UNIVERZA NA PRIMORSKEM
Fakulteta za matematiko, naravoslovje in informacijske tehnologije

# Permutacijske grupe

**doc. dr. Ademir Hujdurović**

DRUGO UČNO GRADIVO
47 strani

Matematika, dodiplomski študijski program

PRVA IZDAJA

Koper, 2017

# Contents

# 1 Introduction

This is set of lecture notes on undergraduate course "Permutation groups" at Faculty of Mathematics, Natural Sciences and Information Technologies of University of Primorska, Slovenia. As this is an undergraduate subject, the material gives only introduction to Permutation groups. The material presented in these lecture notes is collected from different sources, books, lecture notes etc.

# 2 Preliminaries

## 2.1 Groups

In this section we review the background on group theory.

**Definition 2.1.** A *group* is a set $G$ together with a binary operation $*$ such that:

(i) for every $a, b \in G$, $a * b \in G$;

(ii) $(\forall a, b, c \in G)$ $a * (b * c) = (a * b) * c$, ($*$ is associative,);

(iii) there exists an *identity element* $e \in G$, such that $x * e = e * x = x$, $\forall x \in G$;

(iv) given identity element $e \in G$, for every element $x \in G$, there exists its *inverse* $x^{-1} \in G$, such that $x * x^{-1} = x^{-1} * x = e$, for all $x \in G$.

If a subset $H \subseteq G$ is also a group with the same binary operation $*$ then we say that $H$ is a *subgroup* of $G$, and we write $H \leq G$.

Identity element in $G$ will sometimes be denoted with $1_G$ or simply by 1. To simplify the notation, we usually write $gh$ instead of $g * h$. We refer to the number $|G|$ of elements in $G$ as the *order* of the group $G$.

If $x*y = y*x$ then we say that $x$ and $y$ *commute*. If every pair of elements in $G$ commutes, then $G$ is said to be *abelian*.

**Exercise 2.2.** Let $G$ be a group and $H \subseteq G$. Prove that $H \leq G$ if and only if the following three conditions hold:

(i) $1_G \in H$;

(ii) $\forall h_1, h_2 \in H$, $h_1 h_2 \in H$;

(iii) $\forall h \in H$, $h^{-1} \in H$.

**Exercise 2.3.** If $H$ and $K$ are subgroups of $G$, then also $H \cap K$ is a subgroup of $G$.

**Definition 2.4.** If $H \leq G$, then the *right coset* of $H$ in $G$ is the set of the form $Hg = \{hg \mid h \in H\}$. Similarly, *left coset* of $H$ in $G$ is the set of the form $gH = \{gh \mid h \in H\}$.

**Exercise 2.5.** If $Hg_1$ and $Hg_2$ are cosets, then either $Hg_1 = Hg_2$ or $Hg_1 \cap Hg_2 = \emptyset$.

Exercise 2.5 implies that $G$ is a disjoint union of right cosets of $H$.

**Definition 2.6.** If $H \leq G$, then the *index* $[G : H]$ of $H$ in $G$ is the number of cosets of $H$ in $G$.

It is now easy to see that for a finite group $G$, $|G| = [G : H]|H|$, and in particular the order of $H$ divides the order of $G$. This is known as *Lagrange's theorem*.

Note that the possible converse of the Lagrange's whould be the following: If $n$ is a divisor of $|G|$, then there exists $H \leq G$ such that $|H| = n$. We will see latter that this does not hold.

If $g$ is an element of a group $G$, the order of $g$ is the least integer $n \geq 1$ such that $g^n = e$, if such $n$ exists, otherwise we say that $g$ is of *infinite* order. In finite group all elements have finite orders.

If $G$ is any group and $S$ is a subset of $G$, then with $\langle S \rangle$ we denote the smallest subgroup of $G$ that contains $S$, and call it the *subgroup generated by* $S$. If $S = \{g_1, g_2, \ldots, g_n\}$ then instead of $\langle \{g_1, g_2, \ldots, g_n \rangle$ we simply write $\langle g_1, g_2, \ldots, g_n \rangle$.

If a group $G$ contains an element $g$ such that $G = \langle g \rangle$, then we say that $G$ is a *cyclic group*.

**Exercise 2.7.** Let $p$ be a prime, and let $G$ be a group of order $p$. Prove that $G$ is cyclic group.

**Definition 2.8.** Let $G$ be a group and let $N \leq G$. If $g^{-1}Ng = N$ for every $g \in G$, then $N$ is said to be a *normal subgroup* of $G$, and we denote this with $N \lhd G$.

**Exercise 2.9.** Prove that the following claims are equivalent:

(i) $N$ is a normal subgroup of $G$;

(ii) $gN = Ng$ for every $g \in G$;

(iii) the set of all left cosets of $N$ in $G$ coincides with the set of all right cosets of $N$ in $G$.

**Exercise 2.10.** Prove that in an abelian group every subgroup is normal.

**Exercise 2.11.** Let $G$ be a group and $H$ an index 2 subgroup of $G$. Prove that $H$ is a normal subgroup of $G$.

**Exercise 2.12.** Let $G$ be a group and $N_1$ and $N_2$ be two normal subgroups of $G$. Prove that $N_1 \cap N_2$ is a normal subgroup of $G$.

Let $G$ be a group and $H, K \leq G$. Let $HK = \{hk \mid h \in H, k \in K\}$. Set $HK$ is not in general a subgroup of $G$.

**Exercise 2.13.** If $H$ and $K$ are subgroups of $G$ then we have that

$$|HK| = \frac{|H||K|}{|H \cap K|}.$$

**Exercise 2.14.** Let $G$ be a group and $H, K \leq G$. If one of $H$ or $K$ is normal in $G$, then $HK$ is a subgroup of $G$.

**Definition 2.15.** If $G$ is a group and $N \lhd G$, then the *factor group* $G/N$ is the group with elements $\{Ng : g \in G\}$ and the group operation $(Ng_1) * (Ng_2) = N(g_1 g_2)$.

If $G$ is a finite group, then $|G/N| = |G|/|N|$.

**Exercise 2.16.** Prove that the factor group defined in Definition 2.15 is indeed a group.

**Definition 2.17.** If $G$ and $H$ are groups, a *homomorphism* $\varphi : G \to H$ is a map $\varphi$ from $G$ to $H$ such that $\forall g_1, g_2 \in G$:

$$\varphi(g_1 *_G g_2) = \varphi(g_1) *_H \varphi(g_2), \tag{1}$$

where $*_G$ is the group operation in $G$ and $*_H$ is the group operation in $H$.

**Exercise 2.18.** Let $\varphi : G \to H$ be a homomorphism and let $K \leq G$. Prove that $\varphi(K) \leq H$.

**Definition 2.19.** Let $\varphi : G \to H$ be a homomorphism and let $e_H$ denote the identity in $H$. *Kernel* $Ker(\varphi)$ of $\varphi$ is defined with $Ker(\varphi) = \{g \mid g \in G, \varphi(g) = e_H\}$.

**Exercise 2.20.** Let $\varphi : G \to H$ be a homomorphism. Prove that $Ker(\varphi) \lhd G$.

**Definition 2.21.** A bijective homomorphism $\varphi : G \to H$ is called *isomorphism*. If there exists an isomorphism between $G$ and $H$ we say that $G$ and $H$ are *isomorphic* and write $G \cong H$.

## 2.2 Cyclic and dihedral groups

Let $n$ be a positive integer. With $C_n$ we will denote a cylic group of order $n$, that is $C_n = \langle a \rangle$, and $a^n = 1$. It can be shown that any two cyclic groups of order $n$ are isomorphic. The following construction gives of cyclic group of order $n$ will be useful later on.

Let $\mathbb{Z}_n = \{0, 1, \ldots, n-1\}$ be the set of residues modulo $n$. Then it is not difficult to see that $\mathbb{Z}_n$ is a group with operation $+_n$, that is addition modulo $n$. Identity element in this group is 0, and $x^{-1} = -x \pmod{n}$. This group is cyclic and of order $n$.

For a positive integer $n$, *dihedral group* $D_{2n}$ is generated by two elements $\rho$ and $\tau$, such that $\rho^n = 1$ and $\tau^2 = 1$. The remaining elements in $D_{2n}$ are given with

$$D_{2n} = \{1, \rho, \ldots, \rho^{n-1}, \tau, \rho\tau, \ldots, \rho^{n-1}\tau\}.$$

The operation in $D_{2n}$ is given with

$$\begin{aligned} \rho^i * \rho^j &= \rho^{i+j}; \\ \rho^i * \rho^j\tau &= \rho^{i+j}\tau; \\ \rho^i\tau * \rho^j &= \rho^{i-j}\tau; \\ \rho^i\tau * \rho^j\tau &= \rho^{i-j}. \end{aligned}$$

Dihedral group $D_{2n}$ is isomorphic to the group of all symmetries of a regular $n$-gon. One step rotation of the $n$-gon corresponds to the element $\rho$, and $\tau$ corresponds to a reflection of the $n$-gon.

## 2.3 Direct and semidirect product of groups

In this section we briefly present methods of constructing new groups from old ones. The first and the simplest method is the direct product of groups.

**Definition 2.22.** Given two group $G_1$ and $G_2$, the *direct product* $G_1 \times G_2$ of $G_1$ and $G_2$ is the group with elements $\{(g_1, g_2) : g_1 \in G_1, g_2 \in G_2\}$ and the group operation is given with $(x_1, x_2) * (y_1, y_2) = (x_1y_1, x_2y_2)$.

**Exercise 2.23.** Prove that $G_1 \times G_2$ as defined above is indeed a group.

**Theorem 2.24.** Let $G$ be a group and let $H$ and $K$ be a subgroups of $G$. Then $G$ is isomorphic to the direct product of $H$ and $K$ if and only if the following three conditions hold:

(i) $H$ and $K$ are normal in $G$;

(ii) $G = HK$;

(iii) $H \cap K = \{1_G\}$.

**Exercise 2.25.** Determine which of the following groups are isomorphic: $\mathbb{Z}_2 \times \mathbb{Z}_3$, $\mathbb{Z}_6$, $\mathbb{Z}_4 \times \mathbb{Z}_2$, $\mathbb{Z}_8$.

A generalization of the notion of direct product is the notion of semidirect product.

**Definition 2.26.** Let $G$ be a group and let $N$ and $K$ be a subgroups of $G$. Then $G$ is *semidirect* product of $N$ and $K$ if and only if the following three conditions hold:

(i) $N$ is a normal subgroup of $G$;

(ii) $G = NK$;

(iii) $N \cap K = \{1_G\}$.

We let $N \rtimes K$ denote the semidirect product of $N$ by $K$.

It is clear that every direct product is also a semidirect product, but semidirect product does not need to be a direct product. To get a better understanding of the structure of a semidirect product we first need to introduce some more terminology.

**Definition 2.27.** If $G$ is a group then an *automorphism* of $G$ is an isomorphism from $G$ to $G$. The set of all automorphisms of a group $G$ is denoted with $Aut(G)$.

**Exercise 2.28.** The set $Aut(G)$ together with the operation of composition of functions is a group.

**Definition 2.29.** Two elements $x$ and $y$ in a group $G$ are said to be conjugate if there exists an element $g \in G$ such that $g^{-1}xg = y$. We often write $g^{-1}xg = x^g$.

We can extend the notion of conjugate elements to the notion of conjugate subgroups. We say that $H$ and $K$ are conjugate subgroups of $G$ if there exists $g \in G$ such that $g^{-1}Hg = K$. Again we will usually write $H^g = g^{-1}Hg$. It is not difficult to see that the relation "is conjugate" is an equivalence relation in $G$. The equivalence classes of this relation are called *conjugacy classes*.

**Exercise 2.30.** If $G$ is a group and $g \in G$, then the mapping $\varphi : G \to G$ defined with $\varphi(x) = x^g$ is an automorphism of $G$.

The automorphisms given in previous exercise are called *inner automorphisms*.

**Exercise 2.31.** The set $Inn(G)$ of all inner automorphisms of $G$ is a normal subgroup of $Aut(G)$.

**Exercise 2.32.** Prove that $N$ is normal subgroup of $G$ if and only if $\varphi(N) = N$ for every $\varphi \in Inn(G)$.

**Definition 2.33.** A subgroup $N$ of a group $G$ is called *characteristic* if $\varphi(N) = N$, for every $\varphi \in Aut(G)$. If $N$ is characteristic subgroup of $G$ we write $N$ *char* $G$.

**Exercise 2.34.** If $N$ *char* $G$ then $N \lhd G$.

An important property of characteristic subgroup is the following:

**Exercise 2.35.** If $G$ is a group and $C$ and $N$ are subgroups of $G$ with $C \leq N \leq G$ such that $C$ *char* $N$ and $N \lhd G$ then $C \lhd G$.

We now go back to the semidirect product of two groups.

**Theorem 2.36.** Let $N$ and $H$ be a groups and $\varphi : H \to Aut(N)$ be a homomorphism. Let $G$ be the set $N \times H$ with operation

$$(n_1, h_1) * (n_2, h_2) = (n_1 \cdot \varphi(h_1^{-1})(n_2), h_1 h_2).$$

Then $G$ is isomorphic to a semidirect product of $N$ by $H$.

*Proof.* We identify $N$ with the set $\{(n, 1_H) \mid n \in N\}$ and $H$ with the set $\{(1_N, h) \mid h \in H\}$. It is now clear that $N \cap H = \{1\}$. We leave as an exercise to the reader to verify that the operation $*$ in $G$ is associative, that $(1_N, 1_H)$ is the identity element in $G$, and that $(n, h)^{-1} = (\varphi(h)(n^{-1}), h^{-1})$.

To see that $N$ is normal in $G$ we observe that

$$\begin{aligned}(n,h)^{-1}(n',1_H)(n,h) &= (\varphi(h)(n^{-1}),h^{-1})(n',1_H)(n,h)\\ &= (\varphi(h)(n^{-1})\varphi(h)(n')),h^{-1})(n,h)\\ &= (\varphi(h)(n^{-1})\varphi(h)(n')\varphi(h)(n),1)\\ &= (\varphi(h)(n^{-1}n'n),1) \in N\end{aligned}$$

It remains to prove that $G = NH$. Let $g \in G$ be arbitrary. Then by the definition of $G$, it follows that $g = (n, h)$ for some $n \in N$ and $h \in H$. It is now easy to see that $g = \overline{n}\overline{h}$, where $\overline{n} = (n, 1)$ and $\overline{h} = (1, h)$. □

We are now going to show how the dihedral group $D_{2n}$ can be constructed as the semidirect product of groups $C_n$ and $C_2$. Let $N = \langle \rho \mid \rho^n = 1 \rangle$ and $H = \langle \tau \mid \tau^2 = 1 \rangle$. In order to construct a semidirect product of groups $N$ and $H$, we need a homomorphism $\varphi : H \to Aut(N)$. Let $\varphi$ be defined with $\varphi(1_H) = id_N$ and $\varphi(\tau) = \iota_N$, where $id_N$ stands for identity map in $N$, that is $id_N(x) = x$ $(\forall x \in N)$ and $\iota_N$ stands for the inversion map in $N$, that is $\iota_N(x) = x^{-1}$ $(\forall x \in N)$.

**Exercise 2.37.** Prove that $\varphi$ defined as above is indeed a homomorphism that maps $H$ to $Aut(N)$.

Now using Theorem 2.36 we construct the group $N \rtimes H \cong C_n \rtimes C_2$. We have that the elements in the group $N \rtimes H$ are given with $N \rtimes H = \{(\rho^i, \tau^k) : i \in \{0, \ldots, n-1\}, k \in 0, 1\}$. The group operation is given with

$$\begin{aligned}(\rho^i,1_H) * (\rho^j,1_H) &= (\rho^i \cdot \varphi(1_H)(\rho^j),1_H) = (\rho^{i+j},1_H)\\ (\rho^i,1_H) * (\rho^j,\tau) &= (\rho^i \cdot \varphi(1_H)(\rho^j),\tau) = (\rho^{i+j},\tau)\\ (\rho^i,\tau) * (\rho^j,1_H) &= (\rho^i \cdot \varphi(\tau)(\rho^j),1_H) = (\rho^{i-j},\tau)\\ (\rho^i,\tau) * (\rho^j,\tau) &= (\rho^i \cdot \varphi(\tau)(\rho^j),1_H) = (\rho^{i-j},1_H)\end{aligned}$$

**Exercise 2.38.** Prove that the mapping $\phi : N \rtimes H \to D_{2n}$ defined with

$$\begin{aligned} \phi((\rho^i, 1_H)) &= \rho^i; \\ \phi((\rho^i, \tau)) &= \rho^i\tau; \end{aligned}$$

is isomorphism.

# 3 Symmetric group $S_n$

Let $X$ be a nonempty set. A bijective mapping $g$ from $X$ to $X$ is also called a *permutation* of $X$. Let $Sym(X)$ denote the set of all permutations of the set $X$. If $X$ has size $n$, then $|Sym(X)| = n!$.

**Exercise 3.1.** Let $*$ be the binary operation on the set $Sym(X)$ defined with

$$\forall g, h \in Sym(X)\ g * h = h \circ g,$$

where $h \circ g$ is the composition of the functions $g$ and $h$, that is $(h \circ g)(x) = h(g(x))$. Prove that $Sym(X)$ together with operation $*$ forms a group.

The definition of the operation $*$ in $Sym(X)$ means that for $g_1, g_2 \in \mathrm{Sym}(X)$ the product $g_1g_2$ is carried out by first applying $g_1$ to $x \in X$ , and then $g_2$ to the image $g_1(x)$, that is **we are multiplying permutations from left to right**.

**In what follows we also write $x^{g_1}$ for the image $g_1(x)$.** Therefore we have $x^{g_1g_2} = \left(x^{g_1}\right)^{g_2}$ for all $x \in X$.

We denote the identity element of $\mathrm{Sym}(X)$ with $\mathrm{id}_X$. Let $x \in X$ and $g \in \mathrm{Sym}(X)$. We say that $x$ is a fix element of $g$, or $x$ is fixed by $g$ if $x^g = x$. Otherwise, we say $x$ is moved by $g$.

**Definition 3.2.** A **permutation group** is any subgroup $G$ of $\mathrm{Sym}(X)$ for some nonempty set $X$.

We say $G$ is a finite permutation group when $X$ is a finite set. In this note we study mostly finite permutation groups, and because of this every set is meant to be finite, unless it is said otherwise.

Notation. We denote by $S_n$ the permutation group $\mathrm{Sym}(\{1, \ldots, n\})$. We write $\mathrm{id}_n$ (or id when $n$ is understood from the context) for $\mathrm{id}_{\{1,\ldots,n\}}$.

There are two common ways in which permutation groups can be written. First is the two line notation for permutations, that was introduced by Cauchy. A permutation $g$ of a set $X = \{x_1, x_2, \ldots, x_n\}$ is written in the following way:

$$g = \begin{pmatrix} x_1 & x_2 & x_3 & \cdots & x_{n-1} & x_n \\ g(x_1) & g(x_2) & g(x_3) & \cdots & g(x_{n-1}) & g(x_n) \end{pmatrix}$$

The other notation is to write $g \in Sym(X)$ as a product of disjoint cycles.

**Definition 3.3.** A permutation $g \in \mathrm{Sym}(X)$ is called a $k$-cycle if there exists distinct elements $x_1, \ldots, x_k$ in $X$ such that $x_k^g = x_1$, and $x_i^g = x_{i+1}$ for all $i \in \{1, \ldots, k-1\}$, and $x^g = x$ for all $x \in X \setminus \{x_1, \ldots, x_k\}$.

Notation. We denote by $(x_1\ x_2\ \dots\ x_k)$ the $k$-cycle $g$ in Definition 3.3.

A 2-cycle is also called a **transposition**. Two cycles $g_1 = (x_1\ \dots\ x_k)$ and $g_2 = (x'_1\ \dots\ x'_l)$ are **disjoint** if $\{x_1, \dots, x_k\} \cap \{x'_1, \dots, x'_l\} = \emptyset$. Note that, this is equivalent to that $g_1 g_2 = g_2 g_1$.

