INTRODUCTION TO ALGEBRA — HANDOUT 7

1. Structures with one binary operation

Definition 1. Algebraic structure $\langle S, \cdot \rangle$ is a **semigroup** if $\cdot$ is an associative binary operation on S, i.e.

$$\forall abc \;\; a \cdot (b \cdot c) = (a \cdot b) \cdot c.$$

Definition 2. A semigroup is called **monoid** if there is an identity element in it, i.e.,

$$\exists e \forall a \;\; a \cdot e = e \cdot a = a.$$

Definition 3. Algebraic structure $\langle G, \cdot \rangle$ is a **group** if it is a monoid in which every element has an inverse, i.e.,

$$\forall a \exists a^{-1} \;\; a \cdot a^{-1} = a^{-1} a = e.$$

Definition 4. Commutative groups are often called **abelian** groups.

Example 1.

(1) Finite text over an alphabet form a semigroup (monoid) with respect to concatenation.
(2) Odd numbers with multiplication $\langle 2\mathbb{Z} + 1, \cdot \rangle$ is a monoid.
(3) Even numbers with addition $\langle 2\mathbb{Z}, + \rangle$ is a group.
(4) $\langle \mathbb{Z}, \cdot \rangle$ is a monoid.
(5) $\langle \mathbb{Z}, + \rangle$ is an abelian group ($e = 0$ and $a^{-1} = -a$).
(6) $\langle \{0\}, + \rangle \cong \langle \{1\}, \cdot \rangle$ is an abelian group (up to isomorphism the only one element group).
(7) $\langle \{-1, 1\}, \cdot \rangle$ is an abelian group (up to isomorphism the only two element group).
(8) $\langle \{-1, 1, i, -i\}, \cdot \rangle$ is an abelian group (where $i = \sqrt{-1}$).
(9) Positive real (or rational) numbers with multiplication is an abelian group.
(10) Nonzero real (or rational or complex) numbers with multiplication is an abelian group.
(11) Permutations (bijections) of any set with respect of composition is a group. The group of permutations of an n element set is denoted by S_n.
(12) The isometries of the plane with respect to composition is a group.
(13) Symmetries of a geometric shape with composition form a group.
(14) Let $a \sim b$ iff $m | b - a$ and let $\mathbb{Z}_m = \mathbb{Z}/\sim$. Then $\langle \mathbb{Z}_m, + \rangle$ is an abelian group.

Proposition 1. Let G be a group.

(1) If $f \cdot x = x \cdot f = x$ for all $x \in G$, then $f = e$.
(2) If $a \cdot b = e$, then $b = a^{-1}$ and $a = b^{-1}$.
(3) If $ax = bx$, then $a = b$ (right cancelation).
(4) If $ya = yb$, then $a = b$ (cancelation).
(5) $(a^{-1})^{-1} = a$ and $(ab)^{-1} = b^{-1}a^{-1}$.

Definition 5. A nonempty subset H of group G is a **subgroup** of G, in symbols $H \leq G$ if

- If $a, b \in H$, then $a \cdot b \in H$.
- $e \in H$.
- If $a \in H$, then $a^{-1} \in H$.

Example 2.

(1) $\langle Z, +\rangle \leq \langle \mathbb{Q}, +\rangle \leq \langle \mathbb{R}, +\rangle \leq \langle \mathbb{C}, +\rangle$
(2) $\langle \{1\}, \cdot\rangle \leq \langle \{-1, 1\}, \cdot\rangle \leq \langle \{-1, 1, i, -i\}, \cdot\rangle \leq \langle \mathbb{C}\{0\}, \cdot\rangle$
(3) $\begin{array}{ccccc} & & \langle 2\mathbb{Z}, +\rangle & & \\ & \leq & & \leq & \\ \langle 6\mathbb{Z}, +\rangle & & & & \langle \mathbb{Z}, +\rangle \\ & \leq & & \leq & \\ & & \langle 3\mathbb{Z}, +\rangle & & \end{array}$
(4) The translations of the plane is a subgroup of the isometries of the plane.
(5) The isometries of the plane fixing the origin is a subgroup of the isometries of the plane.

Exercise 1. Prove that $\emptyset \neq H \subseteq G$ is a subgroup of group G if and only if $a, b \in H$ implies $ab^{-1} \in H$.

Let us note that the intersection of subgroups is a subgroup.

Definition 6. Let X be a subset of group G. The intersection of subgroups containing X is called the **subgroup generated by** X and it is denoted by $\langle X\rangle$.

Theorem 1. Let $L(G)$ be the set of subgroups of a group G. $L(G)$ is a lattice with respect to inclusion.

Proof. $H \wedge K = H \cap K$ and $H \vee K = \langle H \cup K\rangle$. □

Definition 7. Let A and B two nonempty subsets of group G.

$$AB := \{ab : a \in A \text{ and } b \in B\} \qquad A^{-1} := \{a^{-1} : a \in A\}$$

Notation: we write aB in place of $\{a\}B$.

Let us note $HH = H$ and $H^{-1} = H$ if H is a subgroup.

Proposition 2. Let G be a group and let H be an arbitrary subset of G. Let relation $a \sim b$ hold iff $a^{-1}b \in H$. Then

- $\sim$ is an equivalence relation.
- The equivalence class of $a \in G$ is aH. The equivalence classes are called **left cosets**.
- $|aH| = |H|$ for all $a \in G$.

The notion of **right cosets** can be introduced analogously.

Definition 8. The number of left cosets is called the **index** of H in G, denoted by $[G : H]$.

Theorem 2 (Lagrange)**.** Let G be a finite group and let $H \leq G$ be an arbitrary subgroup of G. Then

$$|G| = |H|[G : H].$$

Corollary 1. If $|G| = n$, then $a^n = e$ for all $a \in G$.

Definition 9. Let $a \equiv b \ (mod\ m)$ denote the equivalence relation on positive integers defined as $m|b - a$.

Proposition 3. If $a \equiv b \ (mod\ m)$ and $c \equiv d \ (mod\ m)$, then

- $a + c \equiv b + d \ (mod\ m)$ and
- $ac \equiv bd \ (mod\ m)$.

Definition 10. Positive integers m and n are called **coprime** if 1 is the only common divisor of m and n. **Euler ϕ-function** is the function that maps positive integer n to the number of coprimes primes less than n.

The residue classes coprime to m is a group having $\phi(m)$ elements. Consequently:

Theorem 3 (Euler)**.** Let a and m be coprime, then $a^{\phi(m)} \equiv 1 \ (mod\ m)$.

Let us note that $\phi(p) = p - 1$ if p is a prime. Consequently:

Theorem 4 (Fermat)**.** $a^p \equiv a \ (mod\ p)$.

Definition 11. Two elements a and b of a group G are called **conjugate** if there is an element g of G such that $a = gbg^{-1}$.

Exercise 2. Prove that being conjugate is an equivalence realtion on G.

Definition 12. A subgroup N of G is called a **normal subgroup**, in symbols $N \triangleleft G$, $gng^{-1} \in N$ for all $g \in G$ and $n \in N$.