UNIVERZA NA PRIMORSKEM
Fakulteta za matematiko, naravoslovje in informacijske tehnologije

# Algebraic Graph Theory

**doc. dr. Ademir Hujdurović**

DRUGO UČNO GRADIVO
41 strani

Matematika, dodiplomski študijski program

PRVA IZDAJA

Koper, 2018

# Contents

# Introduction

This is set of lecture notes on undergraduate course "Algebraic Graph Theory" 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 Algebraic Graph Theory. The material presented in these lecture notes is collected from different sources, books, lecture notes etc.

# 1 Preliminaries

## 1.1 Groups

In this section we review the background on group theory.

**Definition 1.1.** 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 1.2.** 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 1.3.** If $H$ and $K$ are subgroups of $G$, then also $H \cap K$ is a subgroup of $G$.

**Definition 1.4.** 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 1.5.** If $Hg_1$ and $Hg_2$ are cosets, then either $Hg_1 = Hg_2$ or $Hg_1 \cap Hg_2 = \emptyset$.

Exercise 1.5 implies that $G$ is a disjoint union of right cosets of $H$.

**Definition 1.6.** 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 1.7.** Let $p$ be a prime, and let $G$ be a group of order $p$. Prove that $G$ is cyclic group.

**Definition 1.8.** 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 1.9.** 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 1.10.** Prove that in an abelian group every subgroup is normal.

**Exercise 1.11.** Let $G$ be a group and $H$ an index 2 subgroup of $G$. Prove that $H$ is a normal subgroup of $G$.

**Exercise 1.12.** 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 1.13.** If $H$ and $K$ are subgroups of $G$ then we have that

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

**Exercise 1.14.** 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 1.15.** If $G$ is a group and $N \lhd G$, then the *factor group* $G/N$ is the group with elements $\{gN : g \in G\}$ and the group operation $(g_1N) * (g_2N) = (g_1g_2)N$.

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

**Exercise 1.16.** Prove that the factor group defined in Definition 1.15 is indeed a group.

**Definition 1.17.** 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 1.18.** Let $\varphi : G \to H$ be a homomorphism and let $K \leq G$. Prove that $\varphi(K) \leq H$.

**Definition 1.19.** 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 1.20.** Let $\varphi : G \to H$ be a homomorphism. Prove that $Ker(\varphi) \lhd G$.

**Definition 1.21.** 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 $G \cong H$.

## 1.2 Cyclic and dihedral groups

Let $n$ be a positive integer. With $C_n$ we will denote a cyclic 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 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 $n$-gone. One step rotation of the $n$-gon corresponds to the element $\rho$, and $\tau$ corresponds to a reflection of the $n$-gon.

## 1.3 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 1.22.** 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 1.23.** Prove that $G_1 \times G_2$ as defined above is indeed a group.

**Theorem 1.24.** 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 1.25.** 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 1.26.** 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 1.27.** 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 1.28.** The set $Aut(G)$ together with the operation of composition of functions is a group.

**Definition 1.29.** Two elements $x$ and $y$ in a group $G$ are said to be conjugate if there exists an element $g \in G$ such that $gxg^{-1} = y$. We often write $gxg^{-1} = x^g$.

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 $gHg^{-1} = K$. Again we will usually write $H^g = gHg^{-1}$. 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 1.30.** If $G$ is a group and $g \in G$, then the mapping $\varphi : G \to G$ defined with $\varphi(x) = gxg^{-1}$ is an automorphism of $G$.

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

**Exercise 1.31.** The set $Inn(G)$ of all inner automorphisms of $G$ is a normal subgroup of $Aut(G)$.

**Exercise 1.32.** Prove that $N$ is normal subgroup of $G$ if and only if $\varphi(N) = N$ for every $\varphi \in Inn(G)$.

**Definition 1.33.** 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 1.34.** If $N$ *char* $G$ then $N \lhd G$.

An important property of characteristic subgroup is the following:

**Exercise 1.35.** 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 1.36.** 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 1.37.** Prove that $\varphi$ defined as above is indeed a homomorphism that maps $H$ to $Aut(N)$.

Now using Theorem 1.36 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 1.38.** 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.

## 1.4 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 1.39.** Let $\circ$ denote the symbol for composition of functions, that is

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

Prove that $Sym(X)$ together with operation $\circ$ forms a group.

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

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 $g(x) = x$. Otherwise, we say $x$ is moved by $g$.

**Definition 1.40.** 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 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 1.41.** 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 $g(x_k) = x_1$, and $g(x_i) = x_{i+1}$ for all $i \in \{1, \ldots, k-1\}$, and $g(x) = x$ for all $x \in X \setminus \{x_1, \ldots, x_k\}$.

Notation. We denote by $(x_1\ x_2\ \ldots\ x_k)$ the $k$-cycle $g$ in Definition 1.41.

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

**Example 1.42.** 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 1.43.** (**Cyclic Decomposition**) Every permutation $g \in Sym(X)$ can be written as the product of disjoint cycles. Factorization is unique up to the order of factors.

**Corollary 1.44.** Every permutation can be written as the product of transpositions.

*Proof.* It is clear that

$$(a_1\ a_2\ \ldots\ a_r) = (a_1\ a_r)(a_1\ a_{r-1}) \ldots (a_1\ a_2).$$

By Theorem 1.43 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. □

**Exercise 1.45.** Let $g, h \in \mathrm{Sym}(X)$, such that $g$ has a cyclic decomposition

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

Then $hgh^{-1}$ has a cylic decomposition

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

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** $[c_1, \ldots, c_n]$ if a maximal cyclic decomposition of $g$ consists of $c_k$ number of $k$-cycles, where $k \in \{1, \ldots, n\}$. Note that, the equality $c_1 + 2c_2 + \cdots + nc_n = n$ always holds. The following corollary of Theorem 1.45 is useful when studying the conjugacy of two permutations.

**Corollary 1.46.** 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.

**Exercise 1.47.** 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 $hg_1h^{-1} = g_2$.

## 1.5 Alternating group $A_n$

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

**Definition 1.49.** A permutation $g \in S_n$ is called **even (odd)** if $g$ is the product of even (odd) number of transpositions.

**Exercise 1.50.** 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 1.51.** 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 $S_n$, $A_n \lhd S_n$.

**Exercise 1.52.** 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 1.53.** 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 1.54.** Prove that the group $A_n$ ($n \geq 3$) is generated by the set of all cycles of length 3.

**Exercise 1.55.** Prove that $A_4$ has no subgroup of order 6. (Hint: Use Exercises 1.11 and 1.13).

*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 1.11 $N$ 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 1.13 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. □

## 1.6 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 1.56.** An **action** of a group $G$ on a set $X$ is a mapping $f\colon G \times X \to X$ such that, writing the image $f((x, g))$ as $g \cdot x$, the following properties hold.

A1. $1_G \cdot x = x$ for every $x \in X$.

A2. $(g_1 g_2) \cdot x = g_1 \cdot (g_2 \cdot x)$ 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. Instead of $g \cdot x$ we will sometimes write $gx$ or $g(x)$.

**Example 1.57.** Let $G = \mathbb{R} \setminus \{0\}$ 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 $g \cdot (x_1, x_2, x_3) = (gx_1, gx_2, gx_3)$, for $(x_1, x_2, x_3) \in \mathbb{R}^3$ and $g \in \mathbb{R} \setminus \{0\}$.

**Example 1.58.** Let $G \leq Sym(X)$. Then $G$ acts naturally on $X$ with $g \cdot x = g(x)$, for $x \in X$ and $g \in G$.

