ADVANCED ALGEBRA, LECTURE I, SEPTEMBER 9TH

1. Groups

1.1. **Motivation and definitions.** Groups arise in nature as symmetries of objects. Given a set M, a symmetry of M is a *bijective* map $f : M \to M$. Starting from this, we can consider arbitrary maps $f : M \to M$. Given two such maps f and g, one can compose them obtaining the third map $h := f \circ g$. Specifically, given an element $a \in M$, set $(f \circ g)(a) := f(g(a))$. Let $\mathrm{M}aps(M, M)$ denote the set of self-maps from M to M.

1.2. **Semigroups.** The structure of composition of elements of $\mathrm{M}aps(M, M)$ leads to the following definition.

Definition 1.1. *A set M is called a semigroup if there is a binary operation $\circ : M \times M \to M$, usually called* **multiplication***, such that the associativity property holds:*

$$(a \circ b) \circ c = a \circ (b \circ c)$$

for $a, b, c \in M$.

Remark 1.1. One can drop the condition of associativity and consider sets equipped with just a binary operation on those. This leads to a wider class of objects but we are not going to discuss them here.

1.3. **Monoids.** Coming back to $\mathrm{M}aps(M, M)$, we observe that this semigroup has an extra property, namely that it possesses a distinguished element id_M, the identity map on M. A structure modelled on this property gives the next definition.

Definition 1.2. *A semigroup $(M, \circ)$ is called a monoid if there is an element $e \in M$, called* **a neutral element***, such that the following holds:*

$$a \circ e = a = e \circ a$$

for $\forall a \in M$.

One immediate consequence from the above definition is that such a neutral element is unique: assuming that there are two neutral elements e, e' and using the property above, we have, on the one hand

$$e \circ e' = e,$$

since e' is neutral, and on the other hand

$$e \circ e' = e',$$

since e is neutral too. This gives $e = e'$, so we can speak about the neutral element, or simply the unit element of M with respect to the given multiplication $\circ$.

The condition of being neutral can be weakened to the one of being neutral on one side: i.e., instead of demanding the condition $a \circ e = a = e \circ a, \forall a \in M$, we demand $a \circ e = a, \forall a \in M$ (resp.,

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

$a = e \circ a$). One can not claim uniqueness of a neutral element in this situation (see Homework #1 for more about this).

1.4. **Groups.** Given a set M, the monoid $\mathrm{M}aps(M, M)$ contains a subset $\mathrm{B}ij(M, M)$ of bijective self-maps. A bijective map $f : M \to M$ has an inverse map $g : M \to M$ such that both compositions $f \circ g$ and $g \circ f$ are equal to id_M. Formalizing this structure leads to the definition of a group (what has been referred to as "symmetries of objects" in the beginning).

Quite naturally, groups are usually denoted by the letter G. One also stresses that the binary operation $\circ$ on G comes from a sort of multiplication; it is hence denoted by $\cdot$; quite often it will be omitted later on, and the result of multiplication of two elements a and b will be simply written as ab.

Definition 1.3. *A monoid $(G, \cdot)$ is called a group if for any element $a \in G$ there exists an element b called an inverse to a (and usually denoted by a^{-1}) such that*

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

Quite similarly to the uniqueness of neutral element in a monoid, one proves the uniqueness of an inverse element (see Homework #1).

2. Examples and first constructions of groups

Given a group G, sometimes we denote the neutral element $e \in G$ by e_G to emphasise the fact that it belongs to G.

Example 2.1. Integer numbers form a group under addition with the unit element being 0; this group is denoted $\mathbb{Z}$.

Example 2.2. Let $\mathbb{Q}$ denote the rational numbers, i.e. the set of all fractions $\frac{m}{n}$ where m, n are integers, and $n \neq 0$. Then $\mathbb{Q}$ is a group under addition. Furthermore, the non-zero elements of $\mathbb{Q}$ form a group under multiplication, denoted by $\mathbb{Q}^*$.

Example 2.3. The real numbers $\mathbb{R}$ and complex numbers $\mathbb{C}$ are groups under addition. The non-zero real numbers $\mathbb{R}^* := \mathbb{R} \setminus \{0\}$ and non-zero complex numbers $\mathbb{C}^* := \mathbb{C} \setminus \{0\}$ are groups under multiplication.

