Lagrange's Theorem

Hlib Dmytriiev, Pavlo Shekhet, Maria Matsiiako

Mentor: Ivan Yakovlev

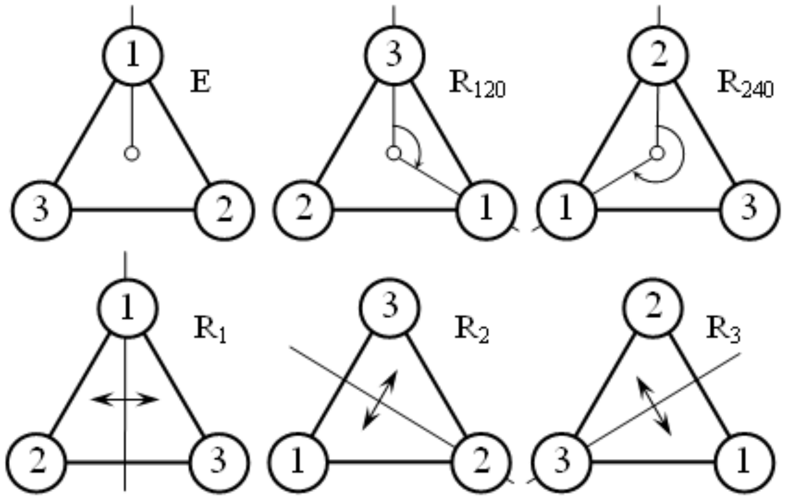
Group

A set *G* of elements of an arbitrary nature, on which can be defined a binary operation such that the following conditions are satisfied, is called a **group**:

1. Associativity: $(ab)c = a(bc)$ for any elements a, b and c of G;
2. In G, there is a unit element e such that $ae = ea = a$ for every element a of G;
3. For every element a of G there is an element $a^{-1} \in G$, an inverse of element a, such that $aa^{-1} = a^{-1}a = e$.

Examples:

✅ All real positive numbers form a group under multiplication
❌ All natural numbers don't form a group under addition (no unit and inverse elements) and multiplication (no inverse elements)
✅ Group D3 (dihedral) can be illustrated by triangle symmetries (6 symmetries: 3 rotations and 3 axial symmetries)



Main Theorem

Let G be a finite group, $g \in G$, $n = |G|$.

$$g^n = e$$

Fermat's Little Theorem

Let p be a prime number and a be an integer number that a is not divisible by p.
Then, $a^{p-1} \equiv 1 \pmod{p}$.

Subgroups

Definition

> A subgroup H is a part of group G ($H \subseteq G$);
> H is a group under a defined operation in the G group.

Lemmas

If H is a subgroup, it satisfies a few rules:

1. If $a,b \in H$, then the element $ab \in H$.
2. When e is a unit element in group G, it is a unit element in a subgroup H.
3. When $a \in H$, then $a^{-1} \in H$.

Lagrange's Theorem

Let's define (right/left) **cosets** as a set of elements $\{xh/hx\}$ defined under a group *G*, where *x* is an element of *G* and *h* runs over all elements of subgroup *H*.

The number of elements in the group (order) G is the product of a multiplication of the number of elements in the subgroup (order) H and the number of (left/right) compatible classes.

Let us denote the order of group *G* as $|G|$,
the order of a subgroup *H* as $|H|$,
the number of (left/right) cosets as $|G/H|$.

Then we get the equation:
$|G| = |H| \cdot |G/H|$ **or** $|G| = |H| \cdot |H\backslash G|$

Equivalence Relation

We can prove Lagrange's theorem *using cosets* or *using the link between cosets and equivalence classes*.

— A **binary relation** over sets X and Y is a new set of ordered pairs (x, y) consisting of elements x in X and y in Y.

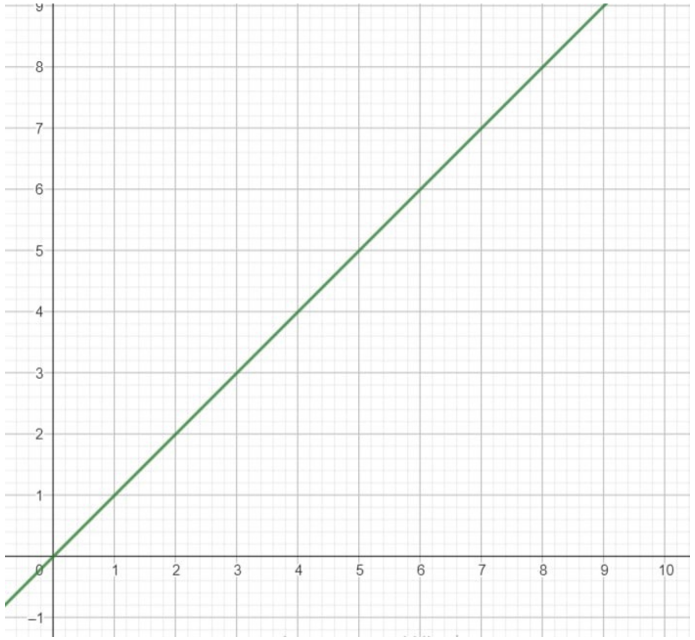
Definition

1. **Reflection**: $a \sim a$.
2. **Symmetry**: $a \sim b$, *if and only if* $b \sim a$.
3. **Transitivity**: $a \sim b$ and $b \sim c$, then $a \sim c$.

