Permutation Groups. Part I: Basics

(the online course)

Andrey Vasil'ev

Sobolev Institute of Mathematics and School of Science of Hainan University

Novosibirsk-Hainan, 28.11.-19.12.2020

Schedule (Beijing Time) and References

- 28.11 10:00-11:30 Lectures 1-2 + Problems for homework
- 05.12 10:00-11:30 Lectures 3-4 + Problems for homework
- 12.12 10:00-11:30 Lectures 5-6 + Problems for homework
- 12.12-16.12.2020 Home test for participants
- 19.12 10:00-11:30 Seminars 1-2 (test results, problems from homeworks, questions, further developments).

The main sources (and references) for this course:

- J. D. Dixon and B. Mortimer, *Permutation Groups*, Graduate Texts in Mathematics, **163**, Springer (1996),
- My Homepage: http://math.nsc.ru/~vasand

Permutation groups (Lagrange, Galois, Jordan)

$\Downarrow$

Modern (abstract) algebra

$\Downarrow$ $\Downarrow$ $\Downarrow$ $\Downarrow$

Group Theory Geometry Combinatorics Et Cetera

$\Updownarrow$ $\Updownarrow$ $\Updownarrow$ $\Updownarrow$

Permutation group theory

1. Permutation and Abstract Groups

Ω is a nonempty set (in most cases, a finite set of size n);
Elements $\alpha, \beta, \ldots \in \Omega$ are called points.

A bijection $x : \Omega \to \Omega$ is called a permutation of Ω, for $\alpha, \beta \in \Omega$, $\beta = \alpha^x$ means that β is the image of α under the action of x:

$$x = \begin{pmatrix} \ldots & \alpha & \ldots \\ \ldots & \beta & \ldots \end{pmatrix} = \begin{pmatrix} \ldots & \alpha & \ldots \\ \ldots & \alpha^x & \ldots \end{pmatrix} =$$

$$= \begin{pmatrix} \alpha_1 & \alpha_2 & \ldots & \alpha_n \\ \beta_1 & \beta_2 & \ldots & \beta_n \end{pmatrix} = \begin{pmatrix} \alpha_1 & \alpha_2 & \ldots & \alpha_n \\ \alpha_1^x & \alpha_2^x & \ldots & \alpha_n^x \end{pmatrix}.$$

Notation: $\mathrm{Sym}(\Omega)$ is the set of all permutations of Ω.

Ex. 1. $|\Omega| = n \Rightarrow |\mathrm{Sym}(\Omega)| = n!$

A product $z = xy$ is the result of composition of $x, y \in \mathrm{Sym}(\Omega)$: given $\alpha \in \Omega$, $\alpha^{xy} = (\alpha^x)^y$ (from left to right: first x, then y), i. e.

$$x \cdot y = \begin{pmatrix} \dots \alpha \dots \\ \dots \beta \dots \end{pmatrix} \cdot \begin{pmatrix} \dots \beta \dots \\ \dots \gamma \dots \end{pmatrix} = \begin{pmatrix} \dots \alpha \dots \\ \dots \gamma \dots \end{pmatrix} = z.$$

The product $z = xy$ belongs to $\mathrm{Sym}(\Omega)$, so a multiplication $(x, y) \mapsto xy$ is a binary algebraic operation on $\mathrm{Sym}(\Omega)$.

Theorem 1. $\mathrm{Sym}(\Omega)$ is a group w.r.t. the multiplication.

1. associativity: $\alpha^{(xy)z} = (\alpha^{xy})^z = ((\alpha^x)^y)^z = (\alpha^x)^{yz} = \alpha^{x(yz)}$ for every $\alpha \in \Omega$, so $(xy)z = x(zy)$ for every $x, y, z \in \mathrm{Sym}(\Omega)$;
2. the neutral element $e \in \mathrm{Sym}(\Omega)$ is the identity map on Ω.
3. $x^{-1} = \begin{pmatrix} \dots\beta\dots \\ \dots\alpha\dots \end{pmatrix}$ is the inverse for $x = \begin{pmatrix} \dots\alpha\dots \\ \dots\beta\dots \end{pmatrix}$. $\square$

The group $\mathrm{Sym}(\Omega)$ is called the symmetric group on Ω.

A permutation group G on (a set) Ω is a subgroup of $\mathrm{Sym}(\Omega)$.

Notation: $G \leq \mathrm{Sym}(\Omega)$ and $\deg(G) = |\Omega|$ is a degree of G.

We are going to study permutation groups!

Groups G and G' are isomorphic, if there is a bijection $\varphi : G \to G'$, called a (group) isomorphism, that preserves the operation:

$$(xy)^\varphi = x^\varphi \cdot y^\varphi \text{ for every } x, y \in G.$$

Permutation groups $G \leq \mathrm{Sym}(\Omega)$ and $G' \leq \mathrm{Sym}(\Omega')$ are permutation isomorphic, if there is a bijection $f : \Omega \to \Omega'$ and a group isomorphism $\varphi : G \to G'$ such that

$$(\alpha^x)^f = (\alpha^f)^{x^\varphi} \text{ for every } \alpha \in \Omega \text{ and } x \in G.$$

If permutation groups are permutation isomorphic, then they are isomorphic (as abstract groups). However, as we will see a bit later, the converse statement is wrong!

Notation: $G \simeq G'$ for gr. iso, and $G \cong G'$ for perm. iso.

Theorem 2. If $|\Omega| = |\Omega'|$, then $\mathrm{Sym}(\Omega) \cong \mathrm{Sym}(\Omega)$.

1. Take any bijection $f : \Omega \to \Omega'$, $\alpha \mapsto \alpha'$.
2. Take the bijection $\varphi : \mathrm{Sym}(\Omega) \to \mathrm{Sym}(\Omega')$ such that
$$x = \begin{pmatrix} \dots & \alpha & \dots \\ \dots & \beta & \dots \end{pmatrix} \mapsto x' = \begin{pmatrix} \dots & \alpha' & \dots \\ \dots & \beta' & \dots \end{pmatrix}.$$
3. Then $(\alpha^x)^f = \beta^f = \beta' = (\alpha')^{x'} = (\alpha^f)^{x^\varphi}$. $\square$

Observe that we do not need to check that φ is an isomorphism, because if $\alpha \xrightarrow{x} \beta \xrightarrow{y} \gamma$, then $\alpha' \xrightarrow{x'} \beta' \xrightarrow{y'} \gamma'$, so for each $\alpha' \in \Omega'$, $(\alpha')^{(xy)'} = (\alpha^{xy})' = \gamma' = ((\alpha')^{x'})^{y'} = (\alpha')^{x'y'} \Rightarrow (xy)^\varphi = x^\varphi y^\varphi$.

Notation: S_n is the symmetric group on the set $\{1, 2, \dots, n\}$.

Corollary. If $|\Omega| = n$, then $\mathrm{Sym}(\Omega) \cong S_n$.

Let $T \subseteq \mathrm{Sym}(\Omega)$. The support and set of fixed points of T are

$\mathrm{supp}(T) = \{\alpha \in \Omega \mid \alpha^x \neq \alpha \text{ for some } x \in T\}$ and

$\mathrm{fix}(T) = \{\alpha \in \Omega \mid \alpha^x = \alpha \text{ for all } x \in T\}$, respectively.

If $T = \{x\}$, then we write simply $\mathrm{supp}(x)$ and $\mathrm{fix}(x)$.

A cycle c of length m (or m-cycle) is a permutation of the form

$$c = \begin{pmatrix} \alpha_1 & \alpha_2 & \dots & \alpha_m & \beta_1 & \dots & \beta_k \\ \alpha_2 & \alpha_3 & \dots & \alpha_1 & \beta_1 & \dots & \beta_k \end{pmatrix}.$$

Here $\mathrm{supp}(c) = \{\alpha_1, \dots, \alpha_m\}$ and $\mathrm{fix}(c) = \{\beta_1, \dots, \beta_k\}$, $m \geq 2$.

Note that '1-cycle' is the identity map on Ω.

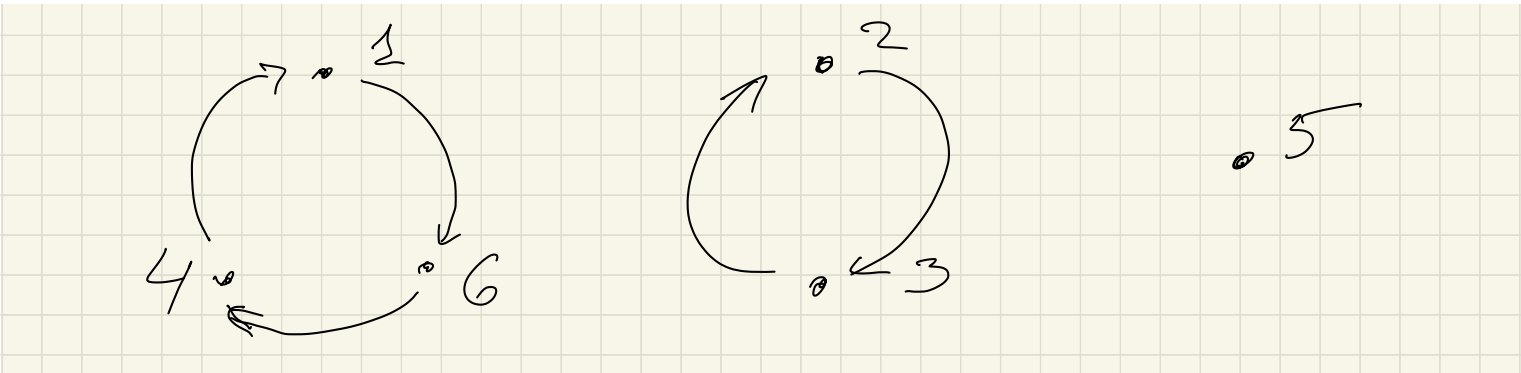
Notation: $c = (\alpha_1, \alpha_2, \dots, \alpha_n) = (\alpha_2, \dots, \alpha_n, \alpha_1) = \dots$

Cycles $c, d \in \mathrm{Sym}(\Omega)$ are disjoint, if $\mathrm{supp}(c) \cap \mathrm{supp}(d) = \varnothing$.

