I. GROUPS: BASIC DEFINITIONS AND EXAMPLES

Definition 1:
An operation on a set $G$ is a function $*: G \times G \to G$.

Definition 2:
A group is a set $G$ which is equipped with an operation $*$ and a special element $e \in G$, called the identity, such that

(i) the associative law holds: for every $x, y, z \in G$,
\[
x \ast (y \ast z) = (x \ast y) \ast z;
\]

(ii) $e \ast x = x = x \ast e$ for all $x \in G$;

(iii) for every $x \in G$, there is $x' \in G$ (so-called, inverse) with $x \ast x' = e = x' \ast x$.

Example:

<table>
<thead>
<tr>
<th>Set</th>
<th>Operation “+”</th>
<th>Operation “*”</th>
<th>Additional Condition</th>
</tr>
</thead>
<tbody>
<tr>
<td>$\mathbb{N}$</td>
<td>no</td>
<td>no</td>
<td>—</td>
</tr>
<tr>
<td>$\mathbb{Z}$</td>
<td>yes</td>
<td>no</td>
<td>—</td>
</tr>
<tr>
<td>$\mathbb{Q}$</td>
<td>yes</td>
<td>no</td>
<td>“*” for $\mathbb{Q} \setminus {0}$</td>
</tr>
<tr>
<td>$\mathbb{R}$</td>
<td>yes</td>
<td>no</td>
<td>“*” for $\mathbb{R} \setminus {0}$</td>
</tr>
<tr>
<td>$\mathbb{R} \setminus \mathbb{Q}$</td>
<td>no</td>
<td>no</td>
<td>—</td>
</tr>
</tbody>
</table>

Example:

<table>
<thead>
<tr>
<th>Set</th>
<th>Operation “+”</th>
<th>Operation “*”</th>
</tr>
</thead>
<tbody>
<tr>
<td>$\mathbb{Z}_{&gt;0}$</td>
<td>no</td>
<td>no</td>
</tr>
<tr>
<td>$\mathbb{Z}_{\geq 0}$</td>
<td>no</td>
<td>no</td>
</tr>
<tr>
<td>$\mathbb{Q}_{&gt;0}$</td>
<td>no</td>
<td>yes</td>
</tr>
<tr>
<td>$\mathbb{Q}_{\geq 0}$</td>
<td>no</td>
<td>no</td>
</tr>
<tr>
<td>$\mathbb{R}_{&gt;0}$</td>
<td>no</td>
<td>yes</td>
</tr>
<tr>
<td>$\mathbb{R}_{\geq 0}$</td>
<td>no</td>
<td>no</td>
</tr>
</tbody>
</table>
Example:

<table>
<thead>
<tr>
<th>Set</th>
<th>Operation “+”</th>
<th>Operation “∗”</th>
</tr>
</thead>
<tbody>
<tr>
<td>{2n : n ∈ \mathbb{Z}}</td>
<td>yes</td>
<td>no</td>
</tr>
<tr>
<td>{2n + 1 : n ∈ \mathbb{Z}}</td>
<td>no</td>
<td>no</td>
</tr>
<tr>
<td>{3n : n ∈ \mathbb{Z}}</td>
<td>yes</td>
<td>no</td>
</tr>
<tr>
<td>{kn : n ∈ \mathbb{Z}}, where k ∈ \mathbb{N} is some fixed number</td>
<td>yes</td>
<td>no</td>
</tr>
<tr>
<td>{k^n : n ∈ \mathbb{Z}}, where a ∈ \mathbb{R} is some fixed number</td>
<td>no</td>
<td>yes</td>
</tr>
<tr>
<td>{\frac{p}{2^n} : p ∈ \mathbb{Z}, n ∈ \mathbb{Z}_{≥0}}</td>
<td>yes</td>
<td>no</td>
</tr>
</tbody>
</table>

Example:

<table>
<thead>
<tr>
<th>Set</th>
<th>Operation: $a ∗ b = a^2b^2$</th>
<th>Operation: $a ∗ b = a^b$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$\mathbb{R}_{&gt;0}$</td>
<td>no</td>
<td>no</td>
</tr>
</tbody>
</table>

Definition 3:
A group is called **abelian** if $x ∗ y = y ∗ x$ for any $x, y ∈ G$.

Example:
The parity group $\mathcal{P}$ has two elements, the words “even” and “odd,” with operation

\[
\text{even} \oplus \text{even} = \text{even} = \text{odd} \oplus \text{odd}
\]

and

\[
\text{even} \oplus \text{odd} = \text{odd} = \text{odd} \oplus \text{even}.
\]

It is clear that:
1. “even” is the identity element;
2. The inverse of “even” is “even” and the inverse of “odd” is “odd”.

2
Example:
The group $\mathbb{Z}_2$ has two elements: $[0]$ is the set of all even numbers and $[1]$ is the set of all odd numbers. Operation:

\[ [0] \oplus [0] = [1] \oplus [1] = [0] \]

and

\[ [0] \oplus [1] = [1] \oplus [0] = [1]. \]

It is clear that:

1. $[0]$ is the identity element;
2. The inverse of $[0]$ is $[0]$ and the inverse of $[1]$ is $[1]$.

