LECTURE 3
Sub-universe, the alternating group

PAVEL RŮŽIČKA

Abstract. We define notions of a sub-universe and a sub-algebra of an algebra. We discuss these notions in the particular case of groups. Then we go back to study of permutations. We define the signum of a permutation by means of the number of its cycles and we prove that the signum can be computed from any decomposition of the permutation into a product of transpositions.

Finally we introduce the 15 puzzle and we prove that standard positions corresponding to odd permutations are unsolvable.

3.1. **Sub-universes and sub-algebras.** Recall that an algebra $\boldsymbol{A}$ of a signature $\mathcal{I} = \langle I_0, I_1, \dots \rangle$ is a set A equipped with j-ary operations f_i^j, $i \in I_j$, $j = 0, 1, 2, \dots$. A *sub-universe* of an algebra $\boldsymbol{A}$ is a subset B of its underlying set A that is closed under all the operations of $\boldsymbol{A}$. Let $\mathcal{C}$ be a class of algebras of a fixed signature (typically algebras whose operations satisfy certain properties), and $\boldsymbol{A}$ an algebra from $\mathcal{C}$. A *$\mathcal{C}$-sub-algebra*, say $\boldsymbol{B}$, of the algebra $\boldsymbol{A}$ consists of a sub-universe B of $\boldsymbol{A}$ together with the restrictions of the operations of $\boldsymbol{A}$ to B and it belongs to $\mathcal{C}$.

Definition 3.1. A *subgroup* of a group $\boldsymbol{G}$ is a $\mathcal{G}$-sub-algebra of $\boldsymbol{G}$, where $\mathcal{G}$ denotes the class of all groups.

Each group $\boldsymbol{G}$ has a subgroup consisting of its unit element and a subgroup corresponding to $\boldsymbol{G}$ itself. These two subgroups are called *trivial*. Other subgroups are *non-trivial*.

We have defined a group as an algebra with a cancellative and divisible binary operation. Observe that not all sub-universes of a group correspond to its subgroups. For example, positive integers form a sub-universe but not a subgroup of the group of all integers with the operation of addition.

On the other hand, we proved that every group has a unique unit element and each element g of a group has a unique inverse g^{-1} such that $g \cdot g^{-1} = g^{-1} \cdot g = u$. Moreover the existence of these elements characterizes semigroups that are groups (cf. Proposition 2.7). Therefore we can define groups as algebras with an associative binary operation and two additional operations of a unit and an inverse. It is easy to see that any sub-universe

---

The Lecture and the tutorial took place in Malá strana, room S11, on October 16, 2018.

(i.e., a subset of closed under all the three operations) of a group is a subgroup. In particular, positive integers are not a sub-universe of the group of all integers when adopting this definition.

Remark 3.2. The binary operation of a group is usually denoted as $\cdot, \circ, \times, *$, the unit element as u or 1, and the inverse of an element g of the group as g^{-1}. Such a notation is called *multiplicative* and it is used for groups in general.

The binary operation of the group of all integers is denoted by $+$, the unit element by 0 (and it is called the *zero* element), and the inverse of an integer z is denoted by $-z$ and it is called the *opposite* element of z. This notation is called *additive*. Historically, the additive notation is used to emphasize that the group is commutative, i.e., that $a + b = b + a$ for all a, b. Let us note that commutative groups are usually called Abelian after the Norwegian mathematician Niels Henrik Abel (1802-1829).

3.2. **The signum of a permutation.**

Definition 3.3. Let π be a permutation on an n-element set. The *signum* of π is defined as $\operatorname{sgn}\pi = (-1)^{n-m}$, where m is the number of blocks of π (both singleton and non-singleton). A permutation π is *even* if $\operatorname{sgn}\pi = 1$ and *odd* if $\operatorname{sgn}\pi = -1$.

A unit permutation on an n-element set υ has exactly n blocks, and so $\operatorname{sgn}\upsilon = (-1)^{n-n} = 1$. Observe that if π is a product $\pi = \sigma_1 \cdot \cdots \cdot \sigma_k$ of permutations $\sigma_1, \ldots, \sigma_k$, then $\pi^{-1} = \sigma_k^{-1} \cdot \cdots \cdot \sigma_1^{-1}$ and that If $\gamma = (a_1, \ldots, a_k)$ is a cycle, then $\gamma^{-1} = (a_k, \ldots, a_1)$. It follows that the permutations π and π^{-1} have the same blocks. We conclude that

Lemma 3.4. *The unit permutation is even and* $\operatorname{sgn}\pi = \operatorname{sgn}\pi^{-1}$*, for every permutation* π*. In particular, the inverse of an even permutation is even.*

We will call 2-cycles *transpositions*.

