ON THE RELATIONSHIP BETWEEN SETS AND GROUPS

ROSE DONG

Abstract. This paper is an introduction to basic properties of sets and groups. After introducing the notion of cardinal arithmetic, it proves the Schroeder-Bernstein Theorem about cardinal equivalence. The paper then focuses on how sets and groups exhibit the properties of each other, specifically, the cardinal relations between groups and the group structures within sets.

Contents

1. Introduction 1
2. Cardinal Arithmetic 1
3. Schroeder-Bernstein Theorem 4
4. Lagrange’s Theorem 6
5. Cyclic Groups 7
6. Understanding Sets within Group Structures 8
Acknowledgments 10
References 10

1. Introduction

The exploration of uncountable sets dates back to the nineteenth century, when Georg Cantor proved the existence of infinite sets that cannot be put into one-to-one correspondence with the set of natural numbers. Through the diagonal argument, Cantor showed that there is no bijection between the sets of real and natural numbers. Stemmed from this discovery, the notion of cardinality helped mathematicians understand more about sets that seem not as approachable.

Groups are a particular kind of sets equipped with a binary operation, which satisfies the four group axioms of closure, associativity, identity and invertibility. Since groups are still sets, anything about sets still holds true in groups. However, due to their specific properties, there is more accessible information about groups themselves.

2. Cardinal Arithmetic

Cardinal numbers measure the cardinality, or size of sets. In terms of bijective functions, it defines an equivalence relation between sets.

Definition 2.1. Two sets $A$ and $B$ are of the same cardinality if there exists a bijection $f : A \rightarrow B$ between $A$ and $B$. 
Definition 2.2. A cardinal number is thought of as an equivalence class of cardinality, i.e. \( \text{card}(A) = \text{card}(B) \) if \( A \) and \( B \) are of the same cardinality.

Definition 2.3. Let \( a, b \) be cardinal numbers. If there exist sets \( A, B \) with \( \text{card}(A) = a \), \( \text{card}(B) = b \) and \( A \subseteq B \), then \( a \leq b \).

Definition 2.4. Let \( a, b \) be cardinal numbers. If \( A, B \) are sets with \( \text{card}(A) = a \), \( \text{card}(B) = b \) and \( A \cap B = \emptyset \), then \( a + b = \text{card}(A \cup B) \).

Definition 2.5. Let \( a, b \) be cardinal numbers. If \( A, B \) are sets with \( \text{card}(A) = a \) and \( \text{card}(B) = b \), then \( a \cdot b = \text{card}(A \times B) \).

Definition 2.6. \( \aleph_0 = \text{card}(\mathbb{N}) \).

Theorem 2.7. For any infinite cardinal number \( a, \aleph_0 \leq a \).

Proof. Let \( A \) be an infinite set with \( \text{card}(A) = a \), and \( F_0 \subset F_1 \subset F_2 \subset \ldots \) be a sequence of subsets of \( A \) with \( |F_i| = i \). Let \( x_i \in F_i \setminus F_{i-1} \). Then \( x_1, x_2, \ldots \in A \) with \( x_i \neq x_j \) for any \( i \neq j \), \( \{x_i \mid i \in \mathbb{N}\} \subseteq A \), \( \text{card}(\{x_i \mid i \in \mathbb{N}\}) \leq \text{card}(A) \), \( \aleph_0 \leq a \). □

An important lemma in set theory is Zorn’s Lemma, which identifies the existence of a maximal element within any partially ordered set that is bounded above.

Definition 2.8. A partially ordered set is a set \( P \) with a binary relation \( \leq \) such that, for all \( a, b, c \in P \):

1. (Reflexivity) \( a \leq a \).
2. (Antisymmetry) If \( a \leq b \) and \( b \leq a \), then \( a = b \).
3. (Transitivity) If \( a \leq b \) and \( b \leq c \), then \( a \leq c \).

Lemma 2.9. (Zorn’s Lemma) Suppose a partially ordered set \( P \) has the property that every chain in \( P \) has an upper bound in \( P \). Then the set \( P \) contains at least one maximal element.

Theorem 2.10. Let \( a \) be an infinite cardinal number. Then \( a + a = a \).

Proof. Following the proof of Z. Nagy, let \( A \) be an infinite set with \( \text{card}(A) = a \).

Let \( S(A) \) be the set of families \( \{A_i \mid i \in I\} \) of subsets of \( A \) with

1. \( \text{card}(A_i) = \aleph_0 \) for all \( i \in I \);
2. \( A_i \cap A_j = \emptyset \) for all \( i, j \in I \).

