Konkuk University Dept. Of Physics

Group Theory

2019 Spring Semester

Youngwan Kim

June 7, 2019

1 Binary Operations

Def 1. *For a set S, a map $* : S \to S$ is a* ***binary operation****.*

Ex 1.

1. *f*

Def 2. *For a given set S, and a binary operation $* : S \to S$,*

1. *$*$ is* ***commutative*** *if for every $a, b \in S$, $a * b = b * a$*
2. *$*$ is* ***associative*** *if for every $a, b, c \in S$, $(a * b) * c = a * (b * c)$*

Remark. *For associative binary operators, we can write $(a * b) * c = a * (b * c)$ as just $a * b * c$.*

Def 3. *Let $*$ be a binary operation on S. Also let H be a subset of S. If H is closed under $*$, we say that $* : H \times H \to H$ is the* ***induced operation*** *of $*$ on H.*

2 Isomorphic Binary Structures

Def 4. *Let $*$ be a binary operation on S. Then $(S, *)$ is called a* ***binary algebraic structure****.*

Def 5. *Let $(S, *), (S', *')$ be binary algebraic structures. An* ***isomorphism*** *is a map $f : S \to S'$ with the following conditions :*

1. *f is a bijection.*
2. *$f(a * b) = f(a) *' f(b)$ for all $a, b \in S$.*

If such isomorphism exists between such binary structures, we say that S is ***isomorphic*** *to S' and denote it as $S \simeq S'$.*

Remark. *For maps between binary algebraic structures such that only the second condition of* ***Def 5*** *holds, are called* ***homomorphisms****.*

Ex 2. *list of isomorphic structures*

Lem 1. *Suppose $(S, *) \simeq (S', *')$. If S is commutative, then $(S', *')$ is also commutative.*

Proof. Let $\phi : S \to S'$ be the isomorphism. For any $a', b' \in S'$ we can let $a' = \phi(a)$ and $b' = \phi(b)$ for some $a, b \in S$ as ϕ is a bijection. As S is commutative, $a * b = b * a$ which implies that $\phi(a*b) = \phi(b*a)$. Then as ϕ is an isomorphism, $\phi(a*b) = \phi(a)*'\phi(b) = a'*'b'$ and also for the other term, $\phi(b * a) = \phi(b) *' \phi(a) = b' *' a'$. Thus for every $a', b' \in S'$, as $a' *' b' = b' *' a$, $(S', *')$ is also commutative.

□

Def 6. *Let $(S, *)$ be a binary structure. An element $e \in S$ is an identity element if for every $a \in S$, $a * e = e * a = a$.*

Ex 3. *Examples of some binary structures and their identity elements.*

Thm 1. *Suppose e is an identity element of $(S, *)$ and consider an isomorphism $\phi : S \to S'$. Then $\phi(e)$ is also an identity element in $(S', *')$.*

Proof. For any $a' \in S'$, since ϕ is bijective, there exists some $a \in S$ such that $\phi(a) = a'$. We will show that $a' *' \phi(e) = \phi(e) *' a' = a'$. The left hand side shows up to be,

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

and the right hand side shows up to be,

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

Thus as this holds for every element in S', we can say that $\phi(e)$ is an identity element in S'.

□

Thm 2. *The identity element of any binary algebraic structure is unique.*

Proof. Consider two identity elements e, e' for a certain binary algebraic structure. As both ar e identities,

$$e * e' = e' * e = e$$

and also

$$e' * e = e * e' = e'$$

which implies that $e = e'$ for any other identity elements if there exists, and thus we can conlude that the identity element uniquely exists.

□

3 Groups

Def 7. *A binary algebraic structure $(G, *)$ is a **group** if the following conditions holds*

*(G_1) **Associativity** :* $\forall a, b, c \in G : (a * b) * c = a * (b * c)$

*(G_2) **Identity element** :* $\exists e \in G : \forall a \in G, e * a = a * e = a$

*(G_3) **Inverse element** :* $\exists b \in G : \forall a \in G, b * a = a * b = e$

Ex 4. *content...*

Def 8. *Let $(G, *)$ be a group. G is **abelian** if $*$ is commutative.*

Lem 2. *Let G be a group and $x \in G$. Then x has a unique inverse element.*

Proof. Suppose y, z are both the inverse element of x. Which is equivalent to,

$$\begin{aligned}
&\iff x * y = e, x * z = e \implies x * y = x * z \\
&\implies y * (x * y) = y * (x * z) \\
&\implies (y * x) * y = (y * x) * z \\
&\implies e * y = e * z \\
&\implies y = z
\end{aligned}$$

□

Thm 3. *Let G be a group where $a, b, c \in G$. Then the following holds*

1. ***left cancellation** : $a * b = a * c \implies b = c$*
2. ***right cancellation** : $b * a = c * a \implies b = c$*

Thm 4. *Let G be a group with $a, b, x \in G$. Then*

1. *$a * x = b$ has a unique solution for x, which is $x = a^{-1}b$.*
2. *$x * a = b$ has a unique solution for x, which is $x = ba^{-1}$.*

Thm 5. *Let G be a group where $a, b \in G$. Then*

1. *$(a^{-1})^{-1} = a$*
2. *$(a * b)^{-1} = b^{-1} * a^{-1}$*

Proof.

1. $a * a^{-1} = a^{-1} * a = e \iff (a^{-1})^{-1} = a$
2. $(a * b) * (b^{-1} * a^{-1}) = (b^{-1} * a^{-1}) * (a * b) = e$

□

Def 9. *Let $(G, *)$ be a group, then we define the **order of the group** denoted as $|G|$, as the number of elements in G. If such $|G|$ is finite, we call G a **finite group**.*

Def 10. *We call a group G, a* ***trivial group*** *if $|G| = 1$. A trivial group only has the identity element as its element.*

Ex 5. *Let us classify finite groups with $|G| \leq 4$.*

1. $|G| = 1$ *: trivial group*

$*$	e
e	e

Every group with order 1 are all isomorphic, as a trivial group only has the identity element as its element.

2. $|G| = 2$

$*$	e	a
e	e	a
a	a	e

Again for every finite groups with order 2 are also all isomorphic.

3. $|G| = 3$

$*$	e	a	b
e	e	a	b
a	a	b	e
b	b	e	a

For every finite groups with order 3 are also all isomorphic.

4. $|G| = 4$

Now we can't say that every finite groups with order 4 are isomorphic, as there exists two different kind of group tables. We will elaborate later but one of them are isomorphic to $\mathbb{Z}_4$ and the other one is to $V \simeq \mathbb{Z}_2 \times \mathbb{Z}_2$ also known as the Vierergruppe, or the Klein 4 group.

$*$	e	a	b	c
e	e	a	b	c
a	a	b	c	e
b	b	c	e	a
c	c	e	a	b

Table 1: $\mathbb{Z}_4$

$*$	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

Table 2: $V \simeq \mathbb{Z}_2 \times \mathbb{Z}_2$

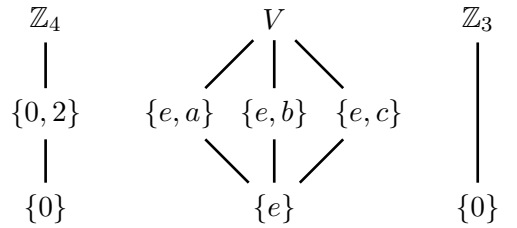
4 Subgroups

Def 11. *Let $(G, *)$ be a group. H is a **subgroup** of G if,*

1. *H is a subset of G.*
2. *H is closed under $*$.*
3. *$(H, *)$ is a group where $*$ is the induced operator.*

We denote such subgroup H of G as $H \leqslant G$.

