ALGEBRA I (LECTURE NOTES 2017/2018)
LECTURE 5 - THE LAGRANGE THEOREM

PAVEL RŮŽIČKA

5.1. **Lagrange theorem.** Let $\boldsymbol{G} = (G, \cdot)$ be a grupoid. We set

$$A \cdot B := \{a \cdot b \mid a, b \in G\}, \tag{5.1}$$

for all $A, B \subseteq G$. We will abuse our notation writing $a \cdot B$ and $A \cdot b$ respectively instead of $\{a\} \cdot B$ and $A \cdot \{b\}$, when one of the sets has a single element.

Given a set G, we put $\mathcal{P}(G) := \{A \mid A \subseteq G\}$, i.e., $\mathcal{P}(G)$ denotes the set of all subsets of G. Observe that if $\boldsymbol{G} = (G, \cdot)$ is a semigroup, the operation $\cdot$ defined by (5.1) on the set $\mathcal{P}(G)$ is associative, and so $\boldsymbol{\mathcal{P}(G)} = (\mathcal{P}(G), \cdot)$ is a semigroup as well. Moreover, if $\boldsymbol{G}$ has a unit, say u, then $\{u\}$ is a unit of $\boldsymbol{\mathcal{P}(G)}$.

Exercise 5.1. *Let $\boldsymbol{G} = (G, \cdot)$ be a finite group and A, B subsets of G.*

(i) *Prove that if $|A| + |B| > |G|$, then $A \cdot B = G$.*
(ii) *Use (i) to prove that every element of a finite field is a sum of two squares.*

Definition 5.1. Let $\boldsymbol{G} = (G, \cdot)$ be a group and $\boldsymbol{H}$ a subgroup of $\boldsymbol{G}$. The sets $g \cdot H$ and $H \cdot g$, $g \in G$, respectively are called *left cosets* and *right cosets* of $\boldsymbol{H}$.

Lemma 5.2. *Let $\boldsymbol{G} := (G, \cdot)$ be a group and H a sub-universe of $\boldsymbol{G}$ containing the unit. For each $f, g \in G$, the following are equivalent:*

(i) $g^{-1} \cdot f \in H$,
(ii) $f \in g \cdot H$,
(iii) $f \cdot H \subseteq g \cdot H$,

Proof. $(i) \Rightarrow (ii)$ If $g^{-1} \cdot f \in H$, then $g = g \cdot (g^{-1} \cdot f) \in f \cdot H$. $(ii) \Rightarrow (iii)$ Since H is a sub-universe of $\boldsymbol{G}$, $h \cdot H \subseteq H$, for all $h \in H$. If $f \in g \cdot H$, then $f = g \cdot h$, for some $h \in H$. It follows that $f \cdot H = g \cdot h \cdot H \subseteq g \cdot H$. $(iii) \Rightarrow (i)$ Assume that $f \cdot H \subseteq g \cdot H$. Left multiplying by g^{-1} gives that $g^{-1} \cdot f \cdot H \subseteq H$. Since the unit u belongs to H, we conclude that $g^{-1} \cdot f = g^{-1} \cdot f \cdot u \in g^{-1} \cdot f \cdot H \subseteq H$. $\square$

Date: October 31, 2017.

Given a group $\boldsymbol{G} := (G, \cdot)$. For each $H \subseteq G$ we define a binary relation $\equiv_H$ on G by

$$f \equiv_H g \text{ if } g^{-1} \cdot f \in H, \text{ for all } f, g \in G. \tag{5.2}$$

Lemma 5.3. *Let $\boldsymbol{G} := (G, \cdot)$ be a group. If $\boldsymbol{H}$ is a subgroup of $\boldsymbol{G}$, then $\equiv_H$ is an equivalence relation and blocks of $\equiv_H$ correspond to left cosets of $\boldsymbol{H}$.*

Proof. Since $\boldsymbol{H}$ is a subgroup, the set H is closed under inverses, and so the relation $\equiv_H$ is symmetric. Indeed if $g^{-1} \cdot f \in H$, then $f^{-1} \cdot g = (g^{-1} \cdot f)^{-1} \in H$, for all $f, g \in G$. The reflexivity and transitivity of $\equiv_H$ follows readily from Lemma 5.2$(i) \Leftrightarrow (iii)$. We conclude that $\equiv_H$ is an equivalence.

It follows from Lemma 5.2$(ii) \Rightarrow (i)$ that if $f \in g \cdot H$, then $f \equiv_H g$. Consequently, each coset is contained in a single block of $\equiv_H$. Conversely, if $g \in k \cdot H$ and $f \equiv_H g$, for some $f, g, k \in G$, then $f \in g \cdot H \subseteq k \cdot H$, due to Lemma 5.2 $(i) \Rightarrow (ii) \Rightarrow (iii)$. Therefore each coset is a union of blocks. We conclude that each coset equals to a single block of $\equiv_H$. $\square$

Lemma 5.4. *Let $\boldsymbol{G} := (G, \cdot)$ be a group and $\boldsymbol{H}$ a subgroup of $\boldsymbol{G}$. Then all left cosets of $\boldsymbol{H}$ have the same size. In particular, $|g \cdot H| = |H|$, for all $g \in G$.*

Proof. Let $g \in G$. It suffices to verify that the map $H \to g \cdot H$ given by $h \mapsto g \cdot h$ is a bijection. It clearly maps H onto $g \cdot H$. If $g \cdot h = g \cdot h'$, for some $h, h' \in H$, then $h = h'$ due to left cancellativity of the group operation. Therefore the map is one-to-one. $\square$

Remark 5.5. We could argue similarly for right cosets instead of left ones. In particular, the right cosets form a partition and they are all of the same size. In fact, since H is both a right and left coset, the size of each right coset equals to the size of any left coset.

Definition 5.6. Let $\boldsymbol{H}$ be a subgroup of a group $\boldsymbol{G}$. The number of left cosets of $\boldsymbol{H}$ is denoted by $[\boldsymbol{G} : \boldsymbol{H}]$ and it is the *index* of $\boldsymbol{H}$ in $\boldsymbol{G}$.

Exercise 5.2. *Observe that the unit permutation and the transposition $(1, 2)$ form a subgroup, say $\boldsymbol{T}$ of $\boldsymbol{S_3}$. Compute all left and right cosets of $\boldsymbol{T}$.*

Since left cosets of $\boldsymbol{H}$ form a partition of G and all have the same size, we get that

Theorem 5.7 (Lagrange)**.** *Let $\boldsymbol{H}$ be a subgroup of a group $\boldsymbol{G}$. Then*

$$|G| = [\boldsymbol{G} : \boldsymbol{H}]|H|.$$

In particular, if G is finite, then $|H|$ divides $|G|$.

Example 5.1. *Let $2 \leq n$ be an integer. If π and ρ are odd permutations from $\boldsymbol{S_n}$, then the permutation $\rho^{-1} \cdot \pi$ is even, due to Lemmas 3.6 and 3.10. Therefore $\pi \equiv_{A_n} \rho$, and so all odd permutations form a left coset of $\boldsymbol{A_n}$. We see that there are exactly two left cosets of $\boldsymbol{A_n}$, the left coset of all odd and the left coset of all even permutations; the latter corresponds to A_n. Hence $[\boldsymbol{S_n} : \boldsymbol{A_n}] = 2$, whence*

$$|A_n| = \frac{|S_n|}{2} = \frac{n!}{2},$$

due to the Lagrange theorem.