1. Lecture 1. Introduction 1
1.1. An algebraic object to study 2
1.2. Group 2
1.3. Isomorphic binary operations 2
2. Lecture 2. Introduction 2
2.1. The multiplication over \( \mathbb{C} \) 3
2.2. The abelian group \( (\mathbb{R}/2\pi\mathbb{Z}, +_{\mathbb{R}/2\pi\mathbb{Z}}) \) 3
2.3. Finite abelian group \( (\mathbb{U}_n(1), \cdot) \) 3
3. Lecture 3, 4, 5. Binary Operations 3
3.1. Definition 3
3.2. Isomorphic binary operations 3
3.3. Examples 4
3.4. Associativity and Commutativity 4
3.5. The identity element 4
4. Lecture 5, 6, 7. The Definition of Group 4
4.1. Inverse 4
4.2. Definition of a group 5
4.3. Key properties of a group 5
4.4. Table of finite groups 5
5. Lecture 8, 9. Subgroups 6
5.1. Definition of a subgroup 6
5.2. Cyclic subgroups 7
6. Lecture 10, 11. Cyclic groups 7
6.1. Definition 7
6.2. Properties 7
6.3. Some applications 8
7. Lecture 12, 13. The permutation groups 8
7.1. Symmetric group 8
7.2. Permutation groups 8
7.3. Cayley’s theorem 9
8. Lecture 14, 15. The concepts for group actions in general 9
8.1. Group \( G \) action on a set \( X \) 9
8.2. Free action, faithful action and transitive action 10
8.3. Orbits 10
8.4. Orbits of an element \( g \in G \) 10
8.5. \( G \)-Invariant subset 11
9. Lecture 17, 18 (Lecture 16 is midterm). The symmetric group \( S_n \) 11
9.1. Cycles 11
9.2. Even and odd permutations 11

Date: March 22, 2017.
1. Lecture 1. Introduction 1

1.1. An algebraic object to study. An algebraic object includes three ingredients:

(1) A set $S$;
(2) A binary operation $\ast$, which is a map from $S \times S$ to $S$;
(3) Certain properties.

Example 1.1. (1) The set $\mathbb{N} = \{0, 1, 2, \cdots\}$ assigned with a binary operation $\ast$. For example,
(a) $a \ast b := a + b$;
(b) $a \ast b := a \cdot b$;
(c) $a \ast b := a^b$
are binary operations. (a)(b) are associative and commutative. (c) is neither. While
(a) $a \ast b := a - b$;
(b) $a \ast b := a/b$
are NOT binary operations.

(2) Similarly, consider $S = \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ for the $\ast$ as above.

1.2. Group. A group is a set $G$ assigned with a binary operation $\ast$, which

(1) is associative;
(2) has identity;
(3) every element has an inverse.

If it is also commutative, it is called a commutative group or an abelian group.

Example 1.2. (1) $(\mathbb{Z}, +)$ is an abelian group with identity 0;
(2) $(\mathbb{R}, \cdot)$ is not a group, but $(\mathbb{R}^*, \cdot) := \mathbb{R} \setminus \{0\}, \cdot)$ is a group with identity 1;

1.3. Isomorphic binary operations. Assume $(S_1, \ast_1)$ and $(S_2, \ast_2)$ are two sets assigned with
binary operations respectively. If there is a bijective map between $S_1$ and $S_2$ such that $\ast_1$ can be
identified with $\ast_2$ via this map, then they are called isomorphic to each other.

Moreover, if both are groups, then they are called isomorphic groups.

For example, the abelian group $(\mathbb{C}, +)$ is isomorphic to $(\mathbb{R} \times \mathbb{R}, +)$.
2. Lecture 2. Introduction 2

2.1. The multiplication over \( \mathbb{C} \).
- \((\mathbb{C}, \cdot)\) is NOT isomorphic to \((\mathbb{R}^* \times \mathbb{R}^*, \cdot)\).
- Use logarithm coordinates, we can make \((\mathbb{C}, \cdot)\) isomorphic to
  \((\mathbb{R} \times (\mathbb{R}/2\pi \mathbb{Z}), +)\),
  where + is defined as the addition on \( \mathbb{R} \) together with \(+_{\mathbb{R}/2\pi \mathbb{Z}}\) on \( \mathbb{R}/2\pi \mathbb{Z} \), which we explain later. This isomorphism can be proved by Euler’s formula.

2.2. The abelian group \((\mathbb{R}/2\pi \mathbb{Z}, +_{\mathbb{R}/2\pi \mathbb{Z}})\).
- As a set, \( \mathbb{R}/2\pi \mathbb{Z} \) is the set of equivalence classes of \( \mathbb{R} \) with respect to the equivalence relation \( \sim \):
  \[ a \sim b \iff a - b \in 2\pi \mathbb{Z}. \]
- The addition \(+\) on \( \mathbb{R} \) is well-defined on this set of equivalence classes, so \(+_{\mathbb{R}/2\pi \mathbb{Z}}\) is a binary operation over \( \mathbb{R}/2\pi \mathbb{Z} \).
- In fact, it is a group and isomorphic to \((U(1) := \{ z \in \mathbb{C} | |z| = 1 \}, \cdot)\).
  (In standard notation, the 1 in \( U(1) \) denotes 1-dimensional linear space \( \mathbb{C} \) over \( \mathbb{C} \). Such groups are called unitary groups in general.)

2.3. Finite abelian group \((U_n(1), \cdot)\).
- For any positive integer \( n = 1, 2, \cdots \), define the finite set
  \[ U_n(1) = \{ z_k := e^{2\pi i k/n} | k = 0, 1, \cdots, n - 1 \}. \]
  For example,
  \[ U_4(1) = \{ z_0 = 1, z_1 = e^{\pi i/2}, z_2 = e^{\pi i}, z_3 = e^{3\pi i/2} \}. \]
  In general, \((U_n(1), +_{\mathbb{R}/2\pi \mathbb{Z}})\) is an abelian group of \( n \) elements.
- It is isomorphic to \((\mathbb{Z}_n, +_n)\), where
  \[ \mathbb{Z}_n := \{ 0, 1, \cdots, n - 1 \} = \mathbb{Z}/n\mathbb{Z} \]
  and \(+_n\) is the addition induced from the addition over \( \mathbb{Z} \).

3. Lecture 3, 4, 5. Binary Operations

3.1. Definition.
- Assume \( S \) is a set. A binary operation on \( S \) is a map
  \[ * : S \times S \to S, \quad (a, b) \mapsto a * b. \]
- Table representation for sets with finite elements.
- Assume \( S \) is assigned with a binary operation. A subset \( H \subset S \) is called closed, if the image \(*(S \times S) \subset S \). In this case, we call the binary operation \(*|_{S \times S} := *_{S} \) is the restriction of \(* \) to \( S \).