Example:
The group $\mathbb{Z}_3$ has three elements:

$[0]$ is the set of numbers which are congruent to 0 mod 3;

$[1]$ is the set of numbers which are congruent to 1 mod 3;

$[2]$ is the set of numbers which are congruent to 2 mod 3.

Operation:

\[ [0] \oplus [0] = [1] \oplus [2] = [2] \oplus [1] = [0], \]

\[ [0] \oplus [1] = [1] \oplus [0] = [2] \oplus [2] = [1], \]

and

\[ [0] \oplus [2] = [2] \oplus [0] = [1] \oplus [1] = [2]. \]

It is clear that:

1. $[0]$ is the identity element;

Example:
The group $\mathbb{Z}_3^\times$ has two elements:

$[1]$ is the set of numbers which are congruent to 1 mod 3;

$[2]$ is the set of numbers which are congruent to 2 mod 3.

Operation:

\[ [1] \otimes [1] = [2] \otimes [2] = [1], \]

and


It is clear that:

1. $[1]$ is the identity element;

3
II. THREE EXAMPLES OF SPECIAL GROUPS

**Definition 4:**
The family of all the permutations of the set $X = \{1, 2, \ldots, n\}$ is called the symmetric group. It is denoted by $S_n$.

**Theorem 1:**
$S_n$ is a nonabelian group under operation of composition.

**Proof (Sketch):** It is obvious that $S_n$ is closed under operation of composition. One can show that this operation is associative. The identity element is $(1)$. Finally, we know that every permutation $\alpha$ is either a cycle or a product of disjoint (with no common elements) cycles and the inverse of the cycle $\alpha = (i_1i_2\ldots i_r)$ is the cycle $\alpha^{-1} = (i_ri_{r-1}\ldots i_1)$. Therefore, every element of $S_n$ is invertible. To show that $S_n$ is nonabelian, we note that, for example, $(123)(13) \neq (13)(123)$. ■

**Definition 5:**
The set of the following four permutations
\[ V = \{(1), (12)(34), (13)(24), (14)(23)\} \]
is called the four-group.

**Definition 6:**
The set of all $2 \times 2$ nonsingular (determinant is nonzero) matrices with real entries and with operation matrix multiplication is called the general linear group. It is denoted by $GL(2, \mathbb{R})$.

**Theorem 2:**
$GL(2, \mathbb{R})$ is a nonabelian group.

**Proof (Sketch):** It is obvious that $GL(2, \mathbb{R})$ is closed under operation of multiplication. One can show that this operation is associative. The identity element is
\[
\begin{bmatrix}
1 & 0 \\
0 & 1
\end{bmatrix}.
\]
Finally, for every element $A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$ there exists the inverse
\[
A^{-1} = \frac{1}{ad-bc} \begin{bmatrix} d & -b \\ -c & a \end{bmatrix}.
\]
To show that $GL(2, \mathbb{R})$ is nonabelian, we note that, for example,
\[
\begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix} \neq \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}.
\] ■
III. MAIN THEOREM ABOUT GROUPS

**Theorem 3:**
Let $G$ be a group.

(i) If $x \ast a = x \ast b$ or $a \ast x = b \ast x$, then $a = b$.

(ii) The identity element $e$ is unique.

(iii) For all $x \in G$, the inverse element $x^{-1}$ is unique.

(iv) For all $x \in G$ we have $(x^{-1})^{-1} = x$.

(v) For all $a, b \in G$ we have $(a \ast b)^{-1} = b^{-1} \ast a^{-1}$.

**Proof:**

(i) Let $x \ast a = x \ast b$, then

$$x^{-1} \ast (x \ast a) = x^{-1} \ast (x \ast b),$$

therefore by the associative law we get

$$\left( x^{-1} \ast x \right) \ast a = \left( x^{-1} \ast x \right) \ast b,$$

so

$$e \ast a = e \ast b,$$

and the result follows. In the same way one can deduce $a = b$ from $a \ast x = b \ast x$.

(ii) Assume to the contrary that there are two identity elements $e_1$ and $e_2$. Then

$$e_1 = e_1 \ast e_2 = e_2,$$

which is a contradiction.

(iii) Assume to the contrary that for some $x \in G$ there are two inverse elements $x_1^{-1}$ and $x_2^{-1}$. Then

$$x_2^{-1} = e \ast x_2^{-1} = (x_1^{-1} \ast x) \ast x_2^{-1} = x_1^{-1} \ast (x \ast x_2^{-1}) = x_1^{-1} \ast e = x_1^{-1},$$

which is a contradiction.

(iv) We have

$$(x^{-1})^{-1} \ast x^{-1} = e.$$

Multiplying both sides by $x$, we get

$$(x^{-1})^{-1} \ast (x^{-1} \ast x) = e \ast x,$$

hence

$$\left( x^{-1} \right)^{-1} \ast e = x,$$

and the result follows.

