

LECTURE 5 Conjugacy

PAVEL RŮŽIČKA

ABSTRACT. We study the conjugacy relation on a group. We prove that the conjugacy classes form a partition of the group. We show that a subgroup is normal if and only if it is a union of conjugacy classes. We will study some examples. We prove that permutations in a symmetric group are conjugated if and only if they have the same type. Finally we study sets of generators of a group. Understanding some sets of generators of an alternating group will help us to prove that all standard positions of the 15 puzzle corresponding to even permutations are solvable.

5.1. **Conjugacy.** Elements g, h of a group G are said to be *conjugate* (which we denote by $g \sim h$) if there is $f \in G$ such that

$$g = f \cdot h \cdot f^{-1}.$$

In this case we say the g is *conjugate to h by f* .

Clearly g is conjugate to g by the unit of G and if g is conjugate to h by f then h is conjugate to g by f^{-1} . It follows that the relation \sim is reflexive and symmetric. If g is conjugate with h by f and h is conjugate with k by e , then g is conjugate with k by $f \cdot e$, indeed, $(f \cdot e) \cdot k \cdot (f \cdot e)^{-1} = f \cdot e \cdot k \cdot e^{-1} \cdot f^{-1} = f \cdot h \cdot f^{-1} = g$. Thus we have the transitivity of \sim . We conclude that the conjugacy form an equivalence relation on G . The blocks of \sim are called the *conjugacy classe* (of *conjugacy blocks*) of G .

It follows from Lemma 4.11 that

Lemma 5.1. *A subgroup N of a group G is normal if and only if it is a union of conjugacy classes of G , that is, if $f \cdot n \cdot f^{-1} \in N$, for all $n \in N$ and all $f \in G$.*

Corollary 5.2. *A subgroup N of a group G is normal if and only if $f \cdot g \in N$ implies that $g \cdot f \in N$ for all $f, g \in G$.*

Proof. (\Rightarrow) Observe that $g \cdot f = g \cdot (f \cdot g) \cdot g^{-1}$, i.e. $f \cdot g$ and $g \cdot f$ are conjugated. (\Leftarrow) Note that $n = f^{-1} \cdot (f \cdot n)$, hence if $n \in N$, then $(f \cdot n) \cdot f^{-1} \in N$. \square

The lecture and the tutorial took place in Malá strana, room S11, on October 30, 2018.

For a group \mathbf{G} let

$$(5.1) \quad Z(\mathbf{G}) := \{g \in G \mid g \cdot f = f \cdot g \text{ for all } f \in G\}.$$

The set $Z(\mathbf{G})$ is called the *center* of the group \mathbf{G} . Observe that $g \in Z(\mathbf{G})$ if and only if $g = f \cdot g \cdot f^{-1}$ for all $f \in G$. This happens if and only if the conjugacy class of g equals to $\{g\}$. It follows that $Z(\mathbf{G})$ is a union of all singleton conjugacy classes of \mathbf{G} .

Proposition 5.3. *The center of a group \mathbf{G} forms a normal subgroup of \mathbf{G} .*

Proof. Let $g, h \in Z(\mathbf{G})$ and $f \in G$. Then

$$g^{-1} \cdot f = g^{-1} \cdot f \cdot g \cdot g^{-1} = g^{-1} \cdot g \cdot f \cdot g^{-1} = f \cdot g^{-1},$$

and

$$g \cdot h \cdot f = g \cdot f \cdot h = f \cdot g \cdot h,$$

for all $f \in G$, hence both g^{-1} and $g \cdot h$ belong to $Z(\mathbf{G})$. It follows that $Z(\mathbf{G})$ forms a subgroup of \mathbf{G} . Furthermore, we have that

$$f \cdot Z(\mathbf{G}) = \{f \cdot g \mid g \in Z(\mathbf{G})\} = \{g \cdot f \mid g \in Z(\mathbf{G})\} = Z(\mathbf{G}) \cdot f$$

for all $f \in G$. It follows that the subgroup $Z(\mathbf{G})$ is normal in \mathbf{G} . \square

Conjugated elements in a group usually share the same properties. Recall from linear algebra that complex matrices \mathbf{A}, \mathbf{B} are called *similar* if there is a regular matrix \mathbf{C} such that $\mathbf{A} = \mathbf{C} \cdot \mathbf{B} \cdot \mathbf{C}^{-1}$. In our terminology, regular matrices are similar provided that they are conjugated by a regular matrix. Similar complex matrices have the same characteristic polynomial and the similarity classes (corresponding to the conjugacy classes) are characterized by the Jordan canonical form. Notice that complex matrices are similar if and only if they are matrices of the same endomorphism, possibly with respect to distinct bases.

