Konkuk University Dept. Of Physics

Group Theory

2019 Spring Semester

Youngwan Kim

April 15, 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: $V \simeq \mathbb{Z}_2 \times \mathbb{Z}_2$

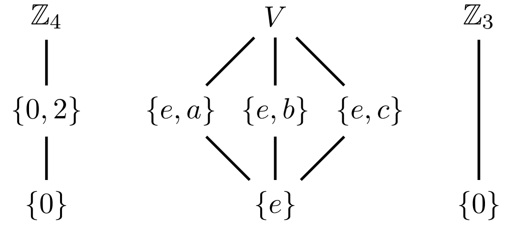
4 Subgroups

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 $h_1', h_2' \in \phi(H) : h_1'h_2' = \phi(h_1h_2) \in \phi(H)$, 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, $y = \phi(a^i) = \phi(a \ldots a) = \phi(a)^i \in \langle \phi(a) \rangle$, 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 $\phi(x) = \phi(a^i) = \phi(a \ldots a) = \phi(a)^i$ 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 $\left\langle a^{n/m} \right\rangle$.*
3. *$\langle a^s \rangle = \left\langle a^t \right\rangle \iff gcd(n,s) = gcd(n,t)$.*

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,

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

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

$$\begin{aligned} \langle a^s \rangle = \left\langle a^t \right\rangle &\implies |\langle a^s \rangle| = |\left\langle a^t \right\rangle| \\ &\iff \frac{n}{gcd(n,s)} = \frac{n}{gcd(n,t)} \\ &\iff gcd(n,s) = gcd(n,t) \end{aligned}$$

   (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.*