**Example 1.59.** Let $G$ be the group acting on a set $X$. Then $G$ acts on the set $X \times X$ with $g \cdot (x_1, x_2) = (g \cdot x_1, g \cdot x_2)$.

**Theorem 1.60.** Let $G$ act on $X$ and fix $g \in G$.

(1) The mapping $\pi_g : X \to X$, $\pi_g : x \mapsto g(x)$ 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 $g \cdot x := \Phi(g)(x)$.

**Definition 1.61.** For an action of a group $G$ on a set $X$ we call the homomorphism $\rho$ in Theorem 1.60 the corresponding **permutation representation of $G$ on $X$**. The **degree** of an action (or a premutation representation) is the size of $X$.

**Definition 1.62.** 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 1.63.** 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 $g \cdot \overline{x_1x_2} = \overline{g(x_1)g(x_2)}$. Determine the image and the kernel of this action. Is this action faithful?

Now we jump to a more theoretical example.

**Theorem 1.64.** Let $G$ be a group, and let us take $X$ to be $G$. Then $G$ acts on $X$ with

$$g \cdot x = gx, \quad x, g \in G.$$

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 $x \in X$, $1_G \cdot x = 1_G x = x$.

A2: For every $x \in X$ and for every $g_1, g_2 \in G$, $(g_1g_2) \cdot x = g_1g_2x = (g_1)(g_2x) = g_1 \cdot (g_2 \cdot x)$.

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

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

**Theorem 1.65** (Cayley)**.** Every group is isomorphic to a permutation group.

*Proof.* Let $G$ be a group. Let $G$ act on $X = G$ via left multiplication. By Theorem 1.60, it follows that $\rho : G \to Sym(X)$ is a group homomorphism (recall that $\rho(g) = \pi_g$, and $\pi_g(x) = gx$ 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 1.65 it follows that $Ker(\rho) = \{1_G\}$ it follows that $G \cong \rho(G)$. □

## 1.7 Orbits and stabilizers

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

**Definition 1.66.** Let $G$ act on $X$, and let $x \in X$. The **orbit of $G$ induced by** $x$ is the set $\{g \cdot x \mid g \in G\}$.

Notation. We denote by $Orb_G(x)$ the orbit of $G$ induced by $x$.

**Definition 1.67.** Let $G$ act on $X$, and let $x \in X$. The **stabilizer of $x$ in $G$** is the set $\{g \in G \mid g \cdot x = x\}$.

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

**Example 1.68.** 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 1.69.** Let $G$ act on $X$ and let $x \in X$.

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

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

**Proposition 1.70.** Let $G$ act on a set $X$, let $g \in G$, $x \in X$ and let $y = g \cdot x$. Then

$$G_y = gG_xg^{-1}.$$

*Proof.*

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

□

**Theorem 1.71** (Orbit-stabilizer)**.** Let $G$ be a group acting on a set $X$. Then for every $x \in X$ it holds $|G| = |Orb_G(x)| \cdot |G_x|$.

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

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

Second, we obtain that

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

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

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

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

$$|\Omega| = \sum_{y \in Orb_G(x)} |G_x| = |Orb_G(x)| \cdot |G_x|.$$

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

□

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

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

**Proposition 1.72.** The conjugation action of a group $G$ on $G$ is well-defined group action. For $g \in G$, the orbit $ORb_G(g)$ 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 1.73.** Does group $G$ act on $G$ with

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

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 left $H$-cosets in $G$ defined with

$$g \cdot (xH) = gxH, \quad x, g \in G.$$

**Proposition 1.74.** The coset action is indeed an action. The stabilizer of $xH$ is $G_{xH} = xHx^{-1}$. The kernel is $\cap_{x \in G} xHx^{-1}$.

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

**Exercise 1.75.** Prove that $\text{core}_G(H)$ is the largest normal subgroup of $G$ which is contained in $H$.

**Exercise 1.76.** 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.

## 1.8 Transitive, semiregular and regular group actions

**Definition 1.77.** 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 1.78.** Left regular representation of $G$, that is the action of $G$ on $G$ given with $g \cdot x = gx$ is regular action.

**Proposition 1.79.** Let $G$ act transitively on $X$. Then cardinality $|X|$ is a divisor of $|G|$.

**Proposition 1.80.** Let $G$ act transitively on $X$. Then $G$ is regular if and only if $|G| = |X|$.

**Proposition 1.81.** 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 $Orb_G(x) = X$. Using Proposition 1.70 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 1.82.** 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 1.83.** Let $G$ be a group. Prove that the direct product $G \times G$ acts on $G$ with $(g_1, g_2) \cdot x = g_1 x g_2^{-1}$. Prove that this action is transitive, and calculate the vertex stabilizer $(G \times G)_1$. When is this action faithful?

**Exercise 1.84.** Let $G$ act transitively on $X$ and let $H \leq G$. Prove that $G = HG_x$ if and only if $H$ is transitive.

## 1.9 Counting orbits

**Definition 1.85.** 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 $fix_X(g) = \{x \in X \mid g \cdot x = x\}$. 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 1.86** (Cauchy-Frobenius or Burnside)**.** 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 $\Omega = \{(x, g) \in X \times G \mid gx = x\}$. 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

$$|\Omega| = \sum_{i=1}^{m} |\{(x, g) \in X_i \times G \mid gx = x\}|. \tag{2}$$

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

$$|\Omega| = \sum_{i=1}^{m} \sum_{x \in X_i} |G_x| = \sum_{i=1}^{m} \sum_{x \in X_i} \frac{|G|}{|X_i|} = \sum_{i=1}^{m} |G| = m|G|. \tag{3}$$

On the other hand we have

$$|\Omega| = \sum_{g \in G} |\{(x, g) \in X \times G \mid gx = x\}| = \sum_{g \in G} |fix(g)|. \tag{4}$$

Combining (3) and (4) the result follows. □

**Corollary 1.87.** 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 $fix(g) = \emptyset$. □

## 1.10 Cycle index of permutation group

**Definition 1.88.** 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 1.89.** Calculate $Z_{S_3}$.

**Exercise 1.90.** Calculate $Z_{S_4}$.

**Exercise 1.91.** Prove that $Z_{C_n} = \frac{1}{n} \sum_{d|n} \varphi(d) x_d^{n/d}$.

**Exercise 1.92.** Prove that $Z_{D_n} = \frac{1}{2} Z_{C_n} + \begin{cases} \frac{1}{2} x_1 x_2^{(n-1)/2}, & n \text{ odd}, \\ \frac{1}{4} \left( x_1^2 x_2^{(n-2)/2} + x_2^{n/2} \right), & n \text{ even}. \end{cases}$

**Exercise 1.93.** 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 $n$.

## 1.11 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 1.94.** 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 $g \cdot f = f \circ g^{-1}$. 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 1.95** (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 $g$. $\square$

# 2 Graphs

A graph $\Gamma$ consist of *vertex* set $V(\Gamma)$ and *edge* set $E(\Gamma)$, where an edge is an unordered pair of distinct vertices $\{u, v\}$. We will sometimes write $uv$ instead of $\{u, v\}$. If $\{u, v\}$ is an edge, we say that $u$ and $v$ are *adjacent* and that $v$ is a *neighbour* of $u$, and we will denote this by $u \sim v$. A set $\Gamma(v)$ denotes the set of all neighbours of $v$, that is $\Gamma(v) = \{u \in V(\Gamma) : u \sim v\}$. *Degree* of a vertex $v \in V(\Gamma)$ is defined as the number of its neighbours, and is denoted by $d_\Gamma(v)$, that is $d_\Gamma(v) = |\Gamma(v)|$. If the graph $\Gamma$ is clear from context, then we simply write $d(v)$. Order of a graph is the cardinality of its vertex-set.

