For comments: litvinov@itp.ac.ru

List of lectures

Lecture 1: Basic definitions, examples of groups, permutation group

Definition 1.1. A group G is a set of elements with a product operation (a map $G \times G \to G$) with the following axioms

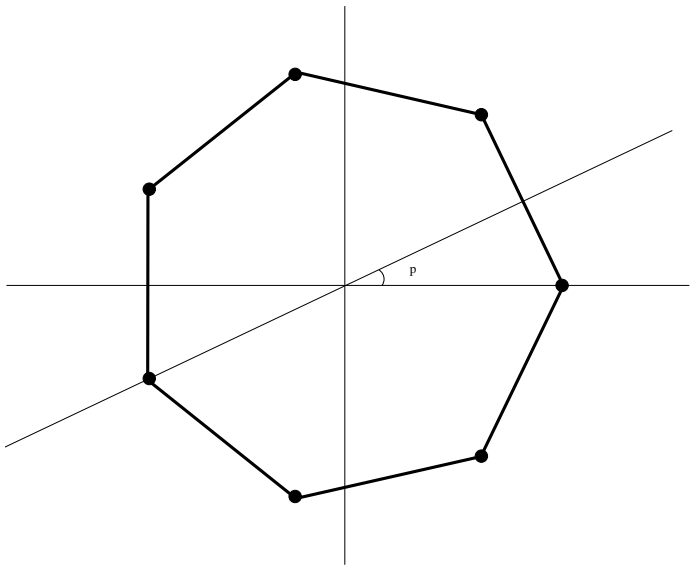
1. Associativity: $\forall\, a, b, c \in G : a \cdot (b \cdot c) = (a \cdot b) \cdot c$
2. Existence of an identity element: $\exists e \in G$: $\forall a \in G$, $a \cdot e = e \cdot a = a$
3. Existence of an inverse element: $\forall a \in G$, $\exists\, b \stackrel{\text{def}}{=} a^{-1} : a \cdot a^{-1} = e$.

Note: this definition in fact implies

1. Uniqueness of the identity element. Indeed, let e_1 and e_2 be two identity elements. Then one has
$$e_1 \cdot e_2 = \begin{cases} e_1 & \text{treating } e_2 \text{ as right identity,} \\ e_2 & \text{treating } e_1 \text{ as left identity} \end{cases} \implies e_1 = e_2.$$
2. Left inverse element is also the right one: $a \cdot a^{-1} = e \implies a^{-1} \cdot a = e$. Indeed
$$a^{-1} \cdot a = a^{-1} \cdot a \cdot e = a^{-1} \cdot a \cdot a^{-1} \cdot \left(a^{-1}\right)^{-1} = a^{-1} \cdot e \cdot \left(a^{-1}\right)^{-1} = a^{-1} \cdot \left(a^{-1}\right)^{-1} = e$$
3. Uniqueness of inverse element. Assume that both b and c are inverse to a. Then
$$b = b \cdot e = b \cdot (a \cdot c) = (b \cdot a) \cdot c = c$$

Examples of groups:

1. Group of integer numbers $\mathbb{Z}$ under addition. Also groups of real $\mathbb{R}$ and complex $\mathbb{C}$ numbers.
2. Group of real $n \times n$ matrices with non-vanishing determinant: $GL(n, \mathbb{R})$. Similar for complex valued matrices: $GL(n, \mathbb{C})$.
3. Cyclic group of n elements C_n: $C_n = \{e, \omega, \omega^2, \ldots, \omega^{n-1}\}$, where $\omega^n = e$. One way to "visualize" the cyclic group C_n is to think of it as a group of rotations in the plane of fractional angle $\frac{2\pi}{n}$
$$r_k = \omega^k = \begin{pmatrix} \cos\frac{2\pi k}{n} & -\sin\frac{2\pi k}{n} \\ \sin\frac{2\pi k}{n} & \cos\frac{2\pi k}{n} \end{pmatrix}$$
Equivalently C_n is the group of rotation symmetries of regular n-polygon.
4. Dihedral group D_n is the group of all symmetries of regular n-polygon. It consists of rotations r_k (the same as for the cyclic group) and reflections s_k
$$r_k = \begin{pmatrix} \cos\frac{2\pi k}{n} & -\sin\frac{2\pi k}{n} \\ \sin\frac{2\pi k}{n} & \cos\frac{2\pi k}{n} \end{pmatrix}, \qquad s_k = \begin{pmatrix} \cos\frac{2\pi k}{n} & \sin\frac{2\pi k}{n} \\ \sin\frac{2\pi k}{n} & -\cos\frac{2\pi k}{n} \end{pmatrix},$$
where s_k is the reflection across the line that makes an angle $\frac{\pi k}{n}$ with x axis. Note that for n odd, these axes are drawn from the center of a polygon to each vertex. For n being even there are $n/2$ axes drawn from the center to the vertices and $n/2$ axes drawn from the center to the middle of opposite faces (see the picture of regular 7-polygon).



Note that matrices r_k and s_k are orthogonal, $\det r_k = 1$ and $\det s_k = -1$. This is in an accordance with the fact that r_k preserves orientation while s_k does not.

5. The tetrahedral group T, the symmetry group of the ideal tetrahedron (preserving orientation). This group consists of $\frac{2\pi}{3}$ rotations around the four axes OA, OB, OC and OD, where (A, B, C, D) are the vertices of the tetrahedron and O is the "center of mass" point, as well as rotations on angle π about an edge linking the central points of opposite edges, e.g. AB and CD.

6. The symmetric group S_n (group of permutations of $n-$elements). By permutation we mean a bijection (one-to-one map) of a set of $n-$elements into itself. The product operation in S_n is the composition of permutations.

More on symmetric group S_n

1. It is convenient to represent permutations by their tables

$$\begin{pmatrix} 1 & 2 & 3 & \dots & n \\ \sigma(1) & \sigma(2) & \sigma(3) & \dots & \sigma(n) \end{pmatrix} \tag{1.1}$$

2. One can equally shuffle the columns of a table of permutations. For example

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 1 & 4 \end{pmatrix} \quad \text{and} \quad \begin{pmatrix} 2 & 1 & 4 & 3 \\ 3 & 2 & 4 & 1 \end{pmatrix}$$

represent the same permutation. We will call (1.1) – the canonical permutation.

3. The product in permutation group is composition. We will use the following convention for composition

$$\tau \cdot \sigma : \; i \overset{\sigma}{\mapsto} \sigma(i) \overset{\tau}{\mapsto} \tau\left(\sigma(i)\right)$$

4. It is clear that composition is a non-commutative operation. Consider the product of two compositions $\tau \cdot \sigma$ and $\sigma \cdot \tau$ from S_4

$$\tau = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 1 & 2 \end{pmatrix} \quad \text{and} \quad \sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 1 & 4 \end{pmatrix}$$

For $\tau \cdot \sigma$ we have

$$\begin{array}{l} \tau(\sigma(1)) = \tau(2) = 3 \\ \tau(\sigma(2)) = \tau(3) = 1 \\ \tau(\sigma(3)) = \tau(1) = 4 \\ \tau(\sigma(4)) = \tau(4) = 2 \end{array} \quad \Longrightarrow \quad \tau \cdot \sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 4 & 2 \end{pmatrix}$$

On the other hand for $\sigma \cdot \tau$ we have

$$\begin{array}{l} \sigma(\tau(1)) = \sigma(4) = 4 \\ \sigma(\tau(2)) = \sigma(3) = 1 \\ \sigma(\tau(3)) = \sigma(1) = 2 \\ \sigma(\tau(4)) = \sigma(2) = 3 \end{array} \quad \Longrightarrow \quad \sigma \cdot \tau = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{pmatrix}$$

5. Any permutation can be represented as a product on non-intersecting cycles. For example[1]

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 1 & 4 & 2 & 5 & 7 & 6 \end{pmatrix} = (1342)(5)(67)$$

Here by $(i_1, i_2, \ldots, i_n)$ we have denoted the cycle: $i_1 \mapsto i_2$, $i_2 \mapsto i_3, \ldots, i_{n-1} \mapsto i_n, i_n \mapsto i_1$, It is clear that non-intersecting cycles commute. The cycle representation of a permutation is convenient for computation of degree of permutation. Consider for example

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 1 & 4 & 2 & 5 & 7 & 6 \end{pmatrix}^{2025} = (1342)^{2025}(5)^{2025}(67)^{2025} = (1342)^{4\cdot 506+1}(5)^{2025}(67)^{2\cdot 1012+1}$$

It is clear that

$$(i_1, i_2, \ldots, i_n)^n = (i_1)(i_2)\ldots(i_n),$$

and hence finally we have

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 1 & 4 & 2 & 5 & 7 & 6 \end{pmatrix}^{2025} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 1 & 4 & 2 & 5 & 7 & 6 \end{pmatrix}$$

Definition 1.2. The order of the element $g \in G$ is the minimal number $n = \mathrm{ord}(g) \in \mathbb{N}$ such that $g^n = e$. If such n does not exists then $\mathrm{ord}(g) = \infty$.

Proposition 1.1. *If the permutation is equal to the product of independent cycles of lengths $d_1, \ldots, d_k$ then it has order $lcm(d_1, \ldots, d_k)$ (least common multiple).*

[1]Note that sometimes the cycles of length 1 are dropped

$$(1342)(5)(67) \quad \text{means the same as} \quad (1342)(67)$$

For example the order of permutation

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 1 & 4 & 2 & 5 & 7 & 6 \end{pmatrix} = (1342)(5)(67)$$

equals to $\mathrm{lcm}(4, 1, 2) = 4$.

Definition 1.3. The order of a group G, denoted by $|G|$, is the cardinality of G as a set (the number of elements in G). A group G is called a finite group if $|G| < \infty$, and is called an infinite group otherwise.

Proposition 1.2. *If $|G| < \infty$, then any element $g \in G$ has finite order:* $\mathrm{ord}(g) \leq |G|$.

Proof. Consider $|G| + 1$ elements $e, g, g^2, \dots, g^{|G|}$. But the group has $|G|$ elements. Thus there should exist $0 \leq i < j \leq |G|$ such that $g^i = g^j$. It implies that $g^{i-j} = e$. □

Definition 1.4. Transposition is a permutation of length 2

$$(a, b) = \begin{pmatrix} 1 & \dots & a & \dots & b & \dots & n \\ 1 & \dots & b & \dots & a & \dots & n \end{pmatrix}$$

Exercise. Compute

$$(a, b) \cdot \begin{pmatrix} 1 & 2 & 3 & \dots & n \\ \sigma(1) & \sigma(2) & \sigma(3) & \dots & \sigma(n) \end{pmatrix} \quad \text{and} \quad \begin{pmatrix} 1 & 2 & 3 & \dots & n \\ \sigma(1) & \sigma(2) & \sigma(3) & \dots & \sigma(n) \end{pmatrix} \cdot (a, b)$$

Proposition 1.3. *Any transposition can be represented as a product of transpositions, as a product of* elementary *transpositions of the form $(i, i + 1)$.*

For example any cycle can be represented as

$$(i_1, \dots, i_k) = (i_1, i_k) \cdot (i_1, i_{k-1}) \dots (i_1, i_2).$$

or

$$(i_1, \dots, i_k) = (i_1, i_2) \cdot (i_2, i_3) \dots (i_{k-1}, i_k)$$

In fact, there are more ways to represent the same permutation

$$(i_1, \dots, i_k) = (i_2, \dots, i_1, i_k) = (i_2, i_1) \cdot (i_2, i_k) \cdot (i_1, i_{k-1}) \dots (i_3, i_2),$$

etc. We note that transpositions do not commute and their number is not an invariant of a given permutation. For example, we have

$$(123) = (13)(12) = (23)(13), \quad (13) = (12)(13)(23) = (23)(13)(12), \tag{1.2}$$

or in terms of elementary transpositions

$$(123) = (12)(23), \quad (13) = (12)(23)(12) = (23)(12)(23). \tag{1.3}$$

Definition 1.5. A set of elements $\{s_1, s_2, \dots\}$ is called a set of *generators* of G if any element of G can be represented as

$$g = s_{i_1}^{\pm j_i} \cdot s_{i_2}^{\pm j_2} \dots s_{i_k}^{\pm j_k}$$

Examples

1. A cyclic group C_n is generated by ω.
2. A dihedral group D_n is generated by r_1 and s_1.
3. A symmetric group S_n is generated by elementary transpositions $(i, i+1)$ for $i = 1, \ldots, n-1$[2].

From examples (1.2) and (1.3) we see that the number of transpositions for given permutation is ambiguous. However, the following theorem suggests that the parity does.

Theorem 1.1. *Let $\sigma \in S_n$ admits the following decomposition*

$$\sigma = \sigma_1 \ldots \sigma_k, \tag{1.4}$$

where σ_j's are some transpositions. Then the number

$$\epsilon(\sigma) \stackrel{def}{=} (-1)^k$$

is completely defined by σ and does not depend on a particular expansion (1.4)*. Moreover,*

$$\epsilon(\sigma \cdot \tau) = \epsilon(\sigma)\epsilon(\sigma).$$

Proof. Assume that there is another representation

$$\sigma = \sigma'_1 \ldots \sigma'_{k'},$$

such that $k + k' \in$ odd. Since $(\sigma'_i)^2 = e$, one can multiply the equality

$$\sigma_1 \ldots \sigma_k = \sigma'_1 \ldots \sigma'_{k'},$$

by $\sigma'_{k'} \ldots \sigma'_1$ from the right. We get

$$\sigma_1 \ldots \sigma_m = \sigma_1 \ldots \sigma_k \cdot \underbrace{\sigma'_{k'} \ldots \sigma'_1}_{\sigma_{k+1} \ldots \sigma_m} = e \quad \text{for} \quad m \in \text{odd}.$$

We have to show that in the equality

$$e = \sigma_1 \ldots \sigma_m, \tag{1.5}$$

m is necessary an even number. Thus we have a contradiction. In order to show that m is an even number, we show that commutation relations between permutations allow one to reduce the number of factors in (1.5) by the factor of 2.

Consider some $1 \leq i \leq n$. Such that

$$e = \sigma_1 \ldots \sigma_{p-1} \cdot \sigma_p \cdot \sigma_{p+1} \ldots \sigma_m,$$

with $\sigma_p = (ij)$ and all $\sigma_{p+1}, \ldots, \sigma_m$ do not contain i. Then for σ_p there are four possibilities

1. $\sigma_{p-1} = (ij) \implies (ij) \cdot (ij) = e$

[2]One might wonder if this is the smallest set of generators. The answer is not. One can generate S_n by just two elements $(1, 2)$ and $(1, 2, \ldots, n)$.