**Example 3.4.** Let $X = \{0, 1, 2, 3, 4, 5, 6\}$ and let $g \in Sym(X)$ be given with $g(x) = 4x + 1 \pmod 7$. Then the permutation $g$ can be written as

$$g = \begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 5 & 2 & 6 & 3 & 0 & 4 \end{pmatrix}$$

or as a product of disjoint cycles $g = (0\ 1\ 5)(2)(6\ 4\ 3) = (6\ 4\ 3)(0\ 1\ 5) = \ldots = (0\ 1\ 5)(3\ 6\ 4)$.

Observe that the order in which the disjoint cycles are written is not important.

**Theorem 3.5.** (**Cyclic Decomposition**) Every permuation $g \in Sym(X)$ can be written as the product of disjoint cycles. Factorization is unique up to the order of factors.

*Proof.* Let $n$ be the size of $X$. The proof is by induction on $n$. It is clear that for $n = 1$ the claim holds. Suppose that the claim holds for every permutation of the set of size $k$, where $1 \leq k \leq n - 1$.

Let $x_1 \in X$, and let $r$ be the least positive integer such that $g^r(x_1) = x_1$. Denote:

$$\begin{aligned} x_2 &= g(x_1), \\ x_3 &= g(x_2) = g^2(x_1), \\ &\dots \\ x_r &= g(x_{r-1}) = g^{r-1}(x_1) \end{aligned}$$

It is easy to see that $x_1, x_2, \dots, x_r$ are distinct elements in $X$. Let $Y = X \setminus \{x_1, \dots, x_r\}$. If $Y = \emptyset$, then $g = (x_1\ x_2 \dots\ x_r)$. On the other hand, if $Y \neq \emptyset$, then for every $y \in Y$, we have $g(y) \in Y$. This means that $g_Y$, the restriction of $g$ to $Y$ is a permutation of the set $Y$. Since $|Y| = |X| - r = n - r \leq n - 1$, we use the induction hypothesis, and conclude that $g_Y$ can be written as the product of disjoint cycles. Let $g_Y = c_2 \dots c_m$ be the cyclic decomposition of $g_Y$ into the product of disjoint cycles. If we denote with $c_1 = (x_1\ x_2 \dots\ x_r)$ then we have $g = c_1 g_Y = c_1 c_2 \dots c_m$, hence $g$ is the product of disjoint cycles.

It remains to prove the uniqueness. Let $g = c_1 c_2 \dots c_m = d_1 d_2 \dots d_k$ where $c_1, \dots c_m$ (resp. $d_1, \dots d_k$) are disjoint cycles of length at least 2. Let $x \in X$. If $x \notin c_i$ $(\forall i)$ then $g(x) = x$, and therefore $x \notin d_i$ $(\forall i)$. If $x \in c_i$ for some $i$, then $g(x) \neq x$. This means that $x \in d_j$ for some $j$. However, in this case $g^r(x) \in c_i$ and $g^r(x) \in d_j$ for every $r \in \mathbb{Z}$. This implies that $c_i$ and $d_j$ are the same cycles.

□

**Corollary 3.6.** Every permutation can be written as the product of transpositions.

*Proof.* It is clear that

$$(a_1\ a_2\ \dots\ a_r) = (a_1\ a_2)(a_1\ a_3) \dots (a_1\ a_r).$$

By Theorem 3.5 it follows that every permutation can be written as a product of disjoint cycles. On the other hand, every cycle can be written as the product of transposition, hence the claim holds. □

**Remark 3.7.** There might be many different ways of writing a permutation as a product of transpositions. For example

$$\begin{aligned}(1\ 2\ 3\ 4\ 5) &= (1\ 5)(2\ 5)(3\ 5)(4\ 5),\\ (1\ 2\ 3\ 4\ 5) &= (1\ 2)(1\ 3)(1\ 4)(1\ 5),\\ (1\ 2\ 3\ 4\ 5) &= (2\ 3)(4\ 5)(3\ 5)(2\ 1)(5\ 3)(1\ 4).\end{aligned}$$

**Theorem 3.8.** Let $g, h \in \mathrm{Sym}(X)$, such that $g$ has as a cyclic decomposition

$$g = (a_1\ \dots\ a_r)\dots(a_s\ \dots\ a_n).$$

Then $h^{-1}gh$ has a cylic decomposition

$$h^{-1}gh = (h(a_1)\ \dots\ h(a_r))\cdots(h(a_s)\ \dots\ h(a_n)).$$

*Proof.* Let $x \in \{1,\dots,n\}$. Then $x = a_i^h$ for some $a_i \in \{1,\dots,n\}$. Then the permutation $(a_1^h,\dots,a_r^h)\cdots(a_s^h,\dots,a_n^h)$ maps $x$ to $a_{i'}^h$, where $i'$ depends only on the cyclic structure $(a_1,\dots,a_r)\cdots(a_s,\dots,a_n)$. Also,

$$x^{h^{-1}gh} = (a_i^h)^{h^{-1}gh} = (a_i^g)^h = a_{i'}^h = x^{(a_1^h,\dots,a_r^h)\cdots(a_s^h,\dots,a_n^h)},$$

and so $h^{-1}gh = (a_1^h,\dots,a_r^h)\cdots(a_s^h,\dots,a_n^h)$. □

We call a cyclic decomposition of $g$ to be **maximal** if it includes all possible 1-cycles. A permutation $g \in \mathrm{Sym}(X)$ has **cyclic structure** $[c_1,\dots,c_n]$ if a maximal cyclic decomposition of $g$ consists of $c_k$ number of $k$-cycles, where $k \in \{1,\dots,n\}$. Note that, the equality $c_1 + 2c_2 + \cdots + nc_n = n$ always holds. The following corollary of Theorem 3.8 is useful when studying the conjugacy of two permutations.

**Corollary 3.9.** The permutations $g_1$ and $g_2$ are conjugate in $\mathrm{Sym}(X)$ if and only if $g_1$ and $g_2$ have the same cyclic structure.

*Proof.* Theorem 3.8 implies that if $g_1$ and $g_2$ are conjugate, then they have the same cyclic structure. Conversely, let $g_1$ and $g_2$ have the same cycle structure. Then $g_1$ and $g_2$ have the cyclic decompositions:

$$\begin{aligned}g_1 &= (a_1\ \dots\ a_r)(a_{r+1}\ \dots a_{r+t})\dots(a_s\ \dots\ a_n)\\ g_2 &= (b_1\ \dots\ b_r)\ (b_{r+1}\ \dots b_{r+t})\dots\ (b_s\ \dots\ b_n)\end{aligned}$$

Define permutation $h \in Sym(X)$ with $h(a_i) = b_i$ $(\forall i \in \{1,\dots,n\})$. It is now easy to see that $h^{-1}g_1h = g_2$ and therefore $g_1$ and $g_2$ are conjugate in $Sym(X)$. □

**Exercise 3.10.** Let $g_1, g_2 \in S_{12}$ be given with their cyclic decompositions:

$$\begin{aligned}g_1 &= (1\ 3\ 5)(2\ 4\ 6)(7)(8\ 12)(9\ 10\ 11)\\ g_2 &= (1)(3\ 2\ 6)(7\ 4\ 5)(9\ 8\ 11)(10\ 12)\end{aligned}$$

Find permutation $h \in S_{12}$ such that $h^{-1}g_1h = g_2$.

## 3.1 Alternating groups $A_n$

In this part we construct a subgroup of $S_n$ of index 2. We saw that any permutation can be written as the product of transpositions. However, the number of transpositions is not uniquely determine. On the other hand, we are now going to prove that the parity of the number of transpositions for a given permutation is fixed.

**Theorem 3.11.** If a permutation $g \in S_n$ can be written as a product of $r$ and $s$ transpositions, then $r \equiv s \pmod 2$.

*Proof.* Let $g = \alpha_1\alpha_2 \dots \alpha_r = \beta_1\beta_2 \dots \beta_s$ be the product of transpositions. Let

$$P = P(x_1, \dots, x_n) = \prod_{i<j}(x_i - x_j)$$

polynomial in $x_1, \dots, x_n$. For $\alpha \in S_n$ define $\alpha(P) = \prod_{i<j}(x_{\alpha(i)} - x_{\alpha(j)})$. We claim that for every transposition $\alpha$ it holds $\alpha(P) = -P$.

Let $\alpha = (k\ l)$ with $k < l$. One of the factors in $P$ is $x_k - x_l$, and its corresponding factor in $\alpha(P)$ is $x_l - x_k$. All the factors of the form $x_i - x_j$ $(i, j \notin \{k, l\})$ remain unchanged in the polynomial $\alpha(P)$. All the remaining factors of $P$ can be written as $\pm(x_i - x_k)(x_i - x_l)$, where the $+$ or $-$ sign depends on the order of integers $i, k, l$. However, each factor of the form $x_i - x_k$ becomes $x_i - x_l$ in $\alpha(P)$, and each factor $x_i - x_l$ becomes $x_i - x_k$ in $\alpha(P)$. This means that the expression $\pm(x_i - x_k)(x_i - x_l)$ remains the same in $\alpha(P)$. Therefore, $\alpha(P) = -P$.

Since $g = \alpha_1\alpha_2 \dots \alpha_r$, it follows that $g(P) = (\alpha_1\alpha_2 \dots \alpha_r)(P) = (-1)^r P$. On the other hand, since $g = \beta_1\beta_2 \dots \beta_s$, it follows that $g(P) = (-1)^s P$. We conclude that $(-1)^r P = (-1)^s P$, hence $r \equiv s \pmod 2$. □

**Definition 3.12.** A permutation $g \in S_n$ is called **even (odd)** if $g$ is the product of even (odd) number of transpositions.

**Exercise 3.13.** Prove that a cycle of length $k$ is even permutation if and only if $k$ is odd.

Notation. We denote by $\mathrm{Alt}(X)$ the subgroup of even permuations in $\mathrm{Sym}(X)$. In the case when $|X| = n$, then we denote by $A_n$ the set all even permuations in $S_n$.

We show below that $A_n, n \geq 2$ is in fact a subgroup of $S_n$ of index 2 . The group $A_n$ is called the **alternating group** of degree $n$.

**Theorem 3.14.** The set $A_n, n \geq 2$ of all even permutations is a subgroup of $S_n$ of index 2.

*Proof.* It is clear that $\mathrm{id} \in A_n$.

Let $g, g' \in A_n$. The group $S_n$ is generated by the set of all transpositions. Thus $g = t_1 \cdots t_r$ and $g' = t'_1 \cdots t'_s$, where $r$ and $s$ are even. Then $gg' = t_1 \cdots t_r t'_1 \cdots t'_s$, $r + s$ is even, and so $gg' \in A_n$. Also, $g^{-1} = t_r \cdots t_1$, and so $g^{-1} \in A_n$. We obtain that $A_n$ is indeed a subgroup of $S_n$. Then $(1, 2) \notin A_n$. It is not difficult to see that the mapping $g \mapsto (1, 2)g$, where $g \in A_n$, is a bijective mapping from $A_n$ to $S_n \setminus A_n$. Thus $|A_n| = n!/2$. □

Note that, since $A_n$ has index 2 in $S_n$, $A_n \triangleleft S_n$.

**Exercise 3.15.** Let $n \geq 2$, and let $H = \{id, (1\ 2)\}$ be a cyclic subgroup of $S_n$ of order 2. Prove that $S_n \cong A_n \rtimes H$.

**Exercise 3.16.** Let $g \in S_n$ be a permutation and let $[c_1, c_2, \ldots, c_n]$ be the cyclic structure of $g$. Prove that $g$ is odd permutation if and only if

$$\sum_{i=1}^{n/2} c_{2i} \equiv 1 \pmod 2.$$

**Exercise 3.17.** Write down all the elements of the groups $A_3$ and $A_4$.

**Exercise 3.18.** Prove that the group $A_n$ ($n \geq 3$) is generated by the set of all cycles of length 3.

**Exercise 3.19.** Prove that $A_4$ has no subgroup of order 6. (Hint: Use Exercises 2.11 and 2.13).

*Proof.* Suppose that $A_4$ has a subgroup $N$ of order 6. Then $N$ is an index 2-subgroup of $A_4$ and by Exercise 2.11 $N$ is normal in $A_4$. Let $V = \{id, (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\}$. Then $V$ is a subgroup of $A_4$ of order 4. Since 4 does not divide 6 and $V$ is not subgroup of $N$, and so $N$ is a proper subgroup of $VN$. This implies that $NV = A_4$. Now, using Exercise 2.13 we obtain

$$|N \cap V| = \frac{|N||V|}{|NV|} = \frac{6 \cdot 4}{12} = 2.$$

Since both $N$ and $V$ are normal in $A_4$, it follows that $N \cap V$ is also a normal subgroup of $A_4$. However, the only subgroups of $A_4$ of order 2 are of the form $\{id, (a\ b)(c\ d)\}$. Let $g = (1\ 2\ 3)$. Then $(1\ 2)(3\ 4)^g = (2\ 3)(1\ 4)$, $(1\ 3)(2\ 4)^g = (2\ 1)(3\ 4)$ and $(1\ 4)(2\ 3)^g = (2\ 4)(3\ 1)$, hence no subgroup of order 2 in $A_4$ is normal. □

# 4 Group actions

In this part we introduce the concept of an action of a group. The motivation behind this concept is to study groups by representing them as permutation groups.

**Definition 4.1.** An **action** of a group $G$ on a set $X$ is a mapping $f\colon X \times G \to X$ such that, writing the image $f((x, g))$ as $x^g$, the following properties hold.

A1. $x^{1_G} = x$ for every $x \in X$.

A2. $x^{g_1 g_2} = (x^{g_1})^{g_2}$ for every $x \in X$ and for every $g_1, g_2 \in G$.

Given an action of a group $G$ on a set $X$, we will also say that $G$ acts on $X$. The cardinality $|X|$ is called the **degree** of the action.

**Example 4.2.** Let $G = \mathbb{R}\backslash\{0\}$ be the group of nonzero real numbers under the multiplication, and let $X$ be the set of all vectors in $\mathbb{R}^3$. Then $G$ acts on $X$ via scalar multiplication, that is $(x_1, x_2, x_3)^g = (gx_1, gx_2, gx_3)$, for $(x_1, x_2, x_3) \in \mathbb{R}^3$ and $g \in \mathbb{R} \setminus \{0\}$.

**Example 4.3.** Let $G \leq Sym(X)$. Then $G$ acts naturally on $X$ with $x^g = g(x)$, for $x \in X$ and $g \in G$.

**Example 4.4.** Let $G$ be the group acting on a set $X$. Then $G$ acts on the set $X \times X$ with $(x_1, x_2)^g = (x_1^g, x_2^g)$.

**Theorem 4.5.** Let $G$ act on $X$ and fix $g \in G$.

(1) The mapping $\pi_g : X \to X$, $\pi_g : x \mapsto x^g$ is in $\mathrm{Sym}(X)$.

(2) The mapping $\rho\colon G \to \mathrm{Sym}(X), \rho : g \mapsto \pi_g$ is a homomorphism.

(3) Let $\Phi : G \to Sym(X)$ be a homomorphism. Then this homomorphism defines action of a group $G$ on the set $X$ with $x^g := \Phi(g)(x) = x^{\Phi(g)}$.

*Proof.* (1): Let $x_1, x_2 \in X$ such that $\pi_g(x_1) = \pi_g(x_2)$. Then $x_1^g = x_2^g$. Axioms A1 and A2 imply $(x_1^g)^{g^{-1}} = x_1^{gg^{-1}} = x_1^{1_G} = x_1$ and $(x_2^g)^{g^{-1}} = x_2^{gg^{-1}} = x_2^{1_G} = x_2$. From these $x_1 = x_2$, and $\pi_g$ is an injective mapping. It follows that $\pi_g$ maps $x^{g^{-1}}$ to $x$, hence $\pi_g$ is also surjective, and by this it is a bijective mapping.

(2): We need to prove that $\rho(g_1g_2) = \rho(g_1)\rho(g_2)$ for every $g_1, g_2 \in G$. It is enough to prove that $\rho(g_1g_2)(x) = (\rho(g_1)\rho(g_2))(x)$, for every $x \in X$. We have that $\rho(g_1g_2) = \pi_{g_1g_2}$, and therefore $\rho(g_1g_2)(x) = \pi_{g_1g_2}(x) = x^{g_1g_2} = (x^{g_1})^{g_2}$. This can be further written as $\left(x^{g_1}\right)^{g_2} = \left(x^{\pi_{g_1}}\right)^{\pi_{g_2}} = x^{\pi_{g_1}\pi_{g_2}}$, and so $\pi_{g_1g_2} = \pi_{g_1}\pi_{g_2}$.

(3): Since $\Phi(1_G) = id_X$, it follows that axiom A1 is satisfied. Since $\Phi$ is homomorphism, it follows that $\Phi(g_1g_2) = \Phi(g_1)\Phi(g_2)$. This implies $x^{g_1g_2} = x^{\Phi(g_1g_2)} = x^{\Phi(g_1)\Phi(g_2)} = (x^{\Phi(g_1)})^{\Phi(g_2)} = (x^{g_1})^{g_2}$.

□

**Definition 4.6.** For an action of a group $G$ on a set $X$ we call the homomorphism $\rho$ in Theorem 4.5 the corresponding **permutation representation of $G$ on $X$**. The **degree** of an action (or a premutation representation) is the size of $X$.

**Definition 4.7.** By the **kernel** and **image** of an action of $G$ on a set $X$ we mean the kernel and image, respectively, of the corresponding permutation representation $\rho$. We say that the action is **faithful** if its kernel is trivial.

We illustrate the above definitions through the following example.

**Example 4.8.** Let $G = D_{12}$ be the group of symmetries of a regular hexagon acting on its points $\{1, 2, 3, 4, 5, 6\}$. Let $d_1 = \overline{14}$, $d_2 = \overline{25}$ and $d_3 = \overline{36}$ be the three main diagonals of the hexagon (order in which the points are written is not important, for example $d_1 = \overline{14} = \overline{41}$). Let $X = \{d_1, d_2, d_3\}$. Prove that $G$ acts on the set $X$ via $\overline{x_1x_2}^g = \overline{x_1^g x_2^g}$. Determine the image and the kernel of this action. Is this action faithful?

Now we jump to a more theorethical example.

**Theorem 4.9.** Let $G$ be a group, and let us take $X$ to be $G$. Then $G$ acts on $X$ with

$$x^g = xg, \quad x, g \in G.$$

This action is faithful.

*Proof.* We show first that we indeed have an action, i.e., the mapping defined above satisfies Axioms A1 and A2.

A1: For every $x \in X$, $x^{1_G} = x1_G = x$.

A2: For every $x \in X$ and for every $g_1, g_2 \in G$, $x^{g_1 g_2} = x(g_1 g_2) = (xg_1)g_2 = (x^{g_1})^{g_2}$.

Let $g \in G$ be in the kernel of the action. This means $x^g = x$ for all $x \in X$. But this just means $xg = x$ for all $x \in X$, hence $g = 1_G$, and the kernel is the trivial group. By definition, the action is faithful. □

**Exercise 4.10.** Prove that a group $G$ acts on $G$ with $x^g = g^{-1}x$, for $x \in G, g \in G$.

The permutation representation corresponding to the action of $G$ in the previous theorem is called the **right regular representation** of $G$. We illustrate the usage of the right regular representation in proving that every group is isomorphic to a permutation group.

**Theorem 4.11** (Cayley)**.** Every group is isomorphic to a permutation group.

*Proof.* Let $G$ be a group. Let $G$ act on $X = G$ via right multiplication. By Theorem 4.5, it follows that $\rho : G \to Sym(X)$ is a group homomorphism (recall that $\rho(g) = \pi_g$, and $\pi_g(x) = xg$ for $x \in G$). Then the image of $G$ under this homomorphism $\rho(G)$ is a subgroup of $Sym(X)$. By the first isomorphism theorem, it follows that $G/Ker(\rho) \cong \rho(G)$. Since by Theorem 4.11 it follows that $Ker(\rho) = \{1_G\}$ it follows that $G \cong \rho(G)$. □

In the following exercise we show how the group actions (that is permutation representations of abstract groups) can be useful in the study of group properties.

