Contents

1 Groups

1.1 Notation

1. $\mathbb{N} = \{1, 2, 3, ...\}$
2. $\mathbb{Z} = \{..., -2, -1, 0, 1, 2, ...\}$
3. $\mathbb{Q} = \left\{\frac{a}{b} : a, b \in \mathbb{N}\right\}$
4. $\mathbb{R} =$ the set of real numbers
5. $\mathbb{C} = \{a + bi : a, b \in \mathbb{R}\}$
6. For $n \in \mathbb{N}$, $\mathbb{Z}_n = \{[0], [1], ..., [n-1]\}$, where congruence class $[r] = \{z \in \mathbb{Z} : z \equiv r \bmod n\}$ for $0 \leq r \leq n-1$.
7. 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 $A = [a_{i,j}] = \begin{bmatrix} a_{1,1} & \cdots & a_{1,n} \\ \vdots & \ddots & \vdots \\ a_{m,1} & \cdots & a_{m,n} \end{bmatrix}$
8. $M_n(\mathbb{R}) =$ the set of $n \times n$ matrices over $\mathbb{R}$ with the usual addition and multiplication

1.2 Groups

Definition 1.2.1

G set, $\star$ operation on $G \times G$. (G, $\star$) is a group if it satisfies the following:

1. $\star$ is associative (if $a, b, c \in G$, then $a \star (b \star c) = (a \star b) \star c$)
2. There exists an (identity) element $e \in G$ such that $a * e = a = e * a$ for all $a \in G$
3. For each $a \in G$, there exists an inverse $a^{-1} \in G$ such that $a * a^{-1} = e = a^{-1} * a$

Definition 1.2.2

A group G is said to be abelian if it is commutative.

Exercise 1.2.1

Prove that in the definition of a group, it suffices to assume only that $e \star a = a$ in (3) and $a^{-1} \star a = e$ in (4).

Proposition 1.1

Let G be a group as defined in the previous exercise. Then $a \star e = a$ and $a \star a^{-1} = e$.

***Proof*:**

$$\begin{aligned} e &= e \star e \\ &= (a^{-1} \star a) \star (a^{-1} \star a) \\ \implies a \star e \star a^{-1} &= a \star (a^{-1} \star a) \star (a^{-1} \star a) \star a^{-1} \\ \implies a \star a^{-1} &= (a \star a^{-1})^3 \\ \implies e \star (a \star a^{-1}) &= (a \star a^{-1})^2 \star (a \star a^{-1}) \\ \implies e &= (a \star a^{-1}) \star (a \star a^{-1}) \\ \implies e &= a \star a^{-1} \\ \implies a \star e &= a \star (a^{-1} \star a) \\ &= (a \star a^{-1}) \star a \\ &= e \star a \end{aligned}$$

□

Proposition 1.2

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

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

***Proof*:**

1. Let e_1, e_2 be identities. Since e_2 is a right identity and e_1 is a left identity, then $e_1 = e_1 \star e_2 = e_2$.
2. Let a_1, a_2 be inverses of a. Then $a_1 = e \star a_1 = (a_2 \star a) \star a_1 = a_2 \star (a \star a_1) = a_2 \star e = a_2$.

□

Example

The sets $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$, $(\mathbb{C}, +)$ are abelian groups, where the additive identity is 0 and the additive inverse of r is $-r$.
Note that $(\mathbb{N}, +)$ is not a group, since it has no identity.

Example

The sets $(\mathbb{Q}, \cdot)$, $(\mathbb{R}, \cdot)$ and $(\mathbb{C}, \cdot)$ are not groups as 0 has no multiplicative inverse in $\mathbb{Q}$, $\mathbb{R}$ or $\mathbb{C}$.

Example

For set $S = (S, \cdot)$, let $S^\star$ denote the subset of S containing all elements with multiplicative inverses.
For example, $\mathbb{Q}^\star = Q \setminus \{0\}$. Then $(\mathbb{Q}^\star, \cdot)$, $(\mathbb{R}^\star, \cdot)$ and $(\mathbb{C}^\star, \cdot)$ are abelian groups, where the multiplicative identity is 1 and the multiplicative inverse of r is $-\frac{1}{r}$.

Exercise 1.2.2

What is $\mathbb{Z}_n^\star$?

Solution:
$\mathbb{Z}_n^* = \{[k] : \gcd(k, n) = 1\}$

Example

The set $M_n(\mathbb{R})$ is an abelian group where the additive identity is the zero matrix and the additive inverse of A is $-A$.

Example

Consider $(M_n(\mathbb{R}), \cdot)$. The identity matrix is $I \in M_n(\mathbb{R})$.
However, since not all $M \in M_n(\mathbb{R})$ has a multiplicative inverse, $(M_n(\mathbb{R}), \cdot)$ is not a group.

Definition 1.2.3

Define the set $GL_n(\mathbb{R}) = \{M \in M_n(\mathbb{R}) : \det(M) \neq 0\}$.

Note

If $A, B \in GL_n(\mathbb{R})$, then $\det(A) \cdot \det(B) \neq 0$ and thus $AB \in GL_n(\mathbb{R})$. The associativity of $GL_n(\mathbb{R})$ inherits from $M_n(\mathbb{R})$'s associativity. Also, the identity matrix I satisfies $\det(I) = 1 \neq 0$ and thus $I \in GL_n(\mathbb{R})$. Finally, for $M \in GL_n(\mathbb{R})$, 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 $M^{-1} \in GL_n(\mathbb{R})$. Thus $(GL_n(\mathbb{R}), \cdot)$ is a group.

Definition 1.2.4

$(GL_n(\mathbb{R}), \cdot)$ is called the general linear group of degree n over $\mathbb{R}$.

Note

If $n \geq 2$, the group $(GL_n(\mathbb{R}), \cdot)$ is not abelian.

Exercise 1.2.3

What is $(GL_1(\mathbb{R}), \cdot)$?

Solution:
$(GL_1(\mathbb{R}), \cdot) \cong (\mathbb{R} \setminus \{0\}, \cdot)$

Example

Let G and H be groups. Then the direct product is the set $G \times H$ with the component-wise operation defined by $(g_1, h_1) \star (g_2, h_2) = (g_1 \star_G g_2, h_1 \star_H h_2)$. One can check that $G \times H$ is a group with the identity (e_G, e_H) and the inverse of (g, h) is (g^{-1}, h^{-1}).

Note

One can show by induction that if $G_1, G_2, ...G_n$ are groups, then $G_1 \times G_2 \times ... \times G_n$ 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 the identity by 1.
Also, the unique inverse of an element $g \in G$ is denoted by g^{-1}.
For $n \in \mathbb{N}$, we define $g^n = g \star g \star ... \star g$ (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. $g^n g^m = g^{n+m} \forall n, m \in \mathbb{Z}$
4. $(g^n)^m = g^{nm} \forall n, m \in \mathbb{Z}$

Proof:

1. Since $g^{-1}g = 1 = gg^{-1}$, then $(g^{-1})^{-1} = g$.
2. $(gh)(h^{-1}g^{-1}) = g(hh^{-1})g^{-1} = g1g^{-1} = gg^{-1} = 1$ Similarly, $(h^{-1}g^{-1})(gh) = 1$. Thus, $(gh)^{-1} = h^{-1}g^{-1}$.

□

Exercise 1.2.4

Prove (3) and (4) from the previous proposition.

Remark

In general, it is not true 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 $g, h, f \in G$. The following are true:

1. They satisfy 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: (1.a): By left-multiplying by g^{-1}, we have

$$\begin{aligned} gh &= gf \\ \Rightarrow g^{-1}(gh) &= g^{-1}(gf) \\ \Rightarrow h &= f \end{aligned}$$

The proof of (1.b) is similar.
(2): Let $x = a^{-1}b$. Then $ax = a(a^{-1}b) = (aa^{-1})b = 1b = b$.
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

Consider the set $L = \{1, 2, 3\}$, which has the following different permutations: $\binom{123}{123}$, $\binom{123}{132}$ (it indicates the bijection $\sigma : \{1, 2, 3\} \to \{1, 2, 3\}$ with $\sigma(1) = 1, \sigma(2) = 3, \sigma(3) = 2$.

Notation

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

Proposition 1.5

We have $|S_n| = n!$

Note

On Mobius Quiz, use "nine dots" to format a permutation.

Given $\sigma, \tau \in S_n$, we can compose them to get a third element $\sigma\tau$, where $\sigma\tau : \{1, 2, ..., n\} \longrightarrow \{1, 2, ..., n\}$ given by $x \mapsto \sigma(\tau(x)) \forall x \in \{1, 2, ..., n\}$. Since both σ, τ are bijections, so is $\sigma\tau$. Thus $\sigma\tau \in S_n$.

Example

Compute $\sigma\tau$ and $\tau\sigma$ if $\sigma = \left(\begin{smallmatrix}1&2&3&4\\3&4&1&2\end{smallmatrix}\right)$ and $\tau = \left(\begin{smallmatrix}1&2&3&4\\2&4&3&1\end{smallmatrix}\right)$
We note that $\sigma\tau \neq \tau\sigma$. For any $\sigma, \tau \in S_n$, we have $\sigma\tau, \tau\sigma \in S_n$, but $\sigma\tau \neq \tau\sigma$ in general. On the other hand, for $\sigma, \tau, \mu \in S_n$, we have that $\sigma(\tau\mu) = (\sigma\tau)\mu$.
Also, the identity permutation $\varepsilon \in S_n$ is defined as

$$\varepsilon = \begin{pmatrix} 1 & 2 & ... & n \\ 1 & 2 & ... & n \end{pmatrix}$$

Then for any $\sigma \in S_n$, we have $\sigma\varepsilon = \sigma = \varepsilon\sigma$.
Finally, for $\sigma \in S_n$, since it is a bijection, there exists a unique bijection σ^{-1}, called the inverse permutation of σ, such that for all $x, y \in \{1, 2, ..., n\}$, $\sigma^{-1}(x) = y$ iff $\sigma(y) = x$. It follows that $\sigma(\sigma^{-1}(x)) = x$ and $\sigma^{-1}(\sigma(y)) = y$.
So we have $\sigma\sigma^{-1} = \varepsilon = \sigma^{-1}\sigma$.
For example, find the inverse of $\sigma = \left(\begin{smallmatrix}1&2&3&4&5\\4&5&1&2&3\end{smallmatrix}\right)$.
Note that $\sigma(1) = 4$. Thus $\sigma^{-1}(4) = 1$. Compute the rest similarly.
We have $\sigma^{-1} = \left(\begin{smallmatrix}1&2&3&4&5\\3&4&5&1&2\end{smallmatrix}\right)$.

Proposition 1.6

S_n is a group under function composition, called the symmetric group of degree n.

Proof: Above example. □

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.

Solution:
$e \in S_3$ corresponds to no rotations nor reflections. $s_1 = \left(\begin{smallmatrix}1&2&3\\2&1&3\end{smallmatrix}\right), s_2 = \left(\begin{smallmatrix}1&2&3\\1&3&2\end{smallmatrix}\right)$ and $s_3 = \left(\begin{smallmatrix}1&2&3\\3&2&1\end{smallmatrix}\right)$ correspond to reflections across the 3 angle bisectors. $s_4 = \left(\begin{smallmatrix}1&2&3\\3&1&2\end{smallmatrix}\right)$ and $s_5 = \left(\begin{smallmatrix}1&2&3\\2&3&1\end{smallmatrix}\right)$ correspond to rotations of $\frac{2}{3}\pi$ radians clockwise and counter-clockwise.

Example

Consider

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 3 & 1 & 7 & 6 & 9 & 4 & 2 & 5 & 8 & 10 \end{pmatrix} \in S_{10}$$

We note the following cycles

$$1 \to 3 \to 7 \to 2 \to 1$$

$$4 \to 6 \to 4$$

$$5 \to 9 \to 8 \to 5$$

$$10 \to 10$$

.

Thus, σ can be decomposed into one 4-cycle (1 3 7 2), one 2-cycle (4 6) and one 3-cycle (5 9 8) and one 1-cycle (10). Note that these cycles are pointwise disjoint and we have $\sigma = (1372)(46)(598)$.

Notation

$$(1372) = \begin{pmatrix} \mathbf{1} & \mathbf{2} & \mathbf{3} & 4 & 5 & 6 & \mathbf{7} & 8 & 9 & 10 \\ \mathbf{3} & \mathbf{1} & \mathbf{7} & 4 & 5 & 6 & \mathbf{2} & 8 & 9 & 10 \end{pmatrix}$$

$$(46) = \begin{pmatrix} 1 & 2 & 3 & \mathbf{4} & 5 & \mathbf{6} & 7 & 8 & 9 & 10 \\ 1 & 2 & 3 & \mathbf{6} & 5 & \mathbf{4} & 7 & 8 & 9 & 10 \end{pmatrix}$$

$$(598) = \begin{pmatrix} 1 & 2 & 3 & 4 & \mathbf{5} & 6 & 7 & \mathbf{8} & \mathbf{9} & 10 \\ 1 & 2 & 3 & 4 & \mathbf{9} & 6 & 7 & \mathbf{5} & \mathbf{8} & 10 \end{pmatrix}$$

$$(10) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & \mathbf{10} \\ 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & \mathbf{10} \end{pmatrix}$$

Note

1. We do not usually write 1-cycles explicitly.
2. We can also write $\sigma = (46)(598)(1372) = (64)(985)(7213)$.

Theorem 1.7 **Cycle Decomposition Theorem**

If $\sigma \in S_n$ 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: Let $\sigma \in S_n$ be arbitrary. Pick $i_1 \in \{1, \ldots, n\}$ arbitrarily. Since σ is a surjection, then there exists $i \in \{1, \ldots, n\}$ such that $\sigma(i) = i_1$. Then there exists a $1 \leq k \leq n$ such that $\sigma^k(i) = i$ □

Notation

Every permutation in S_n can be regarded as a permutation in S_{n+1} by fixing the number (n+1). Thus, $S_1 \subseteq S_2 \subseteq ... \subseteq S_n \subseteq S_{n+1} \subseteq ...$

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 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

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

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

Example

Consider the group $\mathbb{Z}^* = \{1, -1\}$ under multiplication. 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], then the Cayley tables of Z^* and $\mathbb{Z}_2$ become the same. In this case, we say $\mathbb{Z}^*$ and $\mathbb{Z}_2$ are isomporphic, denoted by $\mathbb{Z}^* \cong \mathbb{Z}_2$.

