ALGEBRA I (LECTURE NOTES 2017/2018) LECTURE 6 - NORMAL SUBGROUPS, FACTOR GROUPS, AND CONJUGACY

PAVEL RŮŽIČKA

6.1. Normal subgroups and factor-groups.

Definition 6.1. A subgroup $\boldsymbol{N}$ of a group $\boldsymbol{G}$ is *normal*, (which we denote by $\boldsymbol{N} \trianglelefteq \boldsymbol{G}$) provided that each right coset of $\boldsymbol{N}$ is at the same time a left coset of $\boldsymbol{N}$.

Remark 6.2. Observe that a subgroup of a commutative group is necessarily normal.

Example 6.3. *In case of non-commutative groups it often happens that left and right cosets of a subgroup differ (although they have the same size by Lemma 5.5). Consider for example the 6-element symmetric group $\boldsymbol{S_3}$ and its 2-element subgroup, say $\boldsymbol{H}$, with the universe $\{\upsilon_3, (1,2)\}$. The left cosets of $\boldsymbol{H}$ are $\{\upsilon_3, (1,2)\}$, $\{(2,3),(1,2,3)\}$, and $\{(1,3),(1,3,2)\}$, while the right cosets are $\{\upsilon_3, (1,2)\}$, $\{(1,3),(1,2,3)\}$, and $\{(2,3),(1,3,2)\}$.*

Lemma 6.4. *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.*

Proof. Since $[\boldsymbol{G} : \boldsymbol{N}] = 2$, there are exactly two left cosets of $\boldsymbol{N}$. Since N is one-of them and the left cosets form a partition of G, the remaining one is $G \setminus N$. Similarly we prove that N and $G \setminus N$ are the right cosets of $\boldsymbol{N}$, and so the left and the right cosets of $\boldsymbol{N}$ coincide. □

Since $[\boldsymbol{S_n} : \boldsymbol{A_n}] = 2$ whenever $2 \leq n$, we have that

Corollary 6.5. *For each integer $2 \leq n$, $\boldsymbol{A_n} \trianglelefteq \boldsymbol{S_n}$.*

Lemma 6.6. *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) *$g \cdot N = N \cdot g$, for all $g \in G$,*
(iii) *$g \cdot N \cdot g^{-1} \subseteq N$, for all $g \in G$.*

Date: November 6, 2017.

Proof. $(i) \Rightarrow (iii)$ 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 $g \cdot N \cdot g^{-1} = N \cdot f \cdot g^{-1} \subseteq N \cdot N \subseteq N$. $(iii) \Rightarrow (ii)$ Let $g \in G$. By multiplying both sides of $g \cdot N \cdot g^{-1} \subseteq N$ by g from the right, we get that $g \cdot N \subseteq N \cdot g$. Replacing g with g^{-1} we reformulate (iii) as $g^{-1} \cdot N \cdot g \subseteq N$. Multiplying by both sides by g from the left, we conclude that $N \cdot g \subseteq g \cdot N$. Implication $(ii) \Rightarrow (i)$ 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 6.7. *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 $\boldsymbol{G}$. Since $\boldsymbol{N}$ 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 6.6. 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 a role of 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 $\boldsymbol{G/N}$ and call the *factor group* of $\boldsymbol{G}$ over $\boldsymbol{N}$. The size of the factor group $\boldsymbol{G/N}$ 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

$$|\boldsymbol{G/N}| = \frac{|\boldsymbol{G}|}{|\boldsymbol{N}|}. \tag{6.1}$$

6.2. **Conjugacy.** Elements g, h of a group $\boldsymbol{G}$ 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 $\boldsymbol{G}$ 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 classes* of $\boldsymbol{G}$.

