,b,c \in G$, $a*b=a*c$ imply $b=c$, and $b*a=c*a$ imply $b=c$.

Proof

By (G3), then $\exists a' \in G$ such that $a*a'=a'*a=e$. Thus

$$\begin{aligned}
&a*b=a*c\\
\Rightarrow\, &a'*(a*b)=a'*(a*c)\\
\Rightarrow\, &(a'*a)b=(a'*a)c\\
\Rightarrow\, &b=c.
\end{aligned}$$

Similar, $b*a=c*a \Rightarrow b=c$.

Theorem 1.2

If $(G,*)$ is a group, then

1. $\exists! e \in G$ such that $\forall a \in G$, $a*e=e*a=a$.

2. $\forall a \in G$, $\exists! a' \in G$ such that $a*a'=a'*a=e$.

Proof

1. Suppose $\exists e, e' \in G$ such that $\forall a \in G$, $e * a = a * e = a$ and $e' * a = a * e' = a$. By Theorem 1, $e = e'$. Hence $\exists! e$ is a identity element.

2. Suppose $\exists a', a'' \in G$ such that $a * a' = a' * a = e$ and $a * a'' = a'' * a = e$. By Theorem 1, $a' = a''$. Hence $\exists! a'$ is inverse of a.

Theorem 1.3

If $(G, *)$ is a group, then $\forall a, b \in G$, we have $(a * b)' = b' * a'$.

Proof

Since $(a * b) * (b' * a') = a * (b * b') * a' = aea' = a * a' = e$. Hence $(b' * a')$ is the inverse of $(a * b)$, that is $(a * b)' = (b' * a')$.

Definition 1.5

Let $(G, *)$ be a set of G with a binary operation $*$.

1. If only (G0) hold, then define $(G, *)$ is a **semigroup**.

2. If (G0) and (G1) hold, then define $(G, *)$ is a **monoid**.

Theorem 1.4

Let $(G, *)$ be a semigroup, if

1. $\exists e \in G$ such that $\forall a \in G$, $e * a = a$, and

2. $\forall a \in G$, $\exists a^{-1} \in G$ such that $a^{-1} * a = e$.

then $(G, *)$ is a group.

1.3 Subgroup

Definition 1.6

If $(G, *)$ is a group, then the **order** $|G|$ of G is the number of elements in G.

Definition 1.7

Suppose $(G, *)$ is a group, and $H \subset G$. If H satisfy following condition

1. $\forall a, b \in H$, $a * b \in H$

2. $e \in H$

3. $\forall a \in H$, $a^{-1} \in H$.

then $(H, *)$ is a **subgroup** of $(G, *)$. Denote by $H \leq G$.

Theorem 1.5

Every group G has two subgroup G and $\{e\}$.

Definition 1.8 Let $(G, *)$ be a group, $a \in G$, and $n, m \in\in \mathbb{N} \cup \{0\}$, they following the operation.

1. $a^n = \underbrace{a * a * \cdot * a}_{n \text{ times}}$.
2. $a^{-m} = \underbrace{a^{-1} * a^{-1} * \cdot * a^{-1}}_{m \text{ times}}$.
3. $a^0 = e$, where e is the identity element of G.

Theorem 1.6

Let $(G, *)$ be a group and $a \in G$, then $H = \{a^n | n \in \mathbb{Z}\}$ is a subgroup of G and is the smallest subgroup of G that contains a. That is, every subgroup containing a contains H.

Proof

1. $\forall r, s \in \mathbb{Z}$, $a^r * a^s = a^{r+s} \in H$.
2. $e = a^0 \in H$.
3. $\forall a^r \in H$, $(a^r)^{-1} = a^{-r} \in H$.

So $H \leq G$. Hence H is a subgroup of $(G, *)$.

Definition 1.9

Let $(C, *)$ be a group and $a \in G$. Then $H = \{a^n | n \in \mathbb{Z}\}$ is called a **cyclic subgroup of G generated by** a, denote by $< a >$.

Definition 1.10

If $G =< a >$, then called a is a **generator** of G, or a **generates** G. that is $\forall x \in G$, $\exists n \in \mathbb{Z}_{>0}$ such that $x = a^n$.

1.4 Cyclic Group

Definition 1.11

$(G, *)$ is a cyclic group if $\exists a \in G$ such $G =< a >$.

Theorem 1.7

Every cyclic group is abelian.

Proof

Let $G =< a >$, then $\forall g_1, g_2 \in G$, $\exists r_1, r_2 \in \mathbb{Z}$ such that $g_1 = a^{r_1}$ and $g_2 = a^{r_2}$. Then

$$g_1 * g_2 = a^{a_1} a^{r_2} = a^{r_1 + r_2} = a^{r_2} a^{r_1} = g_2 * g_1.$$

Hence G is abelian.

Theorem 1.8 (Division Algorithm for $\mathbb{Z}$)

If $m \in \mathbb{R}_{>0}$ and $n \in \mathbb{Z}$, then $\exists! q, r \in \mathbb{Z}$ such that $m = qn` + r$ and $0 \leq r < m$.

Theorem 1.9

A subgroup of a cyclic group is cyclic.

Proof

Let $G =< a >$ and $H \leq G$. If $H = \{e\}$, then is cyclic. If $H \neq \{e\}$, then $a^n \in H$ for some $n \in \mathbb{Z}_{>0}$. Let m be the smallest positive integer such that $a^m \in H$. Let $c = a^m \in H$. Claim $H =< c >$. (i.e. $\forall b \in H$, $\exists q \in \mathbb{Z}$ such that $b = c^q$.) Let $b \in H \leq G =< a >$. $\exists n \in \mathbb{Z}$ such that $b = a^n$. By division algorithm, $\exists q, r \in \mathbb{Z}$ such that $n = qm + r$ and $0 \leq r < m$. Then

$$\begin{aligned} a^n &= a^{qm+r} = (a^m)^q * a^r \\ a^r &= a^n * (a^m)^{-q} \in H \text{ (Since } a^n, a^m \in H) \end{aligned}$$

Since m is the mallest positive integer such that $a^m \in H$, and $a^r \in H$ with $0 \leq r < m$, that force $r = 0$. Thus $n = mq \Rightarrow b = a^n = (a^m)^q = c^q \in H$. Hence H is cyclic.

Theorem 1.10

The subgroup of $(\mathbb{Z}, +)$ are precisely the groups $(n\mathbb{Z}, +)$ for $n \in \mathbb{Z}$.

Definition 1.12

Let $r, s \in \mathbb{Z}_{>0}$, then $H = \{nr + ms | n, m \in \mathbb{Z}\}$ is a subgroup of $(\mathbb{Z}, +)$. By Theorem 10, $\exists d \in \mathbb{Z}_{>0}$ such that $H =< d >$. Then d is the **greatest common divisor** (gcd) r and s. On the other hand, if $d = \gcd(r, s)$, then $\exists n, m \in \mathbb{Z}$ such that $d = nr + ms$.

Definition 1.13

Let $(G, *)$ and $(G', *')$ be two groups. Define G is **isomorphic** (同構), if $\exists a$ a one-to-one and onto function $\phi : G \to G'$ such that $\forall a, b \in G$, $\phi(a * b) = \phi(a) *' \phi(b)$, denoted by $G \simeq G'$.

Theorem 1.11

Let $G =< a >$, then

1. If $|G|$ is infinite, then $G \simeq (\mathbb{Z}, +)$.

2. If $|G| = n$ is finite, then $G \simeq (\mathbb{Z}_n, +)$.

Proof

If $\forall m \in \mathbb{Z}_{>0}$, $a^m \neq e$. Claim $a^h \neq a^k$ if $h \neq k$. Assume $a^h = a^k$ and $h > k$. Then $a^h * a^{-k} = a^{h-k} = a^0 = e$ and $h - k \in \mathbb{Z}_{>0}$. So $G = a^m | m \in \mathbb{Z}$. Define $\phi : G \to \mathbb{Z}$ with $a^m \to m$. Then ϕ is one-to-one and onto by claim. and $\phi(a^i * a^j) = \phi(a^{i+j}) = i + j = \phi(a^i) + \phi(a^j)$. Hence $G \simeq (\mathbb{Z}, +)$.

If $\exists m \in \mathbb{Z}_{>0}$ such that $a^m = e$. Let n be the smallest integer such that $a^n = e$. Claim $a^k \neq a^k$ if $0 < h << n$. If $a^h = a^k$, then $a^{k-h} = e$ and $0 < k - h < n$. So $G = a, a^2, \cdots, a^n = e$. Define $\phi : G \to \mathbb{Z}_n$ with $a_i \to i$ for $i = 0, 1, 2, \cdots n - 1$. Then ϕ is one-to-one and onto. Since $a^n = e$, so $a^i a^j = a^k$ where $k = i + j \in \mathbb{Z}_n$. Hence $G \simeq (\mathbb{Z}_n, +)$.

Theorem 1.12

Let $G =< a >$ and $|G| = n$, if $H =< a^r >$ with $r \in \mathbb{Z}_{>0}$, then $|H| = n/d$, where $d = \gcd(n, r)$. Also $< a^r > = < a^s >$ if and only if $\gcd(n, r) = \gcd(n, s)$.

Theorem 1.13

If $G =< a >$ and $|G| = n$. If $\gcd(n, r) = 1$, then $G =< a^r >$.

Chapter 2

Permutations, Cosets and Direct Products

2.1 Groups of Permutations

Definition 2.1

A **permutation** of a set A is a function $\phi : A \to A$ that one-to-one and onto.

Example 2.1

Let $A = \{1, 2, 3, 4\}$ and $\phi : A \to A$

$$1 \mapsto 2, \quad 2 \mapsto 1, \quad 3 \mapsto 4, \quad 4 \mapsto 3$$

is a permutation. As we write

$$\phi = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix} \quad \text{or} \quad \phi = (1, 2)(3, 4)$$

Definition 2.2

Suppose A is a nonempty set, then let S_A be the set of all permutation of A.

Theorem 2.1

Define function composition $\circ$ is a binary operation of S_A, then $(S_A, \circ)$ is a group.

Proof

(G0) Let $f, g \in S_A$ and $a_1, a_2 \in A$. If $f \circ g(a_1) = f \circ g(a_2)$, then $f(g(a_1)) = f(g(a_2))$, since f is one-to-one, then $g(a_1) = g(2)$, since g is one-to-one, then $a_1 = a_2$. Hence $f \circ g$ is one-to-one.

Let $f, g \in S_A$ and $a \in A$. Since f is onto, so $\exists a' \in A$ such that $f(a') = a$. Since g is onto, so $\exists a'' \in A$ such that $g(a'') = a'$. Then $f \circ g(a'') = f(g(a'')) = f(a') = a$. Hence $f \circ g$ is onto.

So $\forall f, g \in S_A$, $f \circ g \in S_A$.

(G1) Let $f, g, h \in S_A$ and $a \in A$, we have

$$(f \circ g) \circ h(a) = (f \circ g)(h(a)) = f(g(h(a)))$$
$$f \circ (g \circ h)(a) = f \circ (g(g(a))) = f(g(h(a)))$$

Hence $\forall f, g, h \in S_A$, $(f \circ g) \circ h = f \circ (g \circ h)$.

(G2) Let $i(a) = a$ for all $a \in A$, then $i \in S_A$. Let $f \in S_A$, then

$$f \circ i(a) = f(i(a)) = f(a)$$
$$i \circ f(a) = i(f(a)) = f(a)$$

Hence i is the identity of S_A, such that $\forall f \in S_A$, $f \circ i = i \circ f = f$.