Ex 2. If cycles c and d are disjoint, then $cd = dc$.

Theorem 3. Every permutation can be written as a product of pairwise disjoint cycles, and this representation is unique up to the order in which the cycles appear.

Idea of proof (example): Let $x = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 3 & 2 & 1 & 5 & 4 \end{pmatrix} \in S_6$.



Ω is the disjoint union of orbits $\{1, 6, 4\}, \{2, 3\}, \{5\}$ of x.

According to this partition,

$x = (1, 6, 4)(2, 3) = (2, 3)(1, 6, 4) = (1, 6, 4)(2, 3)(5)$. $\square$

Advantages of a cyclic representation:

- has short form,
- reflects an internal structure (orbits).

Ex 3. $x = (1,6,4)(2,3)$, $y = (1,5,6,2,4) \Rightarrow xy = (1,2,3,4,5,6)$.

Let us find the order $|x|$ (as element of a group) of a permutation x:

1. if c is an m-cycle, then $|c| = m$,
2. if c and d are disjoint cycles, then $(cd)^k = c^k d^k$,
3. if $x = c_1 \dots c_r$ is a product of disjoint cycles of lengths $m_1, \dots, m_r$, then $|x| = \mathrm{lcm}(m_1, \dots, m_r)$.

Say, $|(1,6,4)(2,3)| = \mathrm{lcm}(3,2) = 6$.

Theorem 4. Every permutation can be written as a product of transpositions, that is of cycles of length two.

Proof. $(1,2,\dots,m) = (1,2)(1,3)\dots(1,m)$. $\square$

There are different ways to write a permutation as a product of transpositions: $(1,2) = (1,3)(2,3)(1,3)$.
What can we say about the number of transpositions there?

$x = c_1 \dots c_r$ is a product of disjoint cycles of lengths $m_1, \dots, m_r$
$\lambda(x) = (m_1 - 1) + \dots + (m_r - 1) = |\operatorname{supp}(x)| - r$ and
$\operatorname{sgn}(x) = (-1)^{\lambda(x)}$ are called the decrement and sign of x,
x is even (odd), if $\lambda(x)$ is even (odd, respectively).
If $x = (1,6,4)(2,3)$, then $\lambda(x) = 5 - 2 = 3$, so x is odd.

Representing as $x = (1,6,4)(2,3)(5)$, we get $\lambda(x) = 6 - 3 = 3$, because $\lambda(x) = |supp(x)| - r = n - r'$, where $n = |\Omega|$ and r' is the number of cycles in the product including '1-cycles'.

Theorem 5. Let $x, y, t \in S_n$ and t be a transposition. Then $\lambda(xt) = \lambda(x) \pm 1$. In particular, $\operatorname{sgn}(xy) = \operatorname{sgn}(x)\operatorname{sgn}(y)$, so $\operatorname{sgn} : S_n \to \{1, -1\}$ is a homomorphism, surjective for $n \geq 2$.

See the proof in [DM, Lemma 1.6A] or prove as an exercise. □

Theorem 5. Let $x, y, t \in S_n$ and t be a transposition. Then $\lambda(xt) = \lambda(x) \pm 1$. In particular, $\operatorname{sgn}(xy) = \operatorname{sgn}(x)\operatorname{sgn}(y)$, so $\operatorname{sgn} : S_n \to \{1, -1\}$ is a homomorphism, surjective for $n \geq 2$.

Ex 4. If $x = t_1 \dots t_s$ is a product of transpositions, then

- s and $\lambda(x)$ are of the same parity;
- $s \geq \lambda(x)$.

Theorem 5 implies that $\operatorname{Alt}(\Omega) = \{x \in \operatorname{Sym}(\Omega) \mid \operatorname{sgn}(x) = 1\}$ is a normal subgroup of $\operatorname{Sym}(\Omega)$ called the alternating group of Ω.

$G = \langle x_i \mid i \in I \rangle$ means that G is generated by $\{x_i \mid i \in I\}$.

Theorem 4 yields that $S_n = \langle (i,j) \mid i \neq j \in \{1, \dots, n\} \rangle$, $n \geq 2$.

Ex 5. Prove that

- $S_n = \langle (1,i) \mid i = 2, \dots, n \rangle = \langle (i-1,i) \mid i = 2, \dots, n \rangle$, $n \geq 2$;
- $A_n = \langle (i,j,k) \mid \text{ distinct } i,j,k \in \{1, \dots, n\} \rangle$, $n \geq 3$;
- $A_n = \langle (i,j)(k,l) \mid \text{ distinct } i,j,k,l \in \{1, \dots, n\} \rangle$, $n \geq 5$.

Let $G \leq \mathrm{Sym}(\Omega)$ and $G' \leq \mathrm{Sym}(\Omega')$.
Examples when $G \simeq G'$ but $G \not\cong G'$:

1. $G = \{e, (1,2)\} = S_2$ and $G' = \{e, (1,2)(3,4)\} \leq S_4$.
2. $G = \{e, (1,2)(3,4), (1,3)(2,4), (1,4)(2,3)\} = K_4 \leq S_4$ and $G' = \{e, (1,3), (2,4), (1,3)(2,4)\} \leq S_4$.

Notation: C_n is a cyclic group of order n.

In (1), $G \simeq C_2 \simeq G'$, but $G \not\cong G'$ because $|\Omega| \neq |\Omega'|$.

In (2) $G \simeq C_2 \times C_2 \simeq G'$, but $G \not\cong G'$ due to

Theorem 6. If $f : \Omega \to \Omega'$ is a bijection inducing the permutation isomorphism $\varphi : G \to G'$, then x and x^φ have the same cyclic decomposition for all $x \in G$.

Permutations x and y have the same cyclic decomposition if they have the same number of cycles of each size (including '1-cycles').

To prove Theorem 6 apply the definition of perm. isomorphism. $\square$

Starting from a permutation group, one can (and must!) study it as an abstract group. Taking an abstract group, we can (and we shall!) study it as a permutation group using the notion of a group action.

G is a (abstract) group and Ω is a nonempty set. The group G acts on Ω if a homomorphism $\rho : G \to \mathrm{Sym}(\Omega)$ is defined, that is for every $x \in G$, $\alpha \in \Omega$ the element $\alpha \circ x = \alpha^{x\rho}$ is uniquely defined.
Notation: $G \curvearrowright \Omega$ means that G acts on Ω.

It follows from the definition that if $G \curvearrowright \Omega$, then

1. $\alpha \circ (xy) = (\alpha \circ x) \circ y$;
2. $\alpha \circ e = \alpha$;
3. $\alpha \circ x = \beta \Rightarrow \beta \circ x^{-1} = \alpha$.

If an action is determined, we write simply α^x instead of $\alpha \circ x$.

We refer to ρ as the action of G on Ω. The degree $\deg \rho$, the kernel $\ker \rho$, the image G^ρ of the action (of ρ) are defined as usual. If $\ker \rho = 1$, then the action is faithful, $G^\rho \simeq G/\ker \rho$ and so on.

Homomorphism ρ is also called a permutation representation of G.

Examples:

1. If $G \leq \mathrm{Sym}(\Omega)$, then $G \curvearrowright \Omega$ naturally: $\alpha \circ x = \alpha^x$.
2. If $\Omega = V$ is a vector space and $G \leq \mathrm{GL}(V)$, then $G \curvearrowright \Omega$ by transformations: $v \circ x = v^x$.
3. If $\Omega = G$, then $G \curvearrowright \Omega$ by right multiplications: $g \circ x = gx$. In this case ρ is called the (right) regular representation or Cayley representation.
4. If $H \leq G$ and $\Omega = G/H = \{Hg \mid g \in G\}$ is the set of right cosets of H in G, then $G \curvearrowright \Omega$ by right multiplications: $Hg \circ x = Hgx$.
5. If $\Omega = G$, then $G \curvearrowright \Omega$ by conjugation: $g \circ x = g^x = x^{-1}gx$.
6. If $\Omega = H$ is a group, and $\rho : G \to \mathrm{Aut}(H)$ is a homomorphism, then $G \curvearrowright \Omega$ by automorphisms: $h \circ x = h^{x\rho}$.

Ex 6. Find the kernels of the actions in (1)–(6).
Ex 7. (Cayley) Every group is isomorphic to a permutation group.

Homework 1

1. Read Sect. 1.1–1.3 from [DM].
2. Let

$$x = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 \\ 9 & 8 & 1 & 6 & 4 & 2 & 7 & 11 & 3 & 10 & 5 \end{pmatrix}$$

$$y = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 \\ 6 & 7 & 10 & 2 & 3 & 1 & 11 & 8 & 4 & 5 & 9 \end{pmatrix}.$$

   Find (i) cyclic representations of x and y, (ii) xy and yx, (iii) $\lambda(x)$ and $\lambda(y)$, (iv) orders of x,y, xy, and yx, (v) y^{24}.
3. Solve Ex. 2, 4–7 from the lecture.
4. Solve Ex. 1.2.6, 1.2.7, 1.2.10 from [DM].
5. Solve Ex. 1.3.2–1.3.5 from [DM].

2. Subsets of Ω and Subgroups of G

Let $G \leq \mathrm{Sym}(\Omega)$ (or wider $G \curvearrowright \Omega$).

For a point $\alpha \in \Omega$, the following two objects are dual to each other:

- $\alpha^G = \{\alpha^x \mid x \in G\} \subseteq \Omega$, the orbit of α under (action of) G.
- $G_\alpha = \{x \in G \mid \alpha^x = \alpha\} \subseteq G$, the (point) stabilizer of α in G.

Theorem 1. Suppose $\alpha, \beta \in \Omega$ and $x, y \in G$. Then

1. α^G and β^G are either equal or disjoint, so the set of all orbits is the partition of Ω.
2. G_α is a subgroup of G and $G_\beta = x^{-1} G_\alpha x$ whenever $\beta = \alpha^x$. Moreover, $\alpha^x = \alpha^y \Leftrightarrow G_\alpha x = G_\alpha y$.
3. $|\alpha^G| = |G : G_\alpha|$ for all $\alpha \in \Omega$. If G is finite, $|\alpha^G||G_\alpha| = |G|$.