\( S(A) \) with set inclusion is a partially ordered set. For any \( S \in S(A), S \subseteq S \). If \( S_1, S_2 \subseteq S(A), S_1 \subseteq S_2 \) and \( S_2 \subseteq S_1 \), then \( S_1 = S_2 \). If \( S_1, S_2, S_3 \in S(A), S_1 \subseteq S_2 \) and \( S_2 \subseteq S_3 \), then \( S_1 \subseteq S_3 \).

Since \( S(A) \) with set inclusion is a partially ordered set and every chain in \( S(A) \) is bounded above by \( \{A_i \mid A_i \subseteq A, \text{card}(A_i) = \aleph_0\} \), \( S(A) \) contains a maximal element \( \{A_i \mid i \in I_0\} \).

Let \( B = A \setminus (\bigcup_{i \in I_0} A_i) \). Since \( \{A_i\} \) is maximal, \( B \) is finite, \( \text{card}(A) = \text{card}(\bigcup_{i \in I_0} A_i) \). Then \( a = \text{card}(A) = \text{card}(\mathbb{N} \times I_0) \). Suppose \( \text{card}(I_0) = c \). Then \( a = \aleph_0 \cdot c \).

Let \( C_0 = \{n \in \mathbb{N} \mid n \text{ even}\}, C_1 = \{n \in \mathbb{N} \mid n \text{ odd}\} \). Since there are bijections \( f(x) = 2x \) between \( \mathbb{N} \) and \( C_0 \), \( g(x) = 2x - 1 \) between \( \mathbb{N} \) and \( C_1 \), \( \text{card}(C_0) = \text{card}(C_1) = \aleph_0 \). Since \( (C_0 \times I_0) \cup (C_1 \times I_0) = \mathbb{N} \times I_0 \), \( (C_0 \times I_0) \cap (C_1 \times I_0) = \emptyset \),
\[ a = \text{card}(\mathbb{N} \times I_0) = \text{card}(C_0 \times I_0) + \text{card}(C_1 \times I_0) \\
= \aleph_0 \cdot \text{card}(I_0) + \aleph_0 \cdot \text{card}(I_0) = \aleph_0 \cdot \aleph_0 + \aleph_0 \cdot \aleph_0 \\
= a + a. \]

\[ \square \]

**Theorem 2.11.** If \( a, b \) are cardinal numbers with \( 1 \leq b \leq a \) and \( a \) infinite, then \( a \cdot b = a \).

**Proof.** Since \( a \leq a \cdot b \leq a \cdot a \), it is sufficient to prove that \( a = a \cdot a \).

Define

\[ \chi = \{(D, f) : D \subset A, f : D \rightarrow D \times D \text{ bijective}\}, \]

and equip \( \chi \) with the order

\[ (D, f) < (D', f') \iff \begin{cases} D \subset D' \\ f = f'|_D \end{cases}. \]

Let \( \tau = \{(D_i, f_i) : i \in I\} \) be a totally ordered subset of \( \chi \), \( D_0 = \bigcup_{i \in I} D_i, f : D_0 \rightarrow D_0 \times D_0 \) be the unique function with \( f|_{D_i} = f_i \). Then \( f \) is injective with

\[ f(D_0) = \bigcup_{i \in I} f(D_i) = \bigcup_{i \in I} f_i(D_i) = \bigcup_{i \in I} (D_i \times D_i) = D_0 \times D_0. \]

\((D, f)\) is an upper bound of \( \tau \). According to Zorn’s Lemma, since \( \forall \tau \subseteq \chi \) is bounded above, there exists a maximal element \( (D, f) \in \chi \). Let \( \text{card}(D) = \mathfrak{d} \).

Since \( (D, f) \in \chi \), \( \mathfrak{d} \cdot \mathfrak{d} = \mathfrak{d} \).

If \( \mathfrak{d} = a \), then \( a \cdot a = a \). By contradiction, assume that \( \mathfrak{d} \neq a \). Since \( \mathfrak{d} \leq a \) as \( D \subset A, \mathfrak{d} < a \). Let \( G = A \setminus D \). Then \( \mathfrak{d} + \text{card}(G) = a \). Since \( \mathfrak{d} < a \), \( \text{card}(G) = a \) by Theorem 2.10, and there exists a subset \( E \subset G \) with \( \text{card}(E) = \mathfrak{d} \).