(G3) Let $f \in S_A$, and $f^{-1} : A \to A$ with $f^{-1}(a) = a'$ where $f(a') = a$. (*Note that $\forall a \in A$, $\exists! a' \in A$ such that $f(a') = a$, since f is one-to-one.*) So

$$f \circ f^{-1}(a) = f(f^{-1}(a)) = f(a') = a = i(a)$$
$$f^{-1} \circ f(a') = f^{-1}(f(a')) = f^{-1}(a) = a' = i(a')$$

Hence $\forall f \in S_A$, $\exists f^{-1} \in S_A$ such that $f \circ f^{-1} = f^{-1} \circ f = i$.

Hence $(S_A, \circ)$ is a group.

Definition 2.3

Let $A = \{1, 2, \cdots, n\}$, The group S_A is called **symmetric group** on n letters, denote by S_n, and $|S_A| = n!$.

Example 2.2

Let $A = 1, 2, 3$, then S_A is S_3, and $|S_3| = 3! = 6$.

$$\phi_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} = e \in S_3, \qquad \phi_2 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} = (2, 3) \in S_3,$$

$$\phi_3 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = (1, 2) \in S_3, \qquad \phi_4 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = (1, 2, 3) \in S_3,$$

$$\phi_5 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = (1, 3, 2) \in S_3, \qquad \phi_6 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} = (1, 3) \in S_3.$$

Operator use first for the latter (先對後項作用).

$$(1\ 2\ 3)^2 = (1\ 2\ 3)(1\ 2\ 3) = (1\ 3\ 2).$$

Remark 2.1

S_3 is **non-abelian**.

$$(1\ 2\ 3)(1\ 2) = (1\ 3)$$
$$(1\ 2)(1\ 2\ 3) = (2\ 3).$$

Definition 2.4

Let G be a group and $a_i \in G$, $i \in I$. If H is the smallest subgroup of G containing $\{a_i | i \in I\}$, then define H **is generated by** $\{a_i | i \in I\}$, and $H =< a_i | i \in I >$.

Theorem 2.2

$H =< a_i | i \in I >$ has at element precisely these element of G.

Definition 2.5

Define $D_n =< a, b | a^n = b^2 = e, bab = a^{-1} >$ is the nth **dihedral group**, that is the group of symmetries of the regular n-gun, which include rotations and reflections.

Remark 2.2

1. $S_3 \simeq D_3$.
2. $|D_n| = 2n$.

Theorem 2.3

Let $(G, *)$ and $(G', *')$ be groups. If $\phi : G \to G'$ be a one-to-one function such that $\forall x, y \in G$, $\phi(x * y) = \phi(x) *' \phi(y)$. Then $\phi(G) \leq G'$ and $G \simeq \phi(G)$.

Proof First

(G0) $\forall x', y' \in \phi(G)$, $\exists x, y \in G$ such that $\phi(x) = x'$ and $\phi(y) = y'$. Then

$$x' *' y' = \phi(x) *' \phi(y) = \phi(x * y) \in \phi(G)$$

(G2) Let e' be the identity of G'. Then

$$e' *' \phi(e) = \phi(e) = \phi(e * e) = \phi(e) *' \phi(e)$$
$$\Rightarrow e' = \phi(e) \in \phi(G).$$

(G2) $\forall x' \in \phi(G)$, $\exists x \in G$ such that $\phi(x) = x'$, then

$$e' = \phi(e) = \phi(x * x^{-1}) = \phi(x) *' \phi(x^{-1}) = x' *' \phi(x^{-1})$$
$$\Rightarrow (x')^{-1} = \phi(x^{-1})$$

Hence $\phi(G) \leq G'$.

Since $\phi : G \to \phi(G)$ is a one-to-one and onto function with $\forall x, y \in G$, $\phi(xy) = \phi(x)\phi(y)$. Hence $G \simeq \phi(G)$.

Theorem 2.4

If G is a group and $|G| = n$, then $G \leq S_n$.

Theorem 2.5 (Cayley's Theorem)

Every group G is isomorphic to a subgroup of S_G.

Proof

x Let G be a group. Define $\phi : G \to S_G$, for $x \in G$, let $\lambda_x : G \to G$ define by $\lambda_x(g) = xg$. Now we check $\lambda_x \in S_G$ (i.e. λ_x is one-to-one and onto.) Assume $\forall g_1, g_2 \in G$, $\lambda_x(g_1) = \lambda_x(g_2)$, then

$$\lambda_x(g_1) = \lambda_x(g_2) \quad \Rightarrow \quad xg_1 = xg_2 \quad \Rightarrow \quad g_1 = g_2$$

thus λ_x is one-to-one. Since $\forall g \in G$, $x^{-1}g \in G$, then

$$\lambda_x(x^{-1}g) = xx^{-1}g = g$$

thus λ_x is onto. Hence $\lambda_x \in S_G$.
Assume $\exists x_1, x_2 \in G$ such that $\phi(x_1) = \phi(x_2)$, then

$$\phi(x_1) = \phi(x_2) \quad \Rightarrow \quad \lambda_{x_1} = \lambda_{x_2},$$

then $\forall g \in G$,

$$\lambda_{x_1}(g) = \lambda_{x_2}(g) \quad \Rightarrow \quad x_1 g = x_2 g \quad \Rightarrow \quad x_1 = x_2$$

then ϕ is one-to-one. Let $x, y \in G$, then

$$\phi(xy) = \lambda_{xy}$$
$$\phi(x)\phi(y) = \lambda_x \circ \lambda_y$$

let $g \in G$, then

$$\lambda_{xy}(g) = xyg$$
$$\lambda_x \circ \lambda_y(g) = \lambda_x(\lambda_y(g)) = \lambda_x(yg) = xyg$$

Hence G is isomorphic to a subgroup of S_G.

2.2 Orbits, Cycles and the Alternating Groups

Definition 2.6

An **equivalence relation** on a set A is a subset R of $A \times A$ satisfies the following properties for $\forall x, y, z \in A$.

Reflexive xRx.

Symmetric If xRy, then yRx.

Transitive If xRy and yRz, then xRz.

The xRy means $(x, y) \in R \subseteq (A \times A)$.

Definition 2.7

A **partition** (分割) of a set A is collection of nonempty subsets of A such that every element of A is in exactly one of the subset.

Theorem 2.6

Let A be a nonempty set and $\sim$ be an equivalence relation on A, then

1. The relation $\sim$ yields a partition of A.
2. Each partition of A give rise to an equivalence relation $\sim$ on A, where $a \sim b$.

Theorem 2.7

Let $A = \{1, 2, \cdots, n\}$ and $\sigma = S_A$. Then $\forall a, b \in A$, $a \sim b$ if and only if $\exists n \in \mathbb{Z}$ such that $\sigma^n(a) = b$, where $\sim$ is an equivalence relation on A.

Proof

Reflexive: Since $a = \sigma^0(a)$ and $\sigma^0(e) = e$, then $a \sim a$.

Symmetric: If $a \sim b$, then $\exists n \in \mathbb{Z}$ such that $\sigma^n(a) = b$, therefore $a = \sigma^{-n}(b)$, since $-n \in \mathbb{Z}$, so $b \sim a$.

Transitive: If $a \sim b$ and $b \sim c$, $\exists m, n \in \mathbb{Z}$ such that $\sigma^m(a) = b$ and $\sigma^n(b) = c$, therefore $c = \sigma^m(b) = \sigma^m(\sigma^n(a)) = \sigma^{m+n}(b)$. Since $(m + n) \in \mathbb{Z}$, then $a \sim c$.

Definition 2.8

Let $\sigma \in A$. The equivalence classes in A determine by $\sim$ are the **orbits** of σ.

Example 2.3

Find all orbits of

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 8 & 6 & 7 & 4 & 1 & 5 & 2 \end{pmatrix} \in S_8.$$

Solution

Since

$$\begin{cases} 1 \xrightarrow{\sigma} 3 \xrightarrow{\sigma} 6 \xrightarrow{\sigma} 1 \\ 2 \xrightarrow{\sigma} 8 \xrightarrow{\sigma} 2 \\ 4 \xrightarrow{\sigma} 7 \xrightarrow{\sigma} 5 \xrightarrow{\sigma} 4 \end{cases}$$

Hence $\{1,3,6\}$, $\{2,8\}$ and $\{4,7,5\}$ are all orbits of σ.

Definition 2.9

1. A **permutation** $\sigma \in S_n$ in a cycle if it has at most one orbit containing more than one element.

2. The **length** of a cycle is the number of elements in its largest orbit.

3. A cycle of length 2 is called **transposition**.

Example 2.4

Let $\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = (1\ 2)$, then $(1,2)$ is a cycle and length of $(1,2)$ is 2.

Theorem 2.8

Every permutation of a finite set is a product of disjoint cycles.

Proof

Let σ is a permutation of a finite set. Suppose $B_1, B_2, \cdots, B_r$ be the orbits of σ, define the cycle

$$\mu_i(x) = \begin{cases} \sigma(x) & \text{if } x \in B_i \\ x & \text{if } x \notin B_i \end{cases}.$$

then $\sigma = \mu_1\mu_2 \cdots m_r$, since $B_1, B_2, \cdots, B_r$ are disjoint, the cycles $\mu_1, \mu_2, \cdots, \mu_r$ are disjoint also.

Remark 2.3

$(1\ 2\ 3) = (1\ 3)(1\ 2)$, and $(a_1\ a_2 \cdots a_n) = (a_1\ a_n)(a_1\ a_{n-1}) \cdots (a_1 a_2)$.

Corollary 2.1

Any permutation of a finite set of at least two elements is a product of transposition.

Theorem 2.9

No permutation in S_n can be expressed both as a product of even number transposition and as a product of odd number transposition.

Definition 2.10

Let $\sigma \in S_n$ is even(odd) if $\sigma = \tau_1\tau_2\cdots\tau_n$, where τ_i are transposition and m is even(odd).

Definition 2.11

The subgroup of S_n consisting of the even permutation of n letters is the **alternating group A_n of n letters**.

Theorem 2.10

If $n \geq 2$, then $A_n \leq S_n$ and $|A_n| = (n!)/2$.

Proof

Claim $A_n \leq S_n$,

(G0) Let $\sigma, \mu \in A_n$, then $\sigma\mu$ is even, therefore $\sigma\mu \in A_n$.

(G2) $e = (1\ 2)(2\ 1) \in A$.

(G3) Let $\sigma = \tau_1\tau_2\cdots\tau_m \in A_n$, where τ_i for $1 \leq i \leq n$ are transposition. Let $\mu = \tau_m\tau_{m-1}\cdots\tau_2\tau_1 \in A_n$. Then $\sigma\mu = e \in A$. Since ${\tau_i}^{-1} = \tau_i$. So $\sigma^{-1} = \mu \in A$

Hence $A_n \leq S_n$. Claim $|A_n| = (n!)/2$, let $\tau = (1\ 2)$ and define $\lambda : A_n \to B_n$ such that $\forall\sigma \in A_n$, $\lambda(\sigma) = \tau\sigma$. If $\tau\sigma_1 = \tau\sigma_2$, then $\sigma_1 = \sigma_2$, so λ is one-to-one. And $\forall\mu \in B_n$, $\tau\mu \in A_n$, so $\lambda(\tau^{-1}u) = \tau\tau^{-1}\mu = \mu$. So we have $|A_n| = |B_n|$ and $|S_n| = n!$. Hence $|A_n| = (n!)/2$.