All regular complex matrices of a given size n form a group, usually denoted by $\text{GL}_n(\mathbb{C})$ or $\text{GL}(n, \mathbb{C})$ and called the *general linear group*. It follows from the definitions that regular complex matrices are conjugated if and only if they are similar if and only if they have the same Jordan canonical form.

Let n be a positive integer. A *type* of a permutation $\pi \in S_n$ is a map $t_\pi: \{1, 2, \dots, n\} \rightarrow \mathbb{N}_0$, where $t_\pi(k)$ is the number of cycles of length k in the decomposition of π into the product of independent cycles, for all $k \in \mathbb{N}_0$. For example, if

$$\pi := (1, 6, 3, 14) \cdot (2, 8, 4, 20, 19) \cdot (7, 11) \cdot (9, 17, 10, 18) \cdot (12, 13)$$

is a permutation from the group \mathbf{S}_{20} , then $t_\pi(1) = 3$, $t_\pi(2) = 2$, $t_\pi(3) = 0$, $t_\pi(4) = 2$, $t_\pi(5) = 1$, and $t_\pi(k) = 0$ for all $k \geq 6$.

We will use the following notation. Given a group \mathbf{G} and elements $g, f \in G$, we set

$${}^f g := f \cdot g \cdot f^{-1},$$

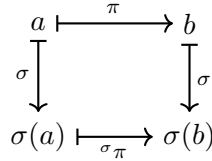
that is, ${}^f g$ is the element of G which is conjugated to g by f .

Theorem 5.4. *Two permutations $\pi, \rho \in S_n$ are conjugated if and only if they have the same type.*

Proof. Let $\pi, \sigma \in S_n$ be permutations and $a, b \in \{1, 2, \dots, n\}$ are such that $\pi(a) = b$. Then $\sigma\pi(\sigma(a)) = \sigma(b)$. Indeed,

$$(5.2) \quad \sigma\pi(\sigma(a)) = \sigma \cdot \pi \cdot \sigma^{-1}(\sigma(a)) = \sigma(\pi(a)) = \sigma(b).$$

Informally saying π maps a to b if and only if $\sigma\pi$ maps $\sigma(a)$ to $\sigma(b)$.



It follows that if $\gamma = (c_1, \dots, c_k)$ is a cycle, then $\sigma\gamma = (\sigma(c_1), \dots, \sigma(c_k))$ is a cycle of the same length and if

$$\pi = \gamma_1 \cdot \gamma_2 \cdots \gamma_m$$

is a decomposition of the permutation π into the product of independent cycles, then

$$\sigma\pi = \sigma\gamma_1 \cdot \sigma\gamma_2 \cdots \sigma\gamma_m$$

is a decomposition of its conjugate $\sigma\pi$ into the product of independent cycles. In particular, the permutations π and $\sigma\pi$ have the same type.

Suppose that permutations π and ρ have the same type. Let $\pi = \gamma_1 \cdot \gamma_2 \cdots \gamma_m$ and $\rho = \delta_1 \cdot \delta_2 \cdots \delta_m$ be decompositions of the permutations into products of independent cycles. Since π and ρ have the same types, we can suppose without loss of generality that the cycles $\gamma_i = (c_{i,1}, \dots, c_{i,k_i})$ and $\delta_i = (d_{i,1}, \dots, d_{i,k_i})$ have the same length k_i , for all $i \in \{1, 2, \dots, m\}$. Let $\sigma \in S_n$ be a permutation such that $\sigma(c_{i,j}) = d_{i,j}$ for all $i \in \{1, 2, \dots, m\}$ and $j \in \{1, 2, \dots, k_i\}$. We infer from (5.2) that $\rho = \sigma\pi$, in particular, the permutations π and ρ are conjugated. \square

