ADVANCED ALGEBRA, LECTURE II, SEPTEMBER 16TH

1. Symmetric groups

The fundamental example of a group is that of the group of automorphisms of some set X. If X is finite of cardinality $n := \#X$ then enumerating its elements one identifies X with $\{1, 2, \dots, n\}$.

Definition 1.1. *The group of automorphisms of the set $\{1, 2, \dots, n\}$ is called the symmetric group (or the permutation group) on n letters and is denoted by S_n.*

Let us find the order of S_n. An element $a \in S_n$ by definition acts as an automorphism of the set $\{1, 2, \dots, n\}$; there are n possibilities of send the element 1 to any other element of $\{1, 2, \dots, n\}$. Once the value of $a(1)$ is fixed, there remain $n-1$ possibilities of sending the element 2 to any other element of $\{1, 2, \dots, n\} \setminus \{a(1)\}$ (recall that a is an automorphism, hence necessarily an injective map). Going down in this fashion to $a(n)$, we obtain $\#S_n = n \cdot (n-1) \cdot (n-2) \cdot \dots \cdot 1 = n!$.

Thus, elements of the symmetric group S_n are simply the permutations of the set $\{1, 2, \dots, n\}$ (hence another name the permutation group for it). It is customary to write such a permutation $a \in S_n$ as the following array:

$$\begin{pmatrix} 1 & 2 & 3 & \cdots & n-1 & n \\ a(1) & a(2) & a(3) & \cdots & a(n-1) & a(n) \end{pmatrix}$$

in which the second line is the image of $\{1, 2, \dots, n\}$ under the map a. It is more often than not the upper line is omitted and the permutation is simply written as $(a(1), a(2), \cdots, a(n-1), a(n))$.

The group S_n has distinguished elements τ_{ij} that send a pair $(i, j), 1 \leq i < j \leq n$ to $(\tau_{ij}(i), \tau_{ij}(j))$ and fix all other elements of $\{1, 2, \dots, n\}$. The elements τ_{ij} are called *transpositions*. Observe that the order of a transposition is equal to two: $\tau_{ij}^2 = e$.

If $n = 1$ then $S_1 = \langle e \rangle$ is the trivial one-element group; for $n = 2$ the group S_2 consists of two elements and is isomorphic to the group $\langle e, a \mid a^2 = e \rangle = \mathbb{Z}/2\mathbb{Z}$. The first interesting case of symmetric groups is that of S_3. Let us look at it more carefully.

1.1. $\mathbf{S_3}$.

First, the order of S_3 is equal to $3! = 6$. We can list its elements by considering all the permutations of $\{1, 2, \dots, 3\}$. This gives:

$$e = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix},\ \tau_{12} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix},\ \tau_{23} = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix},\ \tau_{13} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$$

$$\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix},\ \sigma' = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}.$$

Thus, the non-trivial elements of S_3 consist of the three transpositions $\tau_{12}, \tau_{23}, \tau_{13}$, and the two elements σ, σ'. The example of S_3 is remarkable for a few reasons, one of them being that S_3 is

Date: 09/16/2022, Math in Moscow.

the smallest example of a non-commutative group. Recall that a group $(G, \cdot)$ is commutative if for any elements $a, b \in G$ the equality holds:

$$a \cdot b = b \cdot a.$$

Considering the elements τ_{12} and σ of S_3, and computing their products in different orders, we obtain:

$$\sigma \cdot \tau_{12} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} = \tau_{13}, \quad \tau_{12} \cdot \sigma = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} = \tau_{23}. \tag{1}$$

Thus, $\sigma \cdot \tau_{12} \neq \tau_{12} \cdot \sigma$ and the group S_3 is non-commutative. We have:

Corollary 1.1. *The group S_n is non-commutative for $n \geq 3$.*

Proof. For $n = 3$ this is the statement shown just above. If $n > 3$ then S_3 can be embedded into S_n (i.e., S_3 is a subgroup of S_n) as a subset of those automorphisms of $\{1, 2, \ldots, n\}$ that fix the subset $\{4, 5, \ldots, n\} \subset \{1, 2, \ldots, n\}$ and permute only $\{1, 2, 3\}$. Thus, there are elements inside S_n (belonging to that copy of S_3 - and, in fact, many more) that do not commute with each other. □

Coming back to (1), let us deduce some more consequences from those equalities. The first one gives $\sigma \cdot \tau_{12} = \tau_{13}$. Remembering that the order of a transposition is two, we can multiply the above equation by τ_{12} on the right and obtain

$$\sigma = \sigma \cdot \tau_{12} \cdot \tau_{12}^{-1} = \sigma \cdot \tau_{12} \cdot \tau_{12} = \tau_{13} \cdot \tau_{12}.$$

