LECTURE 4
The Lagrange theorem, normal subgroups

PAVEL RŮŽIČKA

ABSTRACT. We define right and left cosets of a subgroup, say $\boldsymbol{H}$, of a group, say $\boldsymbol{G}$. We prove that all the left cosets of $\boldsymbol{H}$ have the size equal to the size of $\boldsymbol{H}$. We call the number of left cosets the index of the subgroup $\boldsymbol{H}$ and we denote the index by $[\boldsymbol{G} : \boldsymbol{H}]$. We prove the Lagrange theorem that $|G| = [\boldsymbol{G} : \boldsymbol{H}] \cdot |H|$. Finally we define a normal subgroup of a group and we show various equivalent characterizations of normal subgroups.

4.1. **The Lagrange theorem.** Given a grupoid $\boldsymbol{G} = (G, \cdot)$, we set

$$A \cdot B := \{a \cdot b \mid a, b \in G\}, \tag{4.1}$$

for all $A, B \subseteq G$. When one of the sets A, B is a singleton set, say $A = \{a\}$ or $B = \{b\}$, we will abuse our notation writing $a \cdot B$ or $A \cdot b$ instead of $\{a\} \cdot B$ or $A \cdot \{b\}$, respectively.

Given a set G, we will use the notation $\mathcal{P}(G) := \{A \mid A \subseteq G\}$ for the set of all subsets of G. Observe that if $\boldsymbol{G} = (G, \cdot)$ is a semigroup, the operation $\cdot$ defined by (4.1) 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 $\boldsymbol{\mathcal{P}(G)}$.

Definition 4.1. Let $\boldsymbol{H}$ be a subgroup of a group $\boldsymbol{G} = (G, \cdot)$. Sets $g \cdot H$ and $H \cdot g$, $g \in G$, will be called a *left cosets* and a *right cosets* of $\boldsymbol{H}$, respectively.

Lemma 4.2. *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 $g = g \cdot (g^{-1} \cdot f) \in g \cdot H$. $(ii) \Rightarrow (iii)$ 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 $g^{-1} \cdot f = g^{-1} \cdot f \cdot u \in g^{-1} \cdot f \cdot H \subseteq H$. □

The Lecture and the tutorial took place in Malá strana, room S11, on October 23, 2018.

Let $\boldsymbol{G} := (G, \cdot)$ be a group. Given a subset $H \subseteq G$, we define a binary relation $\equiv_H$ on G by $f \equiv_H g$ if $g^{-1} \cdot f \in H$, for all $f, g \in G$.

Lemma 4.3. *Let $\boldsymbol{H}$ be a subgroup of a group $\boldsymbol{G} = (G, \cdot)$. Then the binary relation $\equiv_H$ is an equivalence on G.*

Proof. Since $\boldsymbol{H}$ is a subgroup, the set H is closed under inverses. It follows that $g^{-1} \cdot f \in H$ if and only if $f^{-1} \cdot g = (g^{-1} \cdot f)^{-1} \in H$, for all $f, g \in G$. We conclude that the relation $\equiv_H$ is symmetric. Since H contains a unit element, say u, we have that $g^{-1} \cdot g = u \in H$ for every $g \in G$. It follows that $\equiv_H$ is reflexive. Finally, it follows from Lemma 4.2(i) $\Rightarrow$ (iii) that if $e \equiv_H f$ and $f \equiv_H g$, for some $e, f, g \in G$, then $e \cdot H \subseteq f \cdot H \subseteq g \cdot H$. Applying Lemma 4.2($iii$) $\Rightarrow$ (i), we conclude that $e \equiv_H g$, and so the relation $\equiv_H$ is transitive. We conclude that $\equiv_H$ is an equivalence relation. □

Lemma 4.4. *If $\boldsymbol{H}$ is a subgroup of a group $\boldsymbol{G} = (G, \cdot)$, then blocks of the equivalence $\equiv_H$ correspond to left cosets of $\boldsymbol{H}$.*

Proof. If $f \in g \cdot H$, then $f \equiv_H g$ due to Lemma 4.2(ii) $\Rightarrow$ (i) and the definition of $\equiv_H$. It follows that each left coset of $\boldsymbol{H}$ is contained in a block of $\equiv_H$.