(v) We have

$$(a \ast b) \ast (b^{-1} \ast a^{-1}) = [a \ast (b \ast b^{-1})] \ast a^{-1} = (a \ast e) \ast a^{-1} = a \ast a^{-1} = e,$$

and the result follows.
IV. SUBGROUPS: BASIC DEFINITIONS AND EXAMPLES

Definition 7:
A subset $H$ of a group $G$ is a subgroup if
(i) $e \in H$;
(ii) if $x, y \in H$, then $x \ast y \in H$;
(iii) if $x \in H$, then $x^{-1} \in H$.

Notation:
If $H$ is a subgroup of $G$, we write $H \leq G$.

Example:
It is obvious that $\{e\}$ and $G$ are always subgroups of a group $G$.

Definition 8:
We call a subgroup $H$ proper, and we write $H < G$, if $H \neq G$. We call a subgroup $H$ of $G$ nontrivial if $H \neq \{e\}$.

Example:

1. $\mathbb{Z}^+ < \mathbb{Q}^+ < \mathbb{R}^+$.
2. $\mathbb{Q}_{\neq 0}^x < \mathbb{R}_{\neq 0}^x$.
3. $\mathbb{Q}_{>0}^x < \mathbb{R}_{>0}^x < \mathbb{R}_{\neq 0}^x$.
4. A group of even numbers is a subgroup of $\mathbb{Z}^+$.
5. $V < S_4$. 
V. TWO THEOREMS ABOUT SUBGROUPS

Theorem 4:
A subset \( H \) of a group \( G \) is a subgroup \( \iff \) \( H \) is nonempty and, whenever \( x, y \in H \), then \( xy^{-1} \in H \).

**Proof:**

\( \Rightarrow \): Suppose \( H \) is a subgroup of \( G \). We should prove that \( H \) is nonempty and, whenever \( x, y \in H \), then \( xy^{-1} \in H \). We first note that \( H \) is nonempty, because \( 1 \in H \) by part (i) of definition 7. Finally, if \( x, y \in H \), then \( y^{-1} \in H \) by part (iii) of definition 7, and so \( xy^{-1} \in H \), by part (ii) of definition 7.

\( \Leftarrow \): Suppose \( H \) is a nonempty subset of \( G \) and, whenever \( x, y \in H \), then \( xy^{-1} \in H \). We should prove that \( H \) is a subgroup of \( G \).

Since \( H \) is nonempty, it contains some element, say, \( h \). Taking \( x = h = y \), we see that

\[ 1 = hh^{-1} \in H, \]

and so part (i) of definition 7 holds. If \( y \in H \), then set \( x = 1 \) (which we can do because \( 1 \in H \)), giving

\[ y^{-1} = 1y^{-1} \in H, \]

and so part (iii) holds. Finally, we know that \( (y^{-1})^{-1} = y \), by (iv) of Theorem 3. Hence, if \( x, y \in H \), then \( y^{-1} \in H \), and so

\[ xy = x(y^{-1})^{-1} \in H. \]

Therefore, \( H \) is a subgroup of \( G \). \( \blacksquare \)

Theorem 5:
A nonempty subset \( H \) of a finite group \( G \) is a subgroup \( \iff \) \( H \) is closed.

**Proof:**

\( \Rightarrow \): Suppose \( H \) is a subgroup of \( G \). Then it is closed by part (ii) of definition 7.

\( \Leftarrow \): Suppose \( H \) is a nonempty closed subset of a finite group \( G \). We should prove that \( H \) is a subgroup. We first note that since \( H \) is closed, it follows that part (ii) of definition 7 holds. This, in particular means, that \( H \) contains all the powers of its elements. Let us pick some element \( a \in H \) (we can do that, since \( H \) is nonempty). Then \( a^n \in H \) for all integers \( n \geq 1 \).

**Lemma:**
If \( G \) is a finite group and \( a \in G \), then \( a^k = 1 \) for some integers \( k \geq 1 \).

**Proof:** Consider the subset \( \{1, a, a^2, \ldots, a^n, \ldots\} \). Since \( G \) is finite, there must be a repetition occurring on this infinite list. So, there are integers \( m > n \) with \( a^m = a^n \), hence \( 1 = a^m a^{-n} = a^{m-n} \). So, we have shown that there is some positive power of \( a \) equal to \( 1 \).

By this Lemma for any \( a \in G \) there is an integer \( m \) with \( a^m = 1 \), hence \( 1 \in H \) and part (i) of definition 7 holds. Finally, if \( h \in H \) and \( h^m = 1 \), then \( h^{-1} = h^{m-1} \) (for \( hh^{m-1} = 1 = h^{m-1}h \)), so that \( h^{-1} \in H \) and part (iii) of definition 7 holds. Therefore, \( H \) is a subgroup of \( G \). \( \blacksquare \)
VI. CYCLIC GROUPS

Definition 9:
If $G$ is a group and $a \in G$, write

$$\langle a \rangle = \{a^n : n \in \mathbb{Z}\} = \text{all powers of } a;$$

$\langle a \rangle$ is called the cyclic subgroup of $G$ generated by $a$.