Definition 1.4.2

For $n \in \mathbb{N}$, the cyclic group of order n is defined by $C_n = \{1, a, a^2, ..., a^{n-1}\}$, with $a^n = 1$ and $1, a, ..., a^{n-1}$ 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 $G \cong K_4 \cong C_2 \times C_2$, the Klein 4-group.

Proof:

1. If $|G| = 1$, then $G \cong \{1\}$.
2. If $|G| = 2$, then $G = \{1, g\}$ with $g \neq 1$. Then $g^2 = g$ or $g^2 = 1$. We note that if $g^2 = g$, by cancellation, we get $g = 1$, a contradiction. Therefore, $g^2 = 1$. Hence, the Cayley table of G is

G	1	g
1	1	g
g	g	1

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 $g \cdot 1 = g, g \cdot h = 1$. 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

□

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 that H is a subgroup of G.
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, H is a subgroup of G if it satisfies the Subgroup Test.

Definition 2.1.2 **The Subgroup Test**

Let G be a group and $H \subseteq G$. H is a subgroup if the following are true:
1. If $h_1, h_2 \in H$, then $h_1h_2 \in H$.
2. $1_H \in H$.
3. If $h_1 \in H$, then $h_1^{-1} \in H$.

Exercise 2.1.1

Prove that $1_H = 1_G$.

Proof: Let $H \subseteq G$ be a subgroup. Then $\forall a \in G, a \cdot 1_G = a = 1_G \cdot a$. But $H \subseteq G$, so $\forall a \in H, a \cdot 1_G = a = 1_G \cdot a$. Hence, $1_H = 1_G$. □

Example

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

Example

We have a chain of groups $(\mathbb{Z}, +) \subseteq (\mathbb{Q}, +) \subseteq (\mathbb{R}, +) \subseteq (\mathbb{C}, +)$.

Example

We recall the general linear group of order n over $\mathbb{R}$ is

$$GL_n(\mathbb{R}) = (GL_n(\mathbb{R}), \cdot) := \{M \in M_n(\mathbb{R}), \det(M) \neq 0\}$$

Define

$$SL_n(\mathbb{R}) = (SL_n(\mathbb{R}), \cdot) := \{M \in M_n(\mathbb{R}), \det(M) = 1\} \subseteq GL_n(\mathbb{R})$$

Note that the identity matrix $I \in SL_n(\mathbb{R})$. Let $A, B \in SL_n(\mathbb{R})$. Then $\det(AB) = \det(A)\det(B) = 1 \cdot 1 = 1$ and $\det(A^{-1}) = \frac{1}{\det(A)} = \frac{1}{1} = 1$. So $AB, A^{-1} \in SL_n(\mathbb{R})$. By the Subgroup Test, $SL_n(\mathbb{R})$ is a subgroup of $GL_n(\mathbb{R})$. We call $SL_n(\mathbb{R})$ the special linear group of order n over $\mathbb{R}$.

Definition 2.1.3

Given a group G, we define the center of G to be
$Z(G) = \{z \in G : zg = gz \ \forall g \in G\}$.
Note that $Z(G) = G$ iff G is abelian.

Proposition 2.1

$Z(G)$ 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 $z \in Z(G)$ and $g \in G$, we have

$$zg = gz \Leftrightarrow z^{-1}(zg)z^{-1} = z^{-1}(gz)z^{-1}$$

$$\Leftrightarrow (zz^{-1})gz^{-1} = z^{-1}g(zz^{-1})$$

$$\Leftrightarrow gz^{-1} = z^{-1}g$$

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

Proposition 2.2

Let H and K be subgroups of a group G. Then $H \cap K = \{g \in G : g \in H \wedge g \in K\}$ is a subgroup of G.

Proof: Let $f, g \in H \cap K$. Then $f, g \in H$, so $f \cdot g \in H$ since H is a group. Similarly, $f, g \in K$, so $f \cdot g \in K$ since K is a group. Therefore, $f \cdot g \in H \cap K$. Now, $1_G \in H \cap K$ since $1_H = 1_G$ by Exercise 2.1.1 and $1_H \in H$, and since $1_K = 1_G$ by Exercise 2.1.1 and $1_K \in K$. Finally, if $f \in H \cap K$, then $f \in H$, so $f_H^{-1} \in H$ since H is a group, and similarly, $f \in K$, so $f_K^{-1} \in K$. But $f_H^{-1} = f_K^{-1} = f_G^{-1} := f^{-1}$ since inverses are unique and since H, K are both subgroups of G. Therefore, $f^{-1} \in H \cap K$. Therefore, $H \cap G$ is a subgroup of G. □

Proposition 2.3 **Finite Subgroup Test**

If H is a finite non-empty subset of a group G, then H is a subgroup of G iff H is closed under its operation.

Proof:

$\implies$ Trivial
$\impliedby$ For $H \neq \varnothing$, let $h \in H$. Since H is closed under its operation, we have $h, h^2, h^4, \ldots$ are all 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 subgroup of G. □

2.2 Alernating Groups

Definition 2.2.1

A transposition $\sigma \in S_n$ is a cycle of length 2, ie: $(a\ b)$ with $a, b \in \{1, 2, \ldots, n\}$ and $a \neq b$.

Example

Consider $(1\ 2\ 4\ 5) \in S_5$. Also, the composition $(1\ 2)(2\ 4)(4\ 5)$ can be computed as

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

Thus, we have $(1\ 2\ 4\ 5) = (1\ 2)(2\ 4)(4\ 5)$.
Also, we can show that $(1\ 2\ 4\ 5) = (2\ 3)(1\ 2)(2\ 5)(1\ 3)(2\ 4)$.
We see from this example that the factorization into transpositions are NOT unique. However, one can prove the following theorem (see Bonus 2).

Theorem 2.4 **Parity Theorem**

If a permutation σ has two factorizations $\sigma = \gamma_1\gamma_2\ldots\gamma_r = \mu_1\mu_2\ldots\mu_s$, 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 Theorem 2.4, a permutation is either even or odd, but not both.

Theorem 2.5

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

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 that A_n is a subgroup of S_n, called the alternating group of degree n.

Proof:

1. We can write $\varepsilon = (12)(12)$. Thus, ε is even.
2. If $\sigma, \tau \in A_n$, we can write $\sigma = \sigma_1\sigma_2...\sigma_r$ and $\tau = \tau_1\tau_2...\tau_s$, where σ_i, τ_i are transpositions and r, s are even integers. Then $\sigma\tau = \sigma_1...\sigma_r\tau_1...\tau_s$ is a product of $(r+s)$ transpositions and thus $\sigma\tau \in A_n$.Also, we note that since σ_i is a transposition, we have $\sigma_i^2 = \varepsilon$ and thus $\sigma_i^{-1} = \sigma_i$. It follows that $\sigma^{-1} = (\sigma_1...\sigma_r)^{-1} = \sigma_r\sigma_{r-1}...\sigma_1$, which is an even permutation.
3. Let O_n denote the set of odd permutations in S_n. Thus, $S_n = A_n \cup O_n$ and the parity then implies that $A_n \cap O_n = \varnothing$. 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 $f : A_n \longrightarrow O_n$ 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

$$\langle g \rangle = \{g^\beta : \beta \in \mathbb{Z}\} = \{..., g^{-2}, g^{-1}, g^0, g^1, g^2, ...\}$$

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 $xy = g^m g^n = g^{m+n} \in \langle g \rangle$ and $x^{-1} = g^{-m} \in \langle g \rangle$. Therefore, by Definition 2.1.2, we have the following proposition:

Proposition 2.6

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 and $g \in G$. 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 is a generator of G.

Example

Consider $(\mathbb{Z}, +)$. Note that for $k \in \mathbb{Z}$, we can write

$$k = k \cdot 1 := \underbrace{1 + 1 + \ldots + 1}_{k \text{ times}}$$

Note that when $k = 0$, $k = 1_{\text{id}} = 0 \in \mathbb{Z}$. Thus, $(\mathbb{Z}, +) = \langle 1 \rangle$. Similarly, $(\mathbb{Z}, +) = \langle -1 \rangle$. We observe that for any $n \in \mathbb{Z}$ 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 $(\mathbb{Z}, +)$.

Note

Let G be a group and $g \in G$. Suppose that there exists $k \in \mathbb{Z}, k \neq 0$ such that

$$g^k = 1$$

We can assume that $k \geq 1$ because if $k \leq -1$, then $g^{-k} = 1$. So, 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 that the order of g is n, denoted by $o(g) = n$. If no such n exists, then we say g has **infinite order** and write $o(g) = \infty$.

Proposition 2.7

Let G be a group and $g \in G$ satisfying $o(g) = n \in \mathbb{N}$. 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. $\langle g \rangle = \{1, g, g^2, \ldots, g^{n-1}\}$, where $1, g, g^2, \ldots g^{n-1}$ are all distinct. In particular, we have $|\langle g \rangle| = o(g)$.

Proof:

$(1)(\Longleftarrow)$ 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 $g^r = g^{k-nq} = g^k \cdot (g^n)^{-q} = 1 \cdot 1^{-q} = 1$. Since $0 \leq r < n$ and $o(g) = n$, we have $r = 0$ and hence $n \mid k$.
(2) Note that $g^k = g^m$ iff $g^{k-m} = 1$. By (1), we have $n \mid (k-m)$, which is equivalent to $k \equiv m (\mathrm{mod}\, n)$.
(3) It follows from (2) that $1, g, g^2, ...g^{n-1}$ are all distinct. Clearly, we have $\{1, g, g^2, ..., g^{n-1}\} \subseteq \langle g \rangle$. To prove the other inclusion, let $g^k \in \langle g \rangle$ for some $k \in \mathbb{Z}$. Write $k = nq + r$ with $q, r \in \mathbb{Z}$ and $0 \leq r < n$. Then
$g^k = (g^n)^q \cdot g^r = 1^q \cdot g^r = g^r \in \{1, g, ..., g^{n-1}\}$. Thus, we have $\langle g \rangle = \{1, g, ..., g^{n-1}\}$. □

Proposition 2.8

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

Proposition 2.9

Let G be a group and $g \in G$ with $o(g) = n \in \mathbb{N}$. If $d \in \mathbb{N}$, then $o(g^d) = \frac{n}{\gcd(n,d)}$, where $\gcd(n, d)$ is the gcd of n and 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 in MATH 135, we have $\gcd(n_1, d_1) = 1$. Note that

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

since $o(g) = n$. 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 2.7, we have $n \mid dr$. Thus, there exists $q \in \mathbb{Z}$ 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 $\gcd(n_1, d_1) = 1$, then by a result in MATH 135, we get $n_1 \mid r$, ie: $r = n_1 l$ for some $l \in \mathbb{Z}$. Since $r_1, n_1 \in \mathbb{N}$, it follows that $l \in \mathbb{N}$. Since $l \geq 1$, 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 $a = g^m$ and $b = g^n$ for some $m, n \in \mathbb{Z}$ for some $m, n \in \mathbb{Z}$. We have $ab = g^m g^n = g^{m+n} = g^{m+n} = g^n g^m = ba$.

Proposition 2.10

Every cyclic group is abelian.

Remark

The converse of Proposition 2.10 is false. For example, the Klein 4 group $K_4 \cong C_2 \times C_2$ is abelian, but K_4 is not cyclic.

Proposition 2.11

Every subgroup of a cyclic group is cyclic.

Proof: Let $G = \langle g \rangle$ be cyclic and let H be a subgroup of G. If $H = \{1\}$, then $H = \langle 1 \rangle$ is cyclic.
If $H \neq \{1\}$, then there exists $g^k \in H$ with $k \in \mathbb{Z}$ and $k \neq 0$. Since H is a group, then we have $g^{-k} \in H$. Thus we can assume that $k \in \mathbb{N}$. Let m be the smallest positive integer such that $g^m \in H$.
Claim: $H = \langle g^m \rangle$
Proof of claim: Clearly, $\langle g^m \rangle \subseteq H$. For the other containment, let $g' \in H$. Then $g' = g^{mq+r}$ for some $q \in Z, 0 \leq r < m$, since $H \subseteq G = \langle g \rangle$ and by division algorithm. So $g' = (g^m)^q g^r$. Since H is a group and $g^m \in H$, then $(g^m)^q \in H$. So $g^r = (g^m)^{-q} g' \in H$. However, m is the smallest postiive integer for which $g^r \in H$, so $r = 0$. Hence, $g' = (g^m)^q g^0 = (g^m)^q \cdot 1 = (g^m)^q \in \langle g^m \rangle$. So $H = \langle g^m \rangle$, as required. □

So in either case, H is a cyclic subgroup of G, as required. □

Proposition 2.12

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

Proof: By order-power-finite-group, $o\left(g^k\right) = \frac{n}{\gcd(n,k)} = n$ □

Theorem 2.13 **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 $H = \langle g^d \rangle$ for some $d \mid n$. It follows that $|H| \mid |G|$ (|H| divides |G|).
2. Conversely, if $k \mid n$, then $\left\langle g^{\frac{n}{k}} \right\rangle$ is the unique subgroup of G of order k.