2. $\sigma_{p-1} = (ik) \implies (ik) \cdot (ij) = (ij) \cdot (jk)$

3. $\sigma_{p-1} = (jk) \implies (jk) \cdot (ij) = (ik) \cdot (jk)$

4. $\sigma_{p-1} = (kl) \implies (kl) \cdot (ij) = (ij) \cdot (kl)$

In the case 1 we have reduce the number of factors by 2. In the cases 2, 3 and 4 we have not reduced the number of factors, but have shifted first appearance of the index i to the left. Then we proceed and either will meet a situation 1, or will end up at the extremal case

$$e = (ik) \cdot \tau_1 \dots \tau_{m-1},$$

where none of τ_j's have the index i in it. But such a permutation can not be identical. Thus we come to a contradiction. □

Definition 1.6. A permutation is called even (resp. odd) if $\epsilon(\sigma) = 1$ (resp. $\epsilon(\sigma) = -1$)

Definition 1.7. A subset $H \subset G$ is called a *subgroup*, if $\forall a, b \in H$: $a \cdot b \in H$ and $a^{-1} \in H$.

Proposition 1.4. *Even permutations in S_n form a subgroup. It is known as* alternating *group A_n.*

Examples

1. $A_2 = \{e\}$

2. $A_3 = \{e, (123), (132)\}$. Let us denote $\omega = (123)$, then $\omega^2 = (132)$ and $\omega^3 = e$. Thus we have an isomorphism $A_3 = C_3$.

3. $A_4 = \{e, (123), (132), (124), (142), (134), (143), (234), (243), (12)(34), (13)(24), (14)(23)\}$

Sometimes it is required to find which permutations in S_n commute with given permutation. The following statement helps.

Proposition 1.5. *For any $\sigma \in S_n$ one has*

$$\sigma(i_1, \dots, i_k)\sigma^{-1} = (\sigma(i_1), \dots, \sigma(i_k)), \tag{1.6}$$

where σ_j are some transpositions.

Proof. Set $\tau = (i_1, \dots, i_k)$. It is enough to show that both hand sides of (1.6) act in the same way on any $j \in 1, \dots, n$. For example let $j = \sigma(i_1)$. We have

$$\sigma\tau\sigma^{-1}\left(\sigma(i_1)\right) = \sigma\tau\sigma^{-1}\sigma(i_1) = \sigma\tau(i_1) = \sigma(\tau(i_1)) = \sigma(i_2).$$

□

Probs:

1. Find all $\sigma \in S_5$ such that $\sigma^2 = (1, 2, 3)$.
2. Show that any permutation $\sigma \in S_n$ can be expressed as a product of
   (a) transpositions $(1, 2), (1, 3), \ldots (1, n)$
   (b) elementary transpositions $(1, 2), (2, 3), \ldots (n-1, n)$
   (c) two elements: $(1, 2)$ and $(1, 2, 3, \ldots, n)$.
3. Find all permutations $\sigma \in S_6$ which commute with
$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 2 & 5 & 6 & 3 & 1 \end{pmatrix}$$
4. For any $\sigma \in S_n$ one associates a $n \times n$ matrix $R(\sigma)$ such that $R(\sigma)_{ij} = 1$ if $j = \sigma(i)$ and 0 otherwise. Find eigenvalues of $R(\sigma)$. Express the answer in terms of a cyclic structure of σ.
5. Prove that A_4 coincides with tetrahedral group T.
6. Find the number of even permutations in S_n.

Lecture 2: Finite groups of low orders. Abelian groups. Group presentations.

Definition 2.1. Abstract group can be defined by its multiplication table (Cayley table)

	g_1	g_2	$\dots$	g_n	$\dots$
g_1	$g_1 \cdot g_1$	$g_1 \cdot g_2$	$\dots$	$g_1 \cdot g_n$	$\dots$
g_2	$g_2 \cdot g_1$	$g_2 \cdot g_2$	$\dots$	$g_2 \cdot g_n$	$\dots$
$\dots$	$\dots$	$\dots$	$\dots$	$\dots$	$\dots$
g_n	$g_n \cdot g_1$	$g_n \cdot g_2$	$\dots$	$g_n \cdot g_n$	$\dots$
$\dots$	$\dots$	$\dots$	$\dots$	$\dots$	$\dots$

The size of this table (matrix) is $|G| \times |G|$.

Proposition 2.1. *No row or column of a Cayley table may contain the same element twice.*

Proof. Let a, b and c be the elements of a group. Then in the row representing the element a, the column corresponding to b contains the product $a \cdot b$, and similarly the column corresponding to c contains the product $a \cdot c$. Suppose that the contents are the same, i.e. that $a \cdot b = a \cdot c$, but then $b = c$ and hence we come to a contradiction. □

This corollary allows to classify all finite groups of lower orders.

Group of order 2

There is only one group of order 2, which is C_2

	e	ω
e	e	ω
ω	ω	e

Group of order 3

There is only one group of order 3 as well, which is C_3. Indeed, let $\omega \neq e$ be an element of a group of order 3. Then $\{e, \omega, \omega^2\}$ must be distinct, because otherwise: either $\omega^2 = \omega \implies \omega = e$, or $\omega^2 = e \implies \exists g \neq \omega : \omega \cdot g = g \implies \omega = e$

	e	ω	ω^2
e	e	ω	ω^2
ω	ω	ω^2	e
ω^2	ω^2	e	ω

Group of order 4

It is easy to construct all possible groups with four elements $\{e, g_1, g_2, g_3\}$. Let us start filling the multiplication table. First row and first column are obvious. Then one has to decide whether $g_1 \cdot g_1 = e$ or $g_1 \cdot g_1 = g_2$. In the first case the second row must contain g_2 and g_3. The only possibility is $g_1 \cdot g_2 = g_3$, because the other choice $g_1 \cdot g_2 = g_2 \implies g_1 = e$. The second column is filled similarly (shown in red). The rest of the table is filled by noticing $g_2 \cdot g_2$ can be either e or g_1, but the last case corresponds to the second table with relabelling the indexes $1, 2, 3$. For the second case we have either $g_1 \cdot g_2 = e$, or

$g_1 \cdot g_2 = g_3$. Again the first case is forbidden because $g_1 \cdot g_2 = e \implies g_1 \cdot g_3 = g_3 \implies g_1 = e$. Thus we have $g_1 \cdot g_2 = g_3$ (similarly $g_2 \cdot g_1 = g_3$). Then automatically $g_2 \cdot g_2 = g_1 \cdot g_1 \cdot g_2 = g_1 \cdot g_3 = e$

	e	g_1	g_2	g_3
e	e	g_1	g_2	g_3
g_1	g_1	e	g_3	g_2
g_2	g_2	g_3	e	g_1
g_3	g_3	g_2	g_1	e

or

	e	g_1	g_2	g_3
e	e	g_1	g_2	g_3
g_1	g_1	g_2	g_3	e
g_2	g_2	g_3	e	g_1
g_3	g_3	e	g_1	g_2

Thus there are two groups of order 4. The first group is the dihedral group D_2 also known as Klein's four group and the second is cyclic group C_4.

Definition 2.2. A group G is called *Abelian* if $\forall a, b \in G : a \cdot b = b \cdot a$.

Examples of Abelian groups:

- Cyclic groups C_n.
- Additive group of integers, denoted by $\mathbb{Z}$. Additive group of integers modulo n, denoted by $\mathbb{Z}_n$.
- Multiplicative group of integers modulo n and *coprime* with n, denoted by $\mathbb{Z}_n^*$.

Comment on $\mathbb{Z}_n^*$. It is straightforward to show the group axioms for $\mathbb{Z}_n^*$. Suppose one has to integers a and b from the set $\{1, 2, \ldots, n-1\}$ that are coprime with n (i.e. $a, b \in \mathbb{Z}_n^*$), that is $\gcd(a, n) = \gcd(b, n) = 1$. Then since $\gcd(a \cdot b, n) = 1$ we have $a \cdot b \in \mathbb{Z}_n^*$. To show that every $a \in \mathbb{Z}_n^*$ has an inverse, we note that the equation $a \cdot x = 1 (\mathrm{mod}\, n)$ has a solution because by Bézout's lemma for a such that $\gcd(a, a^-1) = 1$ there are integers x and y such that $ax + ny = 1$. The associativity axiom trivially holds.

The order of the group $\mathbb{Z}_n^*$ is given by Euler's totient function $\varphi(n)$.

Definition 2.3. A map $\varphi : G \to H$ is called a *homomorphism* (of groups) or *group morphism* iff it preserves multiplication, i.e. $\forall a, b \in G, \varphi(a \cdot_G b) = \varphi(a) \cdot_H \varphi(b)$. A homomorphism that is bijective is called *isomorphism*.

Proposition 2.2. *A homomorphism maps identity to identity and inverses to inverses.*

Proof. Let $\varphi : G \to H$ be a homomorphism. By definition of a morphism $\varphi(eg) = \varphi(e)\varphi(g)$, and by definition of identity $eg = g$, so, $\varphi(eg) = \varphi(g)$. Combining these equalities, we conclude that $\varphi(e)$ is the identity in H. Now, for the inverses: $e = \varphi(e) = \varphi(g^{-1}g) = \varphi(g^{-1})\varphi(g)$, so, $\varphi(g^{-1}) = (\varphi(g))^{-1}$. □

Proposition 2.3. *Two groups G and H are called isomorphic (denoted as $G \simeq H$) if there exists an isomorphism $\varphi : G \to H$.*

Proposition 2.4. *The group $\mathbb{Z}_n$ is isomorphic to C_n.*

Proposition 2.5. *A group with n element (of order n) is isomorphic to C_n if and only if G has an element of order n.*

Proposition 2.6. *The group $\mathbb{Z}_5^*$ is isomorphic to C_4 (also $\mathbb{Z}_p^* \simeq C_{p-1}$ for p-prime).*

Proof. The group $\mathbb{Z}_5^*$ as a set consists of 4 elements: $\{1,2,3,4\}$. We already know that there are two groups of order 2: C_4 and D_2. It remains to choose one. In order to do it, we note that 2 has order 4: $2^2 = 4$, $2^3 = 8 = 3 (\mathrm{mod}\, 5)$, $2^4 = 16 = 1 (\mathrm{mod}\, 5)$. Thus by Corollary 4, $\mathbb{Z}_5^*$ is isomorphic to C_4. □

Theorem 2.1 (Cayley)**.** *Every finite group of order n is isomorphic to some subgroup in the symmetric group S_n.*

Proof. See Cayley's table. □

Corollary. *There are finitely many (up to isomorphism) groups of given order n.*

Proof. It is clear that there are finitely many Cayley tables of size $n \times n$. A super rough estimate is $\binom{n!}{n}$ that is the number of n different permutations out of all $n!$. In reality the number of groups of given order is much less. For example there are 5 distinct groups of order 12 which is much less than $\binom{12!}{12} \approx 3.04584 \times 10^{95}$. □

Definition 2.4. A direct product of two groups G and H is a set of pairs $G \times H = \{(g,h) | g \in G, h \in H\}$ with the following multiplication $(g_1, h_1) \cdot (g_2, h_2) = (g_1 \cdot g_2, h_1 \cdot h_2)$. [3]

Proposition 2.7. $D_2 \simeq C_2 \times C_2, \quad C_6 \simeq C_2 \times C_3, \quad \mathbb{Z}_8^* \simeq C_2 \times C_2$.

Theorem 2.2 (Gauss)**.** *$\mathbb{Z}_n^\times$ is cyclic if and only if $n = 1, 2, 4, p^k$ or $2p^k$, where p is an odd prime.*

Theorem 2.3. *The groups $C_m \times C_n$ and C_{mn} are isomorphic if and only if m and n are coprime numbers ($\gcd(m,n) = 1$).*

Proof. Let C_n be generated by ω and C_m be generated by ρ. If $\gcd(m,n) = 1$ then the order of the element (ω, ρ) is mn, so, $C_m \times C_n \simeq C_{mn}$. And vica versa, if $C_m \times C_n$ admits an of order mn then $\gcd(m,n) = 1$. □

An immediate generalization is as follows:

Theorem 2.4 (Chinese remainder theorem)**.** *Let n be a positive integer and $n = p_1^{k_1} \cdot p_2^{k_2} \cdot ... \cdot p_N^{k_N}$ be its (unique) decomposition into a product of primes. Then $C_n = C_{{p_1}^{k_1}} \times C_{{p_2}^{k_2}} \times ... \times C_{{p_N}^{k_N}}$. Or in, additive notation, $\mathbb{Z}_n = \mathbb{Z}_{{p_1}^{k_1}} \oplus \mathbb{Z}_{{p_2}^{k_2}} \oplus ... \oplus \mathbb{Z}_{{p_N}^{k_N}}$.*

Proof. Using Bezoult's identity it is easily checked that the map $[x]_n \longmapsto ([x]_{{p_1}^{k_1}}, ..., [x]_{{p_N}^{k_N}})$ is an isomorphism of groups. Here $[x]_k \equiv x \mod k$ is a positive remainder of x wrt k. □

Theorem 2.5 (Fundamental theorem of finite abelian groups)**.** *Any finite abelian group is isomorphic to the product of finite cyclic groups $G \simeq C_{k_1} \times \cdots \times C_{k_n}$.*

Proof. will be given later □

In fact, there is a slight generalization of this result valid for "sufficiently small" infinite abelian groups. These groups are called finitely generated and are defined in terms of generators and relations.

[3] For abelian groups it is sometimes convenient to denote group multiplication by "+", not by "·". This is called additive notation, as opposed to multiplicative one. In additive variant the direct product $G \times H$ can be conveniently called direct sum and denoted $G \oplus H$. This triggers no confusion, since every abelian group is a module over $\mathbb{Z}$ with respect to action $n \cdot g = \underbrace{g + g + ... + g}_{n \text{ times}}$. A direct product of two abelian groups (in additive notation) is then exactly the direct sum of the corresponding $\mathbb{Z}$-modules.