Example: $G = \{0, \pm 1, \pm 2, \pm 3, \ldots\}$, $H = \{0, \pm 2, \pm 4, \pm 6, \ldots\} = \langle 2 \rangle$.

Definition 10:
A group $G$ is called cyclic if $G = \langle a \rangle$. In this case $a$ is called a generator of $G$.

Example:
(a) $\{e\} = \langle e \rangle$
(b) $\mathbb{Z}^+ = \{0, \pm 1, \pm 2, \pm 3, \ldots\} = \langle 1 \rangle$
(c) $\mathbb{Q}^+, \mathbb{Q}_{>0}^\times, \mathbb{R}^+, \mathbb{R}_{>0}^\times$ are not cyclic
(d) $S_2 = \{(1), (12)\} = \langle (12) \rangle \neq \langle (1) \rangle$
(e) $S_m, m > 2$, is not cyclic
(f) $\mathbb{Z}_m^+ = \{[0], [1], [2], \ldots, [m-1]\} = \langle [1] \rangle$
(g) $\mathbb{Z}_5^\times = \{[1], [2]\} = \langle [2] \rangle \neq \langle [1] \rangle$
(h) $\mathbb{Z}_5^\times = \{[1], [2], [3], [4]\} = \langle [2] \rangle = \langle [3] \rangle \neq \langle [1] \rangle, \langle [4] \rangle$
(i) $\mathbb{Z}_7^\times = \{[1], [2], \ldots, [6]\} = \langle [3] \rangle = \langle [5] \rangle \neq \langle [1] \rangle, \langle [2] \rangle, \langle [4] \rangle, \langle [6] \rangle$
(j) $\mathbb{Z}_m^\times$ is cyclic $\iff m$ is a prime (Lagrange, 1769)

Remark:
Recall, that if $m$ is composite, $\mathbb{Z}_m^\times$ is not a group.
VII. ORDER

Definition 11:
Let $G$ be a group and let $a \in G$. If $a^k = 1$ for some $k \geq 1$, then the smallest such exponent $k \geq 1$ is called the order of $a$; if no such power exists, then one says that $a$ has infinite order.

Example:
(a) Let $G = S_2 = \{(1), (12)\}$, then the order of $(1)$ is 1 and the order of $(12)$ is 2
(b) Let $G = \mathbb{Z}_4^+ = \{0, [1], [2], [3]\}$, then the order of $[0]$ is 1, order of $[1]$ is 4, order of $[2]$ is 2, order of $[3]$ is 4.

Definition 12:
If $G$ is a finite group, then the number of elements in $G$, denoted by $|G|$, is called the order of $G$.

Example: $|S_n| = n!$, $|\mathbb{Z}_n^+| = n$, $|\mathbb{Z}_p^x| = p - 1$.

Theorem 6:
Let $G$ be a finite group and let $a \in G$. Then the order of $a$ is $|\langle a \rangle|$.

Proof:
Part I: We first prove that if $|\langle a \rangle| = k$, then the order of $a$ is $k$. In fact, the sequence

$$1, a, a^2, \ldots, a^{k-1}$$

has $k$ distinct elements, while

$$1, a, a^2, \ldots, a^{k-1}, a^k$$

has a repetition. Hence,

$$a^k \in \{1, a, a^2, \ldots, a^{k-1}\},$$

that is, $a^k = a^i$ for some $i$ with $0 \leq i < k$. If $i \geq 1$, then $a^{k-i} = 1$, contradicting the original list having no repetitions. Therefore $i = 1$, so $a^k = a^0 = 1$, and $k$ is the order of $a$ (being smallest positive such $k$).

Part II: We now prove that if the order of $a$ is $k$, then $|\langle a \rangle| = k$. If

$$H = \{1, a, a^2, \ldots, a^{k-1}\},$$

then $|H| = k$; It suffices to show that $H = \langle a \rangle$. Clearly, $H \subseteq \langle a \rangle$. For the reverse inclusion, take $a^i \in \langle a \rangle$. By the division algorithm,

$$i = qk + r, \quad \text{where} \quad 0 \leq r < k.$$

Hence

$$a^i = a^{qk+r} = a^{qk}a^r = (a^k)^q a^r = a^r \in H;$$

this gives $\langle a \rangle \subseteq H$, and so $\langle a \rangle = H$. ■

Theorem 7:
Let $G$ be a group and let $a \in G$ has finite order $k$. If $a^n = 1$, then $k \mid n$. 

9
VIII. LAGRANGE’S THEOREM

Definition 13:
If \( H \) is a subgroup of a group \( G \) and \( a \in G \), then the coset \( aH \) is the following subset of \( G \):
\[
aH = \{ah : h \in H\}.
\]

Remark:
Cosets are usually not subgroups. In fact, if \( a \notin H \), then \( 1 \notin aH \), for otherwise
\[
1 = ah \implies a = h^{-1} \notin H,
\]
which is a contradiction.

