Week 8
Groups
Discrete Math

Marie Demlová
http://math.fel.cvut.c/zen/people/demlova

April 7, 2022

Groups

Groups. A monoid $(S, \circ, e)$ in which every element is invertible is called a group.

Examples of groups.

- The monoid $(\mathbb{R}, +, 0)$. Indeed, for every $x \in \mathbb{R}$ there exists $-x$ for which $x + (-x) = 0 = (-x) + x$.
- The monoid $(\mathbb{Z}, +, 0)$. Indeed, for each integer x there exists an integer $-x$ for which $x + (-x) = 0 = (-x) + x$.
- The monoid $(\mathbb{R}^+, \cdot, 1)$, where $\mathbb{R}^+$ is the set of all positive real numbers. Indeed, for every positive real number x there exists a positive real number $\frac{1}{x}$ for which $x \cdot \frac{1}{x} = 1 = \frac{1}{x} \cdot x$.
- The monoid $(\mathbb{Z}_n, \oplus, [0]_n)$. Indeed, for a class $[i]_n$ there exists a class $[n-i]_n$ for which $[i]_n \oplus [n-i]_n = [0]_n = [n-i]_n \oplus [i]_n$.

Groups

Examples.

- The monoid $(\mathbb{Z}, \cdot, 1)$ is not a group. Indeed, for example 2 is not invertible.
- The monoid $(\mathbb{Z}_n, \odot, [1]_n)$ is not a group. Indeed, the class $[0]_n$ is not invertible because for any $[i]_n$ we have $[0]_n \odot [i]_n = [0]_n \neq [1]_n$.
- Let A be the set of all permutation of $\{1, 2, \ldots, n\}$, and let $\circ$ be the composition. Then $(A, \circ)$ is a group. Indeed, it is a monoid with the neutral element id; moreover, every permutation ϕ has its inverse permutation ϕ^{-1}.
- Let B be the set of all mappings from the set $\{1, 2, \ldots, n\}$ into itself, where $n > 1$. Let $\circ$ be the composition. Then $(B, \circ, id)$ is not a group; indeed, it is a monoid but any mapping that is not one-to-one is not invertible.

Groups

Proposition. Given a group $(S, \circ)$ with its neutral element e. Then for every two elements $a, b \in S$ there exist unique $x, y \in S$ such that

$$a \circ x = b, \qquad y \circ a = b.$$

Theorem.

A semigroup $(S, \circ)$ is a group if and only if every equation of the form $a \circ x = b$ and every equation of the form $y \circ a = b$ has at least one solution.

More precisely: A semigroup $(S, \circ)$ is a group if and only if for every two elements $a, b \in S$ there exist $x, y \in S$ such that $a \circ x = b$ and $y \circ a = b$.

Groups

Commutative semigroups, monoids, groups.

A semigroup $(S, \circ)$ (monoid, group) is called commutative if it satisfies the *commutative law*, i.e. for every two elements $x, y \in S$

$$x \circ y = y \circ x.$$

Subsemigroups, Submonoids

Subsemigroup.

Given a semigroup $(S, \circ)$. A subset $T \subseteq S$ together with an operation $\circ$ forms a subsemigroup of the semigroup $(S, \circ)$, if for every two elements $x, y \in T$ we have $x \circ y \in T$. (In this case $(T, \circ)$ is also a semigroup.)

Examples of subsemigroups.

- $\mathbb{N}$ together with addition forms a subsemigroup of $(\mathbb{Z}, +)$.
- The set of all regular matrices together with multiplication of matrices forms a subsemigroup of $(M_n, \cdot)$, where M_n is the set of all square matrices of order n.
- The set of all positive real numbers together with multiplication forms a subsemigroup of $(\mathbb{R}, \cdot)$.

Subsemigroups, Submonoids

Submonoid. Given a monoid $(S, \circ, e)$. A subset $T \subseteq S$ forms a submonoid if it forms a subsemigroup and moreover $e \in T$.

Examples of submonoids.