Conversely, if $g \in e \cdot H$ and $f \equiv_H g$, for some $e, f, g, \in G$, then $f \in g \cdot H \subseteq e \cdot H$, due to Lemma 4.2 ($i$) $\Rightarrow$ (ii) $\Rightarrow$ (iii). It follows that each left coset of $\boldsymbol{H}$ is a union of blocks of $\equiv_H$. We conclude that a left coset of $\boldsymbol{H}$ equals to a single block of $\equiv_H$. □

Lemma 4.5. *Let $\boldsymbol{G} := (G, \cdot)$ be a group and $\boldsymbol{H}$ a subgroup of $\boldsymbol{G}$. Then*

$$|g \cdot H| = |H|$$

for all $g \in G$. In particular, all left cosets of $\boldsymbol{H}$ have the same size.

Proof. It suffices to verify that the map $h \mapsto g \cdot h$ form H to $g \cdot H$ is a bijection, for all $g \in G$. The map 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. □

Definition 4.6. Let $\boldsymbol{H}$ be a subgroup of a group $\boldsymbol{G}$. The number of left cosets of $\boldsymbol{H}$, denoted by $[\boldsymbol{G} : \boldsymbol{H}]$, is called the *index* of $\boldsymbol{H}$ in $\boldsymbol{G}$.

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

Theorem 4.7 (Lagrange)**.** *Let $\boldsymbol{H}$ be a subgroup of a group $\boldsymbol{G}$. Then*

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

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

Example 4.8. *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.

4.2. **The left-right symmetry and normal subgroups.** Let $\boldsymbol{H}$ be a subgroup of a group $\boldsymbol{G}$. Similarly as left cosets the right cosets of $\boldsymbol{H}$ form a partition of G and all of them are of the same size equal to the size of H. In particular, H itself is both a left and a right coset of $\boldsymbol{H}$.

Let $\equiv_H^r$ be a binary relation on G defined by $f \equiv_H^r g$ if $g \cdot f^{-1} \in H$. As in the proofs of Lemmas 4.3 and 4.4 we show that $\equiv_H^r$ is an equivalence relation and that blocks of $\equiv_H^r$ correspond to right cosets of $\boldsymbol{H}$.

Lemma 4.9. *Let* $\boldsymbol{H}$ *be a subgroup of a group* $\boldsymbol{G}$*. The map* $g \cdot H \mapsto H \cdot g^{-1}$ *is a bijection from the set of all left cosets of* $\boldsymbol{H}$ *to the set of right cosets of* $\boldsymbol{H}$*.*

Proof. Let $g \in G$. Since $\boldsymbol{H}$ is closed under inverses, we infer from Lemma 4.2 that

$$f \in g \cdot H \iff g^{-1} \cdot f \in H \iff f^{-1} \cdot (g^{-1})^{-1} \in H \iff g^{-1} \in H \cdot f^{-1},$$

for all $f \in G$. Indeed, $(g^{-1} \cdot f)^{-1} = f^{-1} \cdot (g^{-1})^{-1}$. This proves the lemma. □

It follows from Lemma 4.9 that the size of the set of all left cosets of $\boldsymbol{H}$ (which is by the definition the index of $\boldsymbol{H}$ in $\boldsymbol{G}$) equals the size of the set of all right cosets of $\boldsymbol{H}$.

However left and right cosets of a subgroup might not coincide. This is the case of a two-element subgroup of the symmetric group $\boldsymbol{S_3}$ due to Exercise 4.2.

Definition 4.10. A subgroup $\boldsymbol{N}$ of a group algebra G is *normal*, (which we denote by $\boldsymbol{N} \trianglelefteq \boldsymbol{G}$) provided that each right coset of $\boldsymbol{N}$ is also a left coset of $\boldsymbol{N}$.

Observe that every subgroup of an abelian group is normal.