3.2. Isomorphic binary operations.
- Assume \((S_i, *)_i, i = 1, 2\) are two sets with binary operations. They are called isomorphic if there exists bijective map \( \phi : S_1 \to S_2 \) such that
  \[ \phi(a) *_2 \phi(b) = \phi(a *_1 b), \quad a, b \in S_1. \]
- Isomorphism of binary operation is an equivalence relation.
3.3. Examples.
(1) \((\mathbb{C}, +), (\mathbb{C}, \cdot)\), etc.;
(2) \((\mathbb{Z}_n, +)\);
(3) \((\mathbb{M}_{m \times n}(\mathbb{R}), +)\) is a group;
(4) Denote by \(\mathbb{gl}_n(\mathbb{R}) = \mathbb{M}_{n \times n}(\mathbb{R})\), \((\mathbb{gl}_n(\mathbb{R}), \cdot)\) is not a group;
(5) Assume \(V\) is a \(n\)-dimensional linear space. Then \((\mathbb{End}(V), \circ)\) is a set with binary operation, where \(\mathbb{End}(V)\) denotes the set of linear transformations from \(V\) to itself and \(\circ\) denotes the composition of maps;
(6) \((\mathbb{End}(V), \circ) \cong (\mathbb{gl}_n(\mathbb{R}), \cdot)\) if \(V\) is a \(n\)-dimensional linear space over \(\mathbb{R}\);
(7) \((\mathbb{GL}_n(\mathbb{R}), \cdot)\) is a group;
(8) Assume \(V\) is a \(n\)-dimensional linear space. Then \((\mathbb{Aut}(V), \circ)\) is a group, where \(\mathbb{Aut}(V)\) denotes the set of invertible linear transformations of \(V\);
(9) \((\mathbb{Aut}(V), \circ) \cong (\mathbb{GL}_n(\mathbb{R}), \cdot)\) if \(V\) is a \(n\)-dimensional linear space over \(\mathbb{R}\);
(10) Assume \((S, \ast)\) is a set assigned with binary operation and \(X\) is an arbitrary set. Denote by \(C(X, S)\) the set of all maps from the set \(X\) to \(S\). Then \(\ast\) induces a binary operation \(*_X\) on \(C(X, S)\).

3.4. Associativity and Commutativity.
- Call \((S, \ast)\) is associative, if \((a \ast b) \ast c = a \ast (b \ast c)\) for any \(a, b, c \in S\).
- Call \((S, \ast)\) is commutative, if \(a \ast b = b \ast a\) for any \(a, b \in S\).

Remark 3.1. Associativity gives a canonical way of extending the binary operator \(\ast\) to an operator acting on arbitrarily many ordered elements. Moreover, if \(\ast\) is also commutative, this \(\ast\) is independent of orders.

Example 3.2. Assume \((S, \ast)\) is a set assigned with binary operation and \(X\) is an arbitrary set. We have known it induces \((C(X, S), \ast_X)\). If \((S, \ast)\) is associative (or commutative), \((C(X, S), \ast_X)\) is also associative (or commutative).

3.5. The identity element.
- Assume \((S, \ast)\) is a set with a binary operation. An element \(e \in S\) is called an (the) identity, if \(e \ast a = a, \ b \ast e = b\) for any \(a, b \in S\).
- Identity may not exist (e.g. \((\mathbb{N}^*, +)\) has no identity), but if it exists, it must be the unique.
- Examples:
  (1) \((\mathbb{N}, +)\) has the identity \(0\);
  (2) \((\mathbb{N}, \cdot)\) has the identity \(1\).
- Isomorphism of two binary structures must maps identity to identity.

4. Lecture 5, 6, 7. The Definition of Group

4.1. Inverse.
- Assume \((S, \ast)\) is a set with a binary operation and has identity \(e\). An element \(a \in S\) has left (right) inverse, if there exists some \(a' \in S\) such that \(a' \ast a = e \quad (a \ast a' = e)\).

An element \(a \in S\) has inverse, if it has both left inverse and right inverse, and they are the same, i.e., there exists some \(a' \in S\) such that \(a' \ast a = a \ast a' = e\).
- Assume \((S, \ast)\) is associative. If an element has both left inverse and right inverse, then these two inverses must be the same.
• If \((S, \ast)\) is associative, then the inverse of an element is unique. We denote it by \(a^{-1}\) in general, but sometimes by \(-a\) if \(\ast\) is commutative.

4.2. **Definition of a group.** A group is a set \((G, \ast)\) with binary operation satisfying

- It is associative;
- It has identity;
- Every element has an inverse.

**Example 4.1.** Use definition to check \((\mathbb{Z}_n, +_n)\) is a group.

In fact, to check \((G, \ast)\) is a group, we only need the following

**Proposition 4.2.** Assume \((G, \ast)\) is a set with binary operation. It is a group if

- It is associative;
- It has left identity (i.e., there exists some \(e \in G\) such that \(e \ast a = a\) for any \(a \in G\));
- Every element has a left inverse.

**Proof.**

- We first show \(e\) is also a right inverse, i.e., for every \(a \in G\), \(a \ast e = a\). Take \(a'\) as a left inverse of \(a\), then
  
  \[ a' \ast (a \ast e) = (a' \ast a) \ast e = e \ast e = e. \]

  On the other hand, \(a' \ast a = e\). So assume \(a''\) is a left inverse of \(a'\), and then
  
  \[ a'' \ast (a' \ast (a \ast e)) = a'' \ast (a' \ast a). \]

  Use the associativity again, we get \(a \ast e = a\).

- Next we show if \(a'\) is a left inverse of \(a\), then it is also a right inverse of \(a\).
  
  \[ a' \ast (a \ast a') = a' = a' \ast e. \]

  We multiply the left inverse of \(a'\) from left and get \(a \ast a' = e\).

\[ \square \]

4.3. **Key properties of a group.**

- The cancellation rule.
- Existence and uniqueness of the equations \(a \ast x = b, x \ast a = b\).
- Examples in linear algebra.

4.4. **Table of finite groups.** Basic rules:

1. the row/column of \(e\);
2. no repeating element in each row/column, so every element must show once.