Example:
Let \( G = S_3 \) and \( H = \{(1), (12)\} \). Then there are 3 cosets:
\[
(12)H = \{(1), (12)\} = H,
\]
\[
(13)H = \{(13), (123)\} = (123)H,
\]
\[
(23)H = \{(23), (132)\} = (132)H.
\]

Lemma:
Let \( H \) be a subgroup of a group \( G \), and let \( a, b \in G \). Then

(i) \( aH = bH \iff b^{-1}a \in H \).

(ii) If \( aH \cap bH \neq \emptyset \), then \( aH = bH \).

(iii) \( |aH| = |H| \) for all \( a \in G \).

Proof:
(i) \( \Rightarrow \) Let \( aH = bH \), then for any \( h_1 \in H \) there is \( h_2 \in H \) with \( ah_1 = bh_2 \). This gives
\[
b^{-1}a = h_2h_1^{-1} \implies b^{-1}a \in H,
\]
since \( h_2 \in H \) and \( h_1^{-1} \in H \).

\( \Leftarrow \) Let \( b^{-1}a \in H \). Put \( b^{-1}a = h_0 \). Then
\[
aH \subseteq bH, \text{ since if } x \in aH, \text{ then } x = ah \implies x = b(b^{-1}a)h = b h_0 h = bh_1 \in bH;
\]
\[
bH \subseteq aH, \text{ since if } x \in bH, \text{ then } x = bh \implies x = a(b^{-1}a)^{-1}h = a h_0^{-1} h = ah_2 \in aH.
\]
So, \( aH \subseteq bH \) and \( bH \subseteq aH \), which gives \( aH = bH \).
(ii) Let \( aH \cap bH \neq \emptyset \), then there exists an element \( x \) with
\[
x \in aH \cap bH \implies ah_1 = x = bh_2 \implies b^{-1}a = h_2h_1^{-1} \in H,
\]
therefore \( aH = bH \) by (i).

(iii) Note that if \( h_1 \) and \( h_2 \) are two distinct elements from \( H \), then \( ah_1 \) and \( ah_2 \) are also distinct, since otherwise
\[
ah_1 = ah_2 \implies a^{-1}ah_1 = a^{-1}ah_2 \implies h_1 = h_2,
\]
which is a contradiction. So, if we multiply all elements of \( H \) by \( a \), we obtain the same number of elements, which means that \( |aH| = |H| \). ■

**Theorem 8 (Lagrange):**

If \( H \) is a subgroup of a finite group \( G \), then

\[
|H| \text{ divides } |G|.
\]

**Proof:**

Let \( |G| = t \) and
\[
\{a_1H, a_2H, \ldots, a_tH\}
\]
be the family of all cosets of \( H \) in \( G \). Then
\[
G = a_1H \cup a_2H \cup \ldots \cup a_tH,
\]
because \( G = \{a_1, a_2, \ldots, a_t\} \) and \( 1 \in H \). By (ii) of the Lemma above for any two cosets \( a_iH \) and \( a_jH \) we have only two possibilities:
\[
a_iH \cap a_jH = \emptyset \quad \text{or} \quad a_iH = a_jH.
\]
Moreover, from (iii) of the Lemma above it follows that all cosets have exactly \( |H| \) number of elements. Therefore
\[
|G| = |H| + |H| + \ldots + |H| \implies |G| = d|H|,
\]
and the result follows. ■

**Corollary 1:**

If \( G \) is a finite group and \( a \in G \), then the order of \( a \) is a divisor of \( |G| \).

**Proof:**

By Theorem 6, the order of the element \( a \) is equal to the order of the subgroup \( H = \langle a \rangle \). By Lagrange's Theorem, \( |H| \) divides \( |G| \), therefore the order \( a \) divides \( |G| \). ■

**Corollary 2:**

If a finite group \( G \) has order \( m \), then \( a^m = 1 \) for all \( a \in G \).

**Proof:**

Let \( d \) be the order of \( a \). By Corollary 1, \( d \mid m \); that is, \( m = dk \) for some integer \( k \). Thus,
\[
a^m = a^{dk} = (a^d)^k = 1. ■
\]
Corollary 3:
If $p$ is a prime, then every group $G$ of order $p$ is cyclic.

Proof:
Choose $a \in G$ with $a \neq 1$, and let $H = \langle a \rangle$ be the cyclic subgroup generated by $a$. By Lagrange’s Theorem, $|H|$ is a divisor of $|G| = p$. Since $p$ is a prime and $|H| > 1$, it follows that

$$|H| = p = |G|,$$

and so $H = G$, as desired. ■

Theorem 9 (Fermat’s Little Theorem):
Let $p$ be a prime. Then $n^p \equiv n \mod p$ for any integer $n \geq 1$.

Proof: We distinguish two cases.