**Exercise 4.12.** If $G$ is a group of order $4n + 2$, then $G$ has a subgroup of index 2.

**Proof**. Let $\rho$ be the right regular representation of $G$. As $\rho(G) \cong G$ (because that the action is faithful), it is enough to prove that the image $\rho(G)$ has a subgroup of index 2.

According to Cauchy Theorem $G$ has an element $g$ of order 2. Then $\rho(g) = \pi_g$ has no fix point (each cycle in the cyclic decomposition of $\rho(g)$ is of the form $(x\, xg)$.) Because of this and that $\rho(g)$ is of order 2, we obtain

$$\rho(g) = (g_1, g_2) \cdots (g_{4n+1}, g_{4n+2}),$$

where $g_1, \ldots, g_{4n+2}$ comprise the whole group $G$. As $\rho(g)$ is a product of $2n+1$ transpositions, $\rho(g)$ is an odd permutation in $\mathrm{Sym}(G)$. Therefore, $\mathrm{Alt}(G)\rho(G) = \mathrm{Sym}(G)$. Then

$$|\,\mathrm{Sym}(G)| = |\,\mathrm{Alt}(G)\rho(G)| = \frac{|\,\mathrm{Alt}(G)| \cdot |\rho(G)|}{|\,\mathrm{Alt}(G) \cap \rho(G)|} = \frac{|\,\mathrm{Sym}(G)| \cdot |\rho(G)|}{2 \cdot |\,\mathrm{Alt}(G) \cap \rho(G)|}.$$

From this $\mathrm{Alt}(G) \cap \rho(G)$ is a subgroup of $\rho(G)$ of index 2. ∎

## 4.1 Orbits and stabilizers

In this part we introduce the two most basic concepts in connection with an action – the orbits and the stabiliers.

**Definition 4.13.** Let $G$ act on $X$, and let $x \in X$. The **orbit of $G$ induced by** $x$ is the set $\{x^g \mid g \in G\}$.

Notation. We denote by $x^G$ the orbit of $G$ induced by $x$. We will also sometimes write $Orb_G(x)$ for the orbit of $G$ induced by $x$.

**Definition 4.14.** Let $G$ act on $X$, and let $x \in X$. The **stabilizer of $x$ in $G$** is the set $\{g \in G \mid x^g = x\}$.

Notation. We denote by $G_x$ the stabilizer of $x$ in $G$.

**Example 4.15.** Let $X = \mathbb{Z}_{10} = \{0, 1, \ldots, 9\}$, and let $G = Aut(\mathbb{Z}_{10}) = \mathbb{Z}_{10}^*$ acting naturally on $X$. Calculate the stabilizers $G_0, G_1$, and orbits $0^G, 1^G, 2^G$.

We have the following properties of orbits and stabilizers.

**Theorem 4.16.** Let $G$ act on $X$ and let $x \in X$.

(1) The set of all orbits $x^G$ form a partition of $X$.

(2) The stabilizer $G_x$ is a subgroup of $G$.

*Proof.* (1): Define the relation $\sim$ on $X$ as $x_1 \sim x_2$ if and only if $x_1 = x_2^g$ for some $g \in G$. The relation $\sim$ is an equivalence relation. The class of $\sim$ which contains $x$ is just the orbit $x^G$, and so (1) follows.

(2): It is trivial that $\mathrm{id}_X \in G_x$. Let $g_1, g_2 \in G_x$. Then $x_1^g = x$, $x = x^{g_1^{-1}}$, hence $g_1^{-1} \in G_x$. Also, $x^{g_1 g_2} = (x^{g_1})^{g_2} = x^{g_2} = x$, hence $g_1 g_2 \in G_x$, and (2) follows.

□

**Proposition 4.17.** Let $G$ act on a set $X$, let $g \in G$, $x \in X$ and let $y = x^g$. Then

$$G_y = g^{-1} G_x g.$$

*Proof.*

$$\begin{aligned} G_y &= \{h \in G \mid y^h = y\} \\ &= \{h \in G \mid (x^g)^h = x^g\} \\ &= \{h \in G \mid x^{ghg^{-1}} = x\} \\ &= \{h \in G \mid ghg^{-1} \in G_x\} \\ &= \{h \in G \mid h \in g^{-1} G_x g\} \\ &= g^{-1} G_x g. \end{aligned}$$

□

**Theorem 4.18** (Orbit-stabilizer)**.** Let $G$ be a group acting on a set $X$. Then for every $x \in X$ it holds $|G| = |x^G| \cdot |G_x|$.

*Proof.* Let $x \in X$ be fixed. Define the set $\Omega = \{(g, y) \in G \times x^G \mid x^g = y\}$. We calculate the cardinality of $\Omega$ with "double counting". First, we obtain that

$$|\Omega| = \sum_{g \in G} \big| \{(g, y) \in G \times x^G \mid y = x^g\} \big| = \sum_{g \in G} |\{y \in x^G \mid y = x^g\}| = \sum_{g \in G} 1 = |G|.$$

Second, we obtain that

$$|\Omega| = \sum_{y \in x^G} \big| \{(g, y) \in G \times x^G \mid y = x^g\} \big| = \sum_{y \in x^G} |\{g \in G \mid y = x^g\}|.$$

Let $y \in x^G$ be fixed. Then there exists $h \in G$ such that $y = x^h$. Now we have

$$\{g \in G \mid y = x^g\} = \{g \in G \mid x^h = x^g\} = \{g \in G \mid x^{gh^{-1}} = x\} = \{g \in G \mid gh^{-1} \in G_x\} = (G_x)h.$$

Since $|G_x h| = |G_x|$, it follows that

$$|\Omega| = \sum_{y \in x^G} |G_x| = |x^G| \cdot |G_x|.$$

We conclude that $|\Omega|$ equals $|G| = |x^G| \cdot |G_x|$, as required.

□

**Example 4.19.** The Cube has 48 symmetries.

*Proof.* We identify the vertices of the Cube by the numbers $1, \ldots, 8$ as shown in Figure 1. The

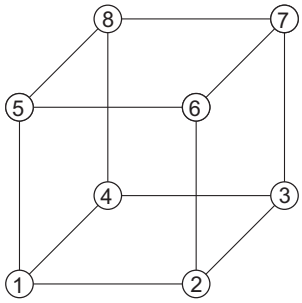


Figure 1: The Cube

group of all symmetries of the Cube acts faithfully on its vertices, i.e., ont the set $\{1, \ldots, 8\}$. Let us denote by $G$ the image of this action. We have $G \leq S_8$, and the required number is the order $|G|$.

We calculate $|G|$ using OSL. Let us consider the orbit of $G$ induced by 1 and the stabilizer of 1 in $G$. According to OSL $|G| = |1^G| \cdot |G_1|$. First, the orbit $1^G = \{1, \ldots, 8\}$. Second, the stabiliser $G_1$ has 6 elements, it is generated by $(2, 5, 4)(3, 6, 8)$ and $(2, 4)(6, 8)$. We obtain $|G| = |1^G| \cdot |G_1| = 8 \cdot 6 = 48$. □

We are now going to present two more important types of group actions. First is the so-called **conjugation action** of $G$ on $G$ defined with

$$x^g = g^{-1}xg, \quad x, g \in G.$$

**Proposition 4.20.** The conjugation action of a group $G$ on $G$ is well-defined group action. For $g \in G$, the orbit $g^G$ is the **conjugacy class of $g$ in $G$**. The stabilizer $G_g$ is the **centralizer** $C_G(g)$ of $g$ in $G$. The kernel of this action is the **center $\mathbf{Z}(G)$** of $G$.

**Exercise 4.21.** Does group $G$ act on $G$ with

$$x^g = gxg^{-1}, \quad x, g \in G?$$

Next important example of group action is the so called coset action. Let $G$ be a group and $H \leq G$. The **coset action** is the action of $G$ on the set of right $H$-cosets in $G$ defined with

$$(Hx)^g = Hxg, \quad x, g \in G.$$

**Proposition 4.22.** The coset action is indeed an action. The stabilizer of $Hx$ is $G_{Hx} = x^{-1}Hx$. The kernel is $\cap_{x \in G} x^{-1}Hx$.

The kernel of the coset action is also called the **core** of $H$ in $G$ (notation: $\mathrm{core}_G(H)$).

**Exercise 4.23.** Prove that $\mathrm{core}_G(H)$ is the largest normal subgroup of $G$ which is contained in $H$.

**Exercise 4.24.** Let $G$ be a $p$-group, that is a group of order $p^k$, where $p$ is a prime. Using the conjugation action, prove that $Z(G)$ the center of $G$, is non-trivial.

**Exercise 4.25.** Let $G$ be a group, $H \leq G$, and let $X = \{gH \mid g \in G\}$ the set of all left cosets of $H$ in $G$. Check if the following are well-defined actions of $G$ on $X$:

1. $(xH)^g = gxH$;
2. $(xH)^g = g^{-1}xH$.

## 4.2 Transitive, semiregular and regular group actions

**Definition 4.26.** Let $G$ act on $X$. The action is **transitive** if it has only one orbits, and it is **semiregular** if $|G_x| = 1$ for all $x \in X$. An action which is both transitive and semiregular is called **regular**.

**Example 4.27.** Right regular representation of $G$, that is the action of $G$ on $G$ given with $x^g = xg$ is regular action.

**Proposition 4.28.** Let $G$ act transitively on $X$. Then cardinality $|X|$ is a divisor of $|G|$.

**Proposition 4.29.** Let $G$ act transitively on $X$. Then $G$ is regular if and only if $|G| = |X|$.

**Proposition 4.30.** Let $G$ be an abelian group which is transitive and faithful on the set $X$. Then $G$ is regular on $X$.

*Proof.* Since $G$ is transitive, it remains to prove that $G$ is semiregular. Suppose that $G$ is not semiregular, that is, there exists $x \in X$, such that $G_x \neq \{1\}$. Since $G$ acts transitively on $X$, then for any $x \in X$ we have $x^G = X$. Using Proposition 4.17 it follows that any two stabilizers are conjugate. However, since $G$ is abelian, it follows that all stabilizers are the same. Then the kernel of this action is equal to $G_x$, which contradicts the assumption that $G$ is faithful. □

**Exercise 4.31.** Let $p$ be a prime, and let $G \leq S_p$ be transitive. Prove that there exists a cyclic subgroup $H$ of $G$, such that $H$ is regular.

**Exercise 4.32.** Let $G$ be a group. Prove that the direct product $G \times G$ acts on $G$ with $x^{(g_1,g_2)} = g_1^{-1}xg_2$. Prove that this action is transitive, and calculate the vertex stabilizer $(G \times G)_1$. When is this action faithful?

**Exercise 4.33.** Let $G$ act transitively on $X$ and let $H \leq G$. Prove that $G = G_xH$ if and only if $H$ is transitive.

# 5 Blocks and primitivity

## 5.1 $G$-invariant partitions

Let a group $G$ act on a set $X$. Group $G$ acts naturally on the set $\mathcal{P}(X)$, of all the subsets of $X$. For every $S \subseteq X$ and for every $g \in G$ we define $S^g = \{x^g \mid x \in S\}$.

**Exercise 5.1.** Prove that $G$ acts on $\mathcal{P}(X)$ with $\forall S \in \mathcal{P}(X), \forall g \in G$; $S^g = \{x^g \mid x \in S\}$. Can this action be transitive?

**Exercise 5.2.** Let $G = D_{12}$ act as the group of symmetries of a regular hexagon $X = \{1, 2, 3, 4, 5, 6\}$. Let $G$ act on $\mathcal{P}(X)$. Calculate orbits $\{1\}^G$, $\{1, 2\}^G$, $\{1, 3, 5\}^G$.

**Definition 5.3.** Let $G$ be a group acting transitively on $X$. A nonempty subset $B \subseteq X$ is called **block** if for each $g \in G$, either $B^g = B$ or $B^g \cap B = \emptyset$.

**Proposition 5.4.** Let $G$ act transitively on $X$. Then for every $x \in X$, the set $\{x\}$ is a block for $G$. Also the whole set $X$ is a block.

*Proof.* Follows directly from the definition. □

Blocks $X$ and $\{x\}$ described in the previous Proposition are called **trivial blocks**. Any other block is called **non-trivial**.

**Exercise 5.5.** Find all non-trivial blocks for the action of $G = D_{12}$ on $X = \{1, 2, 3, 4, 5, 6\}$.

**Exercise 5.6.** If $B$ is a block for $G$, then $B^g$ is also a block, for every $g \in G$.

**Proposition 5.7.** Let $G$ act transitively on $X$, and let $B$ be a block for $G$. Let $\mathcal{B} = \{B^g \mid g \in G\}$. Then $\mathcal{B}$ is a partition of $X$ and $G$ acts transitively on $\mathcal{B}$ with $\forall C \in \mathcal{B}, \forall g \in G$, $g : C \mapsto C^g$.

*Proof.* It is easy to see that $G$ acts on $\mathcal{B}$ and that this action is transitive. Suppose $\mathcal{B}$ is not a partition of $X$. Since $G$ acts transitively on $X$, it follows that for every $x \in X$, there exists $B' \in \mathcal{B}$ with $x \in B'$. Let $B_1, B_2 \in \mathcal{B}$ be such that $B_1 \neq B_2$ and $B_1 \cap B_2 \neq \emptyset$. Then $B_1 = B^{g_1}$ and $B_2 = B^{g_2}$ for some $g_1, g_2 \in G$. Let $x \in B_1 \cap B_2$. Then $x = b_1^{g_1}$ and $x = b_2^{g_2}$ for some $b_1, b_2 \in B$. This implies that $b_1^{g_1} = b_2^{g_2}$, and therefore $b_1^{g_1 g_2^{-1}} = b_2$. This implies that $b_1^{g_1 g_2^{-1}} = b_2 \in B^{g_1 g_2^{-1}} \cap B$ and since $B$ is block it follows that $B^{g_1 g_2^{-1}} = B$. This implies that $B^{g_1} = B^{g_2}$, which contradicts the choice of $B_1$ and $B_2$. We conclude that $\mathcal{B}$ is a partition of $X$. □

**Corollary 5.8.** If $B$ is a block for a transitive permutation group $G$ on $X$, then $|B|$ divides $|X|$.

Partition $\mathcal{B}$ is called **$G$-invariant partition**, or **system of imprimitivity**. The permutation group induced by the action of $G$ on $\mathcal{B}$ is denoted with $G/\mathcal{B}$. With $fix_G(\mathcal{B})$ we denote the kernel of the homomorphism $\rho : G \to Sym(\mathcal{B})$, that is $fix_G(\mathcal{B}) = \{g \in G \mid S^g = S, \forall S \in \mathcal{B}\}$.

**Exercise 5.9.** Prove that $|G| = |G/\mathcal{B}| \cdot |fix_G(\mathcal{B}|$.

**Exercise 5.10.** Let $G = D_{12}$ act on $X = \{1, 2, 3, 4, 5, 6\}$. Let $B = \{1, 4\}$. Prove that $B$ is block for $G$. Calculate $\mathcal{B} = \{B^g \mid g \in G\}$ and $fix_G(\mathcal{B})$. To which group is $G/\mathcal{B}$ isomorphic?

**Exercise 5.11.** Let $G$ be a group acting transitively on $X$, and let $B$ and $C$ be two blocks for $G$. If $B \cap C \neq \emptyset$, then $B \cap C$ is also a block for $G$.

## 5.2 Primitive permutation groups

**Definition 5.12.** Let $G$ act transitively on $X$. If $G$ has only trivial blocks, then we say that $G$ acts **primitively**. If $G$ has also non-trivial blocks, then we say that $G$ acts **imprimitively**.

**Exercise 5.13.** Let $G$ be a finite group, and let $G$ act on $G$ with right multiplication. Find all blocks for this action. When is this action primitive?

**Exercise 5.14.** Can a group $G$ act primitively on some set $X$ and imprimitively on some set $Y$? Hint: Let $G = S_5$ acts on $X = \{1, 2, 3, 4, 5\}$. Prove that $G$ acts primitively on $X$. Consider also the action of $S_5$ on $S_5$ with right multiplication. Is this action primitive?

**Definition 5.15.** Let $G$ act on $X$ and let $A \subseteq X$. Then we define **setwise stabilizer** $G_A = \{g \in G \mid A^g = A\}$ and the **pointwise stabilizer** $G_{(A)} = \{g \in G \mid x^g = x, \forall x \in A\}$.

**Exercise 5.16.** Let $G = S_5$ act on $X = \{1, 2, 3, 4, 5\}$ and let $A = \{1, 2, 4\}$. Calculate $G_A$ and $G_{(A)}$.

**Exercise 5.17.** Let $G$ act transitively on $X$ and let $A \subseteq X$. Prove that both $G_A$ and $G_{(A)}$ are subgroups of $G$, and that $G_{(A)} \lhd G_A$.

**Exercise 5.18.** Let $G$ act transitively on $X$ and let $B$ be a block for $G$. Prove that $G_B$ acts transitively on $B$.

When considering blocks, it is natural to think about methods of constructing all possible blocks for a given group action. The following theorem gives a method of constructing blocks. We will see later that every block can be constructed in such a way.

**Theorem 5.19.** Let $G$ be a group acting transitively on $X$, and let $x \in X$. Let $H$ be a subgroup of $G$ such that $G_x \leq H \leq G$ and let $B = x^H$. Then $B$ is a block for $G$.

*Proof.* Suppose that $B = x^H$ is not a block, that is there exists $g \in G$ such that $B^g \neq B$ and $B^g \cap B \neq \emptyset$. Let $y \in B \cap B^g$. Since $y \in B$ it follows that $y = x^{h_1}$ for some $h_1 \in H$. Since $y \in B^g$ it follows that $y = (x^{h_2})^g$ for some $h_2 \in H$. This implies that $y = x^{h_1} = (x^{h_2})^g$ and therefore $x = x^{h_2 g h_1^{-1}}$. This implies that $h_2 g h_1^{-1} \in G_x \leq H$, and therefore $h_2 g h_1^{-1} \in H$. Since $h_1, h_2 \in H$ it follows that $g \in H$. But then $B^g = \{(x^h)^g \mid h \in H\} = \{x^{h'} \mid h' \in H\} = B$. This contradicts the choice of $B$. The obtained contradiction shows that $B$ is a block for $G$. □

We saw in the previous theorem how we can construct blocks for $G$ that contain $x$. Next we show that every block for $G$ can be constructed in such a way.

**Theorem 5.20.** Let $G$ be a transitive group on $X$ and let $B$ be a block for $G$. Let $x \in B$. Then there exists $H$ such that $G_x \leq H \leq G$ and $B = x^H$.

*Proof.* Let $H = G_B$. Then $H$ is a subgroup of $G$. To see that $G_x \leq H$ let $g \in G_x$. Then $x^g = x$, and therefore $x \in B \cap B^g$. Since $B$ is a block for $G$ it follows that $B = B^g$. Therefore $g \in G_B = H$. Since $H = G_B$ acts transitively on $B$, and $x \in B$ it follows that $B = x^H$. □

**Corollary 5.21.** Let $G$ be a transitive group on a set $X$ with at least two points. Then $G$ is primitive if and only if every stabilizer $G_x$ is a maximal subgroup of $G$.

Previous two theorems give us a method of constructing all blocks for transitive action of a group $G$. However, in order to apply it, one needs to find all subgroups $H$ such that $G_x \leq H \leq G$, which usually is not a simple task. A possible way how to avoid finding all subgroups $H$ lying between $G_x$ and $G$ is the following.

**Proposition 5.22.** Let $G$ be a group acting transitively on $X$ and let $x \in X$. Let $\{x\}, O_1, \ldots, O_k$ be the orbits of $G_x$ on $X$. Let $B$ be a block for $G$ that contains $x$. Then $B = \{x\} \cup_{j \in J} O_j$ for some subset $J \subseteq \{1, \ldots, k\}$.