It follows from Lemma 6.6$(i) \Leftrightarrow (iii)$ that

Lemma 6.8. *A subgroup $\boldsymbol{N}$ of a group $\boldsymbol{G}$ is normal if and only if it is an union of conjugacy classes of $\boldsymbol{G}$, that is, $f \cdot n \cdot f^{-1} \in N$, for all $n \in N$ and all $f \in G$.*

For a group $\boldsymbol{G}$ set

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

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

Proposition 6.9. *The center of a group $\boldsymbol{G}$ forms a normal subgroup of $\boldsymbol{G}$.*

Proof. Let $g, h \in Z(\boldsymbol{G})$ 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 $Z(\boldsymbol{G})$. It follows that $Z(\boldsymbol{G})$ forms a subgroup of $\boldsymbol{G}$. Furthermore, we have that

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

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

Conjugated elements in a group usually share the same properties. Recall from linear algebra that complex matrices $\boldsymbol{A}, \boldsymbol{B}$ are called *similar* if there is a regular matrix $\boldsymbol{C}$ such that $\boldsymbol{A} = \boldsymbol{C} \cdot \boldsymbol{B} \cdot \boldsymbol{C}^{-1}$. Similar complex matrices have the same characteristic polynomial. The similarity classes are characterized by the Jordan canonical form. All regular complex matrices (of a given order n) form a group, usually denoted by $\mathrm{GL}_n(\mathbb{C})$ or $\mathrm{GL}(n, \mathbb{C})$ and called the *general linear group*. It follows from the definitions that matrices in $\mathrm{GL}_n(\mathbb{C})$ 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 $t_\pi \colon \{1, 2, \ldots, n\} \to \mathbb{N}_0$, 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 $\boldsymbol{S_{20}}$, 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 $\boldsymbol{G}$ 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 6.10. *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,

$$^\sigma\pi(\sigma(a)) = \sigma \cdot \pi \cdot \sigma^{-1}(\sigma(a)) = \sigma(\pi(a)) = \sigma(b). \tag{6.2}$$

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 $\pi = \gamma_1 \dots \gamma_2 \cdots \gamma_m$ 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 (6.2) that $\rho = {}^\sigma\pi$, in particular, the permutations π and ρ are conjugated. □

Example 6.11. *Consider a group, say $\boldsymbol{R}$, of all rotations of a cube. We can number (and color accordingly) the vertices of the cube as in the Figure 1. Each rotation of the cube is determined by*

- *which of the six faces is in front,*
- *which of the four vertices of the front face is in the upper left corner,*

after executing the rotation. It follows that there are exactly $6 \cdot 4 = 24$ rotations of the cube. Rotating each of the six faces of the cube so that the vertex numbered 1 is in the upper left corner, we see that all of them are different. Observe tha we get all six possible permutations of

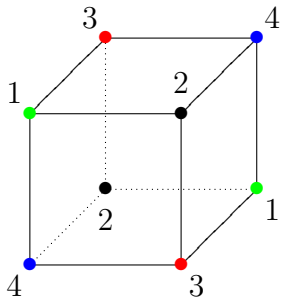

FIGURE 1. The cube

the remaining three vertices (see Figure 2). By rotating the faces we get all 24 *permutations of the set* $\{1, 2, 3, 4\}$. *Thus we can identify the rotations of the cube with the permutations of the four-element set.*

Observe that vertices with the same number are endpoints of the four diagonals of the cube. We can number the diagonals according to their endpoints. The permutations of the numbers of vertices in the front face of the cube correspond to permutations of the diagonals. Therefore there is a one-to-one correspondence between the rotations of the cube and the permutations of the diagonals of the cube. The composition of rotations coincides with the the product of permutations and so the group $\boldsymbol{R}$ *coincides with the permutation group* $\boldsymbol{S_4}$ *(we will say that the groups are* isomorphic*).*

The table below lists the conjugacy classes of the group $\boldsymbol{S_4}$ *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 as a tuple instead a map). The second column contains a representative of a given conjugacy class. In the third column we identify the corresponding rotations of the cube. There are five classes corresponding to*

- *the identity rotation of the cube (i.e., we do nothing),*
- *a rotation over the axis connecting the centers of two opposite edges; the angle of the rotation is necessarily* 180^o,
- *a flip, that is, a rotation over the axis connecting the centers of two opposite faces; the angle of the rotation is* 180^o.
- *a rotation over the diagonal of the cube;*
- *a flip, the angle of the rotation is* 120^o,
- *again a rotation over the axis connecting the centers of two opposite faces but the angle of the rotation is* 90^o.

In the last column of the table we write the sizes of conjugacy classes.