Consider the set

\[ P = (E \times E) \cup (E \times D) \cup (D \times E). \]

Since \( E \cap D = \emptyset, (E \times E), (E \times D), (D \times E) \) are disjoint from each other. According to Theorem 2.10,

\[ \text{card}(P) = \text{card}(E \times E) + \text{card}(E \times D) + \text{card}(D \times E) \\
= \mathfrak{d} \cdot \mathfrak{d} + \mathfrak{d} \cdot \mathfrak{d} + \mathfrak{d} \cdot \mathfrak{d} = \mathfrak{d} \]

\[ = \text{card}(E). \]

There exists a bijection \( g : E \rightarrow P \). Since \( E \cap D = P \cap (D \times D) = \emptyset \), there exists a bijection \( h : D \cup E \rightarrow P \cup (D \times D) \) such that \( h|_D = f \) and \( h|_E = g \). Since \( P \cup (D \times D) = (D \cup E) \times (D \cup E), (D \cup E, h) \in \chi, (D, f) \) is not the maximal element in \( \chi \). \( \Rightarrow \leftrightarrow \)

Hence \( \mathfrak{d} = a, a \cdot a = a \). \[ \square \]
3. Schroeder-Bernstein Theorem

Schroeder-Bernstein Theorem states that if there exists an injection from set $A$ to set $B$ and an injection from set $B$ to set $A$, then there exists a bijection between $A$ and $B$. In terms of cardinality, it means that if $|A| \leq |B|$ and $|B| \leq |A|$, then $|A| = |B|$, which completes the ordering of cardinal numbers.

Proposition 3.1. If $B \subseteq A$ and there exists an injective function $f : A \rightarrow B$, then there exists a bijective function $h : A \rightarrow B$ between $A$ and $B$.

Proof. If $X \subseteq Y$, then $\{f(k) \mid k \in X\} \subseteq \{f(k) \mid k \in Y\}$, $f(X) \subseteq f(Y)$. Since in the base case, we have $A \supseteq B$, $B \supseteq f(A)$,

$$A \supseteq B \supseteq f(A) \supseteq f(B) \supseteq f^2(A) \supseteq f^2(B) \supseteq \ldots$$

by induction.

Consider the sequence of sets

$$X_0 = A \setminus B, X_1 = B \setminus f(A), X_2 = f(A) \setminus f(B), \ldots$$

Since for any $n$, $X_{n+2} = f(P) \setminus f(Q)$ while $X_n = P \setminus Q$, for any $x \in X_{n+2}$,

$x \in f(P)$, there exists $p \in P$ such that $f(p) = x$. Since $p \notin Q$ (or $x = f(p) \notin f(Q)$),

$p \in P \setminus Q = X_n$ with $f(p) = x$. Hence $f$ is both surjective and injective, there exists a bijection $f : X_n \rightarrow X_{n+2}$ between $X_n$ and $X_{n+2}$.

For any $n, m \in \mathbb{N}$ such that $n > m$, since $X_m \cap X_{m+1} = \emptyset$ and $X_{m+1} \supseteq X_n$,

$X_m \cap X_n = \emptyset$. Hence for sets

$$V = \bigcup_{n=0}^{\infty} X_n, \quad W = \bigcup_{n=1}^{\infty} X_n,$$

there exists a bijection $F : V \rightarrow W$ between $V$ and $W$ with

$$F(x) = \begin{cases} x & \text{if } x \in X_n, \text{ } n \text{ odd} \\ f(x) & \text{if } x \in X_n, \text{ } n \text{ even} \end{cases}.$$ 

Since $B \subseteq A$, $V \subseteq A$, $W \subseteq V$, $W \subseteq B$,

$$A = (A \setminus (B \cup V)) \cup (B \setminus V) \cup (V \setminus B) \cup ((B \cap V) \setminus W) \cup W$$

$$B = (B \setminus V) \cup ((B \cap V) \setminus W) \cup W$$

$$V = (V \setminus B) \cup ((B \cap V) \setminus W) \cup W$$

with $(A \setminus (B \cup V)), (B \setminus V), (V \setminus B), ((B \cap V) \setminus W)$, $W$ disjoint from each other. Since $A \setminus B = X_0 = V \setminus W$,

$$A \setminus (B \cup V)) \cup (V \setminus B) = A \setminus B = V \setminus W = (V \setminus B) \cup ((B \cap V) \setminus W)$$

$$A \setminus (B \cup V)) = ((B \cap V) \setminus W)$$

$$A \setminus V = (A \setminus (B \cup V)) \cup (B \setminus V) = (B \setminus V) \cup ((B \cap V) \setminus W) = B \setminus W$$

Let $Z = A \setminus V = B \setminus W$. Since there exists a bijection $f : V \rightarrow W$ between $V$ and $W$, there exists a bijection $h : A \rightarrow B$ between $A$ and $B$ with

$$h(x) = \begin{cases} F(x) & \text{if } x \in V \\ x & \text{if } x \in Z \end{cases}.$$
Theorem 3.2. (Schroeder-Bernstein Theorem) If there exist injective functions \( f: A \rightarrow B \) and \( g: B \rightarrow A \), then there exists a bijective function \( h: A \rightarrow B \) between \( A \) and \( B \).

