PMATH 336 Introduction to Group Theory

Keven Qiu
Instructor: Wentang Kuo
Fall 2024

Contents

Chapter 1

Rings, Fields, and Groups

Definition: Cartesian Product

For a set S, we write $S \times S = \{(a, b) : a \in S, b \in S\}$.

Definition: Binary Operation

A binary operation on S is a map $* : S \times S \to S$, where for $a, b \in S$, we denote $*(a, b) = a * b$.

E.g. For $S = \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$, there are $* : \times, +$.

Definition: Ring (With Identity)

A set R together with two binary operations $+$ and $\times$, where for $a, b \in R$, we often write $a \times b = a \cdot b = ab$ and $a + b$ and two distinct elements 0 and 1, such that

1. $+$ is associative: $(a + b) + c = a + (b + c)$ for all $a, b, c \in R$
2. $+$ is commutative: $a + b = b + a$ for all $a, b \in R$
3. 0 is an additive identity: $0 + a = a$ for all $a \in R$
4. Every element has an additive inverse: $\forall a \in R$, $\exists b \in R$ such that $a + b = 0$
5. $\cdot$ is associative: $(ab)c = a(bc)$ for all $a, b, c \in R$
6. 1 is a multiplicative identity: $1 \cdot a = a \cdot 1 = a$ for all $a \in R$
7. $\cdot$ is distributive over $+$: $a(b + c) = ab + ac$ for all $a, b, c \in R$

Note that we do not assume that $ab = ba$.

Definition: Commutative Ring

A set R that is a ring and $\cdot$ is commutative.

Definition: Right(Left) Inverse

For $a \in R, a \neq 0$, we say a has a right(left) inverse if $\exists b \in R$, $ab = 1$ $(ba = 1)$.

Definition: Unit (Invertible)

We say a is a unit/invertible if a has the same right and left inverse, $ab = ba = 1$.

Definition: Field

A commutative ring that satisfies every non-zero element is a unit.

Remark: For some non-commutative ring, there exists $a \in R$, a has a right inverse, but it has no left inverse. We have $ab = ca = 1$, but $b \neq c$.

E.g. $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ are commutative rings. $\mathbb{Z}$ is not a field, take 2, the inverse is $\frac{1}{2}$, but $\frac{1}{2} \notin \mathbb{Z}$. $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ are all fields.

$\mathbb{F}_p = \mathbb{Z}_p$ where p is prime, then this is a field. $\mathbb{Z}_m$ where $m \in \mathbb{N}$ and m is not prime is a ring, but not a field.

E.g. If R is a ring, then $R[x]$ (the set of all polynomials in x with coefficients in R) is a ring and not a field. x has no inverse.

Proposition

In $R[x]$, the set of units in $R[x]$ is the same as that in R.

So the set of units in $\mathbb{Z}[x]$ is the set of units in $\mathbb{Z}$.

Proposition

If R is a ring and $n \in N$, then $M_n(R)$ (the set of all $n \times n$ matrices with entries in R) is a ring. It is usually non-commutative.

E.g. Let R and S be rings. Then

$$R \times S = \{(r, s) : r \in R, s \in S\}$$

Define $(r_1, s_1) + (r_2, s_2) = (r_1 + r_2, s_1 + s_2)$ and $(r_1, s_1) \cdot (r_2, s_2) = (r_1 r_2, s_1 s_2)$. Then $(R \times S, +, \cdot)$ is a ring with $0_{R \times S} = (0_R, 0_S)$ and $1_{R \times S} = (1_R, 1_S)$.

Theorem (Uniqueness of Inverse)

Let R be a commutative ring. Let $a \in R$, then

1. The additive inverse of a is unique. $(a + b = 0 = a + c \implies b = c)$
2. For $a \neq 0$, if a has an inverse, then it is unique. $(ab = 1 = ac \implies b = c)$

Proof. 1.

$$\begin{aligned} b &= 0 + b \\ &= (c + a) + b \\ &= c + (a + b) \\ &= c + 0 \\ &= c \end{aligned}$$

2. Similar.

Definition: Additive Inverse

For $a \in R$, denote $-a$ as the unique additive inverse of a.

Definition: Inverse

For $a \in R$, if a has an inverse, denote a^{-1} or $\frac{1}{a}$ as the inverse of a.

Theorem (Cancellation)

Let R be a ring, then for all $a, b, c \in R$,

1. If $a + b = a + c$, then $b = c$.
2. If $a + b = a$, then $b = 0$.
3. If $a + b = 0$, then $b = -a$.

Let F be a field, then for all $a, b, c \in F$,

1. If $ab = ac$, then either $a = 0$ or $b = c$.
2. If $ab = a$, then either $a = 0$ or $b = 1$.
3. If $ab = 1$, then $b = a^{-1}$.
4. If $ab = 0$, then either $a = 0$ or $b = 0$.

Proof. 1. $b = 0 + b = (-a + a) + b = -a + (a + b) = -a + (a + c) = (-a + a) + c = 0 + c = c$.

2. $a + b = a + 0$, then it follows from 1.

3. $a + b = 0 = a + (-a)$, then it follows from 1.

4. Recall $A \implies B \vee C$ is the same as $A \wedge \neg B \implies C$. So assume $a \neq 0$. We have $ab = ac$. Since $a \neq 0$ and F is a field, a has the inverse a^{-1}. Thus,

$$\begin{aligned} b = 1 \cdot b &= (a^{-1} \cdot a)b \\ &= a^{-1}(ab) \\ &= a^{-1}(ac) \\ &= (a^{-1}a)c \\ &= 1 \cdot c = c \end{aligned}$$

5, 6, 7 follows from 4.

Theorem

Let R be a ring and $a \in R$, then

1. $0 \cdot a = 0$.
2. $(-1) \cdot a = -a$.

Proof. 1. $0 \cdot a = (0 + 0) \cdot a = 0 \cdot a + 0 \cdot a$. By cancellation theorem (2), $0 \cdot a = 0$.

2. $0 = 0 \cdot a = (1 + (-1)) \cdot a = 1 \cdot a + (-1) \cdot a$. Since $a + (-1) \cdot a = 0$, then by cancellation theorem (3), $(-1) \cdot a = -a$.

Definition: Group

A set G with a binary operation $\cdot : G \times G \to G$ satisfying the following conditions:

1. For all $f, g, h \in G$, $(fg)h = f(gh)$
2. There exists an element e called an identity such that for all $g \in G$,
   (a) $e \cdot g = g$
   (b) there exists an element g^{-1} such that $g^{-1} \cdot g = g \cdot g^{-1} = e$

Remark: In this class, we use the left identity, but we can show that we can use either left or right. Note that commutativity is not implied.

Definition: Order of G

The cardinality of G denoted by $|G|$.

If $|G| = n$ is finite, we say G is a finite group. If $|G| = \infty$, G is an infinite group.

Definition: Abelian Group

A group G where for every $a, b \in G$, $ab = ba$.

If the group is Abelian, we sometimes use $+$ as the binary operation notation. The identity will be denoted by 0. For all $k \in \mathbb{Z}, a \in G$, then $ka := \underbrace{a + a + \cdots + a}_{k}$.

In general, we use 1 or e as the identity of G. So $a^k = \underbrace{a \cdots a}_{k}$. $a^0 = 1$ or e and $a^{-k} = \underbrace{a^{-1} \cdots a^{-1}}_{k}$.

Theorem

Let G be a group with identity e and $a, b, c \in G$.

1. If $ab = ac$ or $ba = ca$, then $b = c$.
2. If $ab = e$, then $a^{-1} = b$ and $b^{-1} = a$.
3. If $ab = a$, then $b = e$.
4. If $ba = a$, then $b = e$.

Proof. 1. Let a^{-1} be an inverse of a.

$$b = eb = (a^{-1}a)b = a^{-1}(ab) = a^{-1}(ac) = (a^{-1}a)c = ec = c$$

2 and 3 are similar.

Corollary

The identity and the inverse are unique.

If $e_1, e_2 \in G$ such that for any $g \in G$, $e_1 g = g e_1, e_2 g = g e_2$, then $e_1 = e_2$. If for $g \in G$, $b_1, b_2 \in G$ such that $b_1 g = g h_1 = e = b_2 g = g b_2$, then $b_1 = b_2$.

E.g. $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ are all Abelian groups with infinite orders. Note that the binary operation is addition.

Let R be a ring. We define

$$R^* = \text{the set of all invertible elements/units in } R$$

Then R^* is a group with binary operation being multiplication. Addition does not work, take 1 and -1, if we add $1 + (-1) = 0$ does not have an inverse and is not in R^*.

Definition: Groups of Units Modulo n

$$U_n = \mathbb{Z}_n^* = \{[b]_n : 1 \leq b \leq n, \gcd(b, n) = 1\}$$

$\mathbb{Z}^* = \{1, -1\}$ is a finite group. $\mathbb{Q}^* = \{r \in \mathbb{Q} : r \neq 0\} = \mathbb{Q} \setminus \{0\}$. $\mathbb{R}^* = \mathbb{R} \setminus \{0\}, \mathbb{C}^* = \mathbb{C} \setminus \{0\}$ are infinite groups.

$U_m = \mathbb{Z}_m^* = \{[b]_m : 1 \leq b \leq m, \gcd(b, m) = 1\}$. $|U_m| = \varphi(m)$

Definition: Euler's Phi Function φ

If $m = p_1^{k_1} \cdots p_\ell^{k_\ell}$, then

$$\varphi(m) = (p_1^{k_1} - p_1^{k_1 - 1}) \cdots (p_\ell^{k_\ell} - p_\ell^{k_\ell - 1})$$

$|\mathbb{Z}_{10}^*| = |\{1, 3, 7, 9\}| = 4 = (5^1 - 5^0)(2^1 - 2^0)$.
$|\mathbb{Z}_{100}^*| = (5^2 - 5^1)(2^2 - 2^1) = 20(2) = 40$.

Recall that $M_n(R)$ where R is a ring is non-commutative. We can define

$$M_n(R)^* = GL_n(R)$$

Definition: General Linear Group

Let R be a ring. The set of $n \times n$ matrices A such that $\det(A) \neq 0$.

$$M_n(R)^* = GL_n(R)$$

Note that $M_1(R)^* = GL_1(R) = R^*$. If R is commutative, $GL_1(R)^* = R^*$ is Abelian. However, if $n \geq 2$, $GL_n(R)$ must be non-Abelian.

$GL_n(\mathbb{Z}_p)$ is finite. $GL_n(\mathbb{Q}), GL_n(\mathbb{R}), GL_n(\mathbb{C}), GL_n(\mathbb{Z})$ are infinite.

$GL_n(\mathbb{Z})$ is infinite for $n \geq 2$. Take $n = 2$. If the matrix is $\begin{pmatrix} n & n-1 \\ n+1 & n \end{pmatrix} \in GL_2(\mathbb{Z})$. So we have infinitely many elements in $GL_2(\mathbb{Z})$.

If G is finite, we would like to know $|G|$.

Proposition

$|GL_n(\mathbb{Z}_p)| = (p^n - 1)(p^n - p) \cdots (p^n - p^{n-1})$.

Proof. For a matrix $A = (v_1, v_2, \ldots, v_n)^T$ where $v_i \in M_{1 \times n}(\mathbb{Z}_p)$. $A \in GL_n(\mathbb{Z}_p)$ if and only if $v_1, \ldots, v_n$ are linearly independent if and only if for all i where $2 \leq i \leq n$, $v_i \notin \operatorname{Span}\{v_1, \ldots, v_{i-1}\}$. Therefore, the number of choices for v_1 is $p^n - 1$. The number of choices for v_2 is $p^n - p$. For v_3 is $p^n - p^2$. For v_n, there are $p^n - p^{n-1}$.

Definition: Special Linear Group

$$SL_n(R) = \text{the set of all } n \times n \text{ matrices } A \text{ with entries in } R \text{ and } \det(A) = 1$$

Proposition

$|SL_n(\mathbb{Z}_p)| = |GL_n(\mathbb{Z}_p)| / (p - 1)$.

Recall s

Definition: Permutation

For a set S, the set of permutations $\text{Perm}(S) = \{f : S \to S : f \text{ is bijective}\}$, $\text{Perm}(S)$ is a group with the composition as its binary operation and the identity bijection as its identity.

Proposition

$|\text{Perm}(S)| = |S|!$.

Definition: nth Symmetric Group

Let $S = \{1, 2, \ldots, n\}$. Then $S_n = \text{Perm}(\{1, 2, \ldots, n\})$.

Definition: Operation/Multiplication Table

For a finite group, we can specify its operation $*$ by making a table showing the value of the product $a * b$ for each pair $a, b \in G^2 = G \times G$.

E.g. $U_{12} = \{1, 5, 7, 11\}$.

a/b	1	5	7	11
1	1	5	7	11
5	5	1	11	7
7	7	11	1	5
11	11	7	5	1

Proposition

If G and H are groups, then $G \times H$ is also a group.
The order is $|G \times H| = |G|\,|H|$.

$(g_1, h_1) \cdot (g_2, h_2) = (g_1 g_2, h_1 h_2)$.

Definition: Order of a in G

Let G be a group and $a \in G$, the order of a in G, denoted by $|a|$ or $ord(a)$, is the smallest positive integer n such that $a^n = e$.
If there is no positive integer, $|a| = \infty$.

If $|a|$ is finite, then we say a has a finite order, otherwise it has infinite order.

$ord(e) = 1$ and in the previous example, $ord(5) = ord(7) = ord(11) = 2$.

E.g. If $G = \mathbb{Z}$ and for all $n \in \mathbb{Z}, n \neq 0$, the order n is infinite.

E.g. If $G = \mathbb{Z}_n$ and $a \in G$, then $|a| = \frac{n}{\gcd(a,n)}$.

E.g. If $G = \mathbb{C}^*$, $|C^*| = \infty$. If $z \in \mathbb{C}^*$, we can write $z = re^{i\theta}$ where $r > 0, \theta \in \mathbb{R}$. What choices of r and θ make $ord(z)$ finite?

By De Mouvre's Theorem, $z^n = r^n e^{in\theta}$. If $|z| = n$, then

$$z^n = r^n e^{in\theta} = 1$$

This implies $r = 1$ and θ/π is rational. Thus, $|z|$ is finite if and only if $r = 1$ and $\theta = s\pi$ where $s \in \mathbb{Q}$.

Proposition

For $a \in G, b \in H$, then $|(a,b)| = lcm(|a|, |b|)$.

Proof. If $|a| = n, |b| = m$, then for $k \in \mathbb{N}$ we have $(a,b)^k = (a^k, b^k) = (e_G, e_H)$ if and only if $a^k = e_G, b^k = e_H$ if and only if $n \mid k$ and $m \mid k$ if and only if $lcm(m,n) \mid k$. Thus, the smallest positive value of k is $lcm(n,m)$.