Proof:
1. By Proposition 2.11, H is cyclic. Write $H = \langle g^m \rangle$ for some $m \in \mathbb{N} \cup \{0\}$. Let $d = \gcd(m, n)$.
   Claim: $H = \langle g^d \rangle$.
   Proof of claim: 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 $d = \gcd(m, n)$, then by Bezout's Lemma, there exist $x, y \in \mathbb{Z}$ such that $d = mx + ny$. Then $g^d = g^{mx+ny} = (g^m)^x (g^n)^y = (g^m)^x \cdot 1^y = (g^m)^x \in \langle g^m \rangle$. 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 2.7 and order-power-finite-group, we have

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

Thus, $|H| \mid |G|$. □

2. By Prop 2.8, the cyclic subgroup $\left\langle g^{\frac{n}{k}} \right\rangle$ is of order

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

To show uniqueness, let K be a subgroup of G, which is of order k with $k \mid n$. By (1), let $K = \langle g^d \rangle$ with $d \mid n$. Then by Prop 2.6 and Prop 2.8, we have $k = |K| = o\left(g^d\right) = \frac{n}{\gcd(n,d)} = \frac{n}{d}$. It follows that $d = \frac{n}{k}$ and thus $K = \left\langle g^{\frac{n}{k}} \right\rangle$.

□

2.5 Non-Cyclic Groups

Definition 2.5.1

Let X be a non-empty subset of a group G, and let $\langle X \rangle = \left\{ x_1^{k_1} x_2^{k_2} \ldots x_m^{k_m} : x_i \in X, k_i \in \mathbb{Z}, m \geq 1 \right\}$ denote the set of all products of powers of (not necessarily distinct) element of X.

Note

If $x_1^{k_1}, \ldots x_m^{k_m} \in \langle X \rangle$ and $y_{1_1}^{r_1} \ldots y_n^{r_n} \in \langle X \rangle$, then $x_1^{k_1} \ldots x_m^{k_m} y_1^{r_{11}} \ldots y_n^{r_n} \in \langle X \rangle$. Also, $x_1^0 \in \langle X \rangle$ and $\left(x_1^{k_1} \ldots x_m^{k_m}\right)^{-1} = x_m^{-k_m} \ldots x_1^{-k_1} \in \langle X \rangle$. Hence, $\langle X \rangle$ is a subgroup of G containing X, called the subgroup of G generated by X.

Example

The Klein 4-group $K_4 = \{1, a, b, c\}$ with $a^2 = b^2 = c^2 = 1$ and $ab = c$ (or $ac = b$ or $bc = a$). Thus, $K_4 =< a, b = a^2 = 1 = b^2 \wedge ab = ba >$.

Example

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 sigma = (1 2 3) and $\tau = (12)$). Thus,

$$S_3 = \langle \sigma, \tau \mid \sigma^3 = \varepsilon = \tau^2 \wedge \sigma\tau = \tau\sigma^2 \rangle$$

We can also replace σ, τ by $\sigma, \tau\sigma$ 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,

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

Note that when $n = 2$ or $n = 3$, we have $D_4 \cong K_4$ and $D_6 \cong S_3$.

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 and H be groups. A mapping $\alpha : G \to H$ is a homomorphism (HM) if

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

To simplify notation, we often write

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

Example

Consider the determinant map

$$\det = (GL_n(\mathbb{R}), \cdot) \to \mathbb{R}^*$$

given by

$$A \to \det(A)$$

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

Proposition 3.1

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

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

Proof:

1. $\alpha(1_G) = \alpha(1_G \cdot 1_G) = \alpha(1_G) \cdot \alpha(1_G)$, so by cancellation, $\alpha(1_G) = 1_H$.
2. $1_H = \alpha(1_G) = \alpha(g \cdot g^{-1}) = \alpha(g) \cdot \alpha(g^{-1})$. So $\alpha(g)^{-1} = \alpha(g^{-1})$.
3. $$\alpha(g^k) = \alpha\left(\underbrace{g \ldots g}_{k \text{ times}}\right) = \underbrace{\alpha(g) \ldots \alpha(g)}_{k \text{ times}} = \alpha(g)^k$$

□

Definition 3.1.2

Let G and H be groups. Consider a mapping $\alpha : G \to H$. If α is a HM and α is bijective, we say α is an isomorphism (IM). In this case, we say G and H are isomorphic and denote it as $G \cong H$.

Proposition 3.2

We have

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

Thus, we see that $\cong$ is an equivalence relation on the class of all groups.

Exercise 3.1.1 **Proof of Proposition 3.2**

1. The identity map is clearly bijective. Moreover, for any $g \in G$, $\mathrm{id}(g \cdot g) = g \cdot g = \mathrm{id}(g) \cdot \mathrm{id}(g)$, so id is a homomorphism. Hence, id is an isomorphism.
2. Suppose σ is an isomorphism. Then σ is bijective. So σ^{-1} is bijective by a result from PMATH 351. Now, for $a, b \in H$, we have that

$$\begin{aligned}
\sigma^{-1}(a \cdot b) &= \sigma^{-1}(\sigma(c) \cdot \sigma(d)) \text{ (for some } c, d \in G, \text{since } \sigma \text{ is bijective)} \\
&= \sigma^{-1}(\sigma(c \cdot d)) \qquad (\text{since } \sigma \text{ is a homomorphism}) \\
&= c \cdot d \\
&= \sigma^{-1}(a) \cdot \sigma^{-1}(b) \quad (\text{since } a = \sigma(c) \Rightarrow c = \sigma^{-1}(a) \text{ and} \\
&\qquad\qquad\qquad\qquad b = \sigma(d) \Rightarrow d = \sigma^{-1}(b))
\end{aligned}$$

   Therefore, σ^{-1} is a homomorphism. Hence, σ^{-1} is an isomorphism.
3. Suppose σ and τ are isomorphisms. Then they are bijections, so $\tau\sigma$ is a bijection by a result from PMATH 351. Now, for $a, b \in G$, we have that

$$\begin{aligned}
(\tau\sigma)(a \cdot b) &= \tau(\sigma(a \cdot b)) \\
&= \tau(\sigma(a) \cdot \sigma(b)) \qquad (\text{Since } \sigma \text{ is a homorphism}) \\
&= \tau(\sigma(a)) \cdot \tau(\sigma(b)) \quad (\text{Since } \tau \text{ is a homorphism}) \\
&= (\tau\sigma)(a) \cdot (\tau\sigma)(b)
\end{aligned}$$

   So $\tau\sigma$ is a homomorphism. Hence, $\tau\sigma$ is an isomorphism.

Example

Let $R^+ = \{r \in \mathbb{R}, r > 0\}$.
Claim: $(\mathbb{R}, +) \cong (\mathbb{R}^+, \cdot)$
Proof: Define $\sigma : (\mathbb{R}, +) \to (\mathbb{R}^+, \cdot)$ by $\sigma(r) = e^r$, where e is the exponential function. Note that the exponential map from $\mathbb{R}$ to $\mathbb{R}^+$ is bijective. Also, for $r, s \in \mathbb{R}$, we have $\sigma(r + s) = e^{r+s} = e^r \cdot e^s = \sigma(r) \cdot \sigma(s)$. So σ is a homomorphism. Thus, σ is isomorphism. □

Example

Claim: $(\mathbb{Q}, +)$ is not isomorphic to $(Q^*, \cdot)$.
Proof: Suppose $\tau : (\mathbb{Q}, +) \to (\mathbb{Q}^*, \cdot)$ is an isomorphism. Thus, τ is surjective. So there exists $q \in \mathbb{Q}$ such that $\tau(q) = 2$. Write $\tau\left(\frac{q}{2}\right) = a \in \mathbb{Q}^* \subseteq \mathbb{Q}$. Since τ is a HM, we have

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

which contradicts the fact that $a \in \mathbb{Q}$. Thus, such a τ does not exist and hence $(\mathbb{Q}, +) \ncong (\mathbb{Q}^*, \cdot)$. □

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. Similarly, we define $aH = \{ah \mid h \in H\}$ to be the left coset of H generated by a. Since $1 \in H$, we have $H1 = H = 1H$ and $a \in Ha$ 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

Let $K_4 = \{1, a, b, ab\}$ with $a^2 = 1 = b^2$ and $ab = ba$. Let $H = \{1, a\}$, which is a subgroup of K_4. Note that since K_4 is abelian, we have $gH = Hg \ \forall g \in K_4$. 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

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

$$H\varepsilon = \{\varepsilon, \tau\} = H\tau$$

$$H\sigma = \{\sigma, \tau\sigma\} = H\tau\sigma$$

$$H\sigma^2 = \{\sigma^2, \tau\sigma^2\} = H\tau\sigma^2$$

Also, the left cosets of H are

$$\varepsilon H = \{\varepsilon, \tau\} = \tau H$$

$$\sigma H = \{\varepsilon, \tau\sigma^2\} = \tau\sigma^2 H$$

$$\sigma^2 H = \{\sigma^2, \tau\sigma, \tau\sigma H\}$$

Note 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 $a, b \in G$. Then

1. $Ha = Hb$ iff $ab^{-1} \in H$. In particular, we have $Ha = H$ iff $a \in H$ (taking $b = 1$).
2. If $a \in Hb$, then $Ha = Hb$.
3. Either $Ha = Hb$ or $Ha \cap Hb = \varnothing$. Thus, the distinct right cosets of H form a partition of G.

Proof:

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 $ab^{-1} \in H$. Then for all $h \in H$,

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

   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 $Ha = Hb$.
2. If $a \in Hb$, then $ab^{-1} \in H$. Thus by (1), we have $Ha = Hb$. Two cases:
   a. If $Ha \cap Hb = \varnothing$, then we are done.
   b. If $Ha \cap Hb \neq \varnothing$, then there exists $x \in Ha \cap Hb$. Since $x \in Ha$, by (2), we have $Hx = Ha$. Since $x \in Hb$, by (2), we have $Hb = Hx$. Thus $Ha = Hx = Hb$.

□

Remark

The analog of Proposition 3.3 also holds for left cosets. For (1), we have $aH = bH$ iff $b^{-1}a \in H$.

Exercise 3.2.1

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

Definition 3.2.2

By Proposition 3.3, 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 **Langrange'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 $Ha_1, Ha_2, ...Ha_k$ be the distinct right cosets of H in G. By Proposition 3.3, we have $G = Ha_1 \cup Ha_2 \cup ... \cup Ha_k$ is a disjoint union. Since $|Ha_i| = |H|$ for each i, we have $|G| = |Ha_i| + |Ha_2| + ... + |Ha_k| = k\ |H|$. It follows that $|H| \mid |G|$ and

$$[G : H] = k = |G| \mid |H|$$

□

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:

1. Take $H = \langle g \rangle$ in Theorem 3.4. Note that $|H| = o(g)$.
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

For $n \in \mathbb{N}$ with $n \geq 2$, let $\mathbb{Z}_n^*$ be the set of (multiplicatively) invertible elements in $\mathbb{Z}_n$. Let the *Euler's φ function*, $\varphi(n)$, denote the order of $\mathbb{Z}_n^*$, ie: $\varphi(n) = \#\{[k] \in \mathbb{Z}_n : k \in \{0, 1, ...n-1\} \wedge \gcd(k, n) = 1\}$. As a direct consequence of Corollary 3.5, we see that if $a \in \mathbb{Z}$ with $\gcd(a, n) = 1$, then $a^{\varphi(n)} \equiv 1 (\mathrm{mod}\, n)$. This is Eurler's Theorem. If $n = p$, a prime number, then Eulers then implies $a^{p-1} \equiv 1 (\mathrm{mod}\, p)$, which is Fermat's Little Theorem from MATH 135.

Recall

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

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 3.5, we have $o(g) \mid p$. Since $g \neq 1$ and p is prime, we have $o(g) = p$. By Prop 2.6 (TODO), we have $|\langle g \rangle| = o(g) = p$. It follows that $G = \langle g \rangle \cong C_p$. □

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: By Proposition 2.2, $H \cap K$ is a subgroup of H and K. By Theorem 3.4, we have $|H \cap K| \mid |H|$ and $|H \cap K| \mid |K|$. It follows that $|H \cap K| \mid \gcd(|H|, |K|)$, ie: $|H \cap K| \mid 1$. 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

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

Example

The center $Z(G)$ of G, $Z(G) = \{z \in G, zg = gz \ \forall g \in G\}$ is an abelian subgroup of G. By its definition, $Z(G) \lhd G$. Thus, every subgroup of $Z(G)$ is normal in G.

Example

If G is an abelian group, then every subgroup of G is normal in G. The converse is false (see the quarternion group Q_8 in A3).