Item (3) of Theorem 1 which expresses the duality is known as the fundamental counting priniciple or generalized Lagrange's theorem. We refer to it as the orbit-stabilizer property.

Theorem 1. Suppose $\alpha, \beta \in \Omega$ and $x, y \in G$. Then

1. α^G and β^G are either equal or disjoint, so the set of all orbits is the partition of Ω.
2. G_α is a subgroup of G and $G_\beta = x^{-1} G_\alpha x$ whenever $\beta = \alpha^x$. Moreover, $\alpha^x = \alpha^y \Leftrightarrow G_\alpha x = G_\alpha y$.
3. $|\alpha^G| = |G : G_\alpha|$ for all $\alpha \in \Omega$. If G is finite, $|\alpha^G||G_\alpha| = |G|$.

1. If $\delta \in \alpha^G \cap \beta^G$, then there are $x, y \in G : \delta = \alpha^x = \beta^y$. So $\delta^G = \{\delta^z \mid z \in G\} = \{\alpha^{xz} \mid z \in G\} = \alpha^G$ and, by the same arguments, $\delta^G = \beta^G$.
2. If $x, y \in G_\alpha$, then $\alpha^{xy^{-1}} = \alpha$, hence $G_\alpha \leq G$. If $\beta = \alpha^x$, then $y \in G_\beta \Leftrightarrow \alpha^{xy} = \alpha^x \Leftrightarrow xyx^{-1} \in G_\alpha$, so $G_\beta = x^{-1} G_\alpha x$. Finally, $\alpha^x = \alpha^y \Leftrightarrow \alpha^{xy^{-1}} = \alpha \Leftrightarrow xy^{-1} \in G_\alpha \Leftrightarrow G_\alpha x = G_\alpha y$.
3. Follows directly from (2). $\square$

G is transitive on Ω if one of the following holds:

1. for every $\alpha, \beta \in \Omega$ there is $x \in G$ such that $\alpha^x = \beta$;
2. for every $\alpha, \beta \in \Omega$, $\alpha^G = \beta^G$;
3. Ω is the only orbit of G.

G is intransitive on Ω if it is not transitive.

G is semiregular if $G_\alpha = 1$ for every $\alpha \in \Omega$,
G is regular if it is transitive and semiregular.

Corollary 2. Suppose that G is transitive on Ω. Then

1. For all $\alpha \in \Omega$, the stabilizers G_α are conjugated in G.
2. $|G : G_\alpha| = |\Omega|$ for each $\alpha \in \Omega$.
3. Let G be finite. Then G is regular $\Leftrightarrow |G| = |\Omega|$.

Let $x \in G \leq \mathrm{Sym}(\Omega)$. We present a new notation $\Omega_x := \mathrm{fix}(x)$ for the set of fixed points of x in order to emphasize another duality:

- $G_\alpha = \{x \in G \mid \alpha^x = \alpha\} \subseteq G$
- $\Omega_x = \{\alpha \in \Omega \mid \alpha^x = \alpha\} \subseteq \Omega$.

We use this duality to prove the following orbit-counting lemma, also called the Cauchy–Frobenius Lemma, or Burnside's lemma, or even "the lemma that is not Burnside's!"

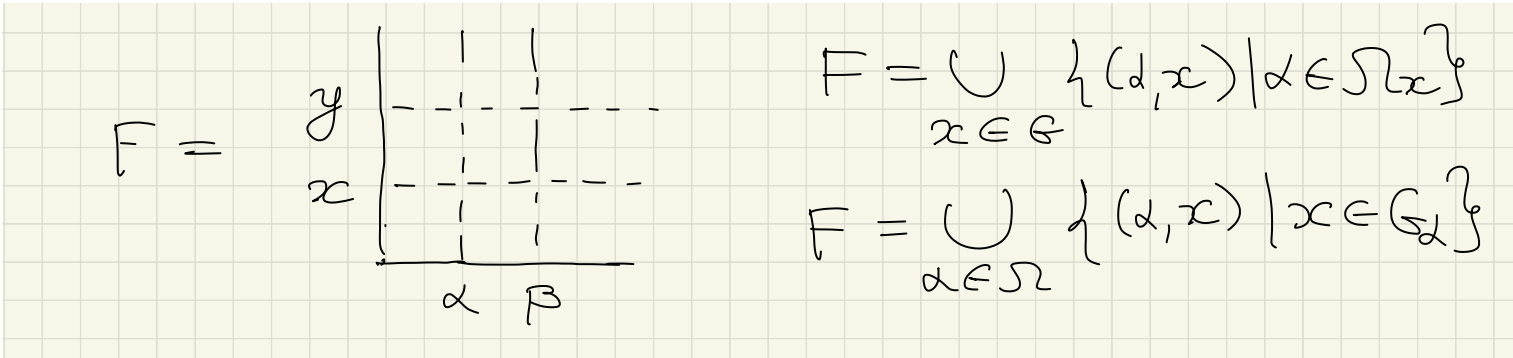
Theorem 3. Let $t(G)$ be the number of the orbits of an action of a (finite) group G on a (finite) set Ω. Then

$$t(G) = \frac{1}{|G|} \sum_{x \in G} |\,\mathrm{fix}(x)|.$$

We will prove the equality in the form $t\,|G| = \sum_{x \in G} |\Omega_x|$, $t = t(G)$.

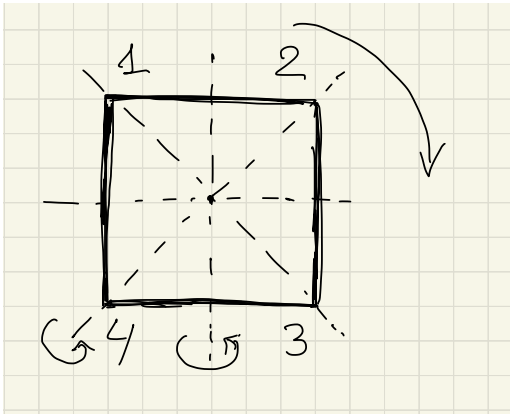
1. Put $F = \{(\alpha, x) \in \Omega \times G \mid \alpha^x = \alpha\}$. Then

$$\sum_{x \in G} |\Omega_x| = |F| = \sum_{\alpha \in \Omega} |G_\alpha|.$$



2. Let $\alpha_i^G = \Omega_i, i = 1, \ldots, t$ be the orbits of G. By Theorem 1,

$$|F| = \sum_{\alpha \in \Omega} |G_\alpha| = \sum_{i=1}^{t} |\alpha_i^G||G_{\alpha_i}| = \sum_{i=1}^{t} |G| = t|G|. \square$$



Example:
$G = \{e, (1,2,3,4), (1,3)(2,4), (1,4,3,2), (1,2)(3,4), (1,4)(2,3), (1,3), (2,4)\} = D_8$ is the group of symmetries of a square and $K = \{e, (1,3)(2,4), (1,3), (2,4)\} \leq G$.

$1^G = \{1,2,3,4\} = \Omega \Rightarrow G$ is transitive, $G_1 = \{e, (2,4)\}$,

$2^{G_1} = \{2,4\}$ and $G_{12} = (G_1)_2 = 1$. Theorem 1 $\Rightarrow$

$|G| = |1^G| \cdot |G_1| = |1^G| \cdot |2^{G_1}| \cdot |G_{12}| = 4 \cdot 2 \cdot 1 = 8.$

$1^K = \{1,3\}$ and $2^K = \{2,4\}$, so $\Omega = 1^K \cup 2^K \Rightarrow K$ is intransitive.

$\Omega_e = \Omega,\ \Omega_{(1,3)(2,4)} = \varnothing,\ \Omega_{(1,3)} = \{2,4\},\ \Omega_{(2,4)} = \{1,3\},$

Theorem 3 $\Rightarrow t(K) \cdot |K| = 2 \cdot 4 = \sum_{x \in K} |\Omega_x| = 4 + 0 + 2 + 2 = 8.$

Ex 1. The group D_{2n} of symmetries of a n-regular polygon is called a dihedral group. Find $|D_{2n}|$.

A subset Δ of Ω is G-invariant if $\Delta^G = \{\delta^G \mid \delta \in \Delta\} \subseteq \Delta$. Clearly, Δ is G-invariant $\iff$ Δ is the union of some orbits of G.

If Δ is G-invariant, then there is the restriction homomorphism from G onto G^Δ, where $x \mapsto x^\Delta$ with $\delta^{x^\Delta} := \delta^x$ for each $\delta \in \Delta$.

If Δ is an orbit of G, then G^Δ is a transitive constituent of G.

Theorem 4. Let $G \leq \mathrm{Sym}(\Omega)$.

1. If Ω is a disjoint union of G-invariant subsets Δ and Γ, then the map $x \mapsto (x^\Delta, x^\Gamma)$, $x \in G$, is an injective homomorphism from G into $G^\Delta \times G^\Gamma \leq \mathrm{Sym}(\Delta \cup \Gamma)$.
2. If $\Omega = \Omega_1 \cup \ldots \cup \Omega_t$, where $\Omega_1, \ldots \Omega_t$ are the orbits of G, then the map $x \mapsto (x^{\Omega_1}, \ldots, x^{\Omega_t})$, $x \in G$, is an injective homomorphism from G into $G^{\Omega_1} \times \ldots \times G^{\Omega_t}$.

Proof follows directly from the definitions.

Permutation Group $\Longrightarrow$ Transitive Group!

Ex 2. Prove that G is abelian (nilpotent, solvable) $\iff$
all transitive constituents of G are.

You can come from groups to transitive ones. But be careful!

Example: $K = \{e, (1,3)(2,4), (1,3), (2,4)\}$, $T = \{e, (1,3)(2,4)\}$,
$\Delta = \{1,3\}$ and $\Gamma = \{2,4\}$ are the orbits of K and T,
$K^\Delta = T^\Delta = \mathrm{Sym}(\Delta)$ and $K^\Gamma = T^\Gamma = \mathrm{Sym}(\Gamma)$,
but K is isomorphic to $\mathrm{Sym}(\Delta) \times \mathrm{Sym}(\Gamma)$ and T is not.