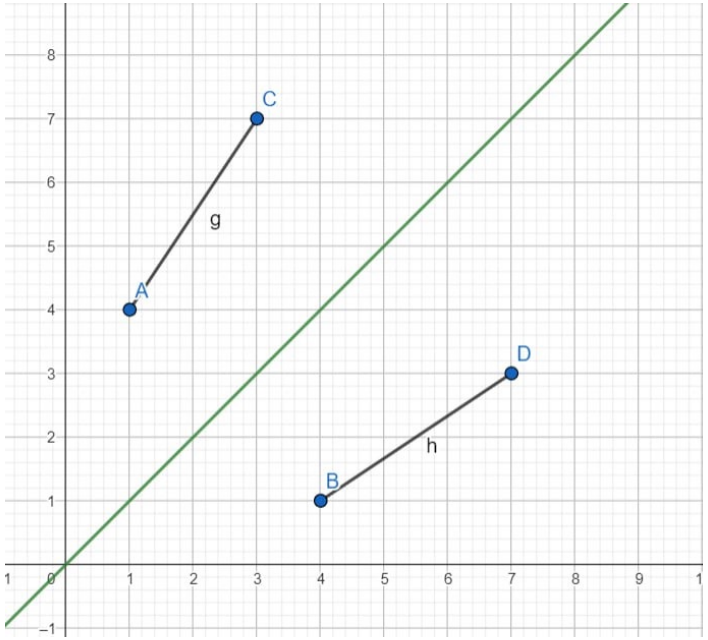
— An **equivalence relation** is a binary operation that is reflexive, symmetric and transitive.

An example is the relation "is equal to".

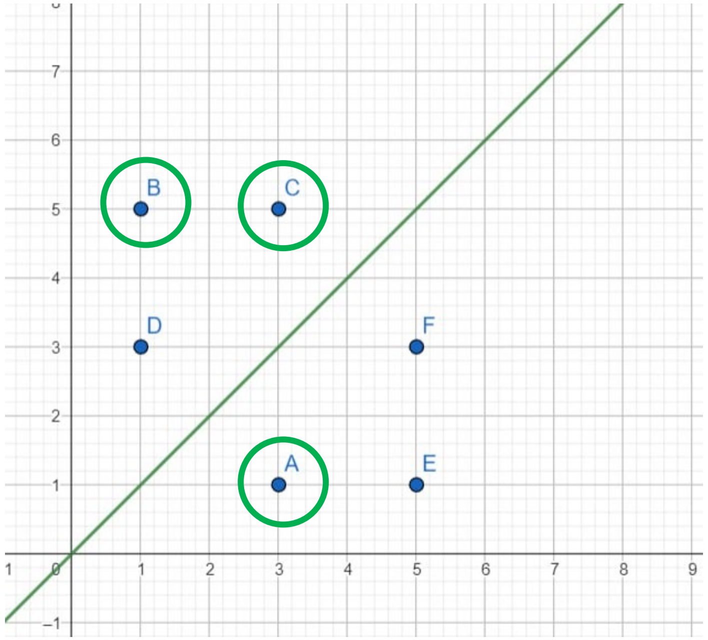
Equivalence Relation



Reflection



Symmetry



Transitivity

Statements we need to prove Lagrange's Theorem

$^2/_3$

1) **Let us introduce a binary relation on the group G like this.** $\boldsymbol{g_1 = h \cdot g_2}$, where $h_i \in H$, and $g_i \in G$.

1. $g_1 \sim g_1$. $g_1 = h \cdot g_1$: h = e
2. $g_1 \sim g_2$ if and only if $g_2 \sim g_1$: $g_1 = h \cdot g_2$ and $g_2 = h^{-1} \cdot g_1$.
3. $g_1 \sim g_2$ and $g_2 \sim g_3$, then $g_1 \sim g_3$: $g_1 = h_1 \cdot g_2$, $g_2 = h_2 \cdot g_3$, then $g_1 = h_1 h_2 \cdot g_3$

This binary relation is equivalence relation!

2) Show that any relation breaks the set into pieces - equivalence classes. S_x - the equivalence class of a number x, such a subset which consists of those y such that $x \sim y$.

If equivalence classes $\boldsymbol{S_x \cap S_y}$, then they coincide:

$z \in S_x \cap S_y$. Then, $x \sim z$, $y \sim z$, $\Rightarrow x \sim y$.

