Introduction to representation theory
Lecture 2. Basic theory of groups

Alexei KOTOV

University of Hradec Králové
Faculty of Science

July 8, 2021, Hradec Kralove

A group is a set G together with an operation, which associates to each pair of elements g_1, g_2 their product $g_1 g_2$, satisfying the following properties :

- the product is associative, i.e. $g_1(g_2 g_3) = (g_1 g_2) g_3$;
- there exists a neutral element (identity) e, such that for any g one has $ge = eg = g$;
- for each g there exists an inverse g^{-1}, such that $gg^{-1} = g^{-1}g = e$.

A semigroup is an algebraic structure consisting of a set together with an associative binary operation. If there exists a neutral element, it is unique (which follows from the associativity). Then the semigroup is called a monoid.

If an inverse g^{-1} is defined, it is also unique. A group is a monoid with inverses.

Examples of groups

1. non-zero real, complex or rational numbers with respect to the usual multiplication;
2. symmetries of a system with respect to the composition;
3. all bijections $\mathrm{Aut}(X)$ of a set X with respect to the composition;
4. the general linear group $GL(V)$ of a vector space V over a field k $(= \mathbb{R}, \mathbb{C})$, consisting of all invertible linear maps $V \to V$.

A group is called commutative or abelian if the multiplication is commutative: $g_1 g_2 = g_2 g_1$ for all $g_1, g_2 \in G$.

Example 1 is commutative, while examples 3 and 4 are generally not, unless $|X| \leq 2$ and $\dim V = 1$, respectively.

A subgroup is a subset $H \subset G$ closed under the group multiplication and taking of inverses.

A subgroup H of G is called normal if it is stable under the conjugation, i.e. for all $g \in G$, $h \in H$

$$ghg^{-1} \in H$$

Given a subgroup $H \subset G$, we say that g_1 and g_2 are related if and only if there exists $h \in H$, such that $g_1 = g_2 h$. It is an equivalence relation, i.e. it is reflexive, symmetric and transitive. The set of equivalence classes $G/\sim$ is denoted by G/H.

If H is a normal group, then G/H is a group with respect to the operations

$$[g_1][g_2] = [g_1 g_2] \quad \text{and} \quad [g]^{-1} = [g^{-1}]$$

which are well-defined, i.e. the result does not depend on the choice of representatives. The neutral element in G/H is $[e]$.

Examples of subgroups

- non-zero rational numbers $\mathbb{Q}^*$ inside non-zero real numbers $\mathbb{R}^*$ and non-zero real numbers $\mathbb{R}^*$ inside non-zero complex numbers $\mathbb{C}^*$ (a subgroup of a subgroup is a subgroup!); all these subgroups are normal as any subgroup of a commutative group is normal!
- symmetries of a system inside all bijections;
- in particular, $\mathrm{GL}(V) \subset \mathrm{Aut}(V)$;
- the special linear group $\mathrm{SL}(V)$ of a finite-dimensional vector space V, consisting of all linear transformations with the determinant equals to 1; it is a normal subgroup
- the group center $Z(G) = \{g \mid gg' = g'g, \forall g' \in G\}$; it is a normal abelian subgroup;
- $\{\mathrm{Id}, -\mathrm{Id}\} \subset \mathrm{GL}(V)$; it is a normal subgroup. Moreover, it is the center of $\mathrm{GL}(V)$ if $\dim V > 1$;

Morphism of groups

A morphism of groups is a map $\phi\colon G_1 \to G_2$ which respects the group operations, i.e. for all $g, g_1, g_2 \in G_1$

$$\phi(g_1 g_2) = \phi(g_1)\phi(g_2) \;\text{ and }\; \phi(g^{-1}) = \phi(g)^{-1}$$

The kernel of a morphism ϕ

$$\mathrm{Ker}\phi = \{g \in G_1 \,|\, \phi(g) = e\}$$

is a normal subgroup of G_1, while the image of ϕ

$$\mathrm{Im}\phi = \{\phi(g) | g \in G_1\}$$

is a subgroup of G_2.

Morphism of groups

A morphism of groups is a monomorphism (epimorphism, isomorphism) if it is injective (surjective, bijective) as a map.

