ABSTRACT ALGEBRA

Groups

Definition. Suppose that:

(1) G is a set and $*$ is a binary operation on G,
(2) $*$ is associative,
(3) there exists an element e of G such that $\forall x \in G$

$$x * e = e * x = x \text{ (identity element)}$$

(4) for each $x \in G$, there exists an element $y \in G$ such that

$$x * y = y * x = e$$

Then G, together with the binary operation $*$, is called a *group* and denoted $(G, *)$.

Theorem. If $(G, *)$ is a group, then there is only one identity element in G.

Theorem. If $(G, *)$ is a group and $x \in G$, then x has only one inverse.

Definition. We say a group G is *abelian* if the group operation is commutative, i.e., if $xy = yx$ for all $x, y \in G$.

Notation. For $g \in G$ and $n \in \mathbb{Z}$, $g^n = g \cdot g \cdots g$ (n-times).

Notation. If the operation of G is called $+$, then we write ng instead of g^n.

Notation. When G is finite, its order $|G|$ is the number of elements in the group.

Notation. When $g \in G$ has finite order, its order $o(g)$ is the smallest integer $m > 0$ with $g^m = e$.

Notation. If $g^m = e$ for some $m \in \mathbb{Z}$, then $o(g) \mid m$.

Subgroups

Definition. Let $(G, *)$ be a group and $H \subseteq G$. H is a *subgroup* of G if the elements of H from a group under $*$. I.e. $(H, *)$ is a group.

Theorem. Let H be a nonempty subset of group G. Then, H is a subgroup of G if and only if

(1) $\forall a, b \in H$, $ab \in H$ and
(2) $\forall a \in H$, $a^{-1} \in H$.

Terminology: If H has property 1 we say it is closed under multiplication. If H has property 2 we say it is closed under inverses.

Definition. An element $g \in G$ generates the *cyclic* subgroup $\langle g \rangle = \{g^m \mid m \in \mathbb{Z}\}$.

Theorem. An element $g \in G$ has finite order if and only if $\langle g \rangle$ is finite, in which case $o(g) = |\langle g \rangle|$.

Theorem (Lagrange's Theorem)**.** If H is a subgroup of a finite group G, then $|H| \mid |G|$.

Corollary. If $|G|$ is prime, the G is cyclic.

Corollary. For all $g \in G$, we have $o(g) \mid |G|$.

Corollary. For all $g \in G$, we have $g^{|G|} = e$.

Cosets

Definition. If H is a subgroup of G, then by *right coset of H in G* we mean a subset of the form Hg, where $g \in G$ and

$$Hg = \{hg \mid h \in H\}.$$

Definition. If H is a subgroup of G, then by *left coset of H in G* we mean a subset of the form gH, where $g \in G$ and

$$gH = \{gh \mid h \in H\}.$$

Theorem. Two right cosets Hx and Hy are either the same set or disjoint sets. (That is, if they share even one element, they are exactly the same set.) The same holds for left cosets. (On the other hand, a right coset and a left coset can intersect each other without being the same set.)

Corollary (Right coset relation)**.** $Hx = Hy \iff xy^{-1} \in H \iff x \in Hy$.

Corollary (Left coset relation)**.** $xH = yH \iff y^{-1}x \in H \iff x \in yH$.

Corollary. $Hx = H \iff x \in H \iff xH = H$.

Notation. If G is abelian and the group operation is written as addition, then the left and right cosets of $H \subseteq G$ coincide and are written

$$H + a = \{h + a \mid h \in H\}.$$

Here, the coset relation becomes

$$H + a = H + b \iff a - b \in H \iff a \in H + b.$$

Definition. When a group G is a union of finitely many left cosets of a subgroup H, we say that H *has finite index in G* and the *index of H in G* is defined to be

$$[G : H] = \text{number of distinct left cosets of } H \text{ in } G.$$

The same holds for right cosets. When G is finite, $[G : H] = |G|/|H|$, since all cosets of H have the same number of elements.

Normal Subgroups

Theorem. Given a subgroup $H \subseteq G$, H being normal in G is equivalent to any of the following conditions:

- $gH = Hg$ for all $g \in G$.
- $gHg^{-1} = H$ for all $g \in G$.
- $ghg^{-1} \in H$ for all $g \in G$ and $h \in H$.

Corollary. When $N \subseteq G$ is a normal subgroup, every left coset is a right coset, and vice versa.

Theorem. The set of all cosets of N in G forms a group and is denoted G/N. The group operation is defined by $Na \cdot Nb = Nab$, which is well-defined since N is normal. When G is finite, G/N is also finite and $|G/N| = [G : N] = |G|/|N|$.

Group Homomorphisms

Definition. Let G and H be groups and let $\phi : G \to H$ be a function. We say that ϕ is a *homomorphism* if for all $a, b \in G$,

$$\phi(ab) = \phi(a)\phi(b).$$

Theorem. If $\phi : G \to H$ is a homomorphism, then

- $\phi(e_G) = e_H$.
- $\phi(g^n) = \phi(g)^n$ for all $g \in G$ and $n \in \mathbb{Z}$.