Two graphs $X_1 = (V_1, E_1)$ and $X_2 = (V_2, E_2)$ are *equal* if $V_1 = V_2$ and $E_1 = E_2$. Although this is a reasonable definition, for most purposes, the model of relationship is not changed if we rename the vertices of a graph. This naturally leads to the definition of *isomorphic graphs*.

**Definition 2.1.** For graphs $X$ and $Y$, a function $\varphi : V(X) \to V(Y)$ is called *isomorphism* from $X$ to $Y$, if

1. $\varphi$ is bijection;
2. $\forall u, v \in V(X)\ \{u, v\} \in E(X) \Leftrightarrow \{\varphi(u), \varphi(v)\} \in E(Y)$.

Graphs $X$ and $Y$ are called isomorphic if there exist an isomorphism from $X$ to $Y$, and we denote this by $X \cong Y$.

For a function $\varphi : A \to B$ and for a subset $S \subseteq A$ we define $\varphi(S) = \{\varphi(s) : s \in S\}$.

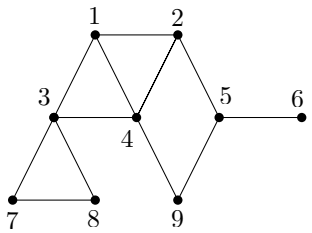
**Lemma 2.2.** Let $\varphi$ be an isomorphism from $X$ to $Y$. Then for every $v \in V(X)$, we have $\varphi(X(v)) = Y(\varphi(v))$.

**Corollary 2.3.** Isomorphisms preserve degrees of vertices, that is for an isomorphism $\varphi$ from $X$ to $Y$ we have $d_X(v) = d_Y(\varphi(v))$, $\forall v \in V$.

One can also consider isomorphism from a graph $\Gamma$ to itself. In this case, instead of "isomorphism" we use word "automorphism". We repeat the definition to stress its importance.

**Definition 2.4.** Let $\Gamma$ be a graph. An *automorphism* of $\Gamma$ is a **bijective** function $\varphi : V(X) \to V(X)$ such that $\forall u, v \in V(X)$ we have $\{u, v\} \in E(\Gamma) \Leftrightarrow \{\varphi(u), \varphi(v)\} \in E(\Gamma)$. The set of all automorphisms of a graph $\Gamma$ is denoted by $\mathrm{Aut}(\Gamma)$.

**Exercise 2.5.** Determine all the automorphisms of the following graph.




**Theorem 2.6.** For a graph $\Gamma$, the set $\mathrm{Aut}(\Gamma)$ is group under the operation of composition of functions, that is for $f, g \in \mathrm{Aut}(\Gamma)$, $fg = f \circ g$, or equivalently $(fg)(v) = f(g(v))$ for every $v \in V(\Gamma)$.

**Definition 2.7.** The complement $\overline{\Gamma}$ of a graph $\Gamma$ is the graph with $V(\overline{\Gamma}) = V(\Gamma)$ and for every two distinct vertices $u, v \in V(\Gamma)$ we have $\{u, v\} \in E(\overline{\Gamma}) \Leftrightarrow \{u, v\} \notin E(\Gamma)$.

**Lemma 2.8.** For every graph $\Gamma$ we have $\mathrm{Aut}(\Gamma) = \mathrm{Aut}(\overline{\Gamma})$.

A graph $\Gamma$ is called *asymmetric* if $\mathrm{Aut}(\Gamma) = \{id\}$.

**Exercise 2.9.** For every positive integer $n \geq 6$ there exists an asymmetric graph with $n$ vertices.

## 2.1 Number of non-isomorphic graphs

In this section we will show how Polya's enumeration theorem can be used for determining the number of non-isomorphic graph of given order. We will first demonstrate this on graphs of order 4.

**Example 2.10.** 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 $V = \{1, 2, 3, 4\}$. Let $X = \{\{i, j\} \mid 1 \leq i < j \leq 4\}$. We can think of $X$ as the edge set of complete graph $K_4$. Let $C = \{w, b\}$. Consider the set $C^X$, that is set of all functions $f : X \to C$. For any such function $f$, one can define a graph $\Gamma_f$, with $E(\Gamma_f) = \{x \in X : f(x) = b\}$, or in other words $f$, is colors edges of $K_4$ with two colors ($w$ for white, and $b$ for black), the graph $\Gamma_f$ is the subgraph with all black edges. Conversely, for any graph $\Gamma$ with vertex set $V$, one can define a function $f_\Gamma : X \to C$, where $f_\Gamma(\{u, v\}) = 1$ if and only if $\{u, v\} \in E(\Gamma)$.

For a permutation $g \in S_4$, with $g^{(2)}$ we denote the permutation of $X$ induced by $g$, and with $S_n^{(2)}$ the corresponding permutation group of $X$. For example, if $g = (1\ 2)(3\ 4)$ then

$$g^{(2)} = (\{1, 2\})(\{3, 4\})(\{1, 3\}\ \{2, 4\})(\{1, 4\}\ \{2, 3\}).$$

It is now easy to see that two graphs with vertex set $V$ are isomorphic if and only if the corresponding collorings are equivalent under the action of $S_4^{(2)}$.

By Polya's theorem, the number of non-equivalent collorings is $Z_{S_4^{(2)}}(x_1 = x_2 = x_3 = x_4 = 2)$. It is left as exercise to calculate the cyclic index of $S_4^{(2)}$. □

**Exercise 2.11.** Let $g \in S_n$ be a permutation with $c_k$ cycles of length $k$. The number of cycles in the cyclic decomposition of $g^{(2)}$ is

$$\gamma(g) = \sum_{k=1}^{n} kc_{2k+1} + \sum_k kc_{2k} + \sum_k \frac{kc_k(c_k - 1)}{2} + \sum_{r<t} (r, t)c_r c_t.$$

**Exercise 2.12.** Let $V = \{1, \ldots, n\}$, let $X = \{\{i, j\} \mid 1 \leq i < j \leq n\}$. For $g \in S_n$ let $g^{(2)}$ denote the induced permutation of $X$ and let $\gamma(g)$ denote the number of cycles in cyclic decomposition of $g^{(2)}$. Prove that the number of non-isomorphic graphs of order $n$ is

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

**Definition 2.13.** 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 2.14.** Determine the number of non-isomorphic hypergraphs with $n$ vertices, for $n \in \{3, 4\}$.

## 2.2 Number of non-equivalent (proper) colourings

Suppose that we are given a graph $\Gamma$ and a set of colors $C$, and we want to color the vertices of $\Gamma$ with colors from $C$. For two such colourings $f_1$ and $f_2$ we will say that are equivalent, if there exist an automorphism $\varphi \in \mathrm{Aut}(\Gamma)$ such that $f_2 = f_1 \circ \varphi$. In other words, two colourings are equivalent, if one can be obtained from the other after applying an automorphism of the graph $\Gamma$. Note that here we are not talking about proper colourings, that is adjacent vertices can be coloured in the same way.