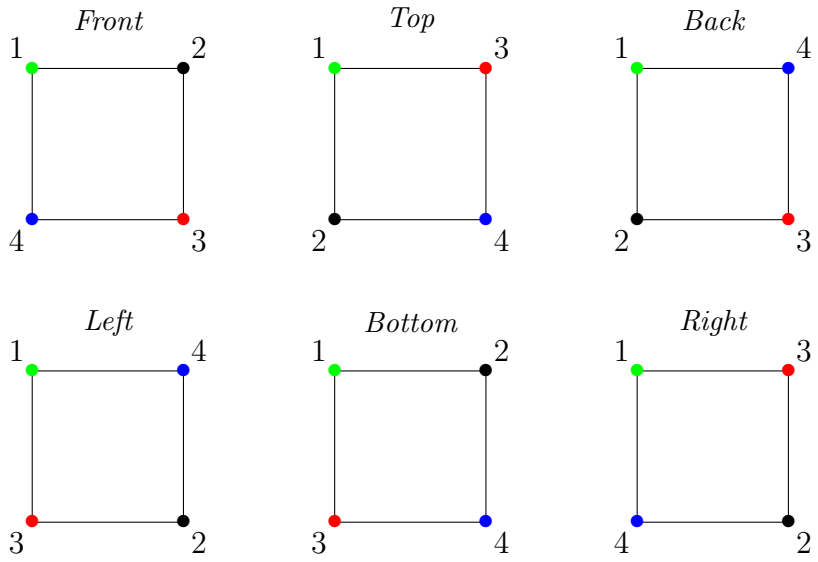

FIGURE 2. Faces

type	***example***	***corresponding rotation***	***size***
$\langle 4,0,0,0\rangle$	υ_4	*the identity*	1
$\langle 2,1,0,0\rangle$	$(1,2)$	*centers of opposite edges;* 180^o	$\binom{4}{2}=6$
$\langle 0,2,0,0\rangle$	$(1,2)\cdot(3,4)$	*centers of opposite faces;* 180^o	3
$\langle 1,0,1,0\rangle$	$(1,2,3)$	*a diagonal,* 120^o	$4\cdot 2=8$
$\langle 0,0,0,1\rangle$	$(1,2,3,4)$	*centers of opposite faces;* 90^o	$3!=6$

Often groups are employed to study behaviours 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.

6.3. **Simplicity of the group A_n for $n \geq 5$.** A (non-trivial) group has two trivial subgroups, the singleton subgroup containing only the unit element and the group itself. These two subgroups are necessarily normal. These are the only subgroups (and *a fortiori* the only normal subgroups) of finite groups of a prime size due to the Langrange theorem. The other groups have non-trivial subgroups but it still can happen that they have only trivial normal subgroups. The groups whose only normal subgroups are the trivial ones are called *simple*. We prove that this is the case of most of the alternating groups (with the only exception of $\boldsymbol{A_4}$).

Theorem 6.12. *The alternating group of permutations $\boldsymbol{A_n}$ is simple for all $n \geq 5$.*

Proof. First we prove that

Claim 1. Every even permutation is a product of 3-cycles.

Proof of Claim 1. Since an even permutation is a product of an even number of transpositions, due to Lemma 4.4, it suffices to show that a product of two transpositions, say τ, σ is at the same time a product of 3-cycles. There three cases to discus: Firstly, when $\operatorname{supp}\tau = \operatorname{supp}\sigma$, then $\tau = \sigma$ and $\tau \cdot \sigma = \upsilon_n$. Secondly if $\operatorname{supp}\tau \cap \operatorname{supp}\sigma \neq \emptyset$ but $\tau \neq \sigma$. Then $\tau = (a, b)$ and $\sigma = (b, c)$ for some pairwise distinct a, b, c. We compute that $\tau \cdot \sigma = (a, b) \cdot (b, c) = (a, b, c)$ is a 3-cycle. Finally we assume that $\operatorname{supp}\tau \cap \operatorname{supp}\sigma = \emptyset$. In this case $\tau = (a, b)$ and $\sigma = (c, d)$ for some pairwise distinct a, b, c, d and we compute that $\tau \cdot \sigma = (a, b) \cdot (c, d) = (a, b) \cdot (b, c) \cdot (b, c) \cdot (c, d) = (a, b, c) \cdot (b, c, d)$. □ Claim 1.