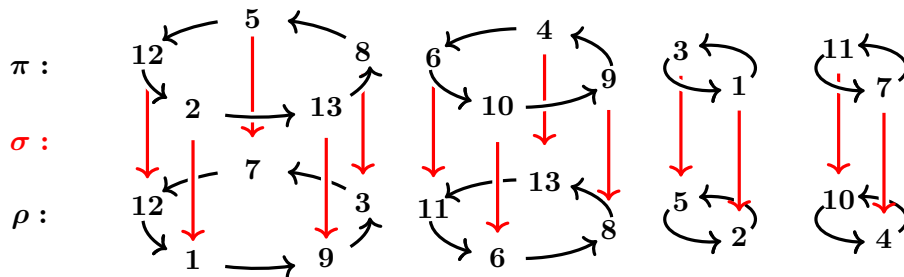


FIGURE 1. ρ is conjugated to π by σ .

Example 5.5. *Permutations*

$$\pi : (2, 13, 8, 5, 12) \cdot (4, 6, 10, 9) \cdot (1, 3) \cdot (7, 11)$$

and

$$\rho : (1, 9, 3, 7, 12) \cdot (13, 11, 6, 8) \cdot (2, 5) \cdot (4, 10)$$

on a 13-elements set have the same type. They are conjugated by a (not unique) permutation σ which can be seen from their decompositions into the products of independent cycles. We can depict the situation as on Figure 1.

The table of σ is

1	2	3	4	5	6	7	8	9	10	11	12	13
2	1	5	13	7	11	4	3	8	6	10	12	9

Example 5.6. Let \mathbf{R} denote the group of all rotations of a cube. Each rotation of the cube is determined by the front faces and the vertex of the front face in the upper left corner after executing the rotation. Since a cube has six faces and each face has four vertices there are exactly $6 \cdot 4 = 24$ rotations of the cube. We can color vertices and diagonals of the cube as in the Figure 2. Observe that colorings of vertices of the front face correspond

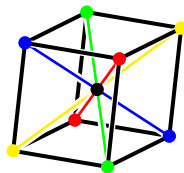


FIGURE 2. The cube with colored vertices and diagonals

to permutations of diagonals of the cube. Rotating each of the six faces of the cube so that the blue vertex is in the upper left corner, we observe that we get six different colorings. They correspond to all six possible permutations of the remaining three vertices green, red, and yellow (see Figure 3).

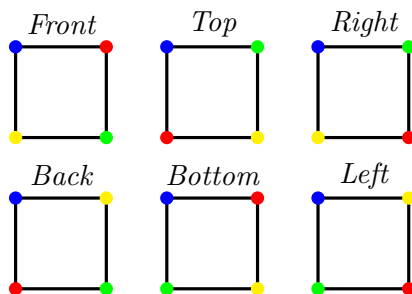


FIGURE 3. The colorings of the faces

By rotating the faces we get all 24 permutations of the four colors. The colorings correspond to permutations of diagonals of the cube. The composition of rotations coincides with the product of their permutations, and so the group \mathbf{R} coincides with the group \mathbf{S}_4 of permutations of a four element set (we will say that the groups are **isomorphic**).

The table below lists the conjugacy classes of the group \mathbf{S}_4 and the types of corresponding rotations of the cube. In the first column we write the type of a permutation characterizing a conjugacy class (we write a tuple instead a map). The second column we write the size of the conjugacy class. In the last column we identify the corresponding rotations of the cube.

Type	Size	The corresponding rotation of the cube
$\langle 4, 0, 0, 0 \rangle$	1	The identity
$\langle 2, 1, 0, 0 \rangle$	$\binom{4}{2} = 6$	A flip over centers of opposite edges; 180°
$\langle 0, 2, 0, 0 \rangle$	3	A flip over centers of opposite faces; 180°
$\langle 1, 0, 1, 0 \rangle$	$\binom{4}{3} \cdot 2 = 8$	A rotation over a diagonal; angle = 120°
$\langle 0, 0, 0, 1 \rangle$	$3! = 6$	A rotation over centers of opposite faces; 90°

Often groups are employed to study behaviors of symmetries of some objects (as the cube here). The outcome of this example should be the intuition that conjugate elements represent same symmetries of the studied object only placed differently.