2.3 Cosets and the Theorem of Lagrange

Theorem 2.11

Suppose G be a group and $H \leq G$. Let the relation $\sim_L$ be defined on G by $a \sim_L b$ if and only if $a^{-1}b \in H$, then $\sim_L$ is a equivalence relation.

Proof

Since

Reflexive $\forall a \in G$, $a^{-1}a = e \in H$, so $a \sim_L a$.

Symmetric If $a \sim_L b$, then $a^{-1}b \in H$. Since $H \leq G$, then $(a^{-1}b)^{-1} = b^{-1}a \in H$, so $b \sim_L b$.

Transitive If $a \sim_L b$ and $b \sim_L c$, then $a^{-1}b \in H$ and $b^{-1}c \in H$, therefore $(a^{-1}b)(b^{-1}c) = a^{-1}c \in H$, so $a \sim_L c$.

Hence $\sim_L$ is a equivalence relation.

Example 2.5

Let $G = \mathbb{Z}$ and $H = 5\mathbb{Z}$, then $a \sim_L b \iff a^{-1}b = -a + b \in 5\mathbb{Z}$.

Definition 2.12

Let G be a group and $H \leq G$. Then the subset $aH = \{ah | h \in H\}$ of G is the **left coset of H containing a**.

Example 2.6

Find all left coset of $5\mathbb{Z}$ of $\mathbb{Z}$.

Solution

Let $a = 1$, then $1 \sim_L b \iff -1 + b \in 5\mathbb{Z} \iff b \in 1 + 5\mathbb{Z} = aH$. Similar, if $a = 2$,then $2 + 5\mathbb{Z} = aH$. Hence $5\mathbb{Z}, 1 + 5\mathbb{Z}, 2 + 5\mathbb{Z}, 3 + 5\mathbb{Z}$ and $4 + 5\mathbb{Z}$ are all cosets of $5\mathbb{Z}$ of $\mathbb{Z}$.

Theorem 2.12 (The Theorem of Lagrange)

If G is a finite group and $H \leq G$, then $|H| \;\Big|\; |G|$.

Proof

Let $g \in G$, define $\phi : H \to gH$ with $\phi(h) = gh$. If $\exists h_1, h_2 \in H$ such that $\phi(h_1) = \phi(h_2)$, then

$$\phi(h_1) = \phi(h_2) \quad \Rightarrow \quad gh_1 = gh_2 \quad \Rightarrow \quad h_1 = h_2$$

thus ϕ is one-to-one. $x \in gH$, then $\exists h \in H$ such that $x = gh$, so

$$\phi(h) = gh = x$$

thus ϕ is onto. Hence $|G| = |gH|$ for all $g \in G$. Let r be the number of left coset of H of G. Then $|G| = r|H|$. Since $\sim_L$ gives a partition of G, so $|H| \;\Big|\; |G|$.

Corollary 2.2

Suppose G is a group. If $|G| = p$ is a prime, then G is cyclic.

Proof

Let $a \in G \backslash \{e\}$ and $H = \langle a \rangle \leq G$. By The Theorem of Lagrange, $|H| \Big| |G|$. Since $|G|$ is a prime and $|H| > 1$. Hence $|H| = |G|$, that is $G = H = \langle a \rangle$.

Theorem 2.13

If G is a finite set, then $|a| \Big| |G|$ for all $a \in G$, where $|a| = |\langle a \rangle|$ is the order of a.

Definition 2.13

Let G is a group and $H \leq G$. Then the number of left cosets of H in G is the **index** $(G : H)$ **of** H **in** G.

Remark 2.4

If G is a finite group and $H \leq G$, then $(G : H) = \dfrac{|G|}{|H|}$.

Theorem 2.14

Suppose G is a group and $K \leq H \leq G$. If $(G : H)$ and $(H : K)$ are both finite, then $(G : K)$ is finite and $(G : K) = (G : H)(H : K)$.

2.4 Direct Products and Finitely Generated Abelian Groups

Direct Products

Definition 2.14

The **Cartesian product of set** $S_1, S_2, \cdots, S_n$ is the set of all ordered n-tuples $(a_1, a_2, \cdots, a_n)$ where $a_i \in S_i$ for $1 \leq i \leq n$, The Cartesian product denoted by

$$S_1 \times S_2 \times \cdots \times S_n \quad \text{or} \quad \prod_{i=1}^{n} S_i.$$

Theorem 2.15

Let $G_1, G_2, \cdots, G_n$ be groups. For $(a_1, a_2, \cdots, a_n), (b_1, b_2, \cdots, b_n) \in \prod_{i=1}^{n} G_i$. If define

$$(a_1, a_2, \cdots, a_n)(b_1, b_2, \cdots, b_n) = (a_1b_1, a_2b_2, \cdots, a_nb_n)$$

then $\prod_{i=1}^{n} G_i$ is a group, and called the **direct product of group** G_i.

Proof

(G0) Since $a_i, b_i \in G_i$ and G_i is a a group, then $a_ib_i \in G_i$, so $\prod_{i=1}^{n} G_i$ is closed under the operator.

(G1) Let $(a_1, a_2, \cdots, a_n), (b_1, b_2, \cdots, b_n), (c_1, c_2, \cdots, c_n) \in \prod_{i=1}^{n} G_i$, then

$$\begin{aligned}
&[(a_1, a_2, \cdots, a_n)(b_1, b_2, \cdots, b_n)]\,(c_1, c_2, \cdots, c_n) = (a_1b_1, a_2b_2, \cdots, a_nb_n)(c_1, c_2, \cdots, c_n) \\
=&((a_1b_1)c_1, (a_2b_2)c_2, \cdots, (a_nb_n)c_n) = (a_1(b_1c_1), a_2(b_2c_2), \cdots, a_n(b_nc_n)) \\
=&(a_1, a_2, \cdots, a_n)(b_1c_1, b_2c_2, \cdots, b_nc_n) = (a_1, a_2, \cdots, a_n)\,[(b_1, b_2, \cdots, b_n)(c_1, c_2, \cdots, c_n)]\,.
\end{aligned}$$

(G2) Let $e_i \in G_i$, then $(e_1, e_2, \cdots, e_n)$ is the identity of $\prod_{i=1}^{n} G_i$ such that $\forall (a_1, a_2, \cdots, a_n) \in \prod_{i=1}^{n} G_i$,

$$(e_1, e_2, \cdots, e_n)(a_1, a_2, \cdots, a_n) = (a_1, a_2, \cdots, a_n) = (a_1, a_2, \cdots, a_n)(e_1, e_2, \cdots, e_n).$$

(G3) Let $a_i \in G_i$, since G_i is a group, then $\exists {a_i}^{-1}$ such that $a_i {a_i}^{-1} = {a_i}^{-1} a_i = e_i$, so

$$
\begin{aligned}
&(a_1, a_2, \cdots, a_n)({a_1}^{-1}, {a_2}^{-1}, \cdots {a_n}^{-1}) = ({a_1}^{-1}, {a_2}^{-1}, \cdots {a_n}^{-1})(a_1, a_2, \cdots, a_n) \\
=&(e_1, e_2, \cdots, e_n).
\end{aligned}
$$

Hence $\prod_{i=1}^{n} G_i$ is a group.

Example 2.7

Show that $\mathbb{Z}_2 \times \mathbb{Z}_3 \simeq \mathbb{Z}_6$.

Solution

We have 1 is the generator of $\mathbb{Z}_2$ and $\mathbb{Z}_3$, and $\mathbb{Z}_2 \times \mathbb{Z}_3 = \{(0,0), (0,1), (0,2), (1,0), (1,1), (1,2)\}$, so

$$
\begin{aligned}
&1 \times (1,1) = (1,1), \quad 2 \times (1,1) = (0,2), \quad 3 \times (1,1) = (1,0), \\
&4 \times (1,1) = (0,1), \quad 5 \times (1,1) = (1,2), \quad 6 \times (1,1) = (0,0)
\end{aligned}
$$

thus $\mathbb{Z}_2 \times \mathbb{Z}_3 = \langle (1,1) \rangle$ and $\mathbb{Z}_2 \times \mathbb{Z}_3 \simeq \mathbb{Z}_6$.

Theorem 2.16

Suppose $m, n \in \mathbb{N}$, then $\gcd(m,n) = 1 \iff \mathbb{Z}_m \times \mathbb{Z}_n \simeq \mathbb{Z}_{mn}$.

Proof

$\Rightarrow$) Claim that $\langle (1,1) \rangle = \mathbb{Z}_m \times \mathbb{Z}_n$. If $k(1,1) = (k,k) = (0,0) \in \mathbb{Z}_m \times \mathbb{Z}_n$, then $m|k$ and $n|k$, thus $mn|k$ since $\gcd(m,n) = 1$. Hence $k \geq mn$. But $mn(1,1) = (mn, mn) = (0,0) \in \mathbb{Z}_m \times \mathbb{Z}_n$, so the order of $(1,1)$ in $\mathbb{Z}_m \times \mathbb{Z}_n$ is mn. So $\langle (1,1) \rangle = \mathbb{Z}_m \times \mathbb{Z}_n$.

$\Leftarrow$) Assume $\gcd(m,n) = d > 1$. Then $m \Big| \dfrac{mn}{d}$ and $n \Big| \dfrac{mn}{d}$. For all $(r,s) \in \mathbb{Z}_m \times \mathbb{Z}_n$, $\dfrac{mn}{d}(r,s) = \left(\dfrac{mn}{d}r, \dfrac{mn}{d}s\right) = (0,0) \in \mathbb{Z}_m \times \mathbb{Z}_n$ since $m \Big| \dfrac{mn}{d}$ and $n \Big| \dfrac{mn}{d}$. Hence $\nexists (r,s) \in \mathbb{Z}_m \times \mathbb{Z}_n$ can generate the entire group. Thus $\mathbb{Z}_m \times \mathbb{Z}_n$ is not cyclic, so $\mathbb{Z}_m \times \mathbb{Z}_n \simeq \mathbb{Z}_{mn}$, it contradict the condition. Hence $\gcd(m,n) = 1$.

Theorem 2.17

$\prod_{i=1}^{n} \mathbb{Z}_i \simeq \mathbb{Z}_{m_1 m_2 \cdots m_n} \iff \gcd(m_i, m_j) = 1$ for all $1 \leq i < j \leq n$.

Definition 2.15

Let $r_1, r_2, \cdots, r_m \in \mathbb{N}$ and let $H = \{n \in \mathbb{N} \big| r_i | n \text{ with } 1 \leq i \leq m\}$. Then $H \leq \mathbb{Z}$ and $\exists l \in \mathbb{N}$ such that $H = \langle l \rangle$, where l is called the **least common Multiple (lcm)** of $r_1, r_2, \cdots, r_m$.

Theorem 2.18

Let $(a_1, a_2, \cdots, a_n) \in \prod_{i=1}^n G_i$. If the finite order of a_i in G_i is r_i, then the order of $(a_1, a_2, \cdots, a_n)$ in $\prod_{i=1}^n G_i$ is $\text{lcm}(r_1, r_2, \cdots, r_n)$.

Example 2.8

Fine the order $(8, 4, 10)$ in $\mathbb{Z}_{12} \times \mathbb{Z}_{60} \times \mathbb{Z}_{24}$.