Proof. Since \( g: B \rightarrow A \), \( g(B) \subseteq A \). Since there exists an injective function \( g \circ f: A \rightarrow g(B) \), according to Proposition 3.1, there exists a bijective function \( h': A \rightarrow g(B) \) between \( A \) and \( g(B) \). Since \( g^{-1}: g(B) \rightarrow B \) is a bijective function between \( g(B) \) and \( B \), \( h = g^{-1} \circ h': A \rightarrow B \) is a bijective function between \( A \) and \( B \). \( \square \)

A graph theory argument can also be used to prove Schroeder-Bernstein Theorem:

Remark 3.3. There is an alternative proof of Theorem 2.2 with graphs.

Following the idea of L. Babai, consider the bipartite graph \( G \) between \( A \) and \( B \) that connects \( a \) to \( f(a) \) for all \( a \in A \), and \( b \) to \( f(b) \) for all \( b \in B \). Then for any \( x \in A \cup B \), \( \deg(x) \) is either 1 or 2.

Let \( \{V_i : i \in I\} \) be the set of connected components of \( G \). Then \( \bigcup_{i \in I} V_i = G \).

Let \( A_i = V_i \cap A \), \( B_i = V_i \cap B \). Then \( \sum |A_i| = |A|, \sum |B_i| = |B| \).

For any \( V_i \), \( V_i \) is a connected graph with each vertex having \( \deg(v) = 1 \) or 2. If \( V_i \) contains a cycle, then each vertex in the cycle cannot connect with any more vertices, \( V_i \) is a cycle. If \( V_i \) does not contain a cycle, then there cannot be more than one path within \( V_i \), \( V_i \) is a path. If \( V_i \) is not a two-side infinite path, then there is an endpoint of \( V_i \) with either \( e \in A \) or \( e \in B \), \( V_i \) is either the path connecting \( \{e, f(e), g(f(e)), f(g(f(e)))\}, \ldots\) or the path connecting \( \{e, g(e), f(g(e)), g(f(g(e)))\}, \ldots\).

Hence \( V_i \) is either a cycle, a two-side infinite path, a one-side infinite path starting from set \( A \), or a one-side infinite path starting from set \( B \). By picture, \( V_i \) is of one of the following forms:

\[
\begin{array}{c}
\text{(1)} \\
\begin{array}{c}
\ldots \ldots \\
\ldots \ldots \\
A \\
\ldots \ldots \\
B
\end{array}
\end{array}
\begin{array}{c}
\text{(2)} \\
\begin{array}{c}
\ldots \ldots \\
\ldots \ldots \\
A \\
\ldots \ldots \\
B
\end{array}
\end{array}
\begin{array}{c}
\text{(3)} \\
\begin{array}{c}
\ldots \ldots \\
\ldots \ldots \\
B \\
\ldots \ldots \\
A
\end{array}
\end{array}
\begin{array}{c}
\text{(4)} \\
\begin{array}{c}
\ldots \ldots \\
\ldots \ldots \\
B \\
\ldots \ldots \\
A
\end{array}
\end{array}
\]

Hence within any \( V_i \), \( |A_i| = |B_i| \). Since \( |A| = \sum |A_i| = \sum |B_i| = |B| \), \( A, B \) are of the same cardinality, there is a bijection between \( A \) and \( B \).
4. Lagrange’s Theorem

As a particular kind of sets, groups themselves contain more accessible information. Lagrange’s Theorem states that for any finite group $G$, the order (number of elements) of every subgroup $H$ of $G$ divides the order of $G$.

**Definition 4.1.** A group $\langle G, * \rangle$ is a set $G$ closed under a binary operation $*$ such that the following axioms are satisfied:

1. (Associativity) For all $a, b, c \in G$, $(a * b) * c = a * (b * c)$.
2. (Identity element) There is an element $e \in G$ such that for all $x \in G$, $e * x = x * e = x$.
3. (Inverse element) For all $a \in G$, there is an element $a^{-1} \in G$ such that $a * a^{-1} = a^{-1} * a = e$.