*Proof.* Let $B$ be a block for $G$ and let $x \in B$. Then $B = x^H$ where $G_x$ is a subgroup of $H$. Then every orbit of $H$ is a union of orbits of $G_x$. Hence the result follows. □

Observe that the claim in the last proposition holds only in one direction, that is, every block for $G$ that contains $x$ is a union of orbits of $G_x$. But it is not true that every union of orbits of $G_x$ is a block for $G$.

**Exercise 5.23.** Let $G = D_{12}$ acting on $X = \{1, 2, 3, 4, 5, 6\}$. Then $G_3 = \{id, (2\ 4)(1\ 5)\}$. Orbits of $G_3$ are $\{3\}$, $O_1 = \{1, 5\}$, $O_2 = \{2, 4\}$ and $O_3 = \{6\}$. Then $B = \{3\} \cup O_2$ is not a block for $G$.

**Exercise 5.24.** Let $G \leq H \leq Sym(X)$. If $G$ is primitive then $H$ is primitive.

*Proof.* Let $G$ be primitive and suppose that $H$ is not primitive, that is there exits a non-trivial block $B \subset X$ for $H$. This means that $B^h = B$ or $B^h \cap B = \emptyset$ for every $h \in H$. Since $G \leq H$, it follows that $B^g = B$ or $B^g \cap B = \emptyset$, for every $g \in G$. This means that $B$ is a block for $G$, contradicting the assumption that $G$ is primitive. □

**Exercise 5.25.** Find transitive permutation groups $G$ and $H$ such that $G \leq H \leq Sym(X)$ such that $H$ is primitive and $G$ is not primitive.
Hint: Take $H = S_4$, and $G = \langle (1\ 2\ 3\ 4) \rangle$.

## 5.3 Quasiprimitive permutation groups

We begin this section with the following important theorem, which gives us a common way of construction $G$-invariant partitions.

**Theorem 5.26.** Let $G \leq Sym(X)$ be transitive. If $N \lhd G$, then the orbits of $N$ form a $G$-invariant partition of $X$.

*Proof.* Let $x \in X$, and let $B = x^N = \{x^n \mid n \in N\}$, be the orbit of $N$ that contains $x$. We claim that $B$ is a block for $G$. Suppose that $B^g \cap B \neq \emptyset$ for some $g \in G$. Let $y \in B^g \cap B$. This implies that $y = x^{n_1}$ and $y = x^{n_2 g}$ for some $n_1, n_2 \in N$. It follows that $x^{n_1} = x^{n_2 g}$ and therefore $x = x^{n_1 g^{-1} n_2^{-1}}$. Observe that since $N \lhd G$, it follows that $Ng = gN$, and hence $ng = gn'$ for some $n' \in N$. We now have

$$B^g = \{x^n \mid n \in N\}^g = \{x^{ng} \mid n \in N\} = \{x^{gn'} \mid n' \in N\} = \{(x^{n_1 g^{-1} n_2^{-1}})^{gn'} \mid n' \in N\}.$$

Since $N$ is normal in $G$ it follows that $n_1 g^{-1} n_2^{-1} g = n_1 (g^{-1} n_2^{-1} g) = n_3 \in N$. Therefore,

$$B^g = \{(x^{(n_1 g^{-1} n_2^{-1} g) n'} \mid n' \in N\} = \{x^{n_3 n'} \mid n' \in N\} = \{x^{n''} \mid n'' \in N\} = B.$$

This shows that $B$ is a block for $G$ and concludes the proof. □

Transitive groups without any nontrivial blocks formed as the orbits of normal subgroups are called quasiprimitive groups.

**Definition 5.27.** Let $G$ be a transitive permutation group on a set $X$. Then $G$ is said to be **quasiprimitive** if every normal subgroup $N$ of $G$ is transitive on $X$.

**Remark 5.28.** If we talk about a group $G$ acting transitively on set $X$, then we say that $G$ is quasiprimitive if every normal subgroup of $G$ is transitive, or is contained in the kernel of the action.

**Corollary 5.29.** Every primitive group is quasiprimitive.

The converse of the above corollary does not hold, as shown by the following example.

**Exercise 5.30.** Group $S_5$ is quasiprmitive in its action on the conjugacy class $(1\ 2)(3\ 4)^{S_5}$. Prove that it is not primitive.

**Exercise 5.31.** Let $n \geq 5$ and let $A_n$ act on itself by right multiplication. Is this action quasiprimitive? Is it primitive?

**Theorem 5.32.** Let $G \leq Sym(X)$ be transitive and let $\mathcal{B}$ be a $G$-invariant partition. If there exists $H \leq G$, such that $\mathcal{B}$ is formed by the orbits of $H$, then there exists a normal subgroup $N \lhd G$, such that $\mathcal{B}$ is formed by the orbits of $N$.

*Proof.* Let $G \leq Sym(X)$ be transitive, and let $\mathcal{B}$ be a $G$-invariant partition formed by the orbits of $H \leq G$. This means that $\mathcal{B} = \{x^H \mid x \in X\}$. Let $N = fix_G(\mathcal{B})$. Since $N$ is the kernel of the homomorphism $\rho : G \to Sym(\mathcal{B})$ it follows that $N \lhd G$. Observe that $H \leq N$. Since $H$ acts transitively on every $B \in \mathcal{B}$ it follows that $N$ also acts transitively on every $B \in \mathcal{B}$. This implies that $x^H = x^N$, for every $x \in X$. Hence, $\mathcal{B}$ is formed by the orbits of $N$. □

**Theorem 5.33.** Let $G \leq Sym(X)$ be transitive and suppose that there exists an abelian regular subgroup $H$ of $G$. Then any $G$-invariant partition is formed by the orbits of a normal subgroup of $G$, and is also formed by the orbits of a subgroup of $H$.

*Proof.* Let $\mathcal{B}$ be a $G$-invariant partition. Then $\mathcal{B}$ is also an $H$-invariant partition. Since $H$ is regular and abelian, it follows that $\mathcal{B}$ is formed by the orbits of $H_1 \leq H$ (see exercise below). Now, since $H_1 \leq H \leq G$, using Theorem 5.32, it follows that $\mathcal{B}$ is formed by the orbits of a normal subgroup $N \lhd G$. This concludes the proof. □

**Exercise 5.34.** Let $H$ be abelian group acting regularly on $X$, and let $\mathcal{B}$ be an $H$-invariant partition. Prove that there exists $H_1 \leq H$ such that $\mathcal{B}$ is formed by the orbits of $H_1$. Does the same result hold if $H$ is not abelian? (see Exercise 5.36)

**Exercise 5.35.** Let $G \leq Sym(X)$ be transitive, and let $\mathcal{B}$ be a $G$-invariant partition such that $\mathcal{B}$ consists of precisely two blocks. Prove that $\mathcal{B}$ is formed by the orbits of a normal subgroup $N \lhd G$. Does the same result hold if there are 3 blocks? (see Exercise 5.36)

*Proof.* Hint: Define $N = fix_G(\mathcal{B})$. Prove that $\mathcal{B}$ is formed by the orbits of $N$. □

**Exercise 5.36.** Let $G = S_3$ acting on set $X = \{(1,2),(2,1),(1,3),(3,1),(2,3),(3,2)\}$ with $(x,y)^g = (x^g, y^g)$. Prove that $G$ acts regularly on $X$. Prove that the set $B = \{(1,2),(2,1)\}$ is block for $G$. Determine $\mathcal{B} = \{B^g \mid g \in G\}$. Determine $fix_G(\mathcal{B})$. Prove that $\mathcal{B}$ is not formed by the orbits of a subgroup of $G$.

**Exercise 5.37.** Let $G$ be a transitive permutation group on set $X$ with $|X| = mp^k$, where $gcd(m,p) = 1$. Let $N$ be a Sylow $p$-subgroup of $G$. Prove that $p^k$ divides the size of every orbit of $N$.

*Proof.* Let $P$ be a Sylow $p$-subgroup of $G$. Then $|P|$ is divisible by $p^k$ and $|G|/|P|$ is not divisible by $p$. Now use orbit-stabilizer property for $G$ and $P$, and we have

$$|G| = |G_x||x^G| = |G_x||mp^k| \quad (2)$$
$$|P| = |P_x||x^P| \quad (3)$$

Now dividing (2) with (3) we obtain

$$\frac{|G|}{|P|} = \frac{|G_x|}{|P_x|}\frac{mp^k}{|x^P|}.$$

Therefore, $|x^P|\frac{|G|}{|P|} = mp^k\frac{|G_x|}{|P_x|}$. Since $P_x \leq G_x$ and $\frac{|G|}{|P|}$ is not divisible by $p$ it follows that $|x^P|$ is divisible by $p^k$. This concludes the proof. □

**Exercise 5.38.** Let $G$ be a transitive permutation group on a set $X$ with $X = mp$, where $m < p$. Suppose that $\mathcal{B}$ is a $G$-invariant partition with $m$ blocks of size $p$. Prove that there exists a normal subgroup $N \lhd G$ such that $\mathcal{B}$ is formed by the orbits of $N$.

*Proof.* Let $P$ be a Sylow $p$-subgroup of $G$ and let $N = fix_G(\mathcal{B})$. It follows that $|G| = |G/\mathcal{B}| \cdot |fix_G(\mathcal{B}| = |G/\mathcal{B}| \cdot |N|$. Observe that $|G/\mathcal{B}| \leq S_m$, hence $|G/\mathcal{B}|$ is not divisible by $p$ (since $m < p$). We claim that $P \leq N$. Let $\rho : G \to Sym(\mathcal{B})$ be the homomorphism that corresponds to the action of $G$ on $\mathcal{B}$. Then $\rho(g) \in G/\mathcal{B}$. Since $\rho$ is homomorphism, it follows

that the order of element $\rho(g)$ in $Sym(\mathcal{B})$ divides the order of $g$. This implies that the order of $\rho(g)$ is 1, and hence $\rho(g) = id$, which means that $g \in fix_G(\mathcal{B})$. This proves that $P \leq N$. Since by the previous exercise, orbits of $P$ must be divisible by $P$, it follows that orbits of $N$ must be divisible by $P$, hence $\mathcal{B}$ is formed by the orbits of $N$. □

# 6 Permutation isomorphic and permutation equivalent

**Definition 6.1.** Let $G \leq Sym(X)$ and $H \leq Sym(Y)$. Then $G$ and $H$ are **permutation isomorphic** if there exists a bijection $f : X \to Y$ and a group isomorphism $\varphi : G \to H$ such that $f(x^g) = (f(x))^{\varphi(g)}$ for all $x \in X$ and $g \in G$.

**Theorem 6.2.** Let $G, H \leq Sym(X)$. Then $G$ and $H$ are permutation isomorphic if and only if $G$ and $H$ are conjugate in $Sym(X)$.

*Proof.* Suppose that $G$ and $H$ are conjugate in $Sym(X)$. Let $f \in Sym(X)$ be such that $f^{-1}Gf = H$. Then it is clear that $f : X \to X$ is a bijection. Let $\varphi : G \to H$ be defined with $\varphi : g \mapsto f^{-1}gf$. Then $\varphi$ is isomorphism. It remains to verify that $f(x^g) = (f(x))^{\varphi(g)}$ for all $x \in X$ and $g \in G$. We leave the details for the reader.

Suppose now that $G, H \leq Sym(X)$ are permutation isomorphic. Then there exists bijection $f : X \to X$ and a group isomorphism $\varphi : G \to H$ such that $f(x^g) = (f(x))^{\varphi(g)}$ for all $x \in X$ and $g \in G$. Then $f \in Sym(X)$. We claim that $f^{-1}Gf = H$. Observe that for any $x \in X$ it holds $x^{gf} = f(x^g) = (f(x))^{\varphi(g)} = x^{f\varphi(g)}$. Therefore $gf = f\varphi(g)$ and hence $f^{-1}gf = \varphi(g) \in H$. It is now easy to conclude that $f^{-1}Gf = H$, as claimed. □

**Theorem 6.3.** Let $G$ be a transitive group acting on $X$ with $G$-invariant partition $\mathcal{B}$. Then the action of $G_B$ on $B$ and the action of $G_{B'}$ on $B'$ are permutation isomorphic, for any two $B, B' \in \mathcal{B}$. Additionally, the action of $fix_G(\mathcal{B})$ on $B$ is permutation isomorphic to the action of $fix_G(\mathcal{B})$ on $B'$.

*Proof.* Let $h \in G$ be such that $B^h = B'$. Define $f : B \to B'$ with $f(x) = x^h$. Then $f$ is bijection. Define $\varphi : G_B \to G_{B'}$ with $\varphi(g) = h^{-1}gh$. □

**Definition 6.4.** Let $G$ be a permutation group acting on sets $X$ and $Y$. The action of $G$ on $X$ is **permutation equivalent** with the action of $G$ on $Y$ if there exists bijective mapping $f : X \to Y$ such that $f(x^g) = (f(x))^g$ for every $x \in X$ and every $g \in G$.

**Proposition 6.5.** Let the action of $G$ on sets $X$ and $Y$ be permutation equivalent. Then these two actions are also permutation isomorphic.

**Theorem 6.6.** Suppose that the group $G$ acts transitively on the two sets $X$ and $Y$, and let $H$ be a stabilizer of a point in the first action. Then the actions are permutation equivalent $\Leftrightarrow$ $H$ is the stabilizer of some point in the second action.

*Proof.* Suppose first that the actions of $G$ on $X$ and $Y$ are permutation equivalent, and let $H = G_{x_0}$ from some $x_0 \in X$. Then there exists bijection $f : X \to Y$ such that $f(x^g) = (f(x))^g$ for every $x \in X$ and every $g \in G$. Let $y_0 = f(x_0)$. It is now straightforward to see that $H = G_{y_0}$.

Suppose now that there exist $x_0 \in X$ and $y_0 \in Y$ such that $G_{x_0} = G_{y_0}$. We claim that $f$ given with

$$f(x_0^g) = y_0^g,$$

is bijective mapping from $X$ to $Y$. We first need to prove that $f$ is well-defined. Let $x_0^{g_1} = x_0^{g_2}$. This implies that $g_1 g_2^{-1} \in G_{x_0} = G_{y_0}$ and therefore $y_0^{g_1} = y_0^{g_2}$. This shows that the values $f(x_0^{g_1})$ and $f(x_0^{g_2})$ are the same, hence $f$ is well-defined mapping. Since $G$ acts transitively on $Y$ it follows that the mapping $f$ is surjective. It is also not difficult to see that $f$ is injective, hence $f : X \to Y$ is bijective mapping.

Finally, let $x \in X$ and $g \in G$ be arbitrary. It remains to prove that $f(x^g) = (f(x))^g$. Since $G$ is transitive on $X$, it follows that there exists $g_0 \in G$ such that $x_0^{g_0} = x$. Now

$$f(x^g) = f((x_0^{g_0})^g) = f(x_0^{g_0 g}) = y_0^{g_0 g} = (y_0^{g_0})^g = f(x_0^{g_0})^g = f(x)^g,$$

which concludes the proof. □

**Corollary 6.7.** Any two regular actions of a group $G$ are permutation equivalent.

**Theorem 6.8.** Let $G$ act transitively on $X$. Then this action is permutation equivalent with the action of $G$ on the right cosets of $G_x$ in $G$, for any $x \in X$.

*Proof.* Let $G$ act transitively on $X$, and let $G_x$ be the stabilizer of some $x \in X$. Consider the action of $G$ on the cosets of $H = G_x$. This action is transitive. Let $g \in G_H$ the stabilizer of coset $H$. Then $Hg = H$. This means that $g \in H$. Hence $G_H = H$. Using Theorem 6.6 the result follows. □

**Theorem 6.9.** Let $G$ be a group and $H, K \leq G$. Prove that the actions of $G$ on the cosets of $H$ and $K$ are permutation equivalent if and only if $H$ and $K$ are conjugate subgroups in $G$, or equivalently, there exists $\alpha \in Inn(G)$ such that $\alpha(H) = K$.

*Proof.* Suppose first that $H$ and $K$ are conjugate subgroups in $G$. Then $H = g^{-1}Kg$ for some $g \in G$. Now the stabilizer of $H$ in the action of $G$ on cosets of $H$ is $G_H = H$, and the stabilizer of $K$ in the action of $G$ on the cosets of $K$ is $G_K = K$. Recall that by Proposition 4.17, stabilizer of coset $K^g = Kg$ is $G_{Kg} = g^{-1}G_K g = g^{-1}Kg = H = G_H$. We conclude that the stabilizer of point $H$ in first action is equal to the stabilizer of point $Kg$ in the second action, hence by Theorem 6.6 the two actions are permutation equivalent.

Suppose now that the actions of $G$ on cosets of $H$ and $K$ are permutation equivalent. Then by Theorem 6.6, it follows that the stabilizer $G_H$ is equal to the stabilizer $G_{Kg}$ for some coset $Kg$ of $K$ in $G$. It is clear that $G_H = H$. Let $a \in G_{Kg}$. Then $Kga = Kg$. This is equivalent with $gag^{-1} \in K$, and therefore $a \in g^{-1}Kg$. We conclude that $G_{Kg} = g^{-1}Kg$. Therefore, $H = g^{-1}Kg$, for some $g \in G$. Hence $H$ and $K$ are conjugate subgroups of $G$. This concludes the proof. □

**Theorem 6.10.** Let $G$ be a group and $H, K \leq G$. Prove that the actions of $G$ on the cosets of $H$ and $K$ are permutation isomorphic if and only if there exists $\varphi \in Aut(G)$ such that $\varphi(H) = K$.

*Proof.* Suppose that the two actions are permutation isomorphic. Then there exists a bijective mapping $f$ from cosets of $H$ to the cosets of $K$, and group automorphism $\alpha \in Aut(G)$, such that $f((Hx)^g) = (f(Hx))^{\alpha(g)}$ for all $x \in G$ and $g \in G$. Then $f(H) = Kx_0$ for some $x_0 \in G$. Now choosing $x = 1_G$ and $g = h \in H$ we obtain $f(H) = (f(H))^{\alpha(h)}$. Hence $\alpha(h) \in G_{Kx_0} = x_0^{-1}Kx_0$ for every $h \in H$, that is $\alpha(H) \subseteq x_0^{-1}Kx_0$. From it can be seen that $\alpha(H) = x_0^{-1}Kx_0$. Since conjugation by $x_0$ is an automorphism of $G$, it follows that $\exists \varphi \in Aut(G)$ such that $\varphi(H) = K$.

Suppose now that there exists $\varphi \in Aut(G)$ such that $\varphi(H) = K$. For $x \in G$ let

$$f(Hx) = K\varphi(x).$$

We claim that $f$ is bijection from right cosets of $H$ into the right cosets of $K$. First we need to establish that $f$ is well-defined mapping. Suppose that $Hx = Hy$. Then $xy^{-1} \in H$ and hence $\varphi(xy^{-1}) \in K$. This implies that $K\varphi(x) = K\varphi(y)$, hence $f$ is well-defined. Similarly we see that $f$ is bijective.

It remains to prove that $f((Hx)^g) = (f(Hx))^{\varphi(g)}$ for all $x \in G$ and $g \in G$. We have

$$f((Hx)^g) = f(Hxg) = K\varphi(x)\varphi(g) = (K\varphi(x))^{\varphi(g)} = (f(Hx)^{\varphi(g)}),$$

proving our claim. □

**Corollary 6.11.** Let $G$ be a group and $H \leq G$, $\alpha \in Aut(G)$ such that $\alpha(H)$ is not conjugate to $H$ in $G$. Then the action on right cosets of $H$ and $K = \alpha(H)$ are permutation isomorphic but not permutation equivalent actions.

Theoretically, we can now determine all transitive and faithful permutation representations of a group $G$ up to either permutation isomorphism or equivalence. First we would need to determine all core-free subgroups $H$ of $G$, as a faithful transitive permutation representation of $G$ is the right coset action of $G$ on a core-free subgroup. Inequivalent permutation representations on the list can be identified using the outer automorphisms of $G$.

**Example 6.12.** Let $G = S_3$. The complete set of representatives of the conjugacy classes of subgroups of $G$ is given by $\{id\}$, $\langle(1\ 2)\rangle$, $\langle(1\ 2\ 3)\rangle$ and $S_3$. This gives us transitive representations of $S_3$ of degree 6, 3, 2 and 1 (degree equals the index of a subgroup). The first two actions are faithful.

