ALGEBRA I (LECTURE NOTES 2017/2018)
LECTURE 3 - SYMMETRIC GROUPS

PAVEL RŮŽIČKA

3.1. **Permutations.** By a *permutation* of a finite set we mean a one-to-one map from the set onto itself.

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, where the multiplication of permutations corresponds to the composition of maps. The composition is associative and so is the multiplication of permutations. The identity map corresponds to the unit element of $\boldsymbol{S_n} = (S_n, \cdot)$, called a *unit permutation*. Since one-to-one maps on a finite set are bijection, they are equipped with inverses. It follows that $\boldsymbol{S_n}$ is a group. We will called $\boldsymbol{S_n}$ the *symmetric group* on the n-elements set.

Exercise 3.1. *Prove that* $|S_n| = n!$.

Similarly as in the case of the composition of maps, we multiply permutations from left to right. That is, given permutations π and $\sigma \in S_n$ and $a \in \{1, 2, \dots, n\}$, we have that

$$(\sigma \cdot \pi)(a) = \sigma(\pi(a)).$$

There are several ways how to write down permutations. The simplest one is to put a permutation $\pi\colon \{1, 2, \dots, n\} \to \{1, 2, \dots, n\}$ down as the sequence $\langle \pi(1), \dots, \pi(n) \rangle$. Another familiar way of writing down a permutation π is to decompose it as a product of independent cycles.

A *block* of a permutation π is the smallest non-empty subset of $\{1, 2, \dots, n\}$, say B, such that $\pi(B) \subseteq B$. Let us use the notation $\pi^k := \underbrace{\pi \cdots \pi}_{k\times}$. Observe that

$$B = \{a, \pi(a), \pi^2(a), \dots\}, \tag{3.1}$$

for an arbitrary $a \in B$. Since the blocks B are finite, (in fact, the size of B is the least positive integer k such that $\pi^k(a) = a$), it suffices to consider, in (3.1), the images $\pi^i(a)$ up to $\pi^{k-1}(a)$.

Date: October 23, 2017.

Lemma 3.1. *Let π be a permutation of the set $\{1,2,\dots,n\}$. The blocks of π form a partition of $\{1,2,\dots,n\}$.*

Proof. If $a \in \{1,2,\dots,n\}$, then $\{a, \pi(a), \pi^2(a), \dots\}$ is a block of π. Therefore $\{1,2,\dots,n\}$ is the union of all blocks of π.

Let A and B be blocks of π and suppose that $a \in A \cap B$. Then both A and B are given by (3.1), and so $A = B$. Therefore the blocks A and B are either disjoint or equal. The lemma readily follows. □

Exercise 3.2. *Let π be a permutation of the set $\{1,2,\dots,n\}$. Write $a \sim_\pi b$ if there is $k \in \mathbb{N}_0$ such that $\pi^k(a) = b$. Prove that $\sim_\pi$ is an equivalence on the set $\{1,2,\dots,n\}$ and that blocks of $\sim_\pi$ correspond to blocks of π.*

Definition 3.2. Let $\boldsymbol{G} = (G, \cdot)$ be a grupoid. We say that elements $a, b \in G$ *commute* if $a \cdot b = b \cdot a$. The grupoid $\boldsymbol{G}$ is called *commutative* provided that all pairs of its elements commute.

Let $\pi \in S_n$ be a permutation. The *support* of π is the set

$$\operatorname{supp} \pi := \{a \in \{1,2,\dots,n\} \mid \pi(a) \neq a\}.$$

Permutations $\pi, \sigma \in S_n$ are called *independent* if $\operatorname{supp}\pi \cap \operatorname{supp}\sigma = \emptyset$. Notice that independent permutations commute. Indeed, since π is one-to-one, $\pi(a) \neq a$, implies that $\pi^2(a) \neq \pi(a)$. Therefore $\pi(\operatorname{supp}\pi) = \operatorname{supp}\pi$. We infer that if $\pi, \sigma \in S_n$ are independent and $a \in \{1,2,\dots,n\}$, then

$$\pi(\sigma(a)) = \sigma(\pi(a)) = \begin{cases} \pi(a) & \text{if } a \in \operatorname{supp}\pi; \\ a & \text{if } a \notin \operatorname{supp}\pi \cup \operatorname{supp}\sigma; \\ \sigma(a) & \text{if } a \in \operatorname{supp}\sigma. \end{cases}$$