**Notation 4.2.** The operation $*$ is sometimes omitted for convenience, in which case $a * b$ is represented by $ab$.

**Definition 4.3.** A subgroup $H$ of $G$ is a subset of $G$ closed under the binary operation of $G$, and is itself a group. $H \leq G$ and $G \geq H$ denote that $H$ is a subgroup of $G$.

**Definition 4.4.** Given $H \leq G$, a coset of $H$ in $G$ is $gH = \{gh \mid h \in H\}$.

**Lemma 4.5.** For $g \in G$, $gH = H$ if and only if $g \in H$.

**Proof.** For any $g \notin H$, since $e \in H$, $ge \in gH$ and $ge = g \notin H$, $gh \neq H$.

For any $g \in H$, $gH = \{gh \mid h \in H\} \subseteq H$ as $H$ is a closed subgroup. For any $h \in H$, since $h = (gg^{-1})h = g(g^{-1}h)$ and $g^{-1}h \in H$, $h \in gH$, $H \subseteq gH$. Hence $gH = H$.

Hence $gH = H$ if and only if $g \in H$. \hfill \Box

**Proposition 4.6.** For $g, g' \in G$, $gH = g'H$ if and only if $g^{-1}g' \in H$.

**Proof.** If $gH = g'H$, then $H = g^{-1}gH = g^{-1}g'H$. According to Lemma 4.5, $H = g^{-1}g'H$ if and only if $g^{-1}g' \in H$. Hence $gH = g'H$ if and only if $g^{-1}g' \in H$. \hfill \Box

**Proposition 4.7.** All cosets of $H$ have the same size as $H$.

**Proof.** For any coset $gH$, $f : h \to gh$ is a bijective map between $H$ and $gH$. Since for any $h \in gH$, there exists $h' \in H$ such that $f(h') = h$, the map is surjective. Since for any $h_1, h_2 \in H$ such that $f(h_1) = f(h_2)$, there is $h_1 = g^{-1}gh_1 = g^{-1}gh_2 = h_2$, the map is injective. Hence there is a bijection between any coset $gH$ and $H$, all cosets of $H$ has the same size as $H$. \hfill \Box

**Proposition 4.8.** For any two cosets of $H$ in $G$, if $g_1H \cap g_2H \neq \emptyset$, then $g_1H = g_2H$.

**Proof.** If $g_1H \cap g_2H \neq \emptyset$, then there exist $h_1, h_2 \in H$ such that $g_1h_1 = g_2h_2$, $g_1^{-1}g_2 = h_2^{-1}h_1 \in H$. According to Proposition 4.6, $g_1H = g_2H$. \hfill \Box

**Proposition 4.9.** For any finite group $G$ and its subgroup $H$, there are totally $|G|/|H|$ cosets of $H$ in $G$. 
Proof. Since each $g \in G$ lies in the coset $gH$, the union of all cosets $\bigcup gH = G$. According to Proposition 4.8, any two cosets of $H$ in $G$ are either identical or disjoint, so there exists a set of disjoint cosets $\{g_i\}$ such that

$$\bigcup g_i H = \bigcup gH = G$$

$$\sum |g_i H| = |G|.$$ 

According to Proposition 4.7, each coset $g_i H$ has $|g_i H| = |H|$, so $|(g_i H)| = |G|/|H|$. \hfill \Box

**Theorem 4.10. (Lagrange’s Theorem)** For any finite group $G$, the order of every subgroup $H$ of $G$ divides the order of $G$.

**Proof.** According to Proposition 4.9, $|G|/|H| = |\{g_i H\}|$. Hence $|H|$ divides $|G|$. \hfill \Box

**Corollary 4.11.** If $g \in G$, $n$ is the minimal positive integer with $g^n = e$ (i.e. $n$ is the order of $g \in G$), then $n \mid |G|$.

5. Cyclic Groups

Cyclic group are groups generated by a single element. Despite the multitude of cyclic groups, they can all be summed up as isomorphisms of $\mathbb{Z}_m$ and $\mathbb{Z}$ with identifiable generators.

**Definition 5.1.** Given a group $G$ and an element $a \in G$. If $G = \{a^n \mid n \in \mathbb{Z}\}$, then the group $G = \langle a \rangle$ is cyclic, and $a$ is a generator of $G$.