Solution

The order of 8 in $\mathbb{Z}_{12}$ is $\dfrac{12}{\gcd(8,12)} = \dfrac{12}{4} = 3$, the order of 4 in $\mathbb{Z}_{60}$ is $\dfrac{60}{\gcd(4,60)} = \dfrac{60}{4} = 15$, and the order of 10 in $\mathbb{Z}_{24}$ is $\dfrac{24}{\gcd(10,24)} = \dfrac{24}{2} = 12$. Hence the order $(8, 4, 10)$ in $\mathbb{Z}_{12} \times \mathbb{Z}_{60} \times \mathbb{Z}_{24}$ is $\text{lcm}(3, 15, 12) = 60$.

Theorem 2.19 (Fundamental Theorem of Finitely Generated Ablien Groups)

Every finitely generated ablien group G is isomorphic to a direct product of cyclic groups of the form $\mathbb{Z}_{{P_1}^{r_1}} \times \mathbb{Z}_{{P_2}^{r_2}} \times \cdots \times \mathbb{Z}_{{P_n}^{r_n}}$. Where p_i are primes, not necessary distinct and $r_i \in \mathbb{N}$.

Example 2.9

Find all ablien groups of order 360.

Solution

Since $360 = 2^3 \times 3^2 \times 5$. So all ablien groups of order 360 are

$$\begin{aligned}
\mathbb{Z}_{360} &\simeq \mathbb{Z}_{2^3} \times \mathbb{Z}_{3^2} \times \mathbb{Z}_5 \\
&\simeq \mathbb{Z}_{2^2} \times \mathbb{Z}_2 \times \mathbb{Z}_{3^2} \times \mathbb{Z}_5 \\
&\simeq \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_{3^2} \times \mathbb{Z}_5 \\
&\simeq \mathbb{Z}_{2^3} \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_5 \\
&\simeq \mathbb{Z}_{2^2} \times \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_5 \\
&\simeq \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_5.
\end{aligned}$$

2.5 Homomorphisms

Definition 2.16

Let $(G, *)$ and $(G', *')$ be two group. A map $\phi : G \to G'$ is a group homomorphism if

$$\phi(a * b) = \phi(a) *' \phi(b)$$

for all $a, b \in G$.

Example 2.10

Let $A \in M_{m\times n}(\mathbb{R})$, then $\phi : \mathbb{R}^n \to \mathbb{R}^m$ with $\phi(v) = Av$ is linear transformation. For all $v, w \in \mathbb{R}^n$,

$$\phi(v + w) = A(v + w) = A(v) + A(w) = \phi(v) + \phi(w).$$

Hence ϕ is a homomorphism.

Definition 2.17

Let $\phi : X \to Y$ be a map, $A \subseteq X$ and $B \subseteq Y$, then

1. The **image** of A in Y under ϕ is $\phi(A) = \{\phi(a)|a \in A\}$.

2. The **inverse image** of B in X under ϕ is $\phi^{-1}(B) = \{x \in X|\phi(x) \in B\}$.

Theorem 2.20

Let $\phi : G \to G'$ be a group homomorphism, then

1. $\phi(e)$ is the identity element e' in G', where e is identity element in G.

2. $\phi(a^{-1}) = [\phi(a)]^{-1}$, for all $a \in G$.

3. $\phi(H) \le G'$, for all $H \le G$.

4. $\phi^{-1}(K') \le G$, for all $k' \le G'$.

Proof

1. For all $a \in G$,

$$\begin{aligned} &\phi(a) = \phi(ae) = \phi(a)\phi(e) \\ \Rightarrow\, &\phi(a)^{-1}\phi(a) = \phi(a)^{-1}\phi(a)\phi(e) \\ \Rightarrow\, &e' = \phi(e) \end{aligned}$$

   were e' is the identity in G', so that $\phi(e) = e'$.

2. For all $a \in G$,

$$\begin{aligned} &e' = \phi(e) = \phi(aa^{-1}) = \phi(a)\phi(a^{-1}) \\ \Rightarrow\, &\phi(a)^{-1}e' = \phi(a)^{-1}\phi(a)\phi(a^{-1}) \\ \Rightarrow\, &\phi(a)^{-1} = \phi(a^{-1}) \end{aligned}$$

3. (G0) For all $a', b' \in \phi(H)$, $\exists a, b \in H$ such that $\phi(a) = a'$ and $\phi(b) = b'$, then $a'b' = \phi(a)\phi(b) = \phi(ab) \in \phi(H)$.

(G2) Since $e \in H$, then $e' = \phi(e) \in \phi(H)$.

(G3) For all $a' \in \phi(H)$, $\exists a \in H$ such that $\phi(a) = a'$, then $(a')^{-1} = \phi(a)^{-1} = \phi(a^{-1}) \in \phi(H)$, since $a' \in H \leq G$.

Hence $\phi(H) \leq G$.

4. Similarly to 3.

Definition 2.18

Let $\phi : G \to G'$ be a group homomorphism. The set

$$\phi^{-1}(e') = \{x \in G | \phi(x) = e'\}$$

is the **kernel** of ϕ, denote by $\ker(\phi)$.

Example 2.11

Let $A \in M_{m\times m}(\mathbb{R})$ and $\phi : \mathbb{R}^n \to \mathbb{R}^m$ with $\phi(v) = Av$. Find the $\ker(\phi)$.

Solution

$$\begin{aligned}\ker(\phi) &= \{v \in \mathbb{R}^n | \phi(v) = 0\} \\ &= \{v \in \mathbb{R}^n | Av = 0\} \\ &= \text{The null space of } A.\end{aligned}$$

Theorem 2.21

Let $\phi : G \to G'$, then $\ker(\phi) \leq G$.

Proof

(G0) Let $a, b \in \ker(\phi)$,

$$\phi(ab) = \phi(a)\phi(b) = e'e' = e'.$$

So $ab \in \ker(\phi)$.

(G2) Since $\phi(e) = e'$, thus $e \in \ker(\phi)$.

(G3) For all $a \in \ker(\phi)$,

$$\phi(a^{-1}) = \phi(a)^{-1} = (e')^{-1} = e'$$

So $a^{-1} \in \ker(\phi)$.

Theorem 2.22

Let $\phi : G \to G'$ be a group homomorphism and $H = \ker(\phi)$, then for all $a \in G$,

$$\{x \in G | \phi(x) = \phi(a)\} = aH = Ha.$$

Solution

Claim $\{x \in G | \phi(x) = \phi(a)\} = Ha$,

$\subseteq$: Assume that $\phi(x) = \phi(a)$, then

$$e' = \phi(a)\phi(a)^{-1} = \phi(x)\phi(a)^{-1} = \phi(x)\phi(a^{-1}) = \phi(xa^{-1}),$$

So $xa^{-1} \in \ker(\phi) = H$, therefore $x \in aH$.

$\supseteq$: For all $x \in Ha$, $\exists h \in H = \ker(\phi)$ such that $x = ha$, so

$$\phi(x) = \phi(ha) = \phi(h)\phi(a) = e\phi(a) = \phi(a),$$

So $x \in \{x \in G | \phi(x) = \phi(a)\}$.

Hence $\{x \in G | \phi(x) = \phi(a)\} = Ha$. Similarly, $\{x \in G | \phi(x) = \phi(a)\} = aH$.

Corollary 2.3

A group homomorphism $\phi : G \to G'$ is one-to-one if and only if $\ker(\phi) = \{e\}$.

Proof

$\Rightarrow$) Since $\phi(e) = e'$, thus $e \in \ker(\phi)$. Since ϕ is one-to-one, thus $\ker(\phi) = \{e\}$.

$\leftarrow$) By Theorem, For all $a \in G$, $\{x \in G | \phi(x) = \phi(a)\} = a \ker(\phi) = a\{e\} = \{a\}$.

Definition 2.19

Let G be a group and $H \leq G$, H is **normal** if for all $g \in G$, $gH = Hg$, denote by $H \trianglelefteq G$.

Theorem 2.23

Let G be a group and $H \leq G$, then the following are equivalence

1. $gH = Hg$, for all $g \in G$.
2. $gHg^{-1} = H$, for all $g \in G$.
3. $gHg^{-1} \subseteq H$, for all $g \in G$.

Proof

1. (1) $\iff$ (2) and (2) $\Rightarrow$ (3) are trival.

2. (3) $\Rightarrow$ (2). For all $g \in G$, $g^{-1} \in G$, then

$$\begin{aligned} & g^{-1}H(g^{-1})^{-1} \subseteq H \\ \Rightarrow & g^{-1}Hg \subseteq H \\ \Rightarrow & H \subseteq gHg^{-1} \end{aligned}$$

   So we have $gHg^{-1} \subseteq H$ and $H \subseteq gHg^{-1}$, thus $gHg^{-1} = H$.

Corollary 2.4

If $\phi : G \to G'$ is a group homomorphism, then $\ker(\phi) \trianglelefteq G$.

Theorem 2.24

Suppose G is a abelian group, if $H \leq G$, then $H \trianglelefteq G$.

Proof

Suppose $H \leq G$. Let $g \in G$, then for all $x \in gH$, $\exists h \in H$ such that $x = gh$, then

$$\begin{aligned} & x = gh = hg \text{ (Since } G \text{ is abelian)} \\ \Rightarrow & x \in Hg \\ \Rightarrow & gH \leq Hg. \end{aligned}$$

Similarly, $Hg \leq gH$, thus $gH = Hg$. Hence $H \trianglelefteq G$.

2.6 Factor Groups

Definition 2.20

Suppose G is a group and $H \leq G$. Define a binary operator on all left cosets by $aHbH = (ab)H$ for all $a, b \in G$.

Theorem 2.25

The left cosets multiplication define by $aHbH = (ab)H$ if and only if $H \trianglelefteq G$.

Proof

$\Rightarrow$) Claim $aH = Ha$ for all $a \in G$.

$\subseteq$) Let $x \in aH$, then $xH = aH$, and

$$\begin{cases} xHa^{-1}H = (xa^{-1})H \\ aHa^{-1}H = (aa^{-1})H = eH = H \end{cases}$$

Since the left cosets multiplication is will define. so

$$(xa^{-1})H = H \quad \Rightarrow \quad xa^{-1} = h \in H \quad \Rightarrow \quad x = ha \in Ha$$

Hence $aH \subseteq Ha$.

$\supseteq$) Since

$$\begin{aligned} a^{-1}HaH &= (aa^{-1})H = H \\ &\Rightarrow a^{-1}ha \in H, \forall h \in H \\ &\Rightarrow ha \in aH, \forall h \in H \\ &\Rightarrow Ha \subseteq aH. \end{aligned}$$

Hence $aH = Ha$.

$\Leftarrow$) Assume $a_1H = a_2H$ and $b_1H = b_2H$, then $\exists h_1, h_2 \in H$ such that $a_1 = a_2h_1$ and $b_1 = b_2h_2$, so

$$a_1b_1 = (a_2h_1)(b_2h_2) = a_2(h_1b_2)h_2$$

Since $Hb_2 = b_2H$, so $\exists h_2 \in H$ such that $h_1b_2 = b_2h_3$, then

$$a_1b_1 = a_2(h_1b_2)h_2 = (a_2b_2)(h_3h_2) \in (a_2b_2)H$$

thus $a_1b_1 \in a_2b_2H$. Hence $a_1b_1H = a_2b_2H$ since left cosets gives a partition of G.

