Contents

1 Groups

1.1 Notation

1. $\mathbb{N} = \{1, 2, ...\}$
2. $\mathbb{Z} = \{..., -1, 0, 1, ...\}$
3. $\mathbb{Q} = \left\{\frac{a}{b} : a \in \mathbb{Z}, b \in \mathbb{N}\right\}$
4. $\mathbb{R} = \text{real numbers}$
5. $\mathbb{C} = \{a + bi : a, b \in \mathbb{R}, i^2 = -1\}$

For $n \in \mathbb{N}$, $\mathbb{Z}_n = \text{integers modulo } n = \{[0], ..., [n-1]\}$ where $[r] = \{z \in \mathbb{Z} : Z \equiv r \bmod n\}$
We note that the set $S = \mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{Z}_n$ has 2 operations $+, \cdot$.
For $n \in \mathbb{N}$, an $n \times n$ matrix over $\mathbb{R}$ (or $\mathbb{Q}$ or $\mathbb{C}$) is an $n \times n$ array

$$A = [a_{ij}] = \begin{bmatrix} a_{11} & \dots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{n1} & \dots & a_{nn} \end{bmatrix}$$

with $a_{ij} \in \mathbb{R}$.
Note we can also do $+, \cdot$. For $A, B \in M_n(\mathbb{R})$

$$A + B := [a_{ij} + b_{ij}] \quad A \cdot B := \left[\sum_{k=1}^{n} a_{ik} b_{kj}\right]$$

1.2 Groups

Definition 1.2.1

Let G be a set and $* : G \times G \to G$. We say G is a *group* if the following are satisfied:

1. Associativity: if $a, b, c \in G$, then $a * (b * c) = (a * b) * c$
2. Identity: there is $e \in G$ such that $a * e = e * a = a$ for all $a \in G$
3. Inverses: for all $a \in G$, there is $a^{-1} \in G$ such that $a * a^{-1} = a^{-1} * a = e$

Definition 1.2.2

A group is called *abelian* if $a * b = b * a$ for all $a, b \in G$

Exercise 1.2.1

Prove in the definition of a group, 1-sided identity and inverses are enough to have 2-sided identity and inverses

Proposition 1.1 previous exercise

Suppose G is a set, $* : G \times G \to G$ is associative. Suppose there is $e \in G$ such that $e * a = a$ for all $a \in G$. Further suppose that for every $a \in G$, there is $a^{-1} \in G$ such that $a^{-1} * a = e$. Then for all $a \in G$,

1. $a * e = a$
2. $a * a^{-1} = e$

Proof of 1: Let $a \in G$, then

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

Multiplying on the left by ${a^{-1}}^{-1}$ gives

$$\begin{aligned} & {a^{-1}}^{-1} * a^{-1} * a * e = {a^{-1}}^{-1} * a^{-1} * a \\ \implies & e * a * e = e * a \\ \implies & a * e = a \end{aligned}$$

□

Proof of 2: Let $a \in G$, then

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

Again multiplying on the left by ${a^{-1}}^{-1}$ gives

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

□

Proposition 1.2

Let G be a group, let $a \in G$. Then

1. The group identity is unique
2. The inverse of a is unique

Proof of 1: Suppose e_1, e_2 are both identities. Then

$$e_1 = e_1 * e_2 = e_2$$

□

Proof of 2: Suppose b_1, b_2 are inverses of a. Then

$$b_1 = b_1 * e = b_1 * (a * b_2) = (b_1 * a) * b_2 = e * b_2 = b_2$$

□

Example 1.2.1

$(\mathbb{Z}, +), (\mathbb{Q}, +), (\mathbb{R}, +), (\mathbb{C}, +)$ are all abelian groups

Example 1.2.2

$(\mathbb{Z},\cdot),(\mathbb{Q},\cdot),(\mathbb{R},\cdot),(\mathbb{C},\cdot)$ are not groups as 0 has no inverse

Example 1.2.3

but $(\mathbb{Q}\setminus\{0\},\cdot),(\mathbb{R}\setminus\{0\},\cdot),(\mathbb{C}\setminus\{0\},\cdot)$ are abelian groups

Definition 1.2.3

For a set $(S,\cdot)$ let $S^* \subseteq S$ denote the set of all elements with inverses.

Exercise 1.2.2

what is $\mathbb{Z}_n^*$?

Example 1.2.4

$(M_n(\mathbb{R}),+)$ is an abelian group.

Example 1.2.5

Consider $\left(M_{n(\mathbb{R})},\cdot\right)$ The identity matrix is $\begin{bmatrix} 1 & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & 1 \end{bmatrix} \in M_n(\mathbb{R})$ However, since not all $M \in M_n(\mathbb{R})$ have multiplicative inverses, $(M_n(\mathbb{R}),\cdot)$ is not a group.

Notation

$\mathrm{GL}_n(\mathbb{R}) = \{M \in M_n(\mathbb{R}) : \det(M) \neq 0\}$

Note

If $A, B \in \mathrm{GL}_n(\mathbb{R})$, then $\det(AB) = \det(A)\det(B) \neq 0$ Thus $AB \in \mathrm{GL}_n(\mathbb{R})$. The associativity of $\mathrm{GL}_n(\mathbb{R})$ inherits from $M_n(\mathbb{R})$. Also the identity matrix satisfies $\det(I) = 1 \neq 0$ and thus $I \in \mathrm{GL}_n(\mathbb{R})$. Finally, for $M \in \mathrm{GL}_n(\mathbb{R})$, there exists $M^{-1} \in M_n(\mathbb{R})$ such that $MM^{-1} = I = M^{-1}M$ since $\det(M^{-1}) = \frac{1}{\det(M)} \neq 0$, we have $M^{-1} \in \mathrm{GL}_n(\mathbb{R})$. Thus $(\mathrm{GL}_n(\mathbb{R}),\cdot)$ is a group, called the *general linear group of degree n over $\mathbb{R}$*

Note

if $n \geq 2$, then $\mathrm{GL}_n(\mathbb{R})$ is not abelian.

Exercise 1.2.3

What is $(\mathrm{GL}_1(\mathbb{R}),\cdot)$?

Example 1.2.6

Let G, H be groups. The *direct product* is the set $G \times H$ with the component wise operation defined by

$$(g_1, h_1) * (g_2, h_2) = (g_1 *_G g_2, h_1 *_H h_2)$$

One can check that $G \times H$ is a group with identity (e_G, e_H) and the inverse of (g, h) is (g^{-1}, h^{-1})

Note

One can show by induction that if $G_1, \ldots, G_n$ are groups, then $G_1 \times \cdots \times G_n$ is also a group.

Notation

Given a group G and $g_1, g_2 \in G$, we often denote $g_1 * g_2$ by $g_1 g_2$ and its identity by 1. Also the unique inverse of an element $g \in G$ is denoted by g^{-1}. Also for $n \in \mathbb{N}$, we define $g^n = g * g * \cdots * g$ (n-times) and $g^{-n} = (g^{-1})^n$. Finally, we denote $g^0 = 1$.

Proposition 1.3

Let G be a group and $g, h \in G$ we have

1. ${g^{-1}}^{-1} = g$
2. $(gh)^{-1} = h^{-1} g^{-1}$
3. $g^n g^m = g^{n+m}$ for all $n, m \in \mathbb{Z}$
4. $(g^n)^m = g^{nm}$ for all $n, m \in \mathbb{Z}$

Proof of 1: Since

$$g^{-1} g = 1 = g g^{-1}$$

so ${g^{-1}}^{-1} = g$ □

Proof of 2:

$$(gh)(h^{-1} g^{-1}) = g(hh^{-1})g^{-1} = g1g^{-1} = 1$$

Similarly,

$$(h^{-1} g^{-1})(gh) = 1$$

Thus $(gh)^{-1} = h^{-1} g^{-1}$ □

Proof of 3: We proceed by considering cases:

1. if $n = 0$ then

$$g^n g^m = g^0 g^m = 1 g^m = g^m = g^{0+m} = g^{n+m}$$

2. if $n > 0$, we will proceed by induction on n. Case 1 establishes the base case. Let $m \in \mathbb{Z}$, $n \in \mathbb{Z}_{\geq 0}$. Suppose that $g^n g^m = g^{n+m}$ Then

$$g^{n+1}g^m = gg^n g^m = gg^{n+m} = g^{n+m+1}$$

3. if $n < 0$, then $n = -k$ for some $k \in \mathbb{N}$. We have

$$g^k g^n g^m = g^{k+n} g^m = g^0 g^m = g^m$$

also

$$g^k g^{n+m} = g^{k+m+n} = g^m$$

Thus

$$g^k g^n g^m = g^k g^{n+m}$$

So

$$g^n g^m = g^{n+m}$$

as desired.

□

Proof of 4: We proceed by considering cases:

1. if $m = 0$, then $(g^n)^m = (g^n)^0 = 1 = g^0 = g^{n0} = g^{nm}$
2. if $m > 0$, then

$$(g^n)^m = \underbrace{g^n g^n \cdots g^n}_{m \text{ times}} = g^{nm}$$

3. if $m < 0$, then $m = -k$ for some $k \in \mathbb{N}$. We will induct on k. For $k = 1$ we see that $(g^n)^{-1} = g^{-n}$ since

$$g^n g^{-n} = g^{n-n} = g^0 = 1$$

Suppose $(g^n)^{-\ell} = g^{-n\ell}$ for all $1 \leq \ell \leq k$ Then

$$(g^n)^{-k-1} = (g^n)^{-k}(g^n)^{-1} = g^{-nk}g^{-n} = g^{-nk-n} = g^{-n(k+1)}$$

□

Exercise 1.2.4

prove 3,4

Warning

In general, it is not the case that if $g, h \in G$ then $(gh)^n = g^n h^n$, this is not true unless G is abelian

Proposition 1.4

Let G be a group and $g, h, f \in G$ Then
1. They satisfy the left and right cancellation. More precisely,
   a. if $gh = gf$ then $h = f$
   b. if $hg = fg$ then $h = f$
2. Given $a, b \in G$ the equations $ax = b$ and $ya = b$ have unique solutions for $x, y \in G$

Proof of 1-a: By left-multiplying by g^{-1}, we have

$$gh = gf \Longleftrightarrow g^{-1}gh = g^{-1}gf \Longleftrightarrow h = f$$

□

Proof of 1-b: similar to 1-a □

Proof of 2: Let $x = a^{-1}b$ then

$$ax = aa^{-1}b = b$$

If u is another solution, then $au = b = ax$. By 1-a, $u = x$. Similarly, $y = ba^{-1}$ is the unique solution of $ya = b$ □

1.3 Symmetric Groups

Definition 1.3.1

Given a non-empty set L, *a permutation* of L is a bijection from L to L. The set of all permutations of L is denoted by S_L

Example 1.3.1

Consider the set $L = \{1, 2, 3\}$ which has the following different permutations

$$\binom{123}{123}, \binom{123}{132}, \binom{123}{213}, \binom{123}{231}, \binom{123}{312}, \binom{123}{321}$$

Where $\binom{123}{123}$ denotes the bijection

$$\sigma : \{1, 2, 3\} \longrightarrow \{1, 2, 3\}$$

$$\sigma(1) = 1, \sigma(2) = 2, \sigma(3) = 3$$

Notation

For $n \in \mathbb{N}$ we denote by $S_n = S_{\{1,2,\ldots,n\}}$ the set of all permutations of $\{1, 2, \ldots, n\}$. We have seen that the order of $S_3 = 3! = 6$. To consider the general S_n, we note that for a permutation $\sigma \in S_n$, there are n choices for $\sigma(1)$, $n - 1$ choices for $\sigma(2)$,…, 1 choice for $\sigma(n)$ Thus

Proposition 1.5

$|S_n| = n!$

Note

For Möbius quizzes, use "9 dots" for permutations.

Remark

Given $\sigma, \tau \in S_n$ we can compose them to get a new element $\sigma\tau$, where $\sigma\tau = \{1, 2, ..., n\} \to \{1, 2, ..., n\}$ given by $x \mapsto \sigma(\tau(x))$ Since both σ, τ are bijections, $\sigma\tau \in S_n$

Example 1.3.2

Compute $\sigma\tau$ and $\tau\sigma$ if

$$\sigma = \begin{pmatrix} 1234 \\ 3412 \end{pmatrix}, \quad \tau = \begin{pmatrix} 1234 \\ 2431 \end{pmatrix}$$

Then $\sigma\tau(1) = \sigma(2) = 4$,... Then $\sigma\tau = \left(\begin{smallmatrix} 1234 \\ 4213 \end{smallmatrix}\right)$, and $\tau\sigma = \left(\begin{smallmatrix} 1234 \\ 3124 \end{smallmatrix}\right)$
We note that $\sigma\tau \neq \tau\sigma$

Note

For any $\sigma, \tau \in S_n$ we have that $\tau\sigma, \sigma\tau \in S_n$ but $\sigma\tau \neq \tau\sigma$ in general on the other hand, for any σ, τ, μ we have $\sigma(\tau\mu) = (\sigma\tau)\mu$. Also note the *identity permutation* $\varepsilon \in S_n$ is defined as

$$\varepsilon = \begin{pmatrix} 12 \cdots n \\ 12 \cdots n \end{pmatrix}$$

Thus for any $\sigma \in S_n$, we have $\sigma\varepsilon = \varepsilon\sigma = \sigma$
Finally, for $\sigma \in S_n$, since it is a bijection, there is a unique bijection $\sigma^{-1} \in S_n$ called the *inverse permutation* of σ such that for all $x, y \in \{1, 2, ..., n\}$

$$\sigma^{-1}(x) = y \Longleftrightarrow \sigma(y) = x$$

It follows that

$$\sigma(\sigma^{-1}(x)) = \sigma(y) = x$$

and

$$\sigma^{-1}(\sigma(y)) = y$$

i.e we have

$$\sigma\sigma^{-1} = \sigma^{-1}\sigma = \varepsilon$$

Example 1.3.3

$$\sigma = \begin{pmatrix} 12345 \\ 45123 \end{pmatrix}$$

Then

$$\sigma^{-1} = \begin{pmatrix} 12345 \\ 34512 \end{pmatrix}$$

From the above we have

Proposition 1.6

$(S_n, \circ)$ is a group, called the *symmetric group of degree* n

Exercise 1.3.1

Write down all rotations and reflections that fix an equilateral triangle. Then check why it is the "same" as S_3

Example 1.3.4

Consider

$$\sigma = \begin{pmatrix} 123456789(10) \\ 317694258(10) \end{pmatrix} \in S_{10}$$

We note that $1 \to 3 \to 7 \to 2 \to 1$ and $4 \to 6 \to 4$ and $5 \to 9 \to 8$ and $10 \to 10$ Thus σ can be *decomposed* into one 4-cycle (1372), one 2-cycle (46), and one 3-cycle (598) and one 1-cycle (10) (we usually do not write 1-cycles) Note that these cycles are *pairwise disjoint* and we have

$$\sigma = (1372)(46)(598)$$

We can also write $\sigma = (46)(598)(1372)$, or $\sigma = (64)(985)(7213)$

Theorem 1.7 **Cycle Decomposition**

If Given $\sigma \in S_n$ with $\sigma \neq \varepsilon$, then σ is a product of (one or more) disjoint cycles of length at least 2. This factorization is unique up to the order of the factors.

Proof: See bonus 1. □

Convention

Every permutation of S_n can be regarded as a permutation in S_{n+1} by fixing the number $n + 1$, thus

$$S_1 \subseteq S_2 \subseteq \cdots \subseteq S_n \subseteq S_{n+1}$$

1.4 Cayley Tables

Definition 1.4.1

For a finite group G, defining its operation by means of a table is sometimes convenient. Given $x, y \in G$, the product xy is the entry of the table in the row corresponding to x and the column corresponding to y, such a table is a *Cayley table*.

Remark

By cancellation, the entries in each row or column of a Cayley table are all distinct

Example 1.4.1

Consider $(\mathbb{Z}_2, +)$ its Cayley table is

$\mathbb{Z}_2$	$[0]$	$[1]$
$[0]$	$[0]$	$[1]$
$[1]$	$[1]$	$[0]$

Example 1.4.2

Consider the group $\mathbb{Z}^* = \{1, -1\}$. Its Cayley table is

$\mathbb{Z}^*$	1	-1
1	1	-1
-1	-1	1

Note

If we replace 1 by $[0]$ and -1 by $[1]$ the Cayley tables of $\mathbb{Z}^*$ and $\mathbb{Z}_2$ become the same. In this case, we say $\mathbb{Z}^*$ and $\mathbb{Z}_2$ are *isomorphic* denoted by

$$\mathbb{Z}^* \cong \mathbb{Z}_2$$

Example 1.4.3

For $n \in \mathbb{N}$, the *cyclic group of order* n is defined by

$$C_n = \{1, a, a^2, ..., a^{n-1}\} \text{ with } a^n = 1 \text{ and } 1, a, ..., a^{n-1} \text{ are distinct}$$

The Cayley table of C_n is as follows

C_n	1	a	a^2	$\cdots$	a^{n-2}	a^{n-1}
1	1	a	a^2	$\cdots$	a^{n-2}	a^{n-1}
a	a	a^2	a^3	$\cdots$	a^{n-1}	1
a^2	a^2	a^3	a^4	$\cdots$	1	a
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\ddots$	$\vdots$	$\vdots$
a^{n-2}	a^{n-2}	a^{n-1}	1	$\cdots$	a^{n-4}	a^{n-3}
a^{n-1}	a^{n-1}	1	a	$\cdots$	a^{n-3}	a^{n-2}

Proposition 1.8

Let G be a group. Up to isomorphism, we have

1. If $|G| = 1$, then $G \cong \{1\}$
2. If $|G| = 2$, then $G \cong C_2$
3. If $|G| = 3$, then $G \cong C_3$
4. If $|G| = 4$, then $G \cong C_4$ or $G \cong K_4 \cong C_2 \times C_2$

Proof of 1: obviously □

Proof of 2: If $|G| = 2$ then $G = \{1, g\}$ with $g \neq 1$ Then $g^2 = g$ or $g^2 = 1$. We note that if $g^2 = g$, then $g = 1$ contradiction.thus $g^2 = 1$. Thus the Cayley table is as follows

G	1	g
1	1	g
g	g	1

which is the same as C_2 □

Proof of 3: If $|G| = 3$, then $G = \{1, g, h\}$ with $g \neq 1, h \neq 1, g \neq h$ By cancellation, we have $gh \neq g, gh \neq h$, thus $gh = 1$. Similarly, we have $hg = 1$. Also, on the row for g, we have $g1 = g$, $gh = 1$. Since all entries in this row are distinct, we have $g^2 = h$. Similarly, we have $h^2 = g$. Thus we obtain the following Cayley table

G	1	g	h
1	1	g	h
g	g	h	1
h	h	1	g

Which is the same as C_3. □

Proof of 4: See assignment 1 □

Exercise 1.4.1

Consider the symmetry group of a non-square rectangle. How is it related to K_4?

2 Subgroups

2.1 Subgroups

Definition 2.1.1

Let G be a group and $H \subseteq G$. IF H itself is a group, then we say H is a *subgroup* of G.

Note

We note that since G is a group, for $h_1, h_2, h_3 \in H \subseteq G$, we have

$$h_1(h_2h_3) = (h_1h_2)h_3$$

Thus

Proposition 2.1 **Subgroup Test**

Let G be a group, $H \subseteq G$. Then H is a subgroup of G if

1. If $h_1, h_2 \in H$, then $h_1h_2 \in H$
2. $1_H \in H$
3. If $h \in H$, then $h^{-1} \in H$

Exercise 2.1.1

Prove that $1_H = 1_G$

Example 2.1.1

Given a group G, then $\{1\}, G$ are subgroups of G

Example 2.1.2

We have a chain of groups

$$(\mathbb{Z}, +) \subseteq (\mathbb{Q}, +) \subseteq (\mathbb{R}, +) \subseteq (\mathbb{C}, +)$$

Example 2.1.3

Define

$$\mathrm{SL}_n(\mathbb{R}) = (\mathrm{SL}_n(\mathbb{R}), \cdot) := \{M \in M_n(\mathbb{R}), \det(M) = 1\} \subseteq \mathrm{GL}_n(\mathbb{R})$$

Note that the identity matrix $I \in \mathrm{SL}_n(\mathbb{R})$. Let $A, B \in \mathrm{SL}_n(\mathbb{R})$, then

$$\det(AB) = \det(A)\det(B) = 1 \cdot 1 = 1$$

and

$$\det(A^{-1}) = \frac{1}{\det(A)} = \frac{1}{1} = 1$$

i.e. $AB, A^{-1} \in \mathrm{SL}_n(\mathbb{R})$. By the subgroup test (Proposition 2.1), $\mathrm{SL}_n(\mathbb{R})$ is a subgroup of $\mathrm{GL}_n(\mathbb{R})$. We call $\mathrm{SL}_n(\mathbb{R})$ the *special linear group of order n over $\mathbb{R}$*

Definition 2.1.2

Given a group G, we define the *center of G* to be

$$Z(G) := \{z \in G \mid zg = gz \ \forall g \in G\}$$

Remark

$Z(G) = G$ iff G is abelian.