Case A: Let $p \mid n$, then, obviously, $p \mid n^p - n$, and we are done.

Case B: Let $p \nmid n$.

Consider the group $\mathbb{Z}_p^\times$ and pick any $[a] \in \mathbb{Z}_p^\times$. Let $k$ be the order of $[a]$. We know that $\langle [a] \rangle$ is a subgroup of $\mathbb{Z}_p^\times$ and by Theorem 6 we obtain

$$|\langle [a] \rangle| = k.$$

By Lagrange’s Theorem we get

$$|\langle [a] \rangle| \text{ divides } |\mathbb{Z}_p^\times|,$$

which gives

$$k \mid p - 1,$$

since $|\langle [a] \rangle| = k$ and $|\mathbb{Z}_p^\times| = p - 1$. So

$$p - 1 = kd$$

for some integer $d$. On the other hand, since $k$ is the order of $[a]$, it follows that for any $n \in [a]$ we have

$$n^k \equiv 1 \mod p,$$

hence

$$n^{kd} \equiv 1^d \equiv 1 \mod p,$$

and the result follows, since $kd = p - 1$. ■
IX. HOMOMORPHISMS AND ISOMORPHISMS

**Definition 14:**
If \((G, \ast)\) and \((H, \circ)\) are groups, then a function \(f : G \rightarrow H\) is a homomorphism if
\[
f(x \ast y) = f(x) \circ f(y)
\]
for all \(x, y \in G\).

**Example:**
Let \((G, \ast)\) be an arbitrary group and \(H = \{e\}\), then the function \(f : G \rightarrow H\) such that
\[
f(x) = e \quad \text{for any} \quad x \in G
\]
is a homomorphism. In fact,
\[
f(x \ast y) = e = e \circ e = f(x) \circ f(y).
\]

**Example:**
Let \((G, \ast)\) be an arbitrary group, then the function \(f : G \rightarrow G\) such that
\[
f(x) = x \quad \text{for any} \quad x \in G
\]
is a homomorphism. In fact,
\[
f(x \ast y) = x \ast y = f(x) \ast f(y).
\]

**Example:**
Let \(f : \mathbb{Z}_2^+ \rightarrow \mathbb{Z}_2^+\) be a function such that \(f(x) = \begin{cases} 0 & \text{if } x \text{ is even} \\ 1 & \text{if } x \text{ is odd} \end{cases}\). Then \(f\) is a homomorphism. In fact, if \(x + y\) is even, then
\[
f(x + y) = 0 = f(x) + f(y).
\]
Similarly, if \(x + y\) is odd, then
\[
f(x + y) = 1 = f(x) + f(y).
\]

**Example:**
Let \(f : GL(2, \mathbb{R}) \rightarrow \mathbb{R}^\times_{\neq 0}\) be a function such that
\[
f(M) = \det M \quad \text{for any} \quad M \in GL(2, \mathbb{R}).
\]
Then \(f\) is a homomorphism. In fact,
\[
f(M_1M_2) = \det(M_1M_2) = \det(M_1)\det(M_2) = f(M_1)f(M_2).
\]
Definition 15:
Let a function \( f : G \rightarrow H \) be a homomorphism. If \( f \) is also a one-one correspondence, then \( f \) is called an isomorphism. Two groups \( G \) and \( H \) are called isomorphic, denoted by

\[ G \cong H, \]

if there exists an isomorphism between them.

Example:
We show that \( \mathbb{R}^+ \cong \mathbb{R}_{>0}^\times \). In fact, let

\[ f(x) = e^x. \]

To prove that this is an isomorphism, we should check that

\[ f : \mathbb{R}^+ \rightarrow \mathbb{R}_{>0}^\times \]

is one-one correspondence and that

\[ f(x + y) = f(x)f(y) \]

for all \( x, y \in \mathbb{R} \). The first part is trivial, since \( f(x) = e^x \) is defined for all \( x \in \mathbb{R} \) and its inverse \( g(x) = \ln x \) is also defined for all \( x \in \mathbb{R}_{>0} \). The second part is also true, since

\[ f(x + y) = e^{x+y} = e^xe^y = f(x)f(y). \]

Definition 16:
Let \( G = \{a_1, a_2, \ldots, a_n\} \) be a finite group. A multiplication table for \( G \) is an \( n \times n \) matrix whose \( i,j \) entry is \( a_ia_j \):