Definition 2.21 Let $H \triangleq G$, then the cosets of H form a group G/H under the binary operator $(aH)(bH) = (ab)H$, called the **factor group (or quotient group) of G by H**

Proof

(G0) By theorem.

(G1) For all $a, b, c \in G$, we have

$$(aHbH)cH = (ab)HcH = ((ab)c)H$$
$$aH(bHcH) = aH(bc)H = (a(bc))H$$

Since $(ab)c = a(bc)$, thus $(aHbH)cH = aH(bHcH)$.

(G2) For all $a \in G$, $(aH)(eH) = (ae)H = aH$, thus $eH = H$ is the identity in G/H.

(G3) For all $a \in G$,

$$(aH)(a^{-1}H) = (aa^{-1})H = H$$
$$(a^{-1}H)(aH) = (a^{-1}a)H = H$$

Example 2.12 Since $\mathbb{Z}$ is an abelian group, then $n\mathbb{Z} \triangleq \mathbb{Z}$ for $n \geq 1$. Let $n = 5$, then $\mathbb{Z}/n\mathbb{Z} = \mathbb{Z}/5\mathbb{Z} = \{5\mathbb{Z}, 1 + 5\mathbb{Z}, 2 + 5\mathbb{Z}, 3 + 5\mathbb{Z}, 4 + 5\mathbb{Z}\}$.

Theorem 2.26 Let $H \triangleq G$, then $\phi : G \to G/H$ with $\phi(x) = xH$ is a group homomorphism with kernel H.

Proof Since $\forall a, b \in G$, we have

$$\phi(ab) = (ab)H = (aH)(bH) = \phi(a)\phi(b).$$

Hence ϕ is a group homomorphism. Since for all $x \in \ker(\phi)$

$$\phi(x) = H \quad \Rightarrow \quad xH = H \quad \Rightarrow \quad x \in H.$$

and for all $x \in H$

$$\phi(x) = xH = H \quad (\text{Since } x \in H) \quad \Rightarrow \quad x \in \ker(\phi).$$

Hence $\ker(\phi) = H$.

Theorem 2.27 (First Homomorphism Theorem) Let $\phi : G \to G'$ be a group homomorphism with kernel H, then $\phi(G) \triangleq G'$ is a group and $\mu : G/H \to \phi(G)$ with $\mu(gH) = \phi(g)$ is a group isomorphism. Moreover, if $\gamma : G \to G/H$ with $\gamma(g) = gH$ is a homomorphism, then for all $g \in G$, $\phi(g) = \mu(\gamma(g))$.

Proof

1. By theorem, $\phi(G) \leq G'$.

2. For all $g_1H, g_2H \in G/H$,

$$\mu((g_1H)(g_2H)) = \mu((g_1g_2)H) = \phi(g_1g_2) = \phi(g_1)\phi(g_2) = \mu(g_1H)\mu(g_2H).$$

   Thus μ is a homomorphism.

3. By theorem, μ is one-to-one if and only if $\ker(\mu) = H$ (since H is the identity in G/H).

   $\subseteq$: For all $gH \in \ker(\mu)$, $e' = \mu(gH) = \phi(g)$, where e' is the identity in G'. Thus $g \in \ker(\phi) = H$, therefore $gH = H$.

   $\supseteq$: Since

$$\mu(H) = \mu(eH) = \phi(e) = e'$$

   Hence $H \in \ker(\mu)$.

4. For all $g' \in \phi(G)$, $\exists g \in G$ such that $\phi(g) = g' \in \phi(G)$. Then $\mu(gH) = \phi(g) = g'$.

Hence $\mu : G/H \to \phi(G)$ is a isomorphism.

Theorem 2.28 Let G be a group and $g \in G$, then $i_g : G \to G$ with $i_g(x) = gxg^{-1}$ is a group isomorphism.

Proof

1. For all $x_1, x_2 \in G$,

$$i_g(x_1x_2) = gx_1x_2g^{-1} = (gx_1g^{-1})(gx_2g^{-1}) = i_g(x_1)i_g(x_2).$$

   Thus i_g is homomorphism.

2. Assume $i_g(x) = e$, then

$$gxg^{-1} = e \quad \Rightarrow \quad g^{-1}gxg^{-1}g = x = g^{-1}eg = e \quad \Rightarrow \quad \ker(\phi) = \{e\}$$

   Thus i_g is one-to-one.

3. For all $g \in G$,

$$x = gg^{-1}xgg^{-1} = i_g(gxg^{-1})$$

   and $gxg^{-1} \in G$. Thus i_g is onto.

Hence i_g is a group isomorphism.

Definition 2.22

Suppose G is a group,

1. A group isomorphism $\phi : G \to G$ is an **automorphism** of G, denote by $\mathrm{Aut}(G)$.

2. The mapping $i_g : G \to G$ with $i_g(x) = gxg^{-1}$ is called the **inner automorphism of G by g**.

2.7 Isomorphism

Theorem 2.29 (First Isomorphism Theorem) Let $\phi : G \to G'$ be a group homomorphism. Then $G/\ker(\phi) \simeq \phi(G)$. Moreover, if ϕ is onto, then $G/\ker(\phi) \simeq G'$.

Definition 2.23 Let G be a group and $H, N \leq G$. Define $HN = \{hn | h \in H, n \in N\}$. So $N \leq HN$ and $H \leq HN$, but $HN \not\leq G$.

Lemma 2.1

1. If $N \trianglelefteq G$ and $H \leq G$, then $NH = HN \leq G$.

2. If $N \trianglelefteq G$ and $H \trianglelefteq G$, then $NH \trianglelefteq G$.

Proof Since $N \trianglelefteq G$, thus $gN = Ng$ for all $g \in G$. And $\forall hn \in HN$, $\exists n' \in N$ such that $hn = n'h \in NH$, therefore $HN \subseteq NH$. Similarly, $NH \subseteq HN$. Hence $NH = HN$.

(G0) For all $h_1n_1, h_2n_2 \in HN$, we have

$$\begin{aligned} h_1n_1h_2n_2 &= h_1(n_1h_2)n_2 = h_1(h_2n_1)n_2 \quad (\text{Since } Nh_2 = h_2N) \\ &= (h_1h_2)(n_1n_2) \in HN. \end{aligned}$$

(G2) $e = ee \in HN$, since $e \in H$ and $e \in N$.

(G3) For all $hn \in HN$, We have $(hn)^{-1} = n^{-1}h^{-1} = h^{-1}n^{-1} \in HN$.

Hence $HN \leq G$. Moreover, assume $N \trianglelefteq G$ and $H \trianglelefteq G$, then $\forall h \in H$, $n \ni N$, $g \in G$, we have

$$ghng^{-1} = ghg^{-1}ghg^{-1} \in HN \quad (\text{Since } ghg^{-1} \in H \text{ and } ghg^{-1} \in N)$$

thus $gHNg^{-1} \subset HN$, then $NH \trianglelefteq G$.

Theorem 2.30 (Second Isomorphism Theorem) If $H \leq G$ and $N \trianglelefteq G$, then $HN/N \simeq H/H \cap N$.

Theorem 2.31 (Third Isomorphism Theorem) If $K \leq H \leq G$ with $H, K \trianglelefteq G$, then $G/H \simeq (G/K)/(H/K)$ as a group.

Proof Define $\phi : G/K \to G/H$ with $\phi(gK) = gH$, then

(Well defined) Let $g_1K, g_2K \in G/K$, assume $g_1K = g_2K$, then ${g_2}^{-1}g_1 \in K \leq H \Rightarrow g_1H = g_2H$. So

$$\phi(g_1K) = g_1H = g_2H = \phi(g_2).$$

Thus ϕ is well-defined.

(Homomorphism) For all $g_1K, g_2K \in G/K$, then

$$\phi((g_1K)(g_2K)) = \phi((g_1g_2)K) = (g_1g_2)H = (g_1H)(g_2H) = \phi(g_1K)\phi(g_2K).$$

Thus ϕ is homomorphism.

(One-to-one) Since ϕ is one-to-one if and only if $\ker(\phi) = H/K$.

($\subseteq$) For all $gK \in \ker(\phi)$,

$$H = \phi(gK) = gH \quad \Rightarrow \quad g \in H \quad \Rightarrow \quad gK \in H/K.$$

($\supseteq$) For all $hK \in H/K \leq G/K$,

$$\phi(hK) = hH = H \quad \Rightarrow \quad hK \in \ker(\phi).$$

Thus ϕ is one-to-one

(Onto) For all $gH \in G/H$ and $gK \in G/K$, since $\phi(gK) = gH$, thus ϕ is onto.

By First Isomorphism Theorem, $(G/K)/(H/K) \simeq G/H$.

Chapter 3

Rings and Fields

3.1 Rings and Fields

Definition 3.1 A **ring** $\langle R, +, \cdot \rangle$ is a set R with two operation addition $+$ and multiplication $\cdot$ defined on R such the following axioms satisfy

(R1) $\langle R, + \rangle$ is abelian.

(R2) Multiplication is associative. (For all $a, b \in R$, $(a \cdot b) \cdot c = a \cdot (b \cdot c)$.)

(R3) Distributive is fold. (For all $a, b, c \in R$, $a \cdot (b + c) = (a \cdot b) + (a \cdot c)$ and $(b + c) \cdot a = (b \cdot a) + (c \cdot a)$).

Example 3.1 $\langle \mathbb{Z}, +, \cdot \rangle$, $\langle \mathbb{Q}, +, \cdot \rangle$, $\langle \mathbb{R}, +, \cdot \rangle$, $\langle \mathbb{C}, +, \cdot \rangle$ are rings.

Definition 3.2 Let $\langle R, +, \cdot \rangle$ be a ring. If $a \in R$ and $n \in \mathbb{Z}_{>0}$, then

$$na = \underbrace{a + a + \cdots + a}_{n \text{ times}}$$

If $n \in \mathbb{Z}_{<0}$, then

$$na = \underbrace{(-a) + (-a) + \cdots + (-a)}_{n \text{ times}}$$

If $n = 0$, then $0a = a0 = 0_R \in R$ is the **additive identity** in $\mathbb{R}$.

Theorem 3.1 If R is a ring with additive identity 0_R, then for all $a, b \in R$,

1. $0a = a0 = 0_R$.

2. $a \cdot (-b) = (-b) \cdot a = -(a \cdot b)$.

3. $(-a) \cdot (-b) = ab$.

Proof

1. By (R1) and (R3),

$$\begin{aligned}
&a0 + a0 = a(0+0) = a0 = a0 + 0_R \\
\Rightarrow & -(a0) + a0 + a0 = (a0) + a0 \\
\Rightarrow & a0 = 0_R.
\end{aligned}$$

   Similarly, $0a = 0_R$.

2. By (R3),

$$\begin{aligned}
&a(-b) + ab = a(-b+b) = a \cdot 0 = 0_R \\
\Rightarrow & a(-b) = -ab.
\end{aligned}$$

   Similarly, $(-a)b = -ab$.

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

Definition 3.3 Let R and R' be tow rings, a map $\phi : R \to R'$ is a **ring homomorphism** if for all $a, b \in R$,

1. $\phi(a+b) = \phi(a) + \phi(b)$, and
2. $\phi(a \cdot b) = \phi(a) \cdot \phi(b)$.

And the kernel of ϕ is $\ker(\phi) = \{a \in R | \phi(a) = 0\}$.

Definition 3.4 Let R and R' be tow rings, a map $\phi : R \to R'$ is a **ring isomorphism** if ϕ is a ring homomorphism with one-to-one and onto.