Ex 6. *We can draw subgroup diagrams for some simple cases.*



(a) $\mathbb{Z}_4$ (b) V (c) $\mathbb{Z}_3$

Figure 1: Subgroup diagrams for $\mathbb{Z}_4$, V, and $\mathbb{Z}_3$

Def 12. *Let $H \leqslant G$. Then,*

1. *H is the **trivial subgroup** if $H = \{e\}$.*
2. *H is a **non trivial subgroup** if $H \neq \{e\}$.*
3. *H is a **proper subgroup** if $H \neq G$.*
4. *H is the **improper subgroup** if $H = G$.*

Thm 6. *Let G be a group. $H \leqslant G$ is equivalent to,*

1. *H is closed under $*$.*
2. *$e \in H$ where e is the identity element of G.*
3. *$\forall a \in H : \exists a^{-1} \in H$.*

Ex 7. *Consider $GL_2(\mathbb{R})$ and $SL_2(\mathbb{R})$. Using* ***Thm 6****, we can show that $SL_2(\mathbb{R}) \leqslant GL_2(\mathbb{R})$.*

1. *$SL_2(\mathbb{R})$ is closed under matrix multiplication as for any $A, B \in SL_2(\mathbb{R})$, $det(AB) = det(A)det(B) = 1 \implies AB \in SL_2(\mathbb{R})$.*
2. *The identity element I_2 is also in $SL_2(\mathbb{R})$ as $det(I_2) = 1$.*
3. *And for any $A \in SL_2(\mathbb{R})$, $A^{-1} \in SL_2(\mathbb{R})$ as $det(A^{-1}) = det(A)^{-1} = 1$.*

Thm 7. *Suppose $\phi : G \to G'$ is a group isomorphism with $H \leqslant G$. Then $\phi(H) = \{\phi(h) : h \in H\}$ is a subgroup in G', i.e $\phi(H) \leqslant G'$.*

Proof.

1. As ϕ is a group isomorphism, for any $h'_1, h'_2 \in \phi(H) : h'_1 h'_2 = \phi(h_1 h_2) \in \phi(H)$, which implies that it is closed.
2. As $H \leqslant G$, $e \in H$. Thus $\phi(e) \in \phi(H)$ where $\phi(e)$ is the identity element of G'.
3. For $\forall h' = \phi(h) \in \phi(H)$, there exists the inverse of it, $\phi(h^{-1})$ and the existence of such element is guranteed as $H \leqslant G$.

□

Def 13. *Let G be a group where $a \in G$, we define $\langle a \rangle = \{a^n : n \in \mathbb{Z}\}$*

Thm 8. *Let G be a group where $a \in G$. Then $\langle a \rangle$ is the smallest subgroup of G containing a.*

Proof.

1. $\langle a \rangle$ is closed under $*$ as for $a^i, a^j \in \langle a \rangle \implies a^i * a^j = a^{i+j} \in \langle a \rangle$.
2. Identity element exists.

   $e \in \langle a \rangle$ as $a^0 = e$.
3. Inverse element exists.

   For $\forall a^i \in \langle a \rangle$ there exists $(a^i)^{-1} = a^{-i}$ and as $i \in \mathbb{Z} \implies -i \in \mathbb{Z}$, thus the inverse of $\forall a^i \in \langle a \rangle$, $(a^i)^{-1} \in \langle a \rangle$.
4. It is the smallest subgroup containing a.

   It suffices to show that $a \in H' \leqslant G \implies \langle a \rangle \subseteq H'$. Since $a \in H'$ and $H' \leqslant G$, $e = a^0 \in H'$ and $a^{-1} \in H'$. Since H' is closed under $*$ and $a, a^{-1} \in H$, a^n for $\forall n \in \mathbb{Z}$ are also elements of H'. This implies that $\langle a \rangle \subseteq H$.

□

Def 14. *Let G be a group and $a \in G$.*

1. *$\langle a \rangle$ is the **cyclic subgroup** of G, **generated** by a. The element a is called the **generator** of $\langle a \rangle$.*
2. *If $G = \langle a \rangle$ for some $a \in G$, then G is **cyclic**.*

Ex 8.

1. *$\mathbb{Z}_3$ is cyclic since $\mathbb{Z}_3 = \langle 1 \rangle = \langle 3 \rangle$.*
2. *$V \simeq \mathbb{Z}_2 \times \mathbb{Z}_2$ is not cyclic.*
3. *$\mathbb{Q}$ is not cyclic.*

5 Cyclic Groups

Def 15. *The **order of an element** $a \in G$ of a group G is defined as $|\langle a \rangle|$ which is also the smallest $n \in \mathbb{N}$ such that $a^n = e$ and denote it as $\mathcal{O}(a)$.*

Remark. *Do not get confused between order of groups and order of elements.*

Thm 9. *If G is a cyclic group which is generated by $a \in G$ then,*

$$G \simeq \begin{cases} \mathbb{Z}_n & \mathcal{O}(a) \in \mathbb{N} \\ \mathbb{Z} & \mathcal{O}(a) = \infty \end{cases}$$

Proof.

1. $\mathcal{O}(a) \in \mathbb{N}$

   Let $\phi : G \to \mathbb{Z}_n$ which maps $\phi(a^i) = i$. Since $|G| = |\mathbb{Z}_n| = n$ such map is bijective. We can also show that it is a homomorphism. Thus such map suffices to be an isomorphism, which implies that $G \simeq \mathbb{Z}_n$.

2. $\mathcal{O}(a) = \infty$

   Again let $\phi : G \to \mathbb{Z}$ by $\phi(a^i) = i$. Same as the above case we can show that ϕ is an isomorphism.

□

Thm 10. *Let G, G' be groups.*

1. *A cyclic group is abelian.*
2. *If $\phi : G \to G'$ is an isomorphism and G is cyclic then G' is also cyclic.*
3. *Suppose $\phi, \psi : G \to G'$ are both homomorphisms and $G = \langle a \rangle$. If $\phi(a) = \psi(a)$, then $\phi = \psi$.*

Proof.

1. Let $G = \langle a \rangle$. Then $a^i a^j = a^{i+j} = a^j a^i$ for every i, j, thus G is abelian.
2. Let $G = \langle a \rangle$. We claim that $G' = \langle \phi(a) \rangle$. It is obvious that $\langle \phi(a) \rangle \subseteq G'$. Let $y \in G'$. Since ϕ is surjective, there exists some $a^i \in G$ such that $\phi(a^i) = y$. And since ϕ is a homomorphism, $y = \phi(a^i) = \phi(a \dots a) = \phi(a)^i \in \langle \phi(a) \rangle$, which implies that $G' \subseteq \langle \phi(a) \rangle$. Thus $G' = \langle \phi(a) \rangle$.
3. Let $G = \langle a \rangle$. Then $\forall x \in G$, there exists some $i \in \mathbb{Z}$ such that $x = a^i$. Then $\phi(x) = \phi(a^i) = \phi(a \dots a) = \phi(a)^i$ as ϕ is an isomorphism. As we assumed that $\phi(a) = \psi(a)$, we can see that $\phi(x) = \phi(a)^i = \psi(a)^i = \psi(a^i) = \psi(x)$. As this holds for every $x \in G$, $\psi = \phi$.

□

Remark. *As any cyclic group is abelian, and any group generated by an element is cyclic, we can always get an abelian subgroup of any group even it is non abelian. For instance consider the non abelian group $GL_n(\mathbb{R})$ where $M \in GL_n(\mathbb{R})$. Then $\langle M \rangle$ is abelian as it is cyclic, and it suffices $\langle M \rangle \leqslant GL_n(\mathbb{R})$ due to* ***Thm 8****.*

Remark. *$V, \mathbb{Q}, \mathbb{R}$ are abelian but not cyclic.*

Thm 11. *Every subgroup of a cyclic group is cyclic.*

Proof. Suppose G is a cyclic group and $H \leqslant G$. If G is a trivial group, H is also a trivial group which trivially suffices the theorem. Thus we will only consider cyclic groups with order greater than 1. Let it $G = \langle a \rangle$ where $a \neq e$.

(i) $H = \{e\}$: cyclic

(ii) $H \neq \{e\}$

Let n be the smallest positive integer such that $a^n \in H$. We claim that $H = \langle a^n \rangle$.

a) $\langle a^n \rangle \subset H$

It is obvious that $\langle a^n \rangle \subset H$ since $a^n \in H$ and H is closed under operation.

b) $H \subset \langle a^n \rangle$

Since $b \in G = \langle a \rangle$ there exists some $m \in \mathbb{Z}$ such that $a^m = b$. Then $m = qn+r$ for some $q, r \in \mathbb{Z}$ such that $0 \leq r \leq n-1$. Then $b = a^m = a^{qn+r} = (a^q)^n a^r$, which again implies that $a^r = a^m (a^n)^{-q}$. As $a^m, (a^n)^{-q} \in H$, it implies that $a^r \in H$. Since n was the smallest integer that makes $a^n \in H$ and $0 \leq r \leq n-1$, r should be 0. So as $m = qn + r = qn$, $b = a^m = a^q n = (a^n)^q$ for some $q \in \mathbb{Z}$. Thus for any $b \in H \implies b \in \langle a^n \rangle$.

