Week 9
Groups
Discrete Math

Marie Demlová
http://math.fel.cvut.cz/en/people/demlova

April 14, 2022

Groups

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

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.

Subgroups

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 $(G, \circ, e)$.

Subgroups

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 $r(a) = |\langle a \rangle|$.

Proposition. 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.

Subgroups

Proposition.

Let $\mathcal{G} = (G, \circ, e)$ be a finite group. Let $a \in G$ have order $r(a)$. Then

$$r(a^i) = \frac{r(a)}{\gcd(r(a), i)}.$$

Cyclic groups

A cyclic group. Given a group $\mathcal{G} = (G, \circ, e)$. If there exists an element $a \in G$ for which $\langle a \rangle = G$ we say that the group is cyclic and that a is a generating element of $(G, \circ, e)$.

Examples.

- $(\mathbb{Z}_n, +, 0)$ (for any natural number $n > 1$) is a cyclic group with its generating element 1.
- For every prime number p the group $(\mathbb{Z}_p^\star, \cdot, 1)$ is a cyclic group. It is not straightforward to show it. Moreover, to find a generating element is a difficult task for some primes p.
- The group $(\mathbb{Z}_8^\star, \cdot, 1)$ **is not** cyclic. We have $\mathbb{Z}_8^\star = \{1, 3, 5, 7\}$ and there is no element with order 4.

Cyclic groups

Proposition.

Given a finite cyclic group $\mathcal{G} = (G, \circ, e)$ with n elements. Then for every natural number d which divides n there exists a subgroup of $\mathcal{G}$ with d elements.

Remark.

A finite cyclic group has only subgroups that itself are cyclic.

Exercises

Exercise 1.
Given a group $(\mathbb{Z}_{17}^{\star}, \cdot, 1)$. Find the order of 2. Is 2 a generating element? Write down $\langle 2 \rangle$ in $\mathbb{Z}_{17}^{\star}$.

Exercise 2.
Given a group $(\mathbb{Z}_{17}^{\star}, \cdot, 1)$. Find all its generating elements.

Exercises

Exercise 3.
Given a group $(\mathbb{Z}_{17}^{\star}, \cdot, 1)$. Find all its subgroups.

Exercise 4.
Given a group $(\mathbb{Z}_{14}^{\star}, \cdot, 1)$.

a) Write down all its elements.

b) Find orders $r(a)$ for all its elements.

c) Is the group a cyclic group?

d) Find all its subgroups.