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 $H \lhd G$ iff H is the only conjugate of H)

Proof:

$(1) \Rightarrow (2)$ 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 $ghg^{-1} = h_1 gg^{-1} = h \in H$.
$(2) \Rightarrow (3)$ If $g \in G$, then by (2), $gHg^{-1} \subseteq H$. Taking g^{-1} in place of g in (2), we get $g^{-1}Hg \subseteq H$. This implies that $H \subseteq gHg^{-1}$. Thus $H = gHg^{-1}$.
$(3) \Rightarrow (1)$ If $gHg^{-1} = H$, then $gH = Hg$. □

Example

Let $G = GL_n(\mathbb{R})$ and $H = SL_n(\mathbb{R})$. For $A \in G$ and $B \in H$, we have

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

Thus $ABA^{-1} \in H$ and it follows taht $AHA^{-1} \subseteq H \forall A \in G$. By the normality test, $H \lhd G$.

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 $G = H \cup Hg$, a disjoint union. Then $Hg = G \setminus H$. Similarly, $gH = G \setminus H$. Thus $gH = Hg$ for all $g \in G$, ie: $H \lhd G$. □

Example

Let A_n be the alternating group contained in A_n. Since $[S_n = A_n] = 2$, by Prop 3.9, we have $A_n \lhd S_n$.

Example

Let $D_{2n} = \langle a, b \mid a^n = 1 = b^2 \wedge aba = b \rangle$ be the dihedral group of order $2n$. Since $[D_{2n} = \langle a \rangle] = 2$, by Prop 3.9, $\langle a \rangle \lhd D_{2n}$.

Recall

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

Note

What is the smallest subgroup containing H and K?
$H \cup K$ is the smallest subset containing H and K, but $H \cup K$ is a subgroup of G if and only if $H \subseteq K$ or $K \subseteq H$ by A2.
A more useful subset to consider is the *product* HK of H and K defined as follows: $HK = \{hk \mid h \in H, k \in K\}$. But HK is not always a subgroup of G.

Lemma 3.10

Let H and K be subgroups of a group G. The following are equivalent:
1. HK is a subgroup of G.
2. $HK = KH$.
3. KH is a subgroup of G.

Proof: We will prove $(1) \Leftrightarrow (2)$. Then $(2) \Leftrightarrow (3)$ follows by interchanging H and K.
$(2) \Rightarrow (1)$ 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 $h, k, h_1, k_1 \in HK$, 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.
$(1) \Rightarrow (2)$ Let $kh \in KH$ with $k \in K$ and $h \in H$. 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 that $HK \subseteq KH$. □

Proposition 3.11

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

Proof: (1) Suppose $H \lhd G$. Then

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

By Lemma 3.10, $HK = KH$ is a subgroup of G.
(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 3.3.2

Let H be a subgroup of a group G. The *normalizer* of H, denoted by $N_G(H)$ is defined to be $N_G(H) = \{g \in G : gH = Hg\}$. We see that $H \lhd G$ if and only if $N_G(H) = G$.

Note

In the proof of Proposition 3.11, we do not need the full assumption that $H \lhd G$. We only need $kH = Hk$ for all $k \in K$, ie: $k \in N_G(H)$. Thus, we have the following corollary:

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 $k \in K$.
Proof of claim: Consider $x = hk(kh)^{-1} = hkh^{-1}k^{-1}$. Note that $kh^{-1}k^{-1} \in kHk^{-1} = H$ (since $H \lhd G$). Thus $x = h(kh^{-1}k) \in H$. Similarly, since $hkh^{-1} \in hKh^{-1} = K$, we have $x = (hkh^{-1})k^{-1} \in K$. Since $x \in H \cap K = \{1\}$, we have $hkh^{-1}k^{-1} = 1$, ie: $hk = kh$. □

Since $H \lhd G$, by Proposition 3.11, we have that $HK \leq G$. Define $\sigma : H \times K \to HK$ by $\sigma((h,k)) = hk$.
Let $(h,k) \in H \times K$. By the claim, we have $h_1 k = k h_1$. Thus, $\sigma((h,k) \cdot (h_1,k_1)) = \sigma((hh_1, kk_1)) = hh_1kk_1 = hkh_1k_1 = \sigma((h,k))\sigma((h_1,k_1))$. 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 $h_1^{-1}h = 1 = k_1k^{-1}$, ie: $h_1 = h$ and $k_1 = k$. Thus σ is injective. Thus, 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 $G \cong H \times K$.

Example

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 $|H| \cdot |K| = mn = |G|$. Since $\gcd(m, n) = 1$. By corollary 3.2.8 (TODO), $H \cap K = \{1\}$. Also, since G is cyclic and thus abelian, we have $H \lhd G$ and $K \lhd G$. Thus, by Corollary 3.14, we have $G \cong H \times K$, ie: $C_{mn} \cong C_m \times C_n$. Hence to consider finite cyclic group, it suffices to consider cyclic groups of prime power order.

4 Isomorphism Theorems

4.1 Quotient Groups

Definition 4.1.1

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

$$Ka \cdot Kb = K \cdot (ab) \ \forall a, b \in G \ (*)$$

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

$$Ka = Ka \wedge Kb = Kb_1 \Rightarrow Kab = Ka_1b_1$$

In this case, we say that the multiplication $KaKb = Kab$ 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 $KaKb = Kab$ is well-defined.

Proof: $(1) \Rightarrow (2)$ Let $Ka = Ka_1$ and $Kb = Kb_1$. Thus $aa_1^{-1} \in K$ and $bb^{-1} \in K$. 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 $Kab = Ka_1b_1$.
$(2) \Rightarrow (1)$ 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 $Kak = Ka1$, ie: $Kak = Ka$. It follows that $aka^{-1} \in K$. $\square$

Proposition 4.2

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

1. G/K is a group under the operation $Ka \star Kb = Kab$.
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*:**

1. By Lemma 4.1, 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.
2. φ is clearly surjective. Also, for $a, b \in G$, we have $\varphi(a)\varphi(b) = KaKb = Kab = \varphi(ab)$. Thus φ is a surjective homomorphism.
3. If $[G = K]$ is finite, by the definition of index, $|G/K| = [G = K]$. Also if $|G|$ is finite, by Lagrange Theorem, $|G/K| = [G = K] = \frac{|G|}{|K|}$.

□

Definition 4.1.2

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 *kernal of* α is defined by

$$\text{Ker } \alpha = \{g \in G : \alpha(g) = 1_H\} \subseteq G$$

and the *image of alpha* is defined by

$$\text{img } \alpha = \alpha(G) = \{\alpha(g) : g \in G\} \subseteq H$$

Proposition 4.3

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

1. img α is a subgroup of H.
2. ker α is a normal subgroup of G.

Proof:

1. Note that $1_H = \alpha(1_G) \in \alpha(G)$. Also, for $h_1 = \alpha(g_1), h_2 = \alpha(g_2) \in \alpha(G)$, we have
$$h_1 h_2 = \alpha(g_1)\alpha(g_2) = \alpha(g_1 g_2) \in \alpha(G)$$
Also, by Prop 3.1, $\alpha(g)^{-1} = \alpha(g^{-1}) \in \alpha(G)$. By the subgroup test, $\alpha(G)$ is a subgroup of G.
2. For Ker α, note that $\alpha(1_G) = 1_H$. Also, for $k_1, k_2 \in$ Ker α, 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 α is a subgroup of G. Note that if $g \in G$ and $k \in$ Ker α, then $\alpha(gkg^{-1}) = \alpha(g)\alpha(k)\alpha(g^{-1}) = \alpha(g) \cdot 1 \cdot \alpha(g)^{-1} = 1$. Thus $g(\text{Ker } \alpha)g^{-1} \subseteq \text{Ker}(\alpha)$. By the normality test, Ker $\alpha \lhd G$.

□

Example

Consider the determinant map $\det : GL_n(\mathbb{R}) \to \mathbb{R}^*$ defined by $A \to \det(A)$. Then $\ker(\det) = SL_n(\mathbb{R})$. Thus $SL_n(\mathbb{R}) \lhd GL_n\mathbb{R}$. This is an alternative proof of this fact.

Example

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

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

Note that $\text{sgn} : S_n \to (\pm 1, \cdot)$ defined by $\sigma \mapsto \text{sgn}(\sigma)$ is a homomorphism. Also, $\ker(\text{sgn}) = A_n$. 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. We have

$$G/\ker(\alpha) \cong \operatorname{img}\ \alpha$$

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

$$\overline{\alpha} : G/K \to \operatorname{img}\ \alpha$$

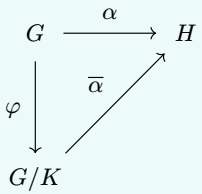
by $\overline{\alpha}(Kg) = \alpha(g)$ for all $Kg \in G/K$. Note that

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

Thus $\overline{\alpha}$ is well-defined (forward direction) and injective (backward direction). 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 $G/\ker(\alpha) \cong \operatorname{img}\ \alpha$. □

Note

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 proof of Theorem 4.4. We have the following diagram.



Note that for $g \in G$, we have $\overline{\alpha}(\varphi(g)) = \overline{\alpha}(Kg) = \alpha(g)$. Thus $\alpha = \overline{\alpha} \circ \varphi$. 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 a 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

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 they indeed are all 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 $\ker \alpha = \{k \in \mathbb{Z} : g^k = 1\}$. Two cases:

1. If $o(g) = \infty$, then $\ker \alpha = \{0\}$. By the First Isomorphism Theorem, we have $G \cong \mathbb{Z}/\langle 0 \rangle \cong \mathbb{Z}$
2. If $o(g) = n$, then by an old prop, $\ker \alpha = n\mathbb{Z}$. By the first isomorphism theorem, $G \cong \mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}_n$.

By (1) and (2), we 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 3.11, HK is a subgroup of G and $HK = KH$. Furthermore, we need to show that $K \lhd HK$. This is equivalent to proving that for any $h \in H, k \in K$, we have that $(hk)K(hk)^{-1} \subseteq K$. Let $k' \in K$ be arbitrary. Then $(hk)k'(hk)^{-1} = h(kk'k^{-1})h^{-1} \in hKh^{-1} = K$, since $h \in H \subseteq G$ and $K \lhd G$.
Now, consider $\alpha : H \to HK/K$ defined by $\alpha(h) = Kh$ (note that $h \in H \subseteq HK$). Then α is a homomorphism because if $h_1, h_2 \in H$, then since the coset product is well-defined on HK/K (by Lemma 4.1), we have that
$\alpha(h_1h_2) = K(h_1h_2) = (Kh_1)(Kh_2) = \alpha(h_1)\alpha(h_2)$. Also, if $x \in HK = KH$, say $x = kh$, then

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

Thus, α is surjective. Finally, by Proposition 4.3,
$\ker(\alpha) = \{h \in H : Kh = K\} = \{h \in H : h \in K\} = H \cap K$ with $H \cap K \lhd H$. By Theorem 4.4, we have

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

□

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 $\alpha = \{Kg : Hg = H\} = \{Kg : g \in H\} = H/K$. 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 $G = \{g_1, ..., g_n\}$ and let S_G be the permutation group of G. By identifying g_i with i $(1 \leq i \leq n)$, we see that $S_G \cong S_n$. Then it suffices to find an 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, so $\mu_a \in S_G$. Define $\sigma : G \to S_G$ by $\sigma(a) = \mu_a$. For $a, b \in G$, we have $\mu_a\mu_b = \mu_{ab}$, so σ is a homomorphism. Also, if $\mu_a = \mu_b$, then $a = \mu_a(1) = \mu_b(1) = b$. Thus σ is an injective homomorphism. By the First Isomorphism Theorem, we have $G \cong \text{img } \sigma$, a subgroup of $S_G \cong S_n$. □

Example

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 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 exists a group homomorphism $\tau : G \to S_X$ with $K = \ker(\tau) \subseteq H$. By the First Isomorphism Theorem, we have $G/K \cong \text{im}(\tau)$. Since $K \subseteq H$ and $K \lhd G$, by the assumption. We have $K = \{1\}$. It follows that $G \cong \text{im}(\tau)$, a subgroup of $S_X \cong S_m$. □

Corollary 5.3

Let G be a finite group and p be 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 $G/K \cong \text{im}(\tau) \subseteq S_p$. 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 $|G/K| = \frac{|G|}{|H|}\frac{|H|}{|K|} = pk$. 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 that 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 **Group Actions**

Let G be a group and X be a non-empty set. A (left) *group action* 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 $X \neq \varnothing$. For $a, b \in G$ and $x, y \in X$, by (1) and (2), we have $a \cdot x = b \cdot y$ if and only if $(b^{-1}a) \cdot x = y$.
In particular, we have $a \cdot x = a \cdot y$ if and only if $x = y$.

Example

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

1. $1 \cdot x = 1x1^{-1} = x$
2. $a(b \cdot x) = a(bxb^{-1})a^{-1} = (ab)x(ab)^{-1} = (ab) \cdot x$

In this case, we say G acts on itself by conjugation.

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 (see A5) that

1. $\sigma_a \in S_X$, the permutation group of X.
2. The function $\Theta : G \to S_X$ given by $\Theta(a) = \sigma_a$ is a group homomorphism with $\ker(\Theta) = \{a \in G : ax = x \text{ for all } x \in X\}$.

