PMATH 336 Introduction to Group Theory

Keven Qiu
Instructor: Wentang Kuo
Fall 2024

Contents

1 Rings, Fields, and Groups 2

2 Subgroups 11

3 Symmetric and Alternating Groups 19

4 Homomorphisms 26

5 Cosets, Normal Subgroups, and Quotient Groups 33

6 Free and Finite Abelian Groups 34

7 Isometrics and Symmetric Groups 35

8 Group Actions 36

9 Sylow Theorems 37

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 $(r_1, s_1)\cdot(r_2, s_2) = (r_1r_2, s_1s_2)$. 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.

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

Definition: Euler's Phi Function ϕ

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

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

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

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 $2 \leq i \leq n$, $v_i \notin \text{Span}\{v_1, \ldots, v_{i-1}\}$. 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	5	7
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 $n|k$ and $m|k$ if and only if $lcm(m, n)|k$. 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 $ord(a)|m$.

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 $n|m$.

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 $\mathbb{Z}_n = \{0, \ldots, n-1\}$, $\mathbb{Z}_n$ 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. ($\Longrightarrow$) Trivial.

($\Longleftarrow$) 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 $\{a, a^2, a^3, \ldots, \} \subseteq H$. 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

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

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

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

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

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

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 $e, a, a^{-1}, a^2, a^3, \dots$. Define

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

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

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 $ord(a) = n$, $n|(k-\ell)$, 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 $\left\langle a^d \right\rangle = \{a^{kd} : k \in \mathbb{Z}_+\} = \{a^{kd} : k \in \mathbb{Z}_{n/d}\} = \{e = a^0, a^d, a^{2d}, \ldots, a^{n-d}\}$ 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 $\ell | m$.

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 $|a| = n, \forall d | n, d > 0$, $\left\langle a^d \right\rangle = \{a^{kd} : k \in \mathbb{Z}_{n/d}\}$ 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 $d | k$ 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 $a^d \subseteq < a^k >$. 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 $|a| = n$, $\left\langle a^k \right\rangle = \langle a \rangle \Leftrightarrow \gcd(k, n) = 1 \Leftrightarrow k \in U_n$.

Definition: ϕ

$$\phi(n) = n\left(\prod_{p|n}\left(1-\frac{1}{p}\right)\right)$$

Corollary

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

Corollary

Let G be a finite group, for all $d \in \mathbb{N}$, 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 $F_k = R_kF_0$.

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

Chapter 3

Symmetric and Alternating Groups

Definition: Symmetric Group S_n

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

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

E.g. S_n is big. Many known groups such as C_n, D_n can be viewed as subgroups of S_n. Recall $C_n \cong \mathbb{Z}_n = \{e^{2\pi ik/n} : k = 1, \dots, n\}$. 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 $\alpha \sim R_1$ 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 $a_1, \dots, a_\ell$ are distinct elements in $\{1, \dots, n\}$, we write $\alpha = (\alpha_1, \alpha_2, \cdots, \alpha_\ell)$ for a permutation $\alpha \in S_n$ given by $\alpha(a_1) = a_2, \alpha(a_2) = a_3, \dots, \alpha(a_{\ell-1}) = a_\ell, \alpha(a_\ell) = a_1$ and $\alpha(k) = k$ for all $k \notin \{a_1, \dots, a_\ell\}$.

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

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

Then we are done.

Proof. (Claim) Given $i, i_j, 1 \le i \le m, 1 \le i_j < \ell_i$. 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 $e = (a_1, b_1)(a_2, b_2) \ldots (a_\ell, b_\ell)$ for $\ell \geq 1$, then ℓ must be even.
3. If $\alpha = (a_1, b_1)(a_2, b_2) \ldots (a_\ell, b_\ell) = (c_1, d_1)(c_2, d_2) \ldots (c_m, d_m)$, 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.

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

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

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

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

Definition: Alternating Group A_n

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

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

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

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

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

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

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

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

$\mathrm{Im}(\phi)$ 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).

Hom(G, H) is the set of all homomorphisms from G to H. Iso(G, H) is the set of all isomorphisms from G to H.

End(G) is the set of all homomorphisms from G to G. 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 e^a. The inverse is $\log_e$.

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, $m|n$ implies $|\phi(a)| \,|\, |a|$.

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.

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

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 $S = \{1, \ldots, n\}$.

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 $f : G \to \{1, \ldots, n\}$. 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. $\mathrm{Hom}(\mathbb{Z}, G) = \{\phi_a : a \in G, \phi(k) = a^k, \forall k \in \mathbb{Z}\}$. $|\mathrm{Hom}(\mathbb{Z}, G)| = |G|$.

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

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

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, i.e. $\{aH : a \in G\}$.

Chapter 6

Free and Finite Abelian Groups

Chapter 7

Isometrics and Symmetric Groups

Chapter 8

Group Actions

Chapter 9

Sylow Theorems