**Example 4.3.**

- If \(|G| = 1\), then \(G = \{e\}\);
- If \(|G| = 2\), then \(G = \mathbb{Z}_2\);
- If \(|G| = 3\), then \(G = \mathbb{Z}_3\);
- If \(|G| = 4\), then \(G = \mathbb{Z}_4\) or \(K_4 = \mathbb{Z}_2 \times \mathbb{Z}_2\).
<table>
<thead>
<tr>
<th>Order</th>
<th>Number</th>
<th>Abelian</th>
<th>Non-Abelian</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>2</td>
<td>1</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>3</td>
<td>1</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>4</td>
<td>2</td>
<td>2</td>
<td>0</td>
</tr>
<tr>
<td>5</td>
<td>1</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>6</td>
<td>2</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>7</td>
<td>1</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>8</td>
<td>5</td>
<td>3</td>
<td>2</td>
</tr>
<tr>
<td>9</td>
<td>2</td>
<td>2</td>
<td>0</td>
</tr>
<tr>
<td>10</td>
<td>2</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>11</td>
<td>1</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>12</td>
<td>5</td>
<td>2</td>
<td>3</td>
</tr>
<tr>
<td>13</td>
<td>1</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>14</td>
<td>2</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>15</td>
<td>1</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>16</td>
<td>14</td>
<td>5</td>
<td>9</td>
</tr>
<tr>
<td>17</td>
<td>1</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>18</td>
<td>5</td>
<td>2</td>
<td>3</td>
</tr>
<tr>
<td>19</td>
<td>1</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>20</td>
<td>5</td>
<td>2</td>
<td>3</td>
</tr>
<tr>
<td>21</td>
<td>2</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>22</td>
<td>2</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>23</td>
<td>1</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>24</td>
<td>15</td>
<td>3</td>
<td>12</td>
</tr>
<tr>
<td>25</td>
<td>2</td>
<td>2</td>
<td>0</td>
</tr>
<tr>
<td>26</td>
<td>2</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>27</td>
<td>5</td>
<td>3</td>
<td>2</td>
</tr>
<tr>
<td>28</td>
<td>4</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>29</td>
<td>1</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>30</td>
<td>4</td>
<td>1</td>
<td>3</td>
</tr>
</tbody>
</table>

5. LECTURE 8, 9. SUBGROUPS

5.1. Definition of a subgroup.

- A subset $H$ of a group $(G, *)$ is called a subgroup, if $H$ is closed under $*$ and the induced binary operation on $H$ makes $(H,*_H)$ be a group. Denote by $H < G$.
- If $H < G$, then the identity of $G$ must be the identity of $H$. Any element $a \in H$, the inverse $a^{-1}$ of $a$ in $G$ is also the inverse of $a$ in $H$.

**Example 5.1.**

1. $(\mathbb{Z}, +) < (\mathbb{R}, +)$;
2. $(U_n(1), \cdot) < (\mathbb{C}, \cdot)$;
3. $(n\mathbb{Z}, +) < (\mathbb{Z}, +)$;
4. $(\mathbb{Z}_n, +_n)$ is not a subgroup of $(\mathbb{Z}, +)$!

**Proposition 5.2.** Assume $G$ is a group. A subset $H$ of $G$ is a subgroup if and only if $ab^{-1} \in H$ for any $a, b \in H$.

**Proposition 5.3.** If $H, K$ are two subgroups of $G$, then $H \cap K$ is also a subgroup of $G$. 
Example 5.4. \( m\mathbb{Z} \cap n\mathbb{Z} = \text{lcm}(m, n)\mathbb{Z} \) as subgroups of \( \mathbb{Z} \).

Remark 5.5. (1) \( H \cup K \) is not a subgroup in general, but it is a subgroup if \( G \) is abelian. (A more general condition is either \( H \) or \( K \) is normal in \( G \). We are going to introduce the concept of normal subgroup later.) (2) \( HK \) is not a subgroup in general.

Example 5.6. Assume \( G \) is a group.

(1) For any \( a \in G \), \( C(a) := \{ x \in G | ax = xa \} \) is called the set of commutators of \( a \). \( C(a) < G \).

(2) For any subset \( S \subset G \), \( C(S) := \{ x \in G | xs = sx \text{, any } s \in S \} \) is called the centralizer of \( S \) in \( G \). \( C(S) < G \).

(3) In particular, \( C(G) := Z(G) \) is called the center of \( G \). It is a normal abelian subgroup of \( G \).

5.2. Cyclic subgroups. Assume \( G \) is a group. Take any \( a \in G \), it generates a subgroup \( \langle a \rangle \) named a cyclic subgroup.

- It is the smallest subgroup containing \( a \). This gives another definition of \( \langle a \rangle \) as \( \langle a \rangle = \cap_{H < G, a \in H} H \).

- Order of \( a \) is defined as the minimal positive integer such that \( a^n = e \). It is the same as \( | \langle a \rangle | \). E.g., In \( \mathbb{Z}_6 \), \( 2 \) has order \( 3 \) which is the same as \( | \langle 2 \rangle | = |\{0, 2, 4\}| = 3 \).

- In a finite group, every element has a finite order.

- Example of element of finite order in an infinite group: 1. \( e^{2\pi i q}, q \in \mathbb{Q} \), in \( \mathbb{C}^* \); 2. \( -I_n \in GL_n(\mathbb{R}) \); 3. \( J \in GL_2(\mathbb{R}) \).

- If there exists some \( a \in G \) such that \( G = \langle a \rangle \), then \( G \) is called a cyclic group. E.g., \( \mathbb{Z} = \langle 1 \rangle = \langle -1 \rangle ; 3\mathbb{Z} = \langle 3 \rangle \). A cyclic group is obviously an abelian group.


6.1. Definition.

- A group \( G \) is called a cyclic group, if there exists some element \( a \in G \) such that \( G = \langle a \rangle \). The element \( a \) is called a generator of \( G \).

- \( (a^n)^{-1} = a^{-n}, a^m a^n = a^{m+n} \).

- Examples:
  (1) \( (\mathbb{Z}, +), \mathbb{Z} = \langle 1 \rangle = \langle -1 \rangle \);
  (2) \( \mathbb{Z}_n = \langle 1 \rangle \).

6.2. Properties.

Proposition 6.1. A cyclic group must be an abelian group.

Proposition 6.2. All subgroups of a cyclic group are cyclic.

Proposition 6.3. \(| \langle a \rangle | = \min_{n \in \mathbb{Z}^+} \{ a^n = e \} \).

Proposition 6.4 (Classification of cyclic groups). Up to group isomorphisms, cyclic groups have only two types:

- \( (\mathbb{Z}, +) \);
- \( (\mathbb{Z}_n, +_n), n = 1, 2, 3, \cdots \) (where \( \mathbb{Z}_1 = \{0\} \)).
6.3. Some applications.