Example 2.4. The complex numbers of absolute value 1 form a group under multiplication.

Example 2.5. The set consisting of the numbers $1, 1$ is a group under multiplication, and this group has 2 elements.

Example 2.6. *Given a group G, let $\cdot$ denote the multiplication operation in G (in what follows, $(G, \cdot)$ is the shortened notation for that). Consider the same set G and define a new multiplication $*$ on G via*

$$g * h := h \cdot g,$$

for any $g, h \in G$. One checks immediately that G with this new operation $*$ is also a group. It is called the **opposite** *group to G.*

Example 2.7. Let n be an integer. Residues modulo n form a group called the cyclic group of order n (see the definition below); this group is denoted $\mathbb{Z}/n\mathbb{Z}$.

Example 2.8. The groups of symmetries of an equilateral n–polygon (e.g., of an equilateral triangle, of a square) is a finite group of order $2n$. We will study these groups later in more detail.

2.1. **Subgroups.** Let $(G, \cdot)$ be a group. Assume given a subset $H \subset G$. We can restrict the multiplication operation in G to H, obtaining the map $\cdot : H \times H \to G \times G \to G$. Here the first map is the embedding of the product and the second map is the multiplication in G.

Definition 2.1. *A subset $H \subset G$ is a subgroup if the above map lands in H, the unit element e_G belongs to H, and moreover for any $h \in H$ its inverse element h^{-1} also belongs to H.*

The first two examples of subgroups of G are the group $\langle e_G \rangle$ consisting of the single unit element and the whole group G.

3. Homomorphisms. Cyclic subgroups.

Definition 3.1. *Let G and G' be two groups. A map $f : G \to G'$ is called a homomorphism if f preserves the group structures on G and G'. In other words, for $a, b \in G$ one has $f(a \cdot b) = f(a) \cdot f(b)$ and $f(e_G) = e_{G'}$.*

Definition 3.2. *Let $f : G \to G'$ be a homomorphism. The subset of elements $g \in G$ such that $f(g) = e_{G'}$ is called the kernel of f and denoted* $\mathrm{Ker}(f)$.

The kernel of a homomorphism f is a subgroup of G; indeed, $e_G \in \mathrm{Ker}(f)$ by the definition of a homomorphism and if $g, h \in \mathrm{Ker}(f)$, then $f(g \cdot h) = f(g) \cdot f(h) = e_{G'}$. Finally, given a $g \in \mathrm{Ker}(f)$, we have

$$f(e_G) = f(g \cdot g^{-1}) = e_{G'} = f(g) \cdot f(g^{-1}) = f(g^{-1}).$$

Hence, $f(g^{-1}) = e_{G'}$ and $g^{-1} \in \mathrm{Ker}(f)$. Thus, $\mathrm{Ker}(f)$ is a subgroup of G.

Definition 3.3. *Let $f : G \to G'$ be a homomorphism. It is called injective if* $\mathrm{Ker}(f) = e_G$.

Given a group G and an element $g \in G$, consider the set of its powers $g^0 := e_G, g, g^2 = g \cdot g, \ldots, g^n = \underbrace{g \cdot \cdots \cdot g}_{n}$. Set $g^n = \underbrace{g^{-1} \cdot \cdots \cdot g^{-1}}_{-n}$ for negative values of n. We can arrange this in a group homomorphism:

$$\psi_g : \mathbb{Z} \to G, \quad n \to g^n.$$

There are two possibilities arising. One is that the above homomorphism is injective; in this case the element g is said to have *infinite* order. Another possibility is that the homomorphism ψ_g has a kernel. This kernel is a subgroup of $\mathbb{Z}$; subgroups of $\mathbb{Z}$ are described by the following lemma:

Lemma 3.1. *A subgroup of $\mathbb{Z}$ has the form $d\mathbb{Z}$ for some $d \geq 0$.*

Assume that ψ_g has a kernel. By the above lemma, $\mathrm{Ker}(\psi_g) = d\mathbb{Z}$ for $d \geq 0$.

Definition 3.4. *Let $g \in G$ be an element, such ψ_g has a kernel. Then d is called the order of g.*

Definition 3.5. *A homomorphism $f : G \to G'$ is called an isomorphism if f is injective and surjective. The latter property means that for any $g' \in G'$ there exists a $g \in G$, such that $f(g) = g'$.*