**Theorem 2.15.** The number of non-equivalent colourings of a graph $\Gamma$ of order $n$ with $m$ colors is given by $Z_{\mathrm{Aut}(G)}(x_1 = \ldots = x_n = m)$

**Example 2.16.** Determine the number of non-equivalent colourings of $C_8$ (cycle of length 8) with 3 colors.

**Definition 2.17.** A proper colouring of a graph $\Gamma$ with a set of colors $S$ is a function $f : V(\Gamma) \to C$ such that adjacent vertices have different colors, that is $\forall u, v \in V(\Gamma)$, $u \sim v \Rightarrow f(u) \neq f(v)$. A chromatic polynomial $\chi(\Gamma, k)$ of a graph $\Gamma$ counts the number of its proper vertex-colourings with $k$ colors, that is $\chi(\Gamma, k)$ is the number of proper colourings of $\Gamma$ with $k$ colors.

**Example 2.18.** Let $P_n$ be a path on $n$ vertices. Then $\chi(P_n, k) = k(k-1)^{n-1}$.

**Example 2.19.** Let $C_n$ be a cycle of length $n$ ($C_1$ is a loop with single vertex, and $C_2 \cong K_2$. Then $\chi(C_n, k) = (k-1)^n + (-1)^n(k-1)$.

*Proof.* By deletion-contraction formula, it follows that $\chi(C_n, k) = \chi(C_n - e, k) - \chi(C_n/e, k)$, where $C_n/e$ is the graph obtained by contracting edge $e$ of $C_n$. Observe that $C_n - e \cong P_n$ and $C_n/e \cong C_{n-1}$. Now use induction, and previous exercise. □

**Definition 2.20.** Let $\Gamma$ be a graph, and let $\mathcal{P}$ be a partition of $V(\Gamma)$. We defined a quotient graph of $\Gamma$ with respect to $\mathcal{P}$ to be the graph with vertex set $\mathcal{P}$ and with two elements $P_1, P_2 \in \mathcal{P}$ being adjacent if and only if there exist $u \in P_1$ and $v \in P_2$ such that $\{u, v\} \in E(\Gamma)$. **In this definition we allow loops as well, that is $P_1 = P_2$ is allowed**. The obtained graph is denoted by $\Gamma_{\mathcal{P}}$. For an automorphism $g \in \mathrm{Aut}(\Gamma)$, let $\mathcal{P}_g$ be the set of orbits of $\langle g \rangle$. The corresponding quotient graph is denoted by $\Gamma_g$.

**Remark 2.21.** If a graph $\Gamma$ contains a loop, then there is no proper colouring of $\Gamma$.

**Theorem 2.22.** The number of non-equivalent proper colourings of a graph $\Gamma$ with $k$ colors is equal to

$$\frac{1}{|\mathrm{Aut}(\Gamma)|} \sum_{g \in \mathrm{Aut}(\Gamma)} \chi(\Gamma_g, k).$$

In the case when $\Gamma \cong C_n$, then we have the following result about the number of non-equivalent proper colourings.

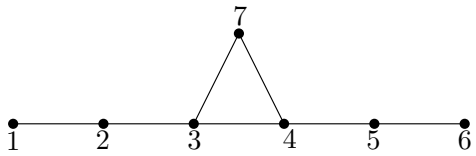
**Theorem 2.23.** Let $C_n$ be the cycle of length $n$. The number of non-equivalent proper colourings of $C_n$ with $k$ colors is equal to

$$\frac{1}{2n}\sum_{d|n}\varphi(d)\chi(C_{\frac{n}{d}},k) \text{ if n is odd },$$

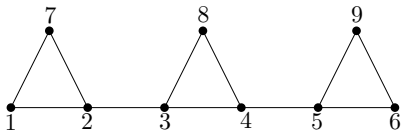
$$\frac{1}{2n}\left(\sum_{d|n}\varphi(d)\chi(C_{\frac{n}{d}},k)+\frac{n}{2}k(k-1)^{n/2}\right) \text{ if n is even}$$

**Exercise 2.24.** Let $X$ be the graph shown below.

- Find all automorphisms of $X$.
- Determine the number of non-equivalent proper colouring of $X$ with $k$ colors.




**Exercise 2.25.** Let $X$ be the graph shown below.




- Find all automorphisms of $X$.
- Determine the number of non-equivalent proper colouring of $X$ with $k$ colors.

# 3 Vertex-transitive graphs

**Definition 3.1.** A graph $\Gamma$ is said to be vertex-transitive if $\mathrm{Aut}(\Gamma)$ acts transitively on $V(\Gamma)$, that is $\forall u, v \in V(\Gamma)$, there exists $\varphi \in \mathrm{Aut}(\Gamma)$ such that $\varphi(u) = v$.

**Example 3.2.** The complete graph $K_n$ of order $n$, is vertex-transitive, for every $n \geq 1$.

**Example 3.3.** The graph $C_n$, cycle of length $n$ is vertex-transitive graph, for every $n \geq 3$.

We will now present some elementary properties of vertex-transitive graphs. Recall that a graph $\Gamma$ is said to be $d$-regular if all the vertices of $\Gamma$ have degree equal to $d$. If $\Gamma$ is $d$-regular for some $d$, then we say that $\Gamma$ is regular, and $d$ is called the valency of $\Gamma$.

**Proposition 3.4.** A graph $\Gamma$ is vertex-transitive if and only if its complement $\overline{\Gamma}$ is vertex-transitive.

*Proof.* The result follows from the fact that $\mathrm{Aut}(\Gamma) = \mathrm{Aut}(\overline{\Gamma})$. □

**Proposition 3.5.** Let $\Gamma$ be a vertex-transitive graph. Then $\Gamma$ is regular.

*Proof.* Let $u, v \in V(\Gamma)$. Since $\Gamma$ is vertex-transitive, it follows that there exists $\varphi \in \mathrm{Aut}(\Gamma)$ such that $\varphi(u) = v$. Then by Corollary 2.3 it follows that $d_\Gamma(u) = d_\Gamma(v)$, hence the result follows. □

We saw that every vertex-transitive graph is regular. The converse is not true, a graph which is regular does not need to be vertex-transitive.

**Example 3.6.** The graph shown on Figure 3.6 is not vertex-transitive. In fact it is the smallest (with respect to the number of vertices) connected regular graph which is not vertex-transitive. To see that this graph is not vertex-transitive, observe that its complement is disjoint union of $C_4$ and $C_3$.

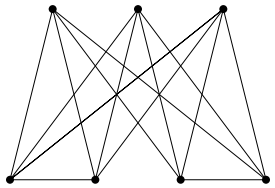


Figure 1: Example of a regular graph which is not vertex-transitive

## 3.1 Cayley graphs

**Definition 3.7.** Let $G$ be a finite group, $S \subset G$ such that $S$ does not contain $1_G$, and $S^{-1} = S$ (here $S^{-1} = \{x^{-1} : x \in S\}$. The **Cayley graph of $G$ with respect to $S$** denoted by $Cay(G, S)$ is the graph with vertex-set $G$, and two vertices $x, y \in G$ are adjacent if and only if $x^{-1}y \in S$. In other words $E(Cay(G, S)) = \{\{x, xs\} : x \in G, s \in S\}$. Set $S$ is called **the connections set** of $Cay(G, S)$.

**Example 3.8.** Let $n \geq 3$, and let $G = \mathbb{Z}_n$ be the cyclic group of order $n$. Let $S = \{1, n-1\}$. Then $Cay(G, S) \cong C_n$.