**Definition 5.2.** If a cyclic group $G = \langle a \rangle$ is finite, then the order of $a$ is the order $|\langle a \rangle|$ of this cyclic group.

**Theorem 5.3.** $\mathbb{Z}_m$ and $\mathbb{Z}$ are the only cyclic groups up to isomorphism.

**Proof.** Let $G$ be a cyclic group generated by $a$.

By cases, if $G = \{e\}$, then $H$ is isomorphic to $\mathbb{Z}_0$.

If $G \neq \{e\}$ and is finite, then there exists $a \neq e \in G$, and $n \in \mathbb{N}$ such that $a^n \in G$. Let $m$ be the smallest positive integer such that $a^m = e$. Consider the linear map

$$f : n \rightarrow a^n$$

between $\mathbb{Z}_m$ and $G$. For all $x, y \in \mathbb{Z}_n$,

$$(x + y)z_n = ((x)z_n + (y)z_n)z_n$$

$$f(x + y) = a^{x+y} = a^x a^y = f(x)f(y).$$

For any $n_1, n_2 \in \mathbb{Z}_m$ such that $f(n_1) = f(n_2)$, $a^{n_1 - n_2} = e$, $m \mid n_1 - n_2$ and $|n_1 - n_2| \leq m - 1$. Then $n_1 = n_2$, $f$ is injective. For any $g \in G$, there exists $n \in \mathbb{N}$ such that $a^n = g$. According to Division Theorem, there exist $q, r \in \mathbb{N}$ such that $n = qm + r \ (0 \leq r < m)$.

Then

$$g = a^n = a^{qm+r} = (a^m)^q a^r = e^q a^r = a^r = f(r)$$

with $0 \leq r < m$ for all $g \in G$, $f$ is surjective. Hence there is a bijection between $\mathbb{Z}_m$ and $G$, $G$ is isomorphic to $\mathbb{Z}_m$. 


If \( G \neq \{e\} \) and is infinite, then there exists \( a \neq e \in G \) with \( a^n \neq e \) for all \( n \in \mathbb{N} \).
Consider the linear map
\[
f : n \rightarrow a^n
\]
between \( \mathbb{Z} \) and \( G \). For any \( x, y \in \mathbb{Z}_n \),
\[
f(x + y) = a^{x+y} = a^xa^y = f(x)f(y).
\]
For any \( n_1, n_2 \in \mathbb{N} \) with \( n_1 \neq n_2 \), \( a^{n_1} \neq a^{n_2} \) (or \( a^{n_1-n_2} = e \)), so \( f \) is injective. For any \( g \in G \), there exists \( n \in \mathbb{N} \) such that \( a^n = g \), so \( f \) is surjective. Hence there is a bijection \( f \) between \( \mathbb{Z} \) and \( G \), \( G \) is isomorphic to \( \mathbb{Z} \).

Hence all cyclic groups are isomorphic either to \( \mathbb{Z}_n \) or to \( \mathbb{Z} \). \( \square \)

**Theorem 5.4.** A subgroup of a cyclic group is cyclic.

**Proof.** Let \( G \) be a cyclic group generated by \( a \) and \( H \leq G \).
If \( H = \{e\} \), then \( H \) is a cyclic group generated by \( e \).
If \( H \neq \{e\} \), then there exists \( a \neq e \in H \) and \( n \in \mathbb{N} \) such that \( a^n \in H \). Let \( m \) be the smallest positive integer such that \( a^m \in H \). Since \( H \) is a subgroup of \( G \), for any \( h \in H \), there exists \( n \in \mathbb{N} \) such that \( a^n = h \). According to Division Theorem, there exist \( q, r \in \mathbb{N} \) such that
\[
n = qm + r \quad (0 \leq r < m).
\]
Then
\[
a^n = a^{qm+r} = (a^m)^q a^r
\]
\[
a^r \in H
\]
by closure. Since \( 0 \leq r < m \) and \( m \) is the smallest positive integer such that \( a^m \in H \), \( r = 0 \). Hence \( n = qm \), \( h = a^n = (a^m)^q \) for all \( h \in H \).

Hence \( H \) is generated by \( a^m \), \( H = \langle a^m \rangle \) is cyclic. \( \square \)

**Theorem 5.5.** For any \( n \in \mathbb{N} \), \( \mathbb{Z}_n \) has \( \varphi(n) \) generators, in which \( \varphi(n) = |\{i | i \in \mathbb{N}, 0 \leq i < n, \gcd(i,n) = 1\}| \).