Theorem 3.2 (Reduction Modulo n) Let $\phi : \mathbb{Z} \to \mathbb{Z}_n$ be the deduction map Modulo n such that $\phi(m) = r$, where $m = nq + r$ with $q, r \in \mathbb{Z}$ and $0 \leq r < n$. Then ϕ is a ring homomorphism and $\ker(\phi) = n\mathbb{Z}$. Moreover, $\langle \mathbb{Z}/n\mathbb{Z}, +, \cdot \rangle \simeq \langle \mathbb{Z}_n, +, \cdot \rangle$ as a ring.

Proof Let $m_1 = q_1 n + r_1$ and $m_2 = q_2 n + r_2$ with $r_1, r_2, q_1, q_2 \in \mathbb{Z}$ and $0 \leq r_1, r_2 < n$.

1. Claim $\phi(m_1 + m_2) = \phi(m_1) + \phi(m_2)$. Write $r_1 + r_2 = q_3 n + r_3$ with $q_3, r_3 \in \mathbb{Z}$ and $0 \leq r_3 < n$, then

$$\phi(m_1 + m_2) = r_3 \underset{\text{in } \mathbb{Z}_n}{=} r_1 + r_2 = \phi(m_1) + \phi(m_2).$$

2. Claim $\phi(m_1m_2) = \phi(m_1)\phi(m_2)$. Note that

$$m_1m_2 = (q_1n + r_1)(q_2n + r_2) = n(q_1q_2n + q_1r_2 + q_2r_1) + r_1r_2.$$

Write $r_1r_2 = q_3n + r_3$ with $q_3, r_3 \in \mathbb{Z}$ and $0 \le r_3 < n$, then

$$\phi(m_1m_2) = r_3 \underset{\text{in } \mathbb{Z}_n}{=} r_1r_2 = \phi(m_1)\phi(m_2).$$

3. Claim $\ker(\phi) = n\mathbb{Z}$.

$\subseteq$: For all $s \in \ker(\phi)$, $\phi(s) = 0$ if and only if $n \big| s$. Hence $s \in n\mathbb{Z}$.

$\supseteq$: For all $s \in n\mathbb{Z}$, $\phi(s) = 0$. Hence $t \in \ker(\phi)$.

Hence ϕ is a ring homomorphism with $\ker(\phi) = n\mathbb{Z}$.

Example 3.2 Show that $\langle \mathbb{Z}, + \rangle$ and $\langle 2\mathbb{Z}, + \rangle$ with $\phi : \mathbb{Z} \to 2\mathbb{Z}$ such that $\phi(x) = 2x$ are group isomorphism, but not ring homomorphism.

Solution Since $\phi(xy) = 2xy \neq 4xy = (2x)(2y) = \phi(x)\phi(y)$. Hence ϕ not a ring homomorphism. Note that $2\mathbb{Z}$ does not have an identity element for multiplication.

Remark 3.1 Let $m, n \in \mathbb{N}$. If $\gcd(m, n) = 1$, then $\mathbb{Z}_{mn} \simeq \mathbb{Z}_m \times \mathbb{Z}_n$ as a ring.

Definition 3.5

1. A ring R is **commutative ring** if for all $a, b \in R$, $ab = ba$.

2. A ring R with **unity** $1_R \neq 0_R$. An element $u \in R$ is a unit if $\exists u^{-1} \in R$ such that $uu^{-1} = u^{-1}u = 1$.

3. If every nonzero element of R is a unit, then R is a **division ring**.

4. A abelian division ring is called a **field**.

Example 3.3 $\langle \mathbb{Q}, +, \cdot \rangle$, $\langle \mathbb{R}, +, \cdot \rangle$ and $\langle \mathbb{C}, +, \cdot \rangle$ are field.

Example 3.4 Find all units of $\mathbb{Z}_{14}$.

Solution Since

$$1 \times 1 = 1$$

$$3 \times 5 = 15 \overset{\text{in } \mathbb{Z}_{14}}{=} 1$$

$$11 \times 9 = 99 \overset{\text{in } \mathbb{Z}_{14}}{=} 1$$

$$13 \times 13 = 169 \overset{\text{in } \mathbb{Z}_{14}}{=} 1.$$

Hence $1, 3, 5, 9, 11$ and 13 are all units of $\mathbb{Z}_{14}$.

Remark 3.2 The units of $\mathbb{Z}$ are ± 1.

Remark 3.3 Let $n \in \mathbb{N}$. Then t is a unit of $\mathbb{Z}_n$ if and only if $\gcd(t, n) = 1$.

3.2 Integral Domains

Definition 3.6 Let R be a ring. $a, b \in R$ are **zero divisors** if $a \cdot b = 0$ in R.

Example 3.5 Solve the equation $x^2 - 5x + 6 = 0$ in $\mathbb{Z}_{12}$.

Solution Since $x^2 - 5x + 6 = (x-3)(x-2)$, then $2, 3$ are solution in $\mathbb{Z}_{12}$.

$$x = 0, (x-3)(x-2) = (-3)(-2) = 6$$
$$x = 1, (x-3)(x-2) = (-2)(-1) = 2$$
$$x = 4, (x-3)(x-2) = (1)(2) = 2$$
$$x = 5, (x-3)(x-2) = (2)(3) = 6$$
$$x = 6, (x-3)(x-2) = (3)(4) = 12 = 0$$
$$x = 7, (x-3)(x-2) = (4)(5) = 20 = 8$$
$$x = 8, (x-3)(x-2) = (5)(6) = 30 = 6$$
$$x = 9, (x-3)(x-2) = (6)(7) = 42 = 6$$
$$x = 10, (x-3)(x-2) = (7)(8) = 56 = 8$$
$$x = 11, (x-3)(x-2) = (8)(9) = 72 = 0$$

Hence $2, 3, 6$ and 11 are all solution in $\mathbb{Z}_{12}$, and $6, 11$ are zero divisors.

Theorem 3.3 In $\langle \mathbb{Z}_n, +, \cdot \rangle$, the number of zero divisors is the number of that nonzero element that are relatively prime to n.

Corollary 3.1 If p is a prime, then $\mathbb{Z}_p$ has no zero divisors.

Theorem 3.4 A ring R has no zero divisors if and only if the cancellation laws (消去律) hols in R.

Definition 3.7 A ring D is an **integral domain** if D with unity $1 \neq 0$, commutation, and containing no zero divisor.

Theorem 3.5 Every field F is an integral domain.

Proof Let $a, b \in F$. Assume $ab = 0$ and $a \neq 0$. Since $a \in F \backslash \{0\}$, so $\exists a^{-1} \in F$ such that $aa^{-1} = 1$. Thus

$$ab = 0 \quad \Rightarrow \quad a^{-1}ab = a^{-1}0 = 0 \quad \Rightarrow \quad b = 0.$$

Hence F has no zero divisor, that is F is an integral domain.

Theorem 3.6 Every finite integral domain D is a field.

Corollary 3.2 If p is a prime, then $\mathbb{Z}_p$ is a field.

Definition 3.8 If $\exists n \in \mathbb{N}$ such that $na = 0$ for all $a \in R$, then the least such positive integer is the **characteristic** of R. If $\nexists n \in \mathbb{N}$ satisfy the condition, then the **characteristic** of R is 0.

Example 3.6 $\mathbb{Z}_n$ is of characteristic n. $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ and $\mathbb{C}$ are characteristic 0.

Theorem 3.7 Let R be a ring with 1, if $\exists n \in \mathbb{N}$ such that $n \cdot 1 = 0$, then the smallest n is the characteristic of R.

Proof Suppose $\exists n \in \mathbb{N}$ such that $n \cdot 1 = 0$, then for all $a \in R$,

$$n \cdot a = \underbrace{a + a + a + \cdots + a}_{n \text{ times}} = a \cdot (\underbrace{1 + 1 + 1 + \cdots + 1}_{n \text{ times}}) = a(n \cdot 1) = a \cdot 0 = 0.$$

3.3 Fermat's and Euler's Theorem

Theorem 3.8 (Fermat's Little Theorem) If $a \in \mathbb{Z}$, p is a prime and $\gcd(a, p) = 1$, then $a^{p-1} \equiv 1 \pmod{p}$.

Proof Define ${\mathbb{Z}_p}^* = \{t | \gcd(t, p) = 1\} = \{1, 2, \cdots, p-1\}$. Since $\mathbb{Z}_p$ is a field, so $\langle {\mathbb{Z}_p}^*, \cdot \rangle$ is a group, and since $|{\mathbb{Z}_p}^*| = p - 1$, so $t^{p-1} = 1$ for all $t \in {\mathbb{Z}_p}^*$.

Corollary 3.3 If $a \in \mathbb{Z}$ and p is a prime, then $a^p \equiv a \pmod{p}$.

Proof If $p \nmid a$, by Fermat's Little Theorem, $a^{p-1} \equiv 1 \pmod{p}$, then $a^p \equiv a \pmod{p}$. If $p | a$, then $a \equiv 0 \pmod{p}$, so $a^p \equiv 0 \equiv a \pmod{p}$.

Theorem 3.9 The set G_n of nonzero element of $\mathbb{Z}_n$ and not zero divisor form a group under multiplication modulo n.

Definition 3.9 Let ${\mathbb{Z}_p}^*$ be the set of units in $\mathbb{Z}_n$, then ${\mathbb{Z}_p}^* = \{t | \gcd(t, p) = 1\}$.

Proof

($\subseteq$) For all $t \in {\mathbb{Z}_n}^*$, $\exists r \in {\mathbb{Z}_n}^*$ such that $tr = 1$ in $\mathbb{Z}_n$, then $n | tr - 1$, so $\exists m \in \mathbb{Z}$ such that $tr - 1 = nm \Rightarrow tr - mn = 1$, that is $\gcd(t, n) = 1$.

($\supseteq$) Let $t \in {\mathbb{Z}_n}^*$ with $\gcd(t, n) = 1$, then $\exists a, b \in \mathbb{Z}$ such that $at + bn = 1$. Therefore $at + bn \equiv at \equiv 1 \pmod{n}$.

Example 3.7 Find the remainder of 8^{103} when divided by 13.

Solution By Fermat's Little Theorem, $8^{12} \equiv 1 \pmod{13}$, thus

$$8^{103} \equiv (8^{12})^8 8^7 \equiv 8^7 \equiv (8^2)^3 8 \equiv (-1)^3 8 \equiv -8 \equiv 5 \pmod{13}.$$

Example 3.8 Find the inverse of 101 in $\mathbb{Z}_{911}$.

Solution By Euclidean algorithm,

$$\begin{array}{r|rr|l} 50 & 101 & 911 & 9 \\ & 100 & 909 & \\ \hline & 1 & 2 & \end{array}$$

We have

$$1 = 101 - 50 \times 2$$

$$2 = 911 - 101 \times 9$$

So

$$1 = 101 - 50 \times (911 - 101 \times 9) = 101 \times 451 + 911 \times (-50)$$

Hence $101 \times 451 \equiv 1 \pmod{911}$. So $101^{-1} = 451$ in $\mathbb{Z}_{911}$.

Definition 3.10 (Euler's Phi Function) Define $\phi : \mathbb{N} \to \mathbb{N}$ with $\phi(n) = |{\mathbb{Z}_p}^*|$ is the **Euler's Phi Function**.