A *cycle* is a permutation with at most one non-singleton block. More precisely, a *k-cycle* (for $2 \geq k$) is a cycle with the non-singleton block of size k. A *1-cycle* or a *trivial cycle* corresponds to the identity. Given a k-cycle γ with $2 \geq k$, we will use the notation

$$\gamma = (a, \gamma(a), \gamma^2(a), \dots, \gamma^{k-1}(a)),$$

where a is an element of $\operatorname{supp}\gamma$. By (i), where $a \in \{1,2,\dots,n\}$ is arbitrary, we mean a trivial cycle.

Let $\pi \in S_n$ be a permutation and $B_1, \dots, B_m$ all non-trivial blocks of π. For each $j \in \{1,2,\dots,m\}$ we pick an element $b_j \in B_j$ and we set

$$\gamma_j := (b_j, \pi(b_j), \dots, \pi^{|B_j|-1}(b_j)).$$

Since the blocks of π form a partition of the set $\{1, 2, \ldots, n\}$ due to Lemma 3.1, the cycles $\gamma_1, \ldots, \gamma_m$ are independent. It follows that

$$\pi = \gamma_1 \cdot \gamma_2 \cdot \cdots \cdot \gamma_m. \tag{3.2}$$

The expression (3.2) is called the *decomposition* of the permutation π into the product of independent cycles. Since the cycles $\gamma_1, \gamma_2, \ldots, \gamma_m$ are independent, we can freely change their order in (3.2). On the other hand, the set $\{\gamma_1, \gamma_2, \ldots, \gamma_m\}$ is determined by the permutation π. It follows that

Theorem 3.3. *Every permutation has a unique (up to the order of cycles) decomposition into the product of independent cycles.*

Let us write a simple algorithm that decomposes a permutation, say π, on a set $\{1, 2, \ldots, n\}$ into a product of independent cyclic permutations:

Algorithm: Decomposition into cyclic permutations

```
 1: procedure Decompose
    input a permutation π ∈ S_n
 2:    R ← {1, 2, ..., n}
 3: loop A:
 4:    until R = ∅ do
 5:    j ← min R
 6:    R ← R \ {j}
 7:    start a new cycle with j
 8:    loop B:
 9:    if π(j) ∈ R do
10:       R ← R \ {j}
11:       j ← π(j)
12:       add j to the cycle
13:       goto loop B
14:    close the cycle
15:    goto loop A
16: remove all cycles of length 1
17: close;
```

Example 3.1. *For example the permutation*

$$\langle 6, 8, 14, 20, 5, 3, 11, 4, 17, 18, 7, 13, 12, 1, 16, 15, 10, 9, 2, 19 \rangle$$

decomposes as

$$(1, 6, 3, 14) \cdot (2, 8, 4, 20, 19) \cdot (7, 11) \cdot (9, 17, 10, 18) \cdot (12, 13) \cdot (15, 16).$$

Exercise 3.3. *Recall that we compose permutations from right to left. Write a pseudo-code of an algorithm whose input is a sequence of (not necessarily independent) cycles from $\boldsymbol{S_n}$ and whose output is the decomposition of their product (in the given order) into a product of independent cycles.*

3.2. **Sub-universes and sub-algebras.** A *sub-universe* of the algebra $\boldsymbol{A}$ is a subset of B of its underlying set A that is closed under all the operations of $\boldsymbol{A}$. Let $\mathcal{C}$ be a class of algebras (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 3.4. By a *subgroup* of a group $\boldsymbol{G}$ we mean its $\mathcal{G}$-sub-algebra, 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*.

Observe that when we define a group as an algebra with a cancellative and divisible operation, not all sub-universes of a groups corresponds to its subgroup in general. For example, the positive integers form a sub-universe but not a subgroup of the group of all integers with the operation of addition.

Exercise 3.4. *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 3.5. *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 3.6. *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.*