Let us choose an element u from S_x. $x \sim u$, $x \sim y \Rightarrow u \sim x$ (therefore, all elements from S_x are in S_y).

We can similarly prove, on the other hand, that $S_y \subseteq S_x$. We set a partition of group G.

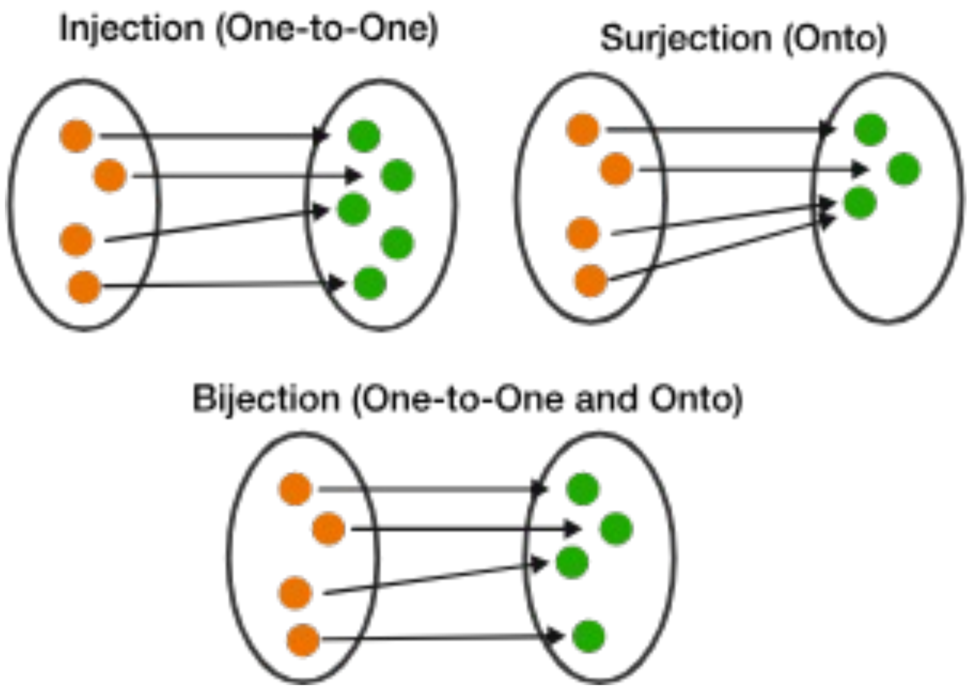
Injection, Surjection, Bijection

Definition

The **injection** is a type of mapping between two sets where all elements of the second set have only one pair or no pair in the first set.

The **surjection** is a type of mapping between two sets where all elements of the second set have at least one pair in the first set.

The **bijection** is a type of mapping between two sets where all elements of the second set have only one pair in the first set and vice versa.



Statements we need to prove Lagrange's Theorem

3) **There is a bijection between the left coset *gH* and the subgroup *H*.**

$h \in H$, $gh \in gH$

1. $h \xrightarrow{g\circ} gh$
2. $gh \xrightarrow{g^{-1}\circ} h$

$|H| = |gH|$

The whole group G is split into disjoint pieces, equivalence classes, each of which has $|H|$ elements.

Therefore, $\boldsymbol{|G| = |H| \cdot |G/H|}$

The Main Theorem

Back to the main goal of our project, we need to prove that $g^n = e$, where g ∈ G, |G| = n, using Lagrange's Theorem.

Definition

The **order of an element** is the smallest integer n such that the element $g^n = e$. If such an integer does not exist, then g is an element of infinite order.

Since the group is finite, then the element g has an order - a finite natural number k, so $g^k = e$. If $g \in G$, then the set of all elements of type g^m ($m \in \mathbb{Z}$) is a subgroup of G (this subgroup is cyclic). Let's call it $<g>$. Using Lagrange's theorem, $n = k \cdot |G/H|$.
Then we can exponentiate an element g to the power n:

$$g^n = g^{kr} = e^r = e$$

Fermat’s Little Theorem

Let p be a prime number and a be an integer number, that a is not divisible by p.
Then, $a^{p-1} \equiv 1 \pmod{p}$.

Let’s prove it:

Let's take the multiplicative group of residues prime modulo p – $Z_p{}^*$. This group consists of elements from *1* to p - 1. The order of any element is p - 1**,** and the unit element is 1. Using the theorem from number theory, $\boldsymbol{a \equiv b \Rightarrow a^n \equiv b^n}$.

$$\boldsymbol{a^{p-1} \equiv [a]^{p-1} \equiv 1 \pmod{p}}$$

We use the main theorem to say that any element $[a] \in Z_p{}^*$ in the power p - 1 is equivalent to the unit element (1).

Thank you for your attention!

Glory to Ukraine!

Слава Україні!