- The concept of g.c.d. can be generalized to any cyclic groups. (In fact, this concept can be introduced to more general algebraic objects that satisfy the division algorithm.)

**Proposition 6.5.** If \( G, H \) are two cyclic groups, and \( \phi : G \to H \) is a group homomorphism, then
\[
g.c.d(\phi(a), \phi(b)) = \phi(\text{g.c.d}(a, b)), \quad \text{for any } a, b \in G.
\]

This can be used to calculate g.c.d.s for any cyclic group, whenever you know a group homomorphism \( \mathbb{Z} \to G \).

- All subgroups of \( \mathbb{Z} \) are of the form \( n\mathbb{Z} \), \( n = 0, 1, 2, \ldots \).
- All subgroups of \( \mathbb{Z}_n \) are of the form \( < k > \), where \( k = 0, 1, \ldots, n - 1 \).

**Proposition 6.6.**

1. The order of \( k, < k > \) equals \( \frac{n}{\text{g.c.d}(k, n)} \).
2. \( < k > < \ell > \) if and only if \( \text{g.c.d}(k, n) = \text{g.c.d}(\ell, n) \).
3. \( < k > = \mathbb{Z}_n \) if and only if \( \text{g.c.d}(k, n) = 1 \), i.e., \( k \) and \( n \) are co-prime.

**Proof.** (1) Denote by \( d = \text{g.c.d}(k, n) \). First, notice that \( \frac{n}{d} \) divides \( \frac{k}{d}n \) which implies \( \frac{n}{d} \) divides \( n \). Thus
\[
\min_{m>0}\{mk = 0\} \leq \frac{n}{d} = \frac{k}{d}n.
\]

On the other hand, from the definition of \( d \), we know \( \frac{n}{d} \) and \( \frac{k}{d} \) are coprime. It follows \( \frac{n}{d} \) divides \( \frac{k}{d}n \) implies \( \frac{n}{d} \) divides \( n \). Thus
\[
\min_{m>0}\{mk = 0\} \geq \frac{n}{d}.
\]

Hence this proves \( \min_{m>0}\{mk = 0\} = \frac{n}{d} \). Since we have shown \( | < k > | = \min_{m>0}\{mk = 0\} \) and we are done.

(2) Denote by \( d = \text{g.c.d}(k, n) = \text{g.c.d}(\ell, n) \). Let’s show in fact \( < d > < k > < \ell > \). Because \( d|k \), then it follows \( < d > \subseteq < k > \). Notice
\[
| < d > | = \frac{n}{d} = | < k > |,
\]
so it follows \( < d > < k > \). The other equality is exactly the same.

(3) Immediately follows from (2).

The above properties hold for any cyclic group from the classification of cyclic groups.

7. Lecture 12, 13. The permutation groups

7.1. Symmetric group.

- Definition of \( S_n \) and notations. (Here we take \( n = 1, 2 \).)
- \( S_n \) is a finite group of \( n! \)'s elements.
- \( S_n \) is abelian if and only if \( n = 1, 2 \).

7.2. Permutation groups.

- Any set \( X \), define \( S_X \) as the set of all bijective maps from \( X \) to itself.
- If \( X \) is ordered and \( |X| = n \), which means there is a bijective map
\[
\text{ord} : \{1, 2, \ldots, n\} \to X,
\]
then \( \text{ord} \) induces a group isomorphism \( S_X \to S_n \).
7.3. **Cayley’s theorem.**
- Definition of group homomorphism.
- Concept of subgroups.

**Theorem 7.1** (Cayley’s). *Any group* $G$ *can be considered as a subgroup of* $S_G$ *via a canonical injective group homomorphism.*

**Proof.** Construct $\phi : G \to S_G$ as $\phi(g) = xg$. \hfill $\square$

This is named a (right) regular representation of $G$. (Convention: My convention here is different from the book that I define the binary operation $\cdot : S_X \times S_X \to S_X$ as $f \cdot g := g \circ f$. In the previous statement, we omit $\cdot$ and write $fg = f \cdot g = g \circ f$.)

**Remark 7.2.** In general, $\phi(g) \notin \text{Aut}(G)$, where $\text{Aut}(G)$ is defined as the group of group isomorphisms of $G$.

- Definition of a group representation in general, and why we can consider the regular representation as a presentation. (Taking $V = C(G, \mathbb{R})$ for example.)

8. **Lecture 14, 15. The concepts for group actions in general**

8.1. **Group $G$ action on a set $X$.** We always assume $X \neq \emptyset$.

**Definition 8.1.** Call a group $G$ acting on a set $X$ (from right), if there exists a map

$A : G \times X \to X$,

satisfying the following two requirements: denote by $A_g(x) := A(g, x)$,

1. $A_e = \text{id}_X$;
2. $A_{g_2} \circ A_{g_1} = A_{g_1 g_2}$.

If a set $X$ admitting a $G$-action, we call $X$ a $G$-set.

**Proposition 8.2.** Assume $G$ is a group, the map

$A : G \times X \to X$,

is a group action of $G$ on $X$ if and only if

$A : G \to S_X, \quad A(g) := A_g$

is group homomorphism.

**Example 8.3.** (1) Any set $X$ admitting $S_X$-action defined as

$A_{\sigma}(x) = \sigma(x)$.

(Ex: Check this is compatible with our convention here.)

(2) Any group $G$ admitting $G$-action of the right multiplication as

$R_g(x) := xg, \quad g \in G$,

and this is named as the right action. The Cayley’s theorem tells us that, by regarding $G$ as a subgroup of $S_X$ by the regular representation, the $G$-action on $G$ is induced from the $S_G$ action on $G$.

(3) Any group $G$ admitting $G$-action of left inverse multiplication as

$L_g(x) := g^{-1}x, \quad g \in G$,

and this is named as the left action.
(4) Any group $G$ admitting an $G$ action defined as $\text{Ad}_g = L_g \circ R_g$, for any $g \in G$. This is called the adjoint action.

(5) For any $H < G$, the $G$ action on $X$ induces $H$ action on $X$. In particular, any element $g \in G$, the $G$-action on $X$ induces the cyclic group $\langle g \rangle$ on $X$.

8.2. Free action, faithful action and transitive action. Assume $G$ acts on a set $X$, for some $x \in X$, denote by $G_x := \{g \in G|A_g(x) = x\}$, and this is called the isotropy group at $x$. For any $x \in X$, $G_x < G$.

Definition 8.4. (1) An action $G$ on $X$ is called a free action, if $G_x = \{e\}$ for any $x \in X$.