Proposition 2.2

$Z(G)$ is an abelian subgroup of G.

Proof: Note that $1 \in Z(G)$. Let $y, z \in Z(G)$ Then for all $g \in G$, we have

$$(yz)g = y(zg) = y(gz) = (yg)z = (gy)z = g(yz)$$

Thus $yz \in Z(G)$. Also, for $z \in Z(G)$, $g \in G$ we have

$$\begin{aligned} zg = gz &\iff z^{-1}(zg)z^{-1} = z^{-1}(gz)z^{-1} \\ &\iff gz^{-1} = z^{-1}g \end{aligned}$$

Thus $z^{-1} \in Z(G)$. By the subgroup test (Proposition 2.1), $Z(G)$ is a subgroup of G. Also, by the definition of $Z(G)$, we see that it is abelian. □

Proposition 2.3

Let H, K be subgroups of a group G. Then $H \cap G$ is also a subgroup.

Proof: Exercise □

Proposition 2.4 **Finite Subgroup Test**

If $H \neq \emptyset$ is a finite subset of a group G, then H is a subgroup of G iff H is closed under its operation.

Proof:
($\Longrightarrow$) obvious
($\Longleftarrow$) For $H \neq \emptyset$, let $h \in H$. Since H is closed under its operation, we have $h, h^2, h^3, \ldots \in H$. Since H is finite, these elements are not all distinct. Thus $h^n = h^{n+m}$ for some $n, m \in \mathbb{N}$. By cancellation, $h^m = 1$ and thus $1 \in H$. Also, $1 = h^{m-1}h$ implies that $h^{-1} = h^{m-1}$ and thus $h^{-1} \in H$. By the subgroup test, H is a subgroup of G. □

2.2 Alternating Groups

Definition 2.2.1

A *transposition* $\sigma \in S_n$ is a cycle of length 2. i.e. $\sigma = (ab)$ with $a, b \in \{1, 2, \ldots, n\}$ and $a \neq b$.

Example 2.2.1

Consider $(1245) \in S_5$. Also the composition $(12)(24)(45)$ can be computed as

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 3 & 5 & 4 \\ 1 & 4 & 3 & 5 & 2 \\ 2 & 4 & 3 & 5 & 1 \end{pmatrix}$$

Thus we have $(1245) = (12)(24)(45)$ Also we can show that

$$(1245) = (23)(12)(25)(13)(24)$$

We see from this example that the factorization into transpositions are NOT unique. However, one can prove (see Bonus 2)

Theorem 2.5 **Parity Theorem**

If a permutation σ has two factorizations

$$\sigma = \gamma_1 \gamma_2 \cdots \gamma_r = \mu_1 \mu_2 \cdots \mu_s$$

Where each γ_i and μ_j is a transposition, then $r \equiv s \pmod 2$

Definition 2.2.2

A permutation σ is *even* (or *odd*) if it can be written as a product of an even (or odd) number of transpositions. By the previous theorem, a permutation is either even or odd, but not both.

Theorem 2.6

For $n \geq 2$, let A_n denote the set of all even permutations in S_n

1. $\varepsilon \in A_n$
2. If $\sigma, \tau \in A_n$, then $\sigma\tau \in A_n$ and $\sigma^{-1} \in A_n$
3. $|A_n| = \frac{1}{2}n!$

From (1) and (2), we see (A_n) is a subgroup of S_n called the *alternating group of degree* n.

Proof of 1: We can write $\varepsilon = (12)(12)$. Thus ε is even. □

Proof of 2: if $\sigma, \tau \in A_n$ we can write $\sigma = \sigma_1 \cdots \sigma_r$ and $\tau = \tau_1 \cdots \tau_s$ where σ_i, τ_j are transpositions and r, s are even integers. Then

$$\sigma\tau = \sigma_1 \cdots \sigma_r \tau_1 \cdots \tau_s$$

is a product of $(r + s)$ transpositions and thus $\sigma\tau \in A_n$. Also, we note that σ_i is a transposition, we have $\sigma_i^2 = \varepsilon$ and thus $\sigma_i^{-1} = \sigma_i$. It follows that

$$\sigma^{-1} = (\sigma_1 \cdots \sigma_r)^{-1} = \sigma_r^{-1} \cdots \sigma_1^{-1} = \sigma_r \cdots \sigma_1$$

which is an even permutation. □

Proof of 3: Let O_n denote the set of odd permutations in S_n. Thus $S_n = A_n \cup O_n$ and the parity theorem implies that $A_n \cap O_n = \emptyset$. Since $|S_n| = n!$, to prove $|A_n| = \frac{1}{2}n!$, it suffices to show that $|A_n| = |O_n|$. Let $\gamma = (12)$ and let $f : A_n \to O_n$ be defined by $f(\sigma) = \gamma\sigma$. Since σ is even, we have $\gamma\sigma$ is odd. Thus the map is well-defined. Also, if we have $\gamma\sigma_1 = \gamma\sigma_2$, then by cancellation, we get $\sigma_1 = \sigma_2$, thus f is injective. Finally, if $\tau \in O_n$, then $\sigma = \gamma\tau \in A_n$ and $f(\sigma) = \gamma\sigma = \gamma(\gamma\tau) = \gamma^2\tau = \tau$. Thus f is surjective. It follows that f is a bijection, thus $|A_n| = |O_n|$. It follows that $|A_n| = \frac{1}{2}n! = |O_n|$ □

2.3 Orders of Elements

Notation

If G is a group and $g \in G$, we denote

$$\langle g \rangle = \{ g^k \mid k \in \mathbb{Z} \} = \{ \ldots, g^{-1}, g^0 = 1, g, g^2, \ldots \}$$

Note that $1 = g^0 \in \langle g \rangle$. Also, if $x = g^m, y = g^n \in \langle g \rangle$ With $m, n \in \mathbb{Z}$, then $xy = g^n g^m = g^{n+m} \in \langle g \rangle$ and $x^{-1} = g^{-m} \in \langle g \rangle$. By the subgroup test, we have

Proposition 2.7

If G is a group and $g \in G$, then $\langle g \rangle$ is a subgroup of G.

Definition 2.3.1

Let G be a group with $g \in G$. We call $\langle g \rangle$ the *cyclic subgroup of* G *generated by* g. If $G = \langle g \rangle$ for some $g \in G$, then we say G is *cyclic* and g a *generator* of G.

Example 2.3.1

Consider $(\mathbb{Z}, +)$ Note that for all $k \in \mathbb{Z}$, we can write $k = k \cdot 1$. Thus we can see $(\mathbb{Z}, +) = \langle 1 \rangle$. Similarly, $(\mathbb{Z}, +) = \langle -1 \rangle$. We observe, for any integer $n \in \mathbb{Z}$ with $n \neq \pm 1$ there exist no $k \in \mathbb{Z}$ such that $k \cdot n = 1$. Thus ± 1 are the only generators of $(\mathbb{Z}, +)$.

Remark

Let G be a group and $g \in G$. Suppose there is $k \in \mathbb{Z}$ $k \neq 0$ such that $g^k = 1$ then $g^{-k} = \left(g^k\right)^{-1} = 1$. Thus we can assume $k \geq 1$. Then by the well-ordering principle, there exists the smallest positive integer n such that $g^n = 1$

Definition 2.3.2

Let G be a group and $g \in G$. If n is the smallest positive integer such that $g^n = 1$, then we say the *order* of g is n, denoted $o(g) = n$. If no such n exists, we say g has *infinite order* and write $o(g) = \infty$

Proposition 2.8

Let G be a group and $g \in G$ with $o(g) = n \in \mathbb{N}$. For $k \in \mathbb{Z}$ we have

1. $g^k = 1$ iff $n \mid k$
2. $g^k = g^m$ iff $k \equiv m \pmod{n}$
3. $\langle g \rangle = \{1, g, g^2, ..., g^{n-1}\}$ where $1, g, ..., g^{n-1}$ are all distinct. In particular, we have $|\langle g \rangle| = o(g)$

Proof of 1:
$(\Longleftarrow)$ if $n \mid k$, then $k = nq$ for some $q \in \mathbb{Z}$. Thus

$$g^k = g^{nq} = (g^n)^q = 1^q = 1$$

$(\Longrightarrow)$ By the division algorithm, we can write $k = nq + r$ with $q, r \in \mathbb{Z}$ and $0 \leq r < n$. Since $g^k = 1$ and $g^n = 1$, we have

$$g^r = g^{k-nq} = g^k (g^n)^{-q} = 1 \cdot 1^{-q} = 1$$

Since $0 \leq r < n$ and $o(g) = n$, we have $r = 0$ and hence $n \mid k$. □

Proof of 2: Note that $g^k = g^m$ iff $g^{km} = 1$. By (1), we have $n \mid (km)$ i.e. $k \equiv m \pmod{n}$ □

Proof of 3: It follows from (2) that $1, g, ..., g^{n-1}$ are all distinct. Clearly, we have $\{1, g, ..., g^{n-1}\} \subseteq \langle g \rangle$. To prove the other inclusion, let $g^k \in \langle g \rangle$ for some $k \in \mathbb{Z}$. Write $k = nq + r$ with $n, r \in \mathbb{Z}$ and $0 \leq r < n$. Then

$$g^k = g^{nq+r} = g^{nq} g^r = (g^n)^q g^r = 1^q g^r = g^r \in \{1, g, ..., g^{n-1}\}$$

Thus $\langle g \rangle = \{1, g, ..., g^{n-1}\}$ □

Proposition 2.9

Let G be a group and $g \in G$ with $o(g) = \infty$. For $k \in \mathbb{Z}$ we have
1. $g^k = 1$ iff $k = 0$
2. $g^k = g^m$ iff $k = m$
3. $\langle g \rangle = \{..., g^{-1}, g^0 = 1, g, ...\}$ where g^i are all distinct

Proposition 2.10

Let G be a group and $g \in G$ with $o(g) = n \in \mathbb{N}$. If $d \in \mathbb{N}$, then $o(g^d) = \frac{n}{\gcd(n,d)}$. In particular, if $d \mid n$, then $\gcd(n, d) = d$ and $o(g^d) = \frac{n}{d}$

Proof: Let $n_1 = \frac{n}{\gcd(n,d)}$ and $d_1 = \frac{d}{\gcd(n,d)}$. By a result from Math 135, we have $\gcd(n_1, d_1) = 1$. Note that

$$\left(g^d\right)^{n_1} = \left(g^d\right)^{\frac{n}{\gcd(n,d)}} = \left(g^n\right)^{\frac{d}{\gcd(n,d)}} = 1$$

Thus it remains to show that n_1 is the smallest such positive integer. Suppose $\left(g^d\right)^r = 1$ with $r \in \mathbb{N}$. Since $o(g) = n$, by proposition, we have $n \mid dr$. Thus there is $q \in \mathbb{Z}$ such that $dr = nq$. Dividing both sides by $\gcd(n, d)$ we get

$$d_1 r = \frac{d}{\gcd(n,d)} r = \frac{n}{\gcd(n,d)} q = n_1 q$$

Since $n_1 \mid d_1 r$ and $\gcd(n_1, d_1) = 1$, by a result from Math 135, we get $n_1 \mid r$ i.e. $r = n_1 \ell$ for some $\ell \in \mathbb{Z}$. Since $r_1, n_1 \in \mathbb{N}$, it follows that $\ell \in \mathbb{N}$. Since $\ell \geq 1$, we get $r \geq n_1$ □

2.4 Cyclic Groups

Remark

For a group G, if $G = \langle g \rangle$ for some $g \in G$, then G is a cyclic group. For $a, b \in G$, we have $a = g^n, b = g^m$ for some $m, n \in \mathbb{Z}$. We have

$$ab = g^n g^m = g^{n+m} = g^{m+n} = g^m g^n = ba$$

Proposition 2.11

Every cyclic group is abelian

Warning

The converse of the above proposition is not true. For example the Klein 4 group is abelian, but not cyclic.

Proposition 2.12

Every subgroup of a cyclic group is cyclic.

Proof: Let $G = \langle g \rangle$ be cyclic and $H \subseteq G$ a subgroup. If $H = \{1\}$, then H is cyclic. Otherwise, there is $g^k \in H$ with $k \in \mathbb{Z} \setminus \{0\}$. Since H is a group, we have $g^{-k} \in H$. Thus we can assume that $k \in \mathbb{N}$. Let m be the smallest positive integer such that $g^m \in H$.
<u>*Claim:*</u> $H = \langle g^m \rangle$
Proof is exercise, by division algorithm. □

Proposition 2.13

Let $G = \langle g \rangle$ be a cyclic group with $o(g) = n$. Then $G = \langle g^k \rangle$ iff $\gcd(k, n) = 1$.

Proof: By proposition,

$$o(g^k) = \frac{n}{\gcd(n,k)} = n$$

□

Theorem 2.14 **Fundamental Theorem of Finite Cyclic Groups**

Let $G = \langle g \rangle$ be a cyclic group with $o(g) = n \in \mathbb{N}$.

1. If H is a subgroup of G, then $G = \langle g^d \rangle$ for some $d \mid n$. It follows that $|H| \mid |G|$.
2. Conversely, if $k \mid n$, then $\langle g^{\frac{n}{k}} \rangle$ is the unique subgroup of G with order k.

Proof of 1: By proposition, H is cyclic. Write $H = \langle g^n \rangle$ for some $m \in \mathbb{N} \cup \{0\}$. Let $d = \gcd(m, n)$.
<u>*Claim:*</u> $H = \langle g^d \rangle$
Since $d \mid m$ we have $m = dk$ for some $k \in \mathbb{Z}$. Then

$$g^m = g^{dk} = \left(g^d\right)^k \in \langle g^d \rangle$$

Thus $H = \langle g^m \rangle \subseteq \langle g^d \rangle$. To prove the other inclusion, since $d = \gcd(m, n)$, there is $x, y \in \mathbb{Z}$ such that $d = mx + ny$. Then

$$g^d = g^{mx+ny} = (g^m)^x (g^n)^y = (g^m)^x 1^y = (g^m)^x \in \langle g^m \rangle$$

Thus $\langle g^d \rangle \subseteq \langle g^m \rangle = H$. It follows that $H = \langle g^d \rangle$. Note that since $d = \gcd(m, n)$, we have $d \mid n$. By proposition, we have

$$|H| = o(g^d) = \frac{n}{\gcd(n,d)} = \frac{n}{d}$$

Thus $|H| \mid |G|$ □

Proof of 2: By proposition, the cyclic subgroup $\langle g^{\frac{n}{k}} \rangle$ is of order

$$\frac{n}{\gcd(n, \frac{n}{k})} = \frac{n}{n/k} = k$$

To show uniqueness, let K be a subgroup of G with order $k \mid n$. By 1, let $K = \langle g^d \rangle$ where $d \mid n$. Then by props, we have,

$$k = |K| = o(g^d) = \frac{n}{\gcd(n,d)} = \frac{n}{d}$$

It follows that $d = \frac{n}{k}$ and thus $K = \langle g^{\frac{n}{k}} \rangle$ $\square$

2.5 Non-cyclic Groups

Definition 2.5.1

Let X be a non-empty subset of a group G, and let

$$\langle X \rangle := \left\{ x_1^{k_1} \cdots x_m^{k_m} \;\middle|\; x_i \in X, k_i \in \mathbb{Z}, m \geq 1 \right\}$$

denote the set of all products of powers of (not necessarily distinct) elements of X. Note that this is clearly a group. $\langle X \rangle$ is called the *subgroup of G generated by X*.

Example 2.5.1

The Klein-4 group $K_4 = \{1, a, b, c\}$ with $a^2 = b^2 = c^2 = 1$ and $ab = c$. Thus

$$K_4 = \langle a, b \mid a^2 = 1 = b^2 \text{ and } ab = ba \rangle$$

Example 2.5.2

The symmetric group of order 3 $S_3 = \{\varepsilon, \sigma, \sigma^2, \tau, \tau\sigma, \tau\sigma^2\}$ where $\sigma^3 = \varepsilon = \tau^2$ and $\sigma\tau = \tau\sigma^2$ (one can take $\tau = (12)$ and $\sigma = (123)$) Thus

$$\langle \sigma, \tau \mid \sigma^3 = \varepsilon = \tau^2 \text{ and } \sigma\tau = \tau\sigma^2 \rangle$$

We can also replace σ, τ with $\sigma, \tau\sigma$ or $\sigma, \tau\sigma^2$, ..., etc

Definition 2.5.2

For $n \geq 2$ the *dihedral group of order $2n$* is defined by

$$D_{2n} = \{1, a, ..., a^{n-1}, b, ba, ..., ba^{n-1}\}$$

Where $a^n = 1 = b^2$ and $aba = b$. Thus

$$D_{2n} = \langle a, b \mid a^n = 1 = b^2 \text{ and } aba = b \rangle$$

Note

For $n = 2$ or 3 we have

$$D_4 \cong K_4 \quad \text{and} \quad D_6 \cong S_3$$

Exercise 2.5.1

For $n \geq 3$, consider a regular n-gon and its group of symmetries. How does it relate to D_{2n}?

3 Normal Subgroups

3.1 Homomorphisms and Isomorphisms

Definition 3.1.1

Let G, H be groups. A mapping $\alpha : G \to H$ is a *homomorphism* if

$$\alpha(a *_G b) = \alpha(a) *_H \alpha(b) \quad \forall a, b \in G$$

To simplify notation, we often write

$$\alpha(ab) = \alpha(a)\alpha(b) \quad \forall a, b \in G$$

Example 3.1.1

Consider the determinant map

$$\begin{aligned} \det : \mathrm{GL}_n(\mathbb{R}) &\longrightarrow \mathbb{R}^* \\ A &\longmapsto \det A \end{aligned}$$

Since $\det AB = \det A \det B$, the mapping det is a homomorphism.

Proposition 3.1

Let $\alpha : g \to H$ be a group homomorphism. Then

1. $\alpha(1_G) = 1_H$
2. $\alpha(g^{-1}) = \alpha(g)^{-1} \quad \forall g \in G$
3. $\alpha(g^k) = \alpha(g)^k \quad \forall k \in \mathbb{Z}$

Definition 3.1.2

Let $\alpha : G \to H$ be a mapping between groups. If α is a homomorphism and α is bijective, we say α is an *isomorphism*. In this case, we say G, H are *isomorphic* and write $G \cong H$.

Proposition 3.2

We have

1. The identity map $\mathrm{id} : G \to G$ is an isomorphism.
2. If $\sigma : G \to H$ is an isomorphism, then the inverse map $\sigma^{-1} : h \to G$ is also an isomorphism.
3. If $\sigma : G \to H$ and $\tau : H \to K$ is an isomorphism, the composite map $\tau\sigma : G \to K$ is also an isomorphism.

So $\cong$ is (sort-of) an equivalence relation

Proof: Exercise. □

Example 3.1.2

Let $\mathbb{R}^+ = \{r \in \mathbb{R} \mid r > 0\}$. Then $(\mathbb{R}, +) \cong (\mathbb{R}^+, \cdot)$ since we see that

$$\begin{aligned} \sigma : \mathbb{R} &\to \mathbb{R}^+ \\ x &\longmapsto e^x \end{aligned}$$

is a bijection. Moreover, $\sigma(x + y) = e^{x+y} = e^x \cdot e^y = \sigma(x)\sigma(y)$ thus σ is an isomorphism.

Example 3.1.3

Claim: $(\mathbb{Q}, +) \ncong (\mathbb{Q}^*, \cdot)$ Suppose $\tau : (\mathbb{Q}, +) \to (\mathbb{Q}^*, \cdot)$ is an isomorphism. Thus τ is surjective. So there is some $q \in \mathbb{Q}$ such that $\tau(q) = 2$. Then

$$\tau\left(\frac{q}{2}\right)^2 = \tau\left(\frac{q}{2}\right)\tau\left(\frac{q}{2}\right) = \tau\left(\frac{q}{2} + \frac{q}{2}\right) = \tau(q) = 2$$

Thus $\tau\left(\frac{q}{2}\right)$ is a rational number whose square is 2, a contradiction.