Theorem 3.10 If $n = {p_1}^{r_1} {p_2}^{r_2} \cdots {p_k}^{r_k} \in \mathbb{N}$, where p_i are distinct primes, then

$$\phi(n) = n \left(1 - \frac{1}{p_1}\right) \left(1 - \frac{1}{p_2}\right) \cdots \left(1 - \frac{1}{p_k}\right).$$

Example 3.9 Calculate $\phi(8)$ and $\phi(24)$.

Solution

Method 1

(a) $\phi(8) = |\{1, 3, 5, 7\}| = 4$.

(b) $\phi(24) = |\{1, 5, 7, 11, 13, 17, 19, 23\}| = 8$.

Method 2

(a) $\phi(8) = \phi(2^3) = 8\left(1 - \frac{1}{2}\right) = 4$.

(b) $\phi(24) = \phi(2^3 \times 3) = 24\left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{3}\right) = 8$.

Theorem 3.11 (Euler's Theorem) Let $n \in \mathbb{N}$, $a \in \mathbb{Z}$. If $\gcd(a, n) = 1$, then $a^{\phi(n)} \equiv 1 \pmod{n}$.

Proof Let $a \in \mathbb{Z}$ with $\gcd(a, n) = 1$, then $a = nq + r$ for $q, r \in \mathbb{Z}$ and $0 < r < n$. Since $\gcd(a, n) = 1$ and $0 < r < n$, so $\gcd(r, n) = 1$. Therefore $r \in {\mathbb{Z}_n}^*$ and since $\langle {\mathbb{Z}_n}^*, \cdot\rangle$ is a group of order $\phi(n)$, so $r^{\phi(a)} \equiv 1 \pmod{n}$. Hence

$$a^{\phi(n)} \equiv (nq + r)^{\phi(n)} \equiv (0 + r)^{\phi(n)} \equiv r^{\phi(n)} \equiv 1 \pmod{n}.$$

Theorem 3.12 Let $n \in \mathbb{N}$ and $a, b \in \mathbb{Z}_n$. Then $ax \equiv b \pmod{n}$ has a solution if and only if $\gcd(a, n)|b$. Moreover, when $ax \equiv b \pmod{n}$ has a solution, then it have exactly $\gcd(a, n)$ solutions.

Proof

($\Rightarrow$) Suppose $\exists t \in \mathbb{Z}_n$ such that $at \equiv b \pmod{n}$. Then $\exists r \in \mathbb{Z}$ such that $at - b = nr \Rightarrow at - nr = b$. Hence $\gcd(a, n)|b$.

($\Leftarrow$) Suppose $d = \gcd(a, n)$ with $d|b$. Let $a = da'$, $n = dn'$ and $b = db'$. Then $n|ax - b \iff dm'|da'x - db' \iff m'|a'x - b$. So $ax \equiv b \pmod{n}$ has solution if and only if $a'x \equiv b \pmod{n}$.

Example 3.10

1. Find all solution of $12x \equiv 27 \pmod{18}$.

2. Find all solution of $15x \equiv 27 \pmod{18}$.

Solution

1. Since $\gcd(12, 18) = 6 \nmid 27$. Hence it has no solution.

2. Since $\gcd(15, 18) = 3|27$, so it has 3 solutions.

$$15x \equiv 27 \pmod{18} \quad \Rightarrow \quad 5x \equiv 9 \equiv 3 \pmod 6 \quad \Rightarrow \quad x = 5^{-1} \times 3 \text{ in } \mathbb{Z}_6,$$

and

$$\begin{array}{|cc|l} 5 & 6 & 1 \\ & 5 & \\ \hline & 1 & \end{array}$$

we have $1 = 6 + (-1) \times 5$. So $(-1) \times (5) \equiv 1 \pmod 6$. Thus 5^{-1} in $\mathbb{Z}_6$ is -1. Hence $x = 5^{-1} \times 3 = (-1) \times 3 = 3$ in $\mathbb{Z}_6$. So all solution are $3 + 18k$, $9 + 18k$ and $15 + 18k$ with $k \in \mathbb{Z}$.

Example 3.11 Show that $383838|n^{37} - n$ for all $n \in \mathbb{N}$. $(383838 = 2 \times 3 \times 7 \times 13 \times 19 \times 37.)$

Solution By Fermat's Little Theorem, if p is a prime, then $n^p \equiv n \pmod p$ for all $n \in \mathbb{Z}$. So

1. $n^2 \equiv n \pmod 2 \Rightarrow n^{37} \equiv (n^{2-1})^{36} n \equiv n \pmod 2 \Rightarrow 2|n^{37} - n$.
2. $n^3 \equiv n \pmod 3 \Rightarrow n^{37} \equiv (n^{3-1})^{18} n \equiv n \pmod 3 \Rightarrow 3|n^{37} - n$.
3. $n^7 \equiv n \pmod 7 \Rightarrow n^{37} \equiv (n^{7-1})^{6} n \equiv n \pmod 7 \Rightarrow 7|n^{37} - n$.
4. $n^{13} \equiv n \pmod{13} \Rightarrow n^{37} \equiv (n^{13-1})^{3} n \equiv n \pmod{13} \Rightarrow 13|n^{37} - n$.
5. $n^{19} \equiv n \pmod{19} \Rightarrow n^{37} \equiv (n^{19-1})^{2} n \equiv n \pmod{19} \Rightarrow 19|n^{37} - n$.
6. $n^{37} \equiv n \pmod{37} \Rightarrow n^{37} \equiv (n^{37-1})^{1} n \equiv n \pmod{37} \Rightarrow 37|n^{37} - n$.

By 1. to 6., since they are distinct primes, so $2 \times 3 \times 7 \times 13 \times 19 \times 37 = 383838|n^{37} - n$.

Theorem 3.13 (Chinese Reminder Theorem) Let $a_i \in \mathbb{Z}$ and $n_i \in \mathbb{N}$ for $i = 1, 2, \cdots, k$. If $\gcd(n_i, n_j)$ for all $i \neq j$, then the system

$$\begin{cases} x \equiv a_1 \pmod{n_1} \\ x \equiv a_2 \pmod{n_2} \\ \quad \vdots \\ x \equiv a_k \pmod{n_k} \end{cases},$$

has solution, and the solution is $x = \sum_{i=1}^{k} a_i x_i N_i$ module $N = \prod_{i=1}^{k} n_i$. Where $N = \sum_{i=1}^{k} n_i$ and $N_i = N/n_i$ for $i = 1, 2, \cdots, k$

Example 3.12 Solve

$$\begin{cases} x \equiv 2 \pmod 9 \\ x \equiv 4 \pmod{11} \\ x \equiv 6 \pmod{19} \end{cases}.$$

Solution Let $N = 9 \cdot 11 \cdot 19 = 1881$, $N_1 = N/9 = 209$, $N_2 = N/11 = 171$, and $N_3 = N/19 = 99$. We solve the solution

$$\begin{cases} 209x_1 \equiv 1 \pmod{9} \\ 171x_2 \equiv 1 \pmod{11} \\ 99x_2 \equiv 1 \pmod{19} \end{cases}.$$

Find $x_1 = -4$, $x_2 = 2$, $x_3 = 5$. So the solution is

$$x = (2)(-4)(209) + (4)(2)(171) + (6)(5)(99) = 2666,$$

module $N = 18881$, Hence $x = 785 + 1881k$ with $k \in \mathbb{Z}$.

3.4 The field of Quotients of an Integral Domain

Definition 3.11 Let D is an integral domain and $S = \{(a, b) | a, b \in D \text{ and } b \neq 0\}$. Then (a, b) and (c, d) are **equivalent** if and only if $ad = bd$, denote by $(a, b) \sim (c, d)$.

Remark 3.4 The relation $\sim$ is an equivalence relation on S.

Proof

Reflexive. $(a, b) \sim (b, a)$ since $ab = ba$.

Symmetric. If $(a, b) \sim (c, d)$, then $ad = bc = cb$, so $(cd) \sim (a, b)$.

Transitive. If $(a, b) \sim (c, d)$ and $(c, d) \sim (e, f)$, then $ad = bc$ and $cf = ed$, so $ade = bdf = dbe \Rightarrow d(af - be) = 0 \Rightarrow af - be = 0$ (since $d \neq 0$), so $af = be \Rightarrow (a, e) \sim (b, f)$.

Lemma 3.1 For every $[(a, b)], [(c, d)] \in F$, define

$$[(a, b)] + [(c, d)] = [(ad + bc, bd)], \quad \text{and} \quad [(a, b)] \cdot [(c, d)] = [(ac, bd)].$$

which gives well-defined operation of addition and multiplication in F.

Theorem 3.14 If $\langle F, +, \cdot \rangle$ is field, then

1. $[(0, 1)]$ the identity in $\langle F, + \rangle$.
2. The addition inverse of $[(a, b)]$ is $[(-a, b)]$.
3. $[(1, 1)]$ the identity in $\langle F, \cdot \rangle$.
4. If $a \neq 0$, then the multiplication inverse of $[(a, b)]$ is $[(b, a)]$.

Lemma 3.2 The map $i : D \to F$ with $i(a) = [(a, 1)]$ is an isomorphism of D with subring F.

Proof

Ring homomorphism. For all $a, b \in D$,

$$i(a + b) = [(a + b, 1)] = [(a, 1)] + [(b, 1)] = i(a) + i(b),$$

and

$$i(ab) = [(ab, 1)] = [(a, 1)][(b, 1)] = i(a)i(b).$$

Thus i is an ring homomorphism.

One-to-one. If $a, b \in D$ such that $i(a) = i(b)$, then

$$i(a) = i(b) \quad \Rightarrow \quad [(a, 1)] = [(b, 1)] \quad \Rightarrow \quad (a, 1) \sim (b, 1) \quad \Rightarrow \quad a \cdot 1 = b \cdot 1 \quad \Rightarrow \quad a = b.$$

Thus i is one-to-one.

Hence $D \simeq i(D) \leq F$.

Theorem 3.15 Let F be a field of quotient of D and let L be any field containing D. Then $\exists \psi : F \to L$ is an isomorphism of F and is a subring of L with $\psi(a) = a$ for $a \in D$.

Corollary 3.4 Every field L containing an integral domain D containing a field of quotient of D.

Corollary 3.5 Any two field of quotient of one integral domain are isomorphism.

3.5 Rings of Polynomial

Definition 3.12

1. Let R be a ring. We called a polynomial $f(x)$ with coefficients in R is a **formal sum**

   $$f(x) = \sum_{i=0}^{n} a_i x^i = a_0 + a_1 x^1 + a_2 x^2 + \cdots + a_n x^n,$$

   where $a_i \in R$ for $i = 1, 2, \cdots, n$.

2. **Degree of** $f(x)$ is the largest number $m \in \mathbb{N}$ such that $a_m \neq 0$, and a_m is called the **leader coefficient**.

3. $f(x)$ is **monic** if it's leader coefficient 1.

4. $R[x] = \{a_n x^n + \cdots + a_2 x^2 + a_1 x^1 + a_0 | n \in \mathbb{N}, a_i \in R \text{ for } i = 1, 2, \cdots, n\}$.