Claim: Let G be a group and $a \in G$. $\forall m \in \mathbb{Z}, a^m = e$, then $ord(a) \mid m$.

Proof. (Claim) Let $n = ord(a)$. Since $a^m = e$, then $ord(a) < \infty$. By the division algorithm, there exists $q, r \in \mathbb{Z}$ where $q \leq r < n$ such that $m = qn + r$.

$$\begin{aligned} e = a^m &= a^{qn+r} \\ &= (a^n)^q \cdot a^r \\ &= e^q \cdot a^r \\ &= a^r \end{aligned}$$

By the definition of $|a|$, $r = 0$, which shows $n \mid m$.

Definition: Conjugate

Let G be a group. For $a, b \in G$, we say a and b are conjugate in G, written as $a \sim b$, when $b = xax^{-1}$ for some $x \in G$.

Definition: Conjugate Class Cl

$$Cl(a) = Cl_G(a) = \{b \in G : b \sim a\} = \{xax^{-1} : x \in G\}$$

Remark: The binary relation $\sim$ is an equivalence relation on G. For all $a, b, c \in G$, we have $a \sim a$, $a \sim b, b \sim a$ and $a \sim b, b \sim c \implies a \sim c$.

Remark: If $a \sim b$, then $|a| = |b|$.

E.g. Consider two groups G and H, when and how can we view them as the same ones. Take $G = \mathbb{Z}^* = \{-1, 1\}$ and $H = \mathbb{Z}_2 = \{0, 1\}$. To view two groups as the same, they must share the operation tables. If ϕ maps 1 to 0 and -1 to 1, then under ϕ, their operation table are the same.

a/b	1	-1
1	1	-1
-1	-1	1

a/b	0	1
0	0	1
1	1	0

Definition: Homomorphism

Let G and H be groups and $\phi : G \to H$, we say ϕ is a homomorphism if for any $a, b \in G$, $\phi(ab) = \phi(a)\phi(b)$.

Definition: Isomorphism

If ϕ and ϕ^{-1} are homomorphisms (ϕ is a bijection), then ϕ is an isomorphism and G and H are isomorphic, denoted by $G \cong H$.

E.g. $\mathbb{Z}^* \cong \mathbb{Z}_2$.

E.g. $U_{12} \cong \mathbb{Z}_2 \times \mathbb{Z}_2$.

Chapter 2

Subgroups

Definition: Subgroup

A subgroup H of a group G is a subset which is also a group under the same binary operation, denoted $H \leq G$.

For any group G, G and $\{e\}$ are subgroups of G. $\{e\}$ is called the trivial subgroup.

Definition: Proper Subgroup

H is a proper subgroup of G if $H \leq G$ and $H \neq G$, denoted $H < G$.

E.g. $\mathbb{Z} < \mathbb{Q} < \mathbb{R} < \mathbb{C}$. $\mathbb{Z}^* < \mathbb{Q}^* < \mathbb{R}^* < \mathbb{C}^*$.

E.g. If we denote $\mathbb{Z}_n = \{0, \dots, n-1\}$, $\mathbb{Z}_n$ is not a subgroup of $\mathbb{Z}$.

U_n is not a subgroup of $\mathbb{Z}_n$ under the binary operation $+$ (U_n has no 0, which is the identity in $\mathbb{Z}_n$).

Theorem (Subgroup Test I)

Let G be a group and $H \subseteq G$, then $H \leq G$ if and only if

1. H contains the identity $e \in G$.
2. H is closed under operation, i.e. $a, b \in H$ then $ab \in H$.
3. H is closed under inversion, i.e. $a \in H$ then $a^{-1} \in H$.

Proof. ($\implies$) 2 and 3 are clear. For 1, let e_H be the identity of H. We have $e_H \cdot e_H = e_H \in G$. By the Cancellation Law in G, we have $e_H = e_G$. Thus, $e_G \in H$.

($\impliedby$) 1 and 3 imply the second condition of a group. The associativity is already true for H. The only problem is that H is closed under operation. This is just 2 of the test.

E.g. $G = \mathbb{R}^2$ and $H = \{(x, y) : xy \geq 0\}$. We have $(0, 0) \in H$ and $(x, y), (-x, -y) \in H$, but number 2 fails. Thus, H is not a subgroup.

Theorem (Subgroup Test II)

Let G be a group and $H \subseteq G$, then $H \leq G$ if and only if

1. $H \neq \emptyset$.
2. For all $a, b \in H$, $ab^{-1} \in H$.

Proof. ($\implies$) Trivial.

($\impliedby$) Since H is nonempty, there exists $a \in H$. By 2, $aa^{-1} = e_G \in H$. For the third point in Subgroup Test I, for any $g \in H$, by 2, $e_G \in H$, $e_G \cdot g^{-1} = g^{-1} \in H$.

For the second point in Subgroup Test I, for all $a, b \in H$, $ab = a(b^{-1})^{-1}$, by the third point, $b^{-1} \in H$ and therefore, $ab \in H$.

Theorem (Finite Subgroup Test)

Let G be a group and $H \subseteq G$ is finite, then $H \leq G$ if and only if

1. $H \neq \emptyset$.
2. For all $a, b \in H$, $ab \in H$.

Proof. By Subgroup Test II, we only need to show that for any $a \in H$, $a^{-1} \in H$.

Consider the set $\{a, a^2, a^3, \dots, \} \subseteq H$. By 2, since H is finite, there exist $i, j \in \mathbb{N}, i < j$, then $a^i = a^j$. By the Cancellation Law, $a^{j-i} = e$, i.e. $a^{-1} = a^{j-i-1} \in H$.

E.g. For all $a \in \mathbb{N}$. Define

$$C_n := \{z \in \mathbb{C} : z^n = 1\} = \{e^{2\pi ik/n} : 0 \leq k \leq n-1\}$$

$$C_\infty := \{z \in \mathbb{C} : z^n = 1 \text{ for some } n \in \mathbb{Z}\} = \text{set of all finite order elements in } \mathbb{C}^*$$

$$S^1 := \{z \in \mathbb{C} : |z| = 1\}$$

We have $C_n < C_\infty < S^1 < \mathbb{C}^*$.

Remark: $|C_n| = n = |\mathbb{Z}_n|$. $C_n \cong \mathbb{Z}_n$.

E.g. Let R be commutative. $GL_n(R)$ is the set of all $n \times n$ invertible matrices with coefficients in R.

$$SL_n(R) = \{A \in M_n(R) : \det(A) = 1\}$$

$$O_n(R) = \{A \in M_n(R) : A^T A = I\}$$

$$SO_n(R) = \{A \in M_n(R) : A^T A = I, \det(A) = 1\}$$

We have $SO_n(R) \leq O_n(R) \leq GL_n(R)$ and $SO_n(R) \leq SL_n(R) \leq GL_n(R)$.

E.g. For $\theta \in \mathbb{R}$, the rotation in $\mathbb{R}^2$ about $(0,0)$ by the angle θ is given by the matrix

$$R_\theta = \begin{bmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{bmatrix}$$

The reflection in $\mathbb{R}^2$ in the line through $(0,0)$ and the point $\left(\cos\frac{\theta}{2}, \sin\frac{\theta}{2}\right)$ is given by the matrix

$$F_\theta = \begin{bmatrix} \cos\theta & \sin\theta \\ \sin\theta & -\cos\theta \end{bmatrix}$$

Define

$$O_2(\mathbb{R}) = \{F_\theta, R_\theta : \theta \in \mathbb{R}\}$$
$$SO_2(\mathbb{R}) = \{R_\theta : \theta \in \mathbb{R}\}$$

For all $\alpha, \beta \in \mathbb{R}$, we have

$$F_\beta F_\alpha = R_{\beta-\alpha}, F_\beta R_\alpha = F_{\beta-\alpha}, R_\beta F_\alpha = F_{\alpha+\beta}, R_\alpha R_\beta = R_{\alpha+\beta}$$

E.g. Let $n \in \mathbb{N}$. Define the dihedral group D_n as

$$D_n = \{R_k, F_k : k \in \mathbb{Z}_n\} = \{R_0, R_1, \ldots, R_{k-1}, F_0, \ldots, F_{k-1}\}$$

where $R_k = R_{\theta_k}, F_k = F_{\theta_k}$ and $\theta_k = \frac{2\pi k}{n}$.

$|D_n| = n + n = 2n$ and $D_n \leq O_2(\mathbb{R})$.

Proposition

If H and K are subgroups of G, then $H \cap K$ is also a subgroup.
In general, $\bigcap\limits_{\alpha \in I} H_\alpha$ for a set I is a subgroup.

Definition: Center

Let G be a group and $a \in G$, the center of G is the set

$$Z(G) = \{a \in G : ax = xa, \forall x \in G\}$$

Theorem

G is Abelian if and only if $Z(G) = G$.

Definition: Centralizer

The centralizer of a in G is the set

$$C(a) = \{x \in G : ax = xa\}$$

We would like to find a subgroup H containing a particular element a. H must contain $e, a, a^{-1}, a^2, a^3, \ldots$. Define

$$\langle a \rangle = \{a^k : k \in \mathbb{Z}\} = \{\ldots, a^{-2}, a^{-1}, e, a, a^2, \ldots\}$$

Then $\langle a \rangle$ is a subgroup of G.

Proof. By Subgroup Test II,

1. $\langle a \rangle \neq \emptyset$ since $e \in \langle a \rangle$.
2. For all $a^i, a^j \in \langle a \rangle$, $a^i \cdot a^{-j} = a^{i-j} \in \langle a \rangle$.

Thus, $\langle a \rangle$ is a subgroup of G.

Definition: Subgroup Generator $\langle \rangle$

Let G be a group and $S \subseteq G$. The subgroup of G generated by S, denoted by $\langle S \rangle$, is the smallest subgroup of G containing S.
The elements of S are called the generators of the group $\langle S \rangle$. When S is finite, we omit brackets and write $\langle a_1, \ldots, a_k \rangle := \langle \{a_1, \ldots, a_k\} \rangle$.

Definition: Cyclic Subgroup

If $S = \{a\}$, $\langle S \rangle = \langle a \rangle$ is a cyclic subgroup of G and $\langle a \rangle$ is called a cyclic subgroup generated by a.

Definition: Cyclic Group

If $G = \langle a \rangle$ for some $a \in G$, then G is cyclic.

E.g. $G = \mathbb{Z}_{12}$ is cyclic. $G = \langle [1] \rangle = \langle [5] \rangle = \langle [7] \rangle = \langle [11] \rangle$ are generators. Note that $1, 5, 7, 11 \in U_{12}$.

Proposition

For all $n \in \mathbb{Z}$, if $\gcd(a, n) = 1$, then $\langle [a] \rangle = \mathbb{Z}_n$.

Remark:

1. If G is cyclic, its generator might not be unique.
2. If G is cyclic and of finite order n, G must be isomorphic to $\mathbb{Z}_n$ by $\phi : G \to \mathbb{Z}_n$, $a \mapsto [1]$ where a is the generator.
3. If G is cyclic and of infinite order, $G \cong \mathbb{Z}$ by $\phi : G \to \mathbb{Z}$, $a \mapsto 1$ where a is the generator.

Theorem (Elements of a Cyclic Group)

Let G be a group and $a \in G$, then

1. $\langle a \rangle = \{a^k : k \in \mathbb{Z}\}$.
2. If $ord(a) = |a| = \infty$, then the elements a^k with $k \in \mathbb{Z}$ are all distinct so we have $|\langle a \rangle| = \infty$.
3. If $|a| = n < \infty$, then for all $k, \ell \in \mathbb{Z}$, we have $a^k = a^\ell$ if and only if $k \cong \ell \pmod{n}$, so
$$\langle a \rangle = \{a^k : k \in \mathbb{Z}\} = \{e, a, \dots, a^{n-1}\} \cong \mathbb{Z}_n$$

Proof. 1 is done.

2. Assume that $a^k = a^\ell$ for $k, \ell \in \mathbb{Z}, k > \ell$. By Cancellation Law, we have $e = a^{k-\ell}$, then $ord(a) \leq k - \ell$, a contradiction.

3. Assume that $a^k = a^\ell$ for $k, \ell \in \mathbb{Z}, k > \ell$. By Cancellation Law, $a^{k-\ell} = e$. Since $ord(a) = n$, $n \mid (k - \ell)$, then $k \cong \ell \pmod{n}$.

Theorem (Classification of Subgroups of a Cyclic Group)

Let G be a group and $a \in G$,

1. Every subgroup of $\langle a \rangle$ is cyclic.
2. If $|a| = \infty$, then $\left\langle a^k \right\rangle = \left\langle a^\ell \right\rangle$ if and only if $\ell = \pm k$. So the distinct subgroups of $\langle a \rangle$ are the trivial group $\langle a^0 \rangle = \{e\}$ and $\left\langle a^d \right\rangle = \{a^{kd} : k \in \mathbb{Z}_+\}$ for $d \in \mathbb{N}$.
3. If $|a| = n$, then we have $\left\langle a^k \right\rangle = \left\langle a^\ell \right\rangle$ if and only if $\gcd(k, n) = \gcd(\ell, n)$. So the distinct subgroups of $\langle a \rangle$ are the groups $\left\langle a^d \right\rangle = \{a^{kd} : k \in \mathbb{Z}_+\} = \{a^{kd} : k \in \mathbb{Z}_{n/d}\} = \{e = a^0, a^d, a^{2d}, \dots, a^{n-d}\}$ where d is a positive divisor of n.

Proof. 1. Let $H \leq \langle a \rangle$. If $H = \{e\}$, we are done. Otherwise, there exists $k \in \mathbb{N}$, $a^k \in H$. If $k < 0$, $(a^k)^{-1} = a^{-k} \in H$, we choose $-k \in \mathbb{N}$.

Let $k = \min\{k : a^k \in H, k \in \mathbb{N}\}$.

Claim: $\left\langle a^k \right\rangle = H$.
Proof. (Claim) For all $m \in \mathbb{Z}$, $a^m \in H$. By the division algorithm, there exists $q \in \mathbb{Z}, r \in \mathbb{Z}_+, r < \ell$ such that $m = q$.

$$\begin{aligned}
a^m &= a^{q \cdot \ell + r} \\
&= (a^\ell)^q \cdot a^r \\
a^r &= a^{m - \ell \cdot q} \\
&= \underbrace{a^m}_{\in H} \cdot (\underbrace{a^\ell}_{\in H})^{(-q)} \in H
\end{aligned}$$

By the minimality of ℓ, $r = 0$ and $\ell \mid m$.