<table>
<thead>
<tr>
<th>( G )</th>
<th>( a_1 )</th>
<th>( a_2 )</th>
<th>( \ldots )</th>
<th>( a_j )</th>
<th>( \ldots )</th>
<th>( a_n )</th>
</tr>
</thead>
<tbody>
<tr>
<td>( a_1 )</td>
<td>( a_1a_2 )</td>
<td>( a_1a_2 )</td>
<td>( \ldots )</td>
<td>( a_1a_j )</td>
<td>( \ldots )</td>
<td>( a_1a_n )</td>
</tr>
<tr>
<td>( a_2 )</td>
<td>( a_2a_1 )</td>
<td>( a_2a_2 )</td>
<td>( \ldots )</td>
<td>( a_2a_j )</td>
<td>( \ldots )</td>
<td>( a_2a_n )</td>
</tr>
<tr>
<td>( \vdots )</td>
<td>( \vdots )</td>
<td>( \vdots )</td>
<td>( \ldots )</td>
<td>( \vdots )</td>
<td>( \ldots )</td>
<td>( \vdots )</td>
</tr>
<tr>
<td>( a_i )</td>
<td>( a_ia_1 )</td>
<td>( a_ia_2 )</td>
<td>( \ldots )</td>
<td>( a_ia_j )</td>
<td>( \ldots )</td>
<td>( a_ia_n )</td>
</tr>
<tr>
<td>( \vdots )</td>
<td>( \vdots )</td>
<td>( \vdots )</td>
<td>( \ldots )</td>
<td>( \vdots )</td>
<td>( \ldots )</td>
<td>( \vdots )</td>
</tr>
<tr>
<td>( a_n )</td>
<td>( a_na_1 )</td>
<td>( a_na_2 )</td>
<td>( \ldots )</td>
<td>( a_na_j )</td>
<td>( \ldots )</td>
<td>( a_na_n )</td>
</tr>
</tbody>
</table>

We will also agree that \( a_1 = 1 \).
Example:

Multiplicative table for $Z_5^\times$ is

\[
\begin{array}{c|cccc}
Z_5^\times & 1 & 2 & 3 & 4 \\
\hline
1 & 1 & 2 & 3 & 4 \\
2 & 2 & 4 & 1 & 3 \\
3 & 3 & 1 & 4 & 2 \\
4 & 4 & 3 & 2 & 1 \\
\end{array}
\]

Remark:

It is clear that two groups $G = \{a_1, a_2, \ldots, a_n\}$ and $H = \{b_1, b_2, \ldots, b_n\}$ of the same order $n$ are isomorphic if and only if it is possible to match elements $a_1, a_2, \ldots, a_n$ with elements $b_1, b_2, \ldots, b_n$ such that this one-one correspondence remains also for corresponding entries $a_ia_j$ and $b_ib_j$ of their multiplication tables.

Example:

1. The multiplication tables below show that $\mathcal{P} \cong Z_2^+ \cong Z_3^x$:

\[
\begin{array}{c|cc}
\mathcal{P} & \text{“even”} & \text{“odd”} \\
\hline
\text{“even”} & \text{“even”} & \text{“odd”} \\
\text{“odd”} & \text{“odd”} & \text{“even”} \\
\end{array}
\begin{array}{c|c|c}
Z_2^+ & 0 & 1 \\
\hline
0 & 0 & 1 \\
1 & 1 & 0 \\
\end{array}
\begin{array}{c|c|c}
Z_3^x & 1 & 2 \\
\hline
1 & 1 & 2 \\
2 & 2 & 1 \\
\end{array}
\]

2. The multiplication tables below show that $Z_4^+ \cong Z_6^\times$:

\[
\begin{array}{c|cccc}
Z_4^+ & 0 & 1 & 2 & 3 \\
\hline
0 & 0 & 1 & 2 & 3 \\
1 & 1 & 2 & 3 & 0 \\
2 & 2 & 3 & 0 & 1 \\
3 & 3 & 0 & 1 & 2 \\
\end{array}
\begin{array}{c|cccc}
Z_6^\times & 1 & 2 & 3 & 4 \\
\hline
1 & 1 & 2 & 3 & 4 \\
2 & 2 & 3 & 4 & 1 \\
3 & 3 & 1 & 2 & 4 \\
\end{array}
\]

3. The multiplication tables below show that $Z_6^+ \cong Z_7^\times$:

\[
\begin{array}{c|cccccc}
Z_6^+ & 0 & 1 & 2 & 3 & 4 & 5 \\
\hline
0 & 0 & 1 & 2 & 3 & 4 & 5 \\
1 & 1 & 2 & 3 & 4 & 5 & 0 \\
2 & 2 & 3 & 4 & 5 & 0 & 1 \\
3 & 3 & 4 & 5 & 0 & 1 & 2 \\
4 & 4 & 5 & 0 & 1 & 2 & 3 \\
5 & 5 & 0 & 1 & 2 & 3 & 4 \\
\end{array}
\begin{array}{c|cccccc}
Z_7^\times & 1 & 2 & 3 & 4 & 5 & 6 \\
\hline
1 & 1 & 3 & 2 & 6 & 4 & 5 \\
2 & 2 & 6 & 4 & 5 & 1 & 3 \\
3 & 3 & 2 & 6 & 4 & 5 & 1 \\
4 & 4 & 5 & 1 & 3 & 2 & 6 \\
5 & 5 & 1 & 3 & 2 & 6 & 4 \\
\end{array}
\]
Theorem 10:
Let \( f : G \rightarrow H \) is a homomorphism of groups. Then

(i) \( f(e) = e \);
(ii) \( f(x^{-1}) = f(x)^{-1} \);
(iii) \( f(x^n) = [f(x)]^n \) for all \( n \in \mathbb{Z} \).