Lemma 3.5. *Let* π *be a permuation an* τ *a transposition. Then*

$$\operatorname{sgn}\tau \cdot \pi = -\operatorname{sgn}\pi. \tag{3.1}$$

Proof. Let $B_1, \ldots, B_m$ be blocks of π corresponding to the decomposition $\pi = \gamma_1 \cdots \gamma_m$ of π into a product of independent cycles (including the singleton ones). According to the definition $\operatorname{sgn}\pi = (-1)^{n-m}$. The proof splits into two cases:

Case 1: $\operatorname{supp}\tau$ *is contained in a block of* π. Since the cycles are independent, and so they commute, we can without loss of generality assume that $\operatorname{supp}\tau \subseteq B_1$, $\tau = (a_1, a_i)$, and $\gamma_1 = (a_1, \ldots, a_k)$. We compute that

$$\tau \cdot \gamma_1 = (a_1, a_i) \cdot (a_1, \ldots, a_{i-1}, a_i, \ldots, a_k) = (a_1, \ldots, a_{i-1}) \cdot (a_i, \ldots, a_k),$$

hence

$$\tau \cdot \pi = \tau \cdot \gamma_1 \cdot \gamma_2 \cdots \gamma_m = (a_1, \ldots, a_{i-1}) \cdot (a_i, \ldots, a_k) \cdot \gamma_2 \cdots \gamma_m,$$

and this is the decomposition of the composition $\tau \cdot \pi$ into a product of independent cycles. It follows that the permutation $\tau \cdot \pi$ has $m+1$ blocks. We conclude that $\operatorname{sgn} \tau \cdot \pi = (-1)^{n-(m+1)} = -\operatorname{sgn} \pi$.

Case 2: $\operatorname{supp} \tau$ *meets two different blocks of* π. By suitably permuting the cycles $\gamma_1 \cdots \gamma_m$, we can assume that $\operatorname{supp} \tau \subseteq B_1 \cup B_2$, $\tau = (a_1, b_1)$, $\gamma_1 = (a_1, \ldots, a_k)$, and $\gamma_2 = (b_1, \ldots, b_l)$. We compute that

$$\tau \cdot \gamma_1 \cdot \gamma_2 = (a_1, b_1) \cdot (a_1, \ldots, a_k) \cdot (b_1, \ldots, b_l) = (a_1, \ldots, a_k, b_1, \ldots, b_l),$$

hence

$$\tau \cdot \pi = \tau \cdot \gamma_1 \cdot \gamma_2 \cdot \gamma_3 \cdots \gamma_m = (a_1, \ldots, a_k, b_1, \ldots, b_l) \cdot \gamma_3 \cdots \gamma_m.$$

It follows that the permutation $\tau \cdot \pi$ is a product of $m-1$ independent cycles, and so it has $m-1$ blocks. We conclude that $\operatorname{sgn} \tau \cdot \pi = (-1)^{n-(m-1)} = -\operatorname{sgn} \pi$.

□

Lemma 3.6. *Every permutation is a product of transpositions.*

Proof. Let n be a positive integer. The identity is the product of an empty set of transpositions. Since every permutation is a product of cycles due to Theorem 2.9, it suffices to prove that every cyclic permutation is a product of transpositions. It is straightforward, indeed, we have that

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

for every cycle $(a_1, \ldots, a_k)$. □

Lemma 3.7. *If a permutation* $\pi = \tau_1 \cdots \tau_k$ *is a product of transpositions* $\tau_1, \ldots, \tau_k$, *then* $\operatorname{sgn} \pi = (-1)^k$.

Proof. By induction on k applying Lemma 3.5. □

There are many ways how to express a permutation as a product o transpositions but the signum is invariant on the expression.

Lemma 3.8. *Let* π, ρ *be permutations on at least two element set. Then*

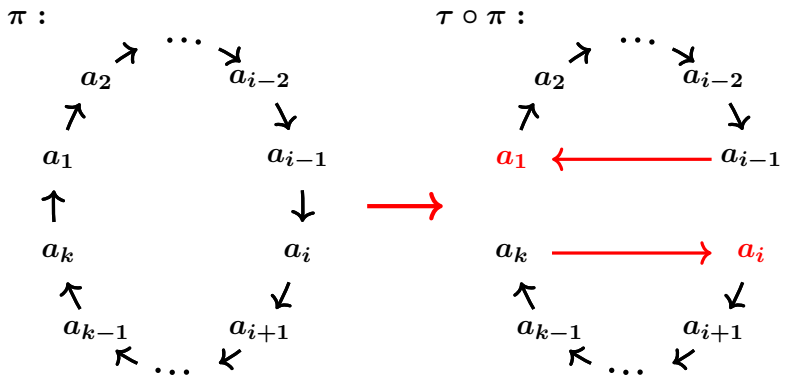
$$\operatorname{sgn}(\pi \cdot \rho) = \operatorname{sgn} \pi \cdot \operatorname{sgn} \rho.$$

