1 Binary Operation

def: Let A be an aribitrary set, a binary operation is a function:

$$f : A \to A$$

- **remark:**
    1. No exception: for every orderd pair (a_1, a_2) and $a_1, a_2 \in A$, there exists a corresponding element
        - Division is not a binary operation on $\mathbb{R}$
        - e.g. $(3, 0) \in \mathbb{R} \times \mathbb{R}$, but $\frac{3}{0}$ is undefined
    2. No ambiguity: for every orderd pair (a_1, a_2) and $a_1, a_2 \in A$, the corresponding pair will be unique defined.
    3. Closed under the operation
- **remark:** Natural Number starts from 1

2 Power Set

def: let S be an aribitrary set. P(S) is a set consists exactly of all subsets of S (including $\emptyset$ and S)

- **e.g.** if $S = \{1, 2\}$, then $P(S) = \{\emptyset, \{1\}, \{2\}, \{1, 2\}\}$

- **Notation:** * , · , +, or nothing. We also denot *(x,y), ·(x,y), +(x,y), or (x,y)

3 Addition Properties

Axiom:

$$+ : A \times A \to A$$

1. closed under operation
2. commutative
3. associative
4. there exists a neutral element,0, s.t. $x + 0 = 0 + x = x$
5. there is an inverse s.t. $x + y = y + x = 0$

- **remark:** neutral element is always unique but may not always exists

    Proof. $e_1 = f(e_1, e_2) = e_2$ □

- **remark:** if S has a neutral element, let $x \in S$. If $y \in S$ satisfies $f(x, y) = f(y, x) = e$, then y is called negative of inverse, which is also unique.
- **remark:** Def associativity, $\forall x, y, z \in S, f(f(x, y), z) = f(x, f(y, z))$
- **remark:** Def commutativity, $\forall x, y, f(x, y) = f(y, x)$

4 Group

def: A set of G if there exists a binary operation * on G such that:

1. there exists a neutral element
2. there exists a unique inverse for every element in G
3. associative

5 Multiplication Axioms

1. there exists a neutral element other than 0, called 1
2. $\forall x \in \mathbb{R}, x \neq 0, \exists! y \in \mathbb{R}$ called the inverse of x
3. associative
4. commutative
5. Distributive Law: Let *, +, be two operations on a set S.
   - left distributive: $x * (y + z) = x * y + x * z$
   - right distributive: $(y + z) * x = y * x + z * x$

remark: In $\mathbb{R}$, $*$ is distributive to $+$

remark: $R^* = R \setminus \{0\}$ becomes a group under $*$

6 Order of Group Elements

Corollary. *Let k be an element of a group G. Then* $ord(k) = | < k > |$
In other words, the order of k is equal to the order of the cyclic group generated by k

Theorem. *(Structure of finite cyclic group)*
Let G be a cyclic group of $< x >$ *with finite order n.*
The following holds:

1. *Every subgroup of G is cyclic and is of the shape* $< x^d >$ *where* $d > 0$ *and* $d|n$
   More concretely, Let $d_1, d_2, ..., d_r$ *be all distinct positive divisor of n. then* $< x^{d_1} >, < x^{d_2} >, ..., < x^{d_r} >$ *exhaust all subgroup of G.*

2. *if d and d' are both positive divisors of n, and $d \neq d'$, then $< x^d > \neq < x^{d'}$*

3. *if $k \in \mathbb{Z}$, then x^k is a generator of G iff $gcd(k, n) = 1$*

4. *$\forall k \in \mathbb{Z}$, we have $< x^k > = < x^d >$, where $d = gcd(n, k)$*

5. *$\forall k \in \mathbb{Z}$, $ord(x^k) = \frac{n}{gcd(n,k)}$*

Proof of the theorem above:

1. *Proof.* Take H be a subgroup of G,.
   if $H = \{e\}$, then $H = < x^n >$
   if $H = G$, then $H = < x >$
   Now let $H \subseteq G$ be a nontrivial subgroup. Since $G = \{e, x^1, x^2, ..., x^{n-1}\}$, thus H contains some elements of the shape x^j, where $j \in \{1, 2, 3, ..., n-1\}$.
   Take $d \in \mathbb{N}$ be the smallest natural number such that $x^d \in H$.
   Claim:$< x^d > = H$.
   1. Since H is a subgroup of G containing x^d. By definition $< x^d >$ is the smallest subgroup of G containing x^d. Thus

   $$< x^d > \subseteq H$$

   2. Take $y \in H \Rightarrow y \in G \Rightarrow y = x^m$, where $m = \{0, 1, ..., n-1\}$
   By definition using Division Algorithm:

   $$\exists! q, r \in \mathbb{Z}$$

   such that $m = qd + r, 0 \leq r < d$

   $$x^r = x^{m-qd} = x^m (x^d)^{-q} \Rightarrow x^m = y \in H, (x^d)^{-q} \in H \Rightarrow x^r \in H$$

   If $r > 0$, then r is a natural number strictly smaller than d, also $x_r \in H$, which contradicts the minimality of d. Thus,

   $$r = 0 \Rightarrow H \subseteq < x^d >$$

   Above all, we know $H = < x^d >$

   Then show that $d|n$
   Again, use Division Algorithm:

   $$\exists! q', r'$$

   such that $n = q'd + r', 0 \leq r' < d$.

   $$x^{r'} = x^n x{-}q'd = e(x^d)^{-q'} \in < x^d >$$

   so it contradicts with the minimality of d. Therefore $r' = 0$ $\square$

2.

7 Study of Symmetric Group and Permutation Group

Def. ***Symmetric Group:*** *Let A be a non-empty set. Then a symmetric group of A is the group consists of all bijective maps from A to itself under the usual compositions of functions.*
Notation: sym(A)

Def. ***Symmetric Group:*** *Let A be a non-empty set. Then a permutation group of A is a group G whose elements are bijective maps from A to itself under usual compositions of functions*

Remark. *Symmetric group is unique, because it contains* ***all*** *of the bijective maps from A to itself.*
Permutation group is not unique, because it contains ***some*** *of the bijective maps from A to itself.*
A permutation group is a subgroup of symmetric group

Prop. *Let S_n be a permutation group, then*

$$|S_n| = n!$$

Def. ***Cauchy's two line notation:***
e.g. Consider $\sigma \in S_3$

$$\sigma(1) = 2, \sigma(2) = 3, \sigma(3) = 1$$

Notation:

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

Theorem. ***Cayley's theorem***
Every group is isomorphic to permutation group of a certain set.

Proof. Let A be the underlying set of G.
Goal: construct a monomorphism $T : G \to sym(A)$
$\forall g \in G$, define: $T_g : A \to A$ such that $T_g(a) = ga$

claim: T_g is injective:
Let $a_1, a_2 \in A$ with $T_g(a_1) = T_g(a_1)$, so $ga_1 = ga_2 \Rightarrow a_1 = a_2$

claim: T_g is surjective:
Let $b \in A$, it suffices to find some $a \in A$, such that $T_g(a) = b$. Thus, $ga = b \Rightarrow a = g^{-1}b \in A$
Thus, we define the map $T : G \to sym(A)$ to be $T(g) = T_g$

claim: T is injective:
Let $g_1, g_2 \in G$

$$T(g_1) = T(g_2) \iff T_{g_1} = T_{g_2}$$

$$T_{g_1} : A \to A \iff T_{g_2} : A \to A$$

as bijective map from A to itself.

$$\iff T_{g_1}(a) = T_{g_2}(a), \forall a \in A$$

Take $a = e_G \Rightarrow T_{g_1}(e_G) = T_{g_2}(e_G) \Rightarrow g_1 e_G = g_2 e_G \Rightarrow g_1 = g_2$

claim: T preserves the group operation:
it suffices to show $\forall g_1, g_2 \in G, T(g_1, g_2) = T(g_1) \circ T(g_2) \iff T_{g_1 g_2} = T_{g_1} \circ T_{g_2}$

$$\forall a \in A, T_{g_1}] \circ T_{g_2}(a) = T_{g_1}(g_2 a) = g_1 g_2 a$$
$$T g_1 g_2(a) = g_1 g_2 a$$

Thus, $T_{g_1 g_2} = T_{g_1} \circ T_{g_2}$.

Therefore, we have a $T : G \to sym(A)$. G is isomorphic to T(G) which is a subgroup of sym(A), which is a permutation group.

$\square$