(2) An action $G$ on $X$ is called a faithful (or effective) action, if $\cap_{x \in X}G_x = \{e\}$.

From definition, a free action must be faithful, but a faithful action may not be free.

Proposition 8.5. A group action $G$ on $X$ is faithful if and only if the group homomorphism $A : G \to S_X$ is injective.

Remark 8.6. In fact, $\ker A = \cap_{x \in X}G_x$ is a normal subgroup of $G$, which we are going to prove in later lectures.

Definition 8.7. An action $G$ on $X$ is called transitive, if for any $x, y \in X$, there exists some $g \in G$, such that $A_g(x) = y$.

Example 8.8. (1) The left and right actions of $G$ on itself are both free and transitive.

(2) For the adjoint action of $G$ on itself, we have
- $G_x = C(x)$, i.e., the commutator of $x \in G$.
- $\ker \text{Ad} = C(G)$, i.e., the center of $G$. Hence the adjoint action is faithful if and only if $G$ has trivial center $C(G)$.

8.3. Orbits. Assume $G$ acts on $X$. Then we can define an equivalence relation on $X$ as:

$$x \sim y \quad \text{if and only if there exists some } g \in G \text{ such that } A_g(x) = y.$$ 

Usually, we use $[x]$ to denote the equivalence class including $x$. In particular, for the group action case, we also call $[x]$ the orbit of $G$ containing $x$, sometimes we use $\text{orb}_G(x)$ to denote it.

Proposition 8.9. $G$ has only one orbit if and only if the action is transitive.

Remark 8.10. There is a very interesting result, which is , if $G$ acts on $X$ transitively and both $G$ and $X$ are finite, then

$$|G| = \Sigma_{g \in G} X_g,$$

where $X_g$ is the fixed point set of $X$, i.e., $X_g = \{x \in X|A_g(x) = x\}$. For example, take $G = S_3$ acting on $N = \{1, 2, 3\}$. It is a transitive action. We know $|S_3| = 3! = 6$. On the other hand,

$$N_{(1)} = 3, \quad N_{(12)} = N_{(23)} = N_{(31)} = 1,$$

and $3 + 1 + 1 + 1 = 6$. This is a special case of the Burnside’s formula, which we can prove after we learn more about finite groups.

8.4. Orbits of an element $g \in G$. Assume group $G$ acting on the set $X$, for any $g \in G$, we know $\langle g \rangle$ is a subgroup of $G$ and hence $\langle g \rangle$ acts on $X$. For any $x \in X$, we call the orbit of $\langle g \rangle$ containing $x$, denote by $\text{orb}_g(x)$ the orbit of $g$ containing $x$.

Example 8.11. (1) Consider $\sigma = \left( \begin{array}{cccccc} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 8 & 6 & 7 & 4 & 1 \\ 5 & 2 & \end{array} \right)$. Then

$$\text{orb}_\sigma(1) = \text{orb}_\sigma(3) = \text{orb}_\sigma(6) = \{1, 3, 6\}$$

$$\text{orb}_\sigma(2) = \text{orb}_\sigma(8) = \{2, 8\}$$

$$\text{orb}_\sigma(4) = \text{orb}_\sigma(5) = \text{orb}_\sigma(7) = \{4, 5, 7\}.$$
8.5. \textit{G-Invariant subset.}

\textbf{Definition 8.12.} Assume the group $G$ acting on a set $X$. A subset $Y \subset X$ is called $G$-invariant, if $A_g(y) \in Y$ for any $y \in Y$, $g \in G$.

If $Y \subset X$ is $G$-invariant subset, then it becomes a $G$-set by the group action induced from $X$.

\textbf{Proposition 8.13.} Assume the group $G$ acting on a set $X$. Then for any $x \in X$, $\text{orb}_G(x)$ is $G$-variant, and the induced $G$ action on $\text{orb}_G(x)$ is transitive.

9. \textsc{Lecture 17, 18 (Lecture 16 is Midterm). The Symmetric Group $S_n$}

This section, we focus on $S_n$. The finiteness of $n$ plays an essential role.

9.1. \textbf{Cycles.}

- Definition of a cycle: $\sigma \in S_n$ is called a cycle if it has at most one orbit containing more than one element.
- Length of a cycle. A cycle of length 2 is called a transposition.
- Example.
- Notation for a cycle, e.g., in $S_8$
  \[ \mu = (1, 3, 6) = \begin{pmatrix} 1 & 3 & 4 & 5 & 6 \\ 2 & 6 & 4 & 7 & 8 \end{pmatrix} = (3, 6, 1) = (6, 1, 3). \]

- Disjoint cycles.
- Any permutation can be written into a product of disjoint cycles.
- Any two disjoint cycles are commutative. (Though not any two permutation commute.)

\textbf{Example 9.1.} (1)
\[ \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 5 & 2 & 4 & 3 & 1 \end{pmatrix} = (1, 6)(2, 5, 3) = (2, 5, 3)(1, 6). \]

(2)
\[ (1, 4, 5, 6)(2, 1, 5) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 4 & 3 & 5 & 2 & 1 \end{pmatrix} \neq (2, 1, 5)(1, 4, 5, 6). \]

9.2. \textbf{Even and odd permutations.}

\textbf{Theorem 9.2.} Assume $n \geq 2$. Any permutation is a product of transpositions.

For example, $(1, 2, 3, 4) = (1, 4)(1, 3)(1, 2)$.

\textbf{Theorem 9.3.} If a permutation $\sigma$ is a product of even number of transpositions, then it can not be written as a product of odd number of transpositions.

\textit{Proof.} Consider the $S_n$ action on $GL_n(\mathbb{R})$ and the map
\[ \phi : S_n \rightarrow \pm 1, \quad \sigma \mapsto \det(A_\sigma(I_n)). \]

This theorem makes us be able to define even/odd permutations.

\textbf{Theorem 9.4.} In $S_n$, the number of odd permutations are the same as the number of even permutations.

Denote by $A_n \subset S_n$ the subset of even permutations.

\textbf{Theorem 9.5.} $A_n$ is a subgroup of $S_n$ of $\frac{n!}{2}$ elements, which is called the alternating group.
Proof. (1) Method 1: Direct proof.
(2) Method 2: Construct group homomorphism \( S_n \to \mathbb{Z}_2 \).