3.2 Cosets and Lagrange's Theorem

Definition 3.2.1

Let H be a subgroup of a group G. If $a \in G$, we define

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

to be the *right coset of H generated by a*. We define the left coset similarly.

Remark

Since $1 \in H$, we have $H1 = H = 1H$. Also $a \in Ha$ and $a \in aH$. Note that in general Ha and aH are not subgroups of G, and $aH \neq Ha$. However, if G is abelian, then $Ha = aH$.

Example 3.2.1

Let $K_4 = \{1, a, b, ab\}$. Let $H = \{1, a\}$ which is a subgroup of K_4. Note that since K_4 is abelian, we have $gH = Hg$ for all $g \in K_4$. Then the (right or left) cosets of H are

$$H1 = \{1, a\} = 1H$$

and

$$Hb = \{b, ab\} = Hab$$

Thus there are exactly two cosets of H in K_4

Example 3.2.2

Let $S_3 = \{\varepsilon, \sigma, \sigma^2, \tau, \tau\sigma, \tau\sigma^2\}$ with $\sigma^3 = \varepsilon = \tau^2$ and $\sigma\tau\sigma = \tau$. Let $H = \{\varepsilon, \tau\}$ which is a subgroup of S_3. Since $\sigma\tau = \tau\sigma^{-1} = \tau\sigma^2$, the right cosets of H are

$$\begin{aligned} H\varepsilon &= \{\varepsilon, \tau\} &&= H\tau \\ H\sigma &= \{\sigma, \tau\sigma\} &&= H\tau\sigma \\ H\sigma^2 &= \{\sigma^2, \tau\sigma^2\} &&= H\tau\sigma^2 \end{aligned}$$

And the left cosets of H are

$$\begin{aligned} \varepsilon H &= \{\varepsilon, \tau\} &&= \tau H \\ \sigma H &= \{\sigma, \tau\sigma^2\} &&= \tau\sigma^2 H \\ \sigma^2 H &= \{\sigma^2, \tau\sigma\} &&= \tau\sigma H \end{aligned}$$

Notice that $H\sigma \neq \sigma H$ and $H\sigma^2 \neq \sigma^2 H$

Proposition 3.3

Let H be a subgroup of a group G and let $a, b \in G$.

1. $Ha = Hb$ if and only if $ab^{-1} \in H$. In particular, we have $Ha = H$ if and only if $a \in H$.
2. If $a \in Hb$, then $Ha = Hb$
3. Either $Ha = Hb$ or $Ha \cap Hb = \emptyset$. Thus, the distinct right cosets of H forms a partition of G.

Proof of 1:
($\Longrightarrow$) If $Ha = Hb$, then $a = 1a \in Ha = Hb$. Thus $a = hb$ for some $h \in H$ and we have $ab^{-1} = h \in H$.
($\Longleftarrow$) Suppose $ab^{-1} \in H$ for all $h \in H$. Then for all $h \in H$,

$$ha = hab^{-1}b = h(ab^{-1})b \in Hb$$

Thus $Ha \subseteq Hb$. Note that if $ab^{-1} \in H$, since H is a subgroup, then

$$(ab^{-1})^{-1} = ba^{-1} \in H$$

Thus for all $h \in H$,

$$hb = h(ba^{-1})a \in Ha$$

Thus $Hb \subseteq Ha$. It follows that $Ha = Hb$. □

Proof of 2: If $a \in Hb$, then $ab^{-1} \in H$. Thus, by (1), we have $Ha = Hb$. □

Proof of 3: Two cases:

1. If $Ha \cap Hb = \emptyset$, then we are done.
2. If $Ha \cap Hb \neq \emptyset$, then there exists $x \in Ha \cap Hb$. Since $x \in Hb$, by (2), we have $Hb = Hx$. Thus

$$Ha = Hx = Hb$$

□

Remark

The analogues of the previous proposition also holds for left cosets

1. $aH = bH$ if and only if $b^{-1}a \in H$

Exercise 3.2.1

Let G be a group and H a subset of G. For $a, b \in G$, do we still have $Ha = Hb$, or $Ha \cap Hb = \emptyset$ if H is not a subgroup of G.

Definition 3.2.2

By the previous proposition, we see that G can be written as a disjoint union of right cosets of H. We define the *index* $[G : H]$ to be the number of disjoint right (or left) cosets of H in G. (Note that $[G : H]$ could be infinite).

Theorem 3.4 **Lagrange's Theorem**

Let H be a subgroup of a finite group G. We have $|H| \mid |G|$ and

$$[G : H] = \frac{|G|}{|H|}$$

Proof: Write $k = [G : H]$ and let $Ha_1, ..., Ha_k$ be the distinct right cosets of H in G. By prop

$$G = Ha_1 \sqcup \cdots \sqcup Ha_k$$

is a disjoint union. Since $|Ha_i| = |H|$ for each i, we have

$$|G| = |Ha_1| + \cdots + |Ha_k| = k|H|$$

It follows that $|H| \mid |G|$ and $[G : H] = k = \frac{|G|}{|H|}$. □

Corollary 3.5

1. If G is a finite group and $g \in G$ then $o(g) \mid |G|$
2. If G is a finite group with $|G| = n$, then for all $g \in G$, we have $g^n = 1$

Proof of 1: Take $H = \langle g \rangle$ in the theorem. Note that $|H| = o(g)$ □

Proof of 2: Let $o(g) = m$ then by (1), we have $m \mid n$. Thus

$$g^n = (g^m)^{\frac{n}{m}} = 1^{\frac{n}{m}} = 1$$

□

Example 3.2.3

For $n \in \mathbb{N}$ with $n \geq 2$, let $\mathbb{Z}_n^*$ be the set of (multiplicative) invertible elements in $\mathbb{Z}_n$. Let the *Euler's φ-function* $\varphi(n)$, denote the order of $\mathbb{Z}_n^*$. i.e.

$$\varphi(n) = |\{[k] \in \mathbb{Z}_n \mid k \in \{0, 1, ..., n-1\} \text{ and } \gcd(k, n) = 1\}|$$

As a direct consequence of the corollary, we see that if $a \in \mathbb{Z}$ with $\gcd(a, n) = 1$, then $a^{\varphi(n)} \equiv 1 \pmod{n}$. This is Euler's Theorem. If $n = p$, a prime number, then Euler's Theorem implies that $a^{p-1} \equiv 1 \pmod{p}$, which is Fermat's little theorem.

Recall

If $|G| = 2$ then $G \cong C_2$, and $|G| = 3$ then $G \cong C_3$.

Corollary 3.6

If G is a group with $|G| = p$ a prime, then $G \cong C_p$, the cyclic group of order p.

Proof: Let $g \in G$ with $g \neq 1$. Then by corollary, we have $o(g) \mid p$. Since $g \neq 1$ and p is a prime, we have $o(g) = p$. By proposition, we have

$$|\langle g \rangle| = o(g) = p$$

It follows that $G \cong \langle g \rangle \cong C_p$ □

Corollary 3.7

Let H and K be finite subgroups of a group G. If $\gcd(|H|, |K|) = 1$, then $H \cap K = \{1\}$.

Proof: Note $H \cap K$ is a subgroup of H and K. So by Lagrange's Theorem, we have $|H \cap K| \mid |H|$ and $|H \cap K| \mid |K|$. It follows that $|H \cap K| \mid \gcd(|H|, |K|)$, i.e. $|H \cap K| = 1$ Thus $H \cap K = \{1\}$. □

3.3 Normal Subgroups

Definition 3.3.1

Let H be a subgroup of a group G. If $gH = Hg$ for all $g \in G$, we say H is *normal*, denoted by $H \lhd G$.

Example 3.3.1

We have $\{1\} \lhd G$ and $G \lhd G$.

Example 3.3.2

The center $Z(G)$ of G is an abelian subgroup of G. By its definition, $Z(G) \lhd G$. Thus every subgroup of $Z(G)$ is normal in G.

Example 3.3.3

If G is an abelian group, then every subgroup of G is normal in G. Note the converse is false (see assignment 3)

Proposition 3.8 **Normality Test**

Let H be a subgroup of a group G. The following are equivalent:

1. $H \lhd G$
2. $gHg^{-1} \subseteq H$ for all $g \in G$. We call gHg^{-1} a *conjugate* of H
3. $gHg^{-1} = H$ for all $g \in G$. (Thus $H \lhd G$ if and only if H is the only conjugate of H)

Proof of $(1) \implies (2)$: Let $ghg^{-1} \in gHg^{-1}$ for some $h \in H$. Then by (1), $gh \in gH = Hg$, say $gh = h_1 g$ for some $h_1 \in H$. Then $ghg^{-1} = h_1 gg^{-1} = h_1 \in H$. □

Proof of $(2) \implies (3)$: If $g \in G$, then by (2), $gHg^{-1} \subseteq H$. Taking g^{-1} in place of g in (2), we get $g^{-1}Hg \subseteq H$. Thus implies that $H \subseteq gHg^{-1}$ Thus $H = gHg^{-1}$. □

Proof of $(3) \implies (1)$: If $gHg^{-1} = H$, then $gH = Hg$. □

Example 3.3.4

Let $G = \mathrm{GL}_n(\mathbb{R})$ and $H = \mathrm{SL}_n(\mathbb{R})$. For $A \in G$ and $B \in H$, we have

$$\det(ABA^{-1}) = \det A \det B \det A^{-1} = \det B = 1$$

Thus $ABA^{-1} \in H$ and it follows that $AHA^{-1} \subseteq H$ for all $A \in G$, so by the normality test, $\mathrm{SL}_n(\mathbb{R}) \lhd \mathrm{GL}_n(\mathbb{R})$.

Proposition 3.9

If H is a subgroup of a group G with $[G : H] = 2$, then $H \lhd G$.

Proof: Let $g \in G$, If $g \in H$, then $Hg = H = gH$. If $g \notin H$, since $[G : H] = 2$, then $G = H \sqcup Hg$, a disjoint union. Then $Hg = G \setminus H$. Similarly, $gH = G \setminus H$. Thus $gH = Hg$ for all $g \in G$ i.e. $H \lhd G$. □

Example 3.3.5

Let A_n be the alternating group contained in S_n. Since $[S_n : A_n] = 2$. By proposition, we have $A_n \lhd S_n$.

Example 3.3.6

Let $D_{2n} = \langle a, b \mid a^n = 1 = b^2 \text{ and } aba = b \rangle$ be the dihedral group of order $2n$. Since $[D_{2n} : \langle a \rangle] = 2$, by proposition, $\langle a \rangle \lhd D_{2n}$

Let H and K be subgroups of a group G. Then the intersection $H \cap K$ is the largest subgroup of G that contained in both H and K.

<u>Question:</u> What is the smallest subgroup containing H and K? Note that $H \cup K$ is the smallest subset

containing H and K, but $H \cup K$ is a subgroup if and only if $H \subseteq K$ or $H \supseteq K$. A more useful subset to consider is the *product* HK of H and K defined as follows

Definition 3.3.2

$HK = \{hk \mid h \in H, k \in K\}$

Remark

The product of 2 subgroups is not always a subgroup.

Lemma 3.10

Let H and K be subgroups of a group G, then the following are equivalent:

1. HK is a subgroup of G
2. $HK = KH$
3. KH is a subgroup of G.

Proof of **$(1 \iff 2)$*:*** Note that $(2 \iff 3)$ will follow after exchanging H and K. Suppose (2) holds, we have $1 = 1 \cdot 1 \in HK$. Also if $hk \in HK$, then $(hk)^{-1} = k^{-1}h^{-1} \in KH = HK$. Also for $hk, h_1, k_1 \in HK$, we have $kh_1 \in KH = HK$, say $kh_1 = h_2k_2$, it follows that

$$(hk)(h_1k_1) = h(kh_1)k_1 = h(h_2k_2)k_1 = (hh_2)(k_2k_1) \in HK$$

By the subgroup test, HK is a subgroup of G. Suppose conversely that (1) holds. Let $kh \in KH$ with $k \in K, h \in H$. Since H and K are subgroups of G, we have $h^{-1} \in H$, and $k^{-1} \in K$. Since HK is a subgroup of G, we have

$$kh = \left(h^{-1}k^{-1}\right)^{-1} \in HK$$

Thus $KH \subseteq HK$, similarly, one can show $HK \subseteq KH$. Thus $HK = KH$. □

Proposition 3.11

Let H and K be subgroups of a group G. Then

1. If $H \lhd G$ or $K \lhd G$, then $HK = KH$ is a subgroup of G
2. If $H \lhd G$ and $K \lhd G$, then $KH \lhd G$

Proof of 1: Suppose $H \lhd G$ then

$$HK = \bigcup_{k \in K} Hk = \bigcup_{k \in K} kH = KH$$

By lemma, $HK = KH$ is a subgroup of G. □

Proof of 2: If $g \in G$ and $hk \in HK$, since $H \lhd G$ and $K \lhd G$ we have

$$g^{-1}(hk)g = (g^{-1}hg)(g^{-1}kg) \in HK$$

Thus $g^{-1}HKg \subseteq HK$ and $HK \lhd G$. □

Definition 3.3.3

Let H be a subgroup of a group G. The *normalizer* of H, denoted by $N_G(H)$ is defined to be

$$N_G(H) = \{g \in G \mid gH = Hg\}$$

We see that $H \lhd G$ if and only if $N_G(H) = G$

Note

In the proof of the previous proposition, we do not need the full assumption that $H \lhd G$. We only need $kH = Hk$ for all $k \in K$, i.e. $k \in N_G(H)$ Thus

Corollary 3.12

Let H and K be subgroups of a group G. If $K \subseteq N_G(H)$ (or $H \subseteq N_G(K)$) then $HK = KH$ is a subgroup of G.

Theorem 3.13

If $H \lhd G$ and $K \lhd G$ satisfy $H \cap K = \{1\}$, then $HK \cong H \times K$.

Proof:
Claim: If $H \lhd G$ and $K \lhd G$ satisfy $H \cap K = \{1\}$ then $hk = kh$ for all $h \in H$ and $k \in K$.
Consider $x = hk(kh)^{-1} = hkh^{-1}k^{-1}$. Note that $kh^{-1}k^{-1} \in kHk^{-1} = H$ (since $H \lhd G$). Thus $x \in H$.
Similarly, since $hkh^{-1} \in hKh^{-1} = K$, we have $x \in K$. Since $x \in H \cap K = \{1\}$, we have $hkh^{-1}k^{-1} = 1$ i.e. $hk = kh$.
Since $H \lhd G$, by proposition, HK is a subgroup of G. Define $\sigma : H \times K \to HK$ by $\sigma(h, k) = hk$.
Claim: σ is an isomorphism.
Let $(h, k), (h_1, k_1) \in H \times K$ By claim 1, we have $h_1 k = k h_1$. Thus

$$\sigma((h, k) \cdot (h_1, k_1)) = \sigma(hh_1, kk_1) = hh_1kk_1 = hkh_1k_1 = \sigma(h, k) \cdot \sigma(h_1, k_1)$$

Thus σ is a homomorphism. Note that by the definition of HK, σ is surjective. Also, if $\sigma(h, k) = \sigma(h_1, k_1)$, we have $hk = h_1k_1$. Thus $h_1^{-1}h = k_1k^{-1} \in H \cap K = \{1\}$ Thus $h_1^{-1}h = 1 = k_1k^{-1}$ i.e. $h_1 = h$ and $k_1 = k$. Thus σ is injective. So σ is an isomorphism and we have $HK \cong H \times K$. □

Corollary 3.14

Let G be a finite group, and let H and K be normal subgroups such that $H \cap K = \{1\}$ and $|H||K| = |G|$. Then $G \cong H \times K$.

Proof:

$$|HK| = \frac{|H||K|}{|H \cap K|} = |H||K| = |G|$$

Thus $HK = G$, and so a direct application of the theorem gives $G = HK \cong H \times K$. □

Example 3.3.7

Let $m, n \in \mathbb{N}$ with $\gcd(m, n) = 1$. Let G be a cyclic group of order mn. Write $G = \langle a \rangle$ with $o(a) = mn$. Let $H = \langle a^n \rangle$ and $K = \langle a^m \rangle$. Thus $|H| = o(a^n) = m$ and $|K| = o(a^m) = n$. It follows that $|H||K| = mn = |G|$. Since $\gcd(m, n) = 1$, by corollary, we have $H \cap K = \{1\}$. Also, since G is cyclic and thus abelian, we have $H \lhd G$ and $K \lhd G$. Then by corollary, we have $G \cong H \times K$, i.e. $C_{mn} \cong C_m \times C_n$. Hence, to consider finite cyclic groups, it suffices to consider cyclic groups of prime power order.

4 Isomorphism Theorems

4.1 Quotient Groups

Remark

Let K be a subgroup of G. Consider the set of right cosets of K, i.e. $\{Ka \mid a \in G\}$. To make it a group, a natural way is to define

$$Ka \cdot Kb = Kab \quad \forall a, b \in G \qquad (*)$$

Note that we could have $Ka = Ka_1$ and $Kb = Kb_1$ with $a \neq a_1$ and $b \neq b_1$, Thus in order for $(*)$ to make sense, a necessary condition is

$$Ka = Ka_1 \text{ and } Kb = Kb_1 \Longrightarrow Kab = Ka_1b_1$$

In this case, we say that the multiplication is *well-defined.*

Lemma 4.1

Let K be a subgroup of a group G, the following are equivalent:

1. $K \lhd G$
2. For $a, b \in G$, the multiplication $Ka \cdot Kb = Kab$ is well-defined.

Proof of $(1 \Rightarrow 2)$***:*** Let $Ka = Ka_1$ and $Kb = Kb_1$. Thus $aa_1^{-1} \in K$ and $bb_1^{-1} \in K$. To get $Kab = Ka_1b_1$, we need $ab(a_1b_1)^{-1} \in K$. Note that since $K \lhd G$, we have $aKa^{-1} = K$. Thus

$$ab(a_1b_1)^{-1} = abb_1^{-1}a_1^{-1} = (abb_1^{-1}a^{-1})(aa_1^{-1}) \in K$$

Thus $Kab = Ka_1b_1$. □

Proof of $(2 \Rightarrow 1)$***:*** If $a \in G$, to show $K \lhd G$, we need $aka^{-1} \in K$ for all $k \in K$. Since $Ka = Ka$ and $Kk = K1$, by (2), we have $Kak = Ka1$ i.e. $Kak = Ka$. It follows that $aka^{-1} \in K$. Thus $K \lhd G$. □

Proposition 4.2

Let $K \lhd G$ and write $G/K = \{Ka \mid a \in G\}$ for the set of all cosets of K. Then

1. G/K is a group under the operation $Ka * Kb = Kab$.
2. The mapping $\varphi : G \to G/K$ given by $\varphi(a) = Ka$ is a surjective homomorphism.
3. If $[G : K]$ is finite, then $|G/K| = [G : K]$. In particular, if $|G|$ is finite, then $|G/K| = \frac{|G|}{|K|}$

Proof of 1: By other proposition, the operation is well defined and G/K is closed under operation. The identity of G/K is $K \cdot 1 = K$. Also, the inverse of Ka is Ka^{-1}. Finally, by the associativity of G, we have

$$Ka(KbKc) = (KaKb)Kc.$$

It follows that G/K is a group. □

Proof of 2: φ is clearly surjective. Also, for $a, b \in G$, we have

$$\varphi(a)\varphi(b) = KaKb = Kab = \varphi(ab)$$

so φ is a homomorphism. □

Proof of 3: If $[G : K]$ is finite, by the definition of index, $|G/K| = [G : K]$. Also, if $|G|$ is finite, by Lagrange's Theorem, $|G/K| = [G : K] = \frac{|G|}{|K|}$ □

Definition 4.1.1

Let $K \lhd G$. The group G/K of all cosets of K in G is called the *quotient group of* G *by* K. Also, the mapping $\varphi : G \to G/K$ given by $\varphi(a) = Ka$ is called the *coset map*.

Exercise 4.1.1

List all normal subgroups of D_{10} and all quotient groups of D_{10}/K.