Thus due to a) and b) we conclude that $H = \langle a^n \rangle$ which is a cyclic group.

□

Remark. *If $n|m$ for $n, m \in \mathbb{Z} \implies \langle a^m \rangle \subset \langle a^n \rangle$.*

Now we know that for any cyclic groups, their subgroups are also cyclic. We also know that if some group is cyclic, it is isomorphic to $\mathbb{Z}$ or $\mathbb{Z}_n$ for some n which is the order of the generator of the group. This implies that cyclic groups are all about $\mathbb{Z}_n$, and its subgroups. The next theorem states about subgroups of $\mathbb{Z}_n$ and which ones are identical. For example consider $\langle 28 \rangle \in \mathbb{Z}_{108}$, we can just derive the group by keep adding up 28 and get the *mod* 108 value. Using the next theorem, we can easily consider certain subgroups of $\mathbb{Z}_n$ by considering the divisibility between the order of the element and the order of the group.

Thm 12. *Let $G = \langle a \rangle$ and $\mathcal{O}(a) = n$.*

1. *$\mathcal{O}(a^s) = \frac{n}{gcd(n,s)}$ for $s \in \mathbb{Z}$.*
2. *For each m such that $m|n$ there exists exactly one subgroup of order m, which is $\langle a^{n/m} \rangle$.*
3. *$\langle a^s \rangle = \langle a^t \rangle \iff gcd(n, s) = gcd(n, t)$.*

Proof.

1. $\mathcal{O}(a^s) = \frac{n}{gcd(n,s)}$ for $s \in \mathbb{Z}$

   Let $m = \mathcal{O}(a^s)$ which implies $(a^s)^m = a^{sm} = e$ in $G = \langle a \rangle$. As $\mathcal{O}(a) = n$, it follows that $n \mid sm$. Then,

$$n|sm \implies \frac{n}{gcd(n,s)} \mid \frac{s}{gcd(n,s)}m$$

$$\implies \frac{n}{gcd(n,s)} \mid m$$

where the second implication was derived by the fact that $\frac{n}{gcd(n,s)} \nmid \frac{s}{gcd(n,s)}$. So as m is the smallest integer that should satisfy the above relation, $m = \mathcal{O}(a^s) = \frac{n}{gcd(n,s)}$.

2. There exists exactly one subgroup of order $m : m|n$, which is $\left\langle a^{n/m} \right\rangle$.

   Suppose $H \leqslant G$ and $|H| = m$. Also as H is a subgroup of a cyclic group it is also cyclic, which implies that $H = \langle a^s \rangle$ for some $s \in \mathbb{Z}$. Then due to 1,

$$|H| = \mathcal{O}(a^s) = \frac{n}{gcd(n,s)} = m$$

   which implies that $gcd(n,s) = \frac{n}{m} \implies \frac{n}{m} \mid s$. Recall that $\frac{n}{m} \mid s \implies \langle a^s \rangle \subset \left\langle a^{\frac{n}{m}} \right\rangle$. But as $\mathcal{O}(a^s) = \mathcal{O}(a^{\frac{n}{m}}) = m$, it should satisfy that $\left\langle a^{\frac{n}{m}} \right\rangle = \langle a^s \rangle$.

3. $\langle a^s \rangle = \left\langle a^t \right\rangle \iff gcd(n,s) = gcd(n,t)$.

   (i) $\langle a^s \rangle = \left\langle a^t \right\rangle \implies gcd(n,s) = gcd(n,t)$.

$$\langle a^s \rangle = \left\langle a^t \right\rangle \implies |\langle a^s \rangle| = |\left\langle a^t \right\rangle|$$

$$\iff \frac{n}{gcd(n,s)} = \frac{n}{gcd(n,t)}$$

$$\iff gcd(n,s) = gcd(n,t)$$

   (ii) $\langle a^s \rangle = \left\langle a^t \right\rangle \impliedby gcd(n,s) = gcd(n,t)$

   Using the result of 2, we can show that $\langle a^s \rangle = \left\langle a^t \right\rangle \impliedby |\langle a^s \rangle| = |\left\langle a^t \right\rangle|$ and using the implications used in (i), we derive that $\langle a^s \rangle = \left\langle a^t \right\rangle \impliedby gcd(n,s) = gcd(n,t)$.

□

We abused the notation of $gcd(n, m)$ without defining it, and even assuming that we all know it. We define the greatest common divisor using group theoretic notions.

Def 16. *The* ***greatest common divisor*** *of $r, s \in \mathbb{Z}$, is an integer $d \in \mathbb{Z}$ which suffices $\langle d \rangle = \{nr + ms : n, m \in \mathbb{Z}\}$, and denote it as $d = gcd(r, s)$. We say that r and s are* ***coprime****, or* ***relatively prime*** *if $gcd(r, s) = 1$.*

Thm 13. *Let $r, s \in \mathbb{Z}$.*

1. *$gcd(r, s) \mid r$ and $gcd(r, s) \mid s$.*
2. *If $d' \mid r$ and $d' \mid s$, then $d' \mid gcd(r, s)$.*
3. *$gcd(r, s) = 1$ and $r \mid sm \implies r \mid m$.*

Proof.

1. As $\langle gcd(r, s) \rangle = \{nr + ms : n, m \in \mathbb{Z}\}$, $\implies gcd(r, s) \mid nr + ms$. Let $n = 0, m = 1$ then $gcd(r, s) \mid nr + ms \implies gcd(r, s) \mid s$. Also if we let $n = 1, m = 0$ then $gcd(r, s) \mid nr + ms \implies gcd(r, s) \mid r$.
2. $gcd(r, s) = nr + ms$ for some $n, m \in \mathbb{Z}$. As $d' \mid r$ and $d' \mid s$, for such n, m, $d' \mid nr + ms = d$. Thus $d' \mid d$.
3. Since $gcd(r, s) = 1 \implies \exists n_0, m_0 \in \mathbb{Z} : n_0 r + m_0 s = gcd(r, s) = 1$. Then $mn_0 r + mm_0 s = m$. Since $r \mid n_0 mr$ and $r \mid sm \implies r \mid m_0 sm$, we can see that $r \mid mn_0 r + mm_0 s = m$. Thus $r \mid m$.

□

Remark. *Since $\langle gcd(r, s) \rangle = \{nr + ms : n, m \in \mathbb{Z}\}$ the problem of finding the greatest common divisor can be viewed in a different perspective, of finding two integers. This can sometimes ease the computational complexity of using prime factorization for calculating greatest common divisors, as finding prime itself is also a quite not so easy problem.*

6 Groups of Permutations

Def 17. *Let S be a set. Then a* ***permutation*** *of S is a bijection from S to S.*

Def 18. *From now on we will use some notations where we will define it here :*

(1) $B_n = \{1, 2, \ldots, n\}$

(2) *For a permutation* σ *of* B_n *we will denote it as :*

$$\sigma = \begin{pmatrix} 1 & 2 & \ldots & n \\ \sigma(1) & \sigma(2) & \ldots & \sigma(n) \end{pmatrix}$$

(3) *For permutations* σ *and* τ *of a same set, we define their product* $\sigma\tau$ *by* $\sigma \circ \tau$*, which is just the composition of functions.*

Def 19. *A* ***group of permutations*** *is a group where elements are permutations.*

Ex 9.

1. $\{id, \sigma\}$ *is a group of permutations where both are permutations of* B_3 *and*

$$\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$$

Also we can see that $\{id, \sigma\} \simeq \mathbb{Z}_2$.

2. *On the other hand* $\{id, \tau\}$ *is not a group of permutations where,*

$$\tau = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$$

as $\tau\tau$ *is not an element of* $\{id, \tau\}$*, i.e the set is not closed under permutation operation.*

3. *Let* S_n *be the set of all permutations of* B_n*. Then* S_n *is a group.*

Def 20. *The group* S_n *is called the* ***symmetric group****.*

By simple set theory, we know that $|S_n| = n!$.