10. Lecture 18, 19. Cosets


**Definition 10.1.** \( H < G \), a left coset containing \( a \) is defined as
\[
aH := \{ ah | h \in H \} \subset G.
\]
Similarly, a right coset containing \( a \in G \) is defined as
\[
Ha := \{ ha | h \in H \} \subset G.
\]

**Remark 10.2.** (1) In general, \( aH \) is not a subgroup of \( G \). But if \( G \) is abelian, \( aH = Ha < G \). (In fact, \( aH = Ha \) if and only if \( H \triangleleft G \).

(2) Consider the right action of \( H \) on \( G \), \( aH = \text{orb}_H(a) \).

**Proposition 10.3.** For each coset \( aH \), there a canonical bijective map from \( H \) to it given as
\[
\phi_a : H \to aH, \ h \mapsto ah.
\]

**Remark 10.4.** This is a general fact that \( G \) acts on \( X \) freely, then there exits a bijective map from \( G \) to each orbit \( \text{orb}_G(x) \) as
\[
\phi_x : G \to \text{orb}_G(x), \ g \mapsto A_g(x).
\]

**Corollary 10.5.** If \( G \) is finite, \( |aH| = |H| \).

**Lemma 10.6.** (1) For any \( a, b \in G \), either \( aH = bH \) or \( aH \cap bH = \emptyset \).
(2) \( aH = bH \) if and only if \( b^{-1}a \in H \).

**Lemma 10.7.** Define \( a \sim_H b \) as \( b^{-1}a \in H \). Then \( \sim_H \) is an equivalence relation on \( G \). Denote by \([G : H]\) the set of such equivalence classes.

Hence

**Proposition 10.8.** Can decompose \( G = \sqcup_{[a] \in [G : H]} aH \) as disjoint union.

10.2. The Lagrange theorem.

**Theorem 10.9** (Lagrange). Assume \( G \) is a finite group and \( H < G \). Then \( |H| \) divides \( |G| \).

In fact, we know \( |G| = |H| |[G : H]| \). Denote by
\[
(G : H) := |[G : H]|
\]
and call it the index of \( H \) in \( G \).

Now we list some applications of the Lagrange theorem on finite groups. Assume \( G \) is a finite group.

(1) If \( |G| \) is prime, then \( G \) is cyclic.
(2) Any \( a \in G, \ |a| \) must divide \( |G| \).
(3) If \( K < G, H < G, K < H \), then \( (G : K) = (G : H)(H : K) \).

11. Lecture 20, 21. Structures of finite abelian groups

11.1. Direct product of groups.

- \( \Pi_{i=1}^n G_i \) is called the direct product of groups \( G_i \)'s, \( i = 1, \cdots, n \).
- If every \( G_i \) is abelian, then \( \Pi_{i=1}^n G_i \) is also abelian. For this case, usually write as \( \bigoplus_{i=1}^n G_i \).
- If every \( G_i \) is finite, then \( |\Pi_{i=1}^n G_i| = \Pi_{i=1}^n |G_i| \).
11.2. Direct product of finite abelian groups.

Proposition 11.1. \( \mathbb{Z}_m \oplus \mathbb{Z}_n \) is isomorphic to \( \mathbb{Z}_{mn} \) if and only if \( \gcd(m, n) = 1 \).

More generally,

Theorem 11.2. \( \bigoplus_{i=1}^m \mathbb{Z}_{n_i} \) is isomorphic to \( \mathbb{Z}_{n_1 n_2 \cdots n_m} \) if and only if \( \gcd(n_i, n_j) = 1 \) for any \( i \neq j \).

Proof. Show \( \phi : \mathbb{Z}_{n_1 n_2 \cdots n_m} \rightarrow \bigoplus_{i=1}^m \mathbb{Z}_{n_i}, \quad a \mapsto ([a]_{n_1}, [a]_{n_2}, \cdots, [a]_{n_m}) \) is a group homomorphism. It is injective if and only if \( \gcd(n_i, n_j) = 1 \) for any \( i \neq j \). \( \square \)

Now given \( n = (p_1)^{n_1} (p_2)^{n_2} \cdots (p_m)^{n_m} \), for \( p_1, \cdots, p_m \) are disjoint prime numbers, then using the previous theorem, we know

\[
\mathbb{Z}_n \cong \mathbb{Z}_{(p_1)^{n_1}} \oplus \mathbb{Z}_{(p_2)^{n_2}} \oplus \cdots \oplus \mathbb{Z}_{(p_m)^{n_m}}.
\]

For example, \( \mathbb{Z}_{72} \cong \mathbb{Z}_8 \oplus \mathbb{Z}_9 \).

Theorem 11.3. Assume \( a_i \in G_i \) has order \( r_i \), then the order of the element \( a = (a_1, a_2, \cdots, a_n) \in \prod_{i=1}^n G_i \) is the least common multiple of \( r_i \)’s, \( i = 1, \cdots, n \).

Proof. We show \( n = 2 \) now and for higher \( n \)’s, you may use induction to see. Assume \( a = (a_1, a_2) \in G_1 \times G_2 \) with \( \text{ord}(a_1) = r_1, \text{ord}(a_2) = r_2 \). We show \( a \) has order \( r := \text{lcm}(r_1, r_2) \) now. First, it is clear that

\[
a^r = e,
\]

so \( r \leq \text{ord}(a) \). On the other hand, any \( a^k = e \), and it follows \( a_1^k = e_1, a_2^k = e_2 \). We have \( r_1 | k, r_2 | k \), so \( k \geq \text{lcm}(r_1, r_2) \). Then we are done. \( \square \)

Example 11.4. The order of \( (8, 4, 10) \in \mathbb{Z}_{12} \oplus \mathbb{Z}_{60} \oplus \mathbb{Z}_{24} \) is 60. That is because the order of \( 8 \in \mathbb{Z}_{12} \) has order \( \frac{12}{\gcd(8, 12)} = 3 \), the order of \( 4 \in \mathbb{Z}_{60} \) has order \( \frac{60}{\gcd(4, 60)} = 15 \), the order of \( 10 \in \mathbb{Z}_{24} \) has order \( \frac{24}{\gcd(10, 24)} = 12 \). The least common multiple of 3, 15, 12 is 60.

Theorem 11.5. Every finite abelian group is isomorphic to some direct product

\[
\mathbb{Z}_{(p_1)^{r_1}} \times \mathbb{Z}_{(p_2)^{r_2}} \cdots \mathbb{Z}_{(p_n)^{r_n}},
\]

where \( p_i \) are prime numbers. It is cyclic if and only if all \( p_i \)’s are disjoint.

