GROUPS

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 $x, y, z \in G$,

$$x * (y * z) = (x * y) * z;$$

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

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

Definition 3:

A group is called abelian if $x * y = y * x$ for any $x, y \in G$.

Theorem:

Let G be a group.

(i) If $x * a = x * b$ or $a * x = b * x$, 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 $(a * b)^{-1} = b^{-1} * a^{-1}$.

SUBGROUPS

Definition 4:

A subset H of a group G is a subgroup if

(i) $e \in H$;

(ii) if $x, y \in H$, then $x * y \in H$;

(iii) if $x \in H$, then $x^{-1} \in H$.

Notation:

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

Definition 5:

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: $\mathbb{Z}^+ < \mathbb{Q}^+ < \mathbb{R}^+$.

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

Theorem 2:
A nonempty subset H of a finite group G is a subgroup $\iff$ H is closed.

Proof:

$\Longrightarrow$) Suppose H is a subgroup of G. Then it is closed by part (ii) of definition 4.

$\Longleftarrow$) 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 4 holds. This, in particularly 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 4 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 4 holds. Therefore, H is a subgroup of G. ■

Definition 6:
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 7:
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) $\mathbb{Q}^+,\ \mathbb{Q}^\times_{>0},\ \mathbb{R}^+,\ \mathbb{R}^\times_{>0}$ 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) $\mathbb{Z}_3^\times = \{[1],\ [2]\} = \langle [2] \rangle \neq \langle [1] \rangle$

(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 $\Leftrightarrow$ m is a prime (Lagrange, 1769)

Remark:

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

Open question:

Given a prime p, create an algorithm for finding a generator of $\mathbb{Z}_p^\times$.

Definition 8:

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
the order of [1] is 4
the order of [2] is 2
the order of [3] is 4

Open question:

Let $n \geq 1$ be an integer. Is it possible to construct an infinite group G such that all its elements have a finite order n.

Definition 9:

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

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

Theorem 3:

Let G be a finite group and let $a \in G$. Then

$$\text{order of } a = |\langle a \rangle|.$$

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,

$$H \subset \langle a \rangle.$$

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

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

this gives

$$\langle a \rangle \subset H,$$

and so $\langle a \rangle = H$. ■

Definition:

A subset H of a group G is a subgroup if

(i) $e \in H$;

(ii) if $x, y \in H$, then $x * y \in H$;

(iii) if $x \in H$, then $x^{-1} \in H$.

Theorem 1:

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

Theorem 2:

A nonempty subset H of a finite group G is a subgroup $\iff$ H is closed.

Theorem 2:

A nonempty subset H of a finite group G is a subgroup $\iff$ H is closed.

Proof:

$\implies$) Suppose H is a subgroup of G. Then it is closed by part (ii) of definition 4.

$\Longleftarrow$) 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 4 holds. This, in particularly 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 integer $k \geq 1$.

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 4 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 4 holds. Therefore, H is a subgroup of G. ■

Definition:

If G is a group and $a \in G$, write

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

$\langle a \rangle$ 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:

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) $Z^+ = \{0,\ \pm 1,\ \pm 2,\ \pm 3, \ldots\} = \langle 1 \rangle$

(c) $Q^+,\ Q^\times_{>0},\ R^+,\ R^\times_{>0}$ **are not cyclic**

(d) $S_2 = \{(1),\ (12)\} = \langle (12) \rangle \neq \langle (1) \rangle$

(e) $S_m,\ m > 2$, **is not cyclic**

Example:

(f) $Z_m^+ = \{[0],\ [1],\ [2], \ldots, [m-1]\} = \langle [1] \rangle$

(g) $Z_3^\times = \{[1],\ [2]\} = \langle [2] \rangle \neq \langle [1] \rangle$

(h) $Z_5^\times = \{[1], [2], [3], [4]\} = \langle [2] \rangle = \langle [3] \rangle \neq \langle [1] \rangle, \langle [4] \rangle$

(i) $Z_7^\times = \{[1], [2], \ldots, [6]\} = \langle [3] \rangle = \langle [5] \rangle \neq \langle [1] \rangle, \langle [2] \rangle, \langle [4] \rangle, \langle [6] \rangle$

(j) $Z_m^\times$ **is cyclic** $\Leftrightarrow$ m **is a prime (Lagrange, 1769)**

Remark:

Recall, that if m is composite, $Z_m^\times$ is not a group.

Open question:

Given a prime p, create an algorithm for finding a generator of $Z_p^\times$.

Definition:

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 $G = \{(1), (12)\}$, then the order of (1) is 1 and the order of (12) is 2

(b) Let $G = Z_4^+ = \{[0], [1], [2], [3]\}$, then the order of $[0]$ is 1

the order of $[1]$ is 4

the order of $[2]$ is 2

the order of $[3]$ is 4

Definition:

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

Example: $|S_n| = n!$, $|Z_n^+| = n$, $|Z_p^\times| = p - 1$.

Theorem:

Let G be a finite group and let $a \in G$. Then

$$\text{order of } a = |\langle a \rangle|.$$

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,

$$H \subset \langle a\rangle.$$

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

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

this gives

$$\langle a\rangle \subset H,$$

and so $\langle a\rangle = H$. ■