Remark. *Let* G *be a set. Then* S_G *the set of bijections from* G *to* G *with permutation operation is also a group.*

Ex 10. *Let us consider the symmetric group S_3. We will denote the elements as :*

$$\rho_0 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} \quad \rho_1 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \quad \rho_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$$

$$\mu_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \quad \mu_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \quad \mu_3 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$$

We can easily see that S_3 is non abelian. In fact S_3 is the smallest non abelian group. The ρ_i can be thought as rotations and μ_is as flipping elements. A more geometric approach is given at the next definition.

Def 21. *The **n-th dihedral group** D_n is the group of symmetries of the regular n-gon.*

Then $D_3 \simeq S_3$ but $D_4 \not\simeq S_4$

Thm 14.

1. *For $m \geq n$ there is a one-to-one homomorphism from $S_n \to S_m$*
2. *S_n is abelian if $n = 1, 2$ and non abelian if $n > 2$.*

Proof.

1. We can define such one-to-one homomorphism $\phi : S_n \hookrightarrow S_m$ as :

$$\sigma \mapsto \phi(\sigma) = \begin{pmatrix} 1 & 2 & \dots & n & n+1 & \dots & m \\ \sigma(1) & \sigma(2) & \dots & \sigma(n) & n+1 & \dots & m \end{pmatrix}$$

2. For S_n such that $n > 2$, consider ρ_1 and μ_1 from S_3. Then using the one-to-one homomorphism defined above, we can show that $\phi(\rho_1)\phi(\mu_1) \neq \phi(\mu_1)\phi(\rho_1)$ for any S_n. Thus $S_n (n > 2)$ are all non abelian.

□

Def 22. *For groups G, G' let $\phi : G \to G'$ be homomorphisms where $H \leqslant G$. Then for H we define $\phi[H] = \{\phi(h) : h \in H\}$, and we call it the **image** of H under ϕ/.*

Lem 3. *Let $\phi : G \to G'$ be a one-to-one homomorphism. Then $G \simeq \phi[G]$ and $\phi[G] \leqslant G'$, i.e G is isomorphic to a subgroup of G'.*

Thm 15. *(Cayley) Every group is isomorphic to a subgroup of a symmetric group.*

Proof. Let G be a group. Due to **Lem 3** it suffices to show that there exists a one-to-one homomorphism such that $\phi : G \to S_G$ where S_G is the group of permutations of G. Define $\phi : G \to S_G$ as, for $x \in G : \phi(x) = \lambda_x$ where the bijection $\lambda_x : G \to G$ is also defined as $\lambda_x(g) = xg$ for all $g \in G$.

i) $\lambda_x \in S_G$

ii) ϕ is one-to-one

Consider $\phi(x) = \phi(y)$ for $x, y \in G$. It implies that :

$$\lambda_x = \lambda_y \implies \lambda_x(e) = \lambda_y(e) \implies x = y$$

thus ϕ is one-to-one.

iii) ϕ is a homomorphism.

To show that ϕ is a homomorphism, we need to show that $\phi(xy) = \phi(x)\phi(y)$ for $x, y \in G$, that is $\lambda_{xy} = \lambda_x\lambda_y$. For any $g \in G$:

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

thus ϕ is also a homomorphism.

□

7 Orbits, Cycles, and Alternating Groups

Def 23. *Let σ be a permutation of a set A. Then the **orbits** of A are the equivalence class determined by the below equivalence relation :*

$$a \sim b \iff \exists n \in \mathbb{Z} : b = \sigma^n(a)$$

As orbits are equivalence classes, it gives us a natural partition to the set. We also define a cycle as,

Def 24. *A permutation $\sigma \in S_n$ is a **cycle** if it has at most one orbit containing more than one element. The **length** of a cycle is the number of elements in its largest orbit.*

Def 25. *We say that a cycle with length of 2 is a* ***transposition****.*

Remark. *For a cycle* $(a_1 a_2 \dots a_n)$ *it can be splitted into transpositions as :*

$$(a_1 a_2 \dots a_n) = (a_1 a_n)(a_1 a_{n-1}) \dots (a_1 a_2)$$

which implies that any cycle is a composition of transpositions.

Lem 4.

1) If σ *is a cycle of length* n*, then* $\mathcal{O}(\sigma) = n$*.*

2) If σ *is a transposition, then* $\sigma^{-1} = \sigma$

Ex 11.

1. $\sigma = (1345) \in S_5$

   Then $\sigma^2 = (14)(35)$*,* $\sigma^3 = (1543)$ *and* $\sigma^4 = id$*. We can see that* $\mathcal{O}(\sigma) = 4$*.*

2. $\sigma = (a_1 a_2 \dots a_n) \implies \sigma^i = (a_{1+i(mod_n)} \dots)$

To sum up the results discussed above,

Lem 5.

1. $(a_1 a_2 \dots a_n) = (a_1 a_n)(a_1 a_{n-1}) \dots (a_1 a_2)$
2. *Every permutation is a product of disjoint cycles.*
3. *Every permutation is a product of transpositions.*

Transpositions serves an important role as it acts as a building block for permutations.

Lem 6. *For a permutation* $\sigma = \sigma_1 \sigma_2 \dots \sigma_n$ *where* σ_i *are all disjoint cycles,*

1) $\mathcal{O}(\sigma) = lcm\,(\mathcal{O}(\sigma_1), \mathcal{O}(\sigma_2), \dots, \mathcal{O}(\sigma_n))$

2) $\sigma^{-1} = \sigma_n^{-1} \sigma_{n-1}^{-1} \dots \sigma_1^{-1} = \sigma_1^{-1} \sigma_2^{-1} \dots \sigma_n^{-1}$

The equality of $\sigma_n^{-1} \sigma_{n-1}^{-1} \dots \sigma_1^{-1} = \sigma_1^{-1} \sigma_2^{-1} \dots \sigma_n^{-1}$ is derived by assumption of the disjointness of each cycles.

Thm 16. *No permutation can be both a product of odd number of permutations and a product of even ones.*

Def 26. *For a permutation $\sigma \in S_n$ we say that σ is **even** or **odd** according to whether it can be expressed as a product of an even number of transpositions or the product of an odd number of transpositions, respectively.*

The above definition is well defined, thanks to **Thm 16**.

Def 27. *We define the **alternating group of n-letters** A_n which is the collection of all even permutations of B_n.*

Thm 17.

1. $A_n \leqslant S_n$
2. $|A_n| = \frac{1}{2}|S_n| = \frac{1}{2}n!$

Proof.

1. $A_n \leqslant S_n$
   i) A_n is closed.

   Let $\sigma, \tau \in A_n$. Then $\sigma = \sigma_1\sigma_2 \dots \sigma_{2m}$ and $\tau = \tau_1\tau_2 \dots \tau_{2n}$ for some $n, m \in \mathbb{N}$ where each σ_i, τ_i are transpositions. Then $\sigma\tau = \sigma_1\sigma_2 \dots \sigma_{2m}\tau_1\tau_2 \dots \tau_{2n}$ which is a product of $2(n+m)$ transpositions, which implies that $\sigma\tau$ is also an even permutation. Thus $\sigma\tau \in A_n$, which implies that A_n is closed.

   ii) $id \in A_n$: obvious as id is even.

   iii) $\sigma \in A_n \implies \sigma^{-1} \in A_n$

   For some $\sigma \in A_n$, $\sigma = \sigma_1\sigma_2 \dots \sigma_{2m}$. Then, $\sigma^{-1} = \sigma_{2m}^{-1}\sigma_{2m-1}^{-1} \dots \sigma_1^{-1}$ where each σ_i^{-1} are also transpositions and $\sigma_i = \sigma_i^{-1}$ due to **Lem 4**. Thus the inverse is also a product of even transpositions, thus an element of A_n.

2. $|A_n| = \frac{1}{2}|S_n|$

   Let $f : A_n \to S_n \setminus A_n$ by $\sigma \mapsto (12)\sigma$. We claim that such f is a bijection, thus $|A_n| = |S_n \setminus A_n|$.

   i) f is one-to-one

   Consider $f(\sigma) = f(\tau)$ for $\sigma, \tau \in A_n$. This implies $(12)\sigma = (12)\tau$, which implies that $\sigma = \tau$ due to the cancellation law of group elements.

ii) f is onto

For any $\sigma \in S_n \setminus A_n$ consider $(12)\sigma \in A_n$. We can see that $f((12)\sigma) = (12)(12)\sigma = \sigma$, which implies that f is onto.