Ex 3. Find all (up to permutation isomorphism) groups having
exactly two orbits of length 3 each.

Let $\rho : G \to \mathrm{Sym}(\Omega)$ and $\sigma : G \to \mathrm{Sym}(\Gamma)$ be two permutation representations of group G. The representations ρ and σ (and the corresponding actions of G) are equivalent if $|\Omega| = |\Gamma|$ and there is a bijection $h : \Omega \to \Gamma$ such that

$$(\alpha^{x^\rho})^h = (\alpha^h)^{x^\sigma} \text{ for all } \alpha \in \Omega \text{ and } x \in G.$$

Notation: $\rho \sim \sigma$.

Ex 4. If $\rho \sim \sigma$, then $G^\rho \cong G^\sigma$.

Ex 5. If $\Omega = \Gamma$, then $\rho \sim \sigma \iff$ there is $c \in G : x^\sigma = c^{-1} x^\rho c$.

Ex 6*. $G^\rho \cong G^\sigma \not\Longrightarrow \rho \sim \sigma$ (see Ex. 1.6.17 in [DM]).

The following assertion is fundamental it theory of transitive groups.

Theorem 5. Let $\rho : G \to \mathrm{Sym}(\Omega)$ be a transitive permutation representation of a group G and $H \leq G$ a point stabilizer in this action. Then ρ is equivalent to the action of G on the set $\Gamma = G/H$ of the right cosets of H in G by right multiplications.

Lemma 6. Suppose that $\rho : G \to \mathrm{Sym}(\Omega)$ and $\sigma \to \mathrm{Sym}(\Gamma)$ are transitive representation of G, and H is a point stabilizer in the first action. Then $\rho \sim \sigma \iff H$ is a point stabilizer in the second.

(See Lemma 1.6B in [DM]). $H = \{x \in G \mid \alpha^{x^\rho} = \alpha\}$ for $\alpha \in \Omega$.

($\Longrightarrow$) Let $h : \Omega \to \Gamma$ be a bijection defining the equivalence $\rho \sim \sigma$ $\Rightarrow \alpha^{x^\rho} = \alpha \Leftrightarrow \alpha^h = (\alpha^{x^\rho})^h = (\alpha^h)^{x^\sigma} \Rightarrow H = \{x \in G \mid \beta^{x^\sigma} = \beta\}$.

($\Longleftarrow$) If $H = \{x \in G \mid \beta^{x^\sigma} = \beta\}$ for some $\beta \in \Gamma$, then $x \in H \iff \alpha^{x^\rho} = \alpha \iff \beta^{x^\sigma} = \beta$.

Define $h : \Omega \to \Gamma$ by $(\alpha^{x^\rho})^h := \beta^{x^\sigma}$.

Then h is well-defined and injective, because ρ is transitive and $\alpha^{x^\rho} = \alpha^{y^\rho} \iff xy^{-1} \in H \iff \beta^{x^\sigma} = \beta^{y^\sigma}$.

Moreover, h is surjective because σ is transitive.

For each $\gamma \in \Omega$ there is $a \in G : \gamma = \alpha^{a^\rho}$, so for each $x \in G$, $(\gamma^{x^\rho})^h = (\alpha^{(ax)^\rho})^h = \beta^{(ax)^\sigma} = (\beta^{a^\sigma})^{x^\sigma} = ((\alpha^{x^\rho})^h)^{x^\sigma} = (\gamma^h)^{x^\sigma}$. $\square$

Theorem 5. Let $\rho : G \to \mathrm{Sym}(\Omega)$ be a transitive permutation representation of a group G and $H \leq G$ a point stabilizer in this action. Then ρ is equivalent to the action of G on the set $\Gamma = G/H$ of the right cosets of H in G by right multiplications.

Proof. By Lemma 6, it suffices to prove that H is a point stabilizer in the second action. But this is clear, because for the point $H \in \Gamma$, we have $H \circ H = H \cdot H = H$. $\square$

It follows from Theorem 5 that we can (at least theoretically) describe all transitive representation of a group G. Taking (up to conjugacy) all subgroups H of G, we obtain (up to equivalence) all the transitive representations of G.

Permutation Group $\Longrightarrow$ Transitive Group $\Longrightarrow$?

A subset Δ of Ω is called a block for G if for each $x \in G$ either $\Delta^x = \Delta$ or $\Delta^x \cap \Delta = \varnothing$.

Easily, every one-element subset of Ω and Ω itself are blocks for G, they are called trivial blocks. Any other block is nontrivial. A block called minimal, if it is nontrivial and does not include any other nontrivial block.

Theorem 7. Let $G \leq \mathrm{Sym}(\Omega)$ be transitive, Δ a block for G. Then

1. Δ^x is a block for every $x \in G$,
2. the blocks from $\Sigma = \{\Delta^x \mid x \in G\}$ form a partition of Ω.

The set Σ is called the system of blocks for G, containing Δ.

Proof. (1) Observe that $(\Delta^x)^y = \Delta^{xy}$. If $\gamma \in \Delta^x \cap \Delta^{xy}$, then $\delta = \gamma^{x^{-1}} \in \Delta \cap \Delta^{xyx^{-1}}$, so $\Delta = \Delta^{xyx^{-1}}$. It follows that $\Delta^x = \Delta^{xy}$.

(2) Follows from (1), transitivity of G, and definition of a block. $\square$

Let $\Delta \subseteq \Omega$.

- $G_{(\Delta)} = \{x \in G \mid \delta^x = \delta \text{ for all } \delta \in \Delta\}$ is pointwise stabilizer
- $G_{\{\Delta\}} = \{x \in G \mid \Delta^x = \Delta\}$ is setwise stabilizer of Δ in G.

Theorem 8. Let G be transitive on Ω, $\Delta \in \Sigma$ a system of blocks.

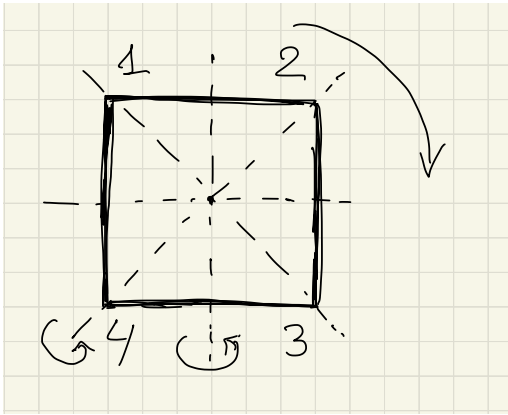
1. $G_{\{\Delta\}}$ is a subgroup of G, $|\Sigma| = |G : G_{\{\Delta\}}|$.
2. $|\Delta| = |G_{\{\Delta\}} : G_\alpha|$, where $\alpha \in \Delta$.
3. If $G_\alpha \leq K \leq G$, then there is a block system Σ_K such that $K = G_{\{\Delta_K\}}$, where $\alpha \in \Delta_K \in \Sigma_K$.

Ex. 7. Prove (1) and (2).

(3) Put $H = G_\alpha$. By Theorem 5, we may assume that $\Omega = G/H$.

$$\text{We have } K = \bigcup_{x \in K} Hx. \text{ Put } \Delta_K := \{Hx \mid x \in K\} \subseteq \Omega.$$

For $x \in G$, $\Delta_K \cap \Delta_K^x = K \cap Kx = K$ or $\varnothing$ by Lagrange's theorem, so Δ_K is a block of a system of blocks $\Sigma_K = \{Kx \mid x \in G\}$. $\square$



Example:
$G = \{e, (1,2,3,4), (1,3)(2,4), (1,4,3,2), (1,2)(3,4), (1,4)(2,3), (1,3), (2,4)\} = D_8$ and $H = G_1 = \{e, (2,4)\} \leq G$.

$\Delta = \{1,3\}$ is a block for G, since $\Delta^x = \Delta$ or $\Gamma = \{2,4\}$.

$K = G_{\{\Delta\}} = \{e, (2,4), (1,3), (1,3)(2,4)\} = \bigcup_{x \in K} Hx$.

$|\Delta| = |G_{\{\Delta\}} : G_1| = |K : H| = 2$.

$\Sigma = \{\Delta, \Gamma\}$ is the system of blocks and $|\Sigma| = |G : K| = 2$.

Vice versa, put $\Delta_K = \{Hx \mid x \in K\}$ and $\Sigma_K = \{Kx \mid x \in G\}$.

Then $\Delta_K = \Delta^{\rho_H}$ and $\Sigma_K = \Sigma^{\rho_H}$, where ρ_H is the representation of G on G/H by right multiplications.

$G_{(\Delta)} = G_{13} = H$ and $G_\Sigma = G_{\{\Delta\}} \cap G_{\{\Gamma\}} = K$, so
$G^\Delta \simeq G_{\{\Delta\}}/G_{(\Delta)} \simeq S_2$ and $G^\Sigma = G/G_\Sigma \simeq S_2$.

Let $G \curvearrowright \Omega$ transitively, Σ a system of blocks for G, containing Δ.

Define $\rho : G_{\{\Delta\}} \to \mathrm{Sym}(\Delta)$ by $x \mapsto x^{\Delta}$ with $\delta^{x^{\Delta}} := \delta^x$. Then ρ is a homomorphism, $\ker\rho = G_{(\Delta)}$, $G^{\Delta} := (G_{\{\Delta\}})^{\rho} \simeq G_{\{\Delta\}}/G_{(\Delta)}$.

Define $\sigma : G \to \mathrm{Sym}(\Sigma)$ by $x \mapsto x^{\Sigma}$ with $\Delta^{x^{\Sigma}} := \Delta^x$. Then σ is a homo-sm, $G_{\Sigma} = \ker\sigma = \bigcap_{\Delta\in\Sigma} G_{\{\Delta\}}$, $G^{\Sigma} := G^{\sigma} \simeq G/G_{\Sigma}$.

Claim. G is permutation isomorphic to a subgroup of the wreath product of G^{Δ} and G^{Σ}.