Next, using the assumption that $n \geq 5$, we show that

Claim 2. All 3-cycles are conjugated in $\boldsymbol{A_n}$.

Proof of Claim 2. Let $\pi = (a, b, c)$ and $\rho = (d, e, f)$ be 3-cycles (with not necessarily disjoint supports). According to (6.2), ρ is conjugated to π by a permutation σ satisfying $\sigma(a) = d$, $\sigma(b) = e$ and $\sigma(c) = f$. If σ is even, we are done. If σ is odd, we find g, h distinct from d, e, f and replace σ with the even permutation $\sigma' = (g, h) \cdot \sigma$. We still have that $\sigma'(a) = d$, $\sigma'(b) = e$ and $\sigma'(c) = f$, and so $\rho = {}^{\sigma'}\pi$. This is possible since $n \geq 5$. □ Claim 2.

Let $\boldsymbol{N}$ be a non-singleton normal subgroup of $\boldsymbol{A_n}$. If $\boldsymbol{N}$ contains a 3-cycle, then it contains all 3-cycles due to Claim 2 and the normality of $\boldsymbol{N}$, and so $\boldsymbol{N} = \boldsymbol{A_n}$ due to Claim 1. We conclude the prove with

Claim 3. The non-singleton normal subgroup $\boldsymbol{N}$ of $\boldsymbol{A_n}$ contains a 3-cycle.

Proof of Claim 3. Let π be a non-unit permutation from $\boldsymbol{N}$ with $\operatorname{supp}\pi$ of the least possible size (among non-unit permutations from $\boldsymbol{N}$). We will discus two complementary cases.

First suppose that in the decomposition of π into the product of independent cycles there is a cycle $(a, b, c, \dots)$ of the length at least 3. If π is a 3-cycle, we are done. Otherwise there is $e \in \operatorname{supp}\pi$ different from a, b, c. We put $f = \pi(e)$. Since $e \neq a$, we have that $f \neq b$. Therefore the permutation $\sigma = (a, e) \cdot (b, f)$ is even. Put $\rho = \pi^{-1} \cdot {}^{\sigma}\pi$. Observe that $\operatorname{supp}\rho \subseteq \operatorname{supp}\pi$ and, since $\boldsymbol{N} \trianglelefteq \boldsymbol{A_n}$, the permutation ρ belongs to $\boldsymbol{N}$. According to (6.2), ${}^{\sigma}\pi(f) = c$. Since $f \neq b$, we

have that ${}^{\sigma}\pi \neq \pi$, hence ρ is a non-unit permutation. We compute that $\rho(a) = \pi^{-1}({}^{\sigma}\pi(a)) = \pi^{-1}(b) = a$, hence $\operatorname{supp}\rho \subsetneq \operatorname{supp}\pi$. This contradicts the choice of π.

The remaining case is when $\pi = (a,b)\cdot(c,d)\cdots$ is a product of independent transpositions. Since $n \geq 5$, we can pick $e \notin \{a,b,c,d\}$ and put $\sigma = (a,b)\cdot(c,e)$. As in the previous case let $\rho = \pi^{-1}\cdot{}^{\sigma}\pi$ (which here equals to $\pi\cdot{}^{\sigma}\pi$). Observe that $\operatorname{supp}\rho \subseteq \operatorname{supp}\pi \cup \{e\}$ and as above $\rho \in \boldsymbol{N}$. We easily compute that $\rho(a) = a$, $\rho(b) = b$ and $\rho(e) = \pi^{-1}(d) = c \neq e$. It follows that ρ is a non-unit permutation and $a, b \notin \operatorname{supp}\rho$. We conclude that $|\operatorname{supp}\rho| < |\operatorname{supp}\pi|$, which is a contradiction. □ Claim 3.

□

Remark 6.13. Note that all the permutations of the type $\langle 0,2,0,0\rangle$ together with the unit-permutation form a non-trivial normal subgroup of $\boldsymbol{A_4}$.

Exercise 6.1. *Decide whether all 3-cycles are conjugated in* $\boldsymbol{A_4}$.