Probs:

1. For abelian groups $\mathbb{Z}_9^\times$, $\mathbb{Z}_{10}^\times$, $\mathbb{Z}_{11}^\times$, $\mathbb{Z}_{40}^\times$ and $\mathbb{Z}_{360}^\times$ find a decomposition into a product of cyclic groups.
2. How many elements are there in $\mathbb{Z}_{40}^\times$? Compute $\frac{1}{3} \cdot \frac{1}{7} \cdot \frac{1}{9}$ in $\mathbb{Z}_{40}^\times$.
3. How many elements are there in $(\mathbb{Z}_{371293})^\times$? List the orders of elements in this group.[4]
4. Show that the sets

$$\mathrm{U}(1) = \Big\{ z \in \mathbb{C} : \ |z| = 1 \Big\},$$
$$\mathrm{O}(2) = \Big\{ A \in \mathrm{Mat}_{2\times 2}(\mathbb{R}) : \ A^{\mathrm{T}} A = E_{2\times 2} \Big\}$$
$$\mathrm{SO}(2) = \Big\{ A \in \mathrm{Mat}_{2\times 2}(\mathbb{R}) : \ A^{\mathrm{T}} A = E_{2\times 2}, \ \det A = 1 \Big\}$$

   form groups wrt usual matrix multiplication. Show that SO(2) and U(1) are isomorphic. Show that SO(2) and O(2) are not.
5. Let $\varphi : G \to H$ be a homomorphism of finite groups. Show that $\mathrm{ord}(\varphi(g))$ divides $\mathrm{ord}(g)$ for any $g \in G$.
6. Denote a set of all homomorphisms from G to H by $\mathrm{Hom}(G, H)$. Describe the sets:
   (a) $\mathrm{Hom}(G, 1)$ and $\mathrm{Hom}(1, H)$
   (b) $\mathrm{Hom}(S_n, \mathbb{Z}_3)$ and $\mathrm{Hom}(S_n, \mathbb{Z}_2)$
   (c) $\mathrm{Hom}(\mathbb{Z}_6, \mathbb{Z}_{25})$ and $\mathrm{Hom}(\mathbb{Z}_6, \mathbb{Z}_{15})$

[4] Hint: what is the number of elements in $(\mathbb{Z}_{p^k})^\times$?

Lecture 3: Generators and relations

Definition 3.1. Let $\mathcal{R}$ be a set. A *free group generated by* $\mathcal{R}$ is a group $F = \langle \mathcal{R} \rangle$, which we now describe. Elements of this group are words w consisting of letters in $\mathcal{R}$:

$$w = \prod_{r \in \mathcal{R}} r^{m(r)},$$

where multiplicity $m(r)$ is an integer. For example, in $\langle r_1, r_2, r_3, r_4, r_5 \rangle$ there is a word

$$w = r_1 \underbrace{r_2 r_2}_{r_2^2} r_3^{-1} \underbrace{r_4 r_4 r_4 r_4}_{r_4^4} \underbrace{r_5^{-1} r_5^{-1} r_5^{-1}}_{r_5^{-3}} ... = r_1 r_2^2 r_3^{-1} r_4^4 r_5^{-3}.$$

The only rule is as follows. If anywhere in a word a combination $r_j r_j^{-1}$ or $r_j^{-1} r_j$ appears, it is replaced by 1 (a trivial word and an identity element of F). Multiplication in F is given by concatenation of words:

$$w_1 = \prod_{j=1}^{J} r_j^{m_j}, \quad w_2 = \prod_{k=1}^{K} s_k^{m_k}, \quad \Rightarrow \quad w_1 w_2 = \prod_{j=1}^{J} r_j^{m_j} \prod_{k=1}^{K} s_k^{m_k}$$

Due to $r r^{-1} = r^{-1} r = 1$ every element of F has a unique inverse:

$$w = \prod_{j=1}^{N} r_j^{m_j} \quad \Rightarrow \quad w^{-1} = \prod_{j'=1}^{N} (r_{N-j'+1})^{m_{N-j'+1}}$$

For example, in $\langle r_1, r_2, r_3, r_4, r_5 \rangle$ the inverse of w is

$$w^{-1} = (r_1 r_2^2 r_3^{-1} r_4^4 r_5^{-3})^{-1} = r_5^3 \, r_4^{-4} \, r_3 \, r_2^{-2} \, r_1^{-1}.$$

Definition 3.2. If a set $\mathcal{R}$ is finite $\mathcal{R} = \{r_1, r_2, ..., r_k\}$, then a free group $F_k = \langle \mathcal{R} \rangle$ is called a *free group of rank* k.

Since for all alphabets $\mathcal{R}$ of the same cardinality the groups freely generated by them are isomorphic, a free group of rank k is unique (up to a isomoprhism). More generally, there is only one free group generated by a set of a given cardinality.

Proposition 3.1.

- *Free groups are infinite except for the trivial one* $F_0 = \{1\}$.
- *A free group of rank 1 is abelian and isomorphic to* $\mathbb{Z}$.
- *Free groups of rank* $k \geq 2$ *are not abelian.*

Clearly not every group is free. For example, no finite group (except for the trivial one) is free. That leads us to the idea of imposing relations on words of $F = \langle \mathcal{R} \rangle$.

Definition 3.3. A presentation of a group G is data $G = \langle \mathcal{R} | \mathcal{S} \rangle$, where $\mathcal{R}$ is a generating set and $\mathcal{S} \subset \langle \mathcal{R} \rangle$ is a set of relations on the generators. The group G is thus constructed analogously to the free group but with a larger amount of relations on generators (not only that $r^{-1} r = r r^{-1} = 1$).

Examples

- A free group: $F = \langle \mathcal{R} | \varnothing \rangle$
- A finite cyclic group: $C_n = \langle\, \omega \,|\, \omega^n \,\rangle = \{1, \omega, \omega^2, \ldots, \omega^{n-1}\}$.
- $\mathbb{Z} \times \mathbb{Z} = \langle\, x, y \,|\, xyx^{-1}y^{-1} \,\rangle$ (multiplicative notation)
- A dihedral group: $D_n = \langle\, r, s \,|\, r^n, s^2, (rs)^2 \,\rangle$
- A tetrahedral group $\mathrm{T} = A_4 = \langle\, s, t \,|\, s^2, t^3, (st)^3 \,\rangle$

Definition 3.4. A group G is said to be *finitely generated* if these exists a presentation $G = \langle \mathcal{R} | \mathcal{S} \rangle$ with finite set of generators $|\mathcal{R}| < \infty$. A group G is said to be *finitely related* if $|\mathcal{S}| < \infty$. If a group turns out to be both finitely generated and finitely related, then it is called *finitely presented*.

We stress that finitely presented group can be infinite, as well as infinitely generated and infinitely related group can be finite. For example,

$$\mathbb{Z} \simeq C_\infty = \langle \omega \rangle = \{1, q, q^{-1}, q^2, q^{-2}, \ldots\},$$
$$1 = \langle \mathbb{Z} | \mathbb{Z} \rangle = \langle x_1, x_2, \ldots \,|\, x_1 = x_2 = \cdots = 1 \rangle$$

Proposition 3.2. *Symmetric group is finitely presented.*

Proof. Symmetric group is generated by elementary transpositions $\sigma_i = (i, i+1)$. One can convince oneself that the presentation

$$S_n = \Big\langle \sigma_i,\ i \in \{1, ..., n\} \quad \Big| \quad \sigma_i^2 = 1, \quad \underbrace{\sigma_i \sigma_j = \sigma_j \sigma_i}_{\text{for } j \neq i \pm 1}, \quad \sigma_i \sigma_{i+1} \sigma_i = \sigma_{i+1} \sigma_i \sigma_{i+1} \Big\rangle$$

is valid. □

Dropping the first set of relations $\sigma_i^2 = 1$, one arrives at the new infinite group:

Definition 3.5. A braid group on n braids:

$$B_n = \Big\langle \sigma_i,\ i \in \{1, ..., n\} \quad \Big| \quad \underbrace{\sigma_i \sigma_j = \sigma_j \sigma_i}_{\text{for } j \neq i \pm 1}, \quad \sigma_i \sigma_{i+1} \sigma_i = \sigma_{i+1} \sigma_i \sigma_{i+1} \Big\rangle$$

Proposition 3.3. *A braid group B_n is infinite and contains finite subgroups isomorphic to S_k for any $1 \leq k \leq n$*

The relation $\sigma_i\, \sigma_{i+1}\, \sigma_i = \sigma_{i+1}\, \sigma_i\, \sigma_{i+1}$ present in S_n and B_n is known in the literature as *Yang-Baxter equation*. It plays an exceedingly important role in theory of classical and quantum integrable systems ans is most conveniently presented by the picture (1)

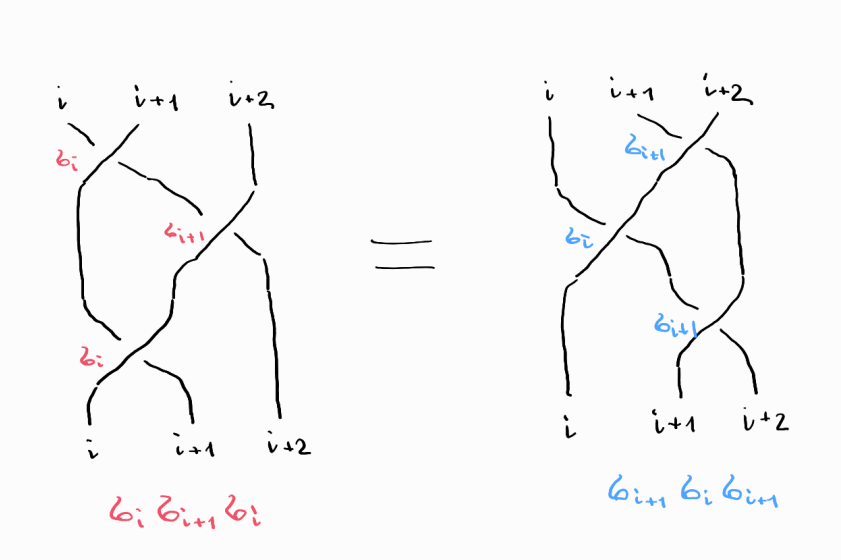


Figure 1: Yang Baxter Equation

Definition 3.6 (Coxeter groups)**.** Let M be an integer symmetric $n \times n$ matrix with $m_{ii} = 1$ and $m_{ij} = m_{ji} \geq 2$ for $i \neq j$. m_{ij} is allowed to be equal to ∞. Then to this matrix one associates a *Coxeter group* $\mathrm{Cox}(M)$ defined by presentation

$$\mathrm{Cox}(M) = \left\langle r_1, r_2, ..., r_n \;\middle|\; (r_i r_j)^{m_{ij}} = 1 \right\rangle.$$

Note that condition $m_{ii} = 1$ implies that every generator is an inversion: $x_i^2 = 1$. Condition $m_{ij} = 2$ implies that generators x_i and x_j commute. Indeed, $(x_i x_j)^2 = 1 \;\Leftrightarrow\; x_i x_j = x_j^{-1} x_i^{-1} \;\Leftrightarrow\; x_i x_j = x_j x_i$. The symmetricity condition $m_{ij} = m_{ji}$ is equivalent to that $(x_i x_j)^m = 1 \;\Leftrightarrow\; (x_j x_i)^m = 1$. In this way, Coxeter groups can (and should) be thought of as of the reflection groups.

Coxeter groups are of great importance to classification of simple finite groups, ADE classification of (semi)simple Lie algebras, elementary catastrophes, minimal models of CFT, *etc.* We will (probably) return to this discussion late in this course.

Finite (and affine finite-type) Coxeter groups have been completely classified. Since Coxeter matrices are symmetric, they can be thought of as the adjacency matrix of finite edge-labeled graph. These graphs are called Coxeter-Dynkin graphs, and the classification is most conveniently presented in terms of them.

Theorem 3.1 (Classification of finite Coxeter groups)**.** *(Simple) Coxeter group is finite if and only if the corresponding Dynkin graph is one of the following:*

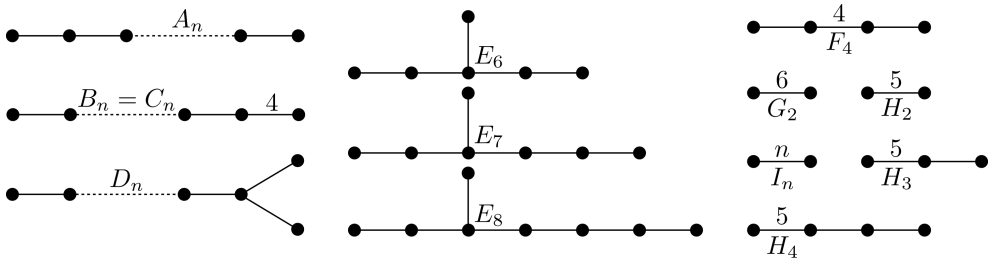


Figure 2: Finite Coxeter groups

Examples

- $\mathrm{Cox}\left(\begin{bmatrix}1 & 2\\ 2 & 1\end{bmatrix}\right) = \mathbb{Z}_2 \oplus \mathbb{Z}_2 \quad \longleftrightarrow \quad A_1 \times A_1$
- $\mathrm{Cox}\left(\begin{bmatrix}1 & 3\\ 3 & 1\end{bmatrix}\right) = \langle x, y \,|\, x^2 = y^2 = (xy)^3 = 1\rangle \simeq S_3 \quad \longleftrightarrow \quad A_2$
- $\mathrm{Cox}\left(\begin{bmatrix}1 & 4\\ 4 & 1\end{bmatrix}\right) = \langle x, y \,|\, x^2 = y^2 = (xy)^4 = 1\rangle \simeq D_4 \quad \longleftrightarrow \quad B_2 \simeq C_2 \simeq I_4$
- $\mathrm{Cox}\left(\begin{bmatrix}1 & 2 & 0\\ 2 & 1 & 2\\ 0 & 2 & 1\end{bmatrix}\right) = \langle x, y, z \,|\, x^2 = y^2 = z^2 = 1,\ [x, y] = [y, z] = 1\rangle \quad \longleftrightarrow \quad A_2 \times A_1,$ non-simple
- $\mathrm{Cox}\left(\begin{bmatrix}1 & 3 & 2 & 2\\ 3 & 1 & 3 & 3\\ 2 & 3 & 1 & 2\\ 2 & 3 & 2 & 1\end{bmatrix}\right) \quad \longleftrightarrow \quad D_4$

Proposition 3.4. *Let G_1 and G_2 be finitely presented. Then their direct product is finitely presented aswell.*

Proof. A direct product of groups $G_1 = \langle \mathcal{R}_1 | \mathcal{S}_1 \rangle$ and $G_2 = \langle \mathcal{R}_2 | \mathcal{S}_2 \rangle$ admits a following presentation:

$$G_1 \times G_2 = \left\langle \quad \mathcal{R}_1 \cup \mathcal{R}_2 \quad \middle| \quad \mathcal{S}_1 \cup \mathcal{S}_2 \cup [\mathcal{R}_1, \mathcal{R}_2] \quad \right\rangle$$

where $[\mathcal{R}_1, \mathcal{R}_2]$ is generated by all the group commutators $r_1\, r_2\, r_1^{-1}\, r_2^{-1}$. In this way G_1 and G_2 commute in $G_1 \times G_2$. Since sets $\mathcal{R}_{1,2}$, $\mathcal{S}_{1,2}$ and $[\mathcal{R}_1, \mathcal{R}_2]$ are finite, $G_1 \times G_2$ is finitely presented. □

Now we can formulate the classification theorem for "sufficiently small" abelian groups

Theorem 3.2 (Classification of finitely generated abelian groups)**.** *Any finitely generated abelian group A is isomorphic to $\mathbb{Z}^r \oplus \mathrm{Tors}(A)$, where subgroup $\mathrm{Tors}(A)$ is finite abelian: $\mathrm{Tors}(A) \simeq \mathbb{Z}_{k_1} \oplus ... \oplus \mathbb{Z}_{k_m}$. A number r is called a rank of group A.*

It is now easy to construct (possibly new, possibly infinite) groups by writing down presentations.