**Theorem 3.9.** Every Cayley graph is vertex-transitive.

*Proof.* Let $\Gamma = Cay(G, S)$. For $g \in G$, let $g_L : G \to G$ be the mapping defined by $g_L(x) = gx$. It is not difficult to see that for every $g \in G$, the mapping $g_L$ is an automorphism of $Cay(G, S)$ (verify this!). Now for any $x, y \in G$, take $g = yx^{-1}$. Observe that $g_L(x) = y$. Hence $Cay(G, S)$ is vertex-transitive graph. □

In fact we proved something stronger in previous theorem. For a group $G$, let $G_L = \{g_L : g \in G\}$. $G_L$ is called left regular representation of $G$. Observe that $G_L$ is a group, $G_L \leq Sym(G)$, and $G_L \cong G$. In previous theorem we proved that $G_L \leq \mathrm{Aut}(Cay(G, S))$.

**Exercise 3.10.** Prove that for every Cayley graph $Cay(G, S)$, the group $G_L$ is a regular subgroup of $\mathrm{Aut}(Cay(G, S))$.

**Exercise 3.11.** Prove that valency of $Cay(G, S)$ is equal to $|S|$.

**Exercise 3.12.** Let $X = Cay(\mathbb{Z}_{10}, \{\pm 2, 5\})$ and $Y = Cay(D_{10}, \{\rho, \rho^4, \tau\})$, where $D_{10}$ is dihedral group of order 10, that is, $D_{10} = \langle \rho, \tau \mid \rho^5 = \tau^2 = 1, \rho\tau = \tau\rho^{-1} \rangle$. Represent graphically graphs $X$ and $Y$ and check if $X$ and $Y$ are isomorphic.

**Lemma 3.13.** Cayley graph $Cay(G, S)$ is connected if and only if $\langle S \rangle = G$ (recall that $\langle S \rangle$ denotes the group generated by $S$).

*Proof.* Suppose that $\langle S \rangle = G$. Let $x, y \in G$, and $g = x^{-1}y$. Then there exists $s_1, \ldots, s_k \in S$ such that $s_1 \cdot s_2 \ldots \cdot s_k = g$. For $1 \leq i \leq k$, let $v_i = x \cdot s_1 \cdot \ldots s_i$. Observe that $v_k = x \cdot s_1 \ldots s_k = xg = x(x^{-1}y) = y$. This constructs a path from $x$ to $y$, $(x, v_1, \ldots, v_{k-1}, v_k = y)$ hence $Cay(G, S)$ is connected.

Suppose now that $Cay(G, S)$ is connected. Then for any $g \in G$, there exists a path $1, v_1, \ldots, v_k = g$. Since $v_i \sim v_{i+1}$ , it follows that $v_{i+1} = v_i s_i$ for some $s_i \in S$. Therefore, $g = v_k = v_{k-1}s_{k-1} = \ldots = s_1 \ldots s_{k-1}$, hence $\langle S \rangle = G$. □

For a graph $\Gamma$ with minimum degree at least 2, **girth** of $\Gamma$ is defined as the minimum number of vertices of a cycle in $\Gamma$.

**Example 3.14.** Let $\Gamma = Cay(G, S)$, where $G$ is abelian group and $|S| \geq 3$. Then girth of $\Gamma$ is at most 4.

*Proof.* Let $a, b, c$ be three distinct elements from $S$. If $a + b \neq 0$, then we obtain a 4-cycle, $0, a, a + b, b$. If $a + b = 0$, then $a + c \neq 0$, and hence we again obtain 4-cycle $0, a, a + c, c$. □

Recall that an automorphism of a group $G$ is a bijective function $\alpha : G \to G$ such that $\alpha(g_1 \cdot g_2) = \alpha(g_1) \cdot \alpha(g_2)$, for every $g_1, g_2 \in G$.

**Lemma 3.15.** Let $G$ be a finite group, $S$ an inverse closed subset of $G$, and $\alpha$ an automorphism of the group $G$. Then $Cay(G, S) \cong Cay(G, \alpha(S))$.

*Proof.* Since $\alpha$ is automorphism of the group $G$, it is bijective mapping of the vertex set of $Cay(G, S)$ into the vertex set of $Cay(G, \alpha(S))$. We leave the details for the reader to verify that $\alpha$ is also an isomorphism between these two graphs. □

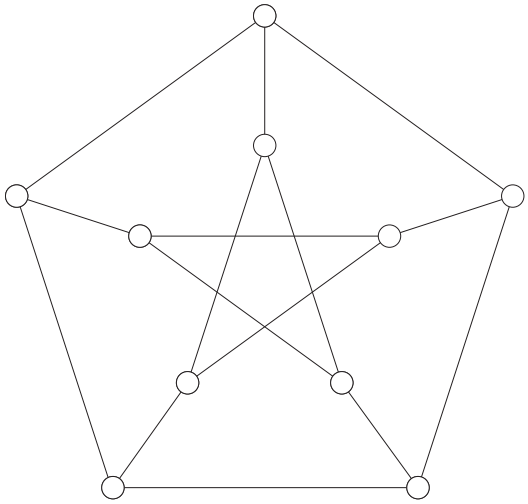


Figure 2: Petersen graph

**Corollary 3.16.** Let $G$ be a group, $S$ an inverse closed subset of $G$ and $\alpha \in \mathrm{Aut}(G)$. Then $\alpha \in \mathrm{Aut}(Cay(G,S))$ if and only if $\alpha(S) = S$.

We denote with $\mathrm{Aut}(G,S) = \{\alpha \in \mathrm{Aut}(G) \mid \alpha(S) = S\}$. The previous corollary shows that $\mathrm{Aut}(G,S)$ is a subgroup of $\mathrm{Aut}(Cay(G,S)$. Hence we have the following.

**Proposition 3.17.** Let $\Gamma = Cay(G,S)$. Then $\langle G_L, \mathrm{Aut}(G,S)\rangle \cong G_L \rtimes \mathrm{Aut}(G,S) \leq \mathrm{Aut}(\Gamma)$.

We have seen that every Cayley graph is vertex-transitive. But it is not true that every vertex-transitive graph is Cayley graph.

**Example 3.18.** Petersen graph shown on Figure 2 is vertex-transitive, but it is not a Cayley graph.

*Proof.* Suppose that there exists a group of $G$ order 10 such that $Cay(G,S)$ is isomorphic to the Petersen graph. Since Petersen graph is 3-valent, then $|S| = 3$. There are two non-isomorphic groups of order 10, $\mathbb{Z}_{10}$ and $D_{10}$. Observe that girth of the Petersen graph is 5. This shows that $G$ cannot be abelian, hence it remains to consider the case when $G = D_{10}$.

Recall that $D_{10} = \{1, \rho, \rho^2, \rho^3, \rho^4, \tau, \tau\rho, \tau\rho^2, \tau\rho^3, \tau\rho^4\}$. Since $S$ is inverse closed, it follows that it contains one or three involutions (elements of order 2). Suppose $S$ contains exactly one involution. Then without loss of generality, we may assume that $S = \{\rho, \rho^{-1}, \tau\}$ (verify this). Observe that the obtained graph is not isomorphic to the Petersen graph. The case when $S$ contains three involutions is left for exercise. □

**Exercise 3.19.** Prove that the automorphism group of the Petersen graph is isomorphic to $S_5$.

*Proof.* We will represent Petersen graph in the following way. Let $I = \{1,2,3,4,5\}$ and let $V = \{A : A \subset I \text{ and } |A| = 2\}$. For $A, B \in V$ we define that $A \sim B \Leftrightarrow A \cap B = \emptyset$. It is left for reader to verify that the graph obtained this way is isomorphic to the Petersen graph.