6.4. **Generating sets and the 15-puzzle.** Let $\boldsymbol{A}$ be an algebra of a given signature. Observe that the set of all sub-universes of the $\boldsymbol{A}$ is closed under arbitrary intersections. It follows that for every $X \subseteq A$ the set

$$\langle X\rangle := \{B \mid B \text{ is a sub-universe of } \boldsymbol{A} \text{ and } X \subseteq B\}$$

is the least sub-universe of $\boldsymbol{A}$ containing the set X. If sub-universes of $\boldsymbol{A}$ coincide with sub-algebras of $\boldsymbol{A}$, we call $\langle X\rangle$ the *(sub-)algebra generated* by the set X.

We get $\langle X\rangle$ by starting from X and repeatedly applying operations of $\boldsymbol{A}$. In particular,

$$\langle X\rangle = \bigcup_{n=0}^{\infty} X_i,$$

where the sets $X_0 \subseteq X_1 \subseteq X_2 \subseteq \dots$ are defined inductively as follows:

(i) $X_0 := X$,
(ii) $X_{n+1} := \{f(\boldsymbol{x}) \mid \boldsymbol{x} \in X_n^k$ and f is a k-ary operation of $\boldsymbol{A}\}$.

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

A subset X of a group $\boldsymbol{G}$ is a *generating set* of $\boldsymbol{G}$ (we also say that X *generates* $\boldsymbol{G}$) provided that $\langle X\rangle = \boldsymbol{G}$. We proved in Lemma 4.3 that every permutation is a product of transpositions. It follows that all transpositions on the set $\{1, 2, \ldots, n\}$ form a generating set of $\boldsymbol{S_n}$. It follows from Theorem 6.12 (Claim 1) that every even permutation is a product of 3-cycles. Consequently, all 3-cycles form a generating set of $\boldsymbol{A_n}$.

Exercise 6.2. *Let n be a positive integer.*

(i) *Prove that the transpositions $(1,2), (2,3), \ldots, (n-1,n)$ generate the group $\boldsymbol{S_n}$.*
(ii) *Prove that $\boldsymbol{S_n}$ is generated by the cycles $(1,2)$ and $(1,2,\ldots,n)$.*
(iii) *Decide whether the cycles $(1,3)$ and $(1,2,3,4)$ generate $\boldsymbol{S_4}$.*

Exercise 6.3. *Let n be a positive integer and X a subset of A_n such that for every $c \in \{3,4,\ldots,n\}$ there is a 3-cycle $(a,b,c) \in X$ with $a, b < c$. Then X is a generating set of $\boldsymbol{A_n}$.*

Exercise 6.4. *Let n be an odd positive integer. Prove that an n-cycle $(a_1, a_2, \ldots, a_n)$ and a 3-cycle (a_1, a_{n-1}, a_n) generate the group $\boldsymbol{A_n}$.*

In Proposition 4.7 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 6.14. *Standard positions of the 15 puzzle corresponding to even permutations are solvable.*

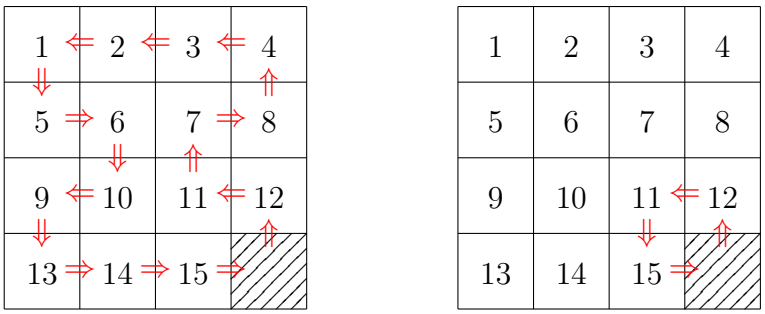

FIGURE 3. The cycles

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

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

It follows that the sequences of moves depicted in the Figure 3 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 6.4 these two cycles generate $\boldsymbol{A_{15}}$. This proves the solubility of every standard position corresponding to an even permutation. □

Exercise 6.5. *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.*

With help of Exercise 6.5 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 $\pi_{a,b,c}$. Many puzzles (as the Rubik cube) can be solved employing the conjugacy of permutations.