If Σ is nontrivial we can reduce some problems about G to problems about smaller groups G^{Δ} and G^{Σ}!

Let $G \leq \mathrm{Sym}(\Omega)$ is transitive, $|\Omega| \geq 2$. A group G is imprimitive if it has a nontrivial system of blocks, and primitive otherwise.

Theorem 8 implies

Corollary 9. Let G act transitively on Ω, then G is primitive if and only if a point stabilizer G_α is a maximal subgroup of G.

Ex. 8. Prove the corollary.

Ex. 9. Let Σ be a system of blocks for G, containing a minimal block Δ. Prove that G^Δ is primitive on Δ.

Perm. Group $\Longrightarrow$ Transitive Group $\Longrightarrow$ Primitive Group!

Homework 2

1. Read Sect. 1.4–1.6 and Theorem 1.7A from [DM].
2. (i) Find (up to permutation isomorphism) all transitive permutation groups of degree at most 4.
   (ii) Which of them are primitive?
3. Find (up to permutation isomorphism) all intransitive groups of degree 5.
4. Solve Ex. 1–9 from the lecture.
5. Solve Ex. 1.4.1–1.4.3 from [DM].
6. Solve Ex. 1.5.4, 1.5.8, 1.6.13, 1.7.1 from [DM].

3. Permutations as Automorphisms

Permutations arise "in nature" as automorphisms of various mathematical objects, which preserve the underlying structure of the object in a suitable sense.

Let $\Omega^k = \underbrace{\Omega \times \ldots \times \Omega}_{k \text{ times}}$ be the kth Cartesian power of a set Ω.

A set $r \subseteq \Omega^k$ is called k-ary relation (or simply a relation) on Ω.

We say that $\mathcal{X} = (\Omega, \mathcal{R})$ is a relational structure on Ω,

if $\mathcal{R}$ is a set of relations (not necessarily of the same arity) on Ω.

$\mathrm{Aut}(\mathcal{X}) = \{x \in \mathrm{Sym}(\Omega) \mid r^x = r, r \in \mathcal{R}\}$ is a subgroup of $\mathrm{Sym}(\Omega)$.

$\mathrm{Aut}(\mathcal{X})$ is called the (full) automorphism group of $\mathcal{X}$.

Remark. $r^x = r$ is the equality of sets (not elements!):

$r^x = r \Longleftrightarrow (\alpha_1^x, \ldots, \alpha_k^x) \in r$ for each $(\alpha_1, \ldots, \alpha_k) \in r$.

Any subgroup of $\mathrm{Aut}(\mathcal{X})$ is an automorphism group of $\mathcal{X}$.

1. Algebraic Structures

- G is an abstract group:

$\mathrm{Aut}(G) = \{x \in \mathrm{Sym}(G) \mid (ab)^x = a^x b^x \text{ for all } ab \in G\} \leq \mathrm{Sym}(G)$

In the language of relational structures: if $\mathcal{X}(G) = (\Omega, \mathcal{R})$, where $\Omega = G$, $\mathcal{R} = \{r\}$ and $r = \{(a, b, ab) \mid \text{ for all } a, b \in G\} \subseteq \Omega^3$, then $\mathrm{Aut}(\mathcal{X}(G)) = \{x \in \mathrm{Sym}(G) \mid r^x = r, r \in \mathcal{R}\} = \mathrm{Aut}(G)$, because $r^x = r \Longleftrightarrow (a^x, b^x, (ab)^x) \in r$ for all $a, b \in G$.

Ex. 1. Define the automorphism groups of a ring R and vector space V over a field F in the language of relational structures.

- $P = (\Omega, \leq)$ is a poset (partially ordered set):

$\mathrm{Aut}(P) = \{x \in \mathrm{Sym}(\Omega) \mid \alpha^x \leq \beta^x \Leftrightarrow \alpha \leq \beta \text{ for all } \alpha, \beta \in \Omega\}$.

Ex. 2. P is a finite totally ordered set $\Longrightarrow \mathrm{Aut}(P) = 1$.

How does it work?

If $K \trianglelefteq G$, i. e. K is a normal subgroup of a group G, then $G \curvearrowright K$ by conjugation, so and $C_G(K) = \{x \in G \mid u^x = u, u \in K\}$, the centralizer of K in G, is the kernel of this action (say, σ).
By the first homomorphism theorem, $G/C_G(K) \simeq G^\sigma \leq \mathrm{Sym}(K)$.
However, σ preserves the group structure of K, so $G^\sigma \leq \mathrm{Aut}(K)$.

If $K = C_G(K)$ is an elementary abelian of order $n = p^d$, then G/K can be embedded not only in S_n, but also in $GL_d(p)$; in particular, we have $|G| \leq p^{d(d+1)}$ instead of $|G| \leq n!\, n$.

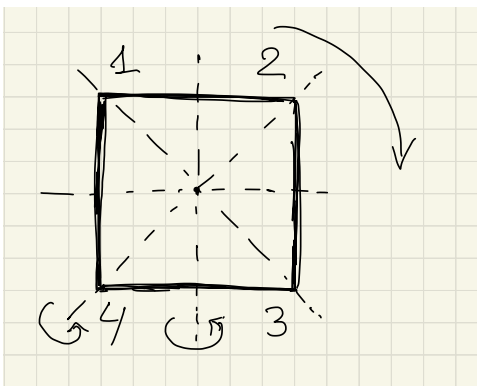
If $K = G$, then $C_G(G) = Z(G)$, the center of G, $G^\sigma \simeq G/Z(G)$.
The subgroup $\mathrm{Inn}(G) = G^\sigma \leq \mathrm{Aut}(G)$ induced by the action is called the group of inner automorphisms of G, $\mathrm{Inn}(G) \trianglelefteq \mathrm{Aut}(G)$.

2. Geometric Structures

- F is a geometric figure in an euclidian space V:

$\mathrm{Aut}(F) = \{x \in \mathrm{GO}(V) \mid F^x = F\} \leq \mathrm{GO}(V) \leq \mathrm{Sym}(V)$
is called the group of symmetries of F. Here for $x \in \mathrm{Sym}(V)$,
$x \in \mathrm{GO}(V) \iff d(v,u) = d(v^x, u^x)$ for all $u, v \in V$.

Given $x \in \mathrm{GO}(V)$, we have $x \in \mathrm{SO}(V) \iff \det(x) = 1$
$\iff x$ does not change the orientation of V. In this case,
$\mathrm{Aut}^+(F) = \{x \in \mathrm{SO}(V) \mid F^x = F\} = \mathrm{Aut}(F) \cap \mathrm{SO}(V)$
is called the group of rotations of F.

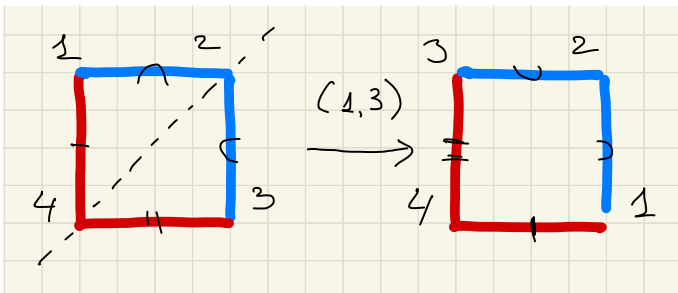


$G = \{e, (1,2,3,4), (1,3)(2,4), (1,4,3,2), (1,2)(3,4), (1,4)(2,3), (1,3), (2,4)\}$ and $G^+ = \{e, (1,2,3,4), (1,3)(2,4), (1,4,3,2)\}$ are the groups of symmetries and rotations of a square F represented in their actions on the set of vertices or set of edges of F.

Problem: How many different squares with edges painted in k colors ($k = 2$ for example) are there?

Answer: There are k possible colors for each of 4 four edges, so the cardinality of the set Ω of different squares is $N(k) = k^4$.

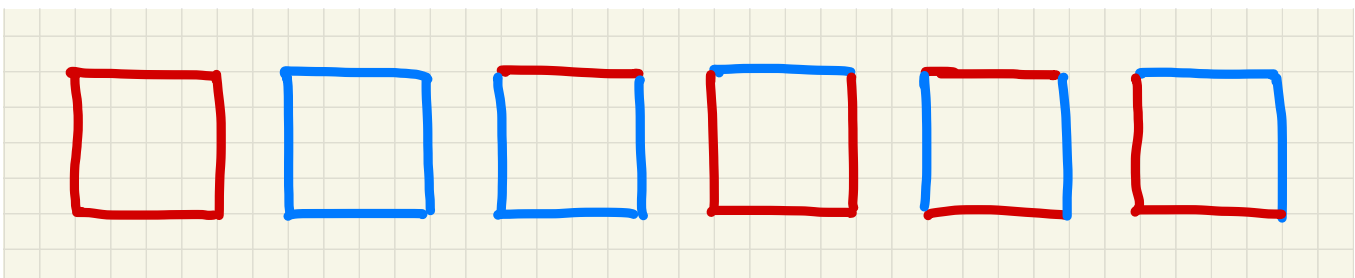
This is true if we cannot move the square. But if we can?



We call two squares fudamentally different if we cannot obtain one from another by moving.

Problem: How many fundamentally different squares with edges painted in k colors are there?

Counting for $k = 2$, we have $FN(2) = 6$, while $N(2) = 16$:



How to solve this kind of problems in general (not only for squares?)

The group G of symmetries of a square acts on the set Ω of different squares, and two squares are fundamentally different if they lie in the distinct orbits of this actions. It follows that the number of fundamentally different squares is equal to the number of orbits of this action. So we may apply the orbit-counting lemma:

$$t(G) = \frac{1}{|G|} \sum_{x \in G} |\Omega_x|.$$

We have

x	e	$(13)(24)$	(1234)	$(12)(34)$	(13)
$\# x$	1	1	2	2	2
$\lvert\Omega_x\rvert$	k^4	k^2	k	k^3	k^2

Therefore

$$FN(k) = \frac{1}{8}(k^4 + k^2 + 2k + 2k^3 + 2k^2) = \frac{k(k^3 + 2k^2 + 3k + 2)}{8}.$$

Ex. 3. Find the number of fundamentally different cubes (with the faces painted in k colors). For this purpose:
(i) find the order of the group G of rotations of the cube (why rotations, not symmetries?);
(ii) write down all the elements of G in its action on the faces of the cube (is this action primitive?);
(iii) apply the orbit-counting lemma to find $t(G)$ in the action of G on the set Ω of different (but not fundamentally different) cubes.