4.2 Isomorphism Theorems

Definition 4.2.1

Let $\alpha : G \to H$ be a group homomorphism. The *kernel of* α is defined by

$$\ker \alpha = \{g \in G \mid \alpha(g) = 1_H\} \subseteq G$$

and the *image of* α is defined by

$$\operatorname{im} \alpha = \alpha(G) = \{\alpha(g) \mid g \in G\} \subseteq H$$

Proposition 4.3

Let $\alpha : G \to H$ be a group homomorphism

1. $\operatorname{im} \alpha$ is a subgroup of H
2. $\ker \alpha$ is a normal subgroup of G

Proof of 1: Note that $1_H = \alpha(1_G) \in \operatorname{im} \alpha$. Also, for $h_1 = \alpha(g_1), h_2 = \alpha(g_2) \in \operatorname{im} \alpha$, we have

$$h_1 h_2 = \alpha(g_1)\alpha(g_2) = \alpha(g_1 g_2) \in \operatorname{im} \alpha$$

Also, by proposition, $\alpha(g)^{-1} = \alpha(g^{-1}) \in \operatorname{im} \alpha$. By the subgroup test, $\operatorname{im} \alpha$ is a subgroup of H. □

Proof of 2: For $\ker \alpha$, note that $\alpha(1_G) = 1_H$. Also, for $k_1, k_2 \in \ker \alpha$, then

$$\alpha(k_1 k_2) = \alpha(k_1)\alpha(k_2) = 1 \cdot 1 = 1$$

and

$$\alpha(k_1^{-1}) = \alpha(k_1)^{-1} = 1^{-1} = 1$$

By the subgroup test, $\ker \alpha$ is a subgroup of G. Note that if $g \in H$ and $k \in \ker \alpha$, then

$$\alpha(gkg^{-1}) = \alpha(g)\alpha(k)\alpha(g^{-1}) = \alpha(g)1\alpha(g)^{-1} = 1$$

Thus $g(\ker \alpha)g^{-1} \subseteq \ker \alpha$. By the normality test, $\ker \alpha \lhd G$. □

Example 4.2.1

Consider the determinant map $\det : \mathrm{GL}_n(\mathbb{R}) \to \mathbb{R}^*$ defined by $A \mapsto \det A$. Then $\ker(\det) = \mathrm{SL}_n(\mathbb{R})$. Thus, we get another proof that $\mathrm{SL}_n(\mathbb{R}) \lhd \mathrm{GL}_n(\mathbb{R})$.

Example 4.2.2

Define the *sign* of a permutation $\sigma \in S_n$ by

$$\operatorname{sgn}(\sigma) = \begin{cases} 1 & \text{if } \sigma \text{ is even} \\ -1 & \text{if } \sigma \text{ is odd} \end{cases}$$

Note that $\operatorname{sgn} : S_n \to (\pm 1, \cdot)$ defined by $\sigma \mapsto \operatorname{sgn}(\sigma)$ is a homomorphism. Also, $\ker(\operatorname{sgn}) = A_n$ Thus we have another proof that $A_n \lhd S_n$.

Theorem 4.4 **First Isomorphism Theorem**

Let $\alpha : G \to H$ be a group homomorphism. Then

$$G / \ker \alpha \cong \operatorname{im} \alpha$$

Proof: Let $K = \ker \alpha$. Since $K \lhd G$, G/K is a group. Define the map

$$\begin{aligned} \overline{\alpha} : G/K &\longrightarrow \operatorname{im} \alpha \\ Kg &\longmapsto \alpha(g) \end{aligned}$$

Note that

$$Kg = Kg_1 \iff gg_1^{-1} \in K \iff \alpha(gg_1^{-1}) = 1 \iff \alpha(g) = \alpha(g_1)$$

Thus, $\overline{\alpha}$ is well-defined and injective. Also $\overline{\alpha}$ is clearly surjective. For $g, h \in G$, we have

$$\overline{\alpha}(KgKh) = \overline{\alpha}(Kgh) = \alpha(gh) = \alpha(g)\alpha(h) = \overline{\alpha}(Kg)\overline{\alpha}(Kh)$$

Thus $\overline{\alpha}$ is a group isomorphism and we have $G / \ker \alpha \cong \operatorname{im} \alpha$. □

Remark

Let $\alpha : G \to H$ be a group homomorphism and $K = \ker \alpha$. Let $\varphi : G \to G/K$ be the coset map and let $\overline{\alpha}$ be defined as in the previous proof. We have the following diagram:

$$\begin{tikzcd}
G \arrow[r, "\alpha"] \arrow[d, "\varphi"'] & \operatorname{im}\alpha \\
G/K \arrow[ur, dashed, "\overline{\alpha}"] &
\end{tikzcd}$$

Note that for $g \in G$, we have

$$\overline{\alpha}\varphi(g) = \overline{\alpha}(\varphi(g)) = \overline{\alpha}(Kg) = \alpha(g)$$

Thus $\alpha = \overline{\alpha}\varphi$ on the other hand, if we have $\alpha = \overline{\alpha}\varphi$, then the action of $\overline{\alpha}$ is determined by α and φ as

$$\overline{\alpha}(Kg) = \overline{\alpha}(\varphi(g)) = \overline{\alpha}\varphi(g) = \alpha(g)$$

Thus $\overline{\alpha}$ is the only homomorphism $G/K \to H$ satisfying $\overline{\alpha}\varphi = \alpha$.

Proposition 4.5

Let $\alpha : G \to H$ be group homomorphism and $K = \ker \alpha$. Then α factors uniquely as $\alpha = \overline{\alpha}\varphi$ where $\varphi : g \to G/K$ is the coset map and $\overline{\alpha} : G/K \to H$ is defined by $\overline{\alpha}(Kg) = \alpha(g)$. Note that φ is surjective and $\overline{\alpha}$ is injective.

Example 4.2.3

We have seen that $(\mathbb{Z}, +) = \langle \pm 1 \rangle$ and for $n \in \mathbb{N}$, $(\mathbb{Z}_n, +) = \langle [1] \rangle$ are cyclic groups. In the following, we will show that these are the only cyclic groups.
Let $G = \langle g \rangle$ be a cyclic group. Consider $\alpha : (\mathbb{Z}, +) \to G$ defined by $\alpha(k) = g^k$ for all $k \in \mathbb{Z}$, which is a group homomorphism. By the definition of $\langle g \rangle$, α is surjective. Note that $\ker \alpha = \{k \in \mathbb{Z} \mid g^k = 1\}$, we have two cases:

1. If $o(g) = \infty$, then $\ker \alpha = \{0\}$. By the first isomorphism theorem, we have
$$G \cong \mathbb{Z}/\{0\} \cong \mathbb{Z}$$
2. If $o(g) = n$, by proposition, $\ker \alpha = n\mathbb{Z}$. By the fist isomorphism theorem,
$$G \cong \mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}_n$$

By (1) and (2), we can conclude that if G is cyclic, then $G \cong \mathbb{Z}$ or $G \cong \mathbb{Z}_n$.

Theorem 4.6 **Second Isomorphism Theorem**

Let H and K be subgroups of a group G with $K \lhd G$. Then HK is a subgroup of G, $K \lhd HK$, $H \cap K \lhd H$ and $HK/K \cong H/H \cap K$.

Proof: Since $K \lhd G$, by proposition, HK is a subgroup, $HK = KH$ and $K \lhd HK$. Consider $\alpha : H \to HK/K$ defined by $\alpha(h) = Kh$. (note that $h \in H \subseteq HK$). Then α is a homomorphism (exercise). Also, if $x \in HK = KH$, say $x = kh$, then

$$Kx = K(kh) = Kh = \alpha(h)$$

Thus α is surjective. Finally, by proposition,

$$\ker \alpha = \{h \in H \mid Kh = K\} = \{h \in H \mid h \in K\} = H \cap K$$

By the first isomorphism theorem,

$$H/H \cap K \cong HK/K$$

□

Theorem 4.7 **Third Isomorphism Theorem**

Let $K \subseteq H \subseteq G$ be groups with $K \lhd G$ and $H \lhd G$. Then $H/K \lhd G/K$ and

$$(G/K)/(H/K) \cong G/H$$

Proof: Define $\alpha : G/K \to G/H$ by $\alpha(Kg) = Hg$ for all $g \in G$. Note that if $Kg = Kg_1$, then $gg_1^{-1} \in K \subseteq H$. Thus $Hg = Hg_1$ and α is well defined. Clearly, α is surjective. Note that

$$\ker \alpha = \{Kg \mid Hg = H\} = \{Kg \mid g \in H\} = H/K$$

By the first isomorphism theorem,

$$(G/K)/(H/K) \cong G/H$$

□

5 Group Actions

5.1 Cayley's Theorem

Theorem 5.1 **Cayley's Theorem**

If G is a finite group of order n, then G is isomorphic to a subgroup of S_n.

Proof: Let $G = \langle g_1, ..., g_n\rangle$ and let S_G be the permutation group of G. By identifying g_i with i, we see that $S_G \cong S_n$. Thus it suffices to find a injective homomorphism $\sigma : G \to S_G$. For $a \in G$, define $\mu_a : G \to G$ by $\mu_a(g) = ag$ for all $g \in G$. Note that $ag = ag_1$ implies $g = g_1$ and $a(a^{-1}g) = g$. Hence μ_a is a bijection and $\mu_a \in S_G$. Define $\sigma : G \to S_G$ by $\sigma(a) = \mu_a$. For $a, b \in G$, we have $\mu_a \mu_b = \mu_{ab}$ and σ is a homomorphism. Also, if $\mu_a = \mu_b$, then $a = \mu_a(1) = \mu_b(1) = b$. Thus, by the first isomorphism theorem, we have $G \cong \operatorname{im} \sigma$, a subgroup of $S_G \cong S_n$. □

Example 5.1.1

Let H be a subgroup of a group G with $[G : H] = m < \infty$. Let $X = \{g_1H, g_2H, ..., g_mH\}$ be the set of all distinct left cosets of H in G. For $a \in G$, define $\lambda_a : X \to X$ by $\lambda_a(gH) = agH$ for all $gH \in X$. Note that $agH = ag_1H$ implies that $gH = g_1H$ and $a(a^{-1}gH) = gH$. Hence λ_a is a bijection and thus $\lambda_a \in S_X$. Consider $\tau : G \to S_X$ defined by $\tau(a) = \lambda_a$. For $a, b \in G$, we have $\lambda_{ab} = \lambda_a\lambda_b$ and thus τ is a homomorphism. Note that if $a \in \ker \tau$, then λ_a is the identity permutation. In particular, $aH = \lambda_a(H) = H$. In particular, $a \in H$. Thus $\ker \tau \subseteq H$.

Theorem 5.2 **Extended Cayley's Theorem**

Let H be a subgroup of a group G with $[G : H] = m < \infty$. If G has no normal subgroup contained in H except for $\{1\}$, then G is isomorphic to a subgroup of S_m.

Proof: Let X be the set of all distinct left cosets of H in G. We have $|X| = m$ and $S_X \cong S_m$. We have seen from the above example that there exist a group homomorphism $\tau : G \to S_X$ with $K = \ker \tau \subseteq H$. By the first isomorphism theorem, we have $G/K \cong \operatorname{im} \tau$. Since $K \subseteq H$ and $K \lhd G$, by the assumption, we have $K = \{1\}$. It follows that $G \cong \operatorname{im} \tau$, a subgroup of $S_X \cong S_m$. □

Corollary 5.3

Let G be a finite group and p the smallest prime dividing $|G|$. If H is a subgroup of G with $[G : H] = p$ then $H \lhd G$.

Proof: Let X be the set of all distinct left cosets of H in G. We have $|X| = p$ and $S_X \cong S_p$. Let $\tau : G \to S_X \cong S_p$ be the group homomorphism defined in the above example with $K := \ker \tau \subseteq H$. By the first isomorphism theorem, we have $G/K \cong \operatorname{im} \tau \subseteq S_p$. Thus G/K is isomorphic to a subgroup of S_p. By Lagrange's Theorem, we have $|G/K| \mid p!$. Also, since $K \subseteq H$, if $[H : K] = k$, then

$$|G/K| = \frac{|G|}{|K|} = \frac{|G|}{|H|}\frac{|H|}{|K|} = pk.$$

Thus $pk \mid p!$ and hence $k \mid (p-1)!$. Since $k \mid |H|$, which divides $|G|$ and p is the smallest prime dividing $|G|$, we see every prime divisor of k must be $\geq p$ unless $k = 1$. Combining this with $k \mid (p-1)!$, this forces $k = 1$, which implies $K = H$, thus $H \lhd G$. □

5.2 Group Actions

Definition 5.2.1

Let G be a group and X a non-empty set. A (left) *group action of G on X* is a mapping $G \times X \to X$ denoted $(a, x) \mapsto a \cdot x$ such that

1. $1 \cdot x = x$ for all $x \in X$
2. $a \cdot (b \cdot x) = (ab) \cdot x$ for all $a, b \in G$ and $x \in X$

In this case, we say *G acts on X*.

Remark

Let G be a group acting on a set $X \neq \emptyset$. For $a, b \in G$ and $x, y \in X$, by (1) and (2), we have

$$a \cdot x = b \cdot y \iff (b^{-1}a) \cdot x = y$$

In particular, we have $a \cdot x = a \cdot y$ if and only if $x = y$.

Example 5.2.1

If G is group, let G act on itself by conjugation. i.e. $X = G$, by $a \cdot x = axa^{-1}$ for all $a, x \in G$. Note that

$$1 \cdot x = 1x1^{-1} = x$$

and

$$a \cdot (b \cdot x) = a(bxb^{-1})a^{-1} = (ab)x(ab)^{-1} = (ab) \cdot x$$

So it is indeed a group action.

Remark

For $a \in G$, define $\sigma_a : X \to X$ by $\sigma_a(x) = a \cdot x$ for all $x \in X$. Then one can show

1. $\sigma_a \in S_X$, the permutation group of X
2. The function $\theta : G \to S_X$ give $\theta(a) = \sigma_a$ is a group homomorphism with $\ker \theta = \{a \in G \mid ax = x \ \forall x \in X\}$

Note that the group homomorphism $\theta : G \to S_X$ gives an equivalent definition of group action of G on X. If $X = G$ with $|G| = n$ and $\ker \theta = \{1\}$, the map $\theta : G \to S_n$ shows that G is isomorphic to a subgroup of S_n, which is Cayley's Theorem. Thus, the notion of group action can be viewed as a generalization of the proof of Cayley's Theorem.

Definition 5.2.2

Let G be a group acting on $X \neq \emptyset$. Let $x \in X$. We call

1. $G \cdot x = \{g \cdot x \mid g \in G\} \subseteq X$ *The orbit of x*
2. $S(x) = \{g \in G \mid g \cdot x = x\} \subseteq G$ *The stabilizer of x*

Proposition 5.4

Let G be a group acting on a set $X \neq \emptyset$ and let $x \in X$. Then

1. $S(x)$ is a subgroup of G.
2. There exists a bijection from $G \cdot x$ to $\{gS(x) \mid g \in G\}$ and thus $|G \cdot x| = [G : S(x)]$

Proof of 1: Since $1 \cdot x = x$, we have $1 \in S(x)$. Also, if $g, h \in S(x)$, then

$$gh \cdot (x) = g \cdot (h \cdot x) = g \cdot x = x$$

and

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

Thus $gh, g^{-1} \in S(x)$. By the subgroup test, $S(x)$ is a subgroup of G. □

Proof of 2: Consider the map $\varphi : G \to \{gS(x) \mid g \in G\}$ defined by $\varphi(g \cdot x) = gS(x)$. Note that

$$g \cdot x = h \cdot x \iff (h^{-1}g) \cdot x = x \iff h^{-1}g \in S(x) \iff hS(x) = gS(x)$$

Thus φ is well-defined and injective. Since φ is clearly surjective, φ is a bijection. It follows that

$$|G \cdot x| = |\{gS(x) \mid g \in G\}| = [G : S(x)]$$

□

Theorem 5.5 **Orbit Decomposition Theorem**

Let G be a group acting on a finite set $X \neq \emptyset$. Let

$$X_f = \{x \in X \mid a \cdot x = x \ \forall a \in G\}$$

(Note that $x \in X_f$ iff $|G \cdot x| = 1$) Let $G \cdot x_1, G \cdot x_2, ..., G \cdot x_n$ denote the distinct non-singleton orbits (i.e. $|G \cdot x_i| > 1$) Then

$$|X| = |X_f| + \sum_{i=1}^{n} [G : S(x_i)]$$

Proof: Note that for $a, b \in G$ and $x, y \in X$,

$$a \cdot x = b \cdot y \iff (b^{-1}a) \cdot x = y \iff y \in G \cdot x \iff G \cdot y = G \cdot x$$

Thus two orbits are either disjoint, or the same. It follows that the orbits form a disjoint union of X. Since $x \in X_f$ iff $|G \cdot x| = 1$, the set $X \setminus X_f$ contains all non-singleton orbits, which are disjoint. Thus by proposition 5.4, we have

$$\begin{aligned} |X| &= |X_f| + \sum_{i=1}^{n} |G \cdot x_i| \\ &= |X_f| + \sum_{i=1}^{n} [G : S(x_i)] \end{aligned}$$

□

Example 5.2.2

Let G be a group acting on itself by conjugation i.e. $g \cdot x = gxg^{-1}$. Then

$$\begin{aligned} G_f &= \{x \in G \mid gxg^{-1} = x \ \forall g \in G\} \\ &= \{x \in G \mid gx = xg \ \forall g \in G\} \\ &= Z(G) \end{aligned}$$

Also, for $x \in G$,

$$S(x) = \{g \in G \mid gxg^{-1} = x\} = \{g \in G \mid gx = xg\}$$

This set is called the *centralizer* of x and is denoted by $S(x) = C_G(x)$. Finally in this case, the orbit

$$G \cdot x = \{gxg^{-1} \mid g \in G\}$$

is called the *conjugacy class of* x.

By Theorem 5.5,

Corollary 5.6 **Class Equation**

Let G be a finite group and let $\{gx_1g^{-1} \mid g \in G\}, ..., \{gx_ng^{-1} \mid g \in G\}$ denote the distinct non-singleton conjugacy classes, then

$$|G| = |Z(G)| + \sum_{i=1}^{n} [G : C_G(x_i)]$$

Lemma 5.7

Let p be a prime and $m \in \mathbb{N}$. Let G be a group of order p^m acting on a finite set $X \neq \emptyset$. Let X_f be defined as in Theorem 5.5. Then we have

$$|X| \equiv |X_f| \pmod{p}$$

Proof: By Theorem 5.5, we have

$$|X| = |X_f| + \sum_{i=1}^{n} [G : S(x_i)] \text{ with } [g : S(x_i)] > 1$$

Since $[G : S(x_i)]$ divides $|G| = p^m$ and $[G : S(x_i)] > 1$. We have $p \mid [G : S(x_i)]$ for all i. It follows that

$$|X| \equiv |X_f| \pmod{p}$$

$\square$

Theorem 5.8 **Cauchy's Theorem**

Let p be a prime and G a finite group. If $p \mid |G|$, then G contains an element of order p.

Proof: Define $X = \{(a_1, ..., a_p) \mid a_i \in G \text{ and } a_1 \cdots a_p = 1\}$. Since a_p is uniquely determined by $a_1, ..., a_{p-1}$, if $|G| = n$, we have $|X| = n^{p-1}$. Since $p \mid n$, we have $|X| \equiv 0 \pmod p$. Let the group $\mathbb{Z}_p = (\mathbb{Z}_p, +)$ acts on X by "cycling", i.e. for $k \in \mathbb{Z}_p$,

$$k \cdot (a_1, ..., a_p) = (a_{k+1}, ..., a_p, a_1, ..., a_k)$$

One can verify that this action is well defined. Let X_f be defined as in theorem 5.5. Then $(a_1, ..., a_p) \in X_f$ iff $a_1 = a_2 = \cdots = a_p$. Clearly $(1, 1, ..., 1) \in X_f$ and hence $|X_f| \geq 1$. Since $|\mathbb{Z}_p| = p$, by lemma 5.7, we have

$$|X_f| \equiv |X| \equiv 0 \pmod p$$

Since $|X_f| \equiv 0 \pmod p$ and $|X_f| \geq 1$. It follows that $|X_f| \geq p$. Therefore, there exists $a \neq 1$ st $(a, .., a) \in X_f$ which implies that $a^p = 1$. Since p is prime and $a \neq 1$, the order of a is p. □

6 Sylow Theorems

6.1 p-groups

Definition 6.1.1

Let p be a prime. A group in which every element has order of a non-negative power of p is called a *p-group*

Remark

As a direct consequence of Cauchy's Theorem we have

Corollary 6.1

A finite group G is a p-group if and only if $|G|$ is a power of p

Lemma 6.2

The center $Z(G)$ of a non-trivial finite p-group G contains more than one element.