Let $A$ be the automorphism group of the Petersen graph. For $g \in S_5$, let $g^{(2)}$ denote the corresponding permutation of $V$. It is easy to see that $g^{(2)}$ is automorphism of the Petersen graph for every $g \in S_5$. Hence $S_5^{(2)} \leq A$. We claim that we have equality. We will use orbit stabilizer lemma several times to prove that $|A| = 120$, which will establish $A = S_5^{(2)} \cong S_5$.

By the orbit stabilizer lemma, it follows that

$$|A| = |A_{\{1,2\}}||Orb_A(\{1,2\})| = 10 \cdot |A_{\{1,2\}}|, \tag{5}$$

since Petersen graph is vertex-transitive. Let $G = A_{\{1,2\}}$. We now use orbit-stabilizer lemma for $G$ to obtain:

$$|G| = |G_{\{3,4\}}||Orb_G(\{3,4\})| = 3 \cdot |G_{\{3,4\}}|, \tag{6}$$

since $|Orb_G(\{3,4\})| = 3$ (To see this we can use elements of $S_5^{(2)}$). Let $H = G_{\{3,4\}}$. Use orbit-stabilizer lemma for $H$ to obtain:

$$|H| = |H_{\{4,5\}}||Orb_H(\{4,5\})| = 2 \cdot |H_{\{4,5\}}|, \tag{7}$$

since $Orb_H(\{4,5\}) = \{\{4,5\},\{3,5\}\}$. To see this one can use automorphism $g^{(2)}$ where $g = (3\ 4) \in S_5$. Let $K = H_{\{4,5\}}$. Use orbit-stabilizer lemma for $K$ to obtain

$$|K| = |K_{\{1,3\}}||Orb_K(\{1,3\})| = 2 \cdot |K_{\{1,3\}}|, \tag{8}$$

since $Orb_K(\{1,3\}) = \{\{1,3\},\{2,3\}\}$. To see this one can use automorphism $g^{(2)}$ where $g = (1\ 2) \in S_5$. Finally, we claim that $K_{\{1,3\}} = \{1_A\}$. Let $\alpha \in K_{\{1,3\}}$. Then $\alpha$ fixes vertices $\{1,2\}$, $\{3,4\}$, $\{4,5\}$ and $\{1,3\}$. Observe that $\{2,4\}$ is the unique common neighbour of $\{3,4\}$ and $\{1,3\}$. Hence it must be fixed by $\alpha$. Now it easy to see that $\alpha$ fixes every vertex. Combining the above equalities implies that $|A| = 120$. □

In the following theorem, we give necessary and sufficient conditions for a given graph to be a Cayley graph. Recall that a permutation group $G \leq Sym(V)$ is called regular if $G$ is transitive, and $G_v = \{1_G\}$ for every $v \in V$.

**Theorem 3.20** (Sabidussi)**.** Let $\Gamma$ be a graph. Then $\Gamma$ is isomorphic to Cayley graph on group $G$ if and only if there exists a regular subgroup $H \leq \mathrm{Aut}(\Gamma)$ such that $H \cong G$.

*Proof.* We already proved that for a Cayley graph $Cay(G,S)$, the group $G_L \leq \mathrm{Aut}(Cay(G,S))$ is regular.

Suppose now that $\Gamma$ is a graph, and that there exists a regular subgroup $H \leq \mathrm{Aut}(\Gamma)$, such that $G \cong H$. Suppose that $V(\Gamma) = \{v_1, \ldots, v_n\}$. Then for each $i \in \{1, \ldots, n\}$, there exists a unique element $h_i \in H$ such that $h_i(v_1) = v_i$ (uniqueness follows from the fact that $H$ is regular). Observe that $h_1 = 1_H$. So we have $H = \{h_1 = 1_H, h_2, \ldots, h_n\}$. Let $\alpha : H \to G$ be an isomorphism, and let $g_i := \alpha(h_i)$. So we have $G = \{g_1 = 1_G, \ldots, g_n\}$. Let $D = \{h_i \in H : v_1 \sim_\Gamma h_i(v_1)\}$, and let $S = \{\alpha(h_i) : h_i \in D\}$. We claim that $\Gamma$ is isomorphic to the graph $Cay(G,S)$. Let $\varphi : V \to G$ be defined with $\varphi(v_i) = g_i$. It is clear that $\varphi$ is bijection.

Let $v_i, v_j \in V(\Gamma)$. Observe that

$$\begin{aligned} v_i \sim_\Gamma v_j &\Leftrightarrow h_i^{-1}(v_i) \sim_\Gamma h_i^{-1}(v_j) \\ &\Leftrightarrow v_1 \sim_\Gamma (h_i^{-1} \circ h_j)(v_1) \\ &\Leftrightarrow h_i^{-1}h_j \in D \\ &\Leftrightarrow \alpha(h_i^{-1}h_j) \in S \\ &\Leftrightarrow \alpha(h_i^{-1})\alpha(h_j) \in S \\ &\Leftrightarrow g_i^{-1}g_j \in S \\ &\Leftrightarrow g_i \sim_{Cay(G,S)} g_j \\ &\Leftrightarrow \alpha(v_i) \sim_{Cay(G,S)} \alpha(v_j) \end{aligned}$$

This shows that $\alpha$ is indeed an isomorphism between $\Gamma$ and $Cay(G, S)$. □

We have seen that Petersen graph is not Cayley graph. The followin result shows that all vertex-transitive graphs of prime order are Cayley graphs.

**Lemma 3.21.** Let $\Gamma$ be a vertex-transitive graph of order $p$, where $p$ is a prime. Then $\Gamma$ is a Cayley graph on cyclic group $\mathbb{Z}_p$.

*Proof.* Let $\Gamma$ be a vertex-transitive graph of order $p$, and let $A = \mathrm{Aut}(\Gamma)$. By orbit-stabilizer theorem, we have $|A| = p|A_v|$ for some vertex $v$. Hence, the order of group $A$ is divisible by $p$. By Cayley theorem, there exists an element $g$ of order $p$ in $A$. Let $G = \langle g \rangle$. Then $G$ is cyclic group of order $p$. Then using the orbit-stabilizer theorem for $G$, it follows that $p = |G| = |G_v||Orb_G(v)|$. Since $p$ is prime, it follows that $|G_v| = p$, or $|G_v| = 1$. It is now easy to see that $G$ is a regular subgroup of $A$, hence by Sabidussi theorem $\Gamma$ is a Cayley graph on $G$. □

Can it happen that $Cay(G, S_1) \cong Cay(H, S_2)$, where $G$ and $H$ are non-isomorphic groups?

**Example 3.22.** Let $G = \mathbb{Z}_2^3$, $H = \mathbb{Z}_4 \times \mathbb{Z}_2$, $S_1 = \{(1,0,0), (0,1,0), (0,0,1)\}$, and $S_2 = \{(1,0), (3,0), (0,1)\}$. Observe that both $Cay(G, S_1)$ and $Cay(H, S_2)$ are isomorphic to the 3-dimensional cube $Q_3$.