- $G_1/\mathrm{Ker}\phi \to G_2$ is a monomorphism;
- $G_1 \to \mathrm{Im}\phi$ is an epimorphism;
- $G_1/\mathrm{Ker}\phi \to \mathrm{Im}\phi$ is an isomorphism.

- The composition of two morphisms of groups is again a morphism of groups;
- The inverse of an isomorphism is an isomorphism.

The category of groups

A category is a collection of "objects"that are linked by "arrows".

A category C consists of

- a class ob(C) of objects;
- a class hom(C) of morphisms, or arrows, or maps between the objects;
- the composition of morphisms $\hom(a, b) \times \hom(b, c) \to \hom(a, c)$ for $a, b, c \in C$, which is associative;
- the identity $1_x \in \hom(x, x)$ for each object x, such that the composition of 1_x with any morphism, whenever it is possible, does not change this morphism.

All groups together with morphisms is a category with respect to the composition of morphisms.

More examples of groups, subgroups, and morphisms

- the set of all orthogonal linear transformations of a real vector space V with a scalar product $(,)$

$$O(V) = \{A \in GL(V) \,|, \; (Av_1, Av_2) = (v_1, v_2), v_1, v_2 \in V\}$$

- similar definition of the unitary group $U(V) \subset GL(V)$ for a complex vector space V with a Hermitian product;
- the subgroups $SO(V) \subset SL(V)$ and $SU(V) \subset SL(V)$ for finite-dimensional V, by requiring $\det A = 1$;
- the inclusion of any subgroup $H \hookrightarrow G$ is a monomorphism;
- the quotient map $G \twoheadrightarrow G/H$ for any normal subgroup $H \subset G$ is an epimorphism.

More examples of groups, subgroups, and morphisms

- $GL_n(k) = \{A \in Mat_n(k) \mid \det A \neq 0\}$
- $GL_n(k)$ is isomorphic to $GL(V)$ for any $n-$dimensional vector space over a field k;
- $SL_n(k) = \{A \in Mat_n(k) \mid \det A = 1\}$
- $SL_n(k)$ is isomorphic to $SL(V)$ for any $n-$dimensional vector space over a field k. In both case the choice of a basis in V uniquely determines such an isomorphism;
- $O_n(\mathbb{R}) = \{A \in Mat_n(\mathbb{R}) \mid AA^T = Id\}$
- $O_n(\mathbb{R})$ is isomorphic to $O(V)$ for any Euclidean $n-$dimensional vector space V; an isomorphism is uniquely determined by the choice of an orthogonal basis in V;
- $O(n) \cap SL(n) = SO_n(\mathbb{R}) \subset SL_n(\mathbb{R}) \subset GL(n, \mathbb{R})$ are subgroups.

More examples of groups, subgroups, and morphisms

- $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, any field k, any vector space V over k with respect to the sum are abelian groups;
- $\mathbb{Z} \subset \mathbb{R}$ is a normal subgroup (all structures are commutative);
- $\mathbb{R}/\mathbb{Z} = S^1$ - the group of rotations of the circle, the angle of rotation is parameterized by points of S^1;
- S^1 is isomorphic to the unitary group $U(1) = U(\mathbb{C}) = \{c \in \mathbb{C} \,|, |c| = 1\}$;
- The projection map $\mathbb{R} \to \mathbb{R}/\mathbb{Z}$ is given by $\mathbb{R} \ni a \mapsto \exp(2\pi i a) \in U(1)$
- $\mathbb{Z} \supset p\mathbb{Z} = \{pz \,|\, z \in \mathbb{Z}\}$ for a fixed $p \in \mathbb{Z}$ is a normal subgroup with respect to the sum. The quotient $\mathbb{Z}_p = \mathbb{Z}/p\mathbb{Z}$ is called the cyclic group of order p; $|\mathbb{Z}_p| = p$, $\mathbb{Z}_2$ is isomorphic to $\{1, -1\}$ (w.r.t. the multiplication of numbers).

Free groups

Let S be a set. The free group F_S over S consists of all words that can be built from elements of S, called the alphabet, considering two words to be different unless their equality follows from the group axioms.

For example, $s_1 s_2 s_3^{-1} s_2^{-1} s_3$ is a "good"word, but $s_1 s_2 s_2^{-1} s_3 = s_1 s_3$ for $s_1, s_2, s_3 \in S$.

