LECTURE 3: ABSTRACT GROUPS AND GROUP PRESENTATIONS

The theory of transformation groups began in the work of several great mathematicians: Lagrange, Galois, Sophus Lie, Felix Klein, Élie Cartan, Herman Weyl. At the beginning of the 20th Century, algebraists decided to "generalize" this theory to the formalistic theory of so-called *abstract groups*. In this lecture we will study this formal theory and learn that it is not a generalization at all: *Cayley's theorem* says that all abstract groups are actually transformation groups. We will also learn that two important classes of groups (*free groups* and *permutation groups*) have certain universality properties. Finally, we will learn how *to present groups* by means of generators and relations (=образующие и соотношения); this allows to replace computations with groups by games with words.

§3.1. Abstract groups

By definition, an (abstract) *group* is a set G of arbitrary elements supplied with a binary operation $*$ (usually called *multiplication*) if it obeys the following rules:

- (*neutral element axiom*) there exists a unique element $e \in G$ such that $g * e = e * g = g$ for any $g \in G$;
- (*inverse element axiom*) for any $g \in G$ there exists a unique element $g^{-1} \in G$, called *inverse to g*, such that $g * g^{-1} = g^{-1} * g = e$;
- (*associativity axiom*) $(g * h) * k = g * (h * k)$ for all $g, h, k \in G$.

A group $(G, *)$ is called *commutative* or *Abelian* if $g * h = h * g$ for all $g, h \in G$ (in that case the operation is usually called the *sum* and the inverse element usually denoted by $-g$ instead of g^{-1}). Let $(G, *)$, $(H, \circ)$ be groups, $\phi : G \to H$ a mapping; ϕ is called a *homomorphism* (or a *morphism of groups*) if it preserves the operations, i.e., $\phi(g_1 * g_2) = \phi(g_1) \circ \phi(g_2)$); a homomorphism ϕ is a *monomorphism* (respectively, an *epimorphism* or an *isomorphism*) if the mapping ϕ is injective (resp., surjective or bijective). From the point of view of abstract algebra, isomorphic groups are identical.

The notions of *order* (of elements of a group and of the group itself) and of *generator* for abstract groups are defined exactly like for transformation groups (see §1.3).

Examples: any transformation group is a group; the following groups are standard (you should know them):

- $\mathbb{Z}_{/m}$, residues modulo m;
- $\mathbb{S}_n$, permutations on n objects;
- $F(a_1, \dots, a_k)$, the free group on k generators;
- $GL(n)$, linear operators on $\mathbb{R}^n$;
- $O(n)$ and $SO(n)$, orthogonal and positive orthogonal operators on $\mathbb{R}^n$.

¿From now on we omit the group operation symbol, i.e., we write gh instead of $g * h$.

A *subgroup* H of a group G is a subset of G which satisfies the group axioms. A subgroup $H \subset G$ is *normal* if $gHg^{-1} = H$ for any $g \in G$. If H is a subgroup of G, then a *coset* (=класс смежности) $H_g \subset G$, for some $g \in G$, is the set of all elements of the form gh for $h \in H$. Two cosets either do not intersect or coincide. If H is normal, there is a well-defined (=корректно определенная) operation in the family of cosets: the product of two cosets is the coset containing the product of any two elements of these cosets; the family of cosets supplied with this product operation satisfies the group axioms; it is called the *quotient group* (=факторгруппа) of G by H and is denoted by G/H.

Example: in the additive group of integers $(\mathbb{Z},+)$, elements of the form $5k$, $k \in \mathbb{Z}$, constitute a normal subgroup, denoted $5\mathbb{Z}$; the corresponding quotient group $\mathbb{Z}/5\mathbb{Z}$ is isomorphic to the group $\mathbb{Z}_5$.

§3.2. The Lagrange theorem

The elementary theorem proved below is the first structure theorem about abstract groups. It was proved (for transformation groups) almost two centuries ago by Lagrange.

Theorem 1. *If H is a subgroup of a finite group G, then the order of H divides the order of G.*

Proof. The cosets of H in G form a partition of the set of elements of G and all have the same number of elements as H. $\square$

Corollary. *Any group G of prime order p is isomorphic to $\mathbb{Z}_p$.*

Proof. Let $g \in G$, $g \neq e$. Let m be the smallest positive integer such that $g^m = e$. Then $H := \{e, g, g^2, \ldots, g^{m-1}\}$ is a subgroup of G (why?) and by Theorem 1, m divides p. This is impossible unless $m = p$, but then $H = G$ is obviously isomorphic to $\mathbb{Z}_p$. $\square$

§3.3. Free groups and permutations

In this section, we study two classes of groups: the free groups (which have the "least structure") and the permutation groups (which have the "most structure").