Definition 3.7. Let $G_1 = \langle \mathcal{R}_1 | \mathcal{S}_1 \rangle$ and $G_2 = \langle \mathcal{R}_2 | \mathcal{S}_2 \rangle$. A *free product* of G_1 and G_2 is a group $G_1 * G_2$ generated by $\mathcal{R}_1$ and $\mathcal{R}_2$ and with no additional relation between these elements:

$$G_1 * G_2 = \left\langle \quad \mathcal{R}_1 \cup \mathcal{R}_2 \quad \middle| \quad \mathcal{S}_1 \cup \mathcal{S}_2 \quad \right\rangle.$$

Example. $\mathrm{Cox}\left(\begin{bmatrix}1 & 0\\ 0 & 1\end{bmatrix}\right) = \mathbb{Z}_2 * \mathbb{Z}_2$

Proposition 3.5.

- *If G and H are nontrivial, then $G * H$ is infinite*
- $G * 1 = 1 * G = G$
- $F_k * F_l = F_l * F_k = F_{k+l}$

Example: modular group A very important case of a free product is modular group $\Gamma = \mathrm{PSL}(2,\mathbb{Z})$:

$$\mathrm{PSL}(2,\mathbb{Z}) = \Big\{ (\pm A) \in \mathrm{Mat}_{2\times 2}(\mathbb{Z}) \;\Big|\; \det(\pm A) = 1 \Big\}.$$

Turns out, $\mathrm{PSL}(2,\mathbb{Z})$ is generated by matrices

$$S = \pm \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \quad \text{and} \quad T = \pm \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}.$$

since $S^2 = \pm E_{2\times 2}$ and $(ST)^3 = \pm E_{2\times 2}$, modular group admits a presentation

$$\Gamma = \Big\langle\; S, T \;\Big|\; S^2 = 1,\ (ST)^3 = 1 \;\Big\rangle \simeq \mathbb{Z}_2 * \mathbb{Z}_3.$$

Problems

1. What is this group: $\langle a, b \,|\, ab^2 = b^2a,\ a^4 = b^3 \rangle$?
2. Let G be a finitely generated group with all generators having finite order. Is G finite?
3. Prove that A_n $(n \geq 3)$ can be generated by
   (a) 3-cycles
   (b) (123) and $(12\ldots n)$
4. Prove the presentations

   $$\begin{array}{ll} \text{a)} & D_n = \langle\, r, s \,|\, r^n, s^2, (rs)^2 \,\rangle, \\ \text{b)} & A_4 = \langle\, s, t \,|\, s^2, t^3, (st)^3 \,\rangle \end{array}$$

   to be correct.
5. Consider the following linear-fractional transformations of complex plane:

   $$z \mapsto w = \frac{az + b}{cz + d},$$

   where $a, b, c, d \in \mathbb{Z}$ and $ad - bc = 1$. Prove that these transformation form a group. Find the identity, the laws of multiplication and inversion. Establish the isomorphism with $\Gamma = \mathrm{PSL}(2,\mathbb{Z})$. What linear-fractional transformations correspond to generating matrices S and T?
6. Prove that any symmetric group S_n is a Coxeter group. Find the corresponding Coxeter matrix and Dynkin graph.

Lecture 4: Group action, Lagrange's theorem, conjugacy classes. Point groups.

In physics, groups usually appear through their action on some sets

Definition 4.1. If G is a group and X is a set, then a (left) group action ρ of G on X is a function $\rho : G \times X \to X$, such that

- $\forall g, h \in G,\ x \in X : \rho(g, \rho(h, x)) = \rho(g \cdot h, x)$
- $\forall x \in X : \rho(e, x) = x$.

In order to simplify notation we will usually write $\rho(g, x) = gx$

Definition 4.2. Let group G act on X

1. An orbit of an element $x \in X$ is a set $Gx \equiv \mathcal{O}_x = \{y \in X | \exists g \in G, y = gx\}$
2. A stabilizer of an element $x \in X$ is a set $G_x \equiv \mathrm{Stab}_G(x) = \{g \in G | gx = x\}$.

The set of orbits is denoted by X/G.

Proposition 4.1. *A stabilizer of any point $x \in X$ is a subgroup of G.*

Proposition 4.2. *Two orbits are either identical or disjoint. Moreover, every element element $x \in X$ lies in some orbit. That is one has an equivalence relation by saying $x \sim y$ if $x \in Gy$.*

Definition 4.3. The group G acts

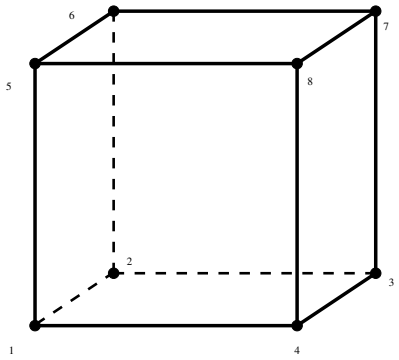
- Transitively on X if $\forall x, y \in X\ \exists g \in G : y = gx$. In other words $X = G_x$ for some $x \in X$.
- Freely on X if $gx = x$ for some $x \in X$ implies $G_x = \{e\}$.
- Faithful or effective if $gx = x\, \forall x \in X$ implies $g = e$.

Proof. First of all $x \in Gx$, so every element is in some orbit. Second suppose that $z \in Gx \cap Gy$ then $z = g_1 x$ and $z = g_2 y$. This implies $x = (g_1^{-1} \cdot g_2)y$ and hence $x \in G_y$. Thus $G_x = G_y$. □

Theorem 4.1. *Orbit-stabilizer theorem. Let G be a group acting on X. Then $|G| = |G_x||Gx|$, where $|G_x|$ is the length of the orbit G_x (cardinality as a set).*

Proof. Denote $m = |Gx|$, $n = |G_x|$, then $Gx = \{g_1 x, \ldots, g_m x\}$ with $g_1 = e$ and $G_x = \{h_1, \ldots, h_n\}$. Then any element $g \in G$ admits the unique decomposition $g = g_i \cdot h_j$. Indeed, since $gx \in Gx$ one can represent $gx = g_i x$ (note that for given g, g_i is unique). Then $h_j = g_i^{-1} \cdot g$ (indeed $g_i^{-1} \cdot g \in G_x$). It is clear that we have constructed a bijection between G and $G_x \times Gx$. □

Example. We can use the orbit-stabilizer theorem to count the dimension of automorphism group of a cube (rotations preserving orientation). Let $(1, 2, 3, 4, 5, 6, 7, 8)$ be the vertices of a cube



It is clear that $|G1| = 8$ (the cube group acts transitively). On the other hand $G_1 = C_3$.

Another way of computing the same number. Let X be the set of faces of the cube, $|X| = 6$. Obviously G acts transitively on X, i.e. the orbit of a given face is the set of all the other faces, which is X. The stabilizer of a face is $\mathbb{Z}_4$. Thus the order of the group is $6 \times 4 = 24$.

Yet another way. Let X be the set of edges, $|X| = 12$. The stabilizer of an edge is $\mathbb{Z}_2$. Thus again $12 \times 2 = 24$.

Proposition 4.3. *Burnside's lemma. Let X^g denote the set of elements in X that are fixed by g, that is $X^g = \{x \in X | gx = x\}$. Then*

$$|X/G| = \frac{1}{|G|} \sum_{g \in G} |X^g|.$$

Proof. It is clear that

$$\sum_{g \in G} |X^g| = \sum_{x \in X} |G_x|$$

Thus

$$\frac{1}{|G|} \sum_{g \in G} |X^g| = \frac{1}{|G|} \sum_{x \in X} |G_x| = \frac{1}{|G|} \sum_{x \in X} \frac{|G|}{|Gx|} = \sum_{x \in X} \frac{1}{|Gx|} = |X/G|.$$

□

Definition 4.4. A group G acts on itself by left multiplication $(g, g') \mapsto g \cdot g'$ (correspondingly by right multiplication $(g, g') \mapsto g' \cdot g^{-1}$). Any subgroup $H \in G$ acts on G as (h, g). The orbits of this action denoted by Hg are called right cosets of H in G.

Theorem 4.2. *Lagrange's theorem. If H is a subgroup of G then*

$$|G| = |H||G/H|$$

Proof. Since $hg = g$ implies $h = e$ and thus the stabilizer of any point is trivial $H_g = \{e\}$. It means that any orbit consists exactly of $|H|$ elements. Thus the size of the subgroup H should divide $|G|$. The ratio $|G|/|H|$ is the number of orbits. □

Proposition 4.4. *Let G be a finite group. The order of any element g divides G. In particular $g^{|G|} = e$.*

Proof. Let $|g| = d$ then $\{e, g, g^2, \ldots g^d\}$ form a subgroup of G of order d. Thus d divides $|G|$. □

Corollary. *Any finite group of prime order p is isomorphic to C_p.*

Remark 4.1. The reverse of Lagrange theorem is not true: given the factor of $|G|$ there might be no subgroup of that size. For example for $G = A_4$ the order is 12, but it turns out that there is no subgroup of order 6.

Proposition 4.5. *Little Fermat's theorem. If p is a simple number and $a \in \mathbb{Z}$, $gcd(1, p) = 1$ then $a^{p-1} = 1 \, mod \, p$.*

Proof. Take $G = \mathbb{Z}_p^\times$ then a can be replaced by its representative in $\mathbb{Z}_p^\times$. Moreover, since $\gcd(1, p) = 1$, $a \neq e$. Since $|\mathbb{Z}_p^\times| = p - 1$, we have $a^{p-1} = e$ in $\mathbb{Z}_p^\times$ and hence $a^{p-1} = 1 \bmod p$. □

Proposition 4.6. *Euler's theorem. If $\gcd(a, n) = 1$ then $a^{\varphi(n)} - 1$ divides n.*

Definition 4.5. A group element g is conjugate to g' if $\exists h \in G \; g' = hgh^{-1}$.

Proposition 4.7. *A group acts on itself by conjugations, moreover conjugation provides an isomorphism.*

Proof. We can check that the action is correctly defined

$$g_1 \cdot (g_2 \cdot g \cdot g_2^{-1}) \cdot g_1^{-1} = (g_1 \cdot g_2) \cdot g \cdot (g_1 \cdot g_2)^{-1}$$

and that conjugation is an isomorphism

$$g \cdot x \cdot y \cdot g^{-1} = (g \cdot x \cdot g^{-1}) \cdot (g \cdot y \cdot g^{-1})$$

□

Definition 4.6. Orbits of conjugated action of a group on itself are called conjugacy classes.

Examples.

1. For abelian group each conjugacy class contains exactly one element.
2. If H is a subgroup of G then gHg^{-1} is also a subgroup of G
3. Two permutations in S_n are conjugated if they have the same cyclic structure. For example S_3 has three classes: e, $(1, 2), (1, 3), (2, 3)$ and $(1, 2, 3), (1, 3, 2)$.
4. The conjugacy classes of S_n are in one-to-one correspondence with the partitions of n. Given a conjugacy class $(1)^{l_2}(2)^{l_2} \dots (n)^{l_n}$ its order[5] is $|Cg| = \frac{n!}{\prod_i i^{l_i} l_i!}$. The length of the orbit, i.e. the number of permutations that commute with given permutation is $\prod_i i^{l_i} l_i!$.

Definition 4.7. Centralizer of an element $x \in G$ is a set $C_x = \{g \in G | gxg^{-1} = x\}$.

Corollary. *Let G be a finite group and $(x_1, \dots x_r)$ its conjugacy classes. Then*

$$|G| = \sum_{i=1}^{r} \frac{|G|}{|C_{x_i}|}$$

[5]Indeed, we have $n!$ choices to arrange $1, \dots, n$. Place them into the parentheses pattern in this order to obtain an element of the conjugacy class. For each r-cycle you divide by r as only the cyclic order matters. Then if there are n_r cycles of length r, you divide by $n_r!$.

Example. Conjugacy classes in D_5. The order of the group is $D_5 = 10$. It is equal to

$$D_5 = \{e, r, r^2, r^3, r^4, s, sr, sr^2, sr^3, sr^4\}$$

Let us identify conjugacy classes of all elements. The identity commutes with everything and hence $|Ce| = 1$. Now consider the reflection s. It is clear that $\{e, s\} \leq C_s \leq D_5$. Then $|C_s|$ must divide 10. It is easy to see that $|C_s| = 2$ and thus $|Cs| = 5$. In fact any reflection is conjugated to every reflection: $C_s = \{\text{all reflections}\}$.

The conjugacy class of r is at least $\{r, r^4\}$ (since we have the following property of the reflection $srs^{-1} = r^4$). It can not be more, since we already have $1 + 5$ of classes, so we only have 4 elements and the order must divide 10. Similarly for r^2 we have $Cr^2 = \{r^2, r^3\}$.

Point groups in three dimensions

An orbit-stabilizer counting formula can be used to describe all three-dimensional point groups. These are defined as finite subgroups of 3-dimensional rotation group and appear as symmetries of different 3-dimensional figures: polyhedra (regular or not), simple molecules, etc.

Definition 4.8. A *point group* is a finite subgroup of $\mathrm{SO}(3, \mathbb{R})$.

Theorem 4.3 (Classification of 3-dimensional point groups)**.** *Point groups in three dimensions are:*

- *cyclic* C_n,
- *dihedral* D_n
- *tetrahedral* $\mathrm{T} \simeq A_4$
- *octahedral* $\mathrm{O} \simeq S_4$
- *icosahedral* $\mathrm{I} \simeq A_5$

Proof. Let $G \subset \mathrm{SO}(3)$ be a point group. Since every element of $\mathrm{SO}(3)$ is a rotation (orientation-preserving), by famous Euler's theorem on Euclidean motions, it has exactly two antipodal fixed points when acting on $\mathbb{S}^2 \subset \mathbb{R}^3$. We call them poles. Let $P \subset \mathbb{S}^2$ be a set of points that arise as fixed points of no-identity element $g \in G$, $g \neq 1$. Obviously, G acts on P. Indeed, if $p \in P$ and is fixed by $x \in G$, then $g \cdot p$ is fixed by $gxg^{-1} \in G$ (stabilizers are conjugated).