Thus as the above holds, we can see that $|A_n| = |S_n \setminus A_n| = \frac{1}{2}|S_n|$

□

8 Cosets and the Theorem of Lagrange

Def 28. *Let $H \leqslant G$ and $a \in G$.*

1) $aH = \{ah : h \in H\}$ is the left coset of H containing a.

2) $Ha = \{ha : h \in H\}$ is the right coset of H containing a.

Ex 12. *Consider $\{0, 2\} \leqslant \mathbb{Z}_4$. Then the*

Remark. *If G is abelian and $H \leqslant G$ with $a \in G$, then $aH = Ha$.*

Lem 7. *Let $H \leqslant G$ and $a, b \in G$.*

1) $aH = bH \iff a \in bH \iff b \in aH$

2) $Ha = Hb \iff a \in Hb \iff b \in Ha$

3) $aH = bH \iff (ca)H = (cb)H$

4) $Ha = Hb \iff H(ac) = H(bc)$

Proof.

1. $aH = bH \iff a \in bH (\iff b \in aH)$

   i) ($\implies$)

   Since $a \in aH$ and as $aH = bH$ by assumption, $a \in bH$.

   ii) ($\impliedby$)

   As $a \in bH$, there exists $h' \in H$ such that $a = bh'$. Then for $h \in H$, $ah = bh'h$. As $H \leqslant G$, $h'h \in H$ which implies that $ah = bh'h \in bH$. Thus $aH \subset bH$. Since $a = bh'$, $b = a(h')^{-1}$. Again as $H \leqslant G$, $b = a(h')^{-1} \in aH$. Using similar arguments used above, we can show that $bH \subset aH$. Thus $aH = bH$.

2. $aH = bH \iff (ca)H = (cb)H$

   We will first show the ($\implies$) direction. Since $a \in aH$ and by assumption $aH = bH$, there exists some $h' \in H$ such that $a = bh'$. Then for $h \in H$

   $$cah = c(bh')h = cb(h'h) \in (cb)H$$

   which implies that $(ca)H \subset (cb)H$. Using similar arguments, we can also show that $(cb)H \subset (ca)H$, thus $(ca)H = (cb)H$.

□

Remark. *For the identity element $e \in H \leqslant G$, $eH = H$.*

Cor 1.

1) $aH = H \iff a \in H$

2) $aH = bH \iff H = a^{-1}bH$

Remark. *Cosets are not necessarily subgroups! For aH to be a subgroup of G, then e should be in aH. Then the following implication tells us :*

$$e \in aH \iff aH = eH \iff H = aH \iff a \in H$$

As the above condition doesn't always hold, we can't really say that cosets are subgroups.

Thm 18. *Let $H \leqslant G$ and $a, b \in G$. Then either $aH = bH$ or $aH \cap bH = \phi$.*

Proof. Suppose $aH \cap bH \neq \phi$, so that there exists $c \in aH \cap bH$. Then $c = ah_1 = bh_2$ for some $h_1, h_2 \in H$. Then $a = bh_2h_1^{-1} \in bH$, and due to **Lem 7**, $aH = bH$.

□

Thm 19. *Let $H \leqslant G$ and $a, b \in G$.*

1. *Let $a \sim b$ be a relation if $aH = bH$. Then $\sim$ is an equivalence relation on G where the equivalence classes are the left cosets of H.*
2. *All left cosets of G have the same cardinality.*

Proof.

1. $\sim$ is an equivalence relation : left as an exercise

2. All left cosets have the same cardinality.

   Let $a \in G$. It suffices to show there exists a bijection. We will claim that $\phi : H \to aH$ which maps $h \mapsto ah$ is a bijection.

   i) ϕ is onto

      For any $b \in aH$, there exists $h \in H$ such that $b = ah = \phi(h)$.

   ii) ϕ is one-to-one

      If $\phi(h_1) = \phi(h_2)$ for $h_1, h_2 \in H$, it implies that $ah_1 = ah_2$ and using the cancellation law of group elements we can easily show that the assumption implies that $h_1 = h_2$.

□

The above implies that every coset (left or right) of a subgroup H of a group G has the same number of elements as H.

Thm 20. *(Lagrange) Let G be a finite group, where $H \leqslant G$. Then $|H| \mid |G|$.*

Proof. Due to **Thm 18**, there exists $a_1, \ldots, a_n \in H$ such that

$$G = \bigcup_{i=1}^{n} a_i H \quad \text{where} \quad a_i H \cap a_j H = \phi$$

This implies that $|G| = \sum_{i=1}^{n} |a_i H|$ and due to **Thm 19**, for any i we know that $|H| = |a_i H|$, thus $|G| = \sum_{i=1}^{n} |a_i H| = n|H|$. Thus $|H| \mid |G|$.

□

Cor 2. *If G is a finite group and $a \in G$ then $\mathcal{O}(a) \mid |G|$.*

Proof. As for $a \in G$ we know that $\langle a \rangle \leqslant G$. Thus using **Lagrange** we know that $|\langle a \rangle| \mid |G|$. But by definition $|\langle a \rangle| = \mathcal{O}(a)$, thus $\mathcal{O}(a) \mid |G|$.

□

Cor 3. *If $|G| = p$ for some prime p, $|G| \simeq \mathbb{Z}_p$.*

Proof. Let $a \in G$ such that $a \neq e$. As $\langle a \rangle \leqslant G$, and applying **Lagrange**, we know that $|\langle a \rangle| \mid |G| = p$. As p is a prime, $|\langle a \rangle| = 1$ or p. But as $a \neq e$, $|\langle a \rangle| = p$, which implies that $\langle a \rangle = G$. Thus as G is a cyclic group of order p, we can conclude that $G \simeq \mathbb{Z}_p$.

□

Def 29. *Let $H \leqslant G$.The **index** of H in G is denoted as $(G : H)$ and defined as the number of left cosets of H in G.*

Remark. *If $|G| < \infty$, then $(G : H) = |G|/|H|$.*

Ex 13.

1. $(\mathbb{Z}_6 : \{0, 3\}) = 6/3 = 2$
2. $(\mathbb{Z} : 3\mathbb{Z}) = 3$

   In this case as $|\mathbb{Z}|$ isn't finite we have to count the number of left cosets. There are 3 left cosests, $1 + 3\mathbb{Z}$,$2 + 3\mathbb{Z}$ and $3\mathbb{Z}$. Thus the index of $3\mathbb{Z}$ in $\mathbb{Z}$ is 3.

9 Direct Products, Finitely Generated Abelian Groups

We can know make more groups by considering their products. Let us first define the product of groups.

Def 30. *Let G_i be groups for $i \in \{1, \ldots, n\}$. For $(a_1, \ldots, a_n), (b_1, \ldots, b_n) \in G$ where G is defined as the product of sets G_i, i.e $G = \prod_{i=1}^{n} G_i$. Define the product of $(a_1, \ldots, a_n)$ and $(b_1, \ldots, b_n)$ as :*

$$(a_1, \ldots, a_n)(b_1, \ldots, b_n) = (a_1 b_1, a_2 b_2, \ldots, a_n b_n)$$

*Then under such binary operation, G is a group and is called the **direct product** of $G_1, \ldots, G_n$.*

We will skip the whole procedure showing that such direct product is a group.

Remark. *If we let e_i each be the identity element for G_i, then $(e_1, e_2, \ldots, e_n)$ is the identity element of $\prod_{i=1}^{n} G_i$. Also for $(a_1, a_2, \ldots, a_n) \in \prod_{i=1}^{n} G_i$, the inverse element is given as*

$$(a_1, a_2, \ldots, a_n)^{-1} = (a_1^{-1}, a_2^{-1}, \ldots, a_n^{-1})$$

where the a_i^{-1} each is the inverse element of G_i.

Ex 14.

1. $\mathbb{Z}_2 \times \mathbb{Z}_2$

   This group has $(0, 0)$ as the identity element, and we can also see that it is isomorphic with the Klein 4 group.