F_S is universal and unique up to an isomorphism.

Assume that all elements of a group G can be represented as a product of elements of a subset $S \subset G$ and their inverses. Then $S \hookrightarrow G$ can be uniquely extended to a epimorphism of groups $F_S \twoheadrightarrow G$.

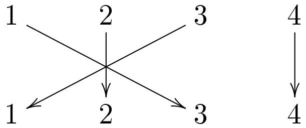
In the above case we say that G is generated by S. The kernel of $F_S \twoheadrightarrow G$ consists of relations.

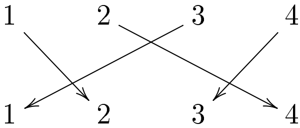
Permutation or symmetric groups

Permutations of n elements, denoted as $\mathbb{S}_{\mathrm{n}}$ is the group of bijections (or automorphisms) of the set $\{1, 2, \ldots, \mathrm{n}\}$.

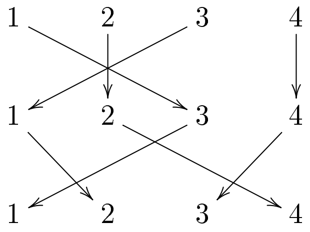
Example of permutations for $\mathrm{n} = 4$.

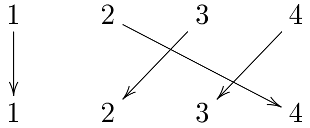
$$\tau = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 1 & 4 \end{pmatrix} \qquad \sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 1 & 3 \end{pmatrix}$$





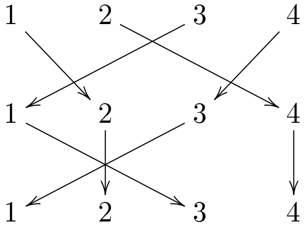
To get the product of two permutations $\sigma \circ \tau$, perform first τ, then σ:

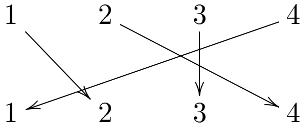




The result is $\quad \sigma \circ \tau = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 2 & 3 \end{pmatrix}$

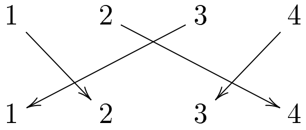
To get the product of two permutations $\tau \circ \sigma$, perform first σ, then τ:

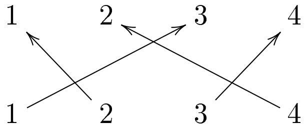




The result is $\tau \circ \sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 3 & 1 \end{pmatrix} \neq \sigma \circ \tau = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 2 & 3 \end{pmatrix}$

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 1 & 3 \end{pmatrix} \qquad \sigma^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 4 & 2 \end{pmatrix}$$



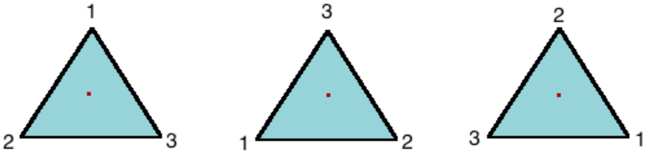


$$\sigma \circ \sigma^{-1} = \sigma^{-1} \circ \sigma = \mathrm{id} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix}$$

The number of elements in $\mathbb{S}_\mathrm{n}$ is $\mathrm{n}! = 1 \cdot 2 \cdot 3 \cdot \ldots \cdot \mathrm{n}$;

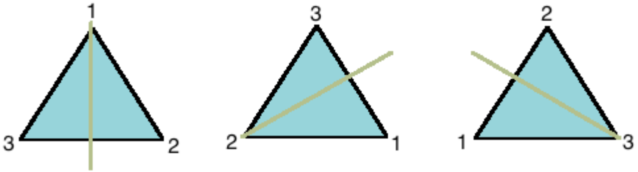
Equilateral triangle symmetry

Counterclockwise rotational symmetries

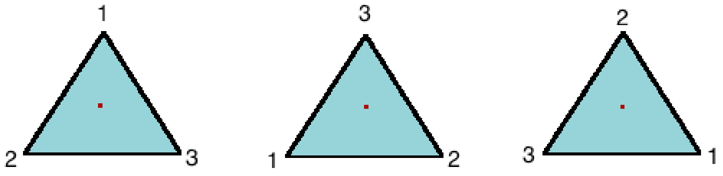


Rotation by 0 degrees. Rotation by 120 degrees. Rotation by 240 degrees.

