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 $H \leq G$.

Example:

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

1. $\mathbb{Z}^+ < \mathbb{Q}^+ < \mathbb{R}^+$.
2. $\mathbb{Q}^\times_{\neq 0} < \mathbb{R}^\times_{\neq 0}$.
3. $\mathbb{R}^\times_{>0} < \mathbb{R}^\times_{\neq 0}$.
4. A group of even numbers is a subgroup of $\mathbb{Z}^+$.

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 1:

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

Proof of Theorem 1:

$\implies$) 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 4. Finally, if $x, y \in H$, then

$$y^{-1} \in H$$

by part (iii) of definition 4, and so

$$xy^{-1} \in H,$$

by part (ii) of definition 4.

$\impliedby$) 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 4 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 the Theorem above. 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. ■

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

Proof of Theorem 2:

$\Longrightarrow$) 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 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

$$x * x' = e = x' * x.$$

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

$$\left(x^{-1}\right)^{-1} = x.$$

(v) For all $a, b \in G$ we have

$$(a * b)^{-1} = b^{-1} * a^{-1}.$$

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

$$H \leq G.$$

Example:

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

1. $\boldsymbol{Z^+ < Q^+ < R^+}$.

2. $\boldsymbol{Q^{\times}_{\neq 0} < R^{\times}_{\neq 0}}$.

3. $\boldsymbol{R^{\times}_{>0} < R^{\times}_{\neq 0}}$.

4. **A group of even numbers is a subgroup of** $\boldsymbol{Z^+}$.

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 of Theorem 1:

$\Longrightarrow$) 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 4. Finally, if $x, y \in H$, then

$$y^{-1} \in H$$

by part (iii) of definition 4, and so

$$xy^{-1} \in H,$$

by part (ii) of definition 4.

$\Longleftarrow$) 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 4 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 the Theorem above. 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. ■

Theorem 2:

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

Proof of Theorem 2:

$\implies$) 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. ■