2. $\mathbb{Z} \times GL_2(\mathbb{R})$

   For this direct product group we can easily see that it is not abelian, as if we choose $A, B \in GL_2(\mathbb{R})$ *such that* $AB \neq BA$ *then we can also see that* $(0, A)(0, B) \neq (0, B)(0, A)$ *in* $\mathbb{Z} \times GL_2(\mathbb{R})$.

The second example leads to the following lemma :

Lem 8. $\prod_{i=1}^{n} G_i$ *is abelian* $\iff$ $\forall i \in \{1, \ldots, n\}$ G_i *is abelian*

Remark. *If all of the* G_i *are abelian, i.e we denote the binary operation as* $+$*, then we write*

$$\bigoplus_{i=1}^{n} G_i = G_1 \oplus G_2 \oplus \cdots \oplus G_n$$

for the direct product of G_i*s and it is called the* ***direct sum*** *of* G_i*s.*

Thm 21. *Let* G_i *be groups for* $i \in \{1, \ldots, n\}$*. Also let* $(a_1, \ldots, a_n) \in \prod_{i=1}^{n} G_i$.

1) $\mathcal{O}((a_1, \ldots, a_n)) = lcm(\mathcal{O}(a_1), \ldots, \mathcal{O}(a_n))$

2) $\mathbb{Z}_m \times \mathbb{Z}_n$ *is cyclic* $\iff$ $lcm(m, n) = mn$ $\iff$ $m \nmid n$

The induction of the second theorem is pretty straigtforward as $mn = gcd(m, n) \times lcm(m, n)$ which implies that $gcd(m, n) = 1$.

Cor 4. $\mathbb{Z}_{m_1} \times \mathbb{Z}_{m_2} \times \cdots \times \mathbb{Z}_{m_n} \simeq \mathbb{Z}_{m_1 m_2 \ldots m_n}$ $\iff$ $gcd(m_i, m_j) = 1$ *for all* $i \neq j$

Ex 15.

1. $\mathbb{Z}_2 \times \mathbb{Z}_2 \not\simeq \mathbb{Z}_4$ *as* $lcm(2, 2) \neq 4$ *but* $\mathbb{Z}_2 \times \mathbb{Z}_3 \simeq \mathbb{Z}_6$ *as* $2 \nmid 3$

2. *Consider* $\mathbb{Z}_{60}$ *:*

   We can see that $\mathbb{Z}_{60} \simeq \mathbb{Z}_4 \times \mathbb{Z}_3 \times \mathbb{Z}_5 \simeq \mathbb{Z}_{12} \times \mathbb{Z}_5 \simeq \mathbb{Z}_4 \times \mathbb{Z}_{15} \simeq \mathbb{Z}_3 \times \mathbb{Z}_{20}$.

Def 31. *Let* G *be a group.* G *is said to be* ***finitely generated*** *if there exists finitely many elements* $a_1, \ldots, a_n \in G$ *such that every element of* G *can be written as a product of* $a_1.a_1^{-1}, \ldots, a_n, a_n^{-1}$.

Remark. *If G is abelian, G is finitely generated if there exists $a_1, \ldots, a_l \in G$ such that $G = \{n_1 a_1 + n_l a_l : n_i \in \mathbb{Z}\}$. This is just the abelian notation for the above definition of finitely generated groups.*

Ex 16.

1. *$\mathbb{Z}_m = \{n \cdot 1 : n \in \mathbb{Z}\}$ is finitely generated : cyclic $\implies$ finintely generated*
2. *$\mathbb{Z}_2 \times \mathbb{Z}_2$ is finitely generated but not cyclic : finitely generated $\not\implies$ cyclic*

   It is generated by $(1,0)$ and $(0,1)$.
3. *If G is finite, it is finitely generated.*

   It holds as we can just choose all of the elements to act as generators.
4. *$\mathbb{Z}$ is infinite but finitely generated, also cyclic.*
5. *$\mathbb{Z} \times \mathbb{Z}$ is infinite and not cyclic but finitely generated.*

   It is generated by $(0,1)$ and $(1,0)$ as any $(a,b) \in \mathbb{Z} \times \mathbb{Z}$, it can be expressed as $(a,b) = a(1,0) + b(0,1)$.
6. *$\mathbb{Z} \times \ldots \mathbb{Z} = \mathbb{Z}^n$ is generated by n elements :*

   $(1,0,\ldots,0)$, $(0,1,\ldots,0)$, ... , $(0,0,\ldots,1)$

Remark.

1. *$\mathbb{Z} \times \ldots \mathbb{Z} = \mathbb{Z}^n$ is said to be a group of **rank** n, or has a **Betti number** of n.*
2. *$\mathbb{Z}^n \simeq \mathbb{Z}^m \iff n = m$*

Thm 22. ***(Fundamental Theorem of Finitely Generated Abelian Groups)***

Let G be a finitely generated abelian group.

1) There exists primes $p, p_1, \ldots, p_n$ and $r_1, \ldots, r_n \in \mathbb{N}$ such that

$$G \simeq \mathbb{Z}_{p_1^{r_1}} \times \mathbb{Z}_{p_2^{r_2}} \times \cdots \times \mathbb{Z}_{p_n^{r_n}} \times \mathbb{Z}^p$$

2) For primes $p, p_1, \ldots, p_n$, $q, q_1, \ldots, q_n$ and $r_1, \ldots, r_n \in \mathbb{N}$, $u_1, \ldots, u_n \in \mathbb{N}$ the following

$$\mathbb{Z}_{p_1^{r_1}} \times \mathbb{Z}_{p_2^{r_2}} \times \cdots \times \mathbb{Z}_{p_n^{r_n}} \times \mathbb{Z}^p \simeq \mathbb{Z}_{q_1^{u_1}} \times \mathbb{Z}_{q_2^{u_2}} \times \cdots \times \mathbb{Z}_{q_n^{u_n}} \times \mathbb{Z}^q$$

is equivalent to $\{p_1^{r_1}, \ldots, p_n^{r_n}\} = \{q_1^{u_1}, \ldots, q_n^{u_n}\}$ as multisets and $p = q$, which implies that the expression of 1) is unique for finitely generated abelian groups.

Remark. *We can also state the previous theorem in another form as :*

$$G \simeq \mathbb{Z}_{d_1} \times \cdots \times \mathbb{Z}_{d_l} \times \mathbb{Z}^n \text{ where } d_1 \mid d_2 \mid \cdots \mid d_l$$

Ex 17.

1. $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_4 \not\simeq \mathbb{Z}_4 \times \mathbb{Z}_4$ *since* $\{2, 2, 4\} \neq \{4, 4\}$.
2. $\mathbb{Z}_4 \times \mathbb{Z}_{35} \simeq \mathbb{Z}_{20} \times \mathbb{Z}_7 \simeq \mathbb{Z}_4 \times \mathbb{Z}_5 \times \mathbb{Z}_7$

Ex 18. *There are also abelian groups but not finitely generated ones, for example* $\mathbb{Q}$. *If* $\mathbb{Q}$ *was generated by* $\frac{b_1}{a_1}, \ldots, \frac{b_n}{a_n}$ *where* $a_i \nmid b_i$ *for each* i, *then* $\mathbb{Q} = \{r_1\frac{b_1}{a_1} + \cdots + r_n\frac{b_n}{a_n} : r_i \in \mathbb{Z}\}$. *But as*

$$\frac{1}{2a_1a_2\cdots a_n} \notin \{r_1\frac{b_1}{a_1} + \cdots + r_n\frac{b_n}{a_n} : r_i \in \mathbb{Z}\}$$

which should be in $\mathbb{Q}$, *we can conclude that* $\mathbb{Q}$ *is not finitely generated.*

Ex 19.

1. $\mathbb{Z} \not\simeq \mathbb{Z} \times \mathbb{Z}$ *as they have different Betti numbers, 1 and 2 respectively.*
2. $\mathbb{Z}_3 \times \mathbb{Z}_3 \not\simeq \mathbb{Z}_9$ *as* $\{3, 3\} \neq \{9\}$.