**Exercise 6.13.** Consider the action of $G = S_3$ on set $X = \{(1,2),(2,1),(1,3),(3,1),(2,3),(3,2)\}$ with $(x,y)^g = (x^g, y^g)$. Consider also the action of $S_3$ on itself by right multiplication. Are these two actions permutation isomorphic and permutation equivalent?

**Exercise 6.14.** Find up to equivalence all transitive actions of $S_4$.

**Example 6.15.** Let $G = S_6$ and let $H = \{g \in G \mid 6^g = 6\}$. It is clear that $H \leq G$ and that $H \cong S_5$. Let $X$ be the set of all Sylow 5-subgroups of $H$. Observe that there are exactly 6 Sylow 5-subgroups in $S_5$, hence $X = \{P_1, P_2, P_3, P_4, P_5, P_6\}$. Let group $G$ (and also $H \leq G$) act on the set $X$ by conjugation. Since all Sylow $p$-subgroups are conjugate, it follows that $H$ acts transitively (and consequently also $G$ acts transitively). Let $\rho$ be the permutation representation of this action, that is $\rho : G \to Sym(X)$ be the corresponding homomorphism.

We claim that this action is faithful. Let $T$ be the kernel of this action, that is $T = \{g \in G \mid \rho(g) = id_X\}$. Then $T$ is normal subgroup of $G \cong S_6$. It is now not difficult to prove that $T = \{1_G\}$. Namely, let $P_1 = \langle(1\ 2\ 3\ 4\ 5)\rangle$. If $g \in T$, then $P_1^g = P_1$, hence $(1\ 2\ 3\ 4\ 5)^g = (1\ 2\ 3\ 4\ 5)^k$, for some $k \in \{1, 2, 3, 4, \}$. It is now not difficult to see that this implies $g \in P_1$. Hence $T \leq \cap_{i=1}^6 P_i = \{1_G\}$. Therefore $\rho : G \to S_6$ is injective homomorphism, hence isomorphism. (We can think of $\rho$ as of the outer automorphism of $S_6$). Now $\rho(H)$ is also a subgroup of $S_6$, and $\rho(H) \cong S_5$. Observe that $H$ and $\rho(H)$ are not conjugate subgroups in $S_6$. Hence, the actions of $G$ on cosets of $H$ and $\rho(H)$ are permutation isomorphic, but are not permutation equivalent.

# 7 Counting orbits

**Definition 7.1.** Let $G$ be a group acting on a set $X$, and let $g \in G$. Then with $fix_X(g)$ we denote the set of elements of $X$ fixed by $g$, that is $fix_X(g) = \{x \in X \mid x^g = x\}$. When the set $X$ is clear from the context we simply write $fix(g)$.

There is a simple relationship between the number of orbits of a finite group acting on a finite set and the number of fixed points of its elements. A wide range of applications in counting problems and combinatorics is based on elaborations of this relationship. The theorem itself has a long history and is often referred to (inaccurately) as the "Burnside Lemma"; the simplest version is the following result.

**Theorem 7.2** (Cauchy-Frobenius)**.** Let $G$ be a finite group acting on a finite set $X$, and let $m$ be the number of orbits in this action. Then

$$m = \frac{1}{|G|} \sum_{g \in G} fix(g).$$

*Proof.* Define the set $\Omega = \{(x, g) \in X \times G \mid x^g = x\}$. We are going to count the number of elements of $\Omega$ in two different ways. First suppose that the orbits of $G$ are $X_1, \ldots, X_m$. Then we have

$$|\Omega| = \sum_{i=1}^{m} |\{(x, g) \in X_i \times G \mid x^g = x\}|. \tag{4}$$

Suppose that $x \in X_i$ is arbitrary. Then $\{(x, g) \in X_i \times G \mid x^g = x\} = \{x_i\} \times G_x$. Recall that by orbit-stabilizer property, we have $|G_x||X_i| = |G|$. Hence we have

$$|\Omega| = \sum_{i=1}^{m} \sum_{x \in X_i} |G_x| = \sum_{i=1}^{m} \sum_{x \in X_i} \frac{|G|}{|X_i|} = \sum_{i=1}^{m} |G| = m|G|. \tag{5}$$

On the other hand we have

$$|\Omega| = \sum_{g \in G} |\{(x, g) \in X \times G \mid x^g = x\}| = \sum_{g \in G} |fix(g)|. \tag{6}$$

Combining (5) and (6) the result follows. □

**Corollary 7.3.** If $G$ is a finite transitive permutation group of degree $n > 1$ then $G$ contains an element with no fixed points.

*Proof.* Since $G$ acts transitively, we have that the number of orbits is $m = 1$. Then by Cauchy-Frobenius theorem, we have $|G| = \sum_{g \in G} |fix(g)|$. Since for $1_G$ we have $fix(1_G) = X$ and $|X| \geq 2$, then it follows that there exists $g \in G$, such that $fix(g) = \emptyset$. □

**Exercise 7.4.** If G is a transitive subgroup of $S_n$, show that $G$ has at least $n - 1$ elements each of which fixes no point. Conclude that if $G$ is any finite group, and $H$ is a subgroup of index $n$ in $G$, then $G$ has at least $n - 1$ elements which are not conjugate to elements in $H$.

**Exercise 7.5.** We are given 4 red beads and 2 blue beads, and we are making a necklace out of these 6 beads. Two necklaces are different, if one cannot be obtained from another by some symmetry of a regular hexagon. How many different necklaces we can make?

*Proof.* Let $X$ be the set of all necklaces, including those that can be obtained from each other by rotation or reflexion. Then 4 red beads can be placed in any 4 out of 6 given positions. This means that red beads can be placed in $\binom{6}{4} = 15$ different ways. Once the red beads are places, the positions for the blue beads are uniquely determined. Hence we have $|X| = 15$, however, some elements in $X$ correspond to the same necklace. The group of symmetries of regular hexagon is $D_{12}$. Two necklaces are different if and only if one cannot be obtained from another by refexion or rotation, hence the number of different necklaces equals the number of orbits of $D_{12}$ acting on $X$, where $G = D_{12} = \langle (1\ 2\ 3\ 4\ 5\ 6), (1\ 2)(3\ 6)(4\ 5) \rangle$. In order to use Cauchy-Frobenius theorem, we need to determine $|\operatorname{fix}(g)|$. These values are given below:

| $g \in G$ | $\lvert\operatorname{fix}(g)\rvert$ | $g \in G$ | $\lvert\operatorname{fix}(g)\rvert$ |
|---|---|---|---|
| id | 15 | $(1\ 6)(2\ 5)(3\ 4)$ | 3 |
| $(1\ 2\ 3\ 4\ 5\ 6)^i, i = 1, 2, 4, 5$ | 0 | $(2\ 6)(3\ 5)$ | 3 |
| $(1\ 4)(2\ 5)(3\ 6)$ | 3 | $(1\ 3)(4\ 6)$ | 3 |
| $(1\ 2)(3\ 6)(4\ 5)$ | 3 | $(1\ 5)(2\ 4)$ | 3 |
| $(2\ 3)(1\ 4)(5\ 6)$ | 3 | | |

Now using the Cauchy-Frobenius Theorem, we have that the number of orbits of $G$ on $X$ is

$$\frac{1}{12}(15 + 7 \cdot 3) = 3,$$

and we conclude that there are 3 different necklaces. □

**Exercise 7.6.** How many different necklaces with 8 beads can be made if we are given 5 red and 3 blue beads?

**Exercise 7.7.** Let the nodes of square be colored with either red, blue or green. Two such colored squares are considered to be the same, if one can be obtained from another by rotations and reflexions. How many different coloured squares are there?

**Definition 7.8.** Let $X_1 = (V_1, E_1)$ and $X_2 = (V_2, E_2)$ be two graph. We say that a function $f : V_1 \to V_2$ is an *isomorphism* if it is bijective and $\forall u_1, v_1 \in V_1$ it holds $\{u_1, v_1\} \in E_1 \leftrightarrow \{f(u_1), f(v_1)\} \in E_2$. Graphs $X_1$ and $X_2$ are called *isomorphic* if there exists an isomorphism between them.

**Exercise 7.9.** Prove that there are 11 non-isomorphic graphs with 4 vertices.

*Proof.* Let $\mathcal{G}(4)$ be the set of all graphs with vertex set $V = \{1, 2, 3, 4\}$ (including also isomorphic graphs). Then $|\mathcal{G}(4)| = 2^6 = 64$. Let $\Omega = \{\{i, j\} \mid 1 \leq i < j \leq 4\}$. We can think of $\Omega$ as the edge set of complete graph. Let $\mathcal{P}(\Omega)$ denote the power set of $\Omega$, that is, the family of subsets of $\Omega$. The function $F : \mathcal{G}(4) \to \mathcal{P}(\Omega)$ defined with $F(X) = E(X)$ (where $E(X)$) denotes the edge set of $X \in \mathcal{G}(4)$ is bijective function. Suppose we are given two graphs $X_1 = (V, E_1)$ and $X_2 = (V, E_2)$. Then $X_1$ and $X_2$ are isomorphic if and only if there exists permutation $g \in S_4$ such that $g(E_1) = E_2$. This implies that the number of non-isomorphic graphs with 4 vertices equals to the number of orbits in the action of $G = S_4$ on the set $\mathcal{P}(\Omega)$. Using Cauchy-Frobenius theorem, it follows that the number of orbits is

$$\frac{1}{4!} \sum_{g \in S_4} |fix_{\mathcal{P}(\Omega)}(g)|.$$

For a permutation $g \in S_4$ let $g^{(2)}$ denote the corresponding permutation of $\Omega$. Let $c(g)$ denote the number of cycles in the cyclic decomposition of $g^{(2)}$. Then it is not difficult to see that $|fix_{\mathcal{P}(\Omega)}(g)| = 2^{c(g)}$. Observe that if two permutations $g_1$ and $g_2$ in $S_4$ have the same cyclic structure (that is they are conjugate), then $g_1^{(2)}$ and $g_2^{(2)}$ have the same cyclic structures. Now calculating the numbers of cycles in $g^{(2)}$ for all representatives of conjugacy classes in $S_4$ gives us the desired result. □

**Exercise 7.10.** Let $V = \{1, \ldots, n\}$, let $\Omega = \{\{i, j\} \mid 1 \leq i < j \leq n\}$, and let $\mathcal{P}(\Omega) = \{E \mid E \subseteq \Omega\}$. For $g \in S_n$ let $g^{(2)}$ denote the induced permutation of $\Omega$ and let $c(g)$ denote the number of cycles in cyclic decomposition of $g^{(2)}$. Prove that the number of non-isomorphic graphs of order $n$ is

$$\frac{1}{n!} \sum_{g \in S_n} 2^{c(g)}.$$

**Exercise 7.11.** Determine the number of non-isomorphic graphs with 5 vertices.

**Definition 7.12.** Let $V$ be a finite set, and let $\mathcal{P}(V)$ denote the power set of $V$. *Hypergraph* $\mathcal{H} = (V, \mathcal{E})$ is given with the vertex set $V$ and the hyperedge set $\mathcal{E} \subseteq \mathcal{P}(V) \setminus \{\emptyset\}$. Two hypergraphs $\mathcal{H}_1 = (V_1, \mathcal{E}_1)$ and $\mathcal{H}_2 = (V_2, \mathcal{E}_2)$ are said to be isomorphic if there exists bijective function $f : V_1 \to V_2$ such that $f(\mathcal{E}_1) = \mathcal{E}_2$.

**Exercise 7.13.** Determine the number of non-isomorphic hypergraphs with $n$ vertices, for $n \in \{3, 4\}$.

## 7.1 Cycle index of permutation group

**Definition 7.14.** Let $G \leq Sym(X)$, where $X$ is a finite set of size $n$, and let $g \in G$. Let $[c_1(g), \ldots, c_n(g)]$ be the cyclic structure of permutation $g$, that is, $c_k(g)$ denotes the number of cycles of length $k$ in the cyclic decomposition of $g$. *The cycle index* $Z(G)$ of permutation group $G$ is the polynomial

$$Z(G) = \frac{1}{|G|} \sum_{g \in G} x_1^{c_1(g)} \cdot x_2^{c_2(g)} \cdot \ldots \cdot x_n^{c_n(g)}$$

**Exercise 7.15.** Calculate $Z(S_3)$.

**Exercise 7.16.** Calculate $Z(S_4)$.

**Exercise 7.17.** Prove that $Z(C_n) = \frac{1}{n}\sum_{d|n}\varphi(d)x_d^{n/d}$.

**Exercise 7.18.** Prove that $Z(D_n) = \frac{1}{2}Z(C_n) + \begin{cases} \frac{1}{2}x_1x_2^{(n-1)/2}, & n \text{ odd}, \\ \frac{1}{4}\left(x_1^2x_2^{(n-2)/2} + x_2^{n/2}\right), & n \text{ even}. \end{cases}$

**Exercise 7.19.** Prove that

$$Z(S_n) = \sum_{(c)} \frac{1}{\prod_{k=1}^{n} k^{c_k} c_k!} \prod_{k=1}^{n} x_k^{c_k},$$

where the summation is over all integer partitions $(c)$ of $n$.

## 7.2 Polya enumeration theorem

The result we are going to present now, and is usually referred to as Polya enumerations theorem, was first published by John Howard Redfield in 1927. In 1937 it was independently rediscovered by George Polya, who then greatly popularized the result by applying it to many counting problems, in particular to the enumeration of chemical compounds.

Let $X$ be a finite set and let $G \leq Sym(X)$ be a group of permutations of $X$. The set $X$ may represent a finite set of beads, and $G$ may be a chosen group of permutations of the beads. For example, if $X$ is a necklace of $n$ beads in a circle, rotations and reflections are relevant so $G$ is the dihedral group $D_{2n}$ of order $2n$.

**Definition 7.20.** Let $C$ be a finite set of colors. Let $C^X$ be the set of functions $X \to C$, that is $C^X$ is the set of all colorings of the set $X$ with colors from $C$.

For $f \in C^X$, and for $g \in G$, we define an induced action of $G$ on the set $C^X$, with $f^g = f \circ g^{-1}$. Two functions $f_1, f_2 \in C^X$ are called *$G$-equivalent*, if they belong to the same orbit under the induced action of $G$ on $C^X$, or more precisely, if there exists $g \in G$ such that $f_1(g(x)) = f_2(x)$, for every $x \in X$. Polya's enumeration theorem given below counts the number of orbits in this action, or equivalently the number of non-equivalent colorings of the set $X$ with colors from $C$.

**Theorem 7.21** (Polya enumeration theorem)**.** Let $X$ and $C$ be finite sets, and let $G \leq Sym(X)$. The number of orbits in the induced action of $G$ on the set $C^X$ is equal to $Z(G)$ with $x_1 = \ldots = x_i = \ldots x_{|X|} = |C|$.

*Proof.* By Cauchy-Frobenius theorem, it follows that the number of orbits is

$$\frac{1}{|G|}\sum_{g\in G} |fix_{C^X}(g)|.$$

It remains to determine the size of $fix_{C^X}(g) = \{f : X \to C \mid f \circ g^{-1} = f\}$. Let $f \in fix_{C^X}(g)$. Suppose that $(x_1\ x_2 \ldots x_k)$ is one cycle in the cyclic decomposition of $g$. Since $f \circ g = f$, it follows that $f(x_2) = (f \circ g^{-1})(x_2) = f(g^{-1}(x_2)) = f(x_1)$. Similarly, we conclude that $f(x_1) = f(x_2) = \ldots f(x_k)$. Therefore, all vertices in the same orbit of $g$ have the same image under $f$. Since the number of possible images under $f$ is $|C|$, it follows that $|fix_{C^X}(g)| = |C|^{c(g)}$, where $c(g)$ is the number of cycles in the cyclic decomposition of $g$. □

**Exercise 7.22.** For a given partition $(c) = (c_1, c_2, \ldots, c_n)$ of a positive integer $n$ let

$$\gamma(c) = \sum_k \left\lfloor \frac{k}{2} \right\rfloor c_k + \sum_k \frac{kc_k(c_k-1)}{2} + \sum_{r<t} gcd(r,t)c_r c_t. \tag{7}$$

The number of non-isomorphic graphs of order $n$ equals

$$\sum_{(c)=(c_1,\ldots,c_n)} \frac{2^{\gamma(c)}}{\prod k^{c_k} c_k!},$$

where the sum goes throughout all the partitions $(c)$ of $n$.

**Exercise 7.23.** Prove that the number of non equivalent colorings of regular 2015-gone with 5 colors is odd.

*Proof.* By Polya enumeration theorem, it follows that the number of non-equivalent colorings is $Z(D_{2\cdot 2015})$ with $x_1 = \ldots = x_{2015} = 5$. Since

$$Z(D_{2\cdot 2015}) = \frac{1}{4030} \sum_{g \in D_{2\cdot 2015}} x_1^{c_1(g)} \ldots x_{2015}^{c_{2015}(g)}$$

. We conclude that the number of non-equivalent colorings is even if and only if the value

$$\sum_{g \in D_{2\cdot 2015}} 5^{c_1(g)} \ldots 5^{c_{2015}(g)}$$

is divisible by 4. However, sine $5 \equiv 1 \pmod 4$ it follows that $5^{c_i(g)} \equiv 1 \pmod 4$, and therefore,

$$\sum_{g \in D_{2\cdot 2015}} 5^{c_1(g)} \ldots 5^{c_{2015}(g)} \equiv \sum_{g \in D_{2\cdot 2015}} 1 = 4030 \equiv 2 \pmod 4.$$

□

# 8 Linear groups and affine groups

## 8.1 General linear group $GL(n, \mathbb{F})$

Let $\mathbb{F}$ be a field, and let $n \in \mathbb{N}$. We denote by $\mathbb{F}^{n\times n}$ the set of all $n \times n$ matrices $A = (a_{ij})$ such that all $a_{ij} \in \mathbb{F}$. We denote by $I_n$ the $n \times n$ identity matrix. We say that $A$ is invertible if there exits $B \in \mathbb{F}^{n\times n}$ such that $AB = BA = I_n$, where ($B$ is called the inverse of $A$ and written as $A^{-1}$). Note that, $A$ is invertible if and only if $\det(A) \neq 0$.

**Definition 8.1.** The **general linear group** $GL(n, \mathbb{F})$ with dimension $n$, is the group of all invertible matrices in $\mathbb{F}^{n\times n}$.

The set of $n$-tuples $(v_1, \ldots, v_n)$, all $v_i \in \mathbb{F}$, form a vector space. This we also call the **space of row vectors with length** $n$ **over the field** $\mathbb{F}$, this vector space we denote by $\mathbb{F}^n$. Vectors in $\mathbb{F}^n$ are written as $\underline{v} = (v_1, \ldots, v_n)$. Two vectors $\underline{v} = (v_1, \ldots, v_n)$ and $\underline{w} = (w_1, \ldots, w_n)$ are added as

$$\underline{v} + \underline{w} = (v_1 + w_1, \ldots, v_n + w_n),$$

and $\underline{v}$ is multiplied by $a, a \in \mathbb{F}$, as $a\,\underline{v} = (av_1, \ldots, av_n)$. We denote by $\langle \underline{v}_1, \ldots, \underline{v}_m \rangle$ the vector subspace generated by the vectors $\underline{v}_1, \ldots, \underline{v}_m$.

The group $GL(n, \mathbb{F})$ acts on the set $\mathbb{F}^n$ as

$$(v_1, \ldots, v_n)^A = (v_1, \ldots, v_n)A, \quad (v_1, \ldots, v_n) \in \mathbb{F}^n,\ A \in GL(n, \mathbb{F}).$$

**Theorem 8.2.** The action of $GL(n, \mathbb{F})$ on $\mathbb{F}^n$ is faithful, and it has two orbits: $\{(0, \ldots, 0)\}$ and $\mathbb{F}^n \setminus \{(0, \ldots, 0)\}$.