**Example 3.23.** Prove that 3-dimensional cube has 48 automorphisms.

*Proof.* We will represent cube as $Cay(\mathbb{Z}_2^3, \{(1,0,0), (0,1,0), (0,0,1)\})$. Let $A$ be the automorphism group of the cube. Then by orbit-stabilizer lemma, it follows that

$$|A| = 8|A_{(0,0,0)}|. \tag{9}$$

Now apply orbit-stabilizer lemma for $A_{(0,0,0)}$. We have

$$|A_{(0,0,0)}| = |A_{(0,0,0),(1,0,0)}||Orb_{|A_{(0,0,0)}|}(0,1,0)|. \tag{10}$$

For a permutation $g \in S_3$ define function $\overline{g} : \mathbb{Z}_2^3 \to \mathbb{Z}_2^3$ with $\overline{g}(x_1, x_2, x_3) = (x_{g(1),x_{g(2)},x_{g(3)}}$. It is left for reader to prove that $\overline{g}$ is automorphism of the cube. Using these permutations, it can be easily seen that $|Orb_{|A_{(0,0,0)}|}(0,1,0)| = 3$. Now again use orbit-stabilizer lemma to obtain:

$$|A_{(0,0,0),(1,0,0)}| = |A_{(0,0,0),(1,0,0),(0,1,0)}||Orb_{A_{(0,0,0),(1,0,0)}}(0,1,0)|. \tag{11}$$

Again using permutations $\overline{g}$ it is easy to see that $|Orb_{A_{(0,0,0),(1,0,0)}}(0,1,0)| = 2$. Furthermore, it is not difficult to verify that $|A_{(0,0,0),(1,0,0),(0,1,0)}| = 1$. Hence

$$|A| = 8|A_{(0,0,0)}| = 8 \cdot 3 \cdot |A_{(0,0,0),(1,0,0)}| = 24 \cdot 2 \cdot |A_{(0,0,0),(1,0,0),(0,1,0)}||Orb_{A_{(0,0,0),(1,0,0)}}(0,1,0)| = 48. \tag{12}$$

□

**Example 3.24.** Let $C_n$ be the cycle of length $n$. Find all groups $G$, such that $C_n$ is cayley graph on $G$.

*Proof.* Let $\Gamma = C_n$. We know that $\mathrm{Aut}(\Gamma) \cong D_{2n} = \langle \rho, \tau \mid \rho^n = \tau^2 = 1, \rho\tau = \tau\rho^{-1} \rangle$. If $\Gamma$ is Cayley graph on $G$, then by Sabidussi theorem, $G$ is regular subgroup of $D_{2n}$. Hence $G$ is of order $n$. It is easy to see that the subgroup generated by $\rho$ (which is cyclic of order $n$) is regular. Denote $H = \langle \rho \rangle$. Let $G \neq H$ be another regular subgroup of $D_{2n}$. Then $GH = D_{2n}$. We have

$$|G \cap H| = \frac{|G||H|}{|GH|} = \frac{n^2}{2n} = n/2.$$

This means that $n$ must be even, and $G \cap H$ is an index 2 subgroup of $H$, hence $G \cap H = \langle \rho^2 \rangle$. So $H$ contains $n/2$ rotations of form $\rho^{2i}$, and $n/2$ reflections without fixed point. It can be seen that $G$ is isomorphic to the dihedral group of order $n$. □

## 3.2 Normal Cayley graphs

Let $\Gamma = Cay(G, S)$. Recall that we proved that $G_L$ is regular subgroup of $\mathrm{Aut}(\Gamma)$, and also that $\mathrm{Aut}(G, S) \leq \mathrm{Aut}(\Gamma)$. For such automorphisms we might say that they are obvious automorphisms of Cayley graphs. In some cases, it turns out that these generate the full automorphism group of a given Cayley graph.

**Definition 3.25.** Let $\Gamma = Cay(G, S)$. If $G_L$ is normal subgroup of $\mathrm{Aut}(G)$ then $Cay(G, S)$ is said to be *normal cayley graph on $G$ with respect to $S$.*

**Theorem 3.26.** Let $\Gamma = Cay(G, S)$ and $A = Aut(X)$. The following claims are equaivalent:

1. $Cay(G, S)$ is normal cayley graph.
2. $A_{1_G} = Aut(G, S)$;
3. $A = \langle G_L, Aut(G, S) \rangle \cong G_L \rtimes Aut(G, S)$;
4. $|A| = |G| \cdot |Aut(G, S)|$.

Remark: If a graph $\Gamma$ can be represented as $Cay(G, S_1)$ and $Cay(H, S_2)$ then it is possible that with respect to one representation it is normal Cayley graph, and with respect to the other one it is not normal Cayley graph.

**Example 3.27.** Let $\Gamma$ be the cube. Then it can be represented as Cayley graph on $\mathbb{Z}_2^3$ and $\mathbb{Z}_4 \times \mathbb{Z}_2$, as we saw in Example 3.22. It can be seen that the first representation is normal, while the second is not.

**Theorem 3.28.** Let $G$ be finite abelian group, and let $S$ be an inverse closed generating set, such that $0 \notin S$. If $S$ satisfies

$$\forall s_1, s_2, s_3, s_4 \in S \quad s_1 + s_2 = s_3 + s_4 \neq 0 \Rightarrow \{s_1, s_2\} = \{s_3, s_4\},$$

then $Cay(G, S)$ is normal Cayley graph.

**Example 3.29.** Let $\Gamma = Cay(\mathbb{Z}_{12}, \{1, 6, 11\})$. Calculate $\mathrm{Aut}(\Gamma)$.

*Proof.* By Theorem 3.28 it follows that $\Gamma$ is normal Cayley graph. Let us determine $\mathrm{Aut}(\mathbb{Z}_{12}, \{1, 6, 11\})$. We know that $\mathrm{Aut}(\mathbb{Z}_{12}) = \{\varphi_1, \varphi_5, \varphi_7, \varphi_{11}\}$, where $\varphi_k(x) = k \cdot x$. It is now easy to see that $\mathrm{Aut}(\mathbb{Z}_{12}, \{1, 6, 11\}) = \{\varphi_1, \varphi_{11}\}$. Observe that $\varphi_1 = id$. Therefore, $|\mathrm{Aut}(\Gamma)| = 12 \cdot 2 = 24$ and $\mathrm{Aut}(\Gamma) = \langle (\mathbb{Z}_{12})_L, \varphi_{11}, \varphi_{11} \rangle$. Observe that elements of $(\mathbb{Z}_{12})_L$ represent rotations, and $\varphi_{11} : x \mapsto -x$ is reflection. Hence $\mathrm{Aut}(\Gamma) \cong D_{24}$. □

**Example 3.30.** Let $\Gamma = Cay(\mathbb{Z}_{29}, \{1, 13, 16, 28\})$. Determine all automorphisms of $\Gamma$.

**Example 3.31.** Let $G = \mathbb{Z}_2^n$ and let $S = \{(1, 0 \ldots, 0), \ldots, (0, 0, \ldots, 1)\}$. Prove that $Cay(G, S)$ is normal, and determine $\mathrm{Aut}(Cay(G, S))$. (Observe that $Cay(G, S)$ is $n$-dimensional cube.)

**Exercise 3.32.** Let $X = Cay(\mathbb{Z}_{25}, \{\pm 1, \pm 7\}$.

- Prove that $X$ is normal Cayley graph.
- Calculate $Aut(\mathbb{Z}_{25}, \{\pm 1, \pm 7\})$.
- Calculate $|Aut(X)|$.

## 3.3 Graph products

In this section we introduce notions of Cartesian, direct, lexicographic and strong product of graphs.