Proof:

(i) We have
\[
e \cdot e = e \implies f(e \cdot e) = f(e) \implies f(e)f(e) = f(e).
\]
Multiplying both sides by \([f(e)]^{-1}\), we get
\[
[f(e)]^{-1}f(e)f(e) = [f(e)]^{-1}f(e) \implies e \cdot f(e) = e \implies f(e) = e.
\]

(ii) We have
\[
x \cdot x^{-1} = e \implies f(x \cdot x^{-1}) = f(e) \implies f(x)f(x^{-1}) = f(e).
\]
Since \( f(e) = e \) by (i), we get
\[
f(x)f(x^{-1}) = e.
\]
Similarly, from \( x^{-1} \cdot x = e \) one can deduce that \( f(x^{-1})f(x) = e \). So,
\[
f(x)f(x^{-1}) = f(x^{-1})f(x) = e,
\]
which means that \( f(x^{-1}) = f(x)^{-1} \).

(iii) If \( n \geq 1 \), one can prove \( f(x^n) = [f(x)]^n \) by induction. If \( n < 0 \), then
\[
f(x^n) = f((x^{-1})^{-n}) = [f(x^{-1})]^{-n},
\]
which is equal to \( [f(x)]^n \) by (ii). \( \blacksquare \)

Theorem 11:
Any two cyclic groups \( G \) and \( H \) of the same order are isomorphic.

Proof (Sketch):
Suppose that \( G = \langle a \rangle = \{1, a, a^2, \ldots, a^{m-1}\} \) and \( H = \langle b \rangle = \{1, b, b^2, \ldots, b^{m-1}\} \). Then
\[
f : G \rightarrow H
\]
with
\[
f(a^i) = b^i, \quad 0 \leq i \leq m - 1,
\]
is an isomorphism and \( G \cong H \). \( \blacksquare \).
Example:
We know that any group of the prime order is cyclic. Therefore by Theorem 11 any two groups of the same prime order are isomorphic.

Example:
Let $p$ be a prime number. We know that the group $\mathbb{Z}_{p-1}^+$ is cyclic, since

$$\mathbb{Z}_{p-1}^+ = \langle [1] \rangle.$$ 

It is possible to prove that $\mathbb{Z}_p^\times$ is also cyclic. Also,

$$|\mathbb{Z}_{p-1}^+| = |\mathbb{Z}_p^\times| = p - 1.$$

Therefore from Theorem 11 it follows that $\mathbb{Z}_{p-1}^+ \cong \mathbb{Z}_p^\times$.

Problem: Show that $V \not\cong \mathbb{Z}_4^+$.

Solution:
Assume to the contrary that $V \cong \mathbb{Z}_4^+$. Then there is a one-one correspondence $f : V \to \mathbb{Z}_4^+$. From this, in particular, follows that there exists $x \in V$ such that

$$f(x) = [1].$$

This and (iii) of Theorem 10 give

$$f(x^2) = [f(x)]^2 = [1]^2 = [1] + [1] = [2].$$

We now recall that for any element $x \in V$ we have

$$x^2 = e.$$

By this and (i) of Theorem 10 we get

$$f(x^2) = f(e) = e = [0].$$

This is a contradiction. ■

Remark:
One can show that any group of order 4 is isomorphic to either $\mathbb{Z}_4^+$ or $V$. 


X. KERNEL

**Definition 17:**
If $f : G \rightarrow H$ is a homomorphism, define

$$\ker f = \{x \in G : f(x) = 1\}.$$  

**Theorem 12:**
Let $f : G \rightarrow H$ be a homomorphism. Then $\ker f$ is a subgroup of $G$.

**Proof 1:**
From (i) of Theorem 10 it follows that $1 \in \ker f$, since $f(1) = 1$. Next, if $x, y \in \ker f$, then

$$f(x) = 1 = f(y),$$

hence

$$f(xy) = f(x)f(y) = 1 \cdot 1 = 1,$$

so $xy \in \ker f$. Finally, if $x \in \ker f$, then $f(x) = 1$ and so

$$f(x^{-1}) = [f(x)]^{-1} = 1^{-1} = 1,$$

hence $x^{-1} \in \ker f$. Therefore $\ker f$ is a subgroup of $G$. ■

**Proof 2:**
From (i) of Theorem 10 it follows that $1 \in \ker f$, since $f(1) = 1$. Therefore $\ker G$ is a nonempty set. Next, by the definition of a homomorphism and Theorem 10 we have

$$f(xy^{-1}) = f(x)f(y^{-1}) = f(x)[f(y)]^{-1} = 1 \cdot 1^{-1} = 1$$

for any $x, y \in \ker f$. This means that if $x, y \in \ker f$, then $xy^{-1} \in \ker f$. This gives the desired result thanks to Theorem 4. ■