**Exercise 8.3.** Prove that $GL(2, \mathbb{F}_2)$ is isomorphic to $S_3$.

**Exercise 8.4.** Let $\mathbb{F}$ be a finite field with $q$ elements. Prove that

$$|GL(n, q)| = (q^n - 1)(q^n - q) \ldots (q^n - q^{n-1}).$$

## 8.2 Permutation matrices

**Definition 8.5.** Let $g \in S_n$. The **permutation matrix** $P(g)$ corresponding to $g$ is the matrix $A$ in $\mathbb{F}^{n \times n}$, $A = (a_{ij})$, such that

$$a_{ij} = \begin{cases} 1 & \text{if } i^g = j \\ 0 & \text{otherwise} \end{cases}.$$

**Exercise 8.6.** Let $g \in S_n$. Prove that $g$ is even permutation if and only if $\det(P(g)) = 1$ and $g$ is odd permutation, if and only if $\det(P(g)) = -1$.

Note that, every permutation matrix $P(g)$ is in fact in $GL(n, \mathbb{F})$, as its determinant $\det(P(g)) = \pm 1$.

**Example 8.7.** Let $g_1 = (1\ 3\ 4)$ and $g_2 = (3\ 4)$ in $S_4$. Then $g_1 g_2 = (1\ 4)$, and $P(g_1), P(g_2)$ and $P(g_1 g_2)$ are the matrices:

$$P(g_1) = \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \end{pmatrix}, \quad P(g_2) = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}, \quad P(g_1 g_2) = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix}.$$

We observe that last matrix equals the product of the first two ones. If $(v_1, v_2, v_3, v_4) \in \mathbb{F}^4$, then we have

$$(v_1, v_2, v_3, v_4)P(g_1) = (v_4, v_2, v_1, v_3) = (v_{g_1^{-1}(1)}, v_{g_1^{-1}(2)}, v_{g_1^{-1}(3)}, v_{g_1^{-1}(4)}).$$

**Theorem 8.8.** (1) The mapping $g \mapsto P(g)$ is a homomorphism from $S_n$ to $GL(n, \mathbb{F})$.

(2) If $(v_1, \ldots, v_n) \in \mathbb{F}^n$, $g \in S_n$, then $(v_1, \ldots, v_n)P(g) = (v_{g^{-1}(1)}, \ldots, v_{g^{-1}(n)})$.

(3) If $A \in GL(n, \mathbb{F}), A = (a_{ij})$, then $P(g)^{-1} A P(g) = A' = (a'_{ij})$, where $a'_{ij} = a_{g^{-1}(i) g^{-1}(j)}$.

*Proof.* (1): Let $g_1, g_2 \in S_n$, and let $P(g_1)P(g_2) = (p_{ij})$. Then $p_{ij} = \sum_{k=1}^{n} P(g_1)_{ik}P(g_2)_{kj}$ is in $\{0,1\}$, and $p_{ij} = 1$ if and only if $i^{g_1} = k$ and $k^{g_2} = j$, which is equivalent to $i^{g_1 g_2} = j$. Thus $P(g_1g_2)_{ij} = p_{ij}1$ for all $i, j \in \{1, \ldots, n\}$.

(2): Let us write $(x_1, \ldots, x_n)P(g) = (x'_1, \ldots, x'_n)$. Then $x'_i = \sum_{k=1}^{n} x_k P(g)_{ki}$, hence $x'_i = x_k$, where $k^g = i$, i.e., $x'_i = x_{g^{-1}(i)}$.

(3): Because of (1) $P(g)^{-1} = P(g^{-1})$, and

$$\begin{aligned} a'_{ij} = \big(\, P(g^{-1})AP(g)\,\big)_{ij} &= \sum_{k=1}^{n} \big(\, P(g^{-1})A\,\big)_{ik} P(g)_{kj} = \big(\, P(g)A\,\big)_{i,g^{-1}(j)} \\ &= \sum_{k=1}^{n} P(g^{-1})_{ik}\, a_{k,g^{-1}(j)} = a_{g^{-1}(i),g^{-1}(j)}. \end{aligned}$$

□

**Theorem 8.9.** The center of $GL(n, \mathbb{F})$ is the subgroup $\{aI_n \mid a \in \mathbb{F}, a \neq 0\}$.

*Proof.* Let $G = GL(n, \mathbb{F})$ and let $Z = \{aI_n \mid a \in \mathbb{F}, a \neq 0\}$. If $n = 1$, then $G = Z$, and the claim is true. We assume that $n \geq 2$. It follows easily that $Z$ is a subgroup of $G$. We denote by $\mathbf{Z}(G)$ the center of the group $G$. For every $A \in G$, $(aI_n)A = aA$, and $A(aI_n) = aA$, hence $Z \leq \mathbf{Z}(G)$.

Let $A \in \mathbf{Z}(G), A = (a_{ij})$. Then $P(g^{-1})AP(g) = A$ for all permutation matrices $P(g)$. Because of (3) in Theorem 8.8, $a_{ij} = a_{g^{-1}(i)g^{-1}(j)}$ for all $i, j \in \{1, \ldots, n\}$ and all $g \in S_n$. Thus we obtain that

$$A = \begin{pmatrix} a & b & \cdots & b \\ b & a & \cdots & b \\ \vdots & \vdots & \vdots & \vdots \\ b & b & \cdots & a \end{pmatrix}.$$

Let $B = (b_{ij})$ be the matrix, where $b_{ii} = 1$ for every $i \in \{1, \ldots, n\}$, $b_{12} = 1$, and $b_{ij} = 0$ for every $i, j \in \{1, \ldots, n\}, i \neq j$ and $(i, j) \neq (1, 2)$. As $A \in \mathbf{Z}(G)$, $AB = BA$. Then $a + b = (AB)_{22} = (BA)_{22} = a$. We obtain $b = 0$ and $a \neq 0$, so that $A = aI_n \in Z$. Thus $\mathbf{Z}(G) \leq Z$, and we obtain $\mathbf{Z}(G) = Z$.

□

**Exercise 8.10.** Let $P = \{P(g) \mid g \in S_n\}$, the set of all permutation matrices.

1. Prove that $P$ is a subgroup of $GL(n, F)$.
2. Prove that $P$ is isomorphic to $S_n$.

**Exercise 8.11.** Let $F$ be a finite field of order $q$, let $Z = \{aI_n \mid a \in \mathbb{F}, a \neq 0\}$, and let $P$ be the subgroup of all permutation matrices in $GL(n, \mathbb{F})$.

1. Prove that $Z$ is isomorphic to $\mathbb{Z}_{q-1}$.
   (Hint: Multiplicative group $\mathbb{F}^*$ is cyclic of order $q - 1$.)
2. Let $G = \langle P, Z \rangle \leq GL(n, \mathbb{F})$. To which group is $G$ isomorphic?
   (Hint: Both $P$ and $Z$ are normal subgroups of $G$.)

## 8.3 Special linear groups $SL(n, \mathbb{F})$

Let $A$ and $B$ two matrices in $\mathbb{F}^{n\times n}$. It is a fact in linear algebra that $\det(AB) = \det(A)\det(B)$. Thus the mapping

$$\phi\colon\ GL(n, \mathbb{F}) \to (\mathbb{F} \setminus \{0\}, \cdot)\ A \mapsto \det(A)$$

is a homomorphism from the group $GL(n, \mathbb{F})$ to the multiplicative group of nonzero elements in $\mathbb{F}$. The kernel of the above homomorphism $\phi$ is a normal subgroup of $GL(n, \mathbb{F})$ which contains all matrices with determinant 1.

**Definition 8.12.** The **special linear group** $SL(n, \mathbb{F})$ over the field $\mathbb{F}$ with dimension $n$ is the group of all $n \times n$ invertible matrices in $\mathbb{F}^{n\times n}$ with determinant 1.

**Exercise 8.13.** Prove that $SL(n, \mathbb{F})$ is normal subgroup of $GL(n, \mathbb{F})$.

The group $SL(n, \mathbb{F})$ acts on the set $\mathbb{F}^n$ as

$$(v_1, \ldots, v_n)^A = (v_1, \ldots, v_n)A, \quad (v_1, \ldots, v_n) \in \mathbb{F}^n,\ A \in SL(n, \mathbb{F}).$$

**Theorem 8.14.** The action of $SL(n, \mathbb{F})$ on $\mathbb{F}^n$ is faithful, and it has two orbits: $\{(0, \ldots, 0)\}$ and $\mathbb{F}^n \setminus \{(0, \ldots, 0)\}$.

**Exercise 8.15.** Let $\mathbb{F}$ be a finite field with $q$ elements. Prove that

$$|SL(n, \mathbb{F})| = (q^n - 1)(q^n - q) \ldots (q^n - q^{n-1})/(q - 1).$$

(Hint: Use the fact that $SL(n, \mathbb{F})$ is the kernel of homomorphism $\phi :\ GL(n, \mathbb{F}) \to \mathbb{F}^*, \phi : A \mapsto \det(A)$.)

**Exercise 8.16.** Let $\mathbb{F} = \{0, 1, 2, 3, 4\}$ be the field of size 5. Let $x_1 = (3, 4, 5)$ and $x_2 = (1, 2, 3)$. Find an element $A$ in $SL(3, \mathbb{F})$ such that $x_1^A = x_2$.

**Exercise 8.17.** Let $G = SL(2, \mathbb{F}_3)$, where $\mathbb{F}_3 = \{0, 1, 2\}$. Let $H = G_{(1,0)}$, be the stabilizer of $(1, 0)$ in $G$. Determine the orbits of $H$. Let $A = \begin{pmatrix} 0 & 1 \\ 2 & 0 \end{pmatrix}$. Determine the cyclic structure of permutation induced by $A$.

**Exercise 8.18.** Determine which permutation matrices belong to $SL(n, \mathbb{F})$.

## 8.4 Projective linear groups $PGL$ and $PSL$

Let $\mathbb{F}$ be the finite field of order $q$. Groups $GL(n, \mathbb{F})$ and $SL(n, \mathbb{F})$ will be denoted by $GL(n, q)$ and $SL(n, q)$.

**Definition 8.19.** Let $U$ be a one-dimensional subspace of $F^n$. Set $U \setminus \{(0, \ldots, 0)\}$ is called a **projective point**. The set of all projective points is called **projective space** and is denoted by $PG(n - 1, q)$.

**Example 8.20.** Let $q = 3$ and $n = 2$. Then projective points in $PG(1, 3)$ are $\{(1, 0), (2, 0)\}$, $\{(1, 1), (2, 2)\}$, $\{(0, 1), (0, 2)\}$, $\{(1, 2), (2, 1)\}$.

**Theorem 8.21.** Any two distinct projective points are disjoint. The number of projective points in $PG(n-1,q)$ is $(q^n-1)/(q-1)$ and each projective point consists of $q-1$ vectors from $\mathbb{F}^n$.

**Theorem 8.22.** $PG(n-1,q)$ is a complete block system for $GL(n,q)$ and $SL(n,q)$.

*Proof.* One dimensional subspaces are mapped by the elements of $GL(n,q)$ into the one-dimensional subspaces. Observe that intersection of two distinct one-dimensional subspaces of $\mathbb{F}^n$ is $\{(0,\ldots,0)\}$. The rest is left as exercise. □

**Theorem 8.23.** The kernel of the action of $GL(n,q)$ on $PG(n-1,q)$ is $Z=\{aI \mid a\in\mathbb{F}^*\}$, that is $fix_{GL(n,q)}(PG(n-1,q))=Z$.

*Proof.* Idea: Consider the stabilizer of $\langle e_i\rangle=\langle(0,0,\ldots,1,0,\ldots,0)\rangle$. □

**Definition 8.24.** The permutation group induced by the action of $GL(n,q)$ on $PG(n-1,q)$ is called **projective general linear group** and is denoted by $PGL(n,q)$. The permutation group induced by the action of $SL(n,q)$ on $PG(n-1,q)$ is called **projective special linear group** and is denoted by $PSL(n,q)$.

Observe that $PGL(n,q)$ and $PSL(n,q)$ are transitive permutation groups of degree $(q^n-1)/(q-1)$.

**Corollary 8.25.** $PGL(n,q)\cong GL(n,q)/Z$ and $PSL(n,q)\cong SL(n,q)/(Z\cap SL(n,q))$.

*Proof.* Since the kernel of action of $GL(n,q)$ (resp. $SL(n,q)$) on $PG(n-1,q)$ is $Z$ (resp. $Z\cap SL(n,q)$), the result follows. □

**Exercise 8.26.** Prove that $SL(n,q)\cap Z=\{wI \mid w\in F^*, w^n=1\}$.

**Exercise 8.27.** Prove that $|PGL(n,q)|=|GL(n,q)|/(q-1)=|SL(n,q)|$.

**Exercise 8.28.** Determine the cyclic structure of elements of $PSL(2,3)$. Prove that it is isomorphic to $A_4$.

**Exercise 8.29.** Prove that $PSL(2,4)\cong PSL(2,5)\cong A5$.

**Exercise 8.30.** Prove that $PSL(2,9)\cong A6$.

## 8.5 Semilinear groups $\Gamma L$ and $\Sigma L$

Let $p$ be a prime, a $q=p^s$ for some positive integer $s$. Let $\mathbb{F}$ be the field of order $q$. Let $f:\mathbb{F}\to\mathbb{F}$ me the mapping defined with $f:x\mapsto x^p$. Mapping $f$ is automorphism of the field $\mathbb{F}$, and is called **Frobenius automorphism** of the field $\mathbb{F}$.

**Exercise 8.31.** Let $f$ be the Frobenius automorphism of the field $\mathbb{F}$ of order $q=p^s$. Observe that $f^k(x)=x^{p^k}$ for every positive integer $k$. For $x=0$ it is clear that $f^k(x)=0$. Since $F^*$ is cyclic group of order $p^s-1$, it follows that $x^{p^s-1}=1$, for every $x\in F^*$. Hence $x^{p^s}=x$, for every $x\in\mathbb{F}$, and therefore $f^s$ is the identity mapping. This shows that $\langle f\rangle$ is cyclic group of order $s$.

**Example 8.32.** Let $\overline{f}$ be the permutation of $\mathbb{F}^n$, induced by the action of $f$ coordinate-wise, that is $\overline{f} : (x_1, \ldots, x_n) \mapsto (x_1^p, \ldots, x_n^p)$. Prove that $\langle \overline{f} \rangle$ is cyclic group of order $s$. Determine the set $fix_{\mathbb{F}^n}(\overline{f})$, of all fixed points in $F^n$ by $\overline{f}$.

**Definition 8.33.** Let $f$ be the Frobenius automorphism of $\mathbb{F}$. Let $F : \mathbb{F}^{n\times n} :\to \mathbb{F}^{n\times n}$ be defined with $F(A)_{i,j} = f(a_{i,j})$.

**Example 8.34.** Let $p = 2$ and $s = 2$. Let $\mathbb{F} = \{0, 1, a, 1 + a\}$ be the field of order $q = 2^2$, where $2x = 0$ and $a^2 + a + 1 = 0$. Let $f$ be the Frobenius automorphism. Then the cyclic decomposition permutation of $\mathbb{F}$ induced by $f$ is $(0)(1)(a,\ 1+a)$. Let $A = \begin{pmatrix} a & 1 \\ 1+a & 0 \end{pmatrix}$. Then $F(A) = \begin{pmatrix} 1+a & 1 \\ a & 0 \end{pmatrix}$.

**Example 8.35.** Let $p = 2$, $s = 3$, and let $\mathbb{F}$ be the field of order 8, $\mathbb{F} = \{\lambda_1 + \lambda_2 a + \lambda_3 a^2 \mid \lambda_i \in \{0, 1\}\}$ where $a \in \mathbb{F}$ is such that $a^3 - a - 1 = 0$. Determine the generator of $F^*$. Determine the cyclic structure of $f$. Let $A = \begin{pmatrix} a^2 & 0 \\ 1+a^2 & 1+a \end{pmatrix}$. Calculate $F(A)$. Determine $(a, a+1)^{F(A)}$ and $(a, a+1)^{\overline{f}^{-1}A\overline{f}}$.

**Theorem 8.36.** Mapping $F$ is an automorphism of the group $GL(n, q)$ (resp. automorphism of the group $SL(n, q)$).

*Proof.* Let $A \in GL(n, q)$. Then $det(A) \neq 0$. Since $det(F(A)) = F(det(A)) \neq 0$, it follows that $F$ maps invertible matrices into invertible matrices. Similarly we see that $F$ maps $SL(n, q)$ to $SL(n, q)$. Let $A, B \in GL(n, q)$. Then for every $i, j \in \{1, \ldots, n\}$ we have

$$F(AB)_{i,j} = f((AB)_{i,j}) = f(\sum_{k=1}^{n} A_{ik}B_{kj}) = \sum_{k=1}^{n} f(A_{ik})f(B_{kj}) = (F(A)F(B))_{i,j}.$$

This shows that $F$ is homomorphism. It remains to prove that $F$ is bijective. Let $A \in GL(n, q)$ be such that $F(A) = I$. Then $f(A_{i,j}) = \delta_{i,j}$. However, since $f$ is bijective mapping from $\mathbb{F}$ to $\mathbb{F}$, and $f(0) = 0$, $f(1) = 1$, it follows that $A = I$, and hence $F$ is injective. Since $GL(n, q)$ is finite, it follows that $F$ is automorphism of $GL(n, q)$. Similarly we see that $F$ is automorphism of $SL(n, q)$. □

**Exercise 8.37.** Prove that the order of $F$ as a permutation of $GL(n, q)$ is $s$.

Define mapping $\varphi : \langle f \rangle \to Aut(GL(n, q))$ with $\varphi(f^i) = F^i$.

**Exercise 8.38.** Prove that the mapping $\varphi$ is homomorphism.

Recall that $GL(n, q)$ acts faithfully on $\mathbb{F}^n$. This means that $GL(n, q) \leq Sym(F^n)$. Also, we have $\overline{f} \in Sym(\mathbb{F}^n)$

**Definition 8.39. General semilinear group** $\Gamma L(n, q)$ is the subgroup of $Sym(\mathbb{F}^n)$ generated by $GL(n, q)$ and $\overline{f}$, that is $\Gamma L(n, q) = \langle GL(n, q), \overline{f} \rangle$.

**Exercise 8.40.** Prove that $\overline{f}^{-1}A\overline{f} = F(A)$.

Hint: Prove that the images $(x_1, \ldots, x_n)^{F(A)}$ and $(x_1, \ldots, x_n)^{\overline{f}^{-1}A\overline{f}}$ are the same.

**Theorem 8.41.** Let $q = p^s$ and $n$ positive integer. Then

(i) $GL(n,q) \lhd \Gamma L(n,q)$;

(ii) $\Gamma L(n,q) \cong GL(n,q) \rtimes \langle \overline{f} \rangle$.

(iii) $|\Gamma L(n,q)| = s \cdot (q^n - 1)(q^n - q) \dots (q^n - q^{n-1})$.

*Proof.* (i) To prove this, it suffices to prove that $\overline{f}^{-1} A \overline{f} \in GL(n,q)$, for every $A \in GL(n,q)$. Since by Exercise 8.40 it follows that $\overline{f}^{-1} A \overline{f} = F(A)$, and by Theorem 8.36 $F$ is automorphism of $GL(n,q)$ it follows that $F(A) \in GL(n,q)$. This proves $(i)$.

(ii) It suffices to prove that $GL(n,q) \cap \langle \overline{f} \rangle = \{id\}$. Observe that $\overline{f}^k$ fixes each of the $e_i = (\delta_{1,i}, \dots, \delta_{n,i})$. Suppose that $f^k = A$, for some $A \in GL(n,q)$. Then also $A$ has to fix each of $e_i$. It is now easy to see that $A = I$.

(iii) Since $|GL(n,q)| = (q^n - 1)(q^n - q) \dots (q^n - q^{n-1})$ and $\langle \overline{f} \rangle = s$, then by $(ii)$ the result follows.