5.2. Generating sets and the 15-puzzle. Let \mathbf{A} be an algebra from a given class of algebras, say \mathcal{A} . If the sub-algebras of \mathbf{A} from \mathcal{A} are closed under intersections, each subset S of \mathbf{A} is contained in a smallest sub-algebra from the class \mathcal{A} . This sub-algebra is called an **\mathcal{A} -sub-algebra generated** by the set S and it is denoted by $\langle S \rangle_{\mathcal{A}}$. Clearly,

$$\langle S \rangle_{\mathcal{A}} := \bigcap \{B \mid B \text{ is an } \mathcal{A}\text{-sub-algebra of } \mathbf{A} \text{ and } S \subseteq B\}.$$

In particular, if \mathcal{A} -sub-algebras of \mathbf{A} correspond to sub-universes of \mathcal{A} , they are closed under intersections and the above applies. We will drop the index writing $\langle S \rangle$ in this case. We obtain the \mathcal{A} -sub-algebra generated by a subset S of A by repeatedly applying operations of \mathbf{A} . Formally

$$\langle S \rangle_{\mathcal{A}} = \bigcup_{n=0}^{\infty} S_n,$$

where the sets $S_0 \subseteq S_1 \subseteq S_2 \subseteq \dots$ are defined inductively as $S_0 := S$ and

$$S_{n+1} := \{f(\mathbf{s}) \mid \mathbf{s} \in S_n^k \text{ and } f \text{ is a } k\text{-ary operation of } \mathbf{A}, k \in \mathbb{N}_0\}.$$

Viewing groups as algebras with a binary operation, an unary operation of the inverse, and a nullary operation corresponding to the unit element, the sub-universes of a group correspond to its subgroups. Therefore given a subset S of a group \mathbf{G} , the subgroup $\langle S \rangle$ generated by the subset S is the intersection of all subgroups of \mathbf{G} containing S . It is easy to see that $\langle S \rangle$ is the set of all products of sequences of elements of S and their inverses.

A subset S of a group \mathbf{G} is a *generating set* of \mathbf{G} (we also say that S *generates* \mathbf{G}) provided that $\langle S \rangle = \mathbf{G}$. We proved in Lemma 3.6 that every permutation is a product of transpositions. It follows that all transpositions on the set $\{1, 2, \dots, n\}$ form a generating set of \mathbf{S}_n .

Lemma 5.7. *Let $3 \leq n$. The group \mathbf{A}_n is generated by the set of all 3-cycles.*

Proof. Since every even permutation is a product of even number of transpositions, it suffices to prove that a product of two transpositions, say $(a, b) \cdot (c, d)$ is a product of 3-cycles. If $\{a, b\} = \{c, d\}$, the transpositions is equal and their product is the identity permutation. It is a product of a 3-cycle and its inverse. Otherwise we can without loss of generality suppose that $b \notin \{c, d\}$ and $c \notin \{a, b\}$. Then

$$(a, b) \cdot (c, d) = (a, b) \cdot (b, c) \cdot (b, c) \cdot (c, d) = (a, b, c) \cdot (b, c, d).$$

□

In Proposition 3.10 we proved that standard positions of the 15 puzzle corresponding to odd permutations are unsolvable. We complete our analysis of the puzzle proving that the other standard positions can be solved.

Proposition 5.8. *Standard positions of the 15 puzzle corresponding to even permutations are solvable.*