**Proof.** For any \( i \in \mathbb{Z}_n \), since \( \mathbb{Z}_n = \{0,1,\ldots,n-1\}, i \in \mathbb{N} \) and \( 0 \leq i < n \).
If \( i \in \mathbb{Z}_n \) and \( \gcd(i,n) \neq 1 \), then for any \( k \in \mathbb{N}, i^k \equiv ki (\text{mod } n), \gcd(i,n)|i^k, i^k \neq 1, i \) does not generate \( \mathbb{Z}_n \).
If \( i \in \mathbb{Z}_n \) and \( \gcd(i,n) = 1 \), then it can be shown that \( i, i^2, \ldots, i^n \) are all distinct.
If there exist \( 1 \leq k, l \leq n \) such that \( i^k = i^l \), then \( (k-l)i \equiv 0 (\text{mod } n) \). Since \( \text{lcm}(n,i) = ni, (k-l)i \) is a multiple of \( ni \), \( k-l \) is a multiple of \( n \). Since \( |k-l| \leq n-1 \), \( |k-l| = 0 \), \( k = l \). Since \( |\mathbb{Z}_n| = n, \{i,i^2,\ldots,i^n\} = \mathbb{Z}_n, i \) generates \( \mathbb{Z}_n \).

Hence \( i \) is a generator of \( \mathbb{Z}_n \) if and only if \( \gcd(i,n) = 1 \), \( \mathbb{Z}_n \) has \( \varphi(n) \) generators. \( \square \)

6. Understanding Sets within Group Structures

According to Theorem 2.11, \( a \cdot a = a \) for \( a \) infinite, which explains the fact that \( \mathbb{R} \) and \( \mathbb{C} = \{a+bi | a, b \in \mathbb{R}\} \) have the same cardinality. Moreover, the sets of real and complex numbers are also isomorphic as additive groups.

**Lemma 6.1.** If there is a bijection between the bases of two vector spaces over the same field, then the two vector spaces are isomorphic as additive groups.
such that for any $v = \lambda_1 v_1 + \ldots + \lambda_n v_n \in V$, $h(v) = \lambda_1 f(v_1) + \ldots + \lambda_n f(v_n) \in W$.

If there exist $v = \lambda_1 v_1 + \ldots + \lambda_n v_n, u = \mu_1 v_1 + \ldots + \mu_n v_n \in V$ such that $h(v) = h(u)$, then

$$\lambda_1 f(v_1) + \ldots + \lambda_n f(v_n) = \mu_1 f(v_1) + \ldots + \mu_n f(v_n).$$

Since each element in $W$ can be uniquely written in a linear combination of basis, $\lambda_i = \mu_i$ for all $i, v = u$. Hence $h$ is injective.

Since for any $w = \lambda_1 w_1 + \ldots + \lambda_n w_n \in W$, there exists

$$v = \lambda_1 f^{-1}(w_1) + \ldots + \lambda_n f^{-1}(w_n) \in V$$

such that $h(v) = w$, $h$ is also surjective and therefore bijective.

Since for any $v = \lambda_1 v_1 + \ldots + \lambda_n v_n, u = \mu_1 v_1 + \ldots + \mu_n v_n \in V$, there is

$$h(v + u) = h(\lambda_1 v_1 + \ldots + \lambda_n v_n + \mu_1 v_1 + \ldots + \mu_n v_n)$$

$$= \lambda_1 f(v_1) + \ldots + \lambda_n f(v_n) + \mu_1 f(v_1) + \ldots + \mu_n f(v_n)$$

$$= h(v) + h(u),$$

$h$ preserves the additive operations of $V$ and $W$.

Hence $h : V \to W$ is a bijection between $V$ and $W$ that preserves additions, $V$ and $W$ are isomorphic as additive groups.

\begin{lemma}
There is a bijection between the bases of $\mathbb{R}$ and $\mathbb{C}$ over $\mathbb{Q}$.
\end{lemma}

\begin{proof}
Let $B$ be a basis of $\mathbb{R}$ over $\mathbb{Q}$. Since $\dim_\mathbb{Q}(\mathbb{R})$ is infinite, $\text{card}(B)$ is infinite.