Reflection symmetries



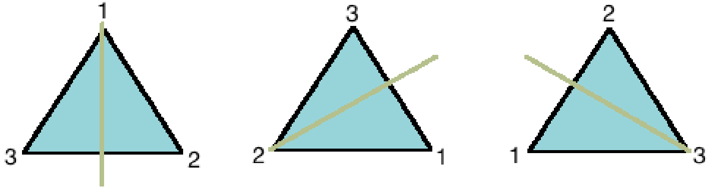
Counterclockwise rotational symmetries of the Equilateral Triangle



Rotation by 0 degrees. Rotation by 120 degrees. Rotation by 240 degrees.

	id	R	R^2
id	id	R	R^2
R	R	R^2	id
R^2	R^2	id	R

Mirror symmetries along an axis symmetry of the Equilateral Triangle



	S_1	S_2	S_3
S_1	id	R	R^2
S_2	R^2	id	R
S_3	R	R^2	id

Cayley (or multiplication) table of symmetries for the Equilateral Triangle

	id	R	R^2	S_1	S_2	S_3
id	id	R	R^2	S_1	S_2	S_3
R	R	R^2	id	S_3	S_1	S_2
R^2	R^2	id	R	S_2	S_3	S_1
S_1	S_1	S_2	S_3	id	R	R^2
S_2	S_2	S_3	S_1	R^2	id	R
S_3	S_3	S_1	S_2	R	R^2	id

The group of symmetries for the Equilateral Triangle is isomorphic to $\mathbb{S}_3$:

$$\mathrm{Id} \mapsto \mathrm{Id} = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} \qquad \mathrm{S}_1 \mapsto (1,3,2) = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$$

$$\mathrm{R} \mapsto (3,1,2) = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \qquad \mathrm{S}_2 \mapsto (3,2,1) = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$$

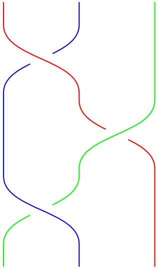
$$\mathrm{R}^2 \mapsto (2,3,1) = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \qquad \mathrm{S}_3 \mapsto (2,1,3) = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$$

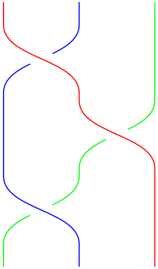
In general, a dihedral group is the group of symmetries of a regular polygon, D_n for the $\mathrm{n}-$gon.

$\mathrm{D}_\mathrm{n} \subsetneq \mathbb{S}_\mathrm{n}$ (a strict subgroup) for $\mathrm{n} > 3$.

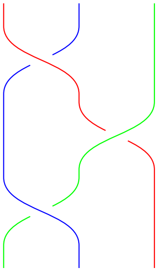
Braid groups

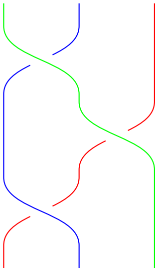
The braid group on n strands (denoted B_n, also known as the Artin braid group), is the group whose elements are equivalence classes of n-braids and whose group operation is composition of braids. Example of braids for $n = 3$.