Proof: The class equation of G (Cor 5.6) states that

$$|G| = |Z(G)| + \sum_{i=1}^{m} [G : C_G(x_i)]$$

where $[G : C_G(x_i)] > 1$. Since G is a p-group, by Cor 6.1, $p \mid |G|$. By lemma 5.7, $|Z(G)| \equiv |G| \equiv 0 \pmod p$. It follows that $p \mid |Z(G)|$. Since $1 \in Z(G)$ and $|Z(G)| \geq 1$, $Z(G)$ has at least p elements. □

Recall

If H is a subgroup of a group G, then $N_G(H) = \{g \in G \mid gHg^{-1} = H\}$ is the *normalizer* of H in G. In particular, $H \lhd N_G(H)$.

Lemma 6.3

If H is a p-subgroup of a finite group G, then

$$[N_G(H) : H] \equiv [G : H] \pmod p$$

Proof: Let X be the set of all left cosets of H in G. Hence $|X| = [G : H]$. Let H act on X by left multiplication. Then for $x \in G$, we have

$$\begin{aligned} xH \in X_f &\iff hxH = xH \ \forall h \in H \\ &\iff x^{-1}hxH = H \ \forall h \in H \\ &\iff x^{-1}Hx = H \\ &\iff x \in N_G(H) \end{aligned}$$

Thus $|X_f|$ is the number of costs xH with $x \in N_G(H)$ and hence $|X_f| = [N_G(H) : H]$. By lemma 5.7,

$$[N_G(H) : H] = |X_f| \equiv |X| = [G : H] \pmod p$$

□

Corollary 6.4

Let H be a p-subgroup of a finite group G. If $p \mid [G : H]$ then $p \mid [N_G(H) : H]$ and $N_G(H) \neq H$.

Proof: Since $p \mid [G : H]$, by lemma 6.3, we have

$$[N_G(H) : H] \equiv [G : H] \equiv 0 \pmod p$$

Since $p \mid [N_G(H) : H]$ and $[N_G(H) : H] \geq 1$, we have $[N_G(H) : H] \geq p$. Thus $N_G(H) \neq H$. □

6.2 Three Sylow Theorems

Recall

Cauchy's theorem states that if $p \mid |G|$, then G contains an element of order p. Thus $|\langle a\rangle| = p$. The following first Sylow Theorem can be viewed as a generalization of Cauchy's Theorem.

Theorem 6.5 **First Sylow Theorem**

Let G be a group of order $p^n m$ where p is a prime, $n \geq 1$ and $\gcd(p, m) = 1$. Then G contains a subgroup of order p^i for all $1 \leq i \leq n$. Moreover, every subgroup of G of order p^i $(i < n)$ is normal in some subgroup of order p^{i+1}.

Proof: We prove this theorem by induction on i. For $i = 1$, since $p \mid |G|$, by Cauchy's theorem, G contains an element a of order p, i.e. $|\langle a\rangle| = p$. Suppose that the statement holds for some $1 \leq i < n$.

Say H is a subgroup of G of order p^i. Then $p \mid [G : H]$, by Cor 6.4, $p \mid [N_G(H) : H]$ and $[N_G(H) : H] \geq p$, $p \mid [G : H]$. Then by Cauchy's theorem, $N_G(H)/H$ contains a subgroup of order p. Such a group is of the form H_1/H, where H_1 is a subgroup of $N_G(H)$ containing H. Since $H \lhd N_G(H)$, we have $H \lhd H_1$. Finally, $|H_1| = |H||H_1/H| = p^i \cdot p = p^{i+1}$. □

Definition 6.2.1

A subgroup P of a group G is said to be a *Sylow p-subgroup* of G if P is a maximal p-group of G i.e. if $P \subseteq H \subseteq G$ with H a p-group, then $P = H$.

As a direct consequence of theorem 6.5,

Corollary 6.6

Let G be a group of order $p^n m$ where p is a prime, $n \geq 1$ and $\gcd(p, m) = 1$. Let H be a p-subgroup of G.

1. H is a Sylow p-subgroup iff $|H| = p^n$
2. Every conjugate of a Sylow p-subgroup is a Sylow p-subgroup.
3. If there is only one Sylow p-subgroup P, then $P \lhd G$.

Theorem 6.7 **Second Sylow Theorem**

If H is a p-subgroup of a finite group G, and P is any Sylow p-subgroup of G, then there exists $g \in G$ such that $H \subseteq gPg^{-1}$. In particular, any two Sylow p-subgroups are conjugate.

Proof: Let X be the set of all left cosets of P in G, and let H act on X by left multiplication. By lemma 5.7, we have $|X_f| \equiv |X| = [G : P] \pmod{p}$. Since $p \nmid [G : P]$, we have $|X_f| \neq 0$. Thus there exists $gP \in X_f$ for some $g \in G$. Note that

$$\begin{aligned} gP \in X_f &\iff hgP = gP \quad \forall h \in H \\ &\iff g^{-1}hgP = P \quad \forall h \in H \\ &\iff g^{-1}Hg \subseteq P \\ &\iff H \subseteq gPg^{-1} \end{aligned}$$

If H is Sylow p-subgroup, then $|H| = |P| = |gHg^{-1}|$, thus $H = gPg^{-1}$. □

Theorem 6.8 **Third Sylow Theorem**

If G is a finite group and p a prime with $p \mid |G|$, then the number of Sylow p-subgroups of G divides $|G|$ and is of the form $kp + 1$ for some $k \in \mathbb{N} \cup \{0\}$.

Proof: By theorem 6.7, the number of Sylow p-subgroups of G is the number of conjugates of any of them, say P. This number is $[G : N_G(P)]$. Which is a divisor of $|G|$. Let X be the set of all Sylow p-subgroups of G and let P act on X by conjugation. Then $Q \in X_f$ iff $gQg^{-1} = Q$ for all $g \in P$. The latter condition holds iff $P \subseteq N_G(Q)$. Both P and Q are Sylow p-subgroups of G and hence $N_G(Q)$. Thus by Cor 6.6, they are conjugate in $N_G(Q)$. Since $Q \lhd N_G(Q)$, this can only occur if $Q = P$ and $X_f = \{P\}$. By lemma 5.7, $|X| \equiv |X_f| \equiv 1 \pmod{p}$. Thus $|X| = kp + 1$ for some $k \in \mathbb{N} \cup \{0\}$. □

Remark

Suppose that G is a group with $|G| = p^n m$ and $\gcd(p, m) = 1$. Let n_p be the number of p-subgroups of G. By the third Sylow theorem, we have $n_p \mid p^n m$ and $n_p \equiv 1 (\operatorname{mod} p)$. Since $p \nmid n_p$, we have $n_p \mid m$.

Example 6.2.1

<u>*Claim:*</u> every group of order 15 is cyclic.
Let n_p be the number of Sylow p-subgroups of G. By the third Sylow theorem, we have $n_3 \mid 5$ and $n_3 \equiv 1 (\operatorname{mod} 3)$. Thus $n_3 = 1$. Similarly, we have $n_5 \mid 3$ and $n_5 \equiv 1 (\operatorname{mod} 5)$, Thus $n_5 = 1$. It follows that there is only one Sylow 3-subgroup and Sylow 5-subgroup, say P_3 and P_5 respectively. Thus $P_3, P_5 \lhd G$. Consider $|P_3 \cap P_5|$, which divides 3 and 5. Thus $|P_3 \cap P_5| = 1$ and $P_3 \cap P_5 = \{1\}$. Also $|P_3 P_5| = 15 = |G|$ Thus

$$G \cong P_3 \times P_5 \cong \mathbb{Z}_3 \times \mathbb{Z}_5 \cong \mathbb{Z}_{15}$$

Example 6.2.2

<u>*Claim:*</u> there are two isomorphism classes of groups of order 21.
Let G be a group of order $21 = 3 \cdot 7$. Let n_p be the number of Sylow p-subgroups of G. By the third Sylow theorem, we have $n_3 \mid 7$ and $n_3 \equiv 1 (\operatorname{mod} 3)$. Thus $n_3 = 1$ or 7. Also we have $n_7 \mid 3$ and $n_7 \equiv 1 (\operatorname{mod} 7)$. Thus $n_7 = 1$. It follows that G has a unique Sylow 7-subgroup, say P_7. Note that $P_7 \lhd G$ and P_7 is cyclic, say $P_7 = \langle x : x^7 = 1 \rangle$. Let H be a Sylow 3-subgroup. Since $|H| = 3$, H is cyclic and $H = \langle y : y^3 = 1 \rangle$. Since $P_7 \lhd G$, we have $yxy^{-1} = x^i$ for some $0 \leq i \leq 6$. It follows that

$$x = y^3 x y^{-3} = y^2 (yxy^{-1}) y^{-2} = y^2 x^i y^{-2} = y(yx^i y^{-1}) y^{-1} = y x^{i^2} y^{-1} = x^{i^3}$$

Since $x^{i^3} = x$ and $x^7 = 1$, we have $i^3 - 1 \equiv 0 (\operatorname{mod} 7)$. Since $0 \leq i \leq 6$, we have $i = 1, 2, 4$.

1. If $i = 1$, then $yxy^{-1} = x$, i.e. $yx = xy$. Thus G is an abelian group. Since $P_3 \lhd G$, $P_7 \lhd G$, $P_3 \cap P_7 = \{1\}$ and $|G| = |P_3 P_7|$, we have
$$G \cong P_3 \times P_7 \cong \mathbb{Z}_3 \times \mathbb{Z}_7 \cong \mathbb{Z}_{21}$$
2. If $i = 2$, then $yxy^{-1} = x^2$. Thus
$$G = \{x^i y^j : 0 \leq i \leq 6, 0 \leq j \leq 2, yxy^{-1} = x^2\}$$
3. If $i = 4$, then $yxy^{-1} = x^4$. Note that
$$\begin{aligned} y^2 x y^{-2} &= y(yxy^{-1})y^{-1} \\ &= yx^4 y^{-1} \\ &= x^{16} = x^2 \end{aligned}$$

Note that y^2 is also a generator of H. Thus by replacing y by y^2, we get back to case 2. It follows that there are two isomorphism classes of groups of order 21.

7 Finite Abelian Groups

7.1 Primary Decomposition

Notation

Let G be a group and $m \in \mathbb{Z}$ we define

$$G^{(m)} = \{g \in G \mid g^m = 1\}$$

Proposition 7.1

Let G be an abelian group. Then $G^{(m)}$ is a subgroup of G.

Proof: We have $1 = 1^m \in G^{(m)}$. Also if $g, h \in G^{(m)}$, since G is abelian, we have $(gh)^m = g^m h^m = 1$ and thus $gh \in G^{(m)}$. Finally, if $g \in G^{(m)}$, we have

$$\left(g^{-1}\right)^m = g^{-m} = (g^m)^{-1} = 1$$

and thus $g^{-1} \in G^{(m)}$. By the subgroup test, $G^{(m)}$ is a subgroup of G. □

Proposition 7.2

Let G be a finite abelian group with $|G| = mk$ with $\gcd(m, k) = 1$. Then

1. $G \cong G^{(m)} \times G^{(k)}$
2. $\left|G^{(m)}\right| = m$ and $\left|G^{(k)}\right| = k$

Proof of 1: Since G is abelian, we have $G^{(m)} \lhd (G)$ and $G^{(k)} \lhd G$. Also, since $\gcd(m, k) = 1$, there exist $x, y \in \mathbb{Z}$ such that $1 = mx + ky$

<u>*Claim:*</u> $G^{(m)} \cap G^{(k)} = \{1\}$

If $g \in G^{(m)} \cap G^{(k)}$, then $g^m = 1 = g^k$. We have

$$g = g^{mx+ky} = (g^m)^x \left(g^k\right)^7 = 1$$

<u>*Claim:*</u> $G = G^{(m)} G^{(k)}$

If $g \in G$, then

$$1 = g^{mk} = (g^m)^k = \left(g^k\right)^m$$

It follows that $g^k \in G^{(m)}$ and $g^m \in G^{(k)}$. Thus

$$g = g^{mx+ky} = \left(g^k\right)^y (g^m)^x \in G^{(m)} G^{(k)}$$

Combining both claims, by Theorem 3.13, we have

$$G \cong G^{(m)} G^{(k)}$$

□

Proof of 2: Write $\left|G^{(m)}\right| = m'$ and $\left|G^{(k)}\right| = k'$. By (1), we have $mk = |G| = m'k'$

<u>*Claim:*</u> $\gcd(m, k') = 1$

Suppose that $\gcd(m, k') \neq 1$. Then there exists a prime p such that $p \mid m$ and $p \mid k'$. By Cauchy's theorem, there exists $g \in G^{(k)}$ with $o(g) = p$. Since $p \mid m$, we have $g^m = (g^p)^{\frac{m}{p}} = 1$, i.e. $g \in G^{(m)}$. By (1), we have $g \in G^{(m)} \cap G^{(k)} = \{1\}$, which gives a contradiction since $o(g) = p$. Thus we have $\gcd(m, k') = 1$. Note that since $m \mid m'k'$ and $\gcd(m, k') = 1$, we have $m \mid m'$. Similarly, we have $k \mid k'$. Since $mk = m'k'$, it follows that $m = m'$ and $k = k'$. □

As a direct consequence of proposition 7.2, we have

Theorem 7.3 **Primary Decomposition Theorem**

Let G be a finite abelian group with $|G| = p_1^{n_1} \cdots p_k^{n_k}$ where $p_1, \ldots, p_k$ are distinct primes and $n_1, \ldots, n_k \in \mathbb{N}$. Then we have

1. $G \cong G^{\left(p_1^{n_1}\right)} \times \cdots \times G^{\left(p_k^{n_k}\right)}$
2. $\left|G^{\left(p_i^{n_i}\right)}\right| = p_i^{n_i} \quad (1 \leq i \leq k)$.

Example 7.1.1

Let $G = \mathbb{Z}_{13}^*$. Then $|G| = 12 = 2^2 3$. Note that

$$G^{(3)} = \{a \in \mathbb{Z}_{13}^* \mid a^3 = 1\} = \{1, 3, 9\}$$
$$G^{(4)} = \{a \in \mathbb{Z}_{13}^* \mid a^4 = 1\} = \{1, 5, 8, 12\}$$

By theorem 7.3, we have

$$\mathbb{Z}_{13}^* \cong \{1, 5, 8, 12\} \times \{1, 3, 9\}$$

7.2 Structure Theorem of Finite Abelian Groups

We have seen that if $|G| = p$ (a prime), then $G \cong C_p$. Also, if $|G| = p^2$, then $G \cong C_{p^2}$ or $G \cong C_p \times C_p$.
Question How about abelian groups of order p^3, p^4 and p^n for general $n \in \mathbb{N}$.

Proposition 7.4

Let G be a finite abelian p-group that contains only one subgroup of order p, then G is cyclic. In other words, if a finite abelian p-group G is not cyclic, then G has at least two subgroups of order p.

Proof: Let $y \in G$ be of maximum order, i.e. $o(y) \geq o(x)\ \forall x \in G$.
Claim: $G = \langle y \rangle$.
Suppose that $G \neq \langle y \rangle$. Then the quotient group $G/\langle y \rangle$ is a nontrivial p-group, which contains an element z of order p by Cauchy's theorem. In particular $z \neq 1$. Consider the coset map $\pi : G \to G/\langle y \rangle$. Let $x \in G$ such that $\pi(x) = z$. Since $\pi(x^p) = \pi(x)^p = z^p = 1$, we see that $x^p \in \langle y \rangle$. Thus $x^p = y^m$ for some $m \in \mathbb{Z}$. Two cases:

1. If $p \nmid m$ since $o(y) = p^r$ for some $r \in \mathbb{N}$, by prop 2.11, $o(y^m) = o(y)$. Since y is of maximum order, we have $o(x^p) < o(x) \leq o(y) = o(y^m) = o(x^p)$ which is a contradiction.
2. If $p \mid m$, then $m = pk$ for some $k \in \mathbb{Z}$. Thus we have $x^p = y^m = y^{pk}$. Since G is abelian, we have $\left(xy^{-k}\right)^p = 1$. Thus xy^{-k} belongs to the one and only subgroup of order p, say H. On the other hand, the cyclic group $\langle y \rangle$ contains a subgroup of order p, which must be the one and only H. Thus $xy^{-k} \in \langle y \rangle$, which implies that $x \in \langle y \rangle$. It follows that $z = \pi(x) = 1$, a contradiction.

By combining the above two cases, we see that $G = \langle y \rangle$. □

Proposition 7.5

Let $G \neq \{1\}$ be a finite abelian p-group. Let C be a cyclic subgroup of maximum order. Then G contains a subgroup B such that

$$G = CB \text{ and } C \cap B = \{1\}$$

Theorem 7.6

Let $G \neq 1$ be a finite abelian p-group. Then G is isomorphic to a direct product of cyclic groups.

Proof: By prop 7.5, there exists a cyclic group C_1 and a subgroup B_1 of G such that $G \cong C_1 \times B_1$. Since $|B_1| \mid |G|$ by Lagrange's theorem, the group B_1 is also a p-group. Thus if $B_1 \neq \{1\}$, by prop 7.5, there exists a cyclic group C_2 and a subgroup B_2 such that $B_1 \cong C_2 \times B_2$. Continue in this way to get cyclic groups $C_1, \ldots, C_k$ until we get $B_k = \{1\}$ for some $k \in \mathbb{N}$. Then $G \cong C_1 \times \cdots \times C_k$. □

Remark

One can show that the decomposition of a finite abelian p-group into a direct product of cyclic groups is unique up to its order.

Combining the remark, theorem 7.6 and theorem 7.3, we have

Theorem 7.7 **Structure Theorem of Finite Abelian Groups**

If G is a finite abelian group, then

$$G \cong \mathbb{Z}_{p_1^{n_1}} \times \cdots \times \mathbb{Z}_{p_k^{n_k}}$$

Where $\mathbb{Z}_{p_i^{n_i}} = \left(\mathbb{Z}_{p_i^{n_i}}, +\right) \cong C_{p_i^{n_i}}$ are cyclic groups of order $p_i^{n_i}$ $(1 \leq i \leq k)$. Note that p_i are not necessarily distinct. The numbers $p_i^{n_i}$ are uniquely determined up to their order.

Note that if p_1 and p_2 are distinct primes, then $C_{p_1^{n_1}} \times C_{p_2^{n_2}} \cong C_{p_1^{n_1} p_2^{n_2}}$. Thus by combining suitable coprime factors together,

Theorem 7.8 **Invariant Factor Decomposition of Finite Abelian Groups**

Let G be a finite abelian group. Then

$$G \cong \mathbb{Z}_{n_1} \times \cdots \times \mathbb{Z}_{n_r}$$

where $n_i \in \mathbb{N}, n_1 > 1$ and $n_1 \mid n_2 \mid \cdots \mid n_r$.

Example 7.2.1

Let G be an abelian group of order 48. Since $48 = 2^4 \cdot 3$, by theorem 7.3, $G \cong H \times \mathbb{Z}_3$, where H is an abelian group of order 2^4. The options for H are $\mathbb{Z}_{2^4}, \mathbb{Z}_{2^3} \times \mathbb{Z}_2, \mathbb{Z}_{2^2} \times \mathbb{Z}_{2^2}, \mathbb{Z}_{2^2} \times \mathbb{Z}_2 \times \mathbb{Z}_2$ and $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$. Thus we have

$$\begin{aligned}
G &\cong \mathbb{Z}_{2^4} \times \mathbb{Z}_3 \cong \mathbb{Z}_{48} \\
G &\cong \mathbb{Z}_{2^3} \times \mathbb{Z}_2 \times \mathbb{Z}_3 \cong \mathbb{Z}_2 \times \mathbb{Z}_{24} \\
G &\cong \mathbb{Z}_{2^2} \times \mathbb{Z}_{2^2} \times \mathbb{Z}_3 \cong \mathbb{Z}_{2^2} \times \mathbb{Z}_{12} \\
G &\cong \mathbb{Z}_{2^2} \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3 \cong \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_{12} \\
G &\cong \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3 \cong \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_6
\end{aligned}$$

There are 5 non-isomorphic groups in total.