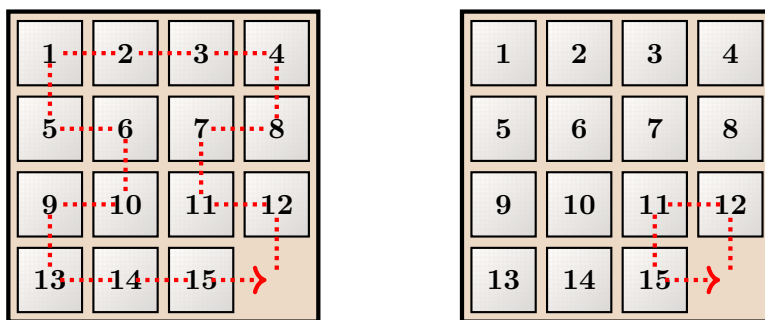


FIGURE 4. The solution of the 15 puzzle

Proof. Let $\{b, a_1, a_2, \dots, a_k\}$ be a $k + 1$ -element subset of $\{1, 2, \dots, n\}$. It is straightforward to see that

$$(a_1, a_2, \dots, a_k) = (b, a_1) \cdot (a_1, a_2) \cdot (a_2, a_3) \cdots (a_{k-1}, a_k) \cdot (a_k, b).$$

It follows that the sequences of moves depicted in the Figure 4 result in the permutations

$$(15, 14, 13, 9, 10, 6, 5, 1, 2, 3, 4, 8, 7, 11, 12) \text{ and } (15, 11, 12).$$

According to Exercise 5.7 these two cycles generate \mathbf{A}_{15} . This proves the solubility of every standard position corresponding to an even permutation. \square

With help of Exercise 5.8 we give another proof of the solubility of all even standard positions. Since every even permutation is a product of 3-cycles, it suffices to prove that all standard positions corresponding to 3-cycles are solvable. However, the standard position corresponding to the 3-cycle (a, b, c) is solved by the sequence of moves leading to the permutation $\pi_{a,b,c}^{-1} \cdot (15, 11, 12) \cdot \pi_{a,b,c}$. The inverse $\pi_{a,b,c}^{-1}$ is obtained by reversing the moves giving $\pi_{a,b,c}$. Various puzzles (the Rubik cube among them) can be solved employing the conjugacy of permutations.

EXERCISES

Exercise 5.1. Find all conjugacy classes and their sizes of the symmetric groups \mathbf{S}_3 and \mathbf{S}_5 .

Exercise 5.2. Find all conjugacy classes and their sizes of the alternating groups \mathbf{A}_3 and \mathbf{A}_4 .

Exercise 5.3. Describe the group of all rotations of a regular tetrahedron. List its conjugacy classes.

Exercise 5.4. Describe the group of all symmetries of a regular pentagon. List its conjugacy classes.

Exercise 5.5. Let n be a positive integer.

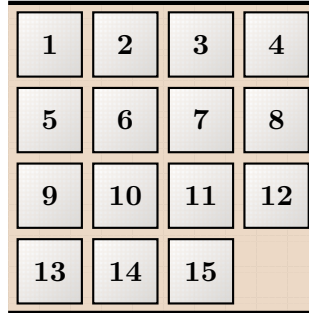
- (i) Prove that the transpositions $(1, 2), (2, 3), \dots, (n-1, n)$ generate the group \mathbf{S}_n .
- (ii) Prove that \mathbf{S}_n is generated by the cycles $(1, 2)$ and $(1, 2, \dots, n)$.
- (iii) Decide whether the cycles $(1, 3)$ and $(1, 2, 3, 4)$ generate \mathbf{S}_4 .

Exercise 5.6. Let n be a positive integer and X a subset of \mathbf{A}_n such that for every $c \in \{3, 4, \dots, n\}$ there is a 3-cycle $(a, b, c) \in X$ with $a, b < c$. Then X is a generating set of \mathbf{A}_n .

Exercise 5.7. Let n be an odd positive integer. Prove that an n -cycle (a_1, a_2, \dots, a_n) and a 3-cycle (a_1, a_{n-1}, a_n) generate the group \mathbf{A}_n .

Exercise 5.8. Prove that for all distinct $a, b, c \in \{1, 2, \dots, 15\}$ there is a sequence, say $\pi_{a,b,c}$, of moves starting and ending in a lower left corner (i.e., transforming a standard position to another standard position) that moves a to 15, b to 11, and c to 12.

Exercise 5.9. Consider a version of the 15 puzzle on a tube, so that we can move around in the horizontal direction (see Figure 5). Find all solvable positions.



1	2	3	4
5	6	7	8
9	10	11	12
13	14	15	

FIGURE 5. The 15 puzzle on a tube.