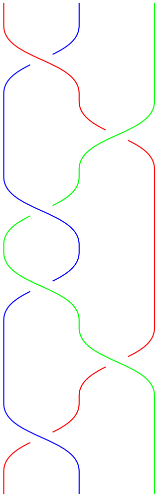




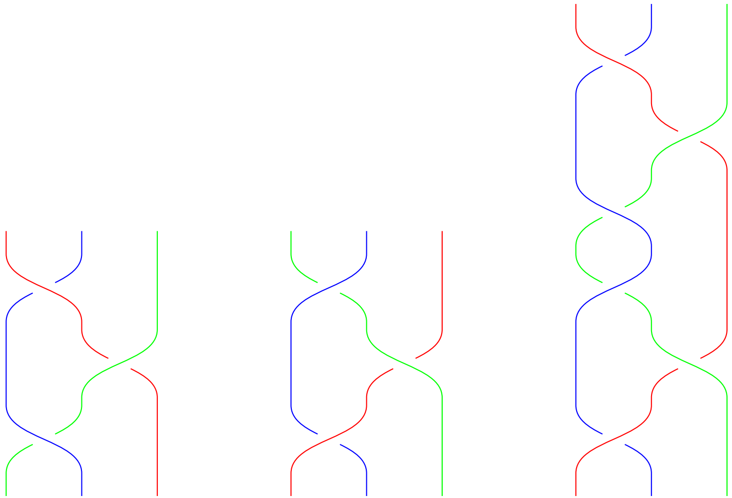
Multiplication in the braid group B_3 (3-braids)



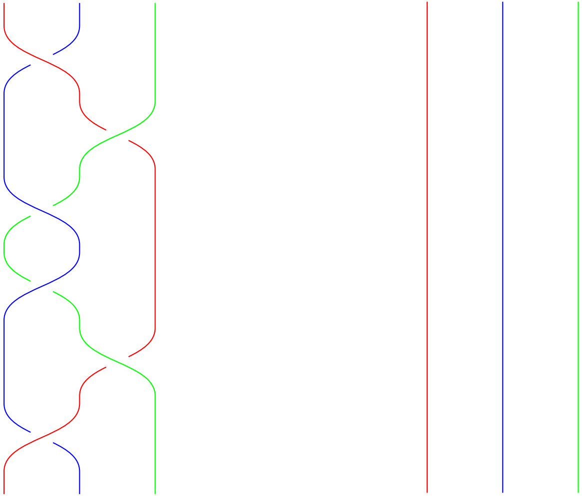




The inverse element

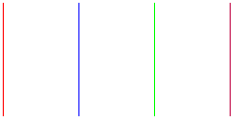


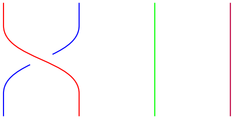
The inverse element

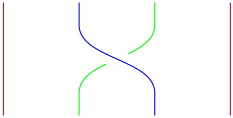


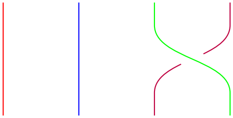
Generators of the Braid group B_n

Example of generators for B_4.

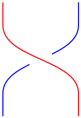
$e =$ 

$\sigma_1 =$ 

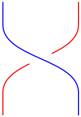
$\sigma_2 =$ 

$\sigma_3 =$ 

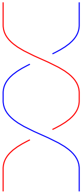
$$\sigma_1 =$$

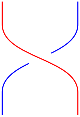


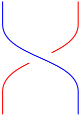
$$\sigma_1 =$$

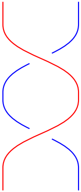
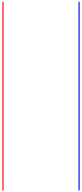


$$\sigma_1 \circ \sigma_1 =$$



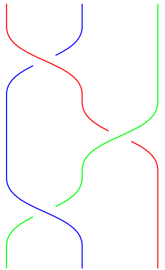
$\sigma_1 =$ 

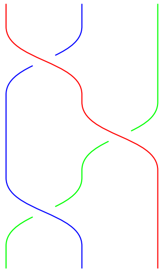
$\sigma_1^{-1} =$ 

$\sigma_1^{-1} \circ \sigma_1 =$  $=$ 

The morphism of groups $B_n \to \mathbb{S}_n$

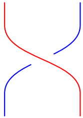
Example for B_3:

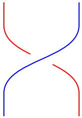


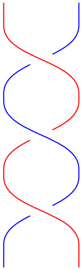


$$\begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \qquad \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$$

$B_n \to \mathbb{S}_n$ is an epimorphism, but not a monomorphism.