Ex 20. *Classification of abelian groups of order 180 up to isomorphism.*

As $180 = 2^2 \times 3^2 \times 5$, *we can consider 4 types of multisets :*

1. $\{2, 2, 3, 3, 5\}$ *:* $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_5$
2. $\{2, 2, 9, 5\}$ *:* $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_5 \times \mathbb{Z}_9$
3. $\{3, 3, 4, 5\}$ *:* $\mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_4 \times \mathbb{Z}_5$
4. $\{4, 9, 5\}$ *:* $\mathbb{Z}_4 \times \mathbb{Z}_5 \times \mathbb{Z}_9$

due to Fundamental Theorem of Finitely Generated Abelian Groups, abelian groups of order 180 can be classified into 4 types of groups up to isomorphism.

Ex 21. *Prime, let it* p, *orderd abelian groups are all isomorphic to* $\mathbb{Z}_p$ *as* $p = 1 \times p$ *which makes* $\{p\}$ *the unique multiset available.*

Remark. *A **finite abelian group** is a finitely generated abelian group with its Betti number being 0.*

Thm 23. *Let G be a finite abelian group. If there exists m such that $m \mid |G|$, then there exists $H \leqslant G$ such that $|H| = m$.*

Proof. Since G is a finite abelian group, due to the Fundamental Theorem, there exists primes $p_1, \ldots, p_n$ and $r_1, \ldots, r_n \in \mathbb{N}$ such that

$$G \simeq \mathbb{Z}_{p_1^{r_1}} \times \ldots \mathbb{Z}_{p_n^{r_n}}$$

Since $m \mid |G|$, for some $s_i \in \mathbb{N} : m = p_1^{s_1} \times \cdots \times p_n^{s_n}$ where $0 \leq s_i \leq r_i$. Then let H as

$$H = \langle p_1^{r_1 - s_1} \rangle \times \cdots \times \langle p_n^{r_n - s_n} \rangle$$

□

Ex 22. *Let $G = \mathbb{Z}_{10}$, then $|G| = 10$. We can find 4 integers, let it m, such that $m \mid 10$*

1. $m = 1$ *:* $H = \langle 10/1 \rangle = \{0\} \leqslant G$
2. $m = 2$ *:* $H = \langle 10/2 \rangle = \{0, 5\} \leqslant G$
3. $m = 5$ *:* $H = \langle 10/5 \rangle = \{0, 2, 4, 6, 8\} \leqslant G$
4. $m = 10$ *:* $H = \langle 10/10 \rangle = G \leqslant G$

Also for each case $|H| = m$.

Ex 23. *Consider $\mathbb{Z}_9 \times \mathbb{Z}_8$. For some $m|(9 \times 8)$:*

1. $m = 3$ *:* $H = \langle 9/3 \rangle \times \{0\} \leqslant \mathbb{Z}_9 \times \mathbb{Z}_8$
2. $m = 4$ *:* $H = \{0\} \times \langle 8/4 \rangle \leqslant \mathbb{Z}_9 \times \mathbb{Z}_8$
3. $m = 6 = 3 \times 2$ *:* $H = \langle 9/3 \rangle \times \langle 8/2 \rangle \leqslant \mathbb{Z}_9 \times \mathbb{Z}_8$

10 Homomorphisms

Def 32. *Let G, G' be groups then $\phi : G \to G'$ is a **homomorphism** if $\phi(ab) = \phi(a)\phi(b)$ for all $a, b \in G$.*

Thm 24. *Let $\phi : G \to G'$ be a homomorphism, where e, e' are the identity elements of each group respectively. Then*

1) $\phi(e) = e'$

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

3) $H \leqslant G \implies \phi[H] \leqslant G'$

4) $H' \leqslant G' \implies \phi^{-1}[H'] \leqslant G$

Def 33. *For a homomorphism $\phi : G \to G'$ the **kernel** of ϕ is*

$$Ker(\phi) = \{g \in G : \phi(g) = e'\} = \phi^{-1}(e')$$

or in words, the preimage of the identity element of G'.

Remark. *Due to **Thm 24** we can see that $Ker(\phi) \leqslant G$, as the kernel is the preimage of the trivial subgroup of G'.*

Thm 25. *Let $\phi : G \to G'$ be a homomorphism. Then ϕ is injective iff $Ker(\phi) = \{e\}$.*

Proof.

i) ($\implies$)

As $\phi(e) = e'$ it is obvious that $e \in Ker(\phi)$. Suppose $a \in Ker(\phi) \implies \phi(a) = e'$. As we've assumed that ϕ is injective, as $\phi(e) = e'$ and $\phi(a) = e'$ it implies that $a = e$. Thus $Ker(\phi) = \{e\}$.

ii) ($\impliedby$)

Suppose $\phi(a) = \phi(b)$

$$\begin{aligned} \phi(a) = \phi(b) &\implies \phi(a)\phi(b)^{-1} = e' \\ &\implies \phi(a)\phi(b^{-1}) = e' \\ &\implies \phi(ab^{-1}) = e' \\ &\implies ab^{-1} \in Ker(\phi) = \{e\} \\ &\implies a = b \end{aligned}$$

□

Thm 26. *Let $\phi : G \to G'$ be a homomorphism. Then, $\phi^{-1}(\phi(a)) = aKer(\phi)$.*

Def 34. *A subgroup H of G is* ***normal*** *if $aH = Ha$ for all $a \in G$, and is denoted as $H \triangleleft G$.*

Thm 27. *Let H be a subgroup of G. Then TFAE :*

1) $aH = Ha$ for all $a \in G$, i.e $H \triangleleft G$.

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

3) $aHa^{-1} = \{aha^{-1} : h \in H\} = H$ for all $a \in G$.

The aHa^{-1} is called the conjugate of H by a.

Ex 24.

1. *For an abelian group G, for every $H \leqslant G \implies H \triangleleft G$.*
2. *$\{\rho_0, \rho_1, \rho_2\} \triangleleft S_3$.*
3. *If $|G| < \infty$ and $(G : H) = 2$ for some $H \leqslant G$ then $H \triangleleft G$.*
4. *$\{e\} \triangleleft G$ and $G \triangleleft G$ for any group G and its identity element e.*

Thm 28. *Let $\phi : G \to G'$ be a homomorphism. Then $Ker(\phi) \triangleleft G$, i.e the kernel of a homomorphism is a normal subgroup.*

Proof. Let $a \in G$ and $h \in Ker(\phi)$. Then

$$\begin{aligned} \phi(aha^{-1}) &= \phi(a)\phi(h)\phi(a^{-1}) \\ &= \phi(a)e\phi(a^{-1}) \\ &= \phi(a)\phi(a)^{-1} = e \end{aligned}$$

which implies that $aha^{-1} \in Ker(\phi)$. Applying **Thm 27**, $Ker(\phi) \triangleleft G$. □

Ex 25. *Consider $\phi : S_n \to \mathbb{Z}_2$ where*

$$\phi(\sigma) = \begin{cases} 0 & (\ \sigma \text{ is even}\ ) \\ 1 & (\ \sigma \text{ is odd}\ ) \end{cases}$$

is a homomorphism. Then $Ker(\phi) = \phi^{-1}(0) = A_n$. Thus $A_n \triangleleft S_n$.

Ex 26. *Consider the determinant* $det : GL_n(\mathbb{R}) \to \mathbb{R} \setminus \{0\}$ *as a homomorphism. Then* $Ker(det) = \{A \in GL_n(\mathbb{R}) : det(A) = 1\} = SL_n(\mathbb{R})$. *Thus* $SL_n(\mathbb{R}) \triangleleft GL_n(\mathbb{R})$.

Def 35. *A group* G *is* ***simple*** *if* G *has no nontrivial proper normal subgroups, i.e* $H \triangleleft G \implies H = \{e\}$ *or* $H = G$.

Def 36. *Let* G *be a group.*

1) *An isomorphism* $\phi : G \to G$ *is called an* ***automorphism***.
2) *For a fixed* $g \in G$ *and* $i_g : G \to G$ *that maps* $a \mapsto gag^{-1}$, *it is an automorphism and we call such* i_g *an* ***inner automorphism***.

11 Factor Groups

Def 37. *For a subgroup* H *of* G, *we define*

$$G/H = \{aH : a \in G\}$$

which is the collection of all left cosets of H.

The above is merely a set, not a group as we haven't defined any binary operations between cosets.

Remark. *If* $|G| < \infty$ *then* $|G/H| = (G : H) = |G|/|H|$ *due to* ***Lagrange***.