**Definition 3.33.** Let $X$ and $Y$ be graphs. Cartesian product $X \square Y$ of graphs $X$ and $Y$ is the graph with vertex set $V(X) \times V(Y)$ and $(x_1, y_1)$ is adjacent to $(x_2, y_2)$ if and only if $x_1 = x_2$ and $\{y_1, y_2\} \in E(Y)$ or $y_1 = y_2$ and $\{x_1, x_2\} \in E(X)$.

**Definition 3.34.** Let $X$ and $Y$ be graphs. Direct product $X \times Y$ of graphs $X$ and $Y$ is the graph with vertex set $V(X) \times V(Y)$ and $(x_1, y_1)$ is adjacent to $(x_2, y_2)$ if and only if $\{x_1, x_2\} \in E(X)$ and $\{y_1, y_2\} \in E(Y)$.

**Definition 3.35.** Let $X$ and $Y$ be graphs. Strong product $X \boxtimes Y$ of graphs $X$ and $Y$ is the graph with vertex set $V(X) \times V(Y)$ and $(x_1, y_1)$ is adjacent to $(x_2, y_2)$ if and only if one of the following holds

1. $x_1 = x_2$ and $\{y_1, y_2\} \in E(Y)$;
2. $y_1 = y_2$ and $\{x_1, x_2\} \in E(X)$;
3. $\{x_1, x_2\} \in E(X)$ and $\{y_1, y_2\} \in E(Y)$.

Observe that the edge set of $X \boxtimes Y$ is disjoint union of edge sets of $X \square Y$ and $X \times Y$.

**Definition 3.36.** Let $X$ and $Y$ be graphs. Lexicographic product $X[Y]$ of $X$ by $Y$ is the graph with vertex set $V(X) \times V(Y)$ and $(x_1, y_1)$ is adjacent to $(x_2, y_2)$ if and only if $x_1 = x_2$ and $\{y_1, y_2\} \in E(Y)$ or $\{x_1, x_2\} \in E(X)$.

The Cartesian, direct, strong and lexicographic products are called standard graph products. If $G \leq Sym(A)$ and $H \leq Sym(B)$, then $G \times H$ acts naturally on $A \times B$ with $(g, h) : (x, y) \mapsto (g(x), h(y)$, for all $g \in G$ and $h \in H$.

**Proposition 3.37.** Let $G \leq \mathrm{Aut}(X)$ and $H \leq \mathrm{Aut}(Y)$. Then:

1. $G \times H \leq \mathrm{Aut}(X \square Y)$;
2. $G \times H \leq \mathrm{Aut}(X \times Y)$;
3. $G \times H \leq \mathrm{Aut}(X \boxtimes Y)$;
4. $G \times H \leq \mathrm{Aut}(X[Y])$.

*Proof.* It is clear that $(g, h)$ is permutation of vertex set of any of the four standard graph products. Case by case analysis leads to the proof that $(g, h)$ is automorphism of graph obtained as one of the four products. Details are left to the reader. □

**Proposition 3.38.** Let $X, Y$ be two graphs and $Z$ is obtained as one of the four standard products of $X$ and $Y$. If $X$ and $Y$ are vertex-transitive then $Z$ is vertex-transitive. If $X$ and $Y$ are Cayley graphs then $Z$ is Cayley graph.

*Proof.* Follows by Proposition 3.37 and Theorem 3.20. □

## 3.4 Hamiltonicity of vertex-transitive graphs

**Definition 3.39.** Hamilton path in a graph $\Gamma$ is a path that visits each vertex exactly once. A Hamilton cycle (or Hamilton circuit) is a Hamilton path that is a cycle. A graph that admits a Hamilton cycle is called Hamiltonian graph.

The problem of determining whether or not a given connected vertex-transitive graph has a Hamilton cycle or Hamilton path is one of the oldest and most well-known problem concerning vertex-transitive graphs, and as we shall see many additional problems have arisen via attempts to solve these problems. The problem began with what is usually referred to as a conjecture, posed by Lovasz.

**Example 3.40.** Let $\Gamma = Cay(\mathbb{Z}_{10}, \{2, 5, 8\})$. Prove that $\Gamma$ has a Hamiltonian cycle.

**Example 3.41.** Find a Hamilton cycle in graph $Cay(\mathbb{Z}_{12}, \{\pm 3, \pm 4\})$.

**Example 3.42.** Petersen graph has a Hamiltonian path, but it has no Hamiltonian cycle.

*Proof.* It is easy to construct a Hamiltonian path in Petersen graph. To see that Petersen graph does not have a Hamilton cycle we will use the fact that the girth of Petersen graph is 5. Now suppose contrary, that there is a cycle $v_0 \dots v_9$ of length 10 in the Petersen graph. There are 5 more edges that are not lying on this cycle, and each vertex $v_i$ is incident with 1 such edge. Since girth of the Petersen graph is 5, it follows that $v_i$ can be adjacent only

with $v_{i+4}, v_{i+5}$ or $v_{i+6}$. If each vertex $v_i$ is adjacent with $v_{i+5}$ then we obtain cycle of length 4, for example $v_0, v_1, v_6, v_5$. So without loss of generality, we may assume that $v_0$ is adjacent with one of $v_4$ or $v_6$, and furthermore, without loss of generality we may assume that $v_0$ is adjacent with $v_6$. By the girth condition, we have that $v_1$ can only be adjacent with $v_5$, $v_6$ or $v_7$. Moreover, since $v_0 \sim v_6$, it follows that $v_1$ is not adjacent with $v_6$. If $v_1 \sim v_5$, we obtain 4-cycle $v_0, v_1, v_5, v_6$ and if $v_1 \sim v_7$ we obtain 4 cycle $v_0, v_1, v_7, v_6$, a contradiction with the fact that girth of Petersen graph is 5. The obtained contradiction shows that Petersen graph does not admit a Hamilton cycle. □

The only known vertex-transitive graphs that don't admit a Hamilton cycle are $K_1$, $K_2$, Petersen graph, truncation of Petersen graph, Coxeter graph (cubic graph of order 28) and truncation of Coxeter graph. Of course graphs $K_1$ and $K_2$ can be considered as trivial examples, as these graphs have no cycles at all. It turns out that none of the 4 non-trivial examples is a Cayley graph. This has led to the following "Folklore" conjecture.

**Conjecture 3.43.** Every connected Cayley graph of order at least 3 has a Hamilton cycle.

This conjecture has drawn a lot of attention of researchers working in the algebraic graph theory.

We will prove that this conjecture is true for Cayley graphs on Abelian groups. Before presenting the proof we need the following lemma.

**Lemma 3.44.** For every $n \geq 1$ and $m \geq 3$ graph $C_m \Box P_n$ admits a Hamilton cycle.

*Proof.* Proof is left for reader as exercise. □

**Theorem 3.45.** A connected Cayley graph of an abelian group of order at least 3 is Hamiltonian.

*Proof.* Let $\Gamma = Cay(G, S)$ be connected, where $G$ is abelian and $S = S^{-1}$. Since $\Gamma$ is connected, it follows that $\langle S \rangle = G$. We proceed by induction on $|S|$. If $|S| = 1$, then $S = \{a\}$, $a \in G$, $a$ is self-inverse and $G$ is generated by $a$. This implies that $G = \{1, a\}$, which is of order 2, a contradiction. If $|S| = 2$, then either $S = \{a, a^{-1}\}$ with $a$ a generator of G, or $S = \{a, b\}$, where both $a$ and $b$ are self-inverse. In the former case, we have the Hamilton cycle $1, a, a^2, \ldots, a^{n-1}$, where $a^