2. Assume that $|a| = \infty$. If $\ell = \pm k$, then we have $\left\langle a^k \right\rangle = \left\langle a^\ell \right\rangle$.

Suppose that $\left\langle a^k \right\rangle = \left\langle a^\ell \right\rangle$. Since $a^k \in \left\langle a^\ell \right\rangle$, we have $a^k = (a^\ell)^t$ for $t \in \mathbb{Z}$. This implies $a^{k-\ell t} = e$, so $k = \ell t$.

Conversely $a^\ell \in \left\langle a^k \right\rangle, a^\ell = a^{kt'}, \ell = kt'$, there exists $t' \in \mathbb{Z}$ such that $\ell = t'k$. Thus, we have $k = \ell t = tt'k$, $\left\langle a^k \right\rangle = \left\langle a^\ell \right\rangle = \{e\}$. If $k = 0$, it is clear. We can assume that $k \neq 0$ and $1 = tt'$. This implies $t = t' = \pm 1$, we are done.

3. Suppose that $|a| = n, \forall d \mid n, d > 0$, $\left\langle a^d \right\rangle = \{a^{kd} : k \in \mathbb{Z}_{n/d}\}$ and $\left|\left\langle a^d \right\rangle\right| = n/d$.

Thus, we only need to show

$$\left\langle a^k \right\rangle = \left\langle a^\ell \right\rangle \Leftrightarrow \gcd(k, n) = \gcd(\ell, n)$$

Claim: $\left\langle a^k \right\rangle = \left\langle a^{\gcd(k,n)} \right\rangle$

Proof. (Claim) Let $d = \gcd(k, n)$. If $k = 0 \pmod n$, $\left\langle a^k \right\rangle = \langle a^0 \rangle = \{e\}$ and $\left\langle a^{\gcd(k,n)} \right\rangle = \langle a^n \rangle = \{e\}$.

So assume that $k \neq 0 \pmod n$, $1 \leq k \leq n$. Thus, $d = \gcd(k, n) \geq 1$. We need to show $a^k \subseteq \left\langle a^d \right\rangle$. Since $d \mid k$ and $d \neq 0$, there exists $t \in \mathbb{Z}$ such that $k = td$. This implies $a^k = (a^d)^t \in \left\langle a^d \right\rangle$.

Now we need to show $a^d \subseteq \left\langle a^k \right\rangle$. Since $d = \gcd(k, n)$ by Extended Euclidean Algorithm, there exists $\ell, t \in \mathbb{Z}$ such that $d = kt + n\ell$.

$$a^d = a^{kt+n\ell} = (a^k)^t (a^n)^\ell = (a^k)^t \cdot e^\ell = (a^k)^t \in \left\langle a^k \right\rangle$$

Proposition

In $\mathbb{Z}_n$, the cyclic group of order n, there are exactly $\phi(n)$ many generators.

Corollary

Let G be a group, $a \in G$, then

1. If $|a| = \infty$, then $|a^0| = |e| = 1$ and $\left|a^k\right| = \infty$ for all $k \in \mathbb{Z}, k \neq 0$.
2. If $|a| = n$, then $\left|a^k\right| = \frac{n}{\gcd(k,n)}$.
3. If $|a| = \infty$, then $\left\langle a^k \right\rangle = \langle a \rangle \Leftrightarrow k = \pm 1$.
4. If $|a| = n$, $\left\langle a^k \right\rangle = \langle a \rangle \Leftrightarrow \gcd(k, n) = 1 \Leftrightarrow k \in U_n$.

Corollary (Number of Elements of Each Order in a Cyclic Group)

Let G be a group and let $a \in G$ with $|a| = n$. Then for each $k \in \mathbb{Z}$, the order of a^k is a positive divisor of n and for each positive divisor d of n, the number of elements in $\langle a \rangle$ of order d is $\varphi(d)$.

Corollary

$$\sum_{d|n} \varphi(d) = n = |\langle a \rangle| = n$$

Corollary (Number of Elements of Each Order in a Finite Group)

Let G be a finite group. For each $d \in \mathbb{N}$, the number of elements in G of order d is equal to $\phi(d)$ multiplied by the number of cyclic subgroups of G of order d.

Theorem (Elements in $\langle S \rangle$)

Let G be a group and $\phi \neq S \subseteq G$, then

$$\begin{aligned}\langle S \rangle &= \{a_1^{k_1} a_2^{k_2} \cdots a_\ell^{k_\ell} : \ell \geq 0, a_i \in S, k_i \in \mathbb{Z}\} \\ &= \{a_1^{k_1} \cdots a_\ell^{k_\ell} : \ell \geq 0, a_i \in S, a_i \neq a_{i+1}, 0 \neq k_i \in \mathbb{Z}\}\end{aligned}$$

where $\ell = 0$ means e.
If G is Abelian, then

$$\langle S \rangle = \{a_1^{k_1} \cdots a_\ell^{k_\ell} : \ell \geq 0, a_i \in S, a_i \neq a_j, \forall i \neq j, 0 \neq k_i \in \mathbb{Z}\}$$

E.g. In $\mathbb{Z}$, $\langle k, \ell \rangle = \langle \gcd(k, \ell) \rangle$. In $D_n = \langle R_1, F_0 \rangle$ in $O_2(\mathbb{R})$ because $R_k = R_1^k$ and $F_k = R_k F_0$.

Definition: Free Group

Let S be a set. The free group on S is the set whose elements are

$$F(S) = \{a_1^{k_1} a_2^{k_2} \cdots a_\ell^{k_\ell} : \ell \geq 0, a_i \in S, 0 \neq k_i \in \mathbb{Z}\}$$

with the operation given by concatenation

$$(a_1^{j_1} \cdots a_\ell^{j_\ell})(b_1^{k_1} \cdots b_m^{k_m}) = a_1^{j_1} \cdots a_\ell^{j_\ell} b_1^{k_1} \cdots b_m^{k_m}$$

followed by grouping and cancellation in the sense that if $a_\ell = b_1$, then we replace $a_\ell^{j_\ell} b_1^{k_1}$ by $a_\ell^{j_\ell + k_1}$ and if in addition, $j_\ell + k_1 = 0$, we can check the next pair $a_{\ell-1}^{j_\ell - 1}$ and $b_2^{k_2}$ and continue the process.

E.g.

$$(ab^2a^{-3}b)(b^{-1}a^3ba^{-2}) = (ab^2a^{-3})(bb^{-1})(a^3ba^{-2}) = (ab^2a^{-3})(a^3ba^{-2}) = ab^2ba^{-2} = ab^3a^{-2}$$

Definition: Free Abelian Group

Let S be a set. The free Abelian group on S is the set

$$A(S) = \{k_1 a_1 + \cdots + k_\ell a_\ell : \ell \geq 0, a_i \in S, a_i \neq a_j, 0 \neq k_i \in \mathbb{Z}\}$$

Remark: $A(S) = \sum_{a \in S} \mathbb{Z} = \{f : S \to \mathbb{Z} : f(a) = 0 \text{ for all but finitely many } a \in S\}$. $(f + g)(a) = f(a) + g(a)$ is the operation.

Chapter 3

Symmetric and Alternating Groups

Definition: Symmetric Group S_n

$$S_n = \mathrm{Perm}\{1, \ldots, n\}$$

For $\alpha \in S_n$, we can write

$$\alpha = \begin{pmatrix} 1 & 2 & \cdots & n \\ \alpha(1) & \alpha(2) & \cdots & \alpha(n) \end{pmatrix}$$

This is called array notation for α.

E.g. $S_2 = \left\{ \begin{pmatrix} 1 & 2 \\ 1 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix} \right\}$. $S_3 \left\{ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \ldots \right\}$.

E.g. S_n is big. Many known groups such as C_n, D_n can be viewed as subgroups of S_n. Recall $C_n \cong \mathbb{Z}_n = \{e^{2\pi ik/n} : k = 1, \ldots, n\}$. For $C_n \to S_n$, $e^{2\pi i/n} \mapsto \begin{pmatrix} 1 & 2 & 3 & \cdots & n-1 & n \\ 2 & 3 & 4 & \cdots & n & 1 \end{pmatrix} = \alpha$. Thus, $\langle \alpha \rangle \cong C_n$ and $|\alpha| = n$.

$D_n \cong \langle \alpha, \beta \rangle$ where $\alpha = R_1$ and $\beta = F_{n-1}$. $\beta = \begin{pmatrix} 1 & 2 & \cdots & n-1 & n \\ n & n-1 & \cdots & 2 & 1 \end{pmatrix}$, $|\beta| = 2, |\alpha| = n$. The reason behind this isomorphism is D_n preserves an n-regular polygon.

Definition: Cyclic Representation

When $a_1, \ldots, a_\ell$ are distinct elements in $\{1, \ldots, n\}$, we write $\alpha = (\alpha_1, \alpha_2, \cdots, \alpha_\ell)$ for a permutation $\alpha \in S_n$ given by $\alpha(a_1) = a_2, \alpha(a_2) = a_3, \ldots, \alpha(a_{\ell-1}) = a_\ell, \alpha(a_\ell) = a_1$ and $\alpha(k) = k$ for all $k \notin \{a_1, \ldots, a_\ell\}$.

E.g. $\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \rightsquigarrow (1, 2, 3)$.

Among those cycle representations for an element in S_n, we can choose one cycle starting with the smallest number in the cycle. Then it becomes unique.

ℓ is called the length of the cycle α and we say α is an ℓ-cycle.

Remark:

1. $|\alpha| = \ell$ is its length.
2. $e = (1) = (2) = \cdots = (n)$.
3. $(1,2)(2,3) = (1,2,3)$. We can multiply cycles using the composition of functions. $(2,3)(1,2) = (1,3,2)$. So $(1,2)(2,3) \neq (2,3)(1,2)$ and therefore, S_3 is non-Abelian.

   In general, S_n is non-Abelian.

Definition: Disjoint Cycles

Two cycles $\alpha = (a_1, \ldots, a_\ell), \beta = (b_1, \ldots, b_m)$ are said to be disjoint when $\{a_1, \ldots, a_\ell\} \cap \{b_1, \ldots, b_m\} = \emptyset$, we can extend this to n cycles.

Remark: If α and β are disjoint, α and β commute, i.e. $\alpha\beta = \beta\alpha$.

Proof. For all $t \in \{1, \ldots, n\}$.

- Case 1: $t \in \{a_1, \ldots, a_\ell\}$.

  $\alpha\beta(t) = \alpha(t), \beta\alpha(t) = \beta(\alpha(t)) = \alpha(t)$.
- Case 2: $t \in \{b_1, \ldots, b_m\}$.

  $\alpha\beta(t) = \alpha(\beta(t)) = \beta(t), \beta\alpha(t) = \beta(t)$.
- $t \notin \{a_1, \ldots, a_\ell\} \cup \{b_1, \ldots, b_m\}$.

  $\alpha\beta(t) = t = \beta\alpha(t)$.

Theorem (Cycle Notation)

Every $\alpha \in S_n$ can be written as a product of disjoint cycles. Indeed, for all $\alpha \neq e$ can be written uniquely in the form

$$\alpha = (a_{1,1}, \ldots, a_{1,\ell_1}), (\cdots), \ldots, (a_{m,1}, \ldots, a_{m,\ell_m})$$

with $m \geq 1$, each $\ell_i \geq 2$, each $a_{i,1} = \min\{a_{i,1}, \ldots, a_{i,\ell_i}\}$ and $a_{1,1} < a_{2,1} < \cdots < a_{m,1}$.

Proof. Let $e \neq \alpha \in S_n$. Choose $a_{1,1}$ to be the smallest k such that $\alpha(k) \neq k, \alpha_{1,2} = \alpha(a_{1,1}), \alpha_{1,3} = \alpha(a_{1,2}), \ldots$ until we find the first k such that $\alpha(k) = a_{1,1}$. Then we have the first cycle.

Choose $a_{2,1}$ to bet he smallest k such that $k \notin \{a_{1,1}, \ldots, a_{1,\ell}\}$ and $\alpha(k) \neq k$. Continue this process by induction.

Remark: In this way, we write $e = (1)$.

E.g. $S_3 \cong D_3 = \{(1), (1,2), (2,3), (1,3), (1,2,3), (1,3,2)\}$.

$S_4 = \{(1), (1,2), (1,3), (1,4), (2,3), (2,4), (3,4), (1,2,3), (1,3,2), (1,2,4), (1,4,2), (2,3,4), (2,4,3), (1,3,4), (1,4,3), (1,2,3,4), (1,3,4,2), (1,4,2,3), \dots\}$.

E.g. $\alpha = (1,3,5,2), \beta = (2,6,3)$. Compute $\alpha\beta$ in cycles.

$\alpha\beta = (1,3,1)(2,6,5,2) = (1,3)(2,6,5)$. $|\alpha| = 2, |\beta| = 3, |\alpha\beta| = 2 \cdot 3 = 6$.

E.g. $|(1,2,3)(4,5,6)| = 3$ since $(1,2,3)^3 = (4,5,6)^3 = e$.

Theorem (Order of Disjoint Cycles Permutation)

Let $\alpha = \alpha_1 \dots \alpha_\ell$ where α_i are disjoint cycles. Then

$$|\alpha| = \operatorname{lcm}(|\alpha_1|, \dots, |\alpha_\ell|)$$

Recall that in a group G, $a, b \in G$, we say a is conjugate to b if $\exists x \in G$, $b = xax^{-1}$. If a is conjugate to b, $|a| = |b|$, since $b^k = (xax^{-1})^k = xa^kx^{-1}$.

Theorem (Conjugacy Class of a Permutation)

Let $\alpha, \beta \in S_n$. Then α and β are conjugate in S_n if and only if when written in cycle notation, α and β have the same number of cycles of each length, or we say that α and β have the same cycle-type.

The cycle type means that if α is written as $\alpha = \alpha_1 \dots \alpha_\ell$ where α_i are disjoint cycles, then $\{|\alpha_1|, \dots, |\alpha_\ell|\}$ is the cycle type of α.

E.g. $(1,2,3)$ is conjugate to $(3,4,5)$. $(1,2,3)(4,5)$ is conjugate to $(1,5)(2,3,4)$. $(1,2)(3,4)$ is conjugate to $(1,3)(2,4)$.

Proof. (Conjugacy Class) Write α is cycle notation as

$$\alpha = (a_{1,1}, \dots, a_{1,\ell_1}) \dots (a_{m,1}, \dots, a_{m,\ell_m})$$

disjoint cycles. Let $\sigma \in S_n$.