Note

Note that the group homomorphism $\Theta : G \to S_X$ gives an equivalent definition of a 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 a non-empty set $X \neq \varnothing$ and $x \in X$. We denote by

$$G \cdot x = \{g \cdot x : g \in G\} \subseteq X$$

the *orbit of* x and

$$S(x) = \{g \in G : g \cdot x = x\} \subseteq G$$

the *stabilizer of* x.

Proposition 5.4

Let G be a group acting on a non-empty set X and $x \in X$. Let $G \cdot x$ and $S(x)$ be the orbit and stabilizer of x, respectively. Then

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

Proof:

1. Since $1 \cdot x = x$, we have $1 \in S(x)$. Also, if $g, h \in S(x)$, then $(gh)x = g(hx) = gx = x$ and $g^{-1}x = g^{-1}(gx) = (g^{-1}g)x = 1x = x$. Thus $gh, g^{-1} \in S(x)$. By the Subgroup Test, $S(x)$ is a subgroup of G.
2. Consider the map $\varphi : G \cdot x \to \{gS(x) : g \in G\}$ defined by $\varphi(g \cdot x) = gS(x)$. Note that $g \cdot x = h \cdot x \Leftrightarrow (h^{-1}g) \cdot x = x \Leftrightarrow h^{-1}g \in S(x) \Leftrightarrow hS(x) = gS(x)$. Thus φ is well-defined and injective. Since φ is clearly surjective, φ is a bijection. It follows that $|G \cdot x| = |\{gS(x) : g \in G\}| = [G : S(x)]$.

□

Theorem 5.5 **Orbit Decomposition Theorem**

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

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

Note that $x \in X_f \Leftrightarrow |G \cdot x| = 1$. Let $G \cdot x_1, G \cdot x_2, G \cdot x_3, ..., G \cdot x_n$ denote the distinct non-singleton orbits (ie: $|G \cdot x_i| > 1$). 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 $x \in X_f$ if and only if $|G \cdot x| = 1$, the set $X \setminus X_f$ contains all non-singleton orbits, which are disjoint. Thus by Proposition 5.4, we have

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

□

Example

Let G be a group acting on itself by conjugation, ie: $g \cdot x = gxg^{-1}$. Then
$G_f = \{x \in G : gxg^{-1} = x \ \forall g \in G\} = \{x \in G : gx = xg \ \forall g \in G\}$ which is exactly the center of G, ie: $G_f = Z(G)$. Also, for $x \in G$,
$S(x) = \{g \in G : gxg^{-1} = x\} = \{g \in G : gx = xg\}$. This set is called the *centralizer* of x and is denoted by $S(x) = C_G(x)$. Finally, in this case, the orbit $G \cdot x = \{gxg^{-1} : g \in G\}$ is called the *conjugacy class of x*. By Theorem 5.5, we get the following corollary:

Corollary 5.6 **Class Equation**

Let G be a finite group and let $\{gx_1g^{-1} : g \in G\}, ..., \{gx_ng^{-1} : g \in G\}$ 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 $X \neq \varnothing$. Let X_f be defined as in Theorem 5.5. Then we have

$$|X| \equiv |X_f| \bmod p$$

Proof: By Theorem 5.5, we have $|X| = |X_f| + \sum_{i=1}^{n} [G = S(x_i)]$ with $[G = S(x_i)] > 1$ $(1 \leq i \leq n)$. 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 $|X| = |X_f| \bmod p$. □

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 $X = \{(a_1, ..., a_p) : a_i \in G \text{ and } a_1 ... a_p = 1\}$. 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 $|X| \equiv 0 \bmod p$. Let the group $\mathbb{Z}_p = (\mathbb{Z}_p, +)$ act on X by "cycling", ie: 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 (Exercise). Let X_f be defined as in Theorem 5.5. Then $(a_1, ..., a_p) \in X_f$ iff $a_1 = a_2 = ... = a_p$. Clearly, $(1, ..., 1) \in X_f$ and hence $|X_f| \geq 1$. Since $|\mathbb{Z}_p| = p$, by Lemma 5.7, we have $|X_f| \equiv |X| \equiv 0 \bmod p$. Since $|X_f| \equiv 0 \bmod p$ and $|X_f| \geq 1$, it follows that $|X_f| \geq p$. Therefore, there exists $a \neq 1$ such that $(a, ..., a) \in X_f$, which implies that $a^p = 1$. Since p is a 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.

Corollary 6.1 **of Cauchy's Theorem**

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

Proof: ($\Longrightarrow$) If G is a finite p-group, then by Lagrange's Theorem, since the cyclic subgroups generated by the elments of G all have size of non-negative powers of p, then $p^k \mid |G|$ for some $k \geq 0$. However, since G contains no elements of order p_1 for any other prime $p_1 \neq p$, then $p_1 \nmid |G|$ by the contrapositive of Cauchy's Theorem. This implies that $|G|$ has no prime divisors besides p. Hence, $|G|$ is a power of p.
($\Longleftarrow$) If $|G|$ is a power of p, then by Lagrange's Theorem, the sizes of all of its subgroups are too. In particular, the sizes of the cyclic subgroups in G are powers of p, so every element has order of a non-negative power of p. Hence, G is a p-group. □

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 (Corollary 5.6) says 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 Corollary 6.1, $p \mid |G|$. By Lemma 5.7, $|Z(G)| \equiv |G| \equiv 0 \bmod p$. 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 $N_G(H) = \{g \in G : gHg^{-1} = H\}$ 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 $[N_G(H) : H] \equiv [G : H] \bmod p$.

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 $\left|X_f\right|$ is the number of cosets of xH with $x \in N_G(H)$ and hence $\left|X_f\right| = [N_G(H) : H]$. By Lemma 5.7, $[N_G(H) : H] = \left|X_f\right| = |X| = [G : H] \bmod p$. □

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 $[N_G(H) : H] \equiv [G : H] \equiv 0 \bmod p$. 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 Sylow's Three Theorems

Recall

Cauchy's Theorem states that if $p \mid |G|$, then G contains an element a 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 **1st 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, ie: $|\langle a \rangle| = p$. Suppose that the statement holds for some $1 \leq i < n$. Say H is a subgroup of order p^i. Then $p \mid [G : H]$. By Corollary 6.4, $p \mid [N_G(H) : H]$ and $[N_G(H) : H] \geq p$. 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, $|H_1| = |H||H_1/H| = p^i p = p^{i+1}$. □

Definition 6.2.1

A subgroup P of a group G is said to be a Sylow p-group of G if P is a maximal p-group of G, ie: if $P \subseteq H \subseteq G$ with H a p-group, then $P = H$. As a direct consequence of Theorem 6.5, we have the following corollary.

Corollary 6.6

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

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

Theorem 6.7 **2nd 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 of G are conjugates.

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 $|X_f| \equiv |X| = [G : P] \bmod p$. 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

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

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

Theorem 6.8 **3rd Sylow Theorem**

If G is a finite group and p is 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 $[G : N_G(P)]$, where $N_G(P) = \{g \in G : gP = Pg\}$, 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 $Q \in X_f$ if and only if $gQg^{-1} = Q$ for all $g \in P$. The latter condition holds if and only if $P \subseteq N_G(Q)$. Both P and Q are Sylow p-subgroups of G and hence $N_G(Q)$. Thus, by Corollary 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, $|X| \equiv |X_f| \equiv 1 \bmod p$. 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 Sylow p-subgroups of G. By Theorem 6.8, we have $n_p \mid p^n m$ and $n_p \equiv 1 \bmod p$. Since $p \nmid n_p$, we have $n_p \mid m$.

Example

We claim that every group of order 15 is cyclic.
Proof: Let G be a group of order $15 = 3 \cdot 5$. Let n_p be the number of Sylow p-subgroups of G. By Theorem 6.8, we have $n_3 \mid 15$ and $n_3 \equiv 1 \bmod 3$. Thus $n_3 = 1$. Similarly, we have $n_5 \mid 15$ and $n_5 \equiv 1 \bmod 5$. Thus $n_5 = 1$. It follows that there is only one Sylow 3-subgroup and one Sylow 5-subgroup of G, say P_3 and P_5, respectively. Thus $P_3 \lhd G$ and $P_5 \lhd G$ by Corollary 6.6. Since $P_3 \cap P_5$ is a subgroup of P_3 and P_5, then $|P_3 \cap P_5| \mid |P_3|$ and $|P_3 \cap P_5| \mid |P_5|$. But $|G| = 5^1 \times 3^1$, where $\gcd(3, 5) = 1$ and $3, 5$ are both prime, so by Theorem 6.5, G contains a subgroup of order 3 and of order 5. So $|P_3 \cap P_5| \mid 3$ and $|P_3 \cap P_5| \mid 5$. Thus $|P_3 \cap P_5| = 1$ and $P_3 \cap P_5 = \{1\}$. Also, $|P_3 P_5| = 15 = |G|$. Thus $G \cong P_3 \times P_5 \cong \mathbb{Z}_3 \times \mathbb{Z}_5 \cong \mathbb{Z}_{15}$. □

Exercise 6.2.1

Construct a cyclic group of order > 100.

Example

We claim that there are two isomorphism classes of group of order 21.
Proof: Let G be a group of order 21. $21 = 3 \times 7$. Let n_p be the number of Sylow p-groups of G. By the 3rd Sylow Theorem, we have $n_3 \mid 7$ and $n_3 \equiv 1 \bmod 3$. Thus $n_3 \in \{1, 7\}$. Also, we have $n_7 \mid 3$ and $n_7 \equiv 1 \bmod 7$. 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

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

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

1. If $i = 1$, then $yxy^{-1} = x$, ie: $yx = xy$. Thus G is an abelian group. Since $P_3 \lhd G$, $P_7 \lhd G$, $P_3 \cap P_7 = \{1\}$ and $|G| = |P_3P_7|$, 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 $G = \{x^iy^i : 0 \leq i \leq 6, 0 \leq j \leq 2, yxy^{-1} = x^2\}$
3. If $i = 4$, then $yxy^{-1} = x^4$. Note that $y^2xy^{-2} = y(yxy^{-1})y^{-1} = yx^4y^{-1} = x^{16} = x^2$.

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

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 $(gh)^m = g^mh^m = 1$ and $gh \in G^{(m)}$. Finally, if $g \in G^{(m)}$, we have $\left(g^{-1}\right)^m = g^{-m} = \left(g^m\right)^{-1} = 1$ 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:

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 $1 = mx + ky$. Now, if $g \in G^{(m)} \cap G^{(k)}$, then $g^m = 1 = g^k$. We have $g = g^{mx+ky} = (g^m)^x \left(g^k\right)^y = 1^x 1^y = 1$. So $G^{(m)} \cap G^{(k)} = \{1\}$. Moreover, 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 these two facts, by Theorem 3.13, we have $G \cong G^{(m)} \times G^{(k)}$.
2. Write $\left|G^{(m)}\right| = m'$ and $\left|G^{(k)}\right| = k'$. By (1), we have $mk = |G| = m'k'$. We claim that $\gcd(m,k') = 1$. Suppose for the sake of contradiction 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 $g^m = (g^p)^{\frac{m}{p}} = 1$, ie: $g \in G^{(m)}$. 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 $k = k'$.

□

Theorem 7.3 **Primary Decomposition Theorem**

Let G be a finite abelian group with $|G| = p_1^{n_1} \ldots p_k^{n_k}$, where $p_1, \ldots, p_k$ are distinct primes and $n_1, \ldots, n_k \in \mathbb{N}$. Then we have
1. $G \cong G^{(p_1)^{n_1}} \times \ldots \times G^{(p_k)^{n_k}}$.
2. $\left|G^{(p_i)^{n_i}}\right| = (p_i)^{n_i}$ $(1 \leq i \leq k)$.

Example

Let $G = \mathbb{Z}_{13}^*$. Then $|G| = 12 = 2^2 \times 3$. Note that
$G^{(3)} = \{a \in \mathbb{Z}_{13}^* : a^3 = 1\} = \{1, 3, 9\}$ (see Piazza)
$G^{(4)} = \{a \in \mathbb{Z}_{13}^* : a^4 = 1\} = \{1, 5, 8, 12\}$ (see Piazza Exercise)
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

Remark

We have seen that if $|G| = p$ (a prime), $G \cong C_p$. Also, if $|G| = p^2$, then $G \cong C_{p^2}$ or $C_p \times C_p$.
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 is not cyclic, then G has at least two subgroups of order p.

Proof: Let $y \in G$ be of maximal order, ie: $o(y) \geq o(x)$ for all $x \in G$.
Claim: $G = \langle y \rangle$.
Proof: Suppose that $G \neq \langle y \rangle$. Then the quotient group $G/\langle y \rangle$ is a non-trivial 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 maximal order, we have proved that $o(x^p) < o(x) \leq o(y) = o(y^m) = o(x^p)$, 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 maximal order. Then there exists a subgroup B such that $G = CB$ and $C \cap B = \{1\}$.

Proposition 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 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 group $C_1, \ldots, C_k$ until we get $B_k = \{1\}$ for some $k \in \mathbb{N}$. Then $G \cong C_1 \times \ldots \times C_k$. □

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.

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

If G is a finite abelian group, then $G \cong \mathbb{Z}_{(p_1)^{n_1}} \times \ldots \times \mathbb{Z}_{(p_k)^{n_k}}$, 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 $p_i^{n_i}$ for $1 \leq i \leq k$. Note that p_i are not necessarily distinct. The numbers $p_i^{n_i}$ are uniquely determined up to their order.