Since every non-identity element of G fixed exactly two points, we det

$$|G| - 1 = \frac{1}{2} \sum_{p \in P} \big(\mathrm{Stab}_G(p) - 1 \big).$$

By orbit-stabilizer theorem,

$$|\,\mathrm{Stab}_G(p)| = \frac{|G|}{|\mathcal{O}_p|}.$$

Combining these two formulas,

$$|G| - 1 = \frac{1}{2} \sum_{p \in P} \left(\frac{|G|}{|\mathcal{O}_p|} - 1 \right) = \frac{1}{2} \sum_{\mathcal{O}} \big(|G| - |\mathcal{O}| \big).$$

Divide by $|G|$:

$$2 - \frac{2}{|G|} = \sum_{\mathcal{O}} \left(1 - \frac{1}{|\operatorname{Stab}_G(p \in \mathcal{O})|}\right),$$

where $p \in \mathcal{O}$ can be taken to be any element of $\mathcal{O}$, since stabilizers of points lying in one orbit are conjugated, and thus are of the same size.

Denote by $a_1, \ldots, a_r$ the sizes of stabilizers of elements lying in distinct orbits $\mathcal{O}_1, \ldots \mathcal{O}_r$. Then the equation of interest is

$$2 - \frac{2}{|G|} = \sum_{i=1}^{r} \left(1 - \frac{1}{a_i}\right).$$

From the general grounds we know that a_i divide $|G|$ and $a_i \geq 2$. Since for non-trivial G's l.h.s is between 1 and 2 and every term in the r.h.s. sum is at least $\frac{1}{2}$, the number of terms r in this sum is at most 3: $r \leq 3$. So, there are essensially two cases:

Two orbits ($r = 2$) The equation above forces the stabilizer sizes to be equal: $a_1 = a_2 = |G| = n$. In other words, both points of P are fixed by the whole group $G \subset \mathrm{SO}(3)$. So, we have a finite group of rotations fixing exactly one line. Thus, $G = C_n$.

Three orbits ($r = 3$)

1. $(a_1, a_2, a_3) = (n, 2, 2)$, $|G| = 2n$, $n \geq 2$. The orbit corresponding to a_1 has size two and the other two orbits have size n. Since the size of the orbit of a point and its antipode are equal, the orbit of size two contains two antipodal points. Its stabilizer is a subgroup of order n acting by orientation-preserving orthogonal transformations on the perpendicular plane. Thus, this is a cyclic subgroup of order n. The element that flips the two antipodal points restricts to that plane as a reflection in some axis in that plane. It follows that the group is a dihedral group of order $2n$, with the usual action on that plane. $G = D_n$.

2. $(a_1, a_2, a_3) = (3, 3, 2)$, $|G| = 12$. A little work shows that this is a tetrahedral group $\mathrm{T} = A_4$.

3. $(a_1, a_2, a_3) = (4, 3, 2)$, $|G| = 24$. A little work shows that this is a octahedral group $\mathrm{O} = S_4$.

4. $(a_1, a_2, a_3) = (5, 3, 2)$, $|G| = 60$. A little work shows that this is an icosahedral group $\mathrm{I} = A_5$.

The classification thus is as follows: there are two infinite series of point groups: C_n (acts on pyramids) and D_n (acts on dihedra) and three exceptional: $\mathrm{T} = A_4$ (acts on a tetrahedron), $\mathrm{O} = S_4$ (acts on a cube and an ocrahedron) and $\mathrm{I} = A_5$ (acts on an icosahedron or a dodecahedron). □

Probs:

1. Let G be the group of a cube preserving orientation. Prove an isomorphism $G \sim S_4$.

2. How many different necklaces can be made with 6 beads of n different colors?

3. $^{(*)}$ Finish the "little works" for exceptional symmetries in the classification of point groups in three dimensions.

Lecture 5: Normal subgroups, quotient groups, semidirect products.

Definition 5.1. Let G and H be groups. The map φ: $G \to H$ is called a homomorphism of groups if $\forall a, b \in G\ \varphi(ab) = \varphi(a)\varphi(b)$

Definition 5.2. Kernel of the map $\varphi : G \to H$: $\ker(\varphi) = \{g \in G | \varphi(g) = e\}$

Definition 5.3. Image of the map $\varphi : G \to H$: $\mathrm{im}(\varphi) = \{h \in H | \exists g \in G\, \varphi(g) = h\}$

Proposition 5.1. *Let $\varphi : G \to H$ be a group homomorphism. Then $\mathrm{im}\,\varphi \subset H$ and $\ker\varphi \subset G$ are subgroups.*

Proposition 5.2. $\varphi(g_1) = \varphi(g_2) \quad \Leftrightarrow \quad g_1 = g_2 \cdot \ker\varphi$.

Corollary. *φ is injective iff* $\ker\varphi = \{1\}$.

Examples of morphisms, kernels and images

- $[-]_n : \mathbb{Z} \to \mathbb{Z}_n$ defined by $x \mapsto [x]_n = x \mod n$. Kernel is a subgroup $n\mathbb{Z}$.
- $\varepsilon : S_n \to \mathbb{Z}_2$, a sign homomorphism. Kernel is A_n-subgroup.
- $\det : \mathrm{GL}(n, \mathbb{K}) \to \mathbb{K}^\times$. Kernel is isomorphic to $\mathrm{SL}(n, \mathbb{K})$
- Group G actions on set $\{1, ..., n\}$ and in 1:1 correspondence with homomorphisms $G \to S_n$.

Definition 5.4. A subgroup N is called normal subgroup in G (denoted as $N \lhd G$) if

$$\forall g \in G: \quad gNg^{-1} \in N.$$

Note that this definition does not mean $g^{-1}ng = n$ for all $n \in N$!

Proposition 5.3. $N \lhd G \quad \Leftrightarrow$ *left and right cosets coincide: $gN = Ng$.*

Proof. Consider an element of the left conjugacy class $gh \in gN$. Then $ghg^{-1}g$ belongs to right conjugacy class Ng since N is normal $ghg^{-1} \in N$ □

Proposition 5.4. $N \lhd G \quad \Leftrightarrow$ *N is a union of conjugacy classes.*

Proof. Since N is normal, there is a G-action on N by conjugations: $x \mapsto x^g = gxg^{-1} \in N$. This action divides N into a union of non-intersecting orbits, $N = \mathcal{O}_{n_1} \cup ... \cup \mathcal{O}_{n_r}$, which are precisely the conjugacy classes of $n_i \in N$. □

Examples of normal subgroups

- Consider the direct product of groups $G_1 \times G_2 = G$. There are (at least) two normal subgroups of G: $G_1 \times 1 \lhd G$ and $1 \times G_2 \lhd G$.
- $A_3 \lhd S_3$ (also seen as a kernel of a sign homomorphism)
- $\ker(\varphi : G \to H) \lhd G$
- translation subgroup in ISO(3) (all orientation-preserving motions of Euclidean 3-space)
- $C_n \lhd D_n$ (can be seen by considering generators r, s and relations $r^n = s^2 = (rs)^2 = 1$)

There is a neat criterion for a group G to be isomorphic to a direct product of two of its subgroups.

Definition 5.5. We call subgroups A and B of group G *complementing* whenever $A \cap B = \{1\}$ and $A \cdot B = G$.

Proposition 5.5. *A and B are complementing if and only if for any $g \in G$ there is a unique decomposition $g = ab$ with $a \in A$, $b \in B$.*

Proposition 5.6. *Let A and B be complementing subgroups of G. Then the following statements are equivalent:*

(1) A and B are both normal

(2) A and B commute

(3) $G = A \times B$

Proof. (1) $\Rightarrow$ (2) Let A and B be normal complementary. Then

$$\underbrace{a \cdot \overbrace{b \cdot a^{-1}}^{\in A} \cdot b^{-1}}_{\in B} \in A \cap B = \{e\} \implies aba^{-1}b^{-1} \implies ab = ba,$$

and A commutes with B.

(2) $\Rightarrow$ (3) Now let A and B be complementary and commuting. Consider a map $\mu : A \times B \to G$ sending a pair (a, b) into the product $ab \in G$. Since $A \cdot B \in G$, this map is surjective. Since $A \cap B = \{1\}$, it is injective, and thus μ is a bijection. Now, since A and B commute, $\mu\big((a_1, b_1) \cdot (a_2, b_2)\big) = \mu(a_1 a_2, b_2 b_2) = a_1 a_2 b_1 b_2 = a_1 b_1 a_2 b_2 = \mu(a_1, b_1)\mu(a_2, b_2)$, and thus μ is in fact an isomorphism of groups.

(3) $\Rightarrow$ (1) is obvious. □

Definition 5.6. If $N \lhd G$, then cosets form a group called quotient group with the multiplication

$$g_1 N \cdot g_2 N \stackrel{\text{def}}{=} g_1 \cdot g_2 N.$$

Proof. One has to check that the multiplication provided above is correctly defined. That is for all $h_1 \in N$ and $h_2 \in N$ there exists $h \in N$ such that

$$g_1 h_1 g_2 h_2 = g_1 g_2 h \implies g_2^{-1} h_1 g_2 = h h_2^{-1},$$

which is provided since N is normal subgroup. □

Examples of quotients

- Subgroups of $\mathbb{Z}$ have the form $n\mathbb{Z}$ with integer n. Since $\mathbb{Z}$ is abelian, every subgroup is normal. Left and right cosets (in additive notation) are $[m_1] = m_1 + n\mathbb{Z}$, $[m_2] = m_2 + n\mathbb{Z}$. Addition of these sets is $[m_1] = [m_2] = [m_1 + m_2]$, just the usual addition modulo n. Quotient group is thus $\mathbb{Z}/n\mathbb{Z} \simeq \mathbb{Z}_n$
- Let $G = V$, an additive abelian group of a vector space over field $\mathbb{K}$, and $H = U \subset V$ be its vector subspace. The quotient abelian group V/U is called quotient space. The elements of it are written as $v + U$ and can be thought of as subspaces parallel to U of dimension $\dim U$. The addition is defined by $(v_1 + U) + (v_2 + U) = v_1 + v_2 + U$. V/U can be equippen with the same multiplication by scalars as V: $\lambda \cdot (v + U) = \lambda \cdot V + U$ (check that this is indeed a correct $\mathbb{K}$-action), making the quotient V/U a $\mathbb{K}$-vector space itself. If V was equipped with an non-degenerate inner product, V/U is canonically identified with $U^\perp$.
- Let $G = G_1 \times G_2$. Then $G/G_1 \simeq G_2$ and $G/G_2 \simeq G_1$
- $\mathrm{ISO}(3)/\mathbb{R}^3 \simeq \mathrm{SO}(3)$
- $S_n/A_n \simeq \mathbb{Z}_2$
- $D_n/C_n \simeq \mathbb{Z}_2$

Theorem 5.1 (First isomorphism theorem)**.** *Let $\varphi : G \to H$ be a group homomorphism. Then we have an isomorphism $\operatorname{im}\varphi \simeq G/\ker\varphi$.*

Proof. Isomorphism is constructed as follows. For every element in image $h \in \operatorname{im}\varphi$ we write $h = \varphi(g_h)$. Map h to class $g_h \cdot \ker\varphi \in G/\ker\varphi$, and check the correctness. □

Corollary. *If G is finite, then $|G| = |\operatorname{im}\varphi| \cdot |\ker\varphi|$ for any $\varphi : G \to H$.*

Let N and K be complementary subgroups of G. We saw that if $G = N \times K$, then $K \simeq G/N$. One might naively think that if $K \simeq G/N$, then $G \simeq N \times K$, but this is far from true: N is normal by construction, but K need not to be so, and certainly H and K need not commute, so, $K = G/N$ does not imply $G = N \times K$ in general.

Definition 5.7 (Inner semidirect product)**.** Let N and K be complementary subgroups of G. Let N be normal: $N \lhd G$. We will require the map $\mu : N \times K \to G$, $(n, k) \mapsto nk$, which is a bijection by construction, to be a homomorpshism of two groups. In other words, we should discover a group law $\star$ on the set $N \times K$, which would make μ an isomorphism of groups $(N \times K, \star)$ and G.

$$\mu\big((n_1, k_1) \star (n_2, k_2)\big) \overset{!}{=} \mu(n_1, k_1) \cdot \mu(n_2, k_2) = n_1 k_1 n_2 k_2 = \underbrace{n_1 k_1 n_2 k_1^{-1}}_{\in N} \cdot \underbrace{k_1 k_2}_{\in K}$$

So, if we define the group law on a set of pair $N \times K$ by the formula

$$(n_1, k_1) \star (n_2, k_2) = (n_1 \cdot k_1 n_2 k_1^{-1}, k_1 k_2),$$

we will arrive at a new group $(N \times K, \star)$, which we denote by $N \rtimes K$ or $K \ltimes N$ and call an *inner semidirect product*

Definition 5.8 (Outer semidirect product)**.** Let N and K be any two groups. Let ϕ be a K-action on N, that is, $\phi : K \to \mathrm{Aut}(N)$. *Outer semidirect product* $N \rtimes_\phi K$ is a set $N \times K$ with a group law

$$(n_1, k_1) \cdot (n_2, k_2) = (n_1 \, \phi_k(n_2), k_1 k_2)$$

By the very construction the following neat criterion holds:

Proposition 5.7. *Let $N \lhd G$ and $K \subset G$ be complementary subgroups. Then $G \simeq N \rtimes K$.*

Note that N and K need not commute and K need not to be normal!

Examples of semidirect products

- $G = N \times K$, trivial K-action on N,
- $D_n = C_n \rtimes \mathbb{Z}_2$. This is most easily seen by $D_n = \langle\, r, s \,|\, r^n = s^2 = 1, srs^{-1} = r^{-1} \,\rangle$,
- $\mathrm{ISO}(3) = \mathbb{R}^3 \rtimes \mathrm{SO}(3)$,
- $\mathrm{GL}(n, \mathbb{K}) = \mathrm{SL}(n, \mathbb{K}) \rtimes \mathbb{K}^\times$
- $\mathbb{Z}_m \rtimes_k \mathbb{Z}_n = \langle\, x, y \,|\, x^m = y^n = 1, yxy^{-1} = x^k \,\rangle$, where $(k, n) = 1$ and $k^n = 1 \mod m$

Exact sequences and group extensions

There is a neat and general way to look at homomorphisms, quotients by kernels and semidirect products in a unified way.