Claim: $\sigma\alpha\sigma^{-1} = (\sigma(a_{1,1}), \dots, \sigma(a_{1,\ell_1})) \dots (\sigma(a_{m,1}), \dots, \sigma(a_{m,\ell_m}))$.

If the claim is true, for any β with the same cycle type, we can define σ by

$$\sigma(a_{i,i_j}) = b_{i,i_j}, 1 \leq i \leq m, 1 \leq i_j \leq \ell_i$$

Then we are done.

Proof. (Claim) Given $i, i_j, 1 \leq i \leq m, 1 \leq i_j < \ell_i$. We also have $\sigma(a_{i,i_j}) = \sigma(a_{i,i_j+1})$.

$$\begin{aligned}
\sigma\alpha\sigma^{-1} &= \sigma\alpha(\sigma^{-1}(\sigma\sigma(a_{i,i_j})) \\
&= \sigma(\alpha(a_i, a_{i_j})) \\
&= \sigma(a_{i,i_j+1})
\end{aligned}$$

If $i_j = \ell_i$, then

$$\begin{aligned} \sim \alpha\sigma^{-1}(\sigma(a_{i,\ell_i})) &= \sigma(\alpha(a_{i,\ell_i})) \\ &= \sigma(a_{i,1}) \end{aligned}$$

Thus, $\sim \alpha\sigma^{-1}$ is as desired.

E.g. In S_{15}, compute the number of elements of cycle type $4, 4, 4$, i.e. three 4-cycles.

We look for a cycle like

$$(a_1, a_2, a_3, a_4)(a_5, a_6, a_7, a_8)(a_9, a_{10}, a_{11}, a_{12})$$

The total choices of a_1 to a_{12} is $\binom{15}{12}$.

a_1 has 1 choice since it must be the smallest one, a_2 has 11, a_3 has 10, and a_4 has 9 choices.

a_5 has 1 choice since it must be the smallest one among the $a_5, \ldots, a_{12}$, a_6 has 7, a_7 has 6, and a_8 has 5 choices.

a_9 has 1 choice among the $a_9, \ldots, a_{12}$, a_{10} has 3, a_{11} has 2, and a_{12} has 1 choice.

The total number is

$$\binom{15}{12} 11(10)(9)(7)(6)(5)(3)(2)(1) = \binom{15}{12} \frac{12!}{12 \cdot 8 \cdot 4}$$

E.g. Compute the number of elements in S_{20} of cycle type four 2-cycles, two 3-cycles, and one 4-cycle.

Consider

$$\alpha = (a_1, a_2)(a_3, a_4)(a_5, a_6)(a_7, a_8)(b_1, b_2, b_3)(b_4, b_5, b_6)(c_1, c_2, c_3, c_4)$$

There are $\binom{20}{8}$ choices for a_1 to a_8. The choices for $a_1, \ldots, a_8$ is $(1, 7), (1, 5), (1, 3), (1, 1)$. So the total for the 2-cycles is $\binom{20}{8} \frac{8!}{8 \cdot 6 \cdot 4 \cdot 2}$.

There are $\binom{12}{6}$ for the b_i's with the choices being $(1, 5, 4), (1, 2, 1)$. So the total is $\binom{12}{6} \frac{6!}{6 \cdot 3}$.

The total for c_i's is $\binom{6}{4} \frac{4!}{4}$.

The total is

$$\binom{20}{8} \frac{8!}{8 \cdot 6 \cdot 4 \cdot 2} \binom{12}{6} \frac{6!}{6 \cdot 3} \binom{6}{4} \frac{4!}{4}$$

Let α be a product of cycles, which may not be disjoint. What can we say about α?

Theorem (Even and Odd Permutations)

In S_n for $n \geq 2$,

1. Every $\alpha \in S_n$ can be written as a product of 2-cycles.
2. If $e = (a_1, b_1)(a_2, b_2) \dots (a_\ell, b_\ell)$ for $\ell \geq 1$, then ℓ must be even.
3. If $\alpha = (a_1, b_1)(a_2, b_2) \dots (a_\ell, b_\ell) = (c_1, d_1)(c_2, d_2) \dots (c_m, d_m)$, then $\ell \equiv m \pmod 2$.

Proof. 1. It is enough to show that every cycle can be written as a product of 2-cycles.

$$(a_1, \dots, a_\ell = (a_1, a_\ell)(a_1, a_{\ell-1}) \cdots (a_1, a_2)$$

We are done.

3. We can use 2 to imply 3.

$$e = \alpha\alpha^{-1} = (a_1, b_1) \cdots (a_\ell, b_\ell)[(c_m, d_m) \cdots, (c_1, d_1)]$$

By 2, $l + m \equiv 0 \pmod 2$ so $\ell \equiv m \pmod 2$.

2. e can not be written as a product of one 2 cycle. However, it can be written as a product of two 2-cycles $e = (a, b)(a, b)$. We may assume $\ell \geq 3$.

We prove by strong induction. For $\ell = 1, 2$, we are done. Assume $\ell \geq 3$. For any $k < \ell$, if e can be written as a product of k 2-cycles, k must be even.

Let $e = (a_1, b_1) \cdots (a_\ell, b_\ell)$ for $\ell \geq 3$. Let $a = a_1$. Of all the ways to write e as a product of ℓ 2-cycles, in the form $e = (x_1, y_1) \cdots (x_\ell, y_\ell)$, with $x_i = a$ for some i (to exchange x_i, y_i if necessary). We choose one way, say $e = (r_1, s_1) \cdots (r_\ell, s_\ell)$, so that $r_m = a$ for $m \leq \ell$ and $r_i, s_i \neq a$ for all $i < m$, and pick up the largest possible m.

Let $(r_1, s_1) \cdots (r_m, s_m) \cdots (r_\ell, s_\ell)$ be the max choice. First we claim that $m \neq \ell$. If $m = \ell$, i.e. $e = (r_1, s_1) \cdots (a, s_\ell)$, then $\alpha(s_\ell) = a \neq s_\ell$, a contradiction.

Thus, we can assume that $m < \ell$. Consider $(r_m, s_m)(r_{m+1}, s_{m+1})$. All possible forms of $(r_m, s_m)(r_{m+1}, s_{m+1})$ are

$$(a, b)(a, b), (a, b)(a, c), (a, b)(b, c), (a, b)(c, d)$$

1. $(a, b)(a, b)$: Then $e = (r_1, s_1) \cdots (a, b)(a, b) \cdots (r_\ell, s_\ell)$. Thus, e is written as a product of $\ell - 2$ 2-cycles. By induction $\ell - 2 \equiv 0 \pmod 2$, so $\ell \equiv 0 \pmod 2$.
2. $(a, b)(b, c)$: We have $(a, b)(b, c) = (a, b, c) = (b, c)(a, c)$. This is impossible since in m is the largest number.
3. $(a, b)(c, d) = (c, d)(a, b)$: This is impossible since m is the largest number.
4. $(a, b)(a, c) = (a, c, b) = (b, c)(a, b)$. This is also impossible since m is the largest number.

Thus, we are done.

Definition: Even/Odd Permutation

For $n \geq 2$, for a permutation $\alpha \in S_n$, α is called an even permutation if α can be written as a product of even 2-cycles. Otherwise we say α is an odd permutation.

We define a sign function

$$\operatorname{sign}(\alpha) = (-1)^\alpha = \begin{cases} 1 & \text{if } \alpha \text{ is even} \\ -1 & \text{if } \alpha \text{ is odd} \end{cases}$$

Then sign is a homomorphism from S_n to $\mathbb{Z}^* = \{1, -1\}$.

Theorem (Property of Parity)

For $n \geq 2$, $\alpha, \beta \in S_n$,

1. $\operatorname{sign}(e) = (-1)^e = 1$.
2. If α is an ℓ-cycle, $\operatorname{sign}(\alpha) = (-1)^{\ell-1}$.
3. $\operatorname{sign}(\alpha\beta) = (-1)^{\alpha\beta} = (-1)^\alpha(-1)^\beta$.
4. $\operatorname{sign}(\alpha^{-1}) = (-1)^{\alpha^{-1}} = (-1)^\alpha = \operatorname{sign}(\alpha)$.

Definition: Alternating Group A_n

For $n \geq 2$, we define the alternating group A_n to be

$$A_n = \{\alpha \in S_n : \operatorname{sign}(\alpha) = (-1)^\alpha = 1\}$$

A_n is a subgroup of S_n. By Property of Parity, $|A_n| = \frac{|S_n|}{2} = \frac{n!}{2}$. This is because of a bijection

$$F : \{\alpha \in S_n : \operatorname{sign}(\alpha) = 1\} \to \{\beta \in S_n : \operatorname{sign}(\beta) = -1\}$$

by $F(\alpha) = (1, 2)\alpha$.

What are generating sets for S_n and A_n? The set of all 2-cycles is a generating set.

Claim: $\langle (1, 2), (1, 3), \ldots, (1, n) \rangle = S_n$.

Proof. (Claim) It is enough to show every 2-cycle is generated. For all k, ℓ, $(k, \ell) = (1k)(1\ell)(1k)$. Next

1. $\langle (1, 2), \ldots, (n - 1, n) \rangle = S_n$.

   Proof. $(1, k) = (1, 2)(2, 3) \ldots (k - 1, k)$.

2. $\langle (1, 2), (1, 2 \ldots, n) \rangle = S_n$.

   Proof. $(k, k + 1) = (1, 2, \ldots, n)^{k-1}(1, 2)(1, 2, \ldots, n)^{-(k-1)}$.

Proposition

A_n is generated by all 3-cycles. Moreover, it can be generated by $\{(a, b, k) : k \neq a, b\}$ for all a, b.

Proof. We know that for all $\alpha \in A_n$, α is a product of even number of 2-cycles. In particular, we just consider a product of two 2-cycles. i.e. $(a, b)(a, b), (a, b)(a, c), (a, b)(c, d)$.

$$\begin{aligned}(a, b)(a, b) &= (a, b, c)(c, b, a) \\ (a, b)(a, c) &= (a, c, b) \\ (a, b)(c, d) = (a, d, c)(a, b, c)\end{aligned}$$

Thus, α is a product of 3-cycles.

For the second part, every 3-cycle is of one of the form:

$$(a, b, k), (a, k, b), (a, k, \ell), (b, k, \ell), (k, \ell, m)$$

$$\begin{aligned}(a, k, b) &= (a, b, k)^2 \\ (a, k, \ell) &= (a, b, \ell)(a, b, k)^2 \\ (b, k, \ell) &= (a, b, \ell)^2(a, b, k) \\ (k, \ell, m) &= (a, b, k)^2(a, b, m)(a, b, \ell)^2(a, b, k)\end{aligned}$$

Chapter 4

Homomorphisms

Definition: Homomorphism

$\phi : G \to H$ such that for all $a, b \in G$, $\phi(ab) = \phi(a)\phi(b)$.

Remark: $\phi(ab)$ has the multiplication in G and $\phi(a)\phi(b)$ has the multiplication in H.

Definition: Isomorphism

$\phi : G \to H$ such that ϕ is a bijective homomorphism and ϕ^{-1} is also a homomorphism.

Definition: Kernel of ϕ

Let ϕ be a homomorphism, then the kernel

$$\ker(\phi) = \phi^{-1}(e_H) = \{a \in G : \phi(a) = e_H\}$$

Definition: Image of ϕ

Let ϕ be a homomorphism, then the image

$$\operatorname{Im}(\phi) = \{\phi(a) : a \in G\} \subseteq H$$

$\ker(\phi)$ is a subgroup of G.

$\operatorname{Im}(\phi)$ is a subgroup of H.

Definition: Endomorphism

An endomorphism of a group G is a homomorphism from G to G (itself).

Definition: Automorphism

An automorphism of a group G is an isomorphism from G to G (itself).

$\mathrm{Hom}(G, H)$ is the set of all homomorphisms from G to H. $\mathrm{Iso}(G, H)$ is the set of all isomorphisms from G to H.

$\mathrm{End}(G)$ is the set of all homomorphisms from G to G. $\mathrm{Aut}(G)$ is the set of all isomorphisms from G to G.

E.g. Let G be a group, $a \in G$. If $|a| = \infty$, then the map $\phi_a : \mathbb{Z} \to G$ by $\phi(k) = a^k$, $k \in \mathbb{Z}$. Then ϕ_a is a homomorphism since

$$\phi(k + \ell) = a^{k+\ell} = a^k \cdot a^\ell = \phi(k)\phi(\ell)$$

$\ker(\phi_a) = \{0\}$, $\mathrm{Im}(\phi_a) = \langle a \rangle$.

If $|a| = n$. then the map $\phi_a : \mathbb{Z} \to G$, $\phi_a(k) = a^k$ is still a homomorphism. $\ker(\phi_a) = n\mathbb{Z} = \{n\ell : \ell \in \mathbb{Z}\} = \langle n \rangle$, $\mathrm{Im}(\phi_a) = \langle a \rangle$.

Consider $\tilde{\phi_a} : \mathbb{Z}_n \to G$ by sending $\tilde{\phi_a}([k]) = a^k$. It is well-defined since $|a| = n$. Then $\ker(\tilde{\phi_a}) = \{[0]\}$, $\mathrm{Im}(\tilde{\phi_a}) = \langle a \rangle \equiv \mathbb{Z}_n$.

E.g. Let R be a commutative ring, ϕ be a determinant map where $\phi : GL_n(R) \to R^*$ is a homomorphism by $\det(AB) = \det(A)\det(B)$.

$\ker(\phi) = \{A \in GL_n(R) : \det(A) = I_R\} = SL_n(R)$ so the kernel is $SL_n(R)$. $\mathrm{Im}(\phi) = R^*$.

E.g. $(\mathbb{R}, +)$ and $(\mathbb{R}^+, \times)$ are isomorphic.

Let $\phi : \mathbb{R} \to \mathbb{R}^+$ where for $a \in \mathbb{R}$, we can map it to k^a. The inverse is $\log_k$.

E.g. $SO_2(\mathbb{R})$ is isomorphic $S^1 = \{z \in \mathbb{C} : \|z\| = 1\} = \{e^{i\theta} : \theta \in \mathbb{R}\}$. $SO_2(\mathbb{R})$ is R_θ, so $\phi : R_\theta \to e^{i\theta}$.

Theorem

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

1. $\phi(e_G) = e_H$
2. $\phi(a^{-1}) = \phi(a)^{-1}$
3. $\phi(a^k) = (\phi(a))^k$
4. For $a \in G$, if $|a| < \infty$, $|\phi(a)| \mid |a|$

Proof. 1. $\phi(e_G) = \phi(e_G \cdot e_G) = \phi(e_G)\phi(e_G)$. Then $e_H = \phi(e_G)$ by the cancellation law.