Proof. We prove if all \( p_i \)’s are disjoint prime numbers, then this direct product is cyclic. It is enough to find an element of order \( \prod_{i=1}^n (p_i)^{r_i} \). Take \( a_i \) as the generator of \( \mathbb{Z}_{(p_i)^{r_i}} \). From Theorem 11.3, we know it has order \( \prod_{i=1}^n (p_i)^{r_i} \). \( \square \)

11.3. Finitely generated abelian groups.

Definition 11.6. Assume \( G \) is a group. We say it is generated by a subset \( S \) of it, if \( G \) is the only subgroup of \( G \) which contains \( S \). A group \( G \) is called finitely generated, if there exists a finite subset \( S \) of \( G \) which generates \( G \).

The following theorem is one the most important results about abelian groups.

Theorem 11.7. If \( G \) is a finitely generated abelian group, then \( G \) is isomorphic to the direct product

\[
\mathbb{Z} \oplus \mathbb{Z} \oplus \cdots \mathbb{Z} \oplus \mathbb{Z}_{(p_1)^{r_1}} \times \mathbb{Z}_{(p_2)^{r_2}} \cdots \mathbb{Z}_{(p_n)^{r_n}},
\]

where \( p_i \) are prime numbers. Moreover, this decomposition is unique up to orders.

This number of copies of \( \mathbb{Z} \)’s is called the rank (or Betti number or dimension) of \( G \). The finite abelian group part \( \mathbb{Z}_{(p_1)^{r_1}} \times \mathbb{Z}_{(p_2)^{r_2}} \cdots \mathbb{Z}_{(p_n)^{r_n}} \) is called the torsion part of \( G \).

Remark 11.8. Finitely generated abelian groups naturally appear as (singular) (co)homology groups of CW complexes.
12. Definition of group homomorphism.

**Definition 12.1.** Assume $G$ and $H$ are two groups. A map $\phi : G \to H$ is a group homomorphism if

$$\phi(g_1g_2) = \phi(g_1)\phi(g_2),$$

for any $g_1, g_2 \in G$.

Here are some basic properties:

- There exists some injective homomorphism $G \to H$ if and only if $G < H$;
- There exists some bijective homomorphism $G \to H$ if and only if $G \cong H$.
- A group homomorphism maps identity to identity, inverse to inverse, subgroup to subgroups, preimage of a subgroup is a subgroup. In particular, the preimage of $\{e_H\} = \ker \phi$ is a normal subgroup of the domain group.
- Composition of two group homomorphisms is a group homomorphism.
- $\text{Aut}(G)$ is a group. (Caution, $S_G \neq \text{Aut}(G)$ in general. e.g., $\text{Aut}(\mathbb{Z}_3) = \mathbb{Z}_2$, but $S_{\mathbb{Z}_3} = S_3$.)

**Proposition 12.2.** A group homomorphism is injective if and only if $\ker \phi = \{e\}$.

**Example 12.3.**

1. Trivial homomorphism.
2. The inclusion of $G_1 \to G_1 \times G_2$;
3. The projection of $G_1 \times G_2 \to G_1$.
4. $G$ action on a set $X$ induces a homomorphism $G \to S_X$.
5. $\mathbb{Z} \to \mathbb{Z}_n$.
6. $S_n \to \mathbb{Z}_2$.
7. $\det : GL_n(F) \to F$, $F = \mathbb{Q}, \mathbb{R}, \mathbb{C}$ or other fields.
8. A homomorphism from a cyclic group completely determined by the image of the generator.

12.2. Normal subgroups.

- A subgroup $N < G$ is called normal, if $g^{-1}ag \in N$ for any $a \in N, g \in G$.
- $N < G$ is normal if and only if $N$ is $Ad$-action invariant.
- $N < G$ if and only if $aN = Na$ for any $a \in G$. In this case, $\{aN | a \in G\}$ becomes a group. This is called the quotient group of $G$ by $N$, which is denoted by $G/N$.
- Any subgroup of an abelian group is normal.

**Proposition 12.4.** Assume $N < G$, then the map

$$\phi : G \to G/N, \quad \phi(g) = gN$$

is a group homomorphism, whose kernel is $N$.

**Definition 12.5.** A group $G$ is called simple if there is no proper nontrivial normal subgroup.

12.3. Fundamental theorem of group homomorphism.

**Theorem 12.6.** Assume $\phi : G \to H$ is a group homomorphism. Then $\phi$ induces a group isomorphism from the quotient group $G/\ker \phi$ to the image $\phi(G)$.


13.1. Simple groups.

**Definition 13.1.** A group is called simple if there is no nontrivial, proper normal subgroups.

**Example 13.2.** The alternating group $A_n$ is simple for $n \geq 5$. 
Definition 13.3. A maximal normal subgroup of a group $G$ is a proper normal subgroup of $G$ such that there is no proper normal subgroup $N$ of $G$ properly containing $M$.

Lemma 13.4. $M$ is a maximal normal subgroup of $G$ if and only if $G/M$ is simple.

13.2. Centers and the commutator subgroup. The subset $Z(G) := \{g \in G | gx = xg, \text{ for any } x \in G\}$ is called the center of $G$, which is a normal subgroup of $G$.

Lemma 13.5. $G = Z(G)$ if and only if $G$ is abelian.

If $Z(G)$ is trivial, i.e., $Z(G) = \{e\}$, we call the group $G$ has trivial center. This indicates this group is ‘most noncommutative’.

Example 13.6. $S_3$ has trivial center.

Lemma 13.7. $Z(G_1 \times G_2) = Z(G_1) \times Z(G_2)$.

Lemma 13.8. The kernel of the surjective homomorphism $c : G \rightarrow \text{Inn}(G)$ is $Z(G)$.

To better characterize non-commutativity, we consider another normal subgroup.

Definition 13.9. The elements of the form $a^{-1}b^{-1}ab$ for some $a, b \in G$ are called commutators of the group $G$. We use $[G, G]$ to denote the subgroup generated by all commutators of the group $G$.

The subgroup $[G, G]$ measures how much the group $G$ is non-commutative. For example,

Lemma 13.10. $G$ is abelian if and only if $[G, G]$ is trivial.

The following observation in essential that people introduce this commutator subgroup.

Lemma 13.11. $[G, G] \triangleleft G$. Moreover, the quotient group $G/[G, G]$ is abelian.