- The set of all natural numbers $\mathbb{N}$ together with addition is a submonoid of $(\mathbb{Z}, +, 0)$, since $0 \in \mathbb{N}$.
- The set of all regular square matrices of order n together with multiplication of matrices forms a submonoid of $(M_n, \cdot, E)$, since the identity matrix E is regular.
- Denote by T_X the set of all mappings from a set X into itself, let $\circ$ be the composition. Then $(T_X, \circ, id)$ where id is the identity mapping is a monoid. The set of all bijections from T_X forms a submonoid of $(T_X, \circ)$, indeed, a composition of two bijections is a bijection, and the identity mapping is a bijection.

Applications to Residue Classes Modulo n

Euler function.

Given a natural number $n > 1$. Then the value of Euler function $\phi(n)$ equals to the number of all natural numbers i, $0 \leq i < n$, that are relatively prime to n.

For example $\phi(6) = 2$, since there are only two natural numbers between 0 and 5 that are relatively prime to 6, namely 1 and 5.

Properties of Euler Function.

- Let p be a prime number, then $\phi(p) = p - 1$.
- If p is a prime number and $k \geq 1$ then $\phi(n) = p^k - p^{k-1}$.
- If n and m are relatively prime natural numbers then $\phi(n \cdot m) = \phi(n) \cdot \phi(m)$.

Applications to Residue Classes Modulo n

The Group of Invertible Elements of $(\mathbb{Z}_n, \cdot, 1)$.

$(\mathbb{Z}_n, \cdot)$ is a monoid with its neutral element 1. The set of all invertible elements of it is

$$\mathbb{Z}_n^\star = \{i \mid 0 \leq i < n, \quad i \text{ and } n \text{ are relatively prime}\}.$$

Therefore, $(\mathbb{Z}_n^\star, \cdot, 1)$ is a group with $\phi(n)$ elements.

Theorem (Euler-Fermat).

Given a natural number $n > 1$. Then for every integer a relatively prime to n we have

$$a^{\phi(n)} \equiv 1 \,(\mod n).$$

Subgroups

A subgroup. Given a group $(G, \circ, e)$. We say that $H \subseteq G$ forms a subgroup of $(G, \circ, e)$ if

- for every $x, y \in H$ it holds that $x \circ y \in H$, (i.e. forms a subsemigroup);
- $e \in H$, (i.e. forms a submonoid);
- for every $x \in H$ it holds that $x^{-1} \in H$.

Theorem. Let $(G, \circ, e)$ be a finite group and $H \subseteq G$ its subgroup. Then the number of elements of H divides the number of elements of G.

Groups

Let $(G, \circ, e)$ be a finite group, $a \in G$. Consider the set of all powers of a:

$$\{a, a^2, a^3, \ldots, a^k, \ldots\}.$$

Since G is a finite set, there must exist i and j, $i < j$, such that $a^i = a^j$. There is a^{-1}. Therefore

$$a^i = a^j \text{ implies } a^{i-1} = a^{j-1}, \text{ etc. } e = a^0 = a^{j-i}.$$

Proposition. Let $(G, \circ, e)$ be a finite group, $a \in G$. Then there exists the smallest positive integer r for which $a^r = e$. Moreover, $\{a, a^2, \ldots, a^r\}$ forms a subgroup of $(G, \circ, e)$.

Groups

The subgroup formed by $\{a, a^2, \ldots, a^r\}$ is the subgroup generated by a and is denoted by $\langle a \rangle$.

The smallest positive r for which $a^r = e$ is the order of a and it is denoted by $r(a)$. Note that $r(a) = |\langle a \rangle|$.

Corollary. Given a finite group $(G, \circ, n)$ with n elements. Then the order of any element $a \in G$ divides n.

Theorem.

Given a finite group $(G, \circ, e)$ with n elements. Then for every $a \in G$ we have

$$a^n = e.$$

Subgroups

Proposition.

A number r equals to the order $r(a)$ of a in a finite group $(G, \cdot, e)$ if and only if the following two conditions are satisfied:

- $a^r = e$.
- If $a^s = e$ for some natural number s then r divides s.