Ex 27.

1. $\mathbb{Z}/3\mathbb{Z} = \{3\mathbb{Z}, 1 + 3\mathbb{Z}, 2 + 3\mathbb{Z}\}$
2. $S_3/H = \{H, \mu_1 H\}$ *where* $H = \{\rho_0, \rho_1, \rho_2\}$

Ex 28. *Consider* $(\mathbb{Z} \times \mathbb{Z}_3)/(\mathbb{Z} \times \{0\})$. *Then*

$$\begin{aligned}(n,1) + \mathbb{Z} \times \{0\} &= (0,1) + \mathbb{Z} \times \{0\} \\ (n,2) + \mathbb{Z} \times \{0\} &= (0,2) + \mathbb{Z} \times \{0\} \\ (n,0) + \mathbb{Z} \times \{0\} &= \mathbb{Z} \times \{0\}\end{aligned}$$

which implies that $(\mathbb{Z} \times \mathbb{Z}_3)/(\mathbb{Z} \times \{0\}) = \{\mathbb{Z} \times \{0\}, (0,1) + \mathbb{Z} \times \{0\}, (0,2) + \mathbb{Z} \times \{0\}\}$.

Thm 29. *For $H \leqslant G$ and $aH, bH \in G/H$ if we let $(aH)(bH) = (ab)H$ as a binary operation between left cosets of H then such operation is well defined iff $H \triangleleft G$.*

Proof. We will just show that $H \triangleleft G \implies$ such operation is well defined.

Suppose $aH = a'H$ and $bH = b'H$. As $H \triangleleft G$ $a' \in aH$ and $b' \in bH$, which implies that $a' = ah_1$ and $b' = bh_2$ for some $h_1, h_2 \in H$. Then $a'b' = ah_1bh_2$. As $H \triangleleft G$, $bH = Hb$ which implies that $h_1b \in Hb \implies h_1b \in bH$. This again implies that there exists some $h_3 \in H$ such that $h_1b = bh_3$. Thus $a'b' = ah_1bh_2 = abh_3h_2$, and as $H \leqslant G$ which implies that $h_3h_2 \in H$, $a'b' \in (ab)H$. Thus as $(ab)H = (a'b')H$ such operation is well defined. □

Def 38. *Suppose $H \triangleleft G$. Then the group G/H equipped with the operation $aH, bH \in G/H : (aH)(bH) = (ab)H$ is called the **factor (quotient) group** of G by H.*

Remark. *For the quotient group G/H of G by $H \triangleleft G$,*

1. *Identity element of G/H : $H = eH$*
2. *Inverse element of $aH \in G/H$: $(aH)^{-1} = (a^{-1})H$*

Remark.

1. *For an abelian group G, for any subgroup $H \leqslant G \implies H \triangleleft G$, G/H is abelian.*
2. *If G is cyclic, i.e $\langle a \rangle = G$ then G/H is also cyclic which is generated by aH, i.e $\langle aH \rangle = G/H$.*

Ex 29. *$\mathbb{Z}/n\mathbb{Z} = \{n\mathbb{Z}, 1 + n\mathbb{Z}, 2 + n\mathbb{Z}, \ldots, (n-1) + n\mathbb{Z}\} = \langle 1 + n\mathbb{Z} \rangle$. As it is a cyclic group with order n it is isomorphic to $\mathbb{Z}_n$, thus $\mathbb{Z}/n\mathbb{Z} \simeq \mathbb{Z}_n$. We can also give an implicit isomorphism ϕ as $\phi(a + n\mathbb{Z}) = a(mod_n)$*

Thm 30. *Let $H \triangleleft G$ and $\phi : G \to G/H$ be a function defined by $\phi(a) = aH$. Then ϕ is a homomorphism and $Ker(\phi) = H$.*

Proof.

i) ϕ is a homomorphism.

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

ii) $Ker(\phi) = H$

Let $a \in Ker(\phi)$ then,

$$\begin{aligned} a \in Ker(\phi) &\iff \phi(a) = H \\ &\iff aH = H \\ &\iff a \in H \end{aligned}$$

Thus $Ker(\phi) = H$.

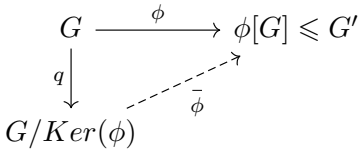
□

Thm 31. *(First Isomorphism Theorem)*

Let $\phi : G \to G'$ be a homomorphism. Then

1) $\bar{\phi} : G/Ker(\phi) \to \phi[G]$ which maps $aKer(\phi) \mapsto \phi(a)$ is an isomorphism.

2) For the homomorphism $q : G \to G/Ker(\phi)$ which maps $a \mapsto aKer(\phi)$ satisfies $\phi = \bar{\phi} \circ q$. Thus the following diagram commutes :



Proof.

i) $\bar{\phi}$ is well defined.

Suppose $aKer(\phi) = bKer(\phi)$. We want to show that $\bar{\phi}(aKer(\phi)) = \bar{\phi}(bKer(\phi))$.

$$\begin{aligned} aKer(\phi) = bKer(\phi) &\implies a \in bKer(\phi) \\ &\implies \exists c \in Ker(\phi) : a = bc \\ &\implies \phi(a) = \phi(bc) \\ &\implies \phi(a) = \phi(b)\phi(c) = \phi(b)e = \phi(b) \\ &\implies \phi(a) = \phi(b) \\ &\implies \bar{\phi}(aKer(\phi)) = \bar{\phi}(bKer(\phi)) \end{aligned}$$

ii) $\bar{\phi}$ is a homomorphism.

Using the same cosets used at i),

$$\begin{aligned} \bar{\phi}\left((aKer(\phi))(bKer(\phi))\right) &= \bar{\phi}((ab)Ker(\phi)) \\ &= \phi(ab) = \phi(a)\phi(b) \\ &= \bar{\phi}(aKer(\phi))\bar{\phi}(bKer(\phi)) \end{aligned}$$

iii) $\bar{\phi}$ is surjective : obvious.

iv) $\bar{\phi}$ is injective.

Recall that the condition for a homomorphism $\bar{\phi}$ to be injective was equivalent with $Ker(\bar{\phi})$ being the singleton set containing the identity element, in this case $Ker(\phi)$. It is obvious that $Ker(\phi) \in Ker(\bar{\phi})$. Suppose $aKer(\phi) \in Ker(\bar{\phi})$:

$$\begin{aligned} aKer(\phi) \in Ker(\bar{\phi}) &\implies \bar{\phi}(aKer(\phi)) = e' \in G' \\ &\implies \phi(a) = e' \\ &\implies a \in Ker(\phi) \\ &\implies aKer(\phi) = Ker(\phi) \end{aligned}$$

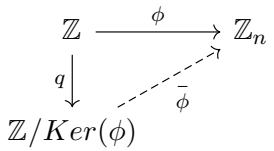
thus $Ker(\bar{\phi}) = \{Ker(\phi)\}$, showing that $\bar{\phi}$ is injective.

v) $\phi = \bar{\phi} \circ q$

Is quit obvious as $(\bar{\phi} \circ q)(a) = \bar{\phi}(aKer(\phi)) = \phi(a)$.

□

Ex 30. *Let us revisit the example of* $\mathbb{Z}/n\mathbb{Z} \simeq \mathbb{Z}_n$ *:*



where we define the functions $\phi, q, \bar{\phi}$ *as :*

$$\begin{aligned} &\phi : \mathbb{Z} \to \mathbb{Z}_n && a \mapsto a(mod_n) \\ &q : \mathbb{Z} \to \mathbb{Z}/Ker(\phi) && a \mapsto a + Ker(\phi) \\ &\bar{\phi} : \mathbb{Z}/Ker(\phi) \to \mathbb{Z} && a + Ker(\phi) \mapsto a(mod_n) \end{aligned}$$

As we know such ϕ *is an homomorphism and the kernel* $Ker(\phi)$ *of it is* $n\mathbb{Z}$*, applying the First Isomorphism Theorem,* $\bar{\phi}$ *becomes an isomorphism, thus* $\mathbb{Z}/Ker(\phi) = \mathbb{Z}/n\mathbb{Z} \simeq \mathbb{Z}_n$*.*