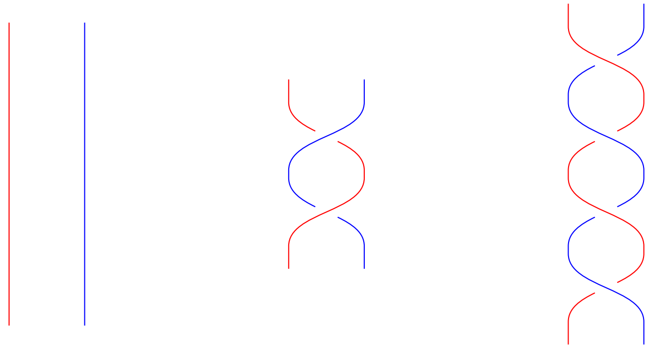






$$\begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix} \qquad \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix} \qquad \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix}$$

The kernel of $B_n \to \mathbb{S}_n$, called the pure braid group and denoted by PB_n or P_n, consists of more than one element.



$$\begin{pmatrix} 1 & 2 \\ 1 & 2 \end{pmatrix} \qquad \begin{pmatrix} 1 & 2 \\ 1 & 2 \end{pmatrix} \qquad \begin{pmatrix} 1 & 2 \\ 1 & 2 \end{pmatrix}$$

B_n is generated by $\sigma_1, \ldots, \sigma_{n-1}$ subject to the relations:

- $\sigma_i \sigma_{i+1} \sigma_i = \sigma_{i+1} \sigma_i \sigma_{i+1}$ for $1 \leq i \leq n-2$
- $\sigma_i \sigma_j = \sigma_j \sigma_i$ for $i - j \geq 2$

The symmetric group $\mathbb{S}_n$ is generated by the adjacent transpositions $\sigma_i = (i, i+1)$ for $1 \leq i \leq n-1$

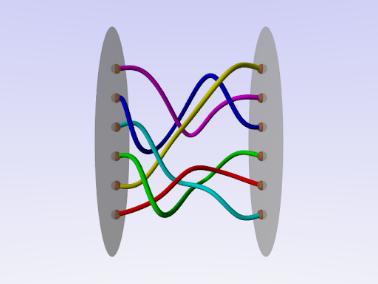
$$\sigma_i = \begin{pmatrix} 1 & \ldots & i & i+1 & \ldots & n \\ 1 & \ldots & i+1 & i & \ldots & n \end{pmatrix}$$

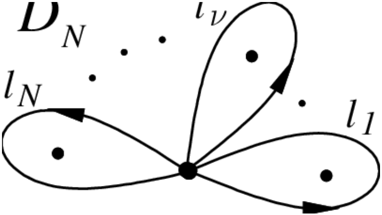
subject to the following relations:

- $\sigma_i^2 = 1$
- $\sigma_i \sigma_{i+1} \sigma_i = \sigma_{i+1} \sigma_i \sigma_{i+1}$ for $1 \leq i \leq n-2$
- $\sigma_i \sigma_j = \sigma_j \sigma_i$ for $i - j \geq 2$

Relation to algebraic topology

The braid group is isomorphic to the fundamental group π_1 of the configuration space of n points on a disc, while F_n, the free group generated by n elements, to the fundamental group of the n−punctured disc.





Action of a group on a set

We say that a group G is acting on a set X, called a $G-$space, if there is $G \times X \to X$, $(g, x) \mapsto gx$ satisfying

- (associativity) $g_1(g_2x) = (g_1g_2)x$ for all $g_1, g_2 \in G$, $x \in X$;
- (neutral element) $ex = x$ for all $x \in X$

As a corollary of the above properties, $g \colon x \mapsto gx$ is a bijection.

Equivalently, there is a morphism of group $G \to \mathrm{Aut}(X)$.

- An action is called free if for any $x \in X$, $gx = x$ implies $g = e$;
- An action is called transitive if for any $x, y \in X$ there exists $g \in G$, such that $gx = y$. Then X is called a homogeneous space;
- If an action is free and transitive, X is called a principal $G-$space or a $G-$torsor.

Examples of a group action

1. Action of $\mathrm{Aut}(X)$ on X;
2. Any subgroup of $\mathrm{Aut}(X)$ is acting on X;
3. Left multiplication in G, $G \times G \to G$, where the right copy of G is regarded as X. This action is free and transitive, G is a $G-$torsor
4. Instead of G take any subgroup H: $H \times G \to G$, where $X = G$. This action is free;
5. $GL(V) \times V \to V$, the action by linear transformations.

An action of G on a vector space V by linear transformations is called a representation of G on V, which is called a $G-$module.

Representations of G on V are in one-to-one correspondence with group morphisms $G \to GL(V)$.