Definition 5.9. A sequence of groups and morphisms

$$\ldots \xrightarrow{f_{i-2}} G_{i_1} \xrightarrow{f_{i-1}} G_i \xrightarrow{f_i} G_{i+1} \xrightarrow{f_{i+1}} \ldots$$

is called *exact in object* G_i if $\mathrm{im}\, f_{i-1} = \ker f_i$. A sequence is called simply *exact* if it is exact in every object.

Definition 5.10. A *short exact sequence* is

$$1 \longrightarrow N \xrightarrow{\iota} G \xrightarrow{\pi} K \longrightarrow 1$$

Proposition 5.8. *In short exact sequence (see above) $N \xrightarrow{\iota} G$ is injective and $G \xrightarrow{\pi} K$ is surjective. Moreover, $K \simeq G/N$.*

Definition 5.11. A group G is called an *extension* of a group K by N if there is a short exact sequence $1 \to N \to G \to K \to 1$ or, equivalently, if $K \simeq G/N$. An extension is called *split* whenever additionally $G = N \rtimes K$.[6] An extension is called *trivial* if additionally $G = N \times K$.

A general group extension need not to be split. For example,

$$1 \longrightarrow \mathbb{Z}_2 \longrightarrow \mathbb{Z}_4 \longrightarrow \mathbb{Z}_2 \longrightarrow 1$$

is not split. If it was, $\mathbb{Z}_4$ would be isomorphic to $\mathbb{Z}_2 \oplus \mathbb{Z}_2$, and it is not.

[6] or, equivalently, when $N \xrightarrow{\iota} G \xrightarrow{\pi} K$ admits a section, which is a map $s : K \to G$ such that $\pi \circ s = \mathrm{id}_K$.

Theorem 5.2. *Let $H \subset G$ be a subgroup of index two. Let there be element $g \notin G$ of order two: $g^2 = 1$. Then G always splits over H with $\mathbb{Z}_2$-fiber: $G = H \rtimes \mathbb{Z}_2$.*

Proof. Note that $\langle g \rangle \cap H = \{1\}$. Since H has index two, it is normal, and $G = \langle g \rangle \cdot H$. By our neat criterion we immediately get $G = H \rtimes \mathbb{Z}_2$. □

Problems

1. Express S_n as a non-trivial semidirect product.
2. Consider an *infinite dihedral group* $D_\infty = \mathbb{Z} \rtimes \mathbb{Z}_2$. Find a presentation for D_∞ and prove it to be an (infinite) Coxeter group.
3. Describe all split metacyclic groups $\mathbb{Z}_m \rtimes_k \mathbb{Z}_n$. What k's are allowed? Are these groups the same or different with different k's?
4. Prove $D_6 \simeq D_3 \times C_2$. Is D_8 isomorphic to $D_4 \times C_2$?
5. Prove that $\mathrm{O}(2) = \mathrm{SO}(2) \rtimes \mathbb{Z}_2$. Is $\mathrm{O}(3)$ isomorphic to $\mathrm{SO}(3) \times \mathbb{Z}_2$?
6. $^{(*)}$ Prove that

$$D_{2\cdot 2n} = D_{2n} \rtimes \mathbb{Z}_2 \qquad \mathrm{O}(2n) = \mathrm{SO}(2n) \rtimes \mathbb{Z}_2$$
$$D_{2\cdot(2n+1)} = D_{2n+1} \times \mathbb{Z}_2 \qquad \mathrm{O}(2n+1) = \mathrm{SO}(2n+1) \times \mathbb{Z}_2$$

Lecture 6: Derived subgroup, solvable groups, simple groups

Definition 6.1. Let G be a group. The commutator of $g, h \in G$ is an element of G defined by $[g,h] \stackrel{\text{def}}{=} ghg^{-1}h^{-1} \in G$.

We note that

- $[x,y] = e$ implies that $xy = yx$.
- $xy = [xy]yx$. Thus $[x,y]$ is a correcting term in commutation relation between x and y.
- $[x,y]^{-1} = [y,x]$
- $g[x,y]g^{-1} = [gxg^{-1}, gyg^{-1}]$
- Let φ be the homomorphism of groups $G \stackrel{\varphi}{\to} H$, then $\varphi([x,y]) = [\varphi(x), \varphi(y)]$

Definition 6.2. The derived subgroup (also called the commutator subgroup) of G, denoted by $[G,G]$, G' or $G^{(1)}$ is a subgroup generated by all commutators $[x,y]$ for $x, y \in G$.

Example. Let $G = S_n$ then $S_n' = A_n$.

Proof. For any two permutations $\sigma, \tau \in S_n$: $[\sigma,\tau] = \sigma\tau\sigma^{-1}\tau^{-1}$ is even and hence $S_n' \subseteq A_n$. On the other hand one can show that A_n is generated by 3-cycles. Indeed, it is clear that A_n is generated by pairs of transpositions. But any pair of transpositions can be rewritten as

$$(ij)(ij) = e, \quad (ij)(jk) = (ijk), \quad (ij)(kl) = (ijk)(jkl).$$

Now we note that any 3-cycle can be represented as a commutator

$$(ijk) = (ij)(ik)(ij)(ik) = [(ij),(jk)]$$

and hence $A_n \subseteq S_n'$. From both $S_n' \subseteq A_n$ and $A_n \subseteq S_n'$ we conclude that $S_n' = A_n$. □

Proposition 6.1. *Let G be a group. Then*

1. *$G' \lhd G$*
2. *G/G' is abelain*
3. *If $N \lhd G$ then G/N is abelian iff $G' \subseteq N$*
4. *If H is a subgroup of G and $G' \subseteq H \subseteq G$ then $H \lhd G$*

Proof. It is clear that 3 and 4 imply 2 and 1 respectively.

3. We note that $\forall g, h \in G$ we have $(gN)(hN) = (hN)(gN) \iff (gN)(hN)(gN)^{-1}(hN)^{-1} = (ghg^{-1}h^{-1}N) = ([g,h]N) = eN \iff [g,h] \in N \iff N$ contains all commutators $\iff G' \subseteq N$.

4. If $g \in G$ and $h \in N$ then $ghg^{-1} = ghg^{-1}h^{-1}h = [g,h]h$. Now, since $G' \subseteq H$, we have $[g,h] \in H \implies [g,h]h \in H \implies ghg^{-1} \in H \implies N \lhd G$.

□

Proposition 6.2.

$$A'_n = \begin{cases} e, & n \leq 3, \\ V_4 = \mathbb{Z}_2 \times \mathbb{Z}_2, & n = 4, \\ A_n, & n \geq 5 \end{cases}$$

Proof. • For $n \leq 3$ A_n is abelian

- For $n = 4$, we have $V_4 \lhd A_4$. Indeed $V_4 = \{e, (12)(34), (13)(24), (14)(23)\}$ is survived by conjugations (no matter even or odd) and hence it is a normal subgroup in either S_4 or A_4. Moreover the order $|A_4/V_4| = 12/4 = 3$ and hence $A_4/V_4 = \mathbb{Z}_3$, i.e. it is an abelian group. Then by proposition 6.1 we have $A'_4 \subseteq V_4$. But $A'_4 \neq e$ since A_4 is non-abelian. Then V_4 consists of two conjugacy classes e and $\{(12)(34), (13)(24), (14)(23)\}$, but any normal subgroup consists of entire conjugacy classes. Thus $A'_4 = V_4$.
- For $n \geq 5$ consider the following permutation $(ij)(kl)$. It belong to the subgroup $A_4 \subset A_n$. Since $A'_4 = V_4$ we conclude that $(ij)(kl) \in A'_n$. But the elements $(ij)(kl)$ (pairs of independent transpositions) generate A_n. Indeed, we know that A_n is generated by pairs of transpositions. Then for $n \geq 5$ we can represent

  $$(ij)(jk) = (ij)(lm)(jk)(lm) \quad \text{for} \quad l, m \leq (i, j, k)$$

  Thus $A'_n = A_n$.

□

Definition 6.3. Let $G^{(k+1)} = \left(G^{(k)}\right)'$, then a group G is called solvable if $\exists k \in \mathbb{N} : G^{(k)} = e$. In this case

$$G \subset G^{(1)} \subset G^{(2)} \subset \cdots \subset G^{(k)} = e$$

and each $G^{(i)}/G^{(i+1)}$ is abelian.

Proposition 6.3. *Let G be a group and there exists a series of subgroups $G \subseteq G_1 \subseteq G_2 \subseteq \cdots \subseteq G_k = e$, such that $G_{i+1} \lhd G_i$ and G_i/G_{i+1} is abelian. Then 11' G is solvable.*

Proof. It is enough to show that $G^{(i)} \subseteq G_i \forall i$ because it will imply that $G^{(k)} \subseteq G_k = e$ and hence $G^{(k)} = e$. For $i = 0$ the statement holds $G^{(0)} = G$. Let $G^{(i)} \subseteq G_i$. We have to check that $G^{(i+1)} \subseteq G_{i+1}$. We know that G_i/G_{i+1} is abelian and hence by proposition 6.1 we have $G'_i \subseteq G_{i+1}$ and hence $G^{(i+1)} = (G^{(i)})' \subseteq G'_i \subseteq G_{i+1}$ □

Example. 1. $G = S_3$, $G' = A_3$, $G^{(2)} = e$

2. $G = S_4$, $G' = A_4$, $G^{(2)} = V_4$, $G^{(3)} = e$
3. S_n is not solvable.

Proposition 6.4. *Let G be a group, $H \lhd G$, H is solvable and G/H is solvable. Then G is solvable.*

Proof. We know that $\exists k > 0 : (G/H)^{(k)} = \{eH\}$. It is convenient to use the following

$$[g_1H, g_2H] = (g_1H)(g_2H)(g_1H)^{-1}(g_2H)^{-1} = [g_1, g_2]H.$$

Consider the projection $\pi : G \to G/H$. Then the equation above implies that $\pi(G^{(k)}) = (G/H)^{(k)} = \{eH\}$ and hence $G^{(k)} \subseteq H$ (since $\pi^{-1}(eH) = H$). From the other hand, we known that H is solvable, i.e. $\exists s \in \mathbb{N}$ such that $H^{(s)} = e \implies (G^{(k)})^{(s)} = G^{(k+s)} \subseteq H^{(s)} = \{e\} \implies G^{(k+s)} = e$ and hence G is solvable. □

Definition 6.4. A simple group is a group whose only normal subgroups are the trivial group and the group itself.

Theorem 6.1. *Let G be a finite group. Then $\exists$ a composition $G \subset H_1 \subset H_2 \subset \cdots \subset H_k = \{e\}$ such that $H_{i+1} \lhd H_i$ and H_{i+1}/H_i are all simple.*

Proof. We prove the statement by induction in $|G|$.

- $|G| = 1 \implies G = \{e\}$
- Let $|G| > 1$ and let $H \lhd G$ of the maximal order, but $|H| < |G|$. Then G/H is simple. Indeed suppose that $N \lhd G/H$ and $1 < |N| < |G/H|$. Consider the homomorphism map $\pi : G \to G/H$ then $\pi^{-1}(N) \lhd G$ (preimage of a normal subgroup in G/H is a normal subgroup in G). Clearly $|H| < |\pi^{-1}(N)| < |G|$. But it contradict the assumption that the order of H is maximal.

  Take $H_1 = H$. Then $|H_1| < |G|$ and by induction assumption $\exists\ H_1 \subset H_2 \subset \cdots \subset H_k = \{e\}$ such that $H_{i+1} \lhd H_i$ and H_i/H_{i+1} is simple. Thus we obtained

$$G \subset H_1 \subset H_2 \subset \cdots \subset H_k = \{e\}$$

□

Proposition 6.5. *Jordan-Hölder theorem. Any two composition series of a given group are equivalent in a sense they have the same composition length and the same composition factors (that is simple quotient groups $\{G/H_1, H_1/H_2, \ldots, H_{k-1}/H_k\}$), up to permutation and isomorphism.*

Proposition 6.6. *Abelian group G is simple iff $G = \mathbb{Z}_p$, where p is prime.*

Proposition 6.7. *A_n is simple $\forall n \geq 5$.*

Proof. Any $N \lhd A_n$ has to be a union of A_n conjugacy classes. Note that given $\sigma \in A_n$ its conjugacy classes in S_n and A_n may not be the same $C_{S_n}(\sigma) \neq C_{A_n}(\sigma)$. However, if either σ has

1. 1 cycle of even length
2. 2 cycles of the same odd length

then

$$C_{S_n}(\sigma) = C_{A_n}(\sigma) = \{\tau \in S_n | \tau \text{ and } \sigma \text{ have the same cyclic structure}\}.$$

It is clear that $C_{A_n}(\sigma) \subseteq C_{S_n}(\sigma)$ (for $C_{A_n}(\sigma)$ we conjugate with even permutations, while for $C_{S_n}(\sigma)$ we conjugate by all). It is enough to prove that if $\tau = \gamma\sigma\gamma^{-1}$ in S_n, then there exists even permutation β such that $\tau = \beta\sigma\beta^{-1}$.

Consider $\tau = \gamma\sigma\gamma^{-1}$. If γ is even, then everything is proved. If γ is odd, then

1. In the case 1, we take $\alpha = (i_1, \ldots, i_{2n})$ i.e. α be exactly that cycle of even length.

2. In the case 2, we have two cycles of the same odd length $(i_1, \ldots, i_q)(j_1, \ldots, j_q)$ with $q \in 2\mathbb{Z} + 1$ take $\alpha = (i_1 j_1) \ldots (i_q j_q)$

In both cases α is odd permutation and $\alpha\sigma = \sigma\alpha$. Thus $\gamma\alpha \in A_n$ and hence $\tau = (\gamma\alpha)\sigma(\gamma\alpha)^{-1}$, i.e. σ and τ are conjugated in A_n.

Now, let $\sigma \in N \lhd A_n$ and $\sigma \neq e$. The order of σ has the form $\mathrm{ord}(\sigma) = pk$ where p is a prime number. Then $\tau = \sigma^k \in N$ and $\mathrm{ord}(\tau) = p$. Thus $\tau =$ product of cycles of length p.