2. $e_H = \phi(e_G) = \phi(a^{-1}a) = \phi(a^{-1})\phi(a)$ so $\phi(a^{-1}) = \phi(a)^{-1}$.

3.

- Case 1: $k > 0$

$$\phi(a^k) = \underbrace{\phi(a) \cdots \phi(a)}_{k} = (\phi(a))^k$$

- Case 2: $k = 0$
$$\phi(a^0) = \phi(e_G) = e_H = \phi(a)^0$$
- Case 3: $k < 0$
$$\phi(a^k) = (\phi(a^{-k}))^{-1} = (\phi(a)^{-k})^{-1} = \phi(a)^k$$

4. Let $|a| = n$, i.e. $a^n = e_G$, and $|\phi(a)| = m$.

$$e_H = \phi(e_G) = \phi(a^n) = (\phi(a))^n$$

By divisibility property, $m \mid n$ implies $|\phi(a)| \mid |a|$.

Theorem

If ϕ is a bijective homomorphism from G to H, then ϕ^{-1} is a homomorphism. Thus, ϕ is an isomorphism.

Proof. For any $a, b \in H$, let $a = \phi(c)$ and $b = \phi(d)$ for $c, d \in G$. By definition, we know that $\phi^{-1}(a) = c$ and $\phi^{-1}(b) = d$ and $\phi(cd) = \phi(c)\phi(d)$.

$$\phi^{-1}(ab) = \phi^{-1}(\phi(c)\phi(d)) = \phi^{-1}(\phi(cd)) = cd = \phi^{-1}(a)\phi^{-1}(b)$$

Thus, ϕ^{-1} is a homomorphism.

Corollary

$\mathrm{Aut}(G)$ is a group under composition with the identity map, i.e. $g \mapsto g$.

Theorem

Let ϕ be a homomorphism from G to H.

1. If $K \leq G$, then $\phi(K) \leq H$. (Special case $\mathrm{Im}(\phi) \leq H$)
2. If $L \leq H$, then $\phi^{-1}(L) = \{a \in G : \phi(a) \in L\} \leq G$. (Special case $\ker(\phi) \leq G$)

Theorem

Let $\phi : G \to H$ be a homomorphism.

1. ϕ is injective if and only if $\ker(\phi) = \{e_G\}$.
2. ϕ is surjective if and only if $\mathrm{Im}(\phi) = H$.

Proof. 1. ($\implies$) Clear.

($\Longleftarrow$) Assume that $\ker(\phi) = \{e_G\}$. Let $a, b \in G$ and $\phi(a) = \phi(b)$. We need to show $a = b$.

$$\begin{aligned}
\phi(a) &= \phi(b) \\
\phi(a)\phi(b)^{-1} &= \phi(b)\phi(b)^{-1} = e_H \\
\phi(a)\phi(b^{-1}) &= e_H \\
\phi(ab^{-1}) &= e_H \\
ab^{-1} \in \ker(\phi) &\implies ab^{-1} = e_G \implies a = b
\end{aligned}$$

Theorem

Let $\phi : G \to H$ be an isomorphism.

1. G is Abelian if and only if H is Abelian.
2. If $a \in G$, then $|\phi(a)| = |a|$.
3. If G is cyclic with $G = \langle a \rangle$, then H is cyclic with $H = \langle \phi(a) \rangle$.
4. For all $n \in \mathbb{N} \cup \{0\}$, $|\{a \in G : |a| = n\}| = |\{b \in H : |b| = n\}|$.
5. For $K \leq G$, the restriction $\phi : K \to \phi(K)$ is an isomorphism.
6. For any group C, we have $|\{K \leq G : K \cong C\}| = |\{L \leq H : L \cong C\}|$.

One of the goals of group theory is to understand all groups up to isomorphism. At least, we hope that, given two groups, we can tell if they are the same, i.e. isomorphic.

E.g. $\mathbb{Q} \ncong \mathbb{R}$ since $\mathbb{Q}$ is countable, but $\mathbb{R}$ is uncountable, so $|\mathbb{Q}| \neq |\mathbb{R}|$.

E.g. $GL_3(\mathbb{Z}_2) \ncong S_5$. $|GL_3(\mathbb{Z}_2)| = (2^3 - 1)(2^3 - 2^1)(2^3 - 2^2) = 162$ and $|S_5| = 5! = 120$.

E.g. $\mathbb{R}^* \ncong \mathbb{C}^*$. Since there are only 2 elements of finite order in $\mathbb{R}^*$, namely 1 and -1, but the set of finite order in $\mathbb{C}^*$ is $\{e^{i\theta} : \theta \in \mathbb{Q}\}$ is infinite.

E.g. $U_{35} \ncong \mathbb{Z}_{24}$. $|U_{35}| = \phi(35) = (7-1)(5-1) = 6(4) = 24 = |\mathbb{Z}_{24}|$. There are exactly 2 elements of order 2 in U_{35}, namely 29 and 34, but there is only 1 element of order 2 in $\mathbb{Z}_{24}$ is 12.

Theorem

Let $a, b \in \mathbb{N}$ and $\gcd(a, b) = 1$.

1. $\mathbb{Z}_{ab} \cong \mathbb{Z}_a \times \mathbb{Z}_b$.
2. $U_{ab} \cong U_a \times U_b$.

Proof. Application of Chinese Remainder Theorem.

So, $U_{35} = U_7 \times U_5$.

Corollary

If $n = \prod_{i=1}^{\ell} p_i^{k_i}$, then

$$\phi(n) = \prod_{i=1}^{\ell}(p_i^{k_i} - p_i^{k_i-1}) = n\prod_{p|n}\left(1 - \frac{1}{p}\right)$$

Proof. $\phi(n) = |U_n|$. Assume that $n = \prod P_i^{\alpha_i}$. $\phi(n) = \prod \phi(P_i^{\alpha_i}) = \prod(p_i^{\alpha_i} - p_i^{\alpha_i - 1})$.

Theorem

$$\phi(p^\ell) = p^\ell - p^{\ell-1}$$

Proof.

$$\begin{aligned}
\phi(p^\ell) &= \left|\{b \in \mathbb{Z} : 1 \leq b \leq p^\ell, \gcd(b, p^\ell) = \gcd(b, p) = 1\}\right| \\
&= \left|\{b \in \mathbb{Z} : 1 \leq b \leq p^\ell\}\right| \\
&= \left|\{b \in \mathbb{Z} : 1 \leq b \leq p^\ell, p \mid b\}\right| \\
&= p^\ell - p^{\ell-1}
\end{aligned}$$

Definition: Left Multiplication

Let G be a group. For $a \in G$, the left multiplication by a to be the map $L_a(x) = ax$ for $x \in G$.

We can define the same for right multiplication except $R_a(x) = xa$.

L_a is a permutation of G, i.e. $L_a \in \text{Perm}(G)$. It is a permutation since $L_{a^{-1}}$ is the inverse of L_a, $L_{a^{-1}}(ax) = a^{-1}(ax) = x$.

Moreover, the map $a \mapsto L_a$ and $G \mapsto \text{Perm}(G)$ is a homomorphism ($L_{ab} = L_a L_b$ since $ab(x) = a(bx)$). Further, L_a is an injection. If L_a is the identity mapping of G, i.e. $L_a(x) = x$ for all $x \in G$, so $a = e$, thus, ker is $\{e\}$.

However, $L_a : G \to G$ is not a homomorphism unless $a = \{e\}$ since $L_a(e) = e$ implies $a = e$.

Similarly, R_a is not a homomorphism. If $G \mapsto \text{Perm}(G)$ and $a \mapsto R_a$ might not be a homomorphism since $R_{ab}(x) = xab = R_b R_a(x)$.

Definition: Conjugation

Define the map $C_a : G \to \ G$

$$C_a = L_a R_{a^{-1}}, C_a(x) = axa^{-1}$$

C_a is a group homomorphism and isomorphism since

$$\begin{aligned} C_{ab}(x) &= ab(x)(ab)^{-1} \\ &= a(bxb^{-1})a^{-1} \\ &= a(C_b(x))a^{-1} \\ &= C_a(C_b(x)) \\ &= C_aC_b(x) \end{aligned}$$

Thus, $C_a \in \mathrm{Aut}(G)$.

Definition: Inner Automorphism

$$\mathrm{Inn}(G) = \{C_a : a \in G\}$$

Since $(C_a)^{-1} = C_{a^{-1}}$, then $\mathrm{Inn}(G)$ is a subgroup of $\mathrm{Aut}(G)$.

We define

$$C_a(H) = \{aha^{-1} : h \in H\} \cong H$$

Then H and $C_a(H)$ are called conjugate subgroups of G.

If G is Abelian, $\mathrm{Inn}(G) = \mathrm{id}$.

Consider $G = \mathbb{Z}_2 \times \mathbb{Z}_2 = \{(a,b) : a \in \{0,1\}, b \in \{0,1\}\}$. $\phi : G \to G$ where $(a,b) \mapsto (b,a)$ is a non-trivial automorphism.

Thus, $\mathrm{Inn}(\mathbb{Z}_2 \times \mathbb{Z}_2) \ncong \mathrm{Aut}(\mathbb{Z}_2 \times \mathbb{Z}_2)$. If an automorphism is not an inner one, it is called an outer automorphism.

E.g. Let G be a finite group with $|G| = n$ and $S = \{1, \dots, n\}$.

Define $f : G \to S$ be a bijection. The map $C_f : \mathrm{Perm}(G) \to S_n$ by

$$C_f(g) = f \circ g \circ f^{-1}$$

is a group isomorphism.

Proof. $C_f(gh) = fghf^{-1} = (fgf^{-1})(fhf^{-1}) = C_f(g) \cdot C_f(h)$. Then we show $C_{f^{-1}} = C_f^{-1}$.

Theorem (Cayley)

Let G be a group.

1. G is isomorphic to a subgroup of $\mathrm{Perm}(G)$.

2. If $|G| = n$, then G is isomorphic to a subgroup of S_n.

Proof. 1. $\phi : G \to \mathrm{Perm}(G)$ where $a \mapsto L_a$. ϕ is an injective homomorphism. Thus, $G \cong \mathrm{Im}(\phi) \leq \mathrm{Perm}(G)$.

2. Since $|G| = n$, there is a bijection $f : G \to \{1, \dots, n\}$. Thus, $C_f = \mathrm{Perm}(G) \to S_n$ is an isomorphism. The map $C_f \circ \phi$ is the injective homomorphism from $G \to S_n$. Thus, G is isomorphic to a subgroup of S_n.

E.g. $\text{Hom}(\mathbb{Z}, G) = \{\phi_a : a \in G, \phi(k) = a^k, \forall k \in \mathbb{Z}\}$. $|\text{Hom}(\mathbb{Z}, G)| = |G|$.

E.g. $\text{Hom}(\mathbb{Z}_n, G) \cong \{\phi_a : a \in G, \phi([1]) = a, |a| \mid n\}$.

Recall $|\phi(a)| \mid |a|$ so $|\phi([1])| \mid n$, which implies $\phi([1]) = a$ and $|a| \mid n$.

Chapter 5

Cosets, Normal Subgroups, and Quotient Groups

Definition: Left Coset

Let G be a group with $*$ binary operation, let $H \leq G$ and $a \in G$. The left coset of H in G containing a is the set

$$aH = a * H = \{ax : x \in H\}$$

The right coset is $Ha = \{xa : x \in H\}$.

We denote G/H to be the set of all left cosets of H in G, i.e. $\{aH : a \in G\}$, and $H \backslash G$ is the set of all right cosets of H in G.

Definition: Index $[G : H]$

The index of H in G is the cardinality of G/H.

Remark: If G is abelian, $aH = Ha$, then the left coset is equal to the right coset.

E.g. $G = \mathbb{Z}_{12}, H = \langle [3] \rangle = \{[3], [6], [9], [0]\}$. The cosets are

$$\begin{aligned}
0 + H &= \{0+3, 0+6, 0+9, 0+0\} = \{0, 3, 6, 9\} = H \\
1 + H &= \{1, 4, 7, 10\} \\
2 + H &= \{2, 5, 8, 11\} \\
3 + H = 6 + H = 9 + H &= \{3, 6, 9, 0\} = 0 + H = H \\
4 + H = 7 + H = 10 + H &= \{4, 7, 10, 1\} = 1 + H \\
5 + H = 8 + H = 11 + H &= 2 + H
\end{aligned}$$

E.g. $G = \mathbb{Z}, H = \langle n \rangle = n\mathbb{Z}$. The set of cosets are $\{k + n\mathbb{Z} : k \in \mathbb{Z}\} = \{k + n\mathbb{Z} : k \in \mathbb{Z}, 0 \leq k \leq n-1\}$ is the congruence class modulo n.

Since we can define the arithmetic on the congruence classes, we can define a group structure on cosets. It gives us new groups. We want the binary operation to be $(aH) * (bH) = abH$. This works in abelian groups.

However, $(ah) * (bh') \neq ab \cdot hh'$ in general.

Theorem

Let G be a group, $H \leq G$, and $a, b \in G$, then

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

(2) Either $aH = bH$ or $aH \cap bH = \emptyset$.

(3) $|aH| = |H|$.

Proof. (1) If $b \in aH$, then there exists $h \in H$ such that $b = ah$ which implies $a^{-1}bh \in H$. Conversely, if $a^{-1}b = h \in H$, then $b = ah \in aH$.

To show $a^{-1}b \in H$ if and only if $aH = bH$, it is enough to show $bH \subseteq aH$. For all $h' \in H$, let $a^{-1}b = h' \in H$, $bh = (ah')h = ah'h \in aH$, so $bH \subseteq aH$.

(2) Assume that $aH \cap bH \neq \emptyset$, i.e. there exists h, h' such that $ah = bh'$. This gives $a^{-1}b = hh'^{-1} \in H$ and $aH = bH$.

Theorem

Let G be a group and $H \leq G$, the following are equivalent:

(1) We can define a binary operation $*$ on G/H by $(aH) * (bH) = abH$.

(2) $aha^{-1} \in H$ for all $a \in G, h \in H$.

(3) $aH = Ha$ for all $a \in G$.

(4) $aHa^{-1} = H$ for all $a \in G$.

Proof. (1) $\iff$ (2) The binary operation is well-defined means that for all $a_1, a_2, b_1, b_2 \in G$, if $a_1H = a_2H, b_1H = b_2H$, then $(a_1H)(b_1H) = (a_2H)(b_2H)$ or equivalently if $a_1^{-1}a_2 \in H$ and $b_1^{-1}b_2 \in H$, then $(a_1b_1)^{-1}(a_2b_2) \in H$.