Proof. Let $\pi = \tau_1 \cdots \tau_k$ and $\rho = \sigma_1 \cdots \sigma_l$ be expressions of the permutations π and σ as products of transpositions. Then $\pi \cdot \rho = \tau_1 \cdots \tau_m \cdot \sigma_1 \cdots \sigma_k$, and Lemma 3.7 gives that

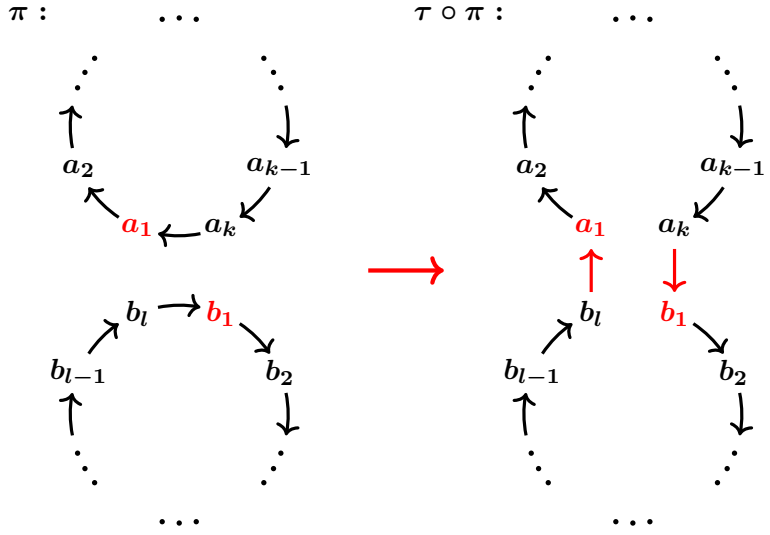
$$\operatorname{sgn}(\pi \cdot \rho) = (-1)^{m+k} = (-1)^m (-1)^k = \operatorname{sgn} \pi \cdot \operatorname{sgn} \rho.$$

□

Corollary 3.9. *The product of even permutations is an even permutation, two odd permutations is an even permutation, and the product of even and odd permutation is an odd permutation.*



Case 1. $\operatorname{supp}\tau = \{a_1, a_i\}$ is contained in a block of π.



Case 2. $\operatorname{supp}\tau = \{a_1, b_1\}$ meets two blocks of π.

3.3. **The symmetric and the alternating group.** We denote by S_n the set of all permutations of the n-element set $\{1, 2, \dots, n\}$. The set S_n is equipped with an operation of multiplication of permutation. Since the identity permutation υ plays the rôle of an unit element and each permutation has an inverse, S_n is the underlying set of a group that will be denoted by $\boldsymbol{S_n}$ and called the *symmetric group* (on the n-elements set $\{1, 2, \dots, n\}$).

Let A_n denote the set of all even permutations from S_n. It follows from Lemma 3.4 and Corollary 3.9 that A_n iis an underlying set of a subgroup of $\boldsymbol{S_n}$. We will called the subgroup the *alternating group* and denote by $\boldsymbol{A_n}$.

3.4. **The 15 puzzle.** The *15 puzzle* is a game invented by invented by Noyes Palmer Chapman, a postmaster in Canastota, NY, around the year

1875. In 1880, the game spread from USA to Canada and Europe and later to Asia and it gained a world-wide popularity.

The puzzle is often credited to Sam Loyd, who falsely claimed its authorship. He is known for offering a $ 1000 prize to a solver of the *advertising position* (see Figure:1). We will see that the advertising position is unsolvable.

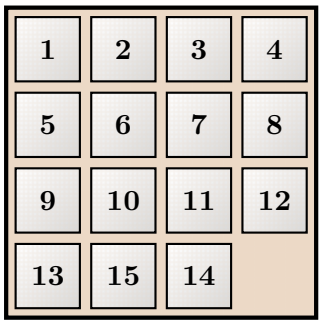


FIGURE 1. The advertising position

The game consists of a box containing fifteen numbered squared tiles and one empty square. You can slide neighboring tiles to the empty square, and so change the position. The aim of the game is to transform a given starting position to the final position in which the tiles are numbered gradually from the top left corner to the right bottom corner, where the empty square is positioned (see Figure 2).