Lemma 4.11. *Let* $\boldsymbol{N}$ *be a subgroup of a group* $\boldsymbol{G}$*. The following are equivalent:*

(i) $\boldsymbol{N}$ *is a normal subgroup of* $\boldsymbol{G}$*;*
(ii) $g \cdot N \cdot g^{-1} \subseteq N$*, for all* $g \in G$*.*
(iii) $g \cdot N \cdot g^{-1} = N$*, for all* $g \in G$*.*
(iv) $g \cdot N = N \cdot g$*, for all* $g \in G$*;*

Proof. *(i)* ⇒ *(ii)* Let u denote the unit of $\boldsymbol{G}$. If $\boldsymbol{N} \trianglelefteq \boldsymbol{G}$, the left coset $g \cdot N$ is a right coset, that is, $g \cdot N = N \cdot f$, for some $f \in G$. It follows that $g = g \cdot u = n \cdot f$, hence $n^{-1} = f \cdot g^{-1}$, for some $n \in N$. In particular, $f \cdot g^{-1} \in N$. Therefore $g \cdot N \cdot g^{-1} = N \cdot f \cdot g^{-1} \subseteq N \cdot N \subseteq N$. *(ii)* ⇒ *(iii)* Let $g \in G$. Then (ii) implies that $g^{-1} \cdot N \cdot g \subseteq N$. Multiplying by g from the left and by g^{-1} from the right we get that $N \subseteq g \cdot N \cdot g^{-1}$. The opposite inclusion $g \cdot N \cdot g^{-1} \subseteq N$ follows from (ii). Implication $(iii) \Rightarrow (iv)$ is proved by multiplying by g from the right. Implication $(iv) \Rightarrow (i)$ is trivial. □

Given a normal subgroup $\boldsymbol{N}$ of a group $\boldsymbol{G}$ we will call left (right) cosets of $\boldsymbol{N}$ simply cosets of $\boldsymbol{N}$.

Lemma 4.12. *Let $\boldsymbol{N}$ be a normal subgroup of a group $\boldsymbol{G}$. The product of cosets of $\boldsymbol{N}$ is a coset of $\boldsymbol{N}$.*

Proof. Let u denote the unit element of $\boldsymbol{G}$. Because $\boldsymbol{N}$ is a subgroup of $\boldsymbol{G}$, we have that $N = u \cdot N \subseteq N \cdot N \subseteq N$. Let $f, g \in G$. Since $\boldsymbol{N}$ is a normal subgroup of $\boldsymbol{G}$, we have that $g \cdot N = N \cdot g$, due to Lemma 4.11. It follows that $f \cdot N \cdot g \cdot N = f \cdot g \cdot N \cdot N = (f \cdot g) \cdot N$, which is a coset. □

The multiplication of cosets of a normal subgroup $\boldsymbol{N}$ is clearly associative, N plays rôle of a unit, and $(g \cdot N)^{-1} = g^{-1} \cdot N$. Therefore the set of all cosets of $\boldsymbol{N}$ together with their multiplication forms a group. We denote this group by $\boldsymbol{G}/\boldsymbol{N}$ and call the *factor group* of $\boldsymbol{G}$ over $\boldsymbol{N}$. The size of the factor group $\boldsymbol{G}/\boldsymbol{N}$ clearly equals $[\boldsymbol{G} : \boldsymbol{N}]$, the size of the set of all cosets of $\boldsymbol{N}$. In particular, if $\boldsymbol{G}$ is finite, we infer from the Lagrange theorem that

$$|\boldsymbol{G}/\boldsymbol{N}| = \frac{|\boldsymbol{G}|}{|\boldsymbol{N}|}. \tag{4.1}$$

Exercises

Exercise 4.1. *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.*

Exercise 4.2. *Let $\boldsymbol{T}$ denote the two-element subgroup of the symmetric group $\boldsymbol{S_3}$ consisting of the transposition $(1, 2)$ and the identity permutation. Compute and compare all left and right cosets of $\boldsymbol{T}$.*

Exercise 4.3. *Let $\boldsymbol{N}$ be a subgroup of a group $\boldsymbol{G}$. If $[\boldsymbol{G} : \boldsymbol{N}] = 2$, then $\boldsymbol{N} \trianglelefteq \boldsymbol{G}$, i.e, a subgroup of the index 2 is normal.*

Exercise 4.4. *Prove that $\boldsymbol{A_n}$ is a normal subgroup of $\boldsymbol{S_n}$, for each $2 \leq n$.*

Exercise 4.5. *Let $\boldsymbol{G}$ be a finite group and p the least prime such that $p \mid |G|$. Prove that a subgroup $\boldsymbol{N}$ of $\boldsymbol{G}$ of the index p is normal.*