Since $B \subseteq \mathbb{R}, iB \subseteq i\mathbb{R}, B \cap iB = \emptyset$. Since $B \cup iB$ is a basis of $\mathbb{C}$ over $\mathbb{Q}$, $B \cap iB = \emptyset$, $\text{card}(B \cup iB) = \text{card}(B) + \text{card}(B) = \text{card}(B)$. Hence there is a bijection between the bases of $\mathbb{R}$ and $\mathbb{C}$ over $\mathbb{Q}$.
\end{proof}

\begin{theorem}
$\mathbb{R}$ and $\mathbb{C}$ are isomorphic as additive groups.
\end{theorem}

\begin{proof}
According to Lemma 6.1 and Lemma 6.2, since there is a bijection between the bases of $\mathbb{R}$ and $\mathbb{C}$ over the same field $\mathbb{Q}$, $\mathbb{R}$ and $\mathbb{C}$ are isomorphic as additive groups.
\end{proof}

Every set admits some group structure. With previous theorems about cardinality, the bijection between $X$ and $F$, the set of all finite subsets of $X$, helps construct a group structure within the set $X$.

\begin{lemma}
For an infinite set $X$, there exists a bijection between $X$ and $F$, in which $F$ is the set of all finite subsets of $X$.
\end{lemma}

\begin{proof}
Since $X$ is infinite, $\aleph_0 \leq |X|$ by Theorem 2.7.

For $n = 0, 1, 2, \ldots$, let $F_n \subseteq F$ be the set of all finite subsets of $|X|$ with cardinality $n$. Then $F = \bigcup_{n \in \mathbb{N}} F_n$. Since there are $|X|^n$ ways to choose $n$ elements, each of which from a group with cardinality $|X|$, $|F_n| \leq |X|^n$. Since $|X|^n = |X|$ according to Theorem 2.11, $|F_n| \leq |X|$. Since $F_0, F_1, F_2, \ldots$ are disjoint from each other and $F = \bigcup_{n \in \mathbb{N}} F_n$, $|F| = \bigcup_{n \in \mathbb{N}} |F_n| \leq \aleph_0 |X| = |X|$ by Theorem 2.11.

Meanwhile, since $|X| = |\{\{x\} \mid x \in F\}| \leq |F|$, $|X| = |F|$. Hence $X$ and $F$ are of the same cardinality, there exists a bijection $f : X \to F$ between $X$ and $F$. \hfill \QED
Lemma 6.5. $F$ admits a group structure.

Proof. For all $f, g \in F$, let $f \cdot g = (f \setminus g) \cup (g \setminus f)$.

Since for any $f, g \in F$, $f \subseteq X$, $g \subseteq X$, $(f \setminus g) \cup (g \setminus f) \subseteq (f \cup g) \subseteq X$, $f \cdot g$ is closed in $F$. For any $f, g, h \in F$, both $(f \cdot g) \cdot h$ and $f \cdot (g \cdot h)$ consist of elements which either are in exactly one of $A, B$ or $C$, or are in all three, so $f \cdot g$ is associative.

Let $\emptyset$ denote the empty set, a perfectly good finite set. Since for any $f \in F$, $f \cdot \emptyset = (f \setminus \emptyset) \cup (\emptyset \setminus f) = f$, there exists an identity element $\emptyset \in F$. Since for any $f \in F$, there exists $f \in F$ such that

$$f \cdot f = (f \setminus f) \cup (f \setminus f) = \emptyset,$$

so there exists an inverse element $\emptyset \in F$.

Hence $\langle F, \cdot \rangle$ is a group. \hfill \Box

Theorem 6.6. Every set admits a group structure.

Proof. Let $X$ be an arbitrary set.

If $|X|$ is finite, then $|X| = n$ for some $n \in \mathbb{N}$, $|X| = |\mathbb{Z}_n|$. Then there exists a bijection $f : X \rightarrow \mathbb{Z}_n$. Since $\langle \mathbb{Z}_n, + \rangle$ is a cyclic group, $\langle X, \circ \rangle$ with

$$x_1 \circ x_2 = f^{-1}(f(x_1) + f(x_2))$$

is a cyclic group.

If $|X|$ is infinite, then according to Lemma 6.4 and Lemma 6.5, there exists a bijection $f : X \rightarrow F$ between $X$ and $F$ with $\langle F, \cdot \rangle$ being a group. Hence $\langle X, \circ \rangle$ is a group in which

$$x_1 \circ x_2 = f^{-1}(f(x_1) \cdot f(x_2)).$$

\hfill \Box

Acknowledgments. It is a pleasure to thank my mentor, Brian Mcdonald, for his guidance in studying group theory and set theory. I would also like to thank Peter May for organizing the REU program at the University of Chicago, and Laszlo Babai for teaching the apprentice program. It is their efforts that created this wonderful summer experience.

References

    https://web.math.rochester.edu/people/faculty/jonpak/N3.pdf