Note

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, we get the following theorem:

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

Let G be a finite abelian group. Then $G \cong \mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2} \times \ldots \times \mathbb{Z}_{n_r}$, where $n_i \in \mathbb{N}, n_1 > 1$ and $n_1 \mid n_2 \mid \ldots \mid n_r$.

Example

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 $G \cong \mathbb{Z}_{2^4} \times \mathbb{Z}_3 \cong \mathbb{Z}_{48}, G \cong \mathbb{Z}_{2^3} \times \mathbb{Z}_2 \times \mathbb{Z}_3 \cong \mathbb{Z}_2 \times \mathbb{Z}_{24}, G \cong \mathbb{Z}_{2^2} \times \mathbb{Z}_{2^2} \times \mathbb{Z}_3 \cong. \mathbb{Z}_{2^2} \times \mathbb{Z}_{12}, G \cong \mathbb{Z}_{2^2} \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3 \cong \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_{12}, G \cong \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3 \cong \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_6$
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 we have

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

The ring is called a **commutative ring** if it also satisfies

1. $ab = ba$

Example

$\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ are commutative rings with the zero being 0 and the unity being 1.

Example

For $n \in \mathbb{N}$ with $n \geq 2$, $\mathbb{Z}_n$ is a commutative ring with the zero being $[0]$ and the unity being $[1]$.

Example

For $n \in \mathbb{N}$ with $n \geq 2$, the set $M_n(\mathbb{R})$ is a ring using matrix addition and matrix multiplication with the zero being the zero matrix and the unity being the identity matrix. Note that $M_n(\mathbb{R})$ is not commutative.

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 $x = y$.

Note

Given a ring R, to distinguish the difference between multiples in addition and in multiplication, for $n \in \mathbb{N}$ and $a \in \mathbb{R}$, we write $na = a + a + ... + a$ (n times addition) and $a^n = a \cdot a...a$ (n-times multiplication)

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 in R, we have $0 \cdot a = 0, 1 \cdot a = a$ and $-(-a) = a$.

Definition 8.1.2

For $n \in \mathbb{N}$, we define $(-n)a = (-a) + ... + (-a)$ (n times). Also, we define $a^0 = 1$. If the multiplicative inverse of a exists, say a^{-1}, ie: $a \cdot a^{-1} = 1 = a^{-1} \cdot a$, we define $a^{-n} = \left(a^{-1}\right)^n$. Also, since $(R, +)$ is an additive group, then by Proposition 1.3, 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 $r, s \in R$. Then

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

Proof:

1. If 0 is the zero of R, we have $0r = (0 + 0)r = 0r + 0r$, so
$$0r - 0r = (0r + 0r) - 0r = 0r + (0r - 0r) \implies 0 = 0r$$
Similarly, $0 = r0$, so $0r = 0 = r0$, as required.
2. $0 = 0s = (r + (-r))s = rs + (-r)s$, so $-(rs) = (-r)s$. Similarly, $0 = r0 = r(s + (-s)) = rs + r(-s)$, so $-(rs) = r(-s)$. Hence, $(-r)s = r(-s) = -(rs)$, as required.
3. $0 = 0(-s) = (r + (-r))(-s) = r(-s) + (-r)(-s) = -(rs) + (-r)(-s)$, so $rs = -(-(rs)) = (-r)(-s)$. Hence, $(-r)(-s) = rs$, as required.
4. $(mr)(ns) = \left(\underbrace{r + r + ... + r}_{m \text{ times}}\right)\left(\underbrace{s + s + ... + s}_{n \text{ times}}\right) = (mn)(rs)$.

□

Definition 8.1.3

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 $r = r \cdot 1$ for all $r \in R$, we have $1 \neq 0$ (otherwise, $r = r1 = r0 = 0$ by Prop 8.1 for all $r \in R$).

Example

Let $R_1, R_2, ..., R_n$ be rings. We define componentwise operations in the product $R_1 \times R_2 \times ... \times R_n$ as follows:

1. $(r_1, r_2, ..., r_n) + (s_1, ..., s_n) = (r_1 + s_1, ..., r_n + s_n)$
2. $(r_1, r_2, ..., r_n) \cdot (s_1, ..., s_n) = (r_1 s_1, ..., r_n s_n)$

One can check that $R_1 \times ... \times R_n$ is a ring with the zero being $\left(0_{R_1}, 0_{R_1}, ..., 0_{R_n}\right)$ and the unity being $\left(1_{R_1}, ...1_{R_n}\right)$ (exercise). This set $R_1 \times ... \times R_n$ is called the **direct product** of $R_1, ..., R_n$.

Definition 8.1.4

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

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

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

$$\begin{aligned} kr &= k(1_R r) \ (\text{since } 1_R r = r \ \forall r \in R) \\ &= (k \cdot 1)(1_R \cdot r) \ (\text{since } k \cdot 1 = k \ \forall k \in \mathbb{Z}) \\ &= (k \cdot 1_R)(1 \cdot r) \ (\text{by Prop 8.1(4)}) \\ &= (k1_R)r \ (\text{since } 1 \cdot r = r \ \forall r \in R) \end{aligned}$$

Thus, $kR = 0 \implies k1_R = 0$ (since $1_R \in R$) and $k1_R = 0 \implies kr = 0r = 0$. So

$$kR = 0 \iff k1_R = 0$$

.

Proposition 8.2

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

1. If $\mathrm{ch}(R) = n \in \mathbb{N}$, then $kR = 0$ if and only if $n \mid k$.
2. If $\mathrm{ch}(R) = 0$, then $kR = 0$ if and only if $k = 0$.

Proof:

1. If $\text{ch}(R) = n \in \mathbb{N}$, then $o(1_R) = n$. But in a group G with $o(g) = n \in \mathbb{N}$ for some $g \in G$, by Proposition 2.7, we have that $g^k = 1_G \iff n \mid k$. But $(R, +)$ is a group, so in particular, $k1_R = 0 \iff n \mid k$. But $k1_R = 0 \iff kR = 0$, so $kR = 0$ if and only if $n \mid k$, as required.
2. If $\text{ch}(R) = 0$, then $o(1_G) = \infty$. But in a group G with $o(g) = \infty$ for some $g \in G$, by Proposition 2.8, we have that $g^k = 1_G \iff k = 0$. In particular, $k1_R = 0 \iff k = 0$. But $k1_R = 0 \iff kR = 0$, so $kR = 0$ if and only if $k = 0$, as required.

□

Example

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 **Subring**

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 $(2), (5), (7)$ and (9) of a ring are automatically satisfied.

Definition 8.2.2 **Subring Test**

To show that S is a subring, it suffices to show

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

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

Example

We have a chain of commutative rings $\mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R} \subseteq \mathbb{C}$.

Example

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

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

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

$$(s-t)r = sr - tr = r(s-t)$$

and

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

So $Z(R)$ is a subring of R.

Example

Let $\mathbb{Z}[i] = \{a + bi : a, b \in \mathbb{Z} \wedge i^2 = -1\} \subseteq \mathbb{C}$. 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 $R/A = \{r + A : r \in R\}$ with $r + A = \{r + a : a \in A\}$. 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. $r + A = s + A$ if and only if $r - s \in A$.
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 $k \in \mathbb{Z}$.

Note

Since R is a ring, it is natural to ask if we could make R/A to be a ring. A natural way to define multiplication in R/A is that $(r+A)(s+A) = rs + A$ for all $r, s \in R$ $(*)$. 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 the 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

$$Ra = \{ra : r \in R\}$$

and

$$aR = \{ar : r \in R\}$$

The following are equivalent:

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

Proof:
$(1) \Rightarrow (2)$. 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 $s - s_1 \in A$, then by (1), we have

$$\begin{aligned} rs - r_1 s_1 &= rs - r_1 s + r_1 s - r_1 s_1 \\ &= (r - r_1)s + r_1(s - s_1) \\ &\in (r - r_1)R + R(s - s_1) \\ &\subseteq A \end{aligned}$$

By Prop 8.3, we have $rs + A = r_1 s_1 + A$.
$(2) \Rightarrow (1)$ Let $r \in R$ and $a \in A$. By Prop 8.3 and 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 **Ideal Test**

An additive subgroup A of a ring R is an ideal of R if for all $a \in A$, $Ra \subseteq A$ and $aR \subseteq A$. We define an **Ideal Test** to determine if a subset $A \subseteq R$ is an ideal of R:

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

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

Example

Let R be a commutative ring and $a_1, ..., a_n \in R$. Consider the set I generated by $a_1, ..., a_n$, ie: $I = \langle a_1, ..., a_n \rangle = \{r_1 a_1 + ... + r_n a_n : r_i \in R\}$. 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 $R = A$. □

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 $A = aR = \{ar : r \in R\} = Ra$ for some $a \in R$, we say A is a **principal ideal** generated by a, and is denoted by $A = \langle a \rangle$.

Example

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

Proposition 8.7

All ideals of $\mathbb{Z}$ are of them form $\langle n \rangle$ 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 $0 \leq r \leq |a|$. 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 $b = qa$, ie $b \in \langle a \rangle$. It follows that $A = \langle a \rangle$. □

8.4 Isomorphism Theorems

Definition 8.4.1

Let R and 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

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

Example

If R_1 and R_2 are rings, the projection $\pi_1 : R_1 \times R_2 \to R_1$ is defined by $\pi_1(r_1, r_2) = r_1$ is a surjective homomorphism. Similarly, $\pi_2 : R_1 \times R_2 \to R_2$ defined by $\pi_2(r_1, r_2) = r_2$ is also a surjective ring homomorphism.

Proposition 8.8

Let $\theta : R \to S$ be a ring homomorphism and let $r \in R$.

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 of R which has the multiplicative inverse), where such a is called a unit of R, then $\theta\left(u^k\right) = \theta(u)^k$ for all $k \in \mathbb{Z}$

Definition 8.4.2

A mapping of a ring $\theta : R \to S$ is a ring isomorphism if θ is a homomorphism and θ is bijective. In this case, we say R and S are isomorphic, denoted as $R \cong S$.

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 $se = es$ 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

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

and the image of θ is defined by

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

Remark

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:

1. Since $\operatorname{im} \theta = \theta(R)$ is an additive subgroup of S, it suffices to show that $\theta(R)$ is closed under the 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.
2. Since $\ker \theta$ is an additive subgroup of R, it suffices to show that $ra, ar \in \ker \theta$ for all $r \in R$ and $a \in \ker \theta$. If $r \in R$ and $a \in \ker \theta$, then $\theta(ra) = \theta(r)\theta(a) = \theta(r)0 = 0$. 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 for Rings**

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, then R/A is a ring. Define the ring map $\overline{\theta} : R/A \to \operatorname{im} \theta$ by $\overline{\theta}(r + A) = \theta(r)$ for all $r + A \in R/A$. Note that

$$r + A = s + A \Leftrightarrow r - s \in A \Leftrightarrow \theta(r - s) = 0 \Leftrightarrow \theta(r) = \theta(s)$$

Thus $\overline{\theta}$ is well-defined and injective. Also, $\overline{\theta}$ is clearly surjective. One can show that $\overline{\theta}$ is a ring homomorphism (exercise). It follows that $\overline{\theta}$ is a ring isomorphism and $\operatorname{im} \theta \cong R/\ker \theta$.

□

Notation

Let A and B be two 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 (exercise). To consider the smallest subring of R containing both A and B (where A and B are not necessarily rings), we define the sum $A + B$ to be

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

One can show (see Piazza)

Proposition 8.11

If R is a ring, then we have

1. If A and B are two 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.

Theorem 8.12 **Second Isomorphism Theorem for Rings**

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 for Rings**

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 be 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

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 and 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) is a direct consequence of (1). Thus, it suffices to prove (1). Define $\theta : R \to R/A \times R/B$ by $\theta(r) = (r + A, r + B)$ for all $r \in R$. Then θ is a ring homomorphism (exercise) 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 $A + B = R$, then there exists $a \in A$ and $b \in B$ with $a + b = 1$. let $r = sb + ta$. Then

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

Thus $s + A = r + A$. Similarly, we have $t + B = r + B$. But $\theta(r) = (r + A, r + B)$. Thus $\mathrm{im}(\theta) = R/A \times R/B$. By the First Isomorphism Theorem, we have

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

□

Example

Note that CRT works on $R = \mathbb{Z}$. Let $m, n \in \mathbb{N}$ with $\gcd(m, n) = 1$. By Bezout'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 $m\mathbb{Z} \cap n\mathbb{Z} = (mn)\mathbb{Z}$.

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 $\gcd(m, n) = 1$, then $\varphi(mn) = \varphi(m)\varphi(n)$, where $\varphi(m) = |\mathbb{Z}_n^*|$ is the Euler φ-function.

Proof:

1. Let $R = \mathbb{Z}$, $A = m\mathbb{Z}$ and $B = n\mathbb{Z}$. Then by the above example and by CRT, we have $\mathbb{Z}/(mn)\mathbb{Z} \cong \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$, which is equivalent to $\mathbb{Z}_{mn} \cong \mathbb{Z}_m \times \mathbb{Z}_n$.
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 Corollary 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 $\mathbb{Z}_n$ 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 Chinese Remainder Theorem 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's Theorem, $o(1_R) = 1$ or p. Since $1_R \neq 0$, we have $o(1_R) = p$. Thus, $[k] = [m] \iff p \mid (k-m) \iff (k-m)1_R = 0_R \iff k1_R = m1_R$ in R. Thus θ is well-defined and injective. Since $|\mathbb{Z}_p| = p = |R|$ and θ is injective, then θ is surjective. Finally, one can prove that θ is a ring homomorphism (exercise). 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 $|R| = p^2$ for prime p?