- $\mathcal{P} = (P, L, \mathcal{I})$ is a projective plane:

Elements of P are points, elements of L are lines,

$I \subseteq P \times L$ is an incidence relation: $(\alpha, I) \in \mathcal{I} = \alpha$ lies on I;

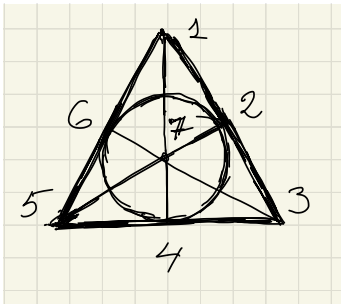
the following axioms hold:

1. any two distinct points from P lie on a unique line from L;
2. any two distinct lines from L meet in a unique point from P;
3. there exist at least four points of which no three are collinear.

$\mathrm{Aut}(\mathcal{P})$ sends point to point, line to line, and preserves $\mathcal{I}$.

Claim. For a finite projective plane $\mathcal{P}$ there is an integer q called the order of $\mathcal{P}$ such that $|P| = |L| = q^2 + q + 1$, each line contains $q + 1$ points, each point lies on $q + 1$ lines.

The Fano plane $\mathcal{F} = (P, L, \mathcal{I})$ is of order 2:



$$L = \{ l_1 = (1,2,3),\ l_2 = (3,4,5),\ l_3 = (5,6,1),\ l_4 = (1,7,4),\ l_5 = (2,7,5),\ l_6 = (3,7,6),\ l_7 = (2,4,6) \}.$$

We find the order of $G = \mathrm{Aut}(\mathcal{P})$. By the orbit-stabilizer property,

$$|G| = |7^G| \cdot |G_7| = 7 \cdot |G_7| = 7 \cdot |1^{G_7}| \cdot |G_{1,7}| = 7 \cdot 6 \cdot |G_{1,7}| = 7 \cdot 6 \cdot |G_{1,7,4}|.$$

If $H = G_{1,7,4}$, then $2^H = \{2, 3, 5, 6\}$ and $H_2 = 1$, so $|H| = 4$.

Finally, $|G| = 7 \cdot 6 \cdot |H| = 7 \cdot 6 \cdot 4 = 168$.

Ex. 4. Let ρ and σ be the natural actions of G on P and L. Prove that $G^\rho \cong G^\sigma$, but ρ and σ are not equivalent (apply Theorem 2.5).

3. Graphs

Ω is a set, $E \subseteq \Omega \times \Omega$ is a binary relation on Ω.

$\Gamma = (\Omega, E)$ is a graph with the vertex set Ω and edge set E.

Remark. E is not necessarily symmetric or irreflexive!

If E is symmetric and irreflexive, Γ is a simple graph.

One may define Γ as a binary relational structure with $\mathcal{R} = \{E\}$, so $\mathrm{Aut}(\Gamma) = \{x \in \mathrm{Sym}(\Omega) \mid E^x = E\}$, where $E^x = E$ means $(\alpha, \beta) \in E \iff (\alpha^x, \beta^x) \in E$ for all $\alpha, \beta \in \Omega$. In other words, $\mathrm{Aut}(\Gamma)$ preserves the adjacency structure of Γ.

First, we consider how groups can help in graph theory.

$G \leq \mathrm{Sym}(\Omega)$ or $G \curvearrowright \Omega$.

Given $k \in \mathbb{N}$, the action of G on Ω induces the action of G on Ω^k:

$(\alpha_1, \ldots, \alpha_k)^x = (\alpha_1^x, \ldots, \alpha_k^x)$, for each $x \in G$.

An orbit r of the induced action is called k-orbit.

Notation: $\mathrm{Orb}_k(G)$ is the set of all k-orbits.

The subset $\Omega^{(k)}$ of Ω^k consisting of distinct points is G-invariant.

Ex. 5. $|\Omega| = n \Longrightarrow |\Omega^{(k)}| = n!/(n-k)!$

A group G is k-transitive, if G is transitive on $\Omega^{(k)}$.

Examples. S_n is n-transitive, A_n is $(n-2)$-transitive (for $n \geq 3$), the automorphism group of the Fano plane is 2-transitive.

A subset of Ω consisting of k points is called a k-subset.

Notation: $\Omega^{\{k\}}$ is the set of all k-subsets.

Ex. 6. $|\Omega| = n \Longrightarrow |\Omega^{\{k\}}| = n!/k!(n-k)!$

A group G is k-homogeneous, if G is transitive on $\Omega^{\{k\}}$.

Clearly, if G is k-transitive, then G is k-homogeneous.

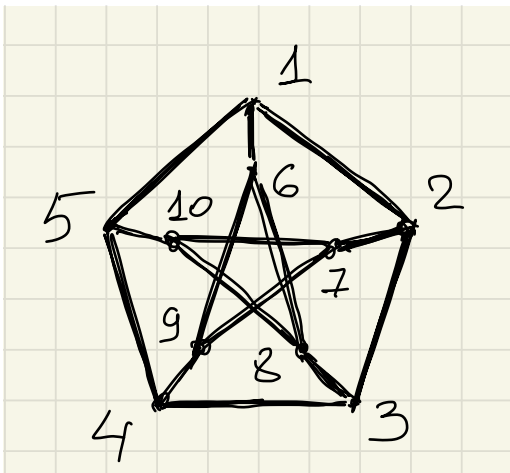
If $\Delta = \{\alpha, \beta, \gamma, \delta, \varepsilon\}$, then $G = \mathrm{Sym}\,\Delta$ acts on $\Omega = \Delta^{\{2\}} =$

$$= \left\{ \begin{array}{cccccccccc} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ \alpha\beta & \gamma\delta & \varepsilon\alpha & \beta\gamma & \delta\varepsilon & \gamma\varepsilon & \varepsilon\beta & \beta\delta & \delta\alpha & \alpha\gamma \end{array} \right\},$$

where $\alpha\beta$ under 1 means $1 := \{\alpha, \beta\}$. Now $G \leq \mathrm{Sym}(\Omega) \cong S_{10}$.

Any 2-orbit R, also called an orbital, of G is a binary relation on Ω, so $\Gamma = (\Omega, R)$ is a graph, an orbital graph of G on Ω.

$\mathrm{Orb}_2(G) = \{R_0, R_1, R_2\}$ is of size 3, $R_0 = \{(i, i) \mid i = 1, \ldots, 10\}$.



$\Gamma_1 = (\Omega, R_1)$ is the Petersen graph
Adjacency:
$\{\alpha, \beta\} \cap \{\gamma, \delta\} = \varnothing \Rightarrow (1, 2) \in E$
$\{\gamma, \varepsilon\} \cap \{\varepsilon, \beta\} = \{\varepsilon\} \Rightarrow (6, 7) \notin E$

$\Gamma_2 = (\Omega, R_1)$, the complement of Γ_1, is the Johnson graph $J(5, 2)$.

Now we consider how graphs can help in permutation group theory by proving Higman's theorem.

Theorem 1. Let $G \leq \mathrm{Sym}(\Omega)$ be transitive. Then G is primitive $\iff$ all nontrivial orbitals graphs of G on Ω are connected.

Notation. $\alpha \rightsquigarrow \beta$ ($\alpha \sim \beta$) means that there is a directed (undirected) path from α to β.

A graph $\Gamma = (\Omega, E)$ is connected if $\alpha \rightsquigarrow \beta$ for every $\alpha, \beta \in \Omega$.

$\Gamma = (\Omega, E)$ is weakly connected if $\alpha \sim \beta$ for every $\alpha, \beta \in \Omega$.

Lemma 2. Let Γ be an orbital graph for a finite transitive group $G \leq \mathrm{Sym}(\Omega)$. Then Γ is connected if it is weakly connected.

Proof. Let $B(\alpha) = \{\beta \in \Omega \mid \alpha \rightsquigarrow \beta\}$. If $\beta \in B(\alpha)$, then $B(\beta) \subseteq B(\alpha)$. Since G is transitive, there is $x \in G$ with $\alpha^x = \beta$. Hence $B(\alpha)^x = B(\beta)$. In particular, $|B(\beta)| = |B(\alpha)|$. Now $B(\beta) \subseteq B(\alpha)$ yields $B(\beta) = B(\alpha)$. $\square$

Theorem 1. Let $G \leq \mathrm{Sym}(\Omega)$ be transitive. Then G is primitive $\iff$ all nontrivial orbitals graphs of G on Ω are connected.

Proof. $\Longrightarrow$) If Δ is a connected component of an orbital graph, then either $\Delta^x = \Delta$ or $\Delta^x \cap \Delta = \varnothing$, so Δ is a block.

$\Longleftarrow$) If Δ is a nontrivial block, then there are $\alpha, \beta \in \Delta$ with $\alpha \neq \beta$. Take the orbital R containing (α, β). The orbital graph $\Gamma = (\Omega, R)$ is disconnected. Indeed, if $\gamma \in \Omega \setminus \Delta$ and $(\gamma, \delta) \in R$ for some $\delta \in \Delta$, then there is $x \in G$ such that $(\alpha, \beta)^x = (\gamma, \delta)$, which is impossible by the definition of a block. $\square$

Example. The Petersen graph and Johnson graph $J(5, 2)$ are connected, so the above group G for which they are orbital graphs is primitive.

Homework 3

1. Read Sect. 1.7 and 2.1–2.4 from [DM].
2. Solve Ex. 1,3,4 from the lecture.
3. Solve Ex. 1.7.5, 2.1.3, 2.1.9 from [DM].
4. Solve Ex. 2.2.1, 2.2.5, 2.2.7, 2.3.4 from [DM].
5. Till the end of Wednesday, December 23, solve the **hometest**, see my Homepage: http://math.nsc.ru/~vasand

4. Problem Solutions and Further Developments

First, we discuss the home test problems.