1. $p \geq 5 \implies \tau = (i_1, \ldots, i_p)\tau_1$ where either $\tau_1 = e$ or it is a product of cycles of length p. Then $\tau' = (i_1 i_2 i_3)\tau(i_1 i_2 i_3)^{-1} = (i_2 i_3 i_1 i_4 \ldots i_p)\tau_1 \in N \implies \tau'\tau^{-1} = (i_1 i_2 i_4) \in N$. It implies that all (xyz) lie in A_n. Indeed, in this case there are at least two cycles of length 1 (since $p \geq 5$, we have $p - 3 \geq 2$) and hence $C_{S_n}((xyz)) = C_{A_n}((xyz))$. But A_n is generated by 3 cycles. Thus $N = A_n$.

2. $p = 3$. If $\tau = (i_1 i_2 i_3)$ then $N = A_n$. If $\tau = (i_1 i_2 i_3)(j_1 j_2 j_3)\tau_1$. Then $\tau' = (i_1 j_1)(i_2 j_2)\tau(i_1 j_1)(i_2 j_2) = (i_1 i_2 j_3)(j_1 j_2 i_3)\tau_1 \in N$ and hence $\tau'\tau^{-1} = (i_1 j_1)(i_2 j_2)$. Thus we have a permutation with even cycle and hence all permutations $(i_1 j_1)(i_2 j_2) \in A_n$. But A_n is generated by pairs of independent cycles (see the proof of proposition 6.2). Hence $N = A_n$.

3. $p = 2$. Hence $\tau = (i_1 i_2)(i_3 i_4)\tau_1$. Take $\tau' = (i_1 i_2 i_3)\tau(i_1 i_2 i_3)^{-1} = (i_2 i_3)(i_1 i_4)\tau_1 \in N$. Thus $\tau'\tau^{-1} = (i_1 i_3)(i_2 i_4) \in N$. Again $N = A_n$.

□

Problems

1. Describe the derived group D_n'

2. Show that a set $\mathrm{GL}(n, \mathbb{F}_q)$, consisting of $n \times n$ invertible matrices with entries in $\mathbb{F}_q$ (a field of q elements, q is prime) form a finite group. Find the order of this group. Is this group simple?

3. A set $\mathrm{SL}(n, \mathbb{F}_q)$ is a set of $n \times n$ matrices of determinant one with entries in $\mathbb{F}_q$. Show that this set form a subgroup of $\mathrm{GL}(n, \mathbb{F}_q)$. Find the order of this subgroup. Is this subgroup normal? If so, what is the quotient group?

4. Describe a center of $\mathrm{SL}(2, \mathbb{F}_q)$. A quotient by this center is by definition $\mathrm{PSL}(2, \mathbb{F}_q)$.
Turns out, $\mathrm{PSL}(2, \mathbb{F}_q)$ is simple except $q = 2$ and 3. Establish isomorphisms of $\mathrm{PSL}(2, \mathbb{F}_2)$ and $\mathrm{PSL}(2, \mathbb{F}_3)$ with known non-simple groups of little order.

5. $^{(*)}$ Describe a center of $\mathrm{SL}(n, \mathbb{F}_q)$. A quotient by this center is by definition $\mathrm{PSL}(n, \mathbb{F}_q)$. Find the order of $\mathrm{PSL}(n, \mathbb{F}_q)$.

Lecture 7: Sylow theorems

Definition 7.1. Center of G

$$Z(G) = \{z \in G | zg = gz \, \forall g \in G\}.$$

Proposition 7.1. *A center of a group is abelian normal subgroup $Z(G) \lhd G$.*

Proof. Indeed

1. $Z(G)$ contains the identity element e
2. If $x \in Z(G)$ and $y \in Z(G)$ then so is xy. Indeed $\forall g \in G$

$$gxyg^{-1} = gxg^{-1}gyg^{-1} = xy$$

3. $\forall x, y \in Z(G)$ one has $xy = yx$. Indeed

$$xy = y(xy)y^{-1} = yx$$

□

Corollary. *Let G be a finite group, $(x_1, \dots x_r)$ its conjugacy classes and let first q of them are one dimensional. Then $Z(G) = \{x_1, \dots, x_q\}$ and*

$$|G| = |Z(G)| + \sum_{i=q+1}^{r} \frac{|G|}{|C_{x_i}|},$$

where C_{x_i} is the cetralizer of the element x_i, i.e. the set $C_x = \{g \in G | gxg^{-1} = x\}$.

Definition 7.2. A group G is called $p-$group if $|G| = p^n$.

Proposition 7.2. *Every finite p-group G (group of order p^n where p is a simple number) has a non-trivial center $Z(G) \neq e$*

Proof. If G is abelian then $Z(G) = G$. In the opposite case the center $Z(G) = \{x_1, \dots, x_q\}$ is smaller than G, i.e. $q < r = |G|$. Centralizers of all elements must divide p^n and hence their sizes are

$$\frac{|G|}{|C_{x_i}|} = p^{n_i} \quad \text{with} \quad n_i > 0$$

by orbit-stabilizer theorem. But in this case the equality

$$|G| = |Z(G)| + \sum_{q+1}^{r} p^{n_i}$$

implies that $Z(G)$ must be divisible by p, i.e. $Z(G) = p^k$ with $k > 0$. □

Corollary. *If $G/Z(G)$ is cyclic then G is abelian.*

Proof. If $G/Z(G)$ is abelian cyclic then there exists $g \in G$ such that $G/Z(G) = Z(G), gZ(G), \dots$ Now $\forall x, y \in G$ one has

$$x = g^i z, \quad y = g^j w, \quad z, w \in Z(G)$$

but then

$$xy = g^i z g^j w = g^{i+j} zw = g^j w g^i z = yz.$$

□

Proposition 7.3. *Any p-group is solvable.*

Proof. It can be proven by induction in k ($|G| = p^k$). For $k = 0$ the statement is obvious. For $k > 0$, $Z(G) \neq e$ and $Z(G) \lhd G \implies |G/Z(G)| = p^l < p^k$. By induction assumption $G/Z(G)$ is solvable. Moreover, $Z(G)$ is abelian and hence solvable. The by proposition 6.4 G is solvable. □

Proposition 7.4. *Any group of order p^2 is abelian. Moreover it is either $\mathbb{Z}_{p^2}$ or $\mathbb{Z}_p \times \mathbb{Z}_p$.*

Proof. Assume that G is non-abelian. On the other hand, by proposition $|Z(G)|$ is divisible by p, i.e. either $|Z(G)| = 1$, $|Z(G)| = p$ or $|Z(G)| = p^2$.

- If $|Z(G)| = 1$. It contradicts Proposition 7.2.
- If $|Z(G)| = p$. Then we can consider the quotient group $G/Z(G)$ (since $Z(G)$ is always normal). Then the order of the quotient group is $|G/Z(G)| = p$ and thus $G/Z(G) = \mathbb{Z}_p$. But this fact contradicts Proposition 7.4.
- If $|Z(G)| = p^2$ then $Z(G) = G$ and thus G is abelian.

Since G is abelian, it is either $\mathbb{Z}_{p^2}$ or $\mathbb{Z}_p \times \mathbb{Z}_p$. □

Remark 7.1. Note that a group of order p^3 is not necessarily abelian. For example $|D_4| = 2^3$, but D_4 is non-abelian. More general example is the group generated by the matrices

$$\begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix}$$

over the field of p elements $\mathbb{F}_p$.

Definition 7.3. Let G be a finite group and p is a prime number such that $|G| = p^k m$, $k \geq 0$ and $\gcd(m, p) = 1$. Then a subgroup $H \subseteq G$ such that $|H| = p^k$ is called a Sylow $p-$subgroup.

Remark 7.2. Consider $G = S_4$ and $p = 2$. Since $|S_4| = 24 = 2^3 \cdot 3$ one expects to have Sylow subgroups of order 8. For example the dihedral group D_4.

Theorem 7.1. *(Sylow first theorem). For any G and any prime p such that $|G| = p^k m$, $gcd(p, m) = 1$ a Sylow subgroup exists.*

Proof. Let us prove the statement by induction. If $|G| = 1$ then the statement of the theorem is obvious. Then assume that theorem holds up to some order $|G| < d$. The take any G with $|G| = d$ and let $d = p^k m$. Then there are 3 possible cases

1. If G is abelian, then by fundamental theorem of finite abelian groups $G = \mathbb{Z}_{k_1} \times \dots \mathbb{Z}_{k_n}$. Then each $k_i = p^{l_1}s$, where s divides m and $\gcd(p, S) = 1$, but then $\mathbb{Z}_{k_i} = \mathbb{Z}_{p^{l_i}} \times \mathbb{Z}_s$. Thus G has a subgroup $\mathbb{Z}_{p^{l_1}} \times \dots \mathbb{Z}_{p^{l_n}}$. The order of this group is exactly p^k.

2. If G is non-abelian and there exists a conjugacy class $C(g)$ with $|C(g)| = n$ (since G is non-abelian, at least one conjugacy class should consists of more that 1 element) such that $\gcd(n, p) = 1$. But then by Lagrange theorem
$$\underbrace{|G|}_{p^k \cdot m} = \underbrace{|C(g)|}_{n} \cdot |C_g|,$$
where C_g is the centralizer of g (a subgroup that survives g by conjugations). From this formula it follows that the order of the centralizer $|C_g|$ divides p^k, that is $|C_g| = p^k \cdot r$ where $r = \frac{m}{n}$. The order of $C_g = p^k \cdot r < d$ and thus by induction assumption there is Sylow subgroup $H \subseteq C_g \subseteq G$.

3. If G is non-abelian and all conjugacy classes $C(g_i)$ that are not in the center (that is $|C(g_i)| > 1$) have orders that divide p (in the opposite case we return to the previous item). Then
$$|G| = |Z(G)| + \sum_i |C(g_i)| = |Z(G)| + p \cdot s.$$
Thus $|Z(G)| = p^l \cdot r$ with $l \geq 1$ and $\gcd(r, p) = 1$. Thus by induction assumption there exists Sylow subgroup $H_1 \subseteq Z(G)$ with $|H_1| = p^l$. Moreover, since $H_1 \leq Z(G)$ it is a normal subgroup $H_1 \lhd G$ (it is clear that any subgroup of the center $Z(G)$ is normal in G) one can consider a quotient group G/H_1 such that $|G/H_1| = p^{k-l} \cdot m$. Thus by induction assumption there exists Sylow subgroup $H_2 \leq G/H_1$ such that $|H_2| = p^{k-l}$.

   Consider a projection $\pi : G \to G/H_1$ and let $H = \pi^{-1}(H_2)$ a subgroup in G. The order of H is the order of H_2 times the order of H_1: $|H| = |H_1| \cdot |H_2| = p^k$. Thus H is a Sylow $p-$subgroup.

□

Corollary. *If p divides $|G|$ then there exists element $g \in G$ of order p.*

Proof. Using theorem 7.1 we know that there exists a subgroup H such that $|H| = p^k$ with $k \geq 1$. Pick some $g \in H$, then g generates $\mathbb{Z}_{p^l}$ with $l \leq k$. Taking $g' = g^{p^{l-1}}$ provides an element of order p. □

Theorem 7.2. *(Sylow second theorem).*

1. *Any $p-$subgroup is contained in Sylow $p-$subgroup.*

2. *Given $H \subseteq G$ a Sylow p-subgroup, any other Sylow p?subgroup H' is conjugate to H; i.e. there exists $g \in G$ such that $H' = gHg^{-1}$.*

Proof. 1. Let $H \subseteq G$ be a Sylow p-subgroup and $H_1 \subseteq G$ some $p-$subgroup. Consider the action of H_1 on the set of left cosets G/H (H is not normal). From orbit/stabilizer theorem we know that the number of elements of any non-trivial orbit (an orbit with more that 1 element) is divisible by p, but $|G/H| = m$ and $\gcd(m, p) = 1$. Thus these exists at least one trivial orbit (of length 1), because otherwise the cardinality of the whole set G/H would be divisible by p. Trivial orbit means that $\exists g \in G : h_1 gH = gH \ \forall h_1 \in H_1$. Thus $g^{-1}h_1 g \in H \forall h_1 \in H_1 \implies H_1 \subseteq gHg^{-1}$, but $g^{-1}Hg$ is also Sylow $p-$subgroup.

2. Assume that H_1 is also Sylow $p-$subgroup. Thus $H_1 \subseteq g^{-1}Hg$, but $|H_1| = |H| = p^k \implies H_1 = g^{-1}Hg$.

□

Corollary. *Let $H \subseteq G$ be a Sylow $p-$subgroup. Then $H \lhd G$ iff H is unique Sylow $p-$subgroup.*

Theorem 7.3. *(Sylow third theorem). The number n_p of Sylow $p-$subgroups of G, $|G| = p^k m$*

1. *Divides m.*
2. *$n_p = 1 \mod p$*

Proof. Consider an action of G on the set of all Sylow $p-$subgroups $(g, H) \mapsto gHg^{-1}$. From the second Sylow theorem 7.2, we know that this action is transitive. By orbit/stabilizer theorem, we have

$$n_p = \frac{|G|}{|N_G(H)|},$$

where $N_G(H)$ is the normalizer of H in G. But $H \subseteq N_G(H) \overset{\text{Lagrange theorem}}{\implies} |N_G(H)| = p^k r$. Hence

$$n_p = \frac{|G|}{|N_G(H)|} = \frac{p^k m}{p^k r} \implies \frac{m}{n_p} = r.$$

Consider an action of a given Sylow $p-$subgroup H_0 on a set of all Sylow $p-$subgroups. Clearly it has at least one fixed point H_0. Let us show that this is the only fixed point. Indeed, let $H \neq H_0 : h_0 H h_0^{-1} = H \; \forall h_0 \in H_0$. Then $H_0 \subseteq N_G(H)$. But $H \subseteq N_G(H)$ as well. Hence we have a group $N_G(H)$ and two Sylow $p-$subgroups in it. Thus by Sylows second theorem 7.2 these two subgroups are conjugated in $N_G(H)$. But $H \lhd N_G(H) \implies H_0 = H$. Thus the set of Sylow $p-$subgroups splits as a set into 1 one dimensional and some number of non-trivial orbits under the action of H_0. But the length of any non-trivial orbit divides p. Thus

$$n_p = 1 + ps \implies n_p = 1 \mod p.$$

□

Probs:

1. How many groups are there of order
   a) $|G| = 77$? b) $|G| = 21$?
2. Let p and q be primes. Prove that there are no simple groups of order pq.
3. Prove that there are no simple groups of order 56.
4. Prove that there are no simple groups of order 250000.
5. Let G be a group generated by the matrices

$$\begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix}$$

   over the field $\mathbb{F}_2$. Find it out if $G = D_4$, $G = Q_8$ (the quaternion group), or some new group of order 8?