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

$$ur = us \Rightarrow r = s$$

and

$$ru = su \Rightarrow r = s$$

Let R^* be the set of all units in R. One can show $(R^*, \cdot)$ is a group (exercise) called the **group of units** of R.

Example

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

Exercise 9.1.1

Consider the ring of Gaussian integers $\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z} \wedge i^2 = 1\} \subseteq \mathbb{C}$. One can show that $\mathbb{Z}[i]^* = \{\pm 1, \pm i\}$.

Note

Define the norm $N(a + bi) = a^2 + b^2$. Prove that $N(xy) = N(x)N(y)$ and $N(x) = 1$ if and only if x is a unit.

Definition 9.1.2

A ring $R \neq \{0\}$ is a **division ring** if $R^* = R \setminus \{0\}$, ie: every non-zero element of R is a unit in R. A commutative division ring is a **field**.

Example

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

Example

We recall that the equation $[a][x] = [1]$ in $\mathbb{Z}_n$ has a solution if and only if $\gcd(a, n) = 1$. Thus, if $n = p$ is a prime, then $\gcd(a, p) = 1$ for all $a \in \{1, 2, ..., p-1\}$. Thus, $\mathbb{Z}_p^* = \mathbb{Z}_p \setminus \{0\}$. So $\mathbb{Z}_p$ is a field. However, if n is not prime, say $n = ab$ with $1 < a, b < n$. Then the non-zero 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 if and only if n is 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 θ from a field F to a ring S, since $\ker\theta$ is an ideal, $\ker\theta = \{0\}$ or F. Hence θ is either injective or a zero map.

Exercise 9.1.2 **Wedderburn's Little Theorem**

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 $x^2 - x - 6 = 0 \iff (x-3)(x-2) = 0 \implies x = 3 \vee x = 2$.
However, this 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 $[(x-3)(x-2)] = [0]$ 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 $0 \neq b$ such that $ab = 0$.

Example

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

Example

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

Proof: We prove $(1) \iff (2)$ and the poof of $(1) \iff (3)$ is similar.
$(1) \Rightarrow (2)$ Let $ab = ac$ with $a \neq 0$. Then $a(b - c) = 0$. By (1), since $a \neq 0$, we have $b - c = 0$, ie $b = c$.
$(2) \Rightarrow (1)$ 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 divisor, ie if $ab = 0$ in R, then $a = 0$ or $b = 0$.

Example

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

Example

If p is a prime, then $p \mid ab$, then $p \mid a$ or $p \mid b$, ie: $[a][b] = [0]$ 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 if and only if 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 $a = 0$ or $b = 0$. Two cases:

1. If $a = 0$, then we are done.
2. If $a \neq 0$, then since R is a field, $a \in R^*$, and $a^{-1} \in R$ exists. Then $b = 1b = (a^{-1}ab) = a^{-1}(ab) = a^{-1}0 = 0$. Thus R is an integral domain.

□

Remark

1. Using the above proof, one can show that every subring of a field is an integral domain.
2. The converse of Prop 9.2 is not true. For example, $\mathbb{Z}$ is an integral domain, but not a field.

Example

The Gaussian ring $\mathbb{Z}[i]$ 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 $a \in R$ with $a \neq b$. Consider the map $\theta : R \to R$ defined by $\theta(r) = ar$. Since R is an integral domain, $ar = as$ and $a \neq 0$ implies that $r = s$. Hence, θ is injective. Since R is finite, then θ is also surjective. In particular, there exists $b \in R$ such that $ab = 1$. Since R is commutative, we have $ab = 1 = ba$, ie 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 $\mathrm{ch}(R) = 0$, 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 $a, b \in \mathbb{R}$, we have

$$(a+b)^p = a^p + \binom{p}{1}a^{p-1}b + \ldots + \binom{p}{p-1}ab^{p-1} + b^p$$

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

Recall

Let p be a prime and $a, b \in \mathbb{Z}$. We recall in 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

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

Example

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 a 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

P is a prime ideal $\iff rs \in P$ implies that $r \in S$ or $s \in P$
$\iff (r+P)(s+P) = 0+P$ implies that $r+P = 0+P$
or $s+P = 0+P$
$\iff R/P$ is an integral domain

□

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 $r \notin M$ if and only if $r+M \neq 0+M$. Thus, we have

M is a max ideal $\iff \langle r \rangle + M = R$ for all $r \notin M$
$\iff 1 \in \langle r \rangle + M$ for all $r \notin M$
$\iff$ for all $r \notin M$, there exists $s \in R$ s.t $1+M = rs+M$
$\iff \forall r+M \neq 0+M$, there exists $s+M \in R/M$ s.t
$(r+M)(s+M) = 1+M$
$\iff R/M$ is a field

□

Corollary 9.7 **of Prop 9.2 & Prop 9.5 & Prop 9.6**

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

Remark

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

Example

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 $\theta(a+bx) = a+bi$. One can check that the kernel of the map is $\langle x^2+1\rangle$ (exercise). 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 $\mathbb{Z}[x]/\langle x^2+1, 3\rangle \cong \mathbb{Z}_3[x]/\langle x^2+1\rangle \cong \mathbb{F}_9$ (a field of order 9).

9.3 Fields of Fractions

Definition 9.3.1

Let R be an integral domain. We now construct a field F of all **fractions** r/s from R. Let R be an integral domain and let $D = R \setminus \{0\}$. Consider the set $X = R \times D = \{(r,s) : r \in R \wedge s \in D\}$. We say $(r,s) \equiv (r_1, s_1)$ on X if and only if $rs_1 = r_1 s$. One can show that $\equiv$ is an equivalence relation (exercise). Motivated by the case $R = \mathbb{Z}$, we 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, ie:

$$F = \left\{\frac{r}{s} : r \in R \wedge s \in D\right\} = \left\{\frac{r}{s} : rs \in R \wedge s \neq 0\right\}$$

The addition and multiplication of F are defined by $\frac{r}{s} + \frac{r_1}{s_1} = \frac{rs_1 + r_1 s}{ss_1}$ and $\frac{rr_1}{ss_1} = \frac{rr_1}{ss_1}$, where $ss_1, rs_1 + r_1 s, rr_1 \in R$. Note that $ss_1 \neq 0$ since R is an integral domain and thus these operations are well-defined. Then one can show that (exercise) 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 $\frac{r}{s} = \frac{-r}{s}$. Moreover, if $\frac{r}{s} \neq 0$ in F, then $r \neq 0$ and thus $\frac{s}{r} \in F$ and we have $\frac{r}{s}\frac{s}{r} = \frac{rs}{sr} = \frac{rs}{rs} = \frac{1}{1} \in F$. In addition, we have $R \cong R'$, where $R' = \left\{\frac{r}{1} : r \in R\right\} \subseteq F$.

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 is called the **field of fractions of R**.

10 Polynomial Rings

10.1 Polynomials

Definition 10.1.1

Let R be a ring and x a variable. Let $R[x] = \{f(x) = a_0 + a_1x + ... + a_mx^m : m \in \mathbb{N} \cup \{0\} \wedge a_i \in R \ \forall 0 \leq i \leq m\}$. 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 that a_m is the **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 $f(x) = 0 \iff a_0 = 0, a_1 = 0, a_2 = 0, ... 0$ is also a constant polynomial and we define $\deg 0 = \infty$. Let $f(x) = a_0 + a_1x + ... + a_{m-1}x^{m-1} + a_mx^m \in R[x]$ and $g(x) = b_0 + b_1 + ... + b_nx^n \in R[x]$ with $m \leq n$. Then we write $a_i = 0$ for all $(m+1) \leq i < n$. We can define addition and multiplication on $R[x]$ as follows:

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

and

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

where $c_i = a_0b_i + a_1 + b_{i-1} + ... + a_{i-1}b_1 + a_ib_0$.

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 $Z = Z(R)$ denotes the center of R, then $Z(R[x]) = Z[x]$.

***Proof*:**

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

   $$f(x)g(x) = c_0 + c_1x + ... + c_{m+n}x^{m+n}$$

   with $c_i = a_0b_i + a_1b_{i-1} + ... + a_{i-1}b_1 + a_ib_0$. 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 $h(x) = c_0 + c_1x + ... + c_sx^s \in Z(R[x])$, then for all

$r \in R$, we have $h(x)r = rh(x)$. Thus, $c_i r = rc_i$ for all $r \in R$ and $0 \leq i \leq s$. 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 $\mathbb{R}$ to $\mathbb{R}$, the polynomial is not the same as the function it defines. For example, if $R = \mathbb{Z}_2$, there are only 4 different function from $\mathbb{Z}_2$ to $\mathbb{Z}_2$ (since there are 2 elements in the domain and 2 in the codomain). 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 $\deg(fg) = \deg(f) + \deg(g)$ (product formula).
3. The units in $R[x]$ are R^*, the units in R.

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

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

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.
For (3), let $u(x) \in R[x]$ be a unit with the 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, $u(x)$ and $v(x)$ are units in R and hence $R[x]^* \subseteq R^*$. Since $R^* \subseteq R[x]^*$. We have $R[x]^* \subseteq R^*$. □

Remark

Note that in $\mathbb{Z}_4(x)$, we have $2x \cdot 2x = 4x^2 = 0$. Thus

$$2 = 1 + 1 = \deg(2x) + \deg(2x) \neq \deg(2x \cdot 2x) = 0$$

Hence, the product formula in Prop 10.2 only applies when R is 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 and $f(x), g(x), h(x) \in F[x]$.

1. If $f(x) \mid g(x)$ and $g(x) \mid h(x)$, then $f(x) \mid h(x)$ (Transitivity of Divisibility (TD)).
2. If $f(x) \mid g(x)$ and $f(x) \mid h(x)$, then $f(x) \mid (g(x)u(x) + h(x)v(x))$ for any $u(x), v(x) \in F[x]$ (Divisibility of Integer Combination (DIC)).

Recall

For $a, b \in \mathbb{Z}$, if $a \mid b$ and $b \mid a$ and a, b are positive, then $a = b$. The following is its analog 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 exists unique $q(x), r(x) \in F[x]$ such that

$$g(x) = q(x)f(x) + r(x)$$

with $\deg(r) < \deg(f)$.

Note

The above proposition includes the case for $r = 0$, which 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 $f(x) = a_0 + a_1 x + ... + a_m x^m$ with $a_m \neq 0$ and $g(x) = b_0 + b_1 x + ... + b_n x^n$. Since F is a field, then a_m^{-1} exists. Consider

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

Since $\deg(g_1) < n$, by induction, there exists $q_1(x), r_1(x) \in F[x]$ 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 $q(x) = q_1(x) + b_n a_m^{-1} + b_n a_m^{-1} x^{n-m}$ and $r(x) = r_1(x)$. We have $g(x) = q(x) f(x) + r(x)$ 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 have

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

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 $r_1(x) = r(x)$. □

Recall

For $a, b \in \mathbb{Z} \setminus \{0\}$, the Bezout 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 $g(x)$, denoted 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 non-zero 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 field, then 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 that $d(x) \mid g(x)$. 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 $l(x) \neq 0$ in $F[x]$ is **irreducible** if $\deg(l) \geq 1$ and whenever $l(x) = l_1(x)l_2(x)$ in $F[x]$, we have $\deg(l_1) = 0$ or $\deg(l_2) = 0$ ($\deg(0)$ polynomials are the units in $F[x]$). Polynomials that are not irreducible are **reducible**.

Example

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

Example

If $\deg(f) \in \{2, 3\}$, then f is irreducible if and only if $f(d) \neq 0$ for all $d \in F$ (See A10).

Example

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

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 $l(x) \in F[x]$ is irreducible and $l(x) \mid f(x)g(x)$, then $l(x) \mid f(x)$ or $l(x) \mid g(x)$.

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

1. If $l(x) \mid f(x)$, then we are done.
2. If $l(x) \nmid f(x)$, then $d(x) = \gcd(l(x), f(x)) = 1$. By Prop 10.6, we have $1 = l(x)u(x) + f(x)v(x)$ for some $u(x), v(x) \in F[x]$. Then $g(x) = g(x)l(x)u(x) + g(x)f(x)v(x)$. Since $l(x) \mid l(x)$ and $l(x) \mid g(x)f(x)$, then by Prop 10.3, we have $l(x) \mid g(x)$.

□

Remark

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

Note

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

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 $f(x) = cl_1(x)...l_n(x)$, where $c \in F^*$ and $l_i(x)$ are monic, irreducible polynomials (but not necessarily distinct). The Factorization is unique up to the order of l_i.

Exercise 10.2.1

Use Theorem 10.8 to prove that 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 them 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 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, then by Prop 10.4, we have $h(x) = h_1(x)$. □

Recall

In $\mathbb{Z}$, all ideals are of the form $\langle n\rangle$ for $n \in \mathbb{Z}$. For $n \geq 2$, if we divide an integer by n, the remainder $r \in \{0, 1, 2, ..., (n-1)\}$. Write $\langle n\rangle = n\mathbb{Z}$. Then we have $\mathbb{Z}_n = \mathbb{Z}/\langle n\rangle = \{0 + \langle n\rangle, 1 + \langle n\rangle, ..., (n-1) + \langle n\rangle\} = \{[0], [1], ..., [n-1]\}$. We now consider an analog in $F[x]$.