8 Rings

8.1 Rings

Definition 8.1.1

A set R is a (unitary) *ring* if it has two operations, addition $+$ and multiplication $\cdot$ such that $(R, +)$ is an abelian group and $(R, \cdot)$ satisfies the closure, associativity and identity properties of a group, in addition to a distributive law. More precisely, if R is a ring, then for all $a, b, c \in R$

1. $a + b \in R$
2. $a + (b + c) = (a + b) + c$
3. There exists $0 \in R$ such that $a + 0 = a = 0 + a$ (0 is called the *zero* of R)
4. There exists $-a \in R$ such that $a + (-a) = 0 = (-a) + a$ ($-a$ is called the *negative* of a)
5. $a + b = b + a$
6. $ab = a \cdot b \in R$
7. $a(bc) = (ab)c$
8. There exists $1 \in R$ such that $a \cdot 1 = a = 1 \cdot a$ (1 is called the *unity* of R)
9. $a(b + c) = ab + ac$ and $(b + c)a = ba + ca$ (distributive law)

The ring R is called a *commutative ring* if it also satisfies $ab = ba$.

Example 8.1.1

$\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ are commutative rings.

Example 8.1.2

For $n \in \mathbb{N}, n \geq 2$, $\mathbb{Z}_n$ is a commutative ring.

Example 8.1.3

For $n \in \mathbb{N}, n \geq 2$, $M_n(\mathbb{R})$ is a (non commutative) ring

Warning

Note that since $(R, \cdot)$ is not a group, there is no left or right cancellation. For example, in $\mathbb{Z}$, $0 \cdot x = 0 \cdot y$ does not imply $x = y$.

Notation

Given a ring R, to distinguish the difference between multiples in addition and in multiplication, for $n \in \mathbb{N}$ and $a \in R$, we write

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

Recall

For a group G and $g \in G$, we have $g^0 = 1, g^1 = g$ and $\left(g^{-1}\right)^{-1} = g$. Thus for addition, we have, for a ring R and $a \in R$

1. $\underbrace{0}_{\text{integer}} \cdot a = \underbrace{0}_{\text{zero of } R}$
2. $\underbrace{1}_{\text{integer}} a = a$
3. $-(-a) = a$

Notation

For $n \in \mathbb{N}$, we define

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

Also, we define $a^0 = 1$. If the multiplicative inverse of a exists,

$$a^{-n} = \left(a^{-1}\right)^n$$

Remark

By Prop 1.2 for $n, m \in \mathbb{Z}$, we have

1. $(na) + (ma) = (n + m)a$
2. $n(ma) = (nm)a$
3. $n(a + b) = na + nb$

Proposition 8.1

Let R be a ring and $r, s \in R$.

1. If 0 is the zero of R, then
$$0r = 0 = r0$$
2. $(-r)s = r(-s) = -(rs)$
3. $(-r)(-s) = rs$
4. For any $m, n \in \mathbb{Z}$,
$$(mr)(ns) = (mn)(rs)$$

Definition 8.1.2

A *trivial ring* is a ring of only one element. In this case, we have $1 = 0$.

Remark

If R is a ring with $R \neq \{0\}$, since $r = r1$ for all $r \in R$, we have $1 \neq 0$.

Example 8.1.4

Let $R_1, \ldots, R_n$ be rings. We define component-wise operations on the product $R_1 \times \cdots \times R_n$ as follows:

$$(r_1, \ldots, r_n) + (s_1, \ldots, s_n) = (r_1 + s_1, \ldots, r_n + s_n)$$
$$(r_1, \ldots, r_n) \cdot (s_1, \ldots, s_n) = (r_1 s_1, \ldots, r_n s_n)$$

One can check that $R_1 \times \cdots \times R_n$ is a ring. This set is called the *direct product* of $R_1, \ldots, R_n$.

Definition 8.1.3

If R is a ring, we define the *characteristic* of R denoted by $\operatorname{ch}(R)$, in terms of the order of 1_R in the additive group $(R, +)$:

$$\operatorname{ch}(R) = \begin{cases} n & \text{if } o(1_R) = n \in \mathbb{N} \text{ in } (R, +) \\ 0 & \text{if } o(1_R) = \infty \text{ in } (R, +) \end{cases}$$

Remark

For $k \in \mathbb{Z}$, we write $kR = 0$ to mean that $kr = 0$ for all $r \in R$.

By Prop 8.1, we have

$$kr = k(1_R r) = (k1_R)r$$

Thus $kR = 0$ if and only if $k1_R = 0$. By Prop 2.6 and 2.7,

Proposition 8.2

Let R be a ring and $k \in \mathbb{Z}$.

1. If $\text{ch}(R) = n \in \mathbb{N}$, then $kR = 0$ iff $n \mid k$
2. If $\text{ch}(R) = 0$, then $kR = 0$ iff $k = 0$

Example 8.1.5

Each of $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ has characteristic 0. For $n \in \mathbb{N}$ with $n \geq 2$, the ring $\mathbb{Z}_n$ has characteristic n.

8.2 Subrings

Definition 8.2.1

A subset S of a ring R is a *subring* if S is a ring itself with $1_S = 1_R$ (with the same addition and multiplication). Note that properties (2),(3),(7), and (9) of a ring are automatically satisfied. Thus to show that S is a subring, it suffices to show

Subring Test:

$S \subseteq R$ is a subring if

1. $1_R \in S$
2. If $s, t \in S$, then $s - t, st \in S$.

Note that if (2) holds, then $0 = s - s \in S$ and $-t = 0 - t \in S$

Example 8.2.1

We have a chain of commutative rings

$$\mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R} \subseteq \mathbb{C}$$

Example 8.2.2

If R is a ring, the *center* $Z(R)$ of R is defined to be

$$Z(R) = \{z \in R \mid zr = rz \ \forall r \in R\}$$

Note that $1_R \in Z(R)$. Also, if $s, t \in Z(R)$, then for $r \in R$,

$$(s - t)r = sr - tr = rs - rt = r(s - t)$$
$$(st)r = s(tr) = s(rt) = (sr)t = (rs)t = r(st)$$

By the subring test, $Z(R)$ is a subring of R.

Example 8.2.3

Let

$$\mathbb{Z}[i] = \left\{a + bi \;\middle|\; a, b \in \mathbb{Z} \text{ and } i^2 = -1\right\} \subseteq \mathbb{C}.$$

Then one can show that $\mathbb{Z}[i]$ is a subring of $\mathbb{C}$, called the *ring of Gaussian integers*.

8.3 Ideals

Note

Let R be a ring and A an additive subgroup of R. Since $(R, +)$ is abelian, we have $A \lhd R$. Thus we have the additive quotient group

$$R/A = \{r + A \mid r \in R\} \text{ with } r + A = \{r + a \mid a \in A\}$$

Using the known properties about cosets and quotient groups, we have

Proposition 8.3

Let R be a ring and A an additive subgroup of R. For $r, s \in R$, we have

1. $r + A = s + A$ iff $(r - s) \in A$
2. $(r + A) + (s + A) = (r + s) + A$
3. $0 + A = A$ is the (additive) identity of R/A
4. $-(r + A) = (-r) + A$ is the (additive) inverse of $r + A$
5. $k(r + A) = kr + A$ for all $k \in \mathbb{Z}$

Remark

Since R is a ring, it is natural to ask if we could make R/A a ring. A natural way to define multiplication in R/A is that

$$(r + A)(s + A) = (rs + A) \quad \forall r, s \in R \quad (*)$$

Note that we could have $r + A = r_1 + A$ and $s + A = s_1 + A$ with $r \neq r_1$ and $s \neq s_1$. Thus in order for $(*)$ to make sense, a necessary condition is

$$r + A = r_1 + A \text{ and } s + A = s_1 + A \Longrightarrow rs + A = r_1 s_1 + A$$

In this case, we say that multiplication $(r + A)(s + A)$ is *well-defined.*

Proposition 8.4

Let A be an additive subgroup of a ring R. For $a \in A$ define

$$Ra = \{ra \mid r \in R\} \text{ and } aR = \{ar \mid r \in R\}$$

Then the following are equivalent:

1. $Ra \subseteq A$ and $aR \subseteq A \quad \forall a \in A$
2. For $r, s \in R$, the multiplication $(r + A)(s + A)$ is well-defined in R/A.

Proof of $(1) \Rightarrow (2)$**:** If $r + A = r_1 + A$ and $s + A = s_1 + A$, we need to show that $rs + A = r_1 s_1 + A$. Since $(r - r_1) \in A$ and $(s - s_1) \in A$, by (1), we have

$$rs - r_1 s_1 = rs - r_1 s + r_1 s - r_1 s_1 = (r - r_1)s + r_1(s - s_1) \in A$$

By proposition 8.3, $rs + A = r_1 s_1 + A$. □

Proof of $(2) \Rightarrow (1)$**:** Let $r \in R$ and $a \in A$. By prop 8.1, we have

$$ra + A = (r + A)(a + A) = (r + A)(0 + A) = r0 + A = 0 + A = A$$

Thus $ra \in A$ and we have $Ra \subseteq A$. Similarly, we can show $aR \subseteq A$. □

Definition 8.3.1

An additive subgroup A of a ring R is an *ideal* of R if $Ra \subseteq R$ and $aR \subseteq A$.

<u>Ideal Test:</u>

1. $0 \in A$
2. For $a, b \in A$ and $r \in R$, we have $a - b \in A$ and $ra, ar \in A$

Example 8.3.1

If R is a ring, then $\{0\}$ and R are ideals of R.

Example 8.3.2

Let R be a commutative ring and $a_1, ..., a_n \in R$. Consider the set I generated by $a_1, ..., a_n$ i.e.

$$I = \langle a_1, ..., a_n \rangle = \{r_1 a_1 + \cdots + r_n a_n \mid r_i \in R\}$$

Then one can show that I is an ideal.

Proposition 8.5

Let A be an ideal of a ring R. If $1_R \in A$, then $A = R$.

***Proof*:** For every $r \in R$, since A is an ideal and $1_R \in A$, we have $r = r1_R \in A$. It follows that $R \subseteq A \subseteq R$ and hence $R = A$. □

From the above discussion, we have

Proposition 8.6

Let A be an ideal of a ring R. Then the additive quotient group R/A is a ring with multiplication $(r+A)(s+A) = rs + A$. The unity of R/A is $1 + A$.

Definition 8.3.2

Let A be an ideal of a ring R. The ring R/A is called a *quotient ring of R by A*.

Definition 8.3.3

Let R be a commutative ring and A an ideal of R. If $A = aR = Ra$ for some $a \in R$, we say A is a *principal ideal generated by a* and is denoted by $A = \langle a \rangle$.

Example 8.3.3

If $n \in \mathbb{Z}$, then $\langle z \rangle = n\mathbb{Z}$ is an ideal of $\mathbb{Z}$.

Proposition 8.7

All ideals of $\mathbb{Z}$ are of the form $\langle z \rangle$ for some $n \in \mathbb{Z}$. If $\langle n \rangle \neq \{0\}$ and $n \in \mathbb{N}$, then the generator is uniquely determined.

Proof: Let A be an ideal of $\mathbb{Z}$. If $A = \{0\}$, then $A = \langle 0 \rangle$. Otherwise, choose $a \in A$ with $a \neq 0$ and $|A|$ minimum. Clearly, $\langle a \rangle \subseteq A$. To prove the other inclusion, let $b \in A$. By the division algorithm, we have $b = qa + r$ with $q, r \in \mathbb{Z}$ and $0 \leq r < |a|$. If $r \neq 0$, since A is an ideal, and $a, b \in A$, we have $r = b - qa \in A$ with $|r| < |a|$, a contradiction. Thus $r = 0$ and $b = qa$, i.e. $b \in \langle a \rangle$. It follows that $A = \langle a \rangle$. □

8.4 Isomorphism Theorems

Definition 8.4.1

Let R, S be rings. A mapping $\theta : R \to S$ is a *ring homomorphism* if for all $a, b \in R$

1. $\theta(a+b) = \theta(a) + \theta(b)$
2. $\theta(ab) = \theta(a)\theta(b)$
3. $\theta(1_R) = 1_S$

Example 8.4.1

The mapping $k \mapsto [k]$ from $\mathbb{Z}$ to $\mathbb{Z}_n$ is a surjective ring homomorphism.

Example 8.4.2

If R_1, R_2 are rings, the projection $\pi_1 : R_1 \times R_2 \to R_1$ defined by $\pi_1(r_1, r_2) = r_1$ is a surjective ring homomorphism. Similarly for π_2.

Proposition 8.8

Let $\theta : R \to S$ be a ring homomorphism.

1. $\theta(0_R) = 0_S$
2. $\theta(-r) = -\theta(r)$
3. $\theta(kr) = k\theta(r)$ for all $k \in \mathbb{Z}$
4. $\theta(r^n) = \theta(r)^n$ for all $n \in \mathbb{N} \cup \{0\}$
5. If $a \in R^*$ (the set of elements in R which have multiplicative inverses, such a is called a *unit* of R) then $\theta\left(a^k\right) = \theta(a)^k$ for all $k \in \mathbb{Z}$.

Definition 8.4.2

A *ring isomorphism* is a bijective homomorphism. If there exists an isomorphism between rings R and S, we say R and S are isomorphic, denoted $R \cong S$.

Exercise 8.4.1

Let $\theta : R \to S$ be a bijection of rings with $\theta(rr') = \theta(r)\theta(r')$ for all $r, r' \in R$. Write $\theta(1_R) = e$. Prove that $se = es = s$ for all $s \in S$ (hence condition 3 for a ring homomorphism can be omitted in this case).

Definition 8.4.3

Let $\theta : R \to S$ be a ring homomorphism. The *kernel* of θ is defined by

$$\ker \theta = \{r \in R \mid \theta(r) = 0\} \subseteq R$$

and the *image* of θ is defined by

$$\operatorname{im} \theta = \theta(R) = \{\theta(r) \mid r \in R\} \subseteq S$$

We have seen earlier that $\ker \theta$ and $\operatorname{im} \theta$ are additive subgroups of R and S respectively.

Proposition 8.9

Let $\theta : R \to S$ be a ring homomorphism. Then

1. $\operatorname{im} \theta$ is a subring of S
2. $\ker \theta$ is an ideal of R

Proof of 1: Since $\operatorname{im} \theta$ is an additive subgroup of S, it suffices to show that $\theta(R)$ is closed under multiplication, and $1_S \in \theta(R)$. Note that $1_S = \theta(1_R) \in \theta(R)$. Also if $s_1 = \theta(r_1)$ and $s_2 = \theta(r_2)$, then

$$s_1 s_2 = \theta(r_1)\theta(r_2) = \theta(r_1 r_2) \in \theta(R)$$

By the subring test, $\operatorname{im} \theta$ is a subring of S. □

Proof of 2: Since $\ker \theta$ is an additive subgroup of R, it suffices to show that $ra, ar \in \ker \theta$ for all $r \in R$, $a \in \ker \theta$. If $r \in R$ and $a \in \ker \theta$, then

$$\theta(ra) = \theta(r)\theta(a) = \theta(r) \cdot 0 = 0$$

Thus $ra \in \ker \theta$. Similarly, one can show $ar \in \ker \theta$. Thus $\ker \theta$ is an ideal of R. □

Theorem 8.10 **First Isomorphism Theorem**

Let $\theta : R \to S$ be a ring homomorphism. We have $R/\ker \theta \cong \operatorname{im} \theta$.

Proof: Let $A = \ker \theta$. Since A is an ideal of R, R/A is a ring. Define the map

$$\begin{aligned} \overline{\theta} : R/A &\longrightarrow \operatorname{im} \theta \\ r + A &\longmapsto \theta(r) \end{aligned}$$

Note that $r + A = s + A \iff r - s \in A \iff \theta(r - s) = 0 \iff \theta(r) = \theta(s)$. Thus $\overline{\theta}$ is well defined and injective. Also, $\overline{\theta}$ is clearly surjective. One can show that $\overline{\theta}$ is a homomorphism. It follows that $\overline{\theta}$ is a ring isomorphism and $\operatorname{im} \theta \cong R/\ker \theta$ □

Remark

Let A, B be subsets of a ring R. If A and B are both subrings, then $A \cap B$ is the largest subring of R contained in both A and B.

Notation

To consider the smallest subring of R containing both A and B (A, B not necessarily subrings), we define the *sum* $A + B$ to be

$$A + B = \{a + b \mid a \in A \text{ and } b \in B\}$$

One can show

Proposition 8.11

If R is a ring, then we have

1. If A, B are subrings of R (with $1_A = 1_B = 1_R$) then $A \cap B$ is a subring of R.
2. If A is a subring and B is an ideal of R, then $A + B$ is a subring of R
3. If A and B are ideals of R, then $A + B$ is an ideal of R.

Using the first isomorphism theorem, one can show (see A8)

Theorem 8.12 **Second Isomorphism Theorem**

Let A be a subring and B an ideal of a ring R. Then $A + B$ is a subring of R, B is an ideal of $A + B$, $A \cap B$ is an ideal of A and

$$(A + B)/B \cong A/(A \cap B)$$

Theorem 8.13 **Third Isomorphism Theorem**

Let A and B be ideals of a ring R with $A \subseteq B$. Then B/A is an ideal in R/A and

$$(R/A)/(B/A) \cong R/B$$

Corollary 8.14 **Correspondence Theorem / Fourth Isomorphism Theorem**

Let R be a ring and A an ideal. There exists a bijection between the set of ideals B of R that contains A and the set of ideals of R/A.

Example 8.4.3

Combining the third isomorphism theorem and the fact that all ideals of $\mathbb{Z}$ are principal, all ideals of $\mathbb{Z}_n$ are principal.

Theorem 8.15 **Chinese Remainder Theorem**

Let A, B be ideals of R

1. If $A + B = R$ then $R/(A \cap B) \cong R/A \times R/B$
2. If $A + B = R$ and $A \cap B = \{0\}$, then $R \cong R/A \times R/B$

Proof: (2) obviously follows from (1), so we prove (1). Define $\theta : R \to R/A \times R/B$ by $\theta(r) = (r + A, r + B)$. Then θ is a ring homomorphism with $\ker \theta = A \cap B$. To show θ is surjective, let $(s + A, t + B) \in R/A \times R/B$ with $s, t \in R$. Since $A + B = R$, there exists $a \in A$ and $b \in B$ such that $1 = a + b$. Let $r = sb + ta$. Then

$$s - r = s - sb - ta = s(1 - b) - ta = sa - ta = (s - t)a \in A$$

Thus $s + A = r + A$. Similarly, we have $t + B = r + B$. Thus $\theta(r) = (r + A, r + B) = (s + A, t + B)$. Thus $\operatorname{im} \theta = R/A \times R/B$. By the first isomorphism theorem, we have

$$R/(A \cap B) \cong R/A \times R/B$$

□

Example 8.4.4

Let $m, n \in \mathbb{N}$ with $\gcd(m, n) = 1$. By Bézout's Lemma, we have $1 = mr + ns$ for some $r, s \in \mathbb{Z}$. Thus $1 \in m\mathbb{Z} + n\mathbb{Z}$ and hence $m\mathbb{Z} + n\mathbb{Z} = \mathbb{Z}$. Also, since $\gcd(m, n) = 1$, we have $m\mathbb{Z} \cap n\mathbb{Z} = mn\mathbb{Z}$. By CRT,

Corollary 8.16

1. If $m, n \in \mathbb{N}$ with $\gcd(m, n) = 1$, then
$$\mathbb{Z}_{mn} \cong \mathbb{Z}_m \times \mathbb{Z}_n$$
2. If $m, n \in \mathbb{N}$ with $m, n \geq 2$ and $\gcd(m, n)$ $\varphi(mn) = \varphi(m)\varphi(n)$, where $\varphi(m) = |\mathbb{Z}_m^*|$ is the Euler φ-function

Proof of 2: From (1), we have
$$(\mathbb{Z}_{mn})^* \cong (\mathbb{Z}_m \times \mathbb{Z}_n)^* \cong \mathbb{Z}_m^* \times \mathbb{Z}_n^*$$
Since $|\mathbb{Z}_m^*| = \varphi(m)$, we have $\varphi(mn) = \varphi(m)\varphi(n)$ □

Remark

Let $m, n \in \mathbb{Z}$ with $\gcd(m, n) = 1$. For $a, b \in \mathbb{Z}$, by Cor 8.16 and the proof of Thm 8.15, for $[a] \in \mathbb{Z}_m$ and $[b] \in \mathbb{Z}_n$, there exists a unique $[c] \in \mathbb{Z}_{mn}$ such that $[c] = [a]$ in $\mathbb{Z}_m$ and $[c] = [b]$ in $\mathbb{Z}_n$. In other words, the simultaneous congruences $x \equiv a \pmod{m}$ and $x \equiv b \pmod{n}$ has a unique solution $x \equiv c \pmod{mn}$, which is CRT in Math 135.

Proposition 8.17

If R is a ring with $|R| = p$ a prime, then $R \cong \mathbb{Z}_p$.