For $a_1^{-1}a_2 = h_1 \in H$, $b_1^{-1}b_2 = h_2 \in H$, we have

$$b_1^{-1}a_1^{-1} \cdot a_2b_2 = b_1^{-1}h_1b_2 = b_1^{-1}b_2(b_2^{-1}h_1b_2) = h_2(b_2^{-1}h_1b_2)$$

$h_2(b_2^{-1}h_1b_2) \in H$ if and only if $b_2^{-1}h_1b_2 \in H$ if and only if for all $b \in G, h \in H$, $b^{-1}hb \in H$.

(2) $\implies$ (3) Assume that (2) holds. Let $x \in aH$, say $x = ah, h \in H$. Then $x = ah = (aha^{-1})a = h'a \in Ha$ since $h' \in H$ cause of conjugation. Thus, $aH \subseteq Ha$ (converse is the same).

(3) $\implies$ (2) Suppose that (3) holds. Let $a \in G, h \in H$. $ah \in aH = Ha$. Thus, there exists $h' \in H$, such that $ah = h'a$. But this means $aha^{-1} = h' \in H$.

Definition: Normal Subgroup $H \trianglelefteq G$

A subgroup satisfying the conditions (1) to (4) from the previous theorem.

Definition: Quotient Group

If $H \trianglelefteq G$, then G/H is the quotient group of G by H.

E.g. $H = \{e\}, G$ are normal subgroups.

Definition: Simple Group

A group is simple if it has two normal subgroups, namely $\{e\}$ and G.

Theorem (Lagrange)

Let G be a group and $H \leq G$, then

$$|G| = |G/H| \cdot |H|$$

If G is finite, then $|G/H| = \frac{|G|}{|H|}$.

Proof. Claim: There is a bijection between H and aH.
Proof. (Claim) $\phi : H \to aH$ by $\phi(h) = ah$ for $h \in H$ and $\phi^{-1} : aH \to H$ by $\phi^{-1}(b) = a^{-1}b$ for $b \in aH$. So $\phi \circ \phi^{-1} = \mathrm{id}_{aH}$ and $\phi^{-1} \circ \phi = \mathrm{id}_H$. Thus, $|G| = |G/H| \cdot |H|$.

Corollary

Let G be a finite group, $H \leq G$, and $a \in G$, then $|H|$ divides $|G|$ and $|a|$ divides $|G|$.

Proof. Since $|G/H| \in \mathbb{Z}$, then by Lagrange's theorem, we have $|H| \mid |G|$. $|a| = |\langle a \rangle| \mid |G|$.

Corollary (Euler-Fermat)

For all $a \in U_n$, $a^{\varphi(n)} = 1$.

Proof. $|U_n| = \varphi(n)$.

Corollary (Classification of Groups of Order p)

Let p be prime and $|G| = p$, then $G \cong \mathbb{Z}_p$.
In particular, G is abelian.

Proof. Let $a \in G, a \neq e$. Since $|a|$ divides $|G| = p$, so $|a| = 1$ or $|a| = p$. Since $a \neq e$, $|a| = p$, so $\langle a \rangle = G$ and $G \cong \mathbb{Z}_p$.

Theorem (First Isomorphism)

(1) If $\phi : G \to H$ is a homomorphism and $\ker(\phi) = K$, then $K \trianglelefteq G$ and $G/K \cong \text{Im}(\phi)$. Indeed, the map $\Phi : G/K \to \phi(G)$ by $\Phi(aK) = \phi(a) \in H$ is an isomorphism.

(2) If $K \trianglelefteq G$, then the map $\phi : G \to G/K$ given by $\phi(a) = aK$ is a homomorphism with $\ker(\phi) = K$.

Proof. (1) For all $k \in K$ and $a \in G$, $\phi(aka^{-1}) = \phi(a)\phi(k)\phi(a^{-1}) = \phi(a) \cdot e_H \cdot \phi(a)^{-1} = e_H$. Thus, $aka^{-1} \in \ker(\phi) = K$ and it shows that K is normal in G.

By definition of Φ, for all $a, b \in G$,

$$\Phi(abK) = \phi(ab) = \phi(a)\phi(b) = \Phi(aK)\phi(bK)$$

Thus, Φ is a homomorphism.

Φ is surjective since for all $b \in \phi(G)$, there exists $a \in G$ with $\phi(a) = b$ and $\Phi(aK) = \phi(a) = b$.

To show Φ is injective, it is enough to show $\ker(\Phi) = \{K\}$, the identity in G/K. Let $aK \in \ker(\Phi)$. $\Phi(aK) = \phi(a) = e_H$. This implies $a \in \ker(\phi) = K$. So $e_G^{-1} \cdot a \in K \implies aK = eK = K$.

(2) For all $a, b \in G$, $\phi(ab) = abK = aK \cdot bK$ since $K \trianglelefteq G$. $aK \cdot bK = \phi(a)\phi(b)$. So ϕ is a homomorphism. ϕ is surjective since for all $aK \in G/K$, $\phi(a) = aK$. For all $a \in \ker(\phi)$ if and only if $\phi(a) = eK = K$ if and only if $aK = K$ if and only if $a \in K$. Thus, $\ker(\phi) = K$.

Theorem (Second Isomorphism)

Let G be a group and $H \leq G$ and $K \trianglelefteq G$, then $K \cap H \trianglelefteq H$.
Let $KH = \{kh : k \in K, h \in H\} \subseteq G$. Then KH is a subgroup of G and $H/(K \cap H) \cong KH/K$.

Theorem (Third Isomorphism)

Let G be a group and $K \trianglelefteq G$, then there is a one-to-one correspondence between $\{H \leq G : K \leq H\}$ and $\{H' : H' \leq G/K\}$.
Moreover, this correspondence preserves the normality, i.e. if $K \leq H \trianglelefteq G$, we have $(G/K)/(H/K) \cong G/H$.

E.g. $\phi : \mathbb{Z} \to \mathbb{Z}_n$. $\ker(\phi) = n\mathbb{Z} = \{n\ell : \ell \in \mathbb{Z}\}$. Then $\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}_n$.

E.g. $\phi : \mathbb{R} \to S^1 = \{e^{i\theta} : \theta \in \mathbb{R}\}$ by $\phi(\theta) = e^{i\theta} = \{z \in \mathbb{C} : |z| = 1\}$. Then $\ker(\phi) = \{2\pi n : n \in \mathbb{Z}\} = 2\pi\mathbb{Z}$. By the Isomorphism theorem, $\mathbb{R}/2\pi\mathbb{Z} \cong S^1$.

E.g. $\phi : \mathbb{C}^* \to \mathbb{R}^+$ by $\phi(z) = |z|$. $\phi(zw) = |zw| = |z|\,|w|$. $\ker(\phi) = S^1$. So $\mathbb{C}^*/S^1 \cong R^+$.

E.g. $\phi : \mathbb{C}^* \to S^1$ by $\phi(z) = \frac{z}{|z|}$. $\ker(\phi) = \{z/\,|z| = 1 : z \in \mathbb{C}^*\} = \{z = |z| : z \in \mathbb{C}^*\} = \mathbb{R}^+$. So $\mathbb{C}^*/\mathbb{R}^+ \cong S^1$.

E.g. $\phi : GL_n(R) \to R^*$. $\ker(\phi) = SL_n(R)$. $GL_n(R)/SL_n(R) \cong R^*$.

E.g. $\text{sign} : S_n \to \mathbb{Z}^* = \{1, -1\}$. $\ker(\phi) = A_n$. So $S_n/A_n \cong \mathbb{Z}^*$.

E.g. $H = \langle (6,2), (3,6) \rangle \trianglelefteq \mathbb{Z}^2$. $|\mathbb{Z}^2/H| = 30$ and $\mathbb{Z}^2/H$ is cyclic and a generator.

E.g. Recall $\forall a \in G, C_a : G \to G$ and $\text{Inn}(G) = \{C_a : a \in G\} \leq \text{Aut}(G)$. Define $\phi : G \to \text{Inn}(G)$ with $a \mapsto C_a$. It is a homomorphism. To understand $\text{Inn}(G)$, we need to understand $\ker(\phi)$.

$a \in \ker(\phi)$ if and only if C_a is the identity map if and only if $\forall g, aga^{-1} = g, ag = ga$ or $a \in Z(G)$. Thus, by the 1st Isomorphism Theorem, $\text{Inn}(G) \cong G/Z(G)$.

Definition: Centralizer

Let $H \leq G$. The centralizer of H in G is the set

$$C(H) = C_G(H) = \{a \in G : ax = xa, \forall x \in H\}$$

Definition: Normalizer

Let $H \leq G$. The normalizer of H in G is the set

$$N(H) = N_G(H) = \{a \in G : aH = Ha\}$$

E.g. Let $H = G$. Then $C(H) = Z(G)$ and $N(H) = G$.

Theorem (Normalizer/Centralizer)

Let $H \leq G$. Then $C(H) \trianglelefteq N(H)$ and $N(H)/C(H)$ is isomorphic to a subgroup of $\text{Aut}(H)$.

Theorem (Characterization of Internal Direct Product)

Let G be a group and $H \trianglelefteq G, K \trianglelefteq G$. Suppose $H \cap K = \{e\}$ and $G = HK = \{hk : h \in H, k \in K\}$, then $G \cong H \times K$.

Proof. Define $\phi : H \times K \to G$ by $\phi((h,k)) = hk$. ϕ is surjective by definition.

ϕ is a homomorphism since

$$\phi((h_1,k_1)(h_2,k_2)) = \phi((h_1h_2, k_1k_2)) = h_1h_2k_1k_2 = h_1(k_1[k_1^{-1})h_2k_1(h_2^{-1}]h_2)k_2$$

We must show $k_1^{-1}h_2k_1h_2^{-1} = e$ (the part is square brackets). If so, then we have

$$\phi((h_1,k_1)(h_2,k_2)) = \phi((h_1,k_1))\phi((h_2,k_2))$$

Since $H \trianglelefteq G$, $k_1^{-1}h_2k_1 \in H$, then $k_1^{-1}h_2k_1h_2^{-1} \in H$. Since $K \trianglelefteq G$, $h_2k_1h_2^{-1} \in K$, then $k_1^{-1}h_2k_1h_2^{-1} \in K$. So $k_1^{-1}h_2k_1h_2^{-1} \in H \cap K = \{e\}$, thus $k_1^{-1}h_2k_1h_2^{-1} = e$.

It remains to show ϕ is injective. This is the same as $\ker(\phi) = (e,e)$. $\phi((h,k)) = e \in G$ if and only if $hk = e$ if and only if $h = k^{-1} \in K \in H$ if and only if $h, k \in K \cap H = \{e\}$ which implies $h = k = e$.

Theorem (Classification of Groups of Order $2p$)

Let p be a prime. If $|G| = 2p$, then $G \cong \mathbb{Z}_{2p}$ or $G \cong D_p$.

Proof. If G is cyclic. Then $G \cong \mathbb{Z}_{2p}$.

So assume G has no element of order $2p$. Every element is of order 2. Since G is not cyclic, for all $a \in G$, $|a| = 1, 2, p$. Thus, if $a \in G, a \neq e$, $|a| = 2$ or p.

Case 1: Every non-identity element is of order 2.
Then G must be abelian, since for all $a, b \in G$, $a^2 = b^2 = (ab)^2 = e$ and $ab = b^2aba^2 = b(baba)a = b(ba)^2a = ba$. Pick up any two distinct non-identity elements a, b. Let $H = \{e, a, b, ab\}$ is a subgroup of G. By Lagrange's Theorem, $4 = |H| \mid |G|$ implies $2 \mid p$, so $p = 2$.

Case 2: There is an element of order p.
We show $G \cong D_p$. Suppose that $a \in G$, $|a| = p$. $\langle a \rangle$ has index 2 in G, i.e. for all $b \in G$, $b \notin \langle a \rangle$ and $\langle a \rangle \cup b \langle a \rangle = G$.

Note that $b^2 \langle a \rangle \neq b \langle a \rangle$ since $b = b^{-1}b^2 \notin \langle a \rangle$, so we must have $b^2 \langle a \rangle = \langle a \rangle$.

Note that $|b| \neq p$ otherwise $b^p = e$ which implies $b = b^{p+1} \in \langle b^2 \rangle \subseteq \langle a \rangle$. Thus, $|b| = 2$.

We know $G = \langle a \rangle \cup \langle a \rangle b$ for $b \notin \langle a \rangle$.

$$G = \{e = a^0, a^1, \dots, a^{p-1}, b, ab, a^2b, \dots, a^{p-1}b\}$$

We only need to know how they multiply together. Consider ab. $ab \notin \langle a \rangle$ since if $ab = a^i$, $b = a^{i-1} \in \langle a \rangle$. Thus, $(ab)^2 = e$ and $aba(bb) = eb = b \implies aba = b$.

For all $b \notin \langle a \rangle$, we know $G = \langle a \rangle \cup b \langle a \rangle$ and $b^2 \langle a \rangle \neq \langle a \rangle$ since $b = b^{-1}b^2 \in \langle a \rangle$. Thus, $b^2 \langle a \rangle = \langle a \rangle$. If $|b| = p$, then $b = b^{p+1} = (b^2)^{(p+1)/2} \in \langle a \rangle$.

$a^{-1}aba = a^{-1}b \implies ba = a^{-1}b \implies ba = a^{p-1}b$. $G = \{b^ja^i : 0 \leq i \leq p-1, 0 \leq j \leq 1\}$. Using this,w e have

$$a^ka^\ell = a^{k+\ell}, a^kba^\ell = ba^{k-\ell}, ba^ka^\ell = ba^{k+\ell}, ba^kba^\ell = a^{\ell-k}$$

Let $\phi : G \to D_p$ with $b \mapsto F_0$ and $a \mapsto R_1$. The multiplication table matches.

Theorem (Classification of Groups of Order p^2)

Let p be a prime. Then if $|G| = p^2$, $G \cong \mathbb{Z}_{p^2} = \mathbb{Z}_p \times \mathbb{Z}_p$.

Proof. By Lagrange's Theorem, $a \in G, a \neq \{e\}$, $|a| = p$ or p^2. If $|a| = p^2$, $G \cong \langle a \rangle \cong \mathbb{Z}_{p^2}$ is cyclic.

Thus, we can assume that for all $a \in G, a \neq e$, $|a| = p$.