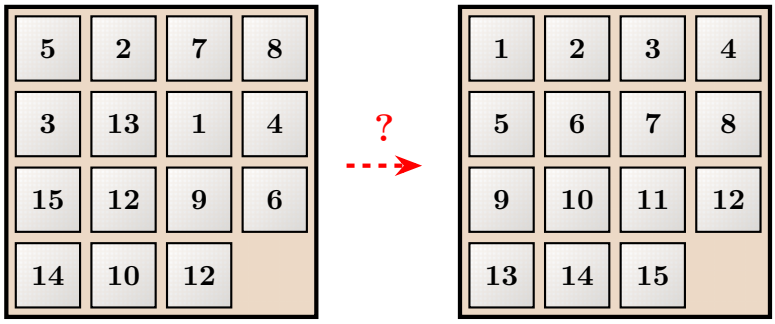


FIGURE 2. The 15 puzzle

We can assign the number 16 to the empty space, and so we can write down each position as a permutation of the set $\{1, 2, \ldots, 16\}$, where the final position corresponds to the unit permutation. For example, the starting position on Figure 2 is written as

$$(1, 7, 3, 5) \cdot (4, 8) \cdot (6, 12, 15, 9, 11, 10, 14, 13).$$

We call a position *standard* if the empty square is in the right bootom corner (the position 16). We claim that

Proposition 3.10. *Standard positions corresponding to odd permutations are unsolvable.*

Proof. We will use the *chessboard trick*. Lets call one slide of a tile to the empty square a *move*. Color the box as in Figure 3 making it a small chessboard, and observe that one-move changes the color of the empty square, from black to white and conversely.

Let the starting position correspond to an odd permutation, say σ. A sequence of moves corresponds to a permutation, say π, and the resulting position corresponds to the product $\pi \cdot \sigma$. Since the starting position is standard, and so the empty square is black, the color of the empty space in the resulting position is black if and only if π is even. Since the product of an even and an odd permutation is odd, the empty space in the resulting position is black if and only if the corresponding permutation is odd. However, the final position corresponds to the unit permutation, which is even. It follows that the starting position is unsolvable.

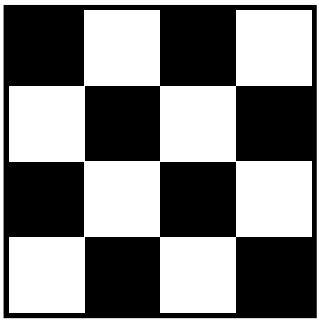


FIGURE 3. The small chessboard

□

EXERCISES

Exercise 3.1. *Let $\boldsymbol{G} = (G, \cdot)$ be a group. Define a binary operation $*$ on the set G by*

$$g * h = g \cdot h^{-1}, \text{ for all } g, h \in G.$$

Prove that all sub-universes of the group $\boldsymbol{G}$ are underlying sets of subgroups of $\boldsymbol{G}$.

Exercise 3.2. *According to Proposition 2.4 we can define a group $\boldsymbol{G}$, as an algebra with an underlying set G and*

- *an associative binary operation, say $\cdot$,*
- *a nulary operation u satisfying $g \cdot u = u \cdot g = g$, for all $g \in G$,*
- *a binary operation $^{-1}$ such that $g \cdot g^{-1} = g^{-1} \cdot g = u$, for all $g \in G$.*

Prove that when we apply this definition, all sub-universes of a group are underlying sets of subgroups.

Exercise 3.3. *Prove that whatever of the two definitions of a group we apply, sub-universes of a finite group are underlying sets of subgroups of the group.*

Exercise 3.4. *Let* $\pi \in \boldsymbol{S_n}$. *Prove that* $\operatorname{sgn} \pi = (-1)^k$ *where* k *is the number of blocks of* π *of even size.*

Exercise 3.5. *Prove that a cycle of the length* k *is not a product of less than* $k-1$ *transpositions.*

Exercise 3.6. *Decide whether the area on Figure 4 can be covered by domino tiles.* [Hint: Use the chessboard trick.]

The area *A domino tile*

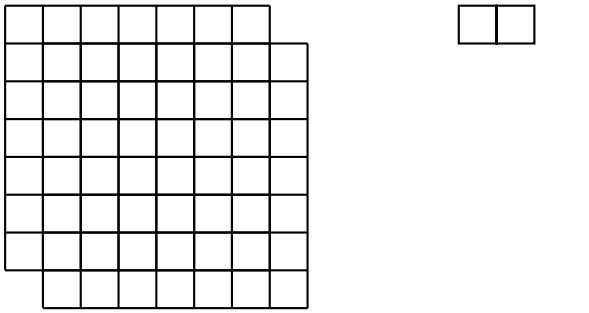


FIGURE 4. Covering by domino tiles