Definition 3.13 Let $f(x), g(x) \in \langle R[x], +, \cdot \rangle$ with

$$f(x) = \sum_{i=0}^{n} a_i x^i, \quad \text{and} \quad g(x) = \sum_{i=0}^{m} b_i x^i.$$

Then

$$f(x) + g(x) = \left(\sum_{i=0}^{n} a_i x^i\right) + \left(\sum_{i=0}^{n} b_i x^i\right) = \sum_{i=0}^{\max(n,m)} (a_i + b_i)\, x^i, \quad \text{and}$$

$$f(x) \cdot g(x) = \left(\sum_{i=0}^{n} a_i x^i\right)\left(\sum_{i=0}^{m} b_i x^i\right) = \sum_{k=0}^{mn}\left(\sum_{i=0}^{k} a_i b_{k-i}\right) x^k.$$

Example 3.13 Let $R = \mathbb{Z}_5$, $f(x) = 3x^3 + 2x^2 + x + 1$ and $g(x) = 3x^2 + 4x + 3$, then $f, g \in \mathbb{Z}_5[x]$ and

$$f(x) + g(x) = 3x^3 + 5x^2 + 5x + 4 = 3x^3 + 4,$$

$$f(x) \cdot g(x) = 9x^5 + 18x^4 + 20x^3 + 13x^2 + 7x + 3 = 4x^5 + 3x^4 + 3x^2 + 2x + 3.$$

Theorem 3.16

1. If R is a ring, then $\langle R[x], +, \cdot \rangle$ is also a ring.
2. If R is commutative, then $R[x]$ is also commutative.
3. If R has a unity $1 \neq 0$, then 1 is also unity of $R[x]$.
4. If R is an integral domain, then $R[x]$ is also an integral domain.
5. If R is a filed, then $R[x]$ is a integral domain, but **not** a filed, since $R[x]$ has no unity.

Proof Let $f(x), g(x) \in R[x] \backslash \{0\}$, $f(x) = a_n x^n + \cdots a_1 x + a_0$ and $g(x) = b_m x^m + \cdots b_1 x^1 + b_0$, with $a_n \neq 0$ and $b_m \neq 0$. Since R is an integral domain. Thus $a_n b_m \neq 0$ and

$$f(x)g(x) = a_n b_m + \sum_{k=0}^{nm-1}\left(\sum_{i=0}^{k} a_i b_{k-i}\right) x^k \neq 0.$$

Hence $R[x]$ is also an integral domain.

Definition 3.14 Let R be a ring, then $R[x_1, x_2, \cdots, x_n]$ is a **ring of polynomial in n variables.**

Example 3.14 Let $R = \mathbb{Z}$, then $f(x, y, z) = x + 2y^2 + 3z^3 \in \mathbb{Z}[x, y, z]$.

Theorem 3.17 (The Evaluation Homomorphism for Field Theorem) Let F be a subfield of field of E and $\alpha \in E$. Let $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0 \in F[x]$, and $f(\alpha) = a_n \alpha^n + a_{n-1}\alpha^{n-1} + \cdots + a_0 \in F$. If $f(\alpha) = 0$, then α is z zero (root) of $f(x)$.

Example 3.15 Prove that $x^2 - 2$ has no zero in $\mathbb{Q}$.

Solution Assume $x^2 - 2 = 0$ with $x \in \mathbb{Q}$, so let $x = m/n$ with $\gcd(n, m) = 1$. Thus

$$0 = x^2 - 2 = \frac{m^2}{n^2} - 2 \quad \Rightarrow \quad m^2 = 2n^2 \quad \Rightarrow \quad 2|m^2 \quad \Rightarrow \quad 2|m \quad \Rightarrow \quad 4|m^2 \quad \Rightarrow \quad 4|2n^2$$
$$\Rightarrow \quad 2|n^2 \quad \Rightarrow \quad 2|n$$

it contract $\gcd(m, n) = 1$. Hence $\nexists x \in \mathbb{Q}$ such that $x^2 - 2 = 0$.

3.6 Factorization of Polynomial over a Field

Theorem 3.18 (Division Algorithm for $F[x]$) Let F is a field, $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$, $g(x) = b_m x^m + b_{m-1}x^{m-1} + \cdots + b_1 x + b_0 \in F[x]$ with $a_n, b_m \neq 0$. Then $\exists! q(x), r(x) \in F[x]$ such that $f(x) = q(x)g(x) + r(x)$ with $\deg(r(x)) = \deg(g(x))$.

Corollary 3.6 Let F is a field, $a \in F$ and $f(x) \in F[x]$. Then $f(a) = 0$ if and only if $\exists g(x) \in F[x]$ such that $f(x) = (x - a)g(x)$.

Corollary 3.7 Let $f(x) \in F[x]$ with $f(x) \neq 0$. If $\deg(f) = n$, then f has at most n roots in F.

Corollary 3.8 If G is a finite subgroup of a multiplication group $\langle F^*, \cdot \rangle$ of F, then G is cyclic.

Example 3.16 Let $G = {\mathbb{Z}_7}^* = \{1, 2, 3, 4, 5, 6\}$. Since $\langle 3 \rangle$ in $\mathbb{Z}_7$ under multiplication is $\langle 3 \rangle = \{3, 2, 6, 4, 5, 1\}$. So ${\mathbb{Z}_7}^* = \langle 3 \rangle$. Hence ${\mathbb{Z}_7}^*$ is cyclic.

Definition 3.15 Let $f(x) \in F[x] \backslash F$, then we called $f(x)$ is **reducible** over F if $\exists g(x), h(x) \in F[x]$ such that $f(x) = g(x)h(x)$. If not, then we called f is **irreducible** over F.

Example 3.17 Let $f(x) = x^2 - 2 = (x - \sqrt{2})(x + \sqrt{2})$. So f is reducible over $\mathbb{R}$. But $f(x)$ is irreducible over $\mathbb{Q}$, since $(x - \sqrt{2}) \notin \mathbb{Q}$.

Theorem 3.19 Let $f(x) \in F[x]$ with degree is 2 or 3. Then f is reducible over F if and only if f has root in F.

Theorem 3.20 Let $f(x) \in \mathbb{Z}[x]$. Then $\exists g(x), h(x) \in \mathbb{Z}[x]$ with $\deg(g) = r$ and $\deg(h) = s$ such that $f(x) = g(x)h(x)$ if and only if $\exists \overline{g}(x), \overline{h}(x) \in \mathbb{Q}[x]$ with $\deg(\overline{g}) = r$ and $\deg(\overline{h}) = s$ such that $f(x) = \overline{g}(x)\overline{h}(x)$.

Corollary 3.9 If $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \in \mathbb{Z}$ with $a_0 \neq 0$. If f has *no* root in $\mathbb{Q}$, then $f(x)$ has a root $m \in \mathbb{Z}$ and $m|a_0$.

Theorem 3.21 (Eisenstein Criterion) Let $p \in \mathbb{Z}$ be a prime and $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \in \mathbb{Z}[x]$. If $p \nmid a_n$, $p | a_i$ for $i = 0, 1, 2, \cdots, n-1$ and $p^2 \nmid a_0$, then $f(x)$ is irreducible over $\mathbb{Q}$.

Theorem 3.22 By Eisenstein Criterion, taking $p = 3$, then

$$25x^5 - 9x^4 - 3x^2 - 12$$

is irreducible over $\mathbb{Q}$.

Definition 3.16 Let $f(x), g(x) \in F[x]$. We say $g(x)$ **divides** $f(x)$ **in** $F[x]$ if $\exists q(x) \in F[x]$ such that $f(x) = g(x)q(x)$, denote by $g(x)|f(x)$.

Theorem 3.23 Let $p(x)$ is an irreducible polynomial over $F[x]$ and $f(x), g(x) \in F[x]$. If $p(x)|f(x)g(x)$, then $p(x)|f(x)$ or $p(x)|g(x)$.

Theorem 3.24 Let $f(x) \in F[x] \backslash F$, then f can be uniquely factored into product of irreducible polynomials in $F[x]$.

3.7 Homomorphism and Factor Rings

Theorem 3.25 A map $\phi : R \to R'$ is a ring homomorphism. Then

1. If S is a subring of R, then $\phi(S)$ is also a subring of R'.
2. If S' is a subring of R', then $\phi^{-1}(S')$ is also a subring of R.
3. If R has a unity 1, then $\phi(1)$ is a unity for $\phi(R)$.

Definition 3.17 Let $\phi : R \to R'$ be a ring homomorphism, we called the subring $\phi^{-1}(0') = \{r \in R | \phi(r) = 0'\}$ is the **kernel** of ϕ.

Theorem 3.26 Let $\phi : R \to R'$ be a ring homomorphism, for all $a \in R$, $\phi^{-1}(\phi(a)) = a + \ker(\phi)$.

Corollary 3.10 Let $\phi : R \to R'$ be a ring homomorphism. Then ϕ is one-to-one if and only if $\ker(\phi) = \{0\}$.

Theorem 3.27 Let $\phi : R \to R'$ be a ring homomorphism with $\ker(\phi) = H$. Then the additive of cosets of H form a group with

1. $(a + H) + (b + H) = (a + b) + H$.
2. $(a + H)(b + H) = (ab) + H$.

Theorem 3.28 Let H be a subring of a ring R. Then for all $a, b \in R$, $(a+H)(b+H) = ab + H$ is well-defined if and only if $ah \in H$ and $bh \in H$ for all $a, b \in R$ and $h \in H$.

Definition 3.18 Let I be a subring of a ring R. We called I is an **ideal of** R if $aI \subseteq I$ and $Ia \subseteq I$ for all $a \in R$.

Remark 3.5

1. A subring I is an ideal of a ring R if and only if $ax \in I$ and $xa \in I$ for all $x \in I$ and $a \in R$.
2. The kernel of a ring homomorphism $\phi : R \to R'$ is an ideal.

Definition 3.19 Let I be an ideal of a ring R, then the ring R/I is a factor ring of R by I.

Theorem 3.29 Let I be an ideal of a ring R. Then $\phi : R \to R/I$ is a ring homomorphism with $\ker(\phi) = I$.

3.8 Prime Ideal and Maximal Ideal

Definition 3.20 Let R be a ring, then R has a least 2 ideals: **improper ideal** R and trivial ideal $\{0\}$. If I is a ideal of R, $I \neq R$ and $I \neq 0$, then we called I is an **proper nontrival ideal of** R.

Theorem 3.30 Let R be a ring with unity 1. If I is a ideal of R containing 1, then $N = R$.

Corollary 3.11 A field contains *no* proper nontrival ideal.

Definition 3.21 Let M is a proper ideal of R with $M \neq R$, then we called M is a **maximal ideal of** R if *not* exists ideal $I \subset R$ such that $M \subset I$.

Example 3.18

1. If p is a prime, then $p\mathbb{Z}$ is a maximal ideal of $\mathbb{Z}$ and $\mathbb{Z}/p\mathbb{Z}$ is a field.
2. If $n = 6$ not a prime, then $6\mathbb{Z}$ si not a maximal ideal of $\mathbb{Z}$, since $6\mathbb{Z} \subset 3\mathbb{Z}$.

Theorem 3.31 Let R be a commutative ring with unity. Then M is a maximal ideal of R if and only if R/M is a field.

Definition 3.22 Let R be a commutative ring. We called a ideal I of R is a **prime ideal** if $ab \in I$, then $a \in I$ or $b \in I$ for all $ab \in I$.

Example 3.19 Let $R = \mathbb{Z}$ and p is a prime. For all $ab \in \mathbb{Z}$, if $ab \in p\mathbb{Z}$, then $a \in p\mathbb{Z}$ or $b \in p\mathbb{Z}$. So $p\mathbb{Z}$ is a prime ideal.

Theorem 3.32 Let R be a commutative ring with unity 1 and I is an proper ideal of R. Then R/I is a field if and only if I is a prime ideal.

Proof