Proof: Define $\theta : \mathbb{Z}_p \to R$ by $\theta[k] = k1_R$. Note that since R is an additive group and $|R| = p$, by Lagrange, $o(1_R) = 1$ or p. Since $1_R \neq 0$, we have $o(1_R) = p$. Thus
$$[k] = [m] \iff p \mid (k - m) \iff (k - m)1_R = 0 \iff k1_R = m1_R \text{ in } R$$
Thus θ is well-defined and injective. Since $|\mathbb{Z}_p| = p = |R|$ and θ is injective, θ is also surjective. Finally, once can prove that θ is a ring homomorphism. It follows that θ is a ring isomorphism and $R \cong \mathbb{Z}_p$. □

Exercise 8.4.2

What are the possible rings R with $|R| = p^2$ where p is a prime.

9 Commutative Rings

9.1 Integral Domains and Fields

Definition 9.1.1

Let R be a ring. We say $u \in R$ is a *unit* if u has a multiplicative inverse in R. Denoted by u^{-1}. We have $uu^{-1} = 1 = u^{-1}u$. Note that if u is a unit in R, and $r, s \in R$ we have
$$ur = us \implies s = s \quad \text{and} \quad ru = su \implies r = s$$
Let R^* denote the set of all units in R. One can show that $(R, \cdot)$ is group called the *group of units* of R.

Example 9.1.1

Note that 2 is a unit in $\mathbb{Q}$, but not a unit in $\mathbb{Z}$. We have $\mathbb{Q}^* = \mathbb{Q} \setminus \{0\}$ and $\mathbb{Z}^* = \{\pm 1\}$.

Exercise 9.1.1

Consider the ring of Gaussian integers $\mathbb{Z}[i]$. One can show $\mathbb{Z}[i]^* = \{\pm 1, \pm i\}$
Hint: Prove that $|xy| = |x||y|$ and $|x| = 1 \iff x$ is a unit.

Definition 9.1.2

A ring $R \neq \{0\}$ is a *division ring* if $R^* = R \setminus \{0\}$ i.e. every nonzero element of R is a unit of R. A commutative division ring is called a *field*.

Example 9.1.2

$\mathbb{Q}, \mathbb{R}, \mathbb{C}$ are fields, but $\mathbb{Z}$ is not a field.

Example 9.1.3

We recall that the equation $[a][x] = [1]$ in $\mathbb{Z}_n$ has a solution iff $\gcd(a, n) = 1$ for all $a \in \{1, 2, ..., p-1\}$. Thus $\mathbb{Z}_p^* = \mathbb{Z}_p \setminus \{0\}$ and $\mathbb{Z}_p$ is a field. However, if n is not prime, say $n = ab$ with $1 < a, b < n$. Then the nonzero congruence classes $[a], [b]$ are not units in $\mathbb{Z}_n$ as there is no solution for $[a][x] = [1]$ and hence $\mathbb{Z}_n^* \neq \mathbb{Z}_n \setminus \{0\}$. Thus $\mathbb{Z}_n$ is a field iff n is a prime.

Remark

If R is a division ring or a field, then its only ideals are $\{0\}$ or R since if $A \neq \{0\}$ is an ideal of R, then $0 \neq a \in A$ implies that $1 = aa^{-1} \in A$. By prop 8.5, $A = R$. As a consequence, if we have a ring homomorphism a field F to a ring S, since $\ker \theta$ is an ideal, $\ker \theta = \{0\}$ or F. Hence θ is either injective or the zero map.

Exercise 9.1.2

(This is quite hard) Prove that every finite division ring is a field.

Note

For $r, s \in \mathbb{R}$, we have $rs = 0$ implies that $r = 0$ or $s = 0$. This property is useful in solving equations, say if $x^2 - x - 6 = 0$ i.e. $(x-3)(x-2) = 0$, then $x = 3$ or $x = 2$. However, such property is not always true. For example, $[2][3] = [6] = [0]$ in $\mathbb{Z}_6$, but $[2] \neq [0]$ and $[3] \neq [0]$.

Exercise 9.1.3

Solve $[(x-2)(x-3)] = [0]$ in $\mathbb{Z}_6$.

Definition 9.1.3

Let $R \neq \{0\}$ be a ring. For $0 \neq a \in R$, we say a is a *zero divisor* if there exists $0 \neq b \in R$ such that $ab = 0$.

Example 9.1.4

In $\mathbb{Z}_6$, $[2], [3], [4]$ are zero divisors since $[2][3] = [0] = [4][3]$.

Example 9.1.5

Note that in $M_2(\mathbb{R})$, we have

$$\begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$$

Thus $\begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}$ is a zero divisor.

Proposition 9.1

Given a ring R, for all $a, b, c \in R$, the following are equivalent:

1. If $ab = 0$, then $a = 0$ or $b = 0$
2. If $ab = ac$ and $a \neq 0$, then $b = c$
3. If $ba = ca$ and $a \neq 0$, then $b = c$

Proof: We prove $(1) \iff (2)$ and the proof of $(1) \iff (3)$ is similar.
$(1) \implies (2)$: Let $ab = ac$ with $a \neq 0$. Then $a(b - c) = 0$. By (1), since $a \neq 0$, we have $b - c = 0$ i.e. $b = c$.
$(2) \implies (1)$: Let $ab = 0$ in R. Two cases:

1. If $a = 0$, then we are done
2. If $a \neq 0$, then $ab = 0 = a0$. By (2), since $a \neq 0$, we have $b = 0$.

□

Definition 9.1.4

A commutative ring $R \neq \{0\}$ is an *integral domain* if it has no zero divisors i.e. if $ab = 0$ in R, then $a = 0$ or $b = 0$.

Example 9.1.6

$\mathbb{Z}$ is an integral domain since for $a, b \in \mathbb{Z}$, $ab = 0$ implies $a = 0$ or $b = 0$.

Example 9.1.7

Note that if p is a prime, if $p \mid ab$ then $p \mid a$ or $p \mid b$ i.e. $[a][b] = [0]$ in $\mathbb{Z}_p$ implies that $[a] = [0]$ or $[b] = [0]$. Thus $\mathbb{Z}_p$ is an integral domain. However, if $n = ab$ with $1 < a, b < n$, then $[a][b] = [0]$ with $[a] \neq [0]$ and $[b] \neq [0]$. Thus $\mathbb{Z}_n$ is an integral domain iff n is a prime.

Proposition 9.2

Every field is an integral domain.

Proof: Let $ab = 0$ in a field R. We need to show that $a = 0$ or $b = 0$. Two cases:

1. If $a = 0$, then we are done
2. If $a \neq 0$, since R is a field, $a \in R^*$ and $a^{-1} \in R$ exists. Then

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

Thus R is an integral domain.

□

Remark

Using the above proof, one can show that every subring of a field is an integral domain.

Remark

The converse of Prop 9.2 is not true, for example, $\mathbb{Z}$ is an integral domain but not a field.

Example 9.1.8

The Gaussian integers $\mathbb{Z}[i]$ is an integral domain, but not a field.

Proposition 9.3

Every finite integral domain is a field.

Proof: Let R be a finite integral domain and $0 \neq a \in R$. Consider the map

$$\begin{aligned} \theta : R &\longrightarrow R \\ r &\longmapsto ar \end{aligned}$$

Since R is an integral domain, $ar = as$ and $a \neq 0$ implies that $r = s$. Hence θ is injective. Since R is finite, θ is surjective. In particular, there is $b \in R$ such that $ab = 1$. Since R is commutative, we have $ab = 1 = ba$, i.e. a is a unit. Hence $R^* = R \setminus \{0\}$ and R is a field. □

Recall

The characteristic of a ring R, denoted by $\mathrm{ch}(R)$ is the order of 1_R in $(R, +)$. We write $\mathrm{ch}(R) = 0$ if $o(1_R) = \infty$ and $\mathrm{ch}(R) = n$ if $o(1_R) = n \in \mathbb{N}$.

Proposition 9.4

The characteristic of any integral domain is either 0 or a prime p.

Proof: Let R be an integral domain. Two cases:

1. If $\mathrm{ch}(R) = \infty$, then we are done.
2. Note that since $R \neq \{0\}$, we have $n \neq 1$. If $\mathrm{ch}(R) = n \in \mathbb{N} \setminus \{1\}$, suppose that n is not prime, say $n = ab$ with $1 < a, b < n$. If 1 is the unity of R, then by Prop 8.1, we have

$$(a \cdot 1)(b \cdot 1) = (ab)(1 \cdot 1) = n \cdot 1 = 0$$

Since R is an integral domain, we have $a \cdot 1 = 0$ or $b \cdot 1 = 0$, which leads to a contradiction since $o(1) = n$. Thus n is prime.

□

Remark

Let R be an integral domain with $\mathrm{ch}(R) = p$, a prime. For $a, b \in R$, we have

$$(a + b)^p = a^p + \binom{p}{1} a^{p-1} b + \binom{p}{2} a^{p-2} b^2 + \cdots + \binom{p}{p-1} a b^{p-1} + b^p$$

Since p is a prime, $p \mid \binom{p}{i}$ for all $1 \leq i \leq (p-1)$. Since $\mathrm{ch}(R) = p$, we have

$$(a + b)^p = a^p + b^p$$

9.2 Prime Ideals and Maximal Ideals

Let p be a prime and $a, b \in \mathbb{Z}$. We recall from Math 135 that $p \mid ab$ implies $p \mid a$ or $p \mid b$. In other words, if $ab \in p\mathbb{Z}$, then $a \in p\mathbb{Z}$ or $b \in p\mathbb{Z}$.

Definition 9.2.1

Let R be a commutative ring. An ideal $P \neq R$ of R is a *prime ideal* if whenever $r, s \in R$ satisfy $rs \in P$, then $r \in P$ or $s \in P$.

Example 9.2.1

$\{0\}$ is prime ideal of $\mathbb{Z}$

Example 9.2.2

For $n \in \mathbb{N}$ with $n \geq 2$, $n\mathbb{Z}$ is a prime ideal of $\mathbb{Z}$ if and only if n is prime.

Proposition 9.5

If R is a commutative ring, then an ideal P of R is a prime ideal if and only if R/P is an integral domain.

Proof: Since R is a commutative ring, so is R/P. Note that

$$R/P \neq \{0\} \iff 0 + P \neq 1 + P \iff 1 \notin P \iff P \neq R.$$

Also, for $r, s \in R$, we have

$$\begin{aligned} P \text{ is a prime ideal} &\iff rs \in P \text{ implies that } r \in P \text{ or } s \in P \\ &\iff (r+P)(s+P) = 0 + P \text{ implies that} \\ &\quad\;\; r + P = 0 + P \text{ or } s + P = 0 + P \\ &\iff R/P \text{ is an integral domain} \end{aligned}$$

□

Definition 9.2.2

Let R be a commutative ring. An ideal $M \neq R$ of R is a *maximal ideal* if whenever A is an ideal such that $M \subseteq A \subseteq R$, then $A = M$ or $A = R$.

Remark

Let M be a maximal ideal of R and $r \notin M$. Then $M \subseteq \langle r \rangle + M \subseteq R$. Since $M \neq \langle r \rangle + M$, we have $\langle r \rangle + M = R$.

Proposition 9.6

If R is a commutative ring, then an ideal M of R is a maximal ideal if and only if R/M is a field.

Proof: Since R is a commutative ring, so is R/M. Note that

$$R/M \neq \{0\} \iff 0 + M \neq 1 + M \iff 1 \notin M \iff M \neq R$$

Also, for $r \in R$, note that $r \notin M$ iff $r + M \neq 0 + M$. Thus we have

$$\begin{aligned} & M \text{ is a maximal ideal} \\ \iff & \langle r \rangle + M = R \text{ for any } r \notin M \\ \iff & 1 \in \langle r \rangle + M \text{ for all } r \notin M \\ \iff & \forall r \notin M, \text{there exists } s \in R \text{ s.t. } 1 + M = rs + M \\ \iff & \forall r + M \neq 0 + M, \text{there exists } s + M \in R/M \text{ s.t. } (r+M)(s+M) = 1 + M \\ \iff & R/M \text{ is a field} \end{aligned}$$

□

Combining Prop 9.2, 9.5 and 9.6, we have

Corollary 9.7

Every maximal ideal of a commutative ring is a prime ideal.

Remark

The converse of Cor 9.7 is not true. For example, in $\mathbb{Z}$, $\{0\}$ is a prime ideal, but not a max ideal.

Example 9.2.3

Consider the ideal $\langle x^2+1\rangle$ in the ring $\mathbb{Z}[x]$. The map $\theta : \mathbb{Z}[x] \to \mathbb{Z}[i]$ defined by $\theta(f(x)) = f(i)$ is surjective since $\theta(a+bx) = a+bi$. Also, one can check that the kernel of the map is $\langle x^2+1\rangle$ (see Piazza). By the first isomorphism theorem, we have $\mathbb{Z}[x]/\langle x^2+1\rangle \cong \mathbb{Z}[i]$. Since $\mathbb{Z}[i]$ is an integral domain, but not a field, we conclude that the ideal $\langle x^2+1\rangle$ is prime, but not maximal. Note that $\langle x^2+1\rangle \subsetneq \langle x^2+1,3\rangle \subsetneq \mathbb{Z}[x]$. We have $\mathbb{Z}[x]/\langle x^2+1,3\rangle \cong \mathbb{Z}_3[x]/\langle x^2+1\rangle$ and x^2+1 is irreducible in $\mathbb{Z}_3[x]$.

9.3 Fields of Fractions

Let R be an integral domain. We now construct a field F of all *fractions* $\frac{r}{s}$ from R.
Let R be an integral domain and let $D = R \setminus \{0\}$. Consider the set $X = R \times D$. We say $(r,s) \equiv (r_1,s_1)$ on X iff $rs_1 = r_1 s$. One can show that $\equiv$ is an equivalence relation on X. Motivated by the case $R = \mathbb{Z}$, we now define the *fraction* $\frac{r}{s}$ to be the equivalence class $[(r,s)]$ of the pair (r,s) on X. Let F denote the set of all these fractions, i.e.

$$F = \left\{ \frac{r}{s} \;\middle|\; r \in R, s \in D \right\} = \left\{ \frac{r}{s} \;\middle|\; r,s \in R, s \neq 0 \right\}$$

The addition and multiplication of F are defined by

$$\frac{r}{s} + \frac{r_1}{s_1} = \frac{rs_1 + r_1 s}{ss_1} \quad \text{and} \quad \frac{r}{s} \cdot \frac{r_1}{s_1} = \frac{rr_1}{ss_1}$$

Note that $ss_1 \neq 0$ since R is an integral domain and thus these operations are well-defined. Then one can show that with the above defined addition and multiplication, F becomes a field with the zero being $\frac{0}{1}$, the unity $\frac{1}{1}$, the negative of $\frac{r}{s}$ is $\frac{-r}{s}$. Moreover, if $\frac{r}{s} \neq 0$ in F, then $r \neq 0$ and thus $\frac{s}{r} \in F$ and we have

$$\frac{r}{s} \cdot \frac{s}{r} = \frac{rs}{sr} = \frac{rs}{rs} = \frac{1}{1} \in F$$

In addition, we have $R \cong R'$ where $R' = \left\{ \frac{r}{1} \;\middle|\; r \in R \right\} \subseteq F$. Thus we have

Theorem 9.8

Let R be an integral domain. Then there exists a field F consisting of fractions $\frac{r}{s}$ with $r,s \in R$ and $s \neq 0$. By identifying $r = \frac{r}{1}$ for all $r \in R$, we can view R as a subring of F. The field F is called the *field of fractions of* R.

10 Polynomial Rings

10.1 Polynomials

Let R be a ring and x a variable. Let

$$R[x] = \{f(x) = a_0 + a_1x + \cdots + a_mx^m \mid m \in \mathbb{N} \cup \{0\} \text{ and } a_i \in R\ (0 \le i \le m)\}$$

Such $f(x)$ is called a *polynomial in x over R*. If $a_m \neq 0$, we say $f(x)$ has degree m, denoted by $\deg f = m$, and we say the a_m is *leading coefficient* of $f(x)$. If the leading coefficient $a_m = 1$, we say $f(x)$ is *monic*. If $\deg f = 0$, then $f(x) = a_0 \in R \setminus \{0\}$. In this case, we say $f(x)$ is a *constant polynomial*. Note that

$$f(x) = 0 \Longleftrightarrow a_0 = 0, a_1 = 0, \ldots$$

0 is also a constant polynomial and we define $\deg 0 = -\infty$. Let $f(x) = a_0 + a_1x + \cdots + a_mx^m \in R[x]$ and $g(x) = b_0 + b_1x + \cdots + b_bx^n \in R[x]$ with $m \le n$. Then we write $a_i = 0$ for all $m + 1 \le i \le n$. We can define addition and multiplication on $R[x]$ as follows:

$$f(x) + g(x) = (a_0 + b_0) + (a_1 + b_1)x + \cdots + (a_n + b_n)x^n$$

and

$$\begin{aligned} f(x)g(x) &= (a_0 + a_1x + \cdots + a_mx^m)(b_0 + b_1x + \cdots + b_nx^n) \\ &= a_0b_0 + (a_0b_1 + a_1b_0)x + (a_2b_0 + a_1b_1 + a_0b_2)x^2 + \cdots + (a_mb_n)x^{m+n} \\ &= c_0 + c_1x + c_2x^2 + \cdots + c_{m+n}x^{m+n} \end{aligned}$$

where

$$c_i = a_0b_i + a_1b_{i-1} + \cdots + a_{i-1}b_1 + a_ib_0$$

Proposition 10.1

Let R be a ring and x a variable

1. $R[x]$ is a ring
2. R is a subring of $R[x]$
3. If $Z = Z(R)$ is the center of R, then $Z(R[x]) = Z[x]$

Proof: (1) and (2) are left as exercises. □

Proof of 3: Let $f(x) = a_0 + a_1x + \cdots + a_mx^m \in Z[x]$ and $g(x) = b_0 + b_1x + \cdots + b_nx^n \in R[x]$. We have

$$f(x)g(x) = c_0 + c_1x + c_2x^2 + \cdots + c_{m+n}x^{m+n}$$

with

$$c_i = a_0b_i + a_1b_{i-1} + \cdots + a_{i-1}b_1 + a_ib_0$$

Since $a_i \in Z$, we have $a_ib_j = a_jb_i$ for all i, j. Thus we get $f(x)g(x) = g(x)f(x)$ for all $g(x) \in R[x]$ and hence $Z[x] \subseteq Z(R[x])$. To show the other inclusion, if $h(x) = c_0 + c_1x + \ldots + c_sx^s \in Z(R[x])$, then for all $r \in R$, we have $h(x)r = rh(x)$. Thus, $c_ir = rc_i$ for all $r \in R$ and $0 \le i \le s$. Thus, $c_i \in Z$ and $Z(R[x]) \subseteq Z[x]$. It follows that $Z(R[x]) = Z[x]$. □

Warning

Although $f(x) \in R[x]$ can be used to define a function from R to R, the polynomial is not the same as the function it defines. For example, if $R = \mathbb{Z}_2$, there are only 4 different functions from $\mathbb{Z}_2$ to $\mathbb{Z}_2$. However, the polynomial ring $\mathbb{Z}_2[x]$ is an infinite set.

Proposition 10.2

Let R be an integral domain. Then

1. $R[x]$ is an integral domain.
2. If $f \neq 0$ and $g \neq 0$ in $R[x]$, then
$$\deg(fg) = \deg(f) + \deg(g) \quad \text{(product formula)}$$
3. The units in $R[x]$ are R^*, the units in R.

Proof of 1,2: Suppose that $f(x) \neq 0$ and $g(x) \neq 0$ are polynomials in $R[x]$, say $f(x) = a_0 + a_1 x + \cdots + a_m x^m$ and $g(x) = b_0 + b_1 x + \cdots + b_n x^n$ with $a_m \neq 0$ and $a_n \neq 0$. Then

$$f(x)g(x) = (a_m b_n)x^{m+n} + \cdots + a_0 b_0$$

Since R is an integral domain, $a_m b_n \neq 0$ and thus $f(x)g(x) \neq 0$. It follows that $R[x]$ is an integral domain. Moreover,

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

Thus (1) and (2) follow. □

Proof of 3: Let $u(x) \in R[x]$ be a unit with inverse $v(x)$. Since $u(x)v(x) = 1$, by (2) we have

$$\deg(u) + \deg(v) = \deg 1 = 0$$

Since $u(x)v(x) = 1$, we have $u(x) \neq 0$ and $v(x) \neq 0$. Since $\deg u \geq 0$ and $\deg v \geq 0$, the above equation implies that $\deg u = 0 = \deg v$. Thus $u(x), v(x)$ are units in R and hence $R[x]^* \subseteq R^*$. Since $R^* \subseteq R[x]^*$, we have $R[x]^* = R^*$. □

Remark

Note that in $\mathbb{Z}_4[x]$, we have $2x \cdot 2x = 4x^2 = 0$ thus the product formula doesn't hold here since $\mathbb{Z}_4$ is not an integral domain.