□

**Exercise 8.42.** Prove that $\Gamma L(2,2) \cong S_3$.

Similar to the case of general semilinear group, we can define special semilinear group. Recall that $SL(n,q)$ can also be seen as a subgroup of $Sym(\mathbb{F}^n)$.

**Definition 8.43. Special semilinear group** $\Sigma L(n,q)$ is the subgroup of $Sym(\mathbb{F}^n)$ generated by $SL(n,q)$ and $\overline{f}$, that is $\Sigma L(n,q) = \langle SL(n,q), \overline{f} \rangle$.

**Theorem 8.44.** Let $q = p^s$ and $n$ positive integer. Then

(i) $SL(n,q) \lhd \Sigma L(n,q)$;

(ii) $\Sigma L(n,q) \cong SL(n,q) \rtimes \langle \overline{f} \rangle$.

(iii) $|\Sigma L(n,q)| = s \cdot (q^n - 1)(q^n - q) \dots (q^n - q^{n-1})/(q-1)$.

## 8.6 Projective semilinear group $P\Gamma L$

Recall that $PG(n-1,q)$ is the set of projective points, that is one-dimensional subspaces of $F^n$ without $(0, \dots, 0)$.

**Theorem 8.45.** $PG(n-1,q)$ is a complete block system for $\Gamma L(n,q)$ and $\Sigma L(n,q)$.

*Proof.* Since we already proved that $PG(n-1,q)$ is a complete block system for $GL(n,q)$ it suffices to prove that $PG(n-1,q)$ are blocks for $\langle \overline{f} \rangle$. Let $\pi \in PG(n-1,q)$. Then there exists $\underline{x} \in \mathbb{F}^n \setminus \{(0, \dots, 0)\}$ such that $\pi = \{\lambda \underline{x} \mid \lambda \in \mathbb{F}^*\}$. Then $\overline{f}(\pi) = \{\lambda \overline{f}(\underline{x}) \mid \lambda \in \mathbb{F}^*\}$, which is also a projective point. □

**Definition 8.46.** The **projective general semilinear group** $P\Gamma L(n,q)$ is the permutation group induced by the action of $\Gamma L(n,q)$ on $PG(n-1,q)$.

**Definition 8.47.** The **projective special semilinear group** $PS\Gamma L(n,q)$ is the permutation group induced by the action of $\Sigma L(n,q)$ on $PG(n-1,q)$.

**Theorem 8.48.** (i) $P\Gamma L(n,q) \cong \Gamma L(n,q)/Z$;

(ii) $PS\Gamma L(n,q) \cong \Sigma L(n,q)/(Z \cap SL(n,q))$

*Proof.* Let $K$ be the kernel of the action of $\Gamma L(n,q)$ on $PG(n-1,q)$. It is easy to see that $Z \leq K$. Since $\overline{f}^k$ fixes each vector with 0 and 1 entries, it is easy to see that $\overline{f}^k A \in K$, implies that $A \in Z$. □

**Exercise 8.49.** Prove that $P\Gamma L(2,2) \cong S_3$

**Exercise 8.50.** Prove that $P\Gamma L(2,4) \cong S_5$.

**Exercise 8.51.** Let $\overline{f}_p$ be the permutation induced by $\overline{f}$ on $PG(n-1,q)$. Prove that $\overline{f}_p$ is of order $s$.

**Exercise 8.52.** Consider the permutation group of $PG(n-1,q)$ induced by $PGL(n,q)$ and $\overline{f}_p$. Prove that

1. $PGL(n,q) \lhd \langle PGL(n,q), \overline{f}_p \rangle$;
2. $\langle PGL(n,q), \overline{f}_p \rangle \cong PGL(n,q) \rtimes \langle f_p \rangle$;
3. $P\Gamma L(n,q) \cong \langle PGL(n,q), \overline{f}_p \rangle$.

## 8.7 Affine groups

**Definition 8.53.** Let $A \in GL(n,\mathbb{F})$ and $b \in \mathbb{F}^n$. Let $t_{A,b} : \mathbb{F}^n \to \mathbb{F}^n$ defined with $t_{A,b} : x \mapsto xA + b$. Mapping $t_{A,b}$ is called **affine transformation** of the vector space $\mathbb{F}^n$.

**Exercise 8.54.** Prove that for every $A \in GL(n,\mathbb{F})$ and every $b \in \mathbb{F}^n$, $t_{A,b}$ is a permutation of $\mathbb{F}^n$.

**Exercise 8.55.** Prove that $t_{A_1,b_1} t_{A_2,b_2} = t_{A_1A_2, b_1A_2+b_2}$.

**Exercise 8.56.** Prove that $t_{A_1,b_1} = t_{A_2,b_2}$ if and only if $A_1 = A_2$ and $b_1 = b_2$.

*Proof.* Suppose that $t_{A_1,b_1} = t_{A_2,b_2}$. Then $xA_1 + b_1 = xA_2 + b_2$, for every $x \in \mathbb{F}^n$. If $x = (0,\ldots,0)$, this implies that $b_1 = b_2$. Hence $x(A_1 - A_2) = (0,\ldots,0)$, for every $x \in \mathbb{F}^n$. Using the last equality for $x = e_1,\ldots,e_n$ it follows that $A_1 = A_2$. □

**Exercise 8.57.** Prove that $t_{A,b}^{-1} = t_{A^{-1},-bA^{-1}}$.

**Definition 8.58.** Let $\mathbb{F}$ be a field, $n$ positive integer, then the **general affine group** $AGL(n,\mathbb{F})$ is the group of all permutations $t_{A,b}$, that is

$$AGL(n,\mathbb{F}) = \{t_{A,b} \mid A \in GL(n,\mathbb{F}), b \in \mathbb{F}^n\}.$$

**Theorem 8.59.** Group $AGL(n,\mathbb{F})$ acts faithfully and transitively on $\mathbb{F}^n$. Stabilizer of a point is isomorphic to $GL(n,\mathbb{F})$.

*Proof.* Since $GL(n,\mathbb{F})$ is a subgroup of $AGL(n,\mathbb{F})$ it follows that $AGL(n,\mathbb{F})$ acts transitively on $\mathbb{F}^n$. By Exercise (8.56) it follows that the action is faithfull, namely the only element in the kernel is $t_{I_n,\mathbf{0}}$.

Let $H$ be the stabilizer of $\mathbf{0} = (0,\ldots,0) \in \mathbb{F}^n$ in the action of $AGL(n,\mathbb{F})$, that is $H = \{t_{A,b} \mid \mathbf{0}^{t_{A,b}} = \mathbf{0}\}$. We have $t_{A,b}(\mathbf{0}) = \mathbf{0}$, if and only if $b = \mathbf{0}$, hence $H = \{t_{A,\mathbf{0}} \mid A \in GL(n,\mathbb{F})\} \cong GL(n,\mathbb{F})$. This concludes the proof. □

**Corollary 8.60.** If $\mathbb{F}$ is a finite field of order $q$ then

$$|AGL(n,\mathbb{F})| = |GL(n,q)|q^n = q^n(q^n-1)(q^n-q)\ldots(q^n-q^{n-1}).$$

**Definition 8.61.** Let $\mathbb{F}$ be a field, $n$ positive integer, then the **special affine group** $ASL(n,\mathbb{F})$ is the group of all permutations $t_{A,b}$, where $A \in SL(n,\mathbb{F})$ that is

$$ASL(n,\mathbb{F}) = \{t_{A,b} \mid A \in SL(n,\mathbb{F}), b \in \mathbb{F}^n\}.$$

**Exercise 8.62.** Let $T = \{t_{I,b} \mid b \in \mathbb{F}^n\}$. Prove that $T$ is a normal subgroup of $AGL(n,\mathbb{F})$. ($T$ is called the group of all translations.) Prove that $T$ is a regular subgroup of $AGL(n,\mathbb{F})$.

**Theorem 8.63.** Let $\mathbb{F}$ be a field and $n$ positive integer. Then

(i) $AGL(n,\mathbb{F}) \cong T \rtimes GL(n,\mathbb{F})$;

(ii) $ASL(n,\mathbb{F}) \cong T \rtimes SL(n,\mathbb{F})$

*Proof.* Let $H$ be the stabilizer of point $(0,0,\ldots,0)$. We already saw that $H \cong GL(n,\mathbb{F})$. Since $T$ is a transitive subgroup of $AGL(n,\mathbb{F})$, it follows that $TH = AGL(n,\mathbb{F})$. Moreover, since $T$ is a normal subgroup of $AGL(n,\mathbb{F})$, and $H \cap T = \{t_{I,\mathbf{0}}\}$, $(i)$ follows. Similarly, $(ii)$ follows. □

**Definition 8.64.** Let $A \in GL(n,\mathbb{F})$ and $b \in \mathbb{F}^n$ and let $\sigma \in Aut(\mathbb{F})$. Let $t_{A,b,\sigma} : \mathbb{F}^n \to \mathbb{F}^n$ defined with $t_{A,b,\sigma} : x \mapsto \sigma(x)A+b$. Mapping $t_{A,b,\sigma}$ is called **affine semilinear transformation** of the vector space $\mathbb{F}^n$.

**Exercise 8.65.** Prove that the product of two affine semilinear transformations is an affine semilinear transformation. Prove that $t_{A_1,b_1,\sigma_1} = t_{A_2,b_2,\sigma_2}$ if and only if $A_1 = A_2$, $b_1 = b_2$ and $\sigma_1 = \sigma_2$.

*Proof.* We leave to reader to verify that the product of two affine semilinear transformations is an affine semilinear transformation. It is also clear that $A_1 = A_2$, $b_1 = b_2$ and $\sigma_1 = \sigma_2$ implies $t_{A_1,b_1,\sigma_1} = t_{A_2,b_2,\sigma_2}$.

Suppose now that $t_{A_1,b_1,\sigma_1} = t_{A_2,b_2,\sigma_2}$ holds. It follows that $\sigma_1(x)A_1 + b_1 = \sigma_2(x)A_2 + b_2$, for every $x \in \mathbb{F}^n$. Choosing $x = (0,\ldots,0)$, it follows that $b_1 = b_2$. Let $x = e_i$. Since $\sigma_1(e_i) = \sigma_2(e_i) = e_i$, it follows that $A_1 = A_2$. This implies that $(\sigma_1(x) - \sigma_2(x))A_1 = 0$, for every $x \in \mathbb{F}^n$. Since $A_1$ is invertible, it follows that $\sigma_1(x) - \sigma_2(x) = 0$, for every $x$, hence $\sigma_1 = \sigma_2$. This concludes the proof. □

**Definition 8.66.** Let $\mathbb{F}$ be a field, $n$ positive integer, then the **affine semilinear group** $A\Gamma L(n,\mathbb{F})$ is the group of all permutations $t_{A,b,\sigma}$, that is

$$A\Gamma L(n,F) = \{t_{A,b,\sigma} \mid A \in GL(n,\mathbb{F}), b \in \mathbb{F}^n, \sigma \in Aut(\mathbb{F})\}.$$

**Theorem 8.67.** $A\Gamma L(n,\mathbb{F})$ is a transitive and faithful permutation group of $\mathbb{F}^n$. Stabilizer of a point is isomorphic to $\Gamma L(n,\mathbb{F})$.

*Proof.* It is clear that $A\Gamma L(n,\mathbb{F})$ acts transitively. By Exercise 8.65 it follows that the action is faithful. Let $H$ be the stabilizer of point $(0,\ldots,0)$. Then $H = \{t_{A,\mathbf{0},\sigma} \mid A \in GL(n,\mathbb{F}), \sigma \in Aut(\mathbb{F})\}$. It is now easy to see that $H \cong \Gamma L(n,\mathbb{F})$. □

# 9 Wreath product

**Definition 9.1.** Let $A$ and $B$ be two finite groups and suppose $B$ acts on the set $\{1,\ldots,n\}$. We define the **wreath product** of $A$ and $B$ with respect to this action, to be

$$AwrB := A^n \rtimes B$$

where the **top group** $B$ acts on the **base group** $A^n$ by

$$(a_1,\ldots,a_n)^{b^{-1}} = (a_{1^b},\ldots,a_{n^b})$$

for all $(a_1,\ldots,a_n) \in A^n$ and $b \in B$.

**Exercise 9.2.** Show that the action of the top group $B$ on the base group $A^n$ given in the definition above is well-defined.

Observe that the definition of wreath product $AwrB$ implies that the product in this group is given with

$$((a_1,\ldots,a_n),b) * ((a'_1,\ldots,a'_n),b') = ((a_1a'_{1^b},\ldots,a_na'_{n^b}),bb')$$

**Example 9.3.** Let $A$ be any group, $B = \{0,1\} \cong \mathbb{Z}_2$, and $B$ acts on $\{1,2\}$ with $1^0 = 1$, $2^0 = 2$, $1^1 = 2$, $2^1 = 1$. Then we have

$$\begin{aligned} ((a_1,a_2),0) * ((a'_1,a'_2),x) &= ((a_1a'_1,a_2a'_2),x) \\ ((a_1,a_2),1) * ((a'_1,a'_2),x) &= ((a_1a'_2,a_2a'_1),1+x) \end{aligned}$$

The group $AwrB$ is defined as abstract group. There are two important permutation groups associated with this abstract group, and we study them in the following two subsections.

## 9.1 Imprimitive wreath product

Suppose that a group $A$ acts on a set $X$, and $B$ acts on a set $N = \{1,\ldots,n\}$.

**Definition 9.4.** The **imprimitive action** of $AwrB$ on $X \times N$, defined by

$$(x,i)^{((a_1,\ldots,a_n),b)} = (x^{a_i},i^b)$$

for all $(x,i) \in X \times N$ and all $((a_1,\ldots,an),b) \in AwrB$.

**Example 9.5.** For $i \in \{1,\ldots,n\}$ let $X_i = X \times \{i\}$. Prove that $X_i$ is a block for $AwrB$.

*Proof.* Let $g = ((a_1, \ldots, a_n), b) \in AwrB$ be such that $X_i^g \cap X_i \neq \emptyset$. It is now clear that $i^b = b$. Therefore $X_i^g = X_i$. □

**Example 9.6.** Let $X = \{a, b, c\}$ and let $A = Sym(X)$. Let $n = 2$, $N = \{1, 2\}$ and $B = Sym(N)$. Consider the action of $AwrB$ on $X \times N = \{(a, 1), (a, 2), (b, 1), (b, 2), (c, 1), (c, 2)\}$. Let $\rho = (a\ b\ c)$ and $\tau = (a\ b) \in Sym(X)$. Then

$$\begin{aligned}
((\rho, \rho), id) &= ((a,1)\ (b,1)\ (c,1))\,((a,2)\ (b,2)\ (c,2)) \\
((\rho, \tau), id) &= ((a,1)\ (b,1)\ (c,1))\,((a,2)\ (b,2)) \\
((\tau, \rho), id) &= ((a,1)\ (b,1))((a,2)\ (b,2)\ (c,2)) \\
((\rho, \tau), (1\ 2)) &= ((a,1)\ (b,2))((a,2)\ (b,1)\ (c,2)\ (c,1)) \\
((\tau, \rho), (1\ 2)) &= ((a,1)\ (b,2)\ (c,1)\ (c,2))((a,2)\ (b,1)).
\end{aligned}$$

The following theorem describes importance of imprimitive wreath product, and shows that every imprimitive permutation group can be identified with a subgroup of impritive wreath product.

**Theorem 9.7.** Let $G$ be a transitive permutation group acting on $\Omega$ with $G$-invariant partition $\mathcal{B}$. Let $A$ be the stabilizer of a block $X \in \mathcal{B}$ in $G$, and let $B$ be the induced action of $G$ on $\mathcal{B}$. Then $G$ is permutation isomorphic to a subgroup of $AwrB$.

## 9.2 Primitive wreath product

The construction in the previous section showed how wreath products arise as imprimitive groups. Wreath products also play an important role in the study of primitive permutation groups, which we now describe.

Suppose that a group $A$ acts on a set $X$, and $B$ acts on a set $N = \{1, \ldots, n\}$.

**Definition 9.8.** The **product action** of $AwrB$ on $X^n$, is defined by

$$(x_1, \ldots, x_n)^{((a_1,\ldots,a_n),b^{-1})} = (x_{1^b}^{a_{1^b}}, \ldots, x_{n^b}^{a_{n^b}})$$

for all $(x_1, \ldots, x_n) \in X^n$ and all $((a_1, \ldots, a_n), b) \in AwrB$.

**Exercise 9.9.** Prove that the product action is well defined action.

**Exercise 9.10.** Let $X = \{x_1, x_2, x_3\}$, $A = Sym(X)$, $N = \{1, 2\}$, $B = Sym(N)$. Let $\rho = (x_1\ x_2\ x_3)$ and $\tau = (x_1\ x_3)$. Write down the cyclic decomposition of $((\rho, id_X), id)$ and $((\rho, \tau), (1, 2))$.

**Exercise 9.11.** Prove that the product action of $AwrB$ is faithful if and only if both actions of $A$ and $B$ are faithful.

**Exercise 9.12.** Let $A \leq Sym(X)$ and $B \leq Sym(N)$ where $N = \{1, \ldots, n\}$, and let $G = AwrB$. Suppose that $A$ has $m$ orbits on $X$. Show that $G$ has

$$\frac{1}{|B|} \sum_{x \in B} m^{c(x)}$$

orbits on $X \times N$, where $c(x)$ denotes the number of cycles of $x \in B$.

*Proof.* Suppose that $A$ has $m$ orbits on $X$, let $O = \{O_1, O_2, \ldots, O_m\}$ be the set of $m$ orbits of $A$ on $X$. Consider now the action of $A^n$ on $X^n$ (that is $(a_1, \ldots, a_n)$ maps $(x_1, \ldots, x_n)$ into $(x_1^{a_1}, \ldots, x_n^{a_n})$. The number of orbits in this action is $m^n$, that is orbits are elements of the set $O^n$. The definition of the product action of wreath product implies that element $((a_1, \ldots, a_n), b)$ is the permutation obtained by first applying $(a_1, \ldots, a_n)$ (as described above) and then permuting the coordinates using $b$. This implies that each set of the form $O_{i_1} \times O_{i_2} \times \ldots \times O_{i_n}$ is block for $A \wr B$. It follows that the number of orbits of $A \wr B$ on $X^n$ is equal to the number of orbits when $B$ acts on $O^n$ by simply permuting the coordinates. To calculate the number of orbits on $B$ on $O^n$, use Cauchy-Frobenius theorem, and observe that an element $b \in B$ fixes exactly $m^c(b)$ elements from $O^n$, that is for each cycle of $b$, the orbits $O_i$ on the corresponding coordinates must be the same. □

**Theorem 9.13.** Suppose $A$ and $B$ are finite groups where $A$ acts on a set $X$ and $B$ acts on the set $\{1, \ldots, n\}$. The wreath product $AwrB$ acts primitively in product action on $X^n$ if and only if $B$ is transitive and $A$ is primitive and not regular on $X$.

*Proof.* Let $G = AwrB$. Let $T = \{((a_1, \ldots, a_n), 1_B) \mid a_i \in A\} \cong A^n$ and $B_0 = \{((1_A, \ldots, 1_A), b) \mid b \in B\} \cong B$. Then $G = TB_0$. Let $x \in X$ be arbitrary. Let $L$ be the stabilizer in $G$ of $(x, \ldots, x)$. Then $L = \{((a_1, \ldots, a_n), b) \mid a_i \in A_x, b \in B\}$. By Corollary 5.21 $G$ is primitive if and only if $L$ is maximal subgroup of $G$.

Suppose first that $G$ acts primitively. Suppose that $B$ is not transitive. Let $S$ be an orbit of $B$. Let $M = \{((a_1, \ldots, a_n), 1_B) \mid a_i \in A_x, \text{ for } i \in S, \ a_i \in A \text{ for } i \in \{1, \ldots, n\} \setminus S\}$. Then $L < MB_0 < G$, and hence $G$ is not primitive. If $A$ is intransitive, then $G$ is also intransitive. Suppose now that $A$ is transitive but imprimitive. Then there exists $A' < A$ such that $A_x < A' < A$. The subgroup $\{((a_1, \ldots, a_n), b) \mid a_i \in A', b \in B\}$ lies strictly between $L$ and $G$, contradicting the assumption that $G$ is primitive. Finally, in the case when $A$ is regular, the subgroup $D = \{((a, \ldots, a), 1_B) \mid a \in A\}$ is normalized by $B_0$ and then $L < DB_0 < G$, a contradiction.