Claim: For all $a \in G, a \neq e$, $\langle a \rangle \trianglelefteq G$.
Proof. (Claim) Assume that $\langle a \rangle \not\trianglelefteq G$, i.e. there exists $x \in G$, $a^k \in \langle a \rangle$ such that $xa^kx^{-1} \notin \langle a \rangle$. This implies $xax^{-1} \notin \langle a \rangle$ since $xa^kx^{-1} = (xax^{-1})^k$ and $xax^{-1} =\neq e$. We have $xax^{-1} =$

p, so $\langle a\rangle \cap \langle xax^{-1}\rangle$ is a proper subgroup of $\langle a\rangle$. Since $|\langle a\rangle| = p$, the only proper is $\{e\}$, i.e. $\langle a\rangle \cap \langle xax^{-1}\rangle = \{e\}$. It follows that

$$e\left\langle xax^{-1}\right\rangle, a\left\langle xax^{-1}\right\rangle, \dots, a^{p-1}\left\langle xax^{-1}\right\rangle$$

are all distinct, since if $a^k\langle xax^{-1}\rangle = a^\ell\langle xax^{-1}\rangle$, $a^{k-\ell} \in \langle xax^{-1}\rangle$ implying $a^{k-\ell} \in \langle a\rangle \cap \langle xax^{-1}\rangle = \{e\}$ so $a^k = a^\ell$.

Thus, $G = \bigcup_{0\le j\le p-1} a^j\langle xax^{-1}\rangle$ (disjoint union). In particular, $x^{-1} \in a^j\langle xax^{-1}\rangle$ for some j. $x^{-1} = a^j(xax^{-1})^i = a^jxa^ix^{-1}$ implying $x = a^{-j-i} \in \langle a\rangle$, a contradiction.

From the proof of the claim, we have that for all $a, b \in G, a \neq e \neq b$, $b \notin \langle a\rangle$, $\langle a\rangle \cap \langle b\rangle = \{e\}$. Moreover, $G = \bigcup_{0\le j\le p-1} a^j\langle b\rangle$. Thus, $G = \langle a\rangle \cdot \langle b\rangle = \{a^jb^i : 0 \le j \le p-1, 0 \le i \le p-1\}$.

Further, $\langle a\rangle \trianglelefteq G, \langle b\rangle \trianglelefteq G$ and $\langle a\rangle \cap \langle b\rangle = \{e\}$ by the characterization of direct product, $G \cong \langle a\rangle \times \langle b\rangle \cong \mathbb{Z}_p \times \mathbb{Z}_p$.

Theorem

For $n \geq 5$, A_n is simple.

Proof. Let $\{e\} \neq H \trianglelefteq A_n$. We would like to show $H = A_n$.

Case 1: H has a 3-cycle, i.e. $(abc) \in H$. Then $k \in \mathbb{N}$, $K \neq a, b, c$, we have $(abk) = (ab)(ck)(abc)^2(ck)(ab) \in H$ since H is normal since $\{(abk) : k \in \mathbb{N}, k \neq ab\}$ generates A_n.

Case 2: H contains an element α containing a 4-cycle in one of its cycle representation $r \geq 4$, $\alpha = (a_1, a_2, \dots, a_r)\beta \in H, r \geq 4$.

$$(a_1a_3a_r) = \alpha^{-1}(a_1a_2a_3)\alpha(a_1a_2a_3)^{-1} \in H$$

Now it goes back to case 1.

Case 3: H contains an element α whose cycle representation has two 3-cycles, i.e. $\alpha = (a_1a_2a_3)(a_4a_5a_6)\beta \in H$.

$$(a_1a_4a_2a_6a_5) = \alpha^{-1}(a_1a_2a_4)\alpha(a_1a_2a_4^{-1}) \in H$$

Now it goes back to case 2.

Case 4: H contains an element α of the following cycle type: $\alpha = (a_1a_2a_3)\beta \in H$, where β is a product of distinct 2-cycles.

$$\alpha^2 = (a_1a_3a_2)\beta^2 = (a_1a_3a_2 \in H$$

This goes back to case 1.

Case 5: H contains α with $\alpha = (a_1a_2)(a_3a_4)\beta \in H$.

$$(a_1a_3)(a_2a_4) = a^{-1}(a_1a_2a_3)\alpha(a_1a_2a_3)^{-1} \in H$$

Let $\gamma = (a_1a_3)(a_2a_4)$ and choose $b \neq 1, 2, 3, 4$,

$$(a_1a_3b) = \gamma(a_1a_2b)\gamma(a_1a_3b)^{-1} \in H$$

This goes back to case 1.

Chapter 6

Classification and Finite Abelian Groups

Definition: Free Abelian Group of Rank n

An abelian group isomorphic to $\mathbb{Z}^n$.

Theorem

Then rank of a free abelian group G is unique, i.e. $G \cong \mathbb{Z}^n \cong \mathbb{Z}^m$ and $n = m$.

Proof. Suppose that $G \cong \mathbb{Z}^n \cong \mathbb{Z}^m$. Thus, there exists an isomorphism $\phi : \mathbb{Z}^n \to \mathbb{Z}^m$. Note that $\phi(2\mathbb{Z}^n) = 2\mathbb{Z}^m$ so it induces an isomorphism $\psi : \mathbb{Z}^n/2\mathbb{Z}^n \to \mathbb{Z}^m/2\mathbb{Z}^m$ given by $\psi(k + 2\mathbb{Z}^n) = \phi(k) + 2\mathbb{Z}^m$. Also note that $\mathbb{Z}^n/\mathbb{Z}^n \cong \mathbb{Z}_2^n$ and $\mathbb{Z}^m/2\mathbb{Z}^m \cong \mathbb{Z}_2^m$, so we have $\mathbb{Z}_2^n \cong \mathbb{Z}_2^m$. Thus, $2^n = |\mathbb{Z}_2^n| = |\mathbb{Z}_2^m| = 2^m$, so $n = m$.

Definition: Linear Combination

Let G be an additive abelian group. Let $u_1, \ldots, u_\ell \in G$ and $U = \{u_1, \ldots, u_\ell\}$. A linear combination of elements in U (over $\mathbb{Z}$) is an element of G of the form

$$aa_1u_1 + a_2u_2 + \cdots + a_\ell u_\ell$$

for $a_i \in \mathbb{Z}$.

Definition: Span

The span of U (over $\mathbb{Z}$) is the set of all linear combinations of elements in U.

$$\mathrm{Span}_{\mathbb{Z}}(U) = \langle U \rangle = \{a_1u_1 + \cdots + a_\ell u_\ell : a_i \in \mathbb{Z}\}$$

Definition: Linear Independent

U is linearly independent (over $\mathbb{Z}$) when for all $a_i \in \mathbb{Z}$, if $a_1u_1 + \cdots + a_\ell u_\ell = 0$, then $a_1 = a_2 = \cdots = a_\ell = 0$.

Definition: Basis

U is a basis for G (over $\mathbb{Z}$) when U is linearly independent and $\mathrm{Span}_{\mathbb{Z}}(U) = G$. An ordered basis for G is an ordered n-tuple $(u_1, \ldots, u_n) \in G^n$ such that $U = \{u_1, \ldots, u_n\}$ is a basis for G with $|U| = n$, the rank of G.
Also, every element in G can be written uniquely as a linear combination of U.

E.g. Let $e_k = (0, \ldots, 0, 1, 0, \ldots, 0) \in \mathbb{Z}^n$ where 1 is in the kth position. Then $\{e_1, e_2, \ldots, e_n\}$ is a basis for $\mathbb{Z}^n$, which we call the **standard basis** for $\mathbb{Z}^n$ over $\mathbb{Z}$.

Theorem

Let G be an abelian group. Then G is a free abelian group of rank n if and only if G has a basis over $\mathbb{Z}$ with n-elements.

Proof. ($\Longrightarrow$) $\{e_k\}$ is a basis of n elements.

($\Longleftarrow$) If $U = \{u_1, \ldots, u_k\}$ be a basis of G over $\mathbb{Z}$, define $\phi(t_1, \ldots, t_n) = t_1u_1 + \cdots + t_nu_n$, then ϕ is an isomorphism.

Theorem

Let $U = (u_1, \ldots, u_n)$ be an ordered basis over $\mathbb{Z}$ for the free abelian group G. Then we can perform any of the following operations to the elements in the basis to obtain a new ordered basis.

1. $u_i \leftrightarrow u_j$ (interchange two elements).
2. $u_i \mapsto \pm u_i$ (multiply an element by ± 1).
3. $u_i \mapsto u_i + ku_j$ (add integer multiple of one element to another).

Theorem (Subgroups and Quotient Groups of $\mathbb{Z}^n$)

Let G be a free abelian group of rank n and $H \leq G$. Then H is a free abelian group of rank r with $0 \leq r \leq n$ and

$$G/H \cong \mathbb{Z}_{d_1} \times \mathbb{Z}_{d_2} \times \cdots \times \mathbb{Z}_{d_r} \times \mathbb{Z}^{n-r}$$

for some $d_i \in \mathbb{N}$ with $d_1 \mid d_2, d_2 \mid d_3, \ldots, d_{r-1} \mid d_r$.

Proof. Claim: There exists a basis $\{u_1, \ldots, u_n\}$ for G and $r \in \mathbb{Z}, 0 \leq r \leq n$ and $d_1 \mid d_2, \ldots, d_{r-1} \mid d_r$ such that $\{d_1u_1, \ldots, d_ru_r\}$ is a basis for H.

If the claim is true, it is clear that

$$G/H \cong \mathbb{Z}_{d_1} \times \cdots \times \mathbb{Z}_{d_r} \times \mathbb{Z}^{n-r}$$

Thus, we only need to prove the claim.

Proof. (Claim) We prove by induction on n.

If $n = 0$, $G = \{0\}$ and $H = \{0\}$.

If $n = 1$, $G \cong \mathbb{Z}$ and $H = d\mathbb{Z}$, so $1 = u_1, d_1 = d$.

Let $n \geq 2$ and suppose that the statement is true for any free abelian group of rank $n - 1$. Let $G \cong \mathbb{Z}^n$ with $H \leq G$. If $H = \{0\}$, then $r = 0$ and we are done.

Assume that $H \neq \{0\}$. Let T be the set of all coefficients t_i in all linear combinations $a = t_1 v_1 + \cdots + t_n v_n$ over all elements $a \in H$ and all possible choices of bases $\{v_1, \ldots, v_n\}$.

Let $d_1 \in \mathbb{N}$ be the smallest positive integer in T. Choose a basis $\{v_1, \ldots, v_n\}$ for G and $a \in H$, $a = d_1 v_1 + t_2 v_2 + \cdots + t_n v_n$. Note that $d_1 \mid t_i$ because if we write $t_i = q_i d_1 + r_i$ with $0 \leq r_i < d_1$, then

$$a = d_1 v_1 + (q_2 d_1 + r_2) v_2 + \cdots = d_1(v_1 + q_2 v_2 + \cdots + q_n v_n) + r_2 v_2 + \cdots + r_n v_n$$

and so each $r_i = 0$ by the choice of d_1 since $\{v_1 + \sum q_i v_i, v_2, \ldots, v_n\}$ is a basis of G. Choose $\{u_1, v_2, \ldots, v_n\}$, $u_1 = v_1 + q_2 v_2 + \cdots + q_n v_n$ to be a basis for G and $a = d_1 u_1 \in H$.

Let $G_0 = \mathrm{Span}_{\mathbb{Z}}\{v_2, \ldots, v_n\}$ and $H_0 = H \cap G$. Since $\{u_1, \ldots, v_n\}$ is a basis for G, for every $a \in G$ where $a = t_1 u_1 + t_2 v_2 + \cdots + t_n v_n$ uniquely, let $a \in H$, then we must have $d_1 \mid t_1$ because if $t_1 = q_1 d_1 + r_1, 0 \leq r_1 < d_1$, then $a = (q_1 d_1 + r_1) u_1 + t_2 v_2 + \cdots + t_n v_n \in H$ and $d_1 u_1 \in H$, then $r_1 u_1 + t_2 u_2 + \cdots + t_n v_n \in H$. So $r_1 = 0$. Thus, for all $a \in H$, $a = t_1(d_1 u_1) + t_2 v_2 + \cdots + t_n v_n$, we have $b = t_2 v_2 + \cdots + t_n v_n = a - t_1(d_1 u_1) \in H$.

By induction hypothesis on G_0 and H_0, there exist a basis $\{u_2, \ldots, u_n\}$ and $d_2, \ldots, d_n$ where $d_2 \mid d_3 \mid \cdots \mid d_r$ such that $\{d_2 u_2, \ldots, d_n u_n\}$ is a basis for H_0. Then $\{d_1 u_1, \ldots, d_n u_n\}$ is a basis for H.

Theorem (Classification of Finite Abelian Groups)

Every finite abelian group is isomorphic to a unique group of the form

$$\mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2} \times \cdots \times \mathbb{Z}_{n_\ell}$$

for some $\ell \geq 0, n_i \in \mathbb{N}, n_1 \geq 2, n_1 \mid n_2, n_2 \mid n_3, \ldots, n_{\ell-1} \mid n_\ell$.
Alternatively, every finite abelian group is isomorphic to a unique group of the form

$$\mathbb{Z}_{p_1^{k_1}} \times \mathbb{Z}_{p_2^{k_2}} \times \cdots \times \mathbb{Z}_{p_m^{k_m}}$$

for some $m \geq 0$, p_i prime with $p_1 \leq p_2 \leq \cdots \leq p_m$ and $k_i \leq k_{i+1}$ when $p_i = p_{i+1}$.
$|G| = \prod\limits_{i=1}^{\ell} n_i = \prod\limits_{i=1}^{m} p_i^{k_i}$.

Proof. **Existence**: First, we prove that every finite abelian group is isomorphic to the first form. Let G be a finite abelian group of order n, i.e. $G = \{a_1, \ldots, a_n\}$. Define $\phi : \mathbb{Z}^n \to G$ by $\phi(t_1, \ldots, t_n) = t_1 a_1 + \cdots + t_n a_n$. ϕ is a homomorphism. By the First Isomorphism Theorem, we have

$$G \cong \mathbb{Z}^n / \ker(\phi) \cong \mathbb{Z}_{d_1} \times \mathbb{Z}_{d_2} \times \cdots \times \mathbb{Z}_{d_r} \times \mathbb{Z}^{n-r}$$

Since G is finite, $n = r$. By theorem $d_1 \mid d_2 \mid \cdots \mid d_r$. Set $d_i = n_i$ and we are done.