Problem 1. Does there exist a permutation x such that

(a) $x \in S_9$,

(b) $\operatorname{sgn}(x) = 1$,

(c) $|x| = 10$?

Solution: For $x = (1,2,3,4,5)(6,7)(8,9) \in S_9$, we have $\lambda(x) = 9 - 3 = 6$, so $\operatorname{sgn}(x) = (-1)^{\lambda(x)} = 1$; and $|x| = \operatorname{lcm}(5,2,2) = 10$.

Note that you cannot find such x in S_n with $n < 9$. Indeed, (c) $\Rightarrow n \geq \operatorname{lcm}(5,2) = 7$, but for a permutation y represented as the product of a 5-cycle and 2-cycle, $\operatorname{sgn}(y) = -1$, because $\lambda(y) = (5+2) - 2 = 5$ is odd.

Problem 2. Let $a = (1, 2, \ldots, n) \in S_n$ be the cycle of length n. Solve in $G = S_n$ a "quadratic" equation: $x^2 = a$.

Solution: (1) If n is even, then $\operatorname{sgn}(a) = -1$, but $\operatorname{sgn}(x^2) = \operatorname{sgn}(x)^2 = 1$. Thus, the equation does not have any solution for even n.

(2) Assume that n is odd. Then $m = (n+1)/2$ is a positive integer. Put $x = a^m$. We have

$$a^n = e \quad \Longrightarrow \quad a^{n+1} = a \quad \Longrightarrow \quad x^2 = (a^m)^2 = a^{n+1} = a,$$

so a^m is the solution. Do we have other solutions?

(3) Let b be a solution. Then

(i) $ba = ab \Leftrightarrow a^b = a \Longrightarrow b \in C_G(a) = \{g \in G \mid a^g = a\}$.

(ii) By the orbit-stabilizer property, $|G : C_G(a)| = |a^G|$ (consider $G \curvearrowright G$ by conjugation).

(iii) $|a^G| = |\{a^g \mid g \in G\}| = |\{c \in G \mid c \text{ is } n\text{-cycle}\}| = (n-1)!$

(iv) $|C_G(a)| = |G|/|a^G| = n!/(n-1)! = n \Longrightarrow C_G(a) = \langle a \rangle$.

(v) $b \in \langle a \rangle \Rightarrow b = a^k, k = 0, \ldots, n-1 \Rightarrow a^{2k} = a \Rightarrow k = m$. $\square$

Problem 3. Let G be a finite abelian permutation group. Prove

(a) if G is transitive, then it is regular;

(b) if G is primitive, then G has a prime order.

Solution: (a) G is regular, if G is transitive and $G_\alpha = 1$ for $\alpha \in \Omega$ (all G_α's are conjugated in transitive group, so 'all α' = 'some α').

Transitivity of $G \Longrightarrow$ for every $\beta \in \Omega$ there is $g \in G : \beta = \alpha^g$.
So $x \in G_\alpha \Longrightarrow \beta^x = (\alpha^g)^x = \alpha^{gx} = \alpha^{xg} = (\alpha^x)^g = \alpha^g = \beta$,
because G is abelian. Since it is true for every $\beta \in \Omega$, $x = e$ is the identity permutation. Thus $G_\alpha = 1$, as required.

Ex 1: If $G \leq S_n$ and $C_{S_n}(G)$ is transitive, then G is semiregular.

(b) a transitive group G is primitive $\Longleftrightarrow$ G_α is maximal
(see Corollary 2.9, i.e, Corollary 9 in Part 2 of the lectures).

From (a) $\Longrightarrow G_\alpha = 1$, so the identity is a maximal subgroup of G.
Thus, G is of prime order. $\square$

Problem 4. Let H be a group. Set $G = H \times H$ and $\Omega = H$. Prove

(a) the rule: $x^{(g,h)} = g^{-1}xh$ for all $x \in \Omega$ and $(g, h) \in G$, defines an action of G on Ω;

(b) the action is always transitive (find the stabilizer G_e of the neutral element $e \in H = \Omega$);

(c) the action is faithful $\Longleftrightarrow$ the center $Z(H) = 1$;

(d) the action is primitive $\Longleftrightarrow$ H is a simple group.

Solution: (a) For $x \in \Omega$ and $(g_1, h_1), (g_2, h_2) \in G$,

$$\left(x^{(g_1,h_1)}\right)^{(g_2,h_2)} = (g_1^{-1}xh_1)^{(g_2,h_2)} = g_2^{-1}g_1^{-1}xh_1h_2 =$$
$$= (g_1g_2)^{-1}x(h_1h_2) = x^{(g_1g_2,h_1h_2)}, \text{ as required.}$$

(b) For $x, y \in H$, we have $x^{(x,y)} = x^{-1}xy = y \Longrightarrow G$ is transitive, and $e^{(g,h)} = e \Leftrightarrow g^{-1}eh = e \Leftrightarrow g = h \Longrightarrow G_e = \{(h, h) \mid h \in H\}$.

Problem 4. Let H be a group. Set $G = H \times H$ and $\Omega = H$. Prove

(c) the action is faithful $\Longleftrightarrow$ the center $Z(H) = 1$;

(d) the action is primitive $\Longleftrightarrow$ H is a simple group.

Solution: (c) $h \in Z(H) \Rightarrow h^{-1}xh = x$ for each $x \in H \Rightarrow$ $(h, h) \in \ker \rho$, so $Z(H) \neq 1 \Longrightarrow \ker \rho \neq 1$.

If $(g, h) \in \ker \rho = \bigcap_{x \in H} G_x$, then, in particular, $(g, h) \in G_e$, so $g = h$. Thus, $x^{(h,h)} = h^{-1}xh = x$ for each $x \in H \Rightarrow h \in Z(H)$, so $ker\rho \neq 1 \Longrightarrow Z(H) \neq 1$.

(d) $K \trianglelefteq H \Rightarrow K^{(g,h)} = g^{-1}Kh = Kg^{-1}h$ is a right coset of K in H. Hence either $K^{(g,h)} \cap K = K$ or $K^{(g,h)} \cap K = \varnothing$, so K is a block. Thus, G is primitive $\Longrightarrow$ H is simple.

$e \in \Delta \subseteq H$ is a block $\Rightarrow \Delta^{(h,h)} = \Delta$ for each $h \in H$ $(h^{-1}eh \in \Delta)$. Hence Δ is a normal subset. If $x, y \in \Delta$, then $x^{-1}xy = y$, so $\Delta = \Delta^{(x,y)} = x^{-1}\Delta y = \Delta x^{-1}y \Rightarrow x^{-1}y \in \Delta$. Therefore, Δ is a subgroup of H. Thus, G is simple $\Longrightarrow$ H is primitive. $\square$

Problem 5. For the graph Γ from the figure below,

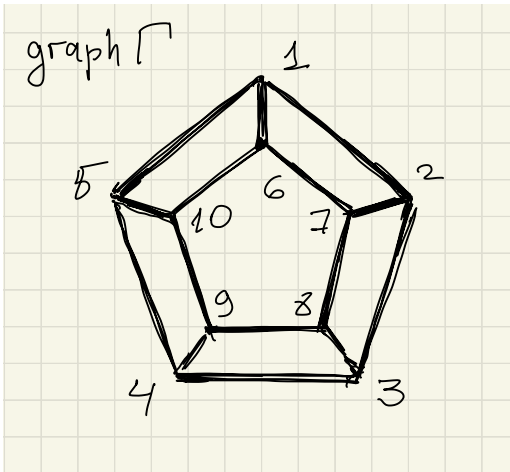
(a) find the order of $\mathrm{Aut}(\Gamma)$;

(b) find some set of generators of $\mathrm{Aut}(\Gamma)$;

(c) prove that $\mathrm{Aut}(\Gamma)$ is transitive and find a point stabilizer;

(d) prove that $\mathrm{Aut}(\Gamma)$ is imprimitive and find all nontrivial blocks.

Solution:



$G = \mathrm{Aut}(\Gamma) \ni (1,2,3,4,5)(6,7,8,9,10)$, $(1,6)(2,7)(3,8)(4,9)(5,10)$, so $1^G = \Omega$. $G_1 = \langle (2,5)(3,4)(7,10)(8,9) \rangle$, therefore $|G| = |1^G| \cdot |G_1| = 10 \cdot |G_1| = 10 \cdot 2 = 20$. The above 3 permutations generate G, so (a), (b), (c) done.

(d) Theorem 2.8 implies that each nontrivial block system Σ_K corresponds to a subgroup K with $G_1 < K < G$. We find such K.

Let $x = (2,5)(3,4)(7,10)(8,9)$, $y = (1,2,3,4,5)(6,7,8,9,10)$, and $z = (1,6)(2,7)(3,8)(4,9)(5,10)$. Then $G = \langle x, y, z \rangle$, $G_1 = \langle x \rangle$.

We have $zx = xz$, $y^x = y^{-1}$, so $K_1 = \langle x, z \rangle$, $K_2 = \langle x, y \rangle \leq G$.

Since $|K_1| = 4$ and $|K_2| = 10$, $G_1 < K_i < G$ for $i = 1, 2$.

Let us prove that there are no other such subgroups.

The element $u = yz = zy = (1,7,3,9,5,6,2,8,4,10)$ has order 10.

Since $u^x = u^{-1}$, $G = \{x^k u^m \mid k = 0,1; m = 0, \ldots, 9\}$.

Let $G \ni w \neq e, x$. Then

$$K = \langle x, w \rangle = \begin{cases} K_1, w = u^5, xu^5, \\ K_2, w = u^2, xu^2, u^4, xu^4, u^6, xu^6, u^8, xu^8, \\ G, \text{ otherwise.} \end{cases}$$

Ex 2: Prove that G isomorphic to the automorphism group of a regular 10-gon, but not permutation isomorphic.

Recall the connection between blocks and subgroups.

Let $G \leq \mathrm{Sym}(\Omega)$ be transitive, Δ a block for G.