Similarly, considering the second equation $\tau_{12} \cdot \sigma = \tau_{23}$ and multiplying it with τ_{12} on the left, we obtain

$$\sigma = \tau_{12}^{-1} \cdot \tau_{12} \cdot \sigma = \tau_{12} \cdot \tau_{12} \cdot \sigma = \tau_{12} \cdot \tau_{23}.$$

Combining the two equalities, we get $\tau_{13} \cdot \tau_{12} = \tau_{12} \cdot \tau_{23} = \sigma$. We have obtained two different presentations of the element σ as a product of transpositions. Observe that, despite that the sets of transpositions in each presentation ($\{\tau_{13}, \tau_{12}\}$ and $\{\tau_{12}, \tau_{23}\}$) are different from one another, the number of transpositions in each presentation is the same and is equal to two. This is a general fact valid for any symmetric group S_n: each element σ of S_n can be presented as a product of transpositions. More importantly, the numbers of transpositions in each presentation of σ with the *minimal* number of transpositions are the same regardless of a presentation. This number is called *the length of* σ and is denoted by $l(\sigma)$.

2. Group actions

2.1. **Automorhisms of sets.** Let X be a set, and G be a group.

Definition 2.1. *A left action of G on X is the map $a : G \times X \to X$, such that the following conditions are satisfied. In what follows, given an element $g \in G$ and an element $x \in X$, we denote $a(g, x) \in X$ by $g \cdot x$.*

1. *$e_G \cdot x = x$ for any $x \in X$;*
2. *$(gh) \cdot x = g \cdot (h \cdot x)$.*

Similarly, a right action of G on X is the map $a : G \times X \to X$, such that:

1. *$e_G \cdot x = x$ for any $x \in X$;*
2. *$(gh) \cdot x = h \cdot (g \cdot x)$.*

An expression justifying the term "right action" of G on X is the data of a map $X \times G \to X$, which is also denoted by $\cdot$, such that

(1) $x = x \cdot e$ for any $x \in X$;
(2) $x \cdot (gh) = (x \cdot g) \cdot h$.

Given a set X, its automorphisms $\mathrm{A}ut(X)$, i.e. bijective maps $X \to X$, form a group under the composition of maps (denoted by $\circ$) and the unit element being the identity map $\mathsf{id} : X \to X$. In these terms, a left action of the group G on X can be expressed as saying that one is given a group homomorphism

$$G \to \mathrm{A}ut(X).$$

In this language, left actions of a group G on a set X can be described precisely as homomorphisms $G \to \mathrm{A}ut(X)$.

To place right actions of G on equal footing, recall that a group $(G, \cdot)$ gives rise to the opposite group $(G, *)$; in this language, a right action of G on X is a homomorphism from the opposite group to G to $\mathrm{A}ut(X)$.

3. Basic theorems on finite groups

3.1. **Examples of group actions.** Let G be a group and $X = G$ be the underlying set of G. There are three natural actions of G on itself:

(1) Left regular action $l_g : G \to \mathrm{A}ut(G)$ defined via

$$l_g(h) := g \cdot h;$$

(2) Right regular action $l_g : G \to \mathrm{A}ut(G)$ defined via

$$r_g(h) := h \cdot g;$$

(3) Conjugation action $c_g : G \to \mathrm{A}ut(G)$ defined via

$$c_g(h) := g \cdot h \cdot g^{-1}.$$

Let us check that l_g is a left action. Setting $g = e_G$, we have $l_{e_G}(h) = e_G \cdot h = h$ for any $h \in G$, so $l_{e_G} = \mathrm{id}_G$. Further, let $g_1, g_2 \in G$ and consider $l_{g_1 \cdot g_2}$; its value on an element $h \in G$ is $l_{g_1 \cdot g_2}(h) = g_1 \cdot g_2 \cdot h = g_1 \cdot (g_2 \cdot h) = l_{g_1}(g_2 \cdot h) = l_{g_1}(l_{g_2}(h))$. Since h was arbitrary, we see that the transformation $l_{g_1 \cdot g_2}$ is equal to the composition $l_{g_1} \circ l_{g_2}$. Finally, for any l_g the transformation $l_{g^{-1}}$ is its inverse in $\mathrm{A}ut(G)$.

Theorem 3.1 (Cayley theorem)**.** *Let G be a finite group of order n. Then there is an injective homomorphism $G \to S_n$.*

Proof. To give such a homomorphism is equivalent to giving a (left) action of G on the set $\{1, 2, \ldots, n\}$ (recall that $n = \#G$). The left action l_g of G on itself gives us the sought-for homomorphism $G \to \mathrm{A}ut(G) = S_n$. One needs only verify that this homomorphism is injective: assuming that there is $g \in G, g \neq e_G$ such that $l_g = \mathrm{id}_G$ we would have

$$l_g(h) = g \cdot h = h \quad \forall h \in G.$$

This can only happen if $g = e_G$, but $g \neq e_G$ by the assumption. Thus, l_g is injective. □