Remark

To extend the product formula in Prop 10.2 to 0, we define $\deg 0 = \pm\infty$.

10.2 Polynomials Over a Field

Definition 10.2.1

Let F be a field and $f(x), g(x) \in F[x]$. We say $f(x)$ *divides* $g(x)$, denoted by $f(x) \mid g(x)$, if there exists $q(x) \in F[x]$ such that $g(x) = q(x)f(x)$.

Proposition 10.3

Let F be a field. $f(x), g(x), h(x) \in F[x]$.

1. If $f(x) \mid g(x)$ and $g(x) \mid h(x)$, then $f(x) \mid h(x)$. (transitivity of divisibility)
2. If $f(x) \mid g(x)$ and $f(x) \mid g(x)$, then $f(x) \mid (g(x)u(x) + h(x)v(x))$ for any $u(x), v(x) \in F[x]$ (divisibility of integer combinations)

Recall

For $a, b \in \mathbb{Z}$ if $a \mid b$ and $b \mid a$ and $a, b > 0$, then $a = b$. The following is its analogue in $F[x]$

Proposition 10.4

Let F be a field and $f(x), g(x) \in F[x]$ be monic polynomials. If $f(x) \mid g(x)$ and $g(x) \mid f(x)$, then $f(x) = g(x)$.

Proof: Since $f(x) \mid g(x)$ and $g(x) \mid f(x)$, we have $g(x) = r(x)f(x)$ and $f(x) = s(x)g(x)$ for some $r(x), s(x) \in F[x]$. Then $f(x) = s(x)r(x)f(x)$. By Prop 10.2, we have $\deg f = \deg s + \deg r + \deg f$, which implies that $\deg s = \deg r = 0$. Thus $f(x) = sg(x)$ for some $s \in F$. Since both $f(x)$ and $g(x)$ are monic, we have $s = 1$ and hence $f(x) = g(x)$. □

Proposition 10.5 **Division Algorithm**

Let F be a field and $f(x), g(x) \in F[x]$ with $f(x) \neq 0$. Then there exist unique $q(x), r(x) \in F[x]$ such that

$$g(x) = q(x)f(x) + r(x) \quad \text{with } \deg r < \deg f$$

Note that this includes the case for $r = 0$ (this explains why we define $\deg 0 = -\infty$).

Proof: We first prove by induction that such $q(x)$ and $r(x)$ exist. Write $m = \deg f$ and $n = \deg g$. If $n < m$, then $g(x) = 0 \cdot f(x) + g(x)$. Suppose $n \geq m$ and the result holds for all $g(x) \in F[x]$ with $\deg g < n$. Write $f(x) = a_0 + a_1 x + \cdots + a_m x^m$ with $a_m \neq 0$ and $g(x) = b_0 + b_1 x + \cdots + b_n x^n$. Since F is a field, a_m^{-1} exists. Consider

$$\begin{aligned} g_1(x) &= g(x) - b_n a_m^{-1} x^{n-m} f(x) \\ &= (b_n x^n + b_{n-1} x^{n-1} + \cdots + b_0) - b_n a_m^{-1} x^{n-m} (a_m x^m + \cdots + a_1 x + a_0) \\ &= 0 \cdot x^n + (b_{n-1} - b_n a_m^{-1} a_{m-1}) x^{n-1} + \cdots \end{aligned}$$

Since $\deg g_1 < n$, by induction, there exist $q_1(x), r_1(x) \in F[x]$ such that $g_1(x) = q_1(x)f(x) + r_1(x)$ with $\deg r_1 < \deg f$. It follows that

$$\begin{aligned} g(x) &= q_1(x) + b_n a_m^{-1} x^{n-m} f(x) \\ &= (q_1(x)f(x) + r_1(x)) + b_n a_m^{-1} x^{n-m} f(x) \\ &= (q_1(x) + b_n a_m^{-1} x^{n-m}) f(x) + r_1(x) \end{aligned}$$

By taking $q(x) = q_1(x) + b_n a_m^{-1} x^{n-m}$ and $r(x) = r_1(x)$, we have

$$g(x) = q(x)f(x) + r(x) \quad \text{with } \deg r < \deg f$$

To prove uniqueness, suppose that we have $g(x) = q_1(x)f(x) + r_1(x)$ with $\deg r_1 < \deg f$. Then

$$r(x) - r_1(x) = (q_1(x) - q(x))f(x).$$

If $q_1(x) - q(x) \neq 0$, we get

$$\deg(r - r_1) = \deg((q_1 - q)f) = \deg(q_1 - q) + \deg f \geq \deg f$$

which leads to a contradiction since $\deg(r - r_1) < \deg f$. Thus $q_1(x) - q(x) = 0$ and hence $r(x) - r_1(x) = 0$. It follows that $q_1(x) = q(x)$ and $r_1(x) = r(x)$. □

Note

For $a, b \in \mathbb{Z} \setminus \{0\}$, the Bézout Lemma states that $\gcd(a, b) = ax + by$ for some $x, y \in \mathbb{Z}$.

Proposition 10.6

Let F be a field and $f(x), g(x) \in F[x] \setminus \{0\}$. Then there exists $d(x) \in F[x]$ which satisfies the following conditions:

1. $d(x)$ is monic
2. $d(x) \mid f(x)$ and $d(x) \mid g(x)$
3. If $e(x) \mid f(x)$ and $e(x) \mid g(x)$, then $e(x) \mid d(x)$
4. $d(x) = u(x)f(x) + v(x)g(x)$ for some $u(x), v(x) \in F[x]$

Note that if both $d(x)$ and $d_1(x)$ satisfy the above conditions, since $d(x) \mid d_1(x)$ and $d_1(x) \mid d(x)$ and both of them are monic, By prop 10.4, we have $d(x) = d_1(x)$. We call such $d(x)$ the greatest common divisor of $f(x)$ and $g(x)$ denote it by $d(x) = \gcd(f(x), g(x))$

Proof: Consider the set $X = \{u(x)f(x) + v(x)g(x), u(x), v(x) \in F[x]\}$. Since $f(x) \in X$, the set X contains nonzero polynomials and thus monic polynomials (since F is a field, if $h(x) \in X$ with leading coefficient a, then $a^{-1}h(x) \in X$ is monic). Among all monic polynomials in X, choose $d(x) = u(x)f(x) + v(x)g(x)$ of minimal degree. Then (1) and (4) are satisfied. For (3), if $e(x) \mid f(x)$ and $e(x) \mid g(x)$, since $d(x) = u(x)f(x) + v(x)g(x)$ by prop 10.3, $e(x) \mid d(x)$. It remains to prove (2). By the division algorithm, write $f(x) = q(x)d(x) + r(x)$ with $\deg r < \deg d$. Then

$$\begin{aligned} r(x) &= f(x) - q(x)d(x) \\ &= f(x) - q(x)(u(x)f(x) + v(x)g(x)) \\ &= (1 - q(x)u(x))f(x) - (q(x)v(x))g(x) \end{aligned}$$

Note that if $r(x) \neq 0$, write $c \neq 0$ be the leading coefficient of $r(x)$. Since F is a field, c^{-1} exists. The above expression shows that $c^{-1}r(x)$ is a monic polynomial of X with $\deg(c^{-1}r) = \deg r < \deg d$, which contradicts the choice of $d(x)$. Thus $r(x) = 0$ and we have $d(x) \mid f(x)$. Similarly, we can show $d(x) \mid g(x)$. Thus (2) follows. □

Recall

$p \in \mathbb{Z}$ is a prime if $p \geq 2$ and whenever $p = ab$ with $a, b \in \mathbb{Z}$, then $a = \pm 1$ or $b = \pm 1$ (note that ± 1 are the units of $\mathbb{Z}$).

Definition 10.2.2

If F is a field, a polynomial $\ell(x) \neq 0$ in $F[x]$ is *irreducible* if $\deg \ell \geq 1$ and whenever $\ell(x) = \ell_1(x)\ell_2(x)$ in $F[x]$, we have $\deg \ell_1 = 0$ or $\deg \ell_2 = 0$ ($\deg 0$ polynomials are the units in $F[x]$). Polynomials that are note irreducible are *reducible*.

Example 10.2.1

If $\ell(x) \in F[x]$ satisfies $\deg \ell = 1$, then $\ell(x)$ is irreducible.

Exercise 10.2.1

One can show that if $\deg f \in \{2, 3\}$, then f is irreducible iff $f(d) \neq 0$ for all $d \in F$.

Example 10.2.2

Let $\ell(x), f(x) \in F[x]$. If $\ell(x)$ is irreducible and $\ell(x) \nmid f(x)$ then $\gcd(\ell(x), f(x)) = 1$

Recall

Given a prime $p \in \mathbb{Z}$ and $a, b \in \mathbb{Z}$, Euclid's Lemma states that if $p \mid ab$ then $p \mid a$ or $p \mid b$.

Proposition 10.7

Let F be a field and $f(x), g(x) \in F[x]$. If $\ell(x) \in F[x]$ is irreducible and $\ell \mid f(x)g(x)$, then $\ell(x) \mid f(x)$ or $\ell(x) \mid g(x)$.

Proof: Suppose $\ell(x) \mid f(x)g(x)$. Two cases:

1. If $\ell(x) \mid f(x)$ then we are done.
2. If $\ell(x) \nmid f(x)$, then $d(x) = \gcd(\ell(x), f(x)) = 1$. By Prop 10.6, we have

$$1 = \ell(x)u(x) + f(x)v(x) \quad \text{for some } u(x), v(x) \in F[x]$$

Then

$$g(x) = g(x)\ell(x)u(x) + g(x)f(x)v(x)$$

Since $\ell(x) \mid \ell(x)$ and $\ell(x) \mid f(x)g(x)$, By prop 10.3, we have $\ell(x) \mid g(x)$.

$\square$

Remark

Let $f_1(x), ..., f_n(x) \in F[x]$ and let $\ell(x) \in F[x]$ be irreducible. If $\ell(x) \mid f_1(x) \cdots f_n(x)$, by applying Prop 10.7 repeatedly, we get $\ell(x) \mid f_i(x)$ for some i.

Recall

For an integer $n \in \mathbb{Z}$ with $|n| \geq 2$, up to ± 1 sign, n can be written uniquely as a product of primes. By induction and Prop 10.7, we have the following analogous result in $F[x]$.

Theorem 10.8 **Unique Factorization Theorem**

Let F be a field and $f(x) \in F[x]$ with $\deg f \geq 1$. Then we can write $f(x) = c\ell_1(x) \cdots \ell_m(x)$ where $c \in F^*$ and $\ell_i(x)$ are monic, irreducible polynomials (not necessarily distinct.) The formulation is unique up to the order of ℓ_i.

Exercise 10.2.2

Use Theorem 10.8 to prove there are infinitely many irreducible polynomials in $F[x]$.

Recall

In $\mathbb{Z}$, all ideals are of the form $\langle n \rangle = n\mathbb{Z}$ and if $n \in \mathbb{N}$, then n is uniquely determined.

Proposition 10.9

Let F be a field. Then all ideals of $F[x]$ are of the form $\langle h(x) \rangle = h(x)F[x]$ for some $h(x) \in F[x]$. If $\langle h(x) \rangle \neq 0$ and $h(x)$ is monic, then the generator is uniquely determined.

Proof: Let A be an ideal of $F[x]$. If $A = \{0\}$, then $A = \langle 0 \rangle$. If $A \neq \{0\}$, then it contains a monic polynomial (since F is a field, if $f \in A$ with leading coefficient a, then $a^{-1}f \in A$). Among all monic polynomials in A, choose $h(x) \in A$ of minimum degree. Then $\langle h(x) \rangle \subseteq A$. To prove the other inclusion, let $f(x) \in A$. By the division algorithm, we have $f(x) = q(x)h(x) + r(x)$ with $q(x), r(x) \in F[x]$ and $\deg r < \deg h$. If $r(x) \neq 0$, let $u \neq 0$ be its leading coefficient. Since A is an ideal and $f(x), h(x) \in A$ we have $u^{-1}r(x) = u^{-1}(f(x) - q(x)h(x)) = u^{-1}f(x) - u^{-1}q(x)h(x) \in A$ which is a monic polynomial in A with $\deg(u^{-1}r) < \deg h$. This contradicts the minimum property of $\deg h$. Thus $r(x) = 0$ and $f(x) = q(x)h(x)$. It follows that $f(x) \in \langle h(x) \rangle$ and hence $A = \langle h(x) \rangle$. To prove uniqueness, suppose $A = \langle h(x) \rangle = \langle h_1(x) \rangle$. Since $h(x) \mid h_1(x)$ and $h_1(x) \mid h(x)$ and both of them are monic, my Prop 10.4, we have $h(x) = h_1(x)$. $\square$

Recall

We have seen in $\mathbb{Z}$ that all ideals are of the form $\langle n \rangle$ for some $n \in \mathbb{Z}$. For $n \geq 2$, if we divide an integer by n, the remainder $r \in \{0, 1, ..., n-1\}$. Write $\langle n \rangle = n\mathbb{Z}$. Then we have

$$\mathbb{Z}_n = \mathbb{Z}/\langle n \rangle = \{0 + \langle n \rangle, ..., (n-1) + \langle n \rangle\} = \{[0], ..., [n-1]\}$$

We now consider its analogue in $F[x]$. Let F be a field. By Prop 10.9, all ideals of $F[x]$ are of the form $\langle h(x)\rangle$. Suppose that $h(x)$ is monic and $\deg h = m \geq 1$. Consider the quotient ring $R = F[x]/\langle h(x)\rangle$ and thus

$$R = \left\{\overline{f(x)} := f(x) + \langle h(x)\rangle \;\middle|\; f(x) \in F[x]\right\}$$

Write $t = \overline{x} = x + \langle h(x)\rangle$. We have $h(t) = 0$ in R (exercise). By the division algorithm, we can write $f(x) = q(x)h(x) + r(x)$ with $\deg r < \deg h = m$. Thus one can show that

$$R = \left\{\overline{a_0} + \overline{a_1}t + \cdots + \overline{a_{m-1}}t^{m-1} \;\middle|\; a_i \in F \text{ and } h(t) = 0\right\}$$

Consider the map $\theta : F \to R$ given by $\theta(a) = \overline{a}$. Since θ is not the zero map and $\ker\theta$ is an ideal of F, we have $\ker\theta = \{0\}$. Thus θ is an injective ring homomorphism. Since $F \cong \theta(F)$, by identifying F with $\theta(F)$, we have

$$R = \left\{a_0 + a_1 t + \cdots + a_{m-1}t^{m-1} \;\middle|\; a_i \in F \text{ and } h(t) = 0\right\}$$

Note that in R we have

$$a_0 + a_1 t + \cdots + a_{m-1}t^{m-1} = b_0 + b_1 t + \cdots + b_{m-1}t^{m-1} \iff a_i = b_i \ (\forall\ 0 \leq i \leq m-1)$$

Hence this representation of the elements in R is unique.

Proposition 10.10

Let F be a field and $h(x) \in F[x]$ be monic with $\deg h = m \geq 1$. Then the quotient ring $R = F[x]/\langle h(x)\rangle$ is given by

$$R = \left\{a_0 + a_1 t + \cdots + a_{m-1}t^{m-1} \;\middle|\; a_i \in F \text{ and } h(t) = 0\right\}$$

in which an element of R can be uniquely represented by the above form.

Example 10.2.3

Consider the ring $\mathbb{R}[x]$. Let $h(x) = x^2 + 1 \in \mathbb{R}[x]$. By Prop 10.10, we have

$$\mathbb{R}[x]/\langle x^2+1\rangle = \left\{a + bt \;\middle|\; a, b \in \mathbb{R} \text{ and } t^2 + 1 = 0\right\} \cong \mathbb{C}$$

Proposition 10.11

Let F be a field and $h(x) \in F[x]$ with $\deg h \geq 1$. The following are equivalent:

1. $F[x]/\langle h(x)\rangle$ is a field.
2. $F[x]/\langle h(x)\rangle$ is a integral domain.
3. $h(x)$ is irreducible in $F[x]$

Proof: Write $A = \langle h(x)\rangle$
$(1 \implies 2)$ Every field is an integral domain.
$(2 \implies 3)$ If $h(x) = f(x)g(x)$ with $f(x), g(x) \in F[x]$, then

$$(f(x) + A)(g(x) + A) = f(x)g(x) + A = h(x) + A = 0 + A \text{ in } F[x]/A$$

By (2), either $f(x) + A = 0 + A$ or $g(x) + A = 0 + A$, i.e. either $f(x) \in A$ or $g(x) \in A$. If $f(x) \in A = \langle h(x) \rangle$, then $f(x) = q(x)h(x)$ for some $q(x) \in F[x]$. Thus $h(x) = f(x)g(x) = q(x)h(x)g(x)$. Since $F[x]$ is an integral domain, this implies that $q(x)h(x) = 1$, which implies that $\deg g = 0$. Similarly, if $g(x) \in A$, then $\deg f = 0$. Thus $h(x)$ is irreducible in $F[x]$.
($3 \Longrightarrow 1$) Note that $F[x]/A$ is a commutative ring. Thus to show that it is a field, it suffices to show that every nonzero element of $F[x]/A$ has an inverse. Let $f(x) + A \neq 0 + A$ with $f(x) \in F[x]$. Then $f(x) \notin A$ and hence $h(x) \nmid f(x)$. Since $h(x)$ is irreducible and $h(x) \nmid f(x)$, we have $\gcd(f(x), h(x)) = 1$. By Prop 10.6, there exist $u(x), v(x) \in F[x]$ such that $1 = u(x)h(x) + v(x)f(x)$. Thus $(v(x) + A)(f(x) + A) = 1 + A$ (since $h(x) \in A$). It follows that $f(x) + A$ has an inverse in $F[x]/A$ and hence $F[x]/A$ is a field. □

Example 10.2.4

Since $\mathbb{R}[x]/\langle x^2 + 1 \rangle \cong \mathbb{C}$, which is a field, the polynomial $x^2 + 1$ is irreducible in $\mathbb{R}[x]$.

Example 10.2.5

Since $x^2 + x + 1$ has no root in $\mathbb{Z}_2$ (since 0 and 1 are not roots), it is irreducible in $\mathbb{Z}_2[x]$. Thus $\mathbb{Z}_2[x]/\langle x^2 + x + 1 \rangle = \{a + bt \mid a, b \in \mathbb{Z}_2 \text{ and } t^2 + t + 1 = 0\}$ is a field of 4 elements.

Remark

Before the previous example, the only finite fields we know are of the form $\mathbb{Z}_p$ where p is a prime. We have seen before that there are infinitely many irreducible polynomials in $\mathbb{Z}_p[x]$. One can show that for any $n \in \mathbb{N}$, there exists at least one irreducible polynomial of degree n in $\mathbb{Z}_p[x]$, say $f_n(x)$. Since $f_n(x)$ is irreducible, $\mathbb{Z}_p[x]/\langle f_n(x) \rangle$ is a field of order p^n. Note that $\mathbb{Z}_{p^n}$ is NOT a field if $n \geq 2$.

Analogies Between $\mathbb{Z}$ and $F[x]$

	$\mathbb{Z}$	$F[x]$
elements	m	$f(x)$
size	$\|m\| = \text{absolute value}$	$\deg f$
units	$\pm 1; \mathbb{Z} \setminus \{0\}/\{\pm 1\}" = "\mathbb{N}$	$F^*; F[x] \setminus \{0\}/F^*" = "\{\text{monic polynomials}\}$
unique factorization	$m = \pm 1 p_1^{\alpha_1} \cdots p_n^{\alpha_n}, p_i$ prime	$f = c\ell_1^{\alpha_1} \cdots \ell_r^{\alpha_r}, c \in F^*, \ell_i = \ell_i(t) =$ monic, irreducible
ideals	$\langle n \rangle$(unique if $n \in \mathbb{N}$)	$\langle h(x) \rangle$ (unique if $h(x)$ monic)
ideals	$\mathbb{Z}/\langle n \rangle$ is a field iff n is a prime	$F[x]/\langle h(x) \rangle$ is a field iff $h(x)$ is irreducible