Suppose now that $B$ is transitive, and $A$ is primitive but not regular. Clearly, $T$ is transitive, hence $G$ is transitive. Thus it is enough to show that $L < M \leq G$ implies $M = G$. Since $G = TB_0 = TL$ we have $M = (M \cap T)L$. Therefore $M \cap T > L \cap T$. This implies that there exists $j \in \{1, \ldots, n\}$ such that $((a_1, \ldots, a_n), 1) \in M \cap T$ with $a_j \notin A_x$. Denote $a = (a_1, \ldots, a_n)$. Since $A$ is primitive and not regular, then $A_x = N_A(A_x)$ (see Exercise 9.14), and therefore for some $u \in A_x$ we have $a_j^{-1} u a_j \notin A_x$. Let $t \in A^n$, with $u$ on $j$-th coordinate and remaining ones, that is $t = (1, \ldots, u, 1, \ldots, 1)$. Let $h = [a, t] = a^{-1}t^{-1}at$. Then $(h, 1) \in ML = M$, and $h_j = [a_j, u] \in AA_x$, $h_i = 1$ for $i \neq j$. Since $A$ is primitive, $A_x$ is maximal, and so $A = \langle A_x, h_j \rangle$; therefore $M$ contains subgroup

$$T(j) = \{(f, 1) \mid f \in A^n, f_i = 1 \text{ for all } i \neq j\}.$$

It is easy to see that $(1, b)T(j)(1, b)^{-1} = T(j^b)$. Since $B_0 \leq M$ and $B$ is transitive on $\{1, \ldots, n\}$ we conclude that $T(i) \leq M$, for all $i \in \{1, \ldots, n\}$. This implies that

$$T = \prod T(i) \leq M$$

and so $M = TB_0 = G$ as required. □

**Exercise 9.14.** Show that a primitive group $G$ is not regular if and only if a point stabilizer $G_x$ equals its normalizer $N_G(G_x)$.

# 10 Multiply transitive permutation groups

Let $X$ be a set. Elements $(x_1, \ldots, x_k)$ in $X^k$ are also called **$k$-tuples**. We denote by $X^{(k)}$ the set of all $k$-tuples $(x_1, \ldots, x_k)$ such that $x_i \neq x_j$ for all $i, j \in \{1, \ldots, n\}$, $i \neq j$. Note that, if $|X| = n$ and $k \in \{1, \ldots, n\}$, then

$$\left|X^{(k)}\right| = n(n-1)\cdots(n-k+1).$$

Let $G$ act on $X$. Then it is easily seen that $G$ acts on the set $X^{(k)}$, $1 \leq k \leq |X|$, as

$$(x_1, \ldots, x_k)^g = (x_1^g, \ldots, x_k^g), \quad (x_1, \ldots, x_k) \in X^{(k)},\ g \in G.$$

To this action we refer to as the **canonical action of $G$ on $X^{(k)}$**.

**Example 10.1.** Let $X = \{1, 2, 3, 4\}$ and $G = S_4$. The canonical action of $G$ on $X^{(2)}$ is faithful and transitive. We denote by $\rho\colon G \to \mathrm{Sym}(X^{(2)})$ the permutation representation corresponding to the canonical action of $G$ on $X^{(2)}$, and write $ij$ for the pair $(i, j)$ in $X^{(2)}$. For example, if $g = (1, 2, 3, 4) \in G$ then

$$\rho(g) = (12, 23, 34, 41)(13, 24, 31, 42)(14, 21, 32, 43).$$

The action is faithful means that its kernel $\ker(\rho)$ is the trivial group. Let $g \in \ker(\rho)$. Then $ij^{\,g} = ij$ for all $ij \in X^{(2)}$. Thus $g = \mathrm{id}$ in $S_4$, $\ker(\rho)$ is the trivial group.

We determine the stabilizer $G_{12}$ in the action of $G$ on $X^{(2)}$. Then $g \in G_{12}$ if and only if $1^g = 1$ and $2^g = 2$. From this we easily obtain $G_{12} = \langle (3, 4) \rangle$. OSL implies $|12^{\,G}| = |G|/|G_{12}| = 24/2 = 12$. Hence $12^{\,G} = X^{(2)}$, $G$ is transitive on $X^{(2)}$. □

**Definition 10.2.** Let $G$ act on $X, |X| = n$, and let $k \in \{1, \ldots, n\}$. The group $G$ is called **$k$-transitive** on $X$ if the canonical action of $G$ on $X^{(k)}$ is transitive.

Note that, the group $G$ is 1-transitive means that $G$ is transitive. Let $G$ act on $X$. We say that $G$ is **multiply transitive** on $X$ if its canonical action on the set $X^{(k)}$ is transitive for some $k \geq 2$.

**Example 10.3.** $A_n, n \geq 3$, is $(n-2)$-transitive on $\{1, 2, \ldots, n\}$. Let $G = A_n$ and let $X = \{1, 2, \ldots, n\}^{(n-2)}$. A simple calculation gives $|X| = n!/2$. Let $x = (1, 2, \ldots, n-2) \in X$. The stabilizer $G_x$ is trivial. OSL implies $|x^G| = |G| = |X|$, hence $G$ is transitive on $X$. □

**Theorem 10.4.** Let $G$ be a $k$-transitive permutation group of $X$ with $k \geq 2$, and let $x \in X$.

(1) $G$ is also $(k-1)$-transitive.

(2) $G_x$ is $(k-1)$-transitive on $X \setminus \{x\}$.

(3) $|G| \geq n(n-1)\cdots(n-k+1)$, where $|X| = n$.

(4) $G$ is primitive.

*Proof.* (1)-(2) are left for exercise.

(3): OSL implies $|G| = n \cdot |G_x|$. Because of (2) the stabilizer $G_x$ is $(k-1)$-transitive on $X \setminus \{x\}$, and thus $|G| = n(n-1) \cdot G_{x_1,x_2}$, where $x_1 = x$ and $x_2 \neq x_1$. Applying this argument repeatedly we obtain that

$$|G| = n(n-1)\cdots(n-k+1) \cdot |G_{x_1,\ldots,x_k}|,$$

where $x_1, x_2, \ldots, x_k$ are distinct elements in $X$. Now $|G| \geq n(n-1)\cdots(n-k+1)$ follows.

(4): We need to prove that every block of $G$ is trivial. Let $B$ be a block which contains $x$, but $B \neq \{x\}$. Since $B$ is a block, it is a union of orbits of $G_x$ (see Proposition 5.22). As $G_x$ is transitive on $X \setminus \{x\}$, it has orbits: $\{x\}$ and $X \setminus \{x\}$. Thus $B = X$, and so $B$ is trivial. □

**Definition 10.5.** A permutation group $G$ of degree $n$ is **sharply $k$-transitive** if $G$ is $k$-transitive and $|G| = n(n-1)\cdots(n-k+1)$.

The following result is useful when proving that a given permutation group is $(k+1)$-transitive.

**Theorem 10.6.** Let $G$ be a transitive permutation group of $X$ such that $G_x$ $(x \in X)$ is $k$-transitive on $X \setminus \{x\}$. Then $G$ is also $(k+1)$-transitive.

*Proof.* We have to show that $G$ acts transitively on the set $X^{(k+1)}$. Let $\underline{x} = (x_1, \ldots, x_{k+1})$ and $\underline{y} = (y_1, \ldots, y_{k+1})$ be from $X^{(k+1)}$. Since $G$ is transitive, there exists $g_1, g_2 \in G$ such that $x_{k+1}^g = x$ and $x^{g_2} = y_{k+1}$. Since $G_x$ is $k$-transitive, there exsits $h \in G_x$ such that

$$(x_1^{g_1}, \ldots, x_k^{g_k})^h = (y_1^{g_2^{-1}}, \ldots, y_k^{g_2^{-1}}).$$

Then $\underline{x}^{g_1 h g_2} = (x_1^{g_1}, \ldots, x_k^{g_1}, x)^{hg_2} = (y_1^{g_2^{-1}}, \ldots, y_k^{g_2^{-1}}, x)^{g_2} = \underline{y}$. This concludes the proof. □

**Exercise 10.7.** Prove that the group $AGL(1,p)$ is sharply 2-transitive.

**Exercise 10.8.** If $G$ is a transitive permutation group on a set $X$, then $G$ is 2-transitive on $X$ if and only if

$$\frac{1}{|G|} \sum_{g \in G} |fix_X(g)|^2 = 2.$$

## 10.1 Regular normal subgroups

In this part we determine the regular normal subgroups of multiply transitive permutation groups.

First, we study regular normal subgroups of an arbitrary permutation group.

**Lemma 10.9.** Let $G$ be a permutation group of $X$, and let $N$ be a regular normal subgroup of $G$. Then there exists a subgroup $A \leq \mathrm{Aut}(N)$ such that the restriction of $G_x$ $(x \in X)$ to $X \setminus \{x\}$ is permutation isomorphic to the restriction of $A$ to $N \setminus \{1_N\}$.

*Proof.* Define a mapping $f\colon N \to X$ as $f\colon n \mapsto x^n$, $n \in N$. Since $N$ is regular, the mapping $f$ is bijective. Then an action of $G$ on $N$ is defined by

$$n^g = f^{-1}(x^{ng}), \quad n \in N,\ g \in G.$$

Denote by $\rho$ the corresponding permutation representation, i.e., $\rho\colon G \to \mathrm{Sym}(N)$ is a homomorphism. Let $g \in \ker(\rho)$. This means $n^g = n$ for all $n$. Then $x^n = f(n) = f(n^g) = x^{ng} = (x^n)^g$, and so $g = \mathrm{id}_X$. Thus $\ker(\rho)$ is trivial, and $\rho$ is an isomorphism from $G$ to the permuation group $\rho(G) \leq \mathrm{Sym}(N)$. Then $f^{-1}$ is a bijective mapping from $X$ to $N$ such that we have the property that for all $n \in N$ and $g \in G$,

$$f^{-1}((x^n)^g) = (f^{-1}(x^n))^{\rho(g)}.$$

This is the same as for all $y \in X$ and $g \in G$,

$$f^{-1}(y^g) = (f^{-1}(y))^{\rho(g)}.$$

This means that $G$ is permutation isomorphic to $\rho(G)$.

Let $g \in G_x$. Then because of $N$ is a normal subgroup in $G$, $g^{-1}ng \in N$, and hence

$$n^{\rho(g)} = n^g = f^{-1}(x^{ng}) = f^{-1}(x^{g^{-1}ng}) = g^{-1}ng.$$

This implies that $\rho(g) \in \mathrm{Aut}(N)$. Thus $\rho(G_x) \leq \mathrm{Aut}(N)$, and the lemma holds with $A = \rho(G_x)$.

□

**Theorem 10.10.** Let $G$ be a $k$-transitive permutation group of $X$ with $k \geq 2$, and let $N$ be a regular normal subgroup of $G$.

(1) If $k = 2$ then $N \cong \mathbb{Z}_p^n$, where $p$ is a prime.

(2) If $k = 3$ then $N \cong \mathbb{Z}_2^n$ or $N \cong \mathbb{Z}_3$.

(3) If $k = 4$ then $N \cong \mathbb{Z}_2^2$.

*Proof.* Because of part (2) in Theorem 10.4 the stabilizer $G_x$ is $(k-1)$-transitive. Let $A$ be the subgroup of $Aut(N)$ described in Lemma 10.9. Then $A$ is $(k-1)$-transitive on $N \setminus \{1_N\}$.

(1): According to Cauchy Theorem there exists $n_1 \in N$ with $\mathrm{ord}(n_1) = p$, where $p$ is a prime. Let $n \in N$, $n \neq 1_H$. Then $n = n_1^\alpha$ for some $\alpha \in A$, and so $\mathrm{ord}(n) = \mathrm{ord}(n_1) = p$. We obtain that $N$ is a $p$-group. Thus the center $\mathbf{Z}(N)$ is nontrivial. Let $n \in \mathbf{Z}(N), n \neq 1_H$. Then $n^\alpha \in \mathbf{Z}(N)$ for all $\alpha \in A$ hence $\mathbf{Z}(N) = N$, and so $N$ is an abelian group. As any abelian $p$-group is the direct product of cyclic groups of $p$-power order, we conclude that $N \cong \mathbb{Z}_p^n$.

(2): Now $A$ is 2-transitive on $N \setminus \{1_N\}$, hence it is primitive. It can be seen that for $n \in N \setminus \{1_N\}$ the set $\{n, n^{-1}\}$ is block for $A$. As $A$ is primitive, $\{n, n^{-1}\} = \{n\}$ for all $n$, or $\{n, n^{-1}\} = N \setminus \{1_H\}$. In the first case $p = 2$ and $N \cong \mathbb{Z}_2^n$, in the second case $p = 3$ and $N \cong \mathbb{Z}_3$.

(3): Because of (2) $N \cong \mathbb{Z}_2^n$, $n \geq 2$. Let $\{1_N, n_1, n_2, n_1n_2\}$ be a subgroup of $N$. Now $A_{n_1}$ is 2-transitive on $N \setminus \{1_N, n_1\}$, hence it is primitive. It can be seen that for $n \in N \setminus \{1_N, n_1\}$ the set $\{n, n_1n\}$, is block for $A_{n_1}$. In particular, $\{n_2, n_1n_2\}$ is a block. Hence $\{n_2, n_1n_2\} = N \setminus \{1_H, n_1\}$, and so $N = \{1_N, n_1, n_2, n_1n_2\}$, $N \cong \mathbb{Z}_2^2$.

□

**Exercise 10.11.** Let $G$ be a group acting 4-transitively on $X$ admitting a regular normal subgroup $N$. Determine all the possibilities for $G$.

*Proof.* By Theorem 10.10, it follows that $N \cong \mathbb{Z}_2^2$. Then using Lemma 10.9, it follows that $G \cong \mathbb{Z}_2^2 \rtimes A$, where $A \leq Aut(\mathbb{Z}_2^2)$ and $A$ acts 3-transitively on $\mathbb{Z}_2^2 \setminus \{1\}$. Since $Aut(\mathbb{Z}_2^2) = GL(2,2)$, it follows that $A \leq GL(2,2)$. It is now easy to see that $A = GL(2,2)$ and hence $G \cong \mathbb{Z}_2^2 \rtimes GL(2,2)$. □

As an application of Theorem 10.10 we give a short proof of the simplicity of the alternating group $A_n, n \geq 5$. We shall need the following lemma.

**Lemma 10.12.** Let $G$ be a primitive permutation group of $X$, such that $G_x$ $(x \in X)$ is a simple group. Then $G$ is a simple group or it has a regular normal subgroup.

*Proof.* We assume that $G$ is not a simple group, and choose a nonrivial normal subgroup $N$, such that $N < G$. Because of Theorem 5.26, $N$ is transitive. Thus $NG_x = G$. Then $N_x = G_x \cap N$, and $N_x \lhd G_x$. As $G_x$ is a simple group, $|N_x| = 1$ or $N_x = G_x$. In the second case $G_x \leq N$, and $N = NG_x = G$, which is a contradiction to $N < G$. Thus $|N_x| = 1$. This implies that $N_y = 1$ for all $y \in X$. We obtain that $N$ is both transitive and semiregular on $X$, i.e., $N$ is a regular subgroup. □

**Theorem 10.13.** If $n \geq 5$ then $A_n$ is a simple group.

*Proof.* We prove the theorem by induction on $n$. The case $n = 5$ is left for exercise. Let $n \geq 6$. The permutation group $A_n$ is $(n-2)$-transitive (see Example 10.3), hence it is primtive. The stabilizer $(A_n)_n$ is isomorphic to $A_{n-1}$. By the induction hypothesis we may assume that $(A_n)_n$ is a simple group, and we may apply Lemma 10.12. It follows that $A_n$ is simple or it has a regular normal subgroup. The group $A_n$ is $(n-2)$-transitive. Theorem 10.10 implies that $A_n$ cannot have a regular normal subgroup. Thus Lemma 10.12 implies that $A_n$ is a simple group. □

# 11 Rank of permutation group

Before introducing the definition of the rank of a permutation group, we are first going to prove the following.

**Proposition 11.1.** Let $G$ be a transitive permutation group on a set $X$ and let $x, y \in X$. The number of orbits of $G_x$ on $X$ equals to the number of orbits of $G_y$ on $X$.

*Proof.* Since $G$ is transitive on $X$, it follows that $y = x^g$, for some $g \in G$. Then $G_y = g^{-1}G_x g$. Let $O$ be an arbitrary orbit of $G_x$, that is $O = z^{G_x} = \{z^a \mid a \in G_x\}$. Permutation $g$ maps $O$ to

$$O^g = \{z^{ag} \mid a \in G_x\} = \{(z^g)^{g^{-1}ag} \mid a \in G_x\} = \{(z^g)^b \mid b \in G_y\} = (z^g)^{G_y}.$$

We proved that $z^{G_x} = (z^g)^{G_y}$, for every $z \in X$. This means that $g$ defines a mapping $\overline{g}$ from the set of orbits of $G_x$ to the set of orbits of $G_y$, that is

$$\overline{g} : z^{G_x} \mapsto (z^g)^{G_y}.$$

It remains to prove that the mapping $\overline{g}$ is bijective. Since $G$ is permutation, it follows that $\overline{g}$ is surjective. Suppose that $(z_1^g)^{G_y} = (z_2^g)^{G_y}$ for some $z_1, z_2 \in X$. This means that $z_2^g = z_1^{gb}$, for some $b \in G_y$. Since $G_y = g^{-1}G_x g$ it follows that $b = g^{-1}ag$, for some $a \in G_x$, and therefore $z_2^g = z_1^{gb} = z_1^{g(g^{-1}ag)} = z_1^{ag}$. We conclude that $z_2^g = (z_1^a)^g$ which implies that $z_2 = z_1^a$. Hence $z_2^{G_x} = z_1^{aG_x} = z_1^{G_x}$, and we conclude that $\overline{g}$ is injective. This concludes the proof. □

**Definition 11.2. Rank** of a transitive permutation group $G \leq X$ is the number of orbits of $G_x$ on $X$.

**Theorem 11.3.** Rank $r$ of a transitive permutation group $G$ is

$$r = \frac{1}{|G|} \sum_{g \in G} |fix_X(g)|^2.$$

*Proof.* By the Cauchy-Frobenius theorem, we have

$$r = \frac{1}{|G_x|} \sum_{g \in G_x} |fix_X(g)|.$$

Summing over elements of $X$ we have

$$r|X| = \sum_{x \in X} \frac{1}{|G_x|} \sum_{g \in G_x} |fix_X(g)| = \frac{|X|}{|G|} \sum_{x \in X} \sum_{g \in G_x} |fix_X(g)|,$$

and hence we obtain

$$r = \frac{1}{|G|} \sum_{x \in X} \sum_{g \in G_x} |fix_X(g)|.$$

We claim that

$$\sum_{g \in G} |fix_X(g)|^2 = \sum_{x \in X} \sum_{g \in G_x} |fix_X(g)|.$$

If $g \notin G_x$, for any $x \in X$, then $|fix_X(g)| = 0$. On the other hand, if $|fix_X(g)| \neq 0$, then there are precisely $|fix_X(g)|$ values of $x \in X$, for which $g \in G_x$. This concludes the proof. □

**Exercise 11.4.** Prove that the transitive group $G \leq Sym(X)$ is 2-transitive if and only if rank of $G$ is 2.

**Exercise 11.5.** Determine the rank of following groups:

1. $S_n$;
2. $A_n$;
3. $D_{2n}$.

**Exercise 11.6.** Let $X = (V, E)$ be a graph, and let $G = Aut(X)$ its automorphism group. If $G$ is rank 3-group, then $X$ is strongly regular graph.

**Exercise 11.7.** Calculate the rank of of the wreath product $S_n \wr S_2$ with the product action of degree $n^2$.