1. Δ^x is a block for every $x \in G$,
2. the blocks from $\Sigma = \{\Delta^x \mid x \in G\}$ form a partition of Ω.

The set Σ is called the system of blocks for G, containing Δ.
$G_{\{\Delta\}} = \{x \in G \mid \Delta^x = \Delta\}$ is setwise stabilizer of Δ in G.

Theorem 8. Let G be transitive on Ω, $\Delta \in \Sigma$ a system of blocks.

1. $G_{\{\Delta\}}$ is a subgroup of G, $|\Sigma| = |G : G_{\{\Delta\}}|$.
2. $|\Delta| = |G_{\{\Delta\}} : G_\alpha|$, where $\alpha \in \Delta$.
3. If $G_\alpha \leq K \leq G$, then there is a block system Σ_K such that $K = G_{\{\Delta_K\}}$, where $\alpha \in \Delta_K \in \Sigma_K$.

Let $H = G_1$ and $K = K_1 = G_\Delta$. By Theorem 8, $|\Delta| = |K : H| = 2$.

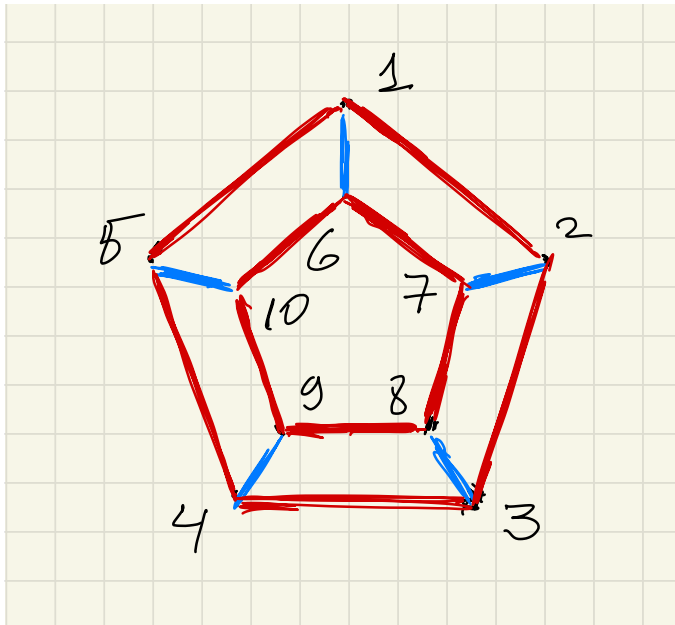
$K = H \cup Hz \implies \Delta = \{1, 6\}$. Thus,

$\Sigma = \{\{1, 6\}, \{2, 7\}, \{3, 8\}, \{4, 9\}, \{5, 10\}\}$.

If $K = K_2 = G_\Delta$, then $|\Delta| = |K : H| = 5$.

$K = H \cup Hy \cup Hy^2 \cup Hy^3 \cup Hy^4 \implies \Delta = \{1, 2, 3, 4, 5\}$. Thus,

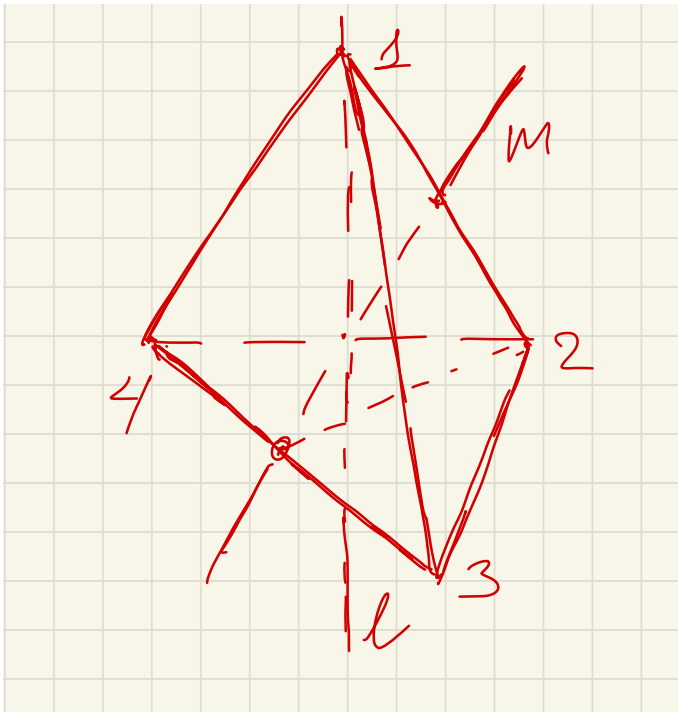
$\Sigma = \{\{1, 2, 3, 4, 5\}, \{6, 7, 8, 9, 10\}\}$.



Problem 6. (a) Find the group of rotations of regular tetrahedron.
(b) How many fundamentally different tetrahedrons with faces painted in 3 colors are there?

Solution: (a) $G = \{e, (1,2)(3,4), (1,3)(2,4), (1,4)(2,3), (1,2,3), (1,3,2), (1,2,4), (1,4,2), (1,3,4), (1,4,3), (2,3,4), (2,4,3)\}$

(b) Ω is the set of different tetrahedrons, $|\Omega| = 3^4$.



e is the identity map, so $|\Omega_e| = 3^4$,

$(2,3,4)$ is the rotation by $120°$ about line l, so $|\Omega_{(2,3,4)}| = 3^2$,

$(1,2)(3,4)$ is the rotation by $180°$ about line m, so $|\Omega_{(1,2)(3,4)}| = 3^2$.

$$t(G) = \frac{1}{|G|}\sum_{x\in G}|\Omega_x| = \frac{(3^4 + 8\cdot 3^2 + 3\cdot 3^2)}{12} = \frac{3^2(9+8+3)}{12} = 15.$$

My research interests in permutation group theory

Graphs $\Gamma = (\Omega, E)$ and $\Gamma' = (\Omega, E')$ are isomorphic, if there is a bijection $f : \Omega \to \Omega'$ such that $E^f = E'$.

One of the most important problem of the modern mathematics is

Graph Isomorphism Problem. Does there exist an effective algorithm to check whether two given finite graphs are isomorphic?

It is tightly connected with the P vs NP-problem, one of the seven Millennium Prize Problems selected by the Clay Mathematics Institute.

Theorem (Laslo Babai, 2016). There is a constant c such that for graphs Γ and Γ' of size n the isomorphism problem can be solved in a quasipolynomial time $\exp(O(\log^c n))$.

Laslo Babai was the invited speaker at the International Congress of Mathematicians, Rio de Janeiro, 2018.

The main problem is does there exist a polynomial time algorithm?

How is it connected with permutation group theory?

It is well known that **GIP** is polynomial time equivalent to

Automorphism Group Problem. Does there exist an effective algorithm to find the automorphism group of a given finite graph?

I am especially interested in this problem for the graphs and other combinatorial structures that naturally grow from groups: orbital graphs and coherent configurations, Cayley graphs and Schur rings.

$G \leq \mathrm{Sym}(\Omega)$ or $G \curvearrowright \Omega$.

Given $k \in \mathbb{N}$, the action of G on Ω induces the action of G on Ω^k:

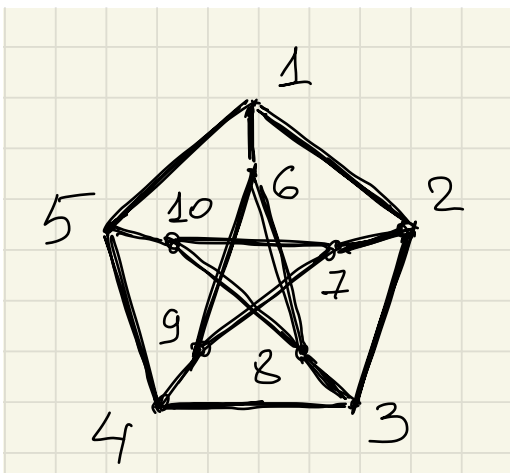
$(\alpha_1, \ldots, \alpha_k)^x = (\alpha_1^x, \ldots, \alpha_k^x)$, for each $x \in G$.

An orbit r of the induced action is called k-orbit.

$\mathrm{Orb}_k(G)$ is the set of k-orbits, $\mathrm{rk}(G) = |\mathrm{Orb}_2(G)|$ is the rank of G.

Any 2-orbit R, also called an orbital, of G is a binary relation on Ω, so $\Gamma = (\Omega, R)$ is a graph, an orbital graph of G on Ω.

If $\mathrm{rk}(G) = 3$ and $R \in \mathrm{Orb}_2(G)$ is one of two irreflexive orbitals, then the orbital graph $\Gamma = (\Omega, R)$ is called graph of rank 3.



Petersen graph $\Gamma = (\Omega, R)$ and its compliment Johnson graph $J(5, 2)$ are orbital graphs of rank 3.

The class of graphs of rank 3 is very important subclass of the class of strongly regular graphs.

Graph Γ is regular (k-regular), if all vertices have the same valency (equal to k).

Graph Γ is strongly regular with parameters (n, k, λ, μ) if it is a k-regular graph on n vertices and the number of common neighbors of two distinct vertices equals λ if they are adjacent and equals μ if they are not.

A. E. Brouwer, A. M. Cohen, A. Neumaier. *Distance-Regular Graphs.* A Series of Modern Surveys in Mathematics. Springer Berlin Heidelberg, 1989.

A. E. Brouwer, H. Van Maldeghem. *Strongly regular graphs.* https://homepages.cwi.nl/ aeb/math/srg/rk3/srgw.pdf

Paradox: The groups of rank 3 are classified. However, the complete description of the automorphism groups of graphs of rank 3 is still an open problem.

The last problem was recently solved for sufficiently large graphs in

S. Skresanov. *On 2-closures of rank 3 groups*, 2020, subm. to Ars Math. Contemporanea, see https://arxiv.org/abs/2007.14696

Problem 1. Describe the automorphism groups of all graphs of rank 3 (i. e. complete this for small graphs).

Problem 2. Describe the automorphism groups of some interesting graphs of small rank (greater than 3).

Problem 3. Describe some interesting classes of permutation groups of small rank (greater than 3).