Let $F := \{f_1, \ldots, f_k\}$ be a set of symbols. Then the set of formal symbols (called *letters*)

$$A := \{e, f_1, \ldots, f_k, f_1^{-1}, \ldots, f_k^{-1}\}$$

will be our *alphabet*. A string of letters from our alphabet will be called a *word*. Two words w_1 and w_2 are called *equivalent*, if one can be obtained from the other by using the following *trivial relations* $f_i f_i^{-1} = f_i^{-1} f_i = e$ for any i and $fe = ef = f$ for any $f \in A$; for example

$$f_1 f_3^{-1} \sim f_1 f_3^{-1} e \sim f_1 f_3^{-1} f_2 f_2^{-1} \sim f_1 f_3^{-1} f_2 e f_2^{-1}.$$

The *product* of two words is defined as their concatenation (i.e., writing then one after the other). The *free group* with generators $f_1, \ldots, f_k$ is defined as the set of equivalence classes of words supplied with the product (concatenation) operation and is denoted by $\mathbb{F} = \mathbb{F}[f_1, \ldots, f_k]$.

For example, $\mathbb{F}[f]$ is isomorphic to $(\mathbb{Z},+)$, while $\mathbb{F}[f_1, f_2]$ is not commutative.

The *permutation group* on n objects (=группа пеерстановок n объектов) is the family of all bijections of the set $\{1, 2, \ldots, n\}$ supplied with the operation of composition; it is denoted by $\mathbb{S}_n$. It consists of $n!$ elements denoted by $[i_1, \ldots, i_n]$, where $i_k := \beta(k)$ and β is the bijection defining the given element.

Free groups and permutation groups have important "universality" properties.

Theorem 2. (i) *For any finite group G there exists a monomorphism of G into $\mathbb{S}_n$ for some n.*

(ii) *For any group G with a finite number of generators there exists an epimorphism of $\mathbb{F}_n$ (for some n) onto G.*

Sketch of the proof. (i) Let $|G| = n$ and $g_0 \in G$; then the mapping

$$G \ni g \mapsto gg_0 \in G$$

is a bijection of the n-element set G; this bijection can be identified with an element of $\mathbb{S}_n$. Thus we have obtained a mapping $G \to \mathbb{S}_n$; it is not difficult to prove that this mapping is a monomorphism.

(ii) Let $g_1, \ldots, g_n$ be a set of generators of G. Then it is not difficult to prove that the mapping $\alpha : \mathbb{F}[f_1, \ldots, f_n] \to G$ given by $\alpha(f_i) = g_i$, $i = 1, \ldots, n$, is an epimorphism. $\square$

§3.4. Group presentations

A presentation of a group (=заадние группы образующими и соотношениями) is a way of defining the group by means of equations (called *defining relations*) in the generators of the group. The formal definition is the following. An expression of the form

$$G = \langle g_1, \ldots, g_n \ : R_1, \ldots, R_k \rangle,$$

where $R_1, \ldots R_k$ are words (*relators*) in the alphabet $A = \{g_1, \ldots, g_n g_1^{-1}, \ldots, g_n^{-1}\}$, is called a *presentation* of the group G; the group G is defined by its presentation as the quotient group

$$\mathbb{F}[g_1, \ldots, g_n]/\{R_1, \ldots, R_k\},$$

where $\{R_1, \ldots, R_k\}$ is the minimal (by inclusion) normal subgroup of $\mathbb{F}[g_1, \ldots, g_n]$ containing the elements $R_1, \ldots, R_k$.

This formal definition is difficult to understand. But the notion of group presentation is simple. It means that elements of G are words in the alphabet A defined up to the trivial relations (see §3.3 above) and the relations $R_1 = e, \ldots, R_k = e$; the product is concatenation.

Here are some examples:

- $\mathbb{Z}_{/m} = \langle a \ : a^m \rangle$;
- $\mathbb{F}[g_1, \ldots, g_n] = \langle g_1, \ldots, g_n \ : \quad \rangle$;
- $\mathbb{S}_3 = \langle s_1, s_2, s_3 \ : s_1^2,\ s_2^2,\ s_3^2,\ s_1 s_2 s_1 s_2^{-1} s_1^{-1} s_2^{-1},\ s_1 s_2 s_1 s_2^{-1} s_1^{-1} s_2^{-1} \rangle$.

More details and examples will be given in the exercise class.

§3.5. Cayley's theorem

The following theorem (due to Cayley) shows that the notion of abstract group is not a real generalization: all groups are in fact transformation groups!

Theorem 3. *Any group G is the transformation group acting on the set G by right multiplication: $g \mapsto gg_0$ for any $g_0 \in G$.*

The proof is a straightforward verification. $\square$

Corollary. *Any group is a geometry in the sense of the formal definition given in* §1.1.