Example: $G = \mathbb{Z}_2 \times \mathbb{Z}_4 \times \mathbb{Z}_{12} \times \mathbb{Z}_{24} \times \mathbb{Z}_{720}$. Recall $\mathbb{Z}_{m \times n} \cong \mathbb{Z}_m \times \mathbb{Z}_n$ if $\gcd(m, n) = 1$. So

$$G \cong \mathbb{Z}_2 \times \mathbb{Z}_4 \times (\mathbb{Z}_4 \times \mathbb{Z}_3) \times (\mathbb{Z}_8 \times \mathbb{Z}_3) \times (\mathbb{Z}_{16} \times \mathbb{Z}_9 \times \mathbb{Z}_5)$$

$$G \cong \mathbb{Z}_2 \times \mathbb{Z}_{2^2} \times \mathbb{Z}_{2^2} \times \mathbb{Z}_{2^3} \times \mathbb{Z}_{2^4} \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_{3^2} \times \mathbb{Z}_5$$

To get from 2nd form to 1st form:

$$\begin{aligned} G &\cong \mathbb{Z}_2 \times \mathbb{Z}_4 \times \mathbb{Z}_4 \times \mathbb{Z}_8 \times \mathbb{Z}_{16} \\ &\quad \times \mathbb{Z}_{3^0} \times \mathbb{Z}_{3^0} \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_{3^2} \\ &\quad \times \mathbb{Z}_{3^0} \times \mathbb{Z}_{5^0} \times \mathbb{Z}_{5^0} \times \mathbb{Z}_{5^0} \times \mathbb{Z}_5 \\ &= \mathbb{Z}_2 \times \mathbb{Z}_4 \times \mathbb{Z}_{12} \times \mathbb{Z}_{24} \times \mathbb{Z}_{720} \end{aligned}$$

by multiplying each column.

Uniqueness: Suppose that

$$G \cong \mathbb{Z}_{p_1^{k_1}} \times \cdots \times \mathbb{Z}_{p_m^{k_m}}$$

Let n_k be the number of elements in G whose order divides p^k. Note that n_k is invariant under isomorphisms. Let a_k be the number of indices i such that $p_i = p$ and $k_i = k$. Let b_k be the number of indices i such that $k_i \geq k$. Note that $a_k = b_k - b_{k+1}$.

Using the fact that for $x_i \in \mathbb{Z}_{p_i^{k_i}}$,

$$|(x_1, \ldots, x_m)| = \operatorname{lcm}(|x_1|, \ldots, |x_m|)$$

so

$$\begin{aligned} n_1 &= p^{b_1} \\ n_2 &= p^{a_1} p^{2b_2} \\ n_3 &= p^{a_1} p^{2a_2} p^{3b_3} \\ &\vdots \\ n_k &= p^{a_1} p^{2a_2} p^{3a_3} \ldots p^{(k-1)a_{k-1}} p^{kb_k} \end{aligned}$$

The factorization of n_i gives us p_i, a_i, b_i. In general, $\frac{n_k}{n_{k-1}} = p^{b_k}$ and $p^{a_k} = \frac{n_k^2}{n_{k-1} \cdot n_{k+1}}$. Therefore, p_i, a_i, b_i are unique.

Corollary

Let G and H be two finite abelian groups. If G and H have the same number of elements each other, then $G \cong H$.

Corollary

Let $n = \prod p_i^{k_i}$ be a prime factorization of n, where p_i are distinct primes. Then the number of distinct abelian groups of order n (up to isomorphisms) is equal to $\prod p(k_i)$, where $p(k)$ is the number of partitions of k.

Proof. The abelian group of order p^k is the group $\prod \mathbb{Z}_{p^{j_i}}$ with $\sum j_i = k$.

E.g. Construct all abelian groups of order 72.

$72 = 2^3 \cdot 3^2$. The partitions of $3 = 3 = 2 + 1 = 1 + 1 + 1$ and $2 = 2 = 1 + 1$. So we have $\mathbb{Z}_{2^3}, \mathbb{Z}_{2^2} \times \mathbb{Z}_{2^1}, \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$ and $\mathbb{Z}_{3^2}, \mathbb{Z}_3 \times \mathbb{Z}_3$. The groups are $\mathbb{Z}_{2^3} \times \mathbb{Z}_{3^2}, \mathbb{Z}_{2^3} \times \mathbb{Z}_3 \times \mathbb{Z}_3$, etc. So we have 6 possible abelian groups of order 72.

Chapter 7

Isometrics and Symmetric Groups

$\|x-y\| = \sqrt{(x_1-y_1)^2+\cdots+(x_n-y_n)^2}$, $\|x\| = \sqrt{x_1^2+\cdots+x_n^2}$.

Definition: Preserves Distance

For a map $S : \mathbb{R}^n \to \mathbb{R}^n$, we say S preserves distance when $\|S(x)-S(y)\| = \|x-y\|$. for all $x, y \in \mathbb{R}^n$.

Definition: Isometry

An isometry on $\mathbb{R}^n$ is an invertible map $S : \mathbb{R}^n \to \mathbb{R}^n$ which preserves distance.

Theorem

The set of isometries on $\mathbb{R}^n$ is a group under composition.

Proof. The identity map $I : \mathbb{R}^n \to \mathbb{R}^n$ is an isometry because for any $x, y \in \mathbb{R}^n$, $\|I(x)-I(y)\| = \|x-y\|$.

Let S, T be isometries and for all $x, y \in \mathbb{R}^n$,

$$\|S(T(x)) - S(T(y))\| = \|T(x)-T(y)\| = \|x-y\|$$

Let S be an isometry. Given $u, v \in \mathbb{R}^n$, $x = S^{-1}(u), y = S^{-1}(v)$ and

$$\left\|S^{-1}(u) - S^{-1}(v)\right\| = \|x-y\| = \|S(x)-S(y)\| = \|u-v\|$$

Thus, S^{-1} preserves distance and it is an isometry. By the Subgroup Test, the set of all isometries is a group.

Definition: $\operatorname{Isom}(\mathbb{R}^n)$

$\operatorname{Isom}(\mathbb{R}^n)$ is the set of all isometries of $\mathbb{R}^n$ and $\operatorname{Isom}(\mathbb{R}^n) \leq \operatorname{Perm}(\mathbb{R}^n)$.

E.g. For a vector $u \in \mathbb{R}^n$, the translation by u is the map $T_u : \mathbb{R}^n \to \mathbb{R}^n$ given by $T_u(x) = x + u$. T_u is an isometry on $\mathbb{R}^n$ because $T_u^{-1} = T_{-u}$ and

$$\|T_u(x) - T_u(y)\| \, \|(u + x) - (u + y)\| = \|x - y\|$$

E.g. If $A \in O_n(\mathbb{R}) = \{B \in M_n(\mathbb{R}) : B^T B = I\}$, then the map $S : \mathbb{R}^n \to \mathbb{R}^n$ given by $S_A(x) = Ax$ is an isometry because $S_A^{-1} = S_{A^{-1}}$ and for $x, y \in \mathbb{R}^n$,

$$\begin{aligned}
\|Ax - Ay\|^2 &= \|A(x - y)\|^2 \\
&= (A(x - y))^T (A(x - y)) \\
&= (x - y)^T A^T A(x - y) \\
&= (x - y)^T (x - y) \\
&= \|x - y\|^2
\end{aligned}$$

Remark: Define the inner product $x\dot{y}$ by $x^T y$. We say that $M \in M_n(\mathbb{R})$ preserves the inner product if $M(x) \cdot M(y) = x \cdot y$. Then $S_M : \mathbb{R}^n \to \mathbb{R}^n$ where $S_M(x) = Mx$ is an isometry.

E.g. For a proper subspace U of $\mathbb{R}^n$, the reflection in U is the map $F_U : \mathbb{R}^n \to \mathbb{R}^n$ given by $F_U(x) = x - 2\,\mathrm{Proj}_{U^\perp}(x)$, where $\mathrm{Proj}_{U^\perp}(x)$ is the orthogonal product of x onto $U^\perp$ and $U^\perp = \{x \in \mathbb{R}^n : x \cdot y = 0, y \in U\}$.

When $\{u_1, \ldots, u_k\}$ is an orthonormal basis for $U^\perp$, $\|u_i\| = 1$ and $u_i \cdot u_j = 1$ if $i = j$ and $u_i \cdot u_j = 0$ if $i \neq j$ and $A = (u_1, \ldots, u_k) \in M_{n\times k}(\mathbb{R})$. Then $\mathrm{Proj}_{U^\perp}(x) = \sum_{i=1}^{k} (x \cdot u_i)u_i = AA^T x$.

$$\begin{aligned}
F_U(x) &= x - 2AA^T x \\
&= (I - 2AA^T)x \\
&= S_{(I - 2AA^T)}
\end{aligned}$$

$$(I - 2AA^T)^T (I - 2AA^T) = (I - 2AA^T)(I - 2AA^T) = I$$

Definition: Affine Space

An affine space in $\mathbb{R}^n$ is a set of the form $P = p + U = \{p + x : x \in U\}$ for some point $p \in \mathbb{R}^n$ and some vector space $U \in \mathbb{R}^n$.

Definition: Reflection

For an affine space $P = p + U$ in $\mathbb{R}^n$, the reflection in P is the map $F_P : \mathbb{R}^n \to \mathbb{R}^n$ given by

$$F_P(x) = p + F_U(x - p)$$

Note that $F_P \in \mathrm{Isom}(\mathbb{R}^n)$ because F_P is equal to the composite $F_P = T_P F_U T_{-p}$.

Theorem (Algebraic Classification of Isometries)

A map $S : \mathbb{R}^n \to \mathbb{R}^n$ preserves distance if and only if S is of the form $S(x) = Ax + b$ for some $A \in O_n(\mathbb{R})$ and some $b \in \mathbb{R}^n$.

Proof. Set $x = 0$, and $b = S(0)$. Define $L : \mathbb{R}^n \to \mathbb{R}^n$ with $L(x) = S(x) - b$. Then L preserves distance since

$$\|L(x) - L(y)\| = \|(S(x) - b) - (S(y) - b)\| = \|S(x) - S(y)\| = \|x - y\|$$

So $L(0) = S(0) - b = 0$.

We need to show $A \in O_n(\mathbb{R})$ such that $L(x) = Ax$. For $x, y \in \mathbb{R}^n$, we have

$$\|x - y\|^2 = (x - y)^T(x - y) = x^T x - x^T y - y^T x + y^T y = \|x\|^2 - 2x \cdot y + \|y\|^2$$

which we obtain the Polarization Identity:

$$x \cdot y = \frac{1}{2}(\|x\|^2 + \|y\|^2 - \|x - y\|^2)$$

Thus,

$$\begin{aligned} L(x) \cdot L(y) &= \frac{1}{2}(\|L(x)\|^2 + \|L(y)\|^2 - \|L(x) - L(y)\|^2) \\ &= \frac{1}{2}(\|x\|^2 + \left\|y^2\right\| - \|x - y\|^2) \\ &= x \cdot y \end{aligned}$$

Thus, L preserves inner product.

Let $\{e_i\}$ be the standard basis for $\mathbb{R}^n$. $L(e_i) \cdot L(e_j) = e_i \cdot e_j$ is 1 if $i = j$ and 0 if $i \neq j$. This implies $\{L(e_i)\}$ is an orthonormal basis for $\mathbb{R}^n$. Let $A = (L(e_1), \dots, L(e_n))$ and since $\{L(e_i)\}$ is an orthonormal basis and $A \in O_n(\mathbb{R})$, then $A^T A = I$.

Let $x = \sum_{i=1}^n x_i e_i$ and $L(x) = \sum_{i=1}^n t_i L(e_i)$, then for all $j \in \mathbb{N}, 1 \leq j \leq n$, we have $L(x) \cdot L(e_j) = x \cdot e_j = x_j$ since L preserves inner product. On the other hand, $L(x) \cdot L(e_j) = \left(\sum_{i=1}^n t_i L(e_i)\right) L(e_j) = t_j L(e_j) L(e_j) = t_i$. Then $x_j = t_j$. Thus, $L(x) = \sum x_i L(e_i) = Ax$.

Corollary

Every distance preserving map $S : \mathbb{R}^n \to \mathbb{R}^n$ is an isometry.

Definition: Preserves/Reverses Orientation

Let $S \in \mathrm{Isom}(\mathbb{R}^n)$ with $S(x) = Ax + b$ with $A \in O_n(\mathbb{R})$ and $b \in \mathbb{R}^n$. since $A^T A = I$ we have $\det(A) = \pm 1$. S preserves orientation when $\det(A) = 1$ and reverses orientation when $\det(A) = -1$.
We write $\mathrm{Isom}_+(\mathbb{R}^n) = \{S \in \mathrm{Isom}(\mathbb{R}^n) : S \text{ preserves orientation}\}$ and $\mathrm{Isom}_-(\mathbb{R}^n)$ likewise.

Definition: Symmetry Group

For a nonempty set $X \subseteq \mathbb{R}^n$, the symmetry group of X in $\mathbb{R}^n$ is

$$\mathrm{Sym}(X) = \{S \in \mathrm{Isom}(\mathbb{R}^n) : S(x) \in X, \forall x \in X\} = \{S \in \mathrm{Isom}(\mathbb{R}^n) : S(X) = X\}$$

Definition: Rotation Group

For a nonempty set $X \subseteq \mathbb{R}^n$, the rotation group of X in $\mathbb{R}^n$ is

$$\mathrm{Rot}(X) = \mathrm{Sym}(X) \cap \mathrm{Isom}_+(\mathbb{R}^n) = \{S \in \mathrm{Isom}_+(\mathbb{R}^n) : S(X) = X\}$$

Theorem (Fixed Point Theorem)

Let G be a finite subgroup of $\mathrm{Isom}(\mathbb{R}^n)$. Then G has a fixed point, that is there is a point $p \in G$ such that $S(p) = p$ for all $S \in G$.

Proof. Let $G = \{S_1, \ldots, S_m\} \leq \mathrm{Isom}(\mathbb{R}^n)$. Fix a point $a \in \mathbb{R}^n$ and $p = \frac{1}{m}\sum_{i=1}^m S_i(a)$.

Let $k \in \{1, \ldots, m\}$ and say $S_k = Ax + b$.

$$\begin{aligned}
S_k(p) &= S_k\left(\frac{1}{m}\sum_{i=1}^m S_i(a)\right) \\
&= A\left(\frac{1}{m}\sum_{i=1}^m S_i(a)\right) + b \\
&= \left(\frac{1}{m}\sum_{i=1}^m AS_i(a)\right) + b \\
&= \frac{1}{k}\sum_{i=1}^m (AS_i(a) + b) \\
&= \frac{1}{m}\sum_{i=1}^m S_k S_i(a) \\
&= \frac{1}{m}\sum_{i=1}^m S_i \\
&= p
\end{aligned}$$

Thus, $S_k(p) = p$ for all indices k.

E.g. Let $b \in \mathbb{R}^n$, then $H = \langle T_b \rangle \leq \mathrm{Isom}(\mathbb{R}^n)$ is the translation subgroup. $|H| = \infty$ and H has no fixed point.

Chapter 8

Group Actions

Chapter 9

Sylow Theorems