Lecture 8: Representations: introduction

Definition 8.1 (Representation)**.** Let G be a finite group and V be a complex vector space of complex dimension $\dim_{\mathbb{C}} V = n$. A *linear* action $G \times V \to V$ is called *a (complex linear n-dimensional) representation* of G in V. In other words, a representation of G in V is a homomorphism $\rho : G \to \mathrm{GL}(V)$.

Definition 8.2 (Kernel)**.** A *kernel* of a representation is a kernel of ρ: $\ker \rho = \{g \in G \,|\, \rho(g) = \mathrm{id}_V\}$. We call a representation $\rho : G \to \mathrm{GL}(V)$ *faithful* if ρ is injective, that is, $\ker \rho = \{1\}$.

If V is equipped with a preferrable basis $e_1, ..., e_n$, then $\mathrm{GL}(V) \simeq \mathrm{GL}(n, \mathbb{C})$, and so any representation ρ of G in V defines a homomorphism $\rho : G \to \mathrm{GL}(n, \mathbb{C})$. That is, any group element $g \in G$ is mapped to a square invertible complex-valued $n \times n$ matrix $\rho(g) \in \mathrm{GL}(n, \mathbb{C})$ in a way that preserves group structure: $g_1 g_2 \longmapsto \rho(g_1)\rho(g_2)$.

We will often abuse the notations by calling a vector space V itself a representation of G whenever the linear action $G \times V \to V$ is clear from the context. The right and pedantic way is to call ρ (or, equivalently a pair (V, ρ)) a representation. We will sometimes also omit the ρ sign in $\rho(g)v$ and simply write gv whenever the action is clear from the context.

Definition 8.3 (Morphism)**.** Let G be a fixed group and (V_1, ρ_1), (V_2, ρ_2) be two representations of G. A *morphism* of representations is a linear map $\varphi : V_1 \to V_2$ which commutes with G-action: $\varphi \circ \rho_1 = \rho_2 \circ \varphi$. In other words, the square

$$\begin{array}{ccc} V_1 & \xrightarrow{\varphi} & V_2 \\ \downarrow{\scriptstyle \rho_1} & & \downarrow{\scriptstyle \rho_2} \\ V_1 & \xrightarrow{\varphi} & V_2 \end{array}$$

commutes. Sometimes such a map $\varphi : V_1 \to V_2$ is called G-equivariant

Definition 8.4 (Isomorphism)**.** Let G be a group and V_1, V_2 be two representations of G. A inversible G-equivariant map $\varphi : V_1 \to V_2$ is called an *isomorphism* of representations V_1 and V_2. Representations are called *isomorphic* or *equivalent* if there is an isomorphism between them.

In terms of matrices an isomorphism is a square matrix φ such that $\rho_1(g) = \varphi\, \rho_2(g)\, \varphi^{-1}$. In other words, equivalent representations are really the same representation written in different bases.

Examples

1. Any group G admits a 1-dimensional representation $\mathbb{C}$, in which every element of G acts trivially: $\rho(g) = 1$, $\forall g \in G$. This representation is called *a trivial representation*. Trivial representation is never faithful for non-trivial groups.

2. Consider dihedral group $D_n = \langle r, s \,|\, r^n = s^2 = 1,\, srs^{-1} = r^{-1} \rangle$. In the first lecture we actually described a 2-dimensional representation $\mathbb{C}^2$ of it:

$$r \longmapsto R = \begin{pmatrix} \cos\frac{2\pi}{n} & -\sin\frac{2\pi}{n} \\ \sin\frac{2\pi}{n} & \cos\frac{2\pi}{n} \end{pmatrix}, \qquad s \longmapsto S = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}.$$

   It can be easily verified that this map is indeed a representation, that is, $R^n = S^2 = E$, $SRS^{-1} = R^{-1}$. This representation is faithful (check!)

3. Consider integral quaternion group $Q_8 = \{\pm 1, \pm i, \pm j, \pm k\}$. It is easily checked that this group admits two-dimensional representation $\mathbb{C}^2$ by Pauli matrices:

$$\pm 1 \longmapsto \pm \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad \pm i \longmapsto \pm \begin{pmatrix} 0 & -i \\ -i & 0 \end{pmatrix}, \quad \pm j \longmapsto \pm \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \quad \pm k \longmapsto \pm \begin{pmatrix} -i & 0 \\ 0 & i \end{pmatrix}$$

   This representation is faithful.

4. (Defining representation)
   Matrix groups $\mathrm{GL}(n, \mathbb{F})$, $\mathrm{SL}(n, \mathbb{F})$, $\mathrm{U}(n, \mathbb{F})$, $\mathrm{SU}(n, \mathbb{F})$, $\mathrm{O}(n, \mathbb{F})$, $\mathrm{SO}(n, \mathbb{F})$, $\mathrm{Sp}(n, \mathbb{F})$, etc are defined by their n-dimensional representations in $\mathbb{F}^n$.

5. (Permutation representation)
   Let G be a finite group. Let X be a set on which G acts from the left, $|X| = n$. Choose a basis in $\mathbb{C}^n$ enumerated by elements of X: $\{e_x\}_{x \in X}$. Then *permutation representation* of G in $\mathbb{C}^n$ is defined by an action $\rho(g)e_x = e_{gx}$.

   For example, consider a natural action of S_3 on $X = \{1, 2, 3\}$. Matrices of $\sigma \in S_3$ in a permutation representation $\mathbb{C}^3$ (in a usual basis) are just permutation matrices: $\sigma \longmapsto \rho(\sigma)_{ij} = \delta_{i,\sigma(j)}$. For instance,

$$(12) \longmapsto \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \qquad (123) \longmapsto \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}.$$

   Permutation representation is faithful if and only if the initial G-action on X is effective (i.e., such that every $g \in G$ moves at least one point in X).

6. (Regular representation)
   A particular case of permutation representation for which G acts on itself by left shifts: $X = G$ is called a *regular representation*. So, if $|G| = n$, we enumerate basis vectors of $\mathbb{C}^n$ by elements of G, $\{e_h\}_{h \in G}$, and consider the following linear action: $\rho(g)e_h = e_{gh}$.

Definition 8.5 (Subrepresentation)**.** Let V be a group representation of G. A vector subspace $U \subset V$ is said to be G-invariant if $G(U) \subset U$, i.e.,

$$\forall g \in G, \ \forall u \in U \quad g(u) \in U.$$

Such a G-invariant vector subspace U is called a *subrepresentation* of V.

Remark 8.1. A subrepresentation $U \subset V$ can be identified with an image of an injective morphism (of representations) $\iota : U \hookrightarrow V$.

Remark 8.2. It is clear that $\{0\}$ and V itself are always G-invariant. These two subspaces are thus called trivial subrepresentations of V.

Definition 8.6 ((Ir)reducible)**.** A group representation G is called *reducible* if it admits a non-trivial subrepresentation. If all the subrepresentations of V are trivial, then V is called *irreducible*.

Example. Consider a natural permutation representation of S_3 in $\mathbb{C}^3$. It admits two non-trivial subrepresentations:

$$U_1 = \left\{ x_1e_1 + x_2e_2 + x_3e_3 \;\middle|\; x_1 = x_2 = x_3 \right\}, \quad \dim U_1 = 1 \tag{8.1}$$
$$U_2 = \left\{ x_1e_1 + x_2e_2 + x_3e_3 \;\middle|\; x_1 + x_2 + x_3 = 0 \right\}, \quad \dim U_2 = 2.$$

Bases of them are $U_1 = \text{span}\,(e_1+e_2+e_3)$ and $U_2 = \text{span}\,(e_1-e_2, e_2-e_3)$. We see that the representation space $\mathbb{C}^3$ decomposes into a direct sum of G-invariant subspaces U_1 and U_2. In the basis $\{f_1, f_2, f_3\} = \{e_1 + e_2 + e_3, e_1 - e_2, e_2 - e_3\}$ the matrices of S_3 take the block-diagonal form:

$$\sigma \longmapsto \begin{pmatrix} 1 & 0 & 0 \\ 0 & a & b \\ 0 & c & d \end{pmatrix} = (1) \oplus \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

This is a particular case of a so-called direct sum of representations. The coordinate-free definition is as follows:

Definition 8.7 (Direct sum)**.** Let V_1 and V_2 be representations of a group G. *A direct sum* of these representations is a vector space $V_1 \oplus V_2$ equipped with a G-action

$$g(v_1 \oplus v_2) = g(v_1) \oplus g(v_2).$$

This action is sometimes denoted by $\rho_1 \oplus \rho_2$.

Remark 8.3. If we picked a basis in $V_1 \oplus V_2$ compatible with the direct sum structure (meaning $V_1 = \text{span}(e_1, ..., e_n)$, $V_2 = \text{span}(e_{n+1}, ..., e_{n+m})$ with $\dim V_1 = n$, $\dim V_2 = m$), then the G-action is represented by block-diagonal matrices

$$(\rho_1 \oplus \rho_2)(g) \begin{pmatrix} v_1 \\ v_2 \end{pmatrix} = \begin{pmatrix} A_1 & 0 \\ 0 & A_2 \end{pmatrix} \begin{pmatrix} v_1 \\ v_2 \end{pmatrix}.$$

Definition 8.8 (Completely reducible)**.** If a representation V is decomposed into a direct sum of (two or more) irreducible representations $V = V_1 \oplus V_2 \oplus ... \oplus V_r$, then V is said to be *completely reducible* or *semisimple*.

Proposition 8.1. *A representation V is a direct sum of V_1 and V_2 if and only if V_1 and V_2 are both G-invariant, $V_1 \cap V_2 = \{0\}$ and $V = V_1 + V_2$ as vector spaces.*

Remark 8.4. Let V_1 and V_2 be subrepresentations of V (G-invariant vector subspaces). Then $V_1 + V_2$ is G-invariant too. $V_1 \cap V_2$ is not G-invariant in general.

Let us consider a more general situation: let U be a subrepresentation of V. Let $\dim V = n$, $\dim U = k < n$. Choose a basis $(e_1, ..., e_k)$ of U and complete it to a basis of V by adding another $n - k$ linearly-independent vectors $e_{k+1}, ..., e_n$. In this basis the group G acts via the block-upper-triangular matrices:

$$g \longmapsto \rho(g) = \begin{pmatrix} A & B \\ 0 & D \end{pmatrix}. \qquad \rho(g) \begin{pmatrix} u \\ 0 \end{pmatrix} = \begin{pmatrix} Au \\ 0 \end{pmatrix}, \qquad \rho(g) \begin{pmatrix} u \\ v \end{pmatrix} = \begin{pmatrix} Au + Bv \\ Dv \end{pmatrix}$$

ρ is a representation whenever $\rho(gg') = \rho(g)\rho(g')$. In terms of matrices:

$$\begin{pmatrix} A & B \\ 0 & D \end{pmatrix} \begin{pmatrix} A' & B' \\ 0 & D' \end{pmatrix} = \begin{pmatrix} AA' & AB' + BD' \\ 0 & DD' \end{pmatrix}$$

We thus see that $(1,1)$ and $(2,2)$ blocks of the above *r.h.s.* behave as G-representations. The matrix A is a matrix in a *restriction representation* on an invariant subspace U. The matrix D is a matrix in *quotient representation* V/U.

Restriction and quotient representations can, of course, be defined without any need of choosing a U-compatible basis.

Definition 8.9 (Restriction)**.** Let U be an invariant subspace in the G-representation (V, ρ). *A restriction* of ρ on U is a G-representation $(U, \rho|_U)$, where $\rho|_U : G \to \mathrm{GL}(U)$ is just a restriction of $\rho : G \to \mathrm{GL}(V)$ onto U.

Definition 8.10 (Quotient)**.** Let U be an invariant subspace in the G-representation (V, ρ). *A quotient representation* of V by U is a G-representation $(V/U, \rho|_{V/U})$, where $V/U = \{v + U | v \in V\}$ is a quotient vector-space, and G-action is defined by formula $g(v + U) = gv + U$.

Exercise. Check that definitions of restiction and quotient representations are indeed correct provided $U \subset V$ is G-invariant.

Remark 8.5. If V is a representation of G and U is a subrepresentation, then there is a natural short exact sequence of representations:

$$0 \xrightarrow{0} U \xrightarrow{\iota} V \xrightarrow{\pi} V/U \xrightarrow{0} 0.$$

A natural question arises: given a G-invariant subspace U inside a representation V, it is always possible to find another G-invariant U' such that $V = U \oplus U'$? In other words, is any reducible representation of G completely reducible? Turns out, in general, the answer is no.

Example. Consider a two-dimensional $\mathbb{Z}$-representation $\mathbb{C}^2$:

$$n \longmapsto \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix}; \qquad n + m \longmapsto \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & m \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & n+m \\ 0 & 1 \end{pmatrix}$$

A subspace $U = \mathrm{span} \begin{pmatrix} 1 \\ 0 \end{pmatrix}$ is the only $\mathbb{Z}$-invariant subspace of $\mathbb{C}^2$.

But if the group G is finite (or, more generally, topologically compact), then it is true that every reducible representation is completely reducible.

Lemma 8.1. *Let G be a finite group. Let V be its representation and $U \subset V$ a subrepresentation. Then there exists a complementary G-invariant subspace U', so, $V = U \oplus U'$ as representations.*

Proof. Denote

$$S = \frac{1}{|G|} \sum_{g \in G} A(g)B(g^{-1}), \qquad \text{where} \qquad g \longmapsto \begin{pmatrix} A(g) & B(g) \\ 0 & D(g) \end{pmatrix} \tag{8.2}$$

A clever triangular change of basis via the g-independent matrix $\begin{pmatrix} 1 & S \\ 0 & 1 \end{pmatrix}$ does the trick. □

Theorem 8.1 (Maschke)**.** *Every finite-dimensional representation of finite group is completely reducible.*

Proof. Easily follows from the above lemma by induction. □

Probs:

1. Pick an appropriate basis in natural permutation representation of S_3 (see Example 5) and write down matrices in the two-dimensional U_2 of (8.1). Show that U_2 is irreducible.

2. Describe all one-dimensional representations of $\mathbb{Z}_n$.

3. Prove that in every one-dimensional representation of G its commutant $G' = [G, G]$ acts trivially.

4. Describe all one-dimensional representations of S_n and A_n.

5. Check the definitions of restriction and quotient representation to be correct.

6. Show that a clever triangular change (8.2) of basis in the proof of Maschke lemma indeed does the trick:
$$\begin{pmatrix} 1 & S \\ 0 & 1 \end{pmatrix} \begin{pmatrix} A(g) & B(g) \\ 0 & D(g) \end{pmatrix} \begin{pmatrix} 1 & -S \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} A(g) & 0 \\ 0 & D(g) \end{pmatrix}$$