14. Semidirect-products and Split Extension

14.1. Semidirect-products. Assume $G$ and $Q$ are two groups, and

$$\alpha : Q \rightarrow \text{Aut}(G)$$

is a group homomorphism, we can create a new group structure on the set $Q \times G$ using $\alpha$. Define

$$(q_1, g_1) *_{\alpha} (q_2, g_2) := (q_1 q_2, \alpha(q_2)g_1g_2).$$

Lemma 14.1. $Q \times G$ becomes a group with respect to the binary operation $*_{\alpha}$, if and only if $\alpha$ is a group homomorphism. The identity element is $(e_Q, e_G)$ and the inverse of $(q, g)$ is

$$(q, g)^{-1} = (q^{-1}, \alpha(q^{-1})(g^{-1})).$$

Usually we use $Q \ltimes G$ to denote this group and call it a semidirect-product of $Q$ and $G$.

Example 14.2. (1) The direct product $Q \times G$ is a special case of semidirect-product as $\alpha \equiv \text{id}_G$.

(2) Take $Q = \mathbb{Z}_2$ and $G = \mathbb{Z}_3$. Define

$$\alpha(0) = \text{id}_{\mathbb{Z}_3}, \quad \alpha(1) = (\cdot)^{-1}.$$

Direct checking shows that $\alpha : \mathbb{Z}_2 \rightarrow \text{Aut}(\mathbb{Z}_3)$ is a group homomorphism. The semidirect-product $\mathbb{Z}_2 \ltimes \alpha \mathbb{Z}_3$ in fact is isomorphic to $S_3$, which is different from $\mathbb{Z}_2 \times \mathbb{Z}_3$ (to see they are different, e.g., the inverse of $(1, 1)$ in $\mathbb{Z}_2 \times \mathbb{Z}_3$ is $(1, 2)$, but in $\mathbb{Z}_2 \ltimes \mathbb{Z}_3$ is $(1, 1)$).

(3) In fact, for all $n \geq 2$, we can similarly construct $\mathbb{Z}_2 \ltimes \alpha \mathbb{Z}_n$, which turns to be the same as $D_n$, the symmetry group of regular $n$-polygons (the Dihedral group). In particular, $D_2 = K_4$, $D_3 \cong S_3$. (You can check, all $D_n$ with $n \geq 3$ are nonabelian.)
14.2. **Splitting extension.** Assume \( \phi : H \rightarrow Q \) is a surjective group homomorphism.

**Definition 14.3.** A map

\[
s : Q \rightarrow H
\]
satisfying \( \phi \circ s = \text{id}_H \), is called a section of \( \phi : H \rightarrow Q \).

**Remark 14.4.** In general, we can not expect to find a section which is a group homomorphism.

Define \( \alpha : Q \rightarrow \text{Aut}(H) \) as follows: For each \( q \), define

\[
\alpha_s(q)(x) = \text{Ad}_{s(q)}(x).
\]

Denote by \( G := \ker \phi \). Since \( G < H \), \( G \) is invariant under the adjoint action. So we obtain a map

\[
\alpha_s : Q \rightarrow \text{Aut}(G).
\]

**Lemma 14.5.** If \( s \) is a group homomorphism, then \( \alpha_s \) is a group homomorphism.

We know if \( \alpha_s \) is a group homomorphism, then it defines the semidirect-product \( Q \ltimes_{\alpha_s} G \). Hence for this situation, we have

**Proposition 14.6.** If the group extension \( H \) has a section \( s \) which is a homomorphism, then it must be isomorphic to \( Q \ltimes_{\alpha_s} G \). (Of course, by this, the semidirect-product \( Q \ltimes_{\alpha_s} G \) is independent of choices of sections \( s \) whenever they are homomorphisms.)

**Proof.** Consider

\[
\Psi_s : Q \times G \rightarrow H, \quad (q, g) \mapsto s(q)g
\]

Direct checking shows that when \( s \) is a homomorphism, \( \Psi_s \) is a group isomorphism. \( \square \)

If there exists such homomorphic section \( s \), the homomorphism \( \phi : H \rightarrow Q \) is called split. We have shown that, for this case, \( H \) must be a semidirect-product. Conversely, given a semidirect-product \( Q \ltimes_{\alpha} G \), we can construct a group extension

\[
Q \ltimes_{\alpha} G \rightarrow Q,
\]

using the projection

\[
\phi : Q \times G \rightarrow Q, \quad \phi(q, g) = q.
\]

Then the section \( s : Q \rightarrow Q \times G \) defined as

\[
s(q) = (q, e)
\]

is a group homomorphism by direct checking. We summarize it as

**Proposition 14.7.** A surjective group homomorphism \( \phi : H \rightarrow Q \) splits if and only if \( H \) is a semidirect-product of \( Q \) and \( \ker \phi \).

**Remark 14.8.** Notation: We define here \( (q_1, g_1) \ast_{\alpha} (q_2, g_2) = (q_1 q_2, \alpha(q_2)(g_1)g_2) \). So, if follows,

\[
(q, e_G) \ast_{\alpha} (e_Q, g) = (q, g)
\]

but

\[
(e_Q, g) \ast_{\alpha} (q, e_G) = (q, \alpha(q)(g))
\]

which is not the same as \( (q, g) \) in general when \( \alpha \) is not trivial map.

However, if you define the semidirect-product (you can check this defines a group too) as

\[
(q_1, g_1) \ast'_{\alpha} (q_2, g_2) = (q_1 q_2, g_1 \alpha(q_1)(g_2)),
\]

then

\[
(e_Q, g) \ast'_{\alpha} (q, e_G) = (q, g)
\]

which is somehow wired. To resolve it, we can write \( G \times Q \) instead. Hence usually, this way is referred as \( G \ltimes_{\alpha} Q \).
I didn’t use this way, because when we take a section \( s \) and define \( \alpha_s(q) = \text{Ad}_{s(q)} \), you will find, the second convention leads to

\[
\alpha_s : Q \rightarrow \text{Aut}(G)
\]

is homomorphism if and only if \( s(q_1q_2) = s(q_2)s(q_1) \), which is not consistent with the notations we have used for this whole quarter.

When we identify \( S_3 \) with \( \mathbb{Z}_2 \ltimes \mathbb{Z}_3 \), you may take

\[
\tau = (1, 2), \quad \sigma = (1, 2, 3)
\]

for example. Then we map

\[
\tau \mapsto (1, 0) \in \mathbb{Z}_2 \times \mathbb{Z}_3, \quad \sigma \mapsto (0, 1) \in \mathbb{Z}_2 \times \mathbb{Z}_3.
\]

Then by the semidirect-product \( \ast \), we used, there is

\[
\tau \sigma := \sigma \circ \tau \mapsto (1, 0) \ast \sigma (0, 1) = (1, 1)
\]

and

\[
\sigma \tau := \tau \circ \sigma \mapsto (0, 1) \ast \sigma (1, 0) = (1, 2) = (1, -1).
\]