Note

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

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

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 (exercise)

$$R = \{\overline{a_0} + \overline{a_1}t + ... + \overline{a_{n-1}}t^{n-1} \mid a_i \in F \text{ and } h(t) = 0\}$$

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 $\ker(\theta) = \{0\}$. Then θ is an injective ring homomorphism. Since $F \cong \theta(F)$, by identifying F with $\theta(F)$, we have

$$R = \{a_0 + a_1t + ... + a_{m-1}t^{m-1} \mid a_i \in F \text{ and } h(t) = 0\}$$

Note

In R, we have

$$a_0 + a_1 t + \ldots + a_{m-1} t^{m-1} = b_0 + b_1 t + \ldots + b_{m-1} t^{m-1}$$

if and only if $a_i = b_i$ for all $0 \leq i \leq (m-1)$. Hence, this representation of the elments of R is unique.

Proposition 10.10

Let F be a field and $h(x) \in F[x]$ be monic 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

$$R = \{a_0 + a_1 t + \ldots + a_{m-1} t^{m-1} \mid a_i \in F \text{ and } h(t) = 0\}$$

in which an element of R can be uniquely represented in the above form.

Example

Consider the ring $R[x]$. Let $h(x) = x^2 + 1 \in \mathbb{R}[x]$. By Prop 10.10, we have

$$\begin{aligned} \mathbb{R}[x]/\langle x^2 + 1 \rangle &= \{a + bt : a, b \in R \text{ and } t^2 + 1 = 0\} \\ &\cong \{a + bi : a, b \in R \text{ and } i^2 = -1\} \\ &\cong \mathbb{C} \end{aligned}$$

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 an integral domain.
3. $h(x)$ is irreducible in $F[x]$.

Example

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

Since $x^2 + x + 1$ has no roots in $\mathbb{Z}_2$ (since 0 and 1 are not roots), it is irreducible in $\mathbb{Z}_2[x]$. Thus, $\mathbb{Z}_2[x]/\langle x^2 + x + 1 \rangle = \{a + bt : a, b \in \mathbb{Z}_2 \text{ and } t^2 + t + 1 = 0\}$ is a field of 4 elements.

Proof of Prop 10.11: Write $A = \langle h(x) \rangle$.
(1) $\implies$ (2) A field is an integral domain.
(2) $\implies$ (3) If $h(x) = f(x)h(x)$ with $f(x), g(x) \in F[x]$, then

$$(f(x) + A)(g(x) + A) = f(x)g(x) + A = h(x) + A = 0 + A$$

in $F[x]/A$. By 2, either $f(x) = A = 0 + A$ or $g(x) + A = 0 + A$, ie 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 $\deg(g) = 0$. Similarly, if $g(x) \in A$, then $\deg(f) = 0$. Thus $h(x)$ is indeed in $F[x]$.
(3) $\implies$ (1) Note that $F[x]/A$ is a commutative ring. Thus, to show that it is a field, it suffices to show that every non-zero 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 $h(x) + f(x)$ is too, we have $\gcd(f(x), h(x)) = 1$. By Prop 10.6, there exists $u(x), v(x) \in F[x]$ such that $1 = u(x)h(x) + v(x)f(x)$. Thus,

$$(v(x) + A)(f(x) + A) = 1 + A \text{ (since } A = \langle h(x) \rangle)$$

It follows that $f(x) + A$ has an inverse in $F[x]/A$ and hence $F[x]/A$ is a field. □

> **Remark**
>
> Before the previous example, the only finite fields we know are of the form $\mathbb{Z}_p$, where p is prime. We have seen before that there are ∞-many irreducible polynomials in $\mathbb{Z}_p[x]$. Indeed, one can show that for any $n \in \mathbb{N}$, there exists at least one irreducible polynomial of $\deg(n)$ 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 $F[x]$:

Properties	$\mathbb{Z}$	$F[x]$
elements	m	$f(x)$
size	$\lvert m \rvert$	$\deg(f)$
units	$\pm 1; \mathbb{Z} \setminus \{0\}/\{\pm 1\} = \mathbb{N}$	$F^*; F[x] \setminus \{0\}/F^* = \{\text{monic polynomials}\}$
unique factorization	$m = \pm 1 p_1^{\alpha_1} ... p_n^{\alpha_n} = p_i = \text{prime}$	$f = c \cdot l_1^{\alpha_1} ... l_r^{\alpha_r}, c \in F^*, l_i = l_i(t) = \text{monic irreducible}$
ideals	$\langle n \rangle$ (unique if $n \in \mathbb{N}$)	$\langle h(x) \rangle$ (unique if $h(x)$ is monic)
more ideals	$\mathbb{Z}/\langle n \rangle$ is a field iff n is prime	$F[x]/\langle h(x) \rangle$ is a field iff $h(x)$ is irreducible

10.3 Fermat's Last Theorem in $F[x]$

Example

The triples $(x, y, z) = (3, 4, 5)$ and $(5, 12, 13)$ are positive integer solutions.

Lemma 10.12 **Euclid's Formula**

For $a, b \in \mathbb{N}$ with $a > b$, we can take $x = a^2 - b^2, y = 2ab, z = a^2 + b^2$. Then take the triple (x, y, z) satisfies $x^2 + y^2 = z^2$ and we have infinitely many positive integer solutions.

Note

How about positive integer solutions for $x^n + y^n = z^n$ with $n \in \mathbb{N}$ and $n \geq 3$?

Theorem 10.13 **Fermat's Last Theorem**

For $n \in \mathbb{N}$ with $n \geq 3$, the equations $x^n + y^n = z^n$ have no solution with $x, y, z \in \mathbb{N}$.

Note

1. The result was first claimed by Fermat in the mid 17th century without proof.
2. The theorem was proved by Frey, Serre, Ribet, Tayler and Wiles in 1994.
3. The proof involves the use of elliptic curves, modular forms and Galois representations.

Example

Let F be a field and $n \in \mathbb{N}$. Consider

$$f^n(x) = g^n(x) = h^n(x)$$

with $f(x), g(x), h(x) \in F[x]$. We say a solution (f, g, h) is **non-trivial** if $\deg(f), \deg(g), \deg(h) \geq 1$.

Theorem 10.14

Let F be a field with $\mathrm{ch}(F) = 0$. For $n \in \mathbb{N}$ with $n \geq 3$, there is no non-trivial solutions for the equation

$$f^n(x) + g^n(x) = h^n(x)$$

with $f(x), g(x), h(x) \in F[x]$.

Proof: Suppose we have a non-trivial solution $f^n + g^n = h^n$. By dividing all common divisors of f, g, h, we can suppose that (f, g, h) is "coprime", ie

$$\gcd(f, g) = \gcd(f, h) = \gcd(g, h) = 1$$

Without loss of generality, suppose

$$\deg(f) + \deg(h) \geq \deg(g)$$

Write $f' = \frac{df}{dx}$. Since $f^n + g^n = h^n$, by the chain rule, we have

$$nf^{n-1}f' + ng^{n-1}g' = nh^{n-1}h'$$

Since $\mathrm{ch}(F) = 0$, we have $n \cdot 1 \neq 0$. By multiplying both sides by n^{-1}, then h, we get

$$f^{n-1}f'h + g^{n-1}g'h = h^n h' = f^n h' + g^n h'$$

ie:

$$f^{n-1}(f'h - fh') = g^{n-1}(gh' - g'h)$$

Since f and g are coprime, the above equation implies that $f^{n-1} \mid (gh' - g'h)$ Thus $(n-1)\deg(f) \leq \deg(g) + \deg(h) - 1$. Since $\deg(f) = \deg(h) \geq \deg(g)$, we have $(n-2)\deg(g) \leq (n-2)\deg(f) \leq \deg(g) - 1$, which is a contradiction if $n \geq 3$. □

Note

Let p be a prime and consider $\mathbb{Z}_p[x]$. We have

$$(f(x) + g(x))^p = f(x)^p + g(x)^p$$

Let $h(x) = f(x) + g(x)$. Then the equation $f(x)^p + g(x)^p = h(x)^p$ have infinitely many non-trivial solutions.

Theorem 10.15

Let F be a field with $\mathrm{ch}(F) = p$. For $n \in \mathbb{N}$ with $n \geq 3$ and $\gcd(n, p) = 1$, there is no non-trivial solutions for the equation

$$f^n(x) + g^n(x) = h^n(x)$$

with $f(x), g(x), h(x) \in F[x]$.

10.4 Prime Number Theorem and Riemann Hypothesis in $\mathbb{Z}_p[t]$

Define

$$\pi(x) = \#\{p \leq x, p = \text{prime}\}$$

Conjecture:
$\pi(x) \sim \mathrm{li}(x) = \int_2^x \frac{\mathrm{dt}}{\log(t)} \sim \frac{x}{\log x}$.

Hence, the probability of primes $\leq x$ is $\frac{1}{\log x}$. For example, about 1% of $n \in \mathbb{N}$ with $n < e^{100}$ are primes.

Definition 10.4.1

For $s \in \mathbb{C}$, the **Riemann Zeta function** is defined to be

$$\begin{aligned}\zeta(s) &= \sum_{n\in\mathbb{N}} \frac{1}{n^s} \\ &= \prod_{p \text{ prime}} \left(1 + \frac{1}{p^s} + \frac{1}{p^{2s}} + \ldots\right) \\ &= \prod_{p \text{ prime}} \left(1 - \frac{1}{p^s}\right)^{-1}\end{aligned}$$

Remark

1. The **Riemann zeta function** absolutely converges for $\mathrm{Re}(s) > 1$.
2. Functional equation relates $\zeta(s)$ with $\zeta(1-s)$.
3. The analytic continuation involves extending $\zeta(s)$ to $s \in \mathbb{C}$.

Theorem 10.16 **Riemann Hypothesis**

All non-trivial zeros of $\zeta(s)$ lie on $\mathrm{Re}(s) = \frac{1}{2}$.

Theorem 10.17 **Prime Number Theorem**

For any $n \in \mathbb{N}$, we have $\pi(x) = \mathrm{li}(x) + O\left(\frac{x}{(\log x)^n}\right)$.

Theorem 10.18 **Prime Number Theorem with RH**

For any $\varepsilon > 0$, assuming RH, $\pi(x) = \mathrm{li}(x) + O\left(x^{\frac{1}{2}+\varepsilon}\right)$.

Example

Let's consider PNT in $\mathbb{Z}_p[t]$. For $f \in \mathbb{Z}_p[t]$, define $|f| = p^{\deg f}$. For $s \in \mathbb{C}$, the **Zeta function** of $\mathbb{Z}_p[t]$ is defined to be

$$\begin{aligned}\zeta_p(s) &= \sum_{f \text{ monic}} \frac{1}{|f|^s} \\ &= \prod_{\ell\text{: monic \& irreducible}} \left(1 - \frac{1}{|\ell|^s}\right)^{-1}\end{aligned}$$

Note that $\#\{f : \text{monic}, \deg(f) = d\} = p^d$.

$$\zeta_p(s) = \sum_{d=0}^{\infty} \frac{p^d}{(p^d)^s} = \frac{1}{1 - p^{1-s}}$$

1. Functional equation: relate $\zeta_p(s)$ with $\zeta_p(1-s)$.
2. Analytic continuation: extend $\zeta(s)$ to $s \in \mathbb{C}$.

Define $a_d = \#\{\ell : \text{monic irreducible}, \deg(l) = d\}$.
We have

$$\zeta_p(s) = \prod_{d=1}^{\infty} \left(1 - \frac{1}{(p^d)^s}\right)^{-a_d}$$

Write $T = p^{-s}$. Then

$$\zeta_p(s) = \frac{1}{1 - pT} = \prod_{d=1}^{\infty} \left(1 - T^d\right)^{-a_d}$$

Note that

$$\begin{aligned}\log\left(\frac{1}{1-pT}\right)' &= (-\log(1-pT))' \\ &= -\frac{-p}{1-pT} = \frac{p}{1-pT}\end{aligned}$$

By taking log derivatives and multiplying by T, we have

$$\frac{pT}{1-pT} = \sum_{d=1}^{\infty} \frac{d a_d T^d}{1 - T^d}$$

By expanding both sides into power series and comparing the coefficients of T^n, we have

$$p^n = \sum_{d|n} d a_d$$

Definition 10.4.2

The Mobius function on $d \in \mathbb{N}$ is defined as follows:

$$\mu(d) = \begin{cases} 1 \text{ if } d = 1 \\ (-1)^r \text{ if } d \text{ is a product of distinct } r \text{ primes} \\ 0 \text{ otherwise} \end{cases}$$

Theorem 10.19 **Mobius inversion formula**

$$f(n) = \sum_{d|n} g(d) \iff g(n) = \sum_{d|n} \mu(d) f\left(\frac{n}{d}\right)$$

By $*$ and Mobius inversion formula, we have

$$da_d = p^d + O\left(p^{\frac{d}{2}}\right)$$

In other words,

$$a_d = \frac{p^d}{d} + O\left(\frac{p^{\frac{1}{2}}}{d}\right)$$

Define

$$\pi_p(x) = \#\{\ell : \text{monic } \& \text{ irreducible}, |\ell| \leq x\}$$

By the estimates of a_d, we have

$$\pi_p(x) = \frac{p}{p-1} \frac{x}{\log x} + O\left(x^{\frac{1}{2}+\varepsilon}\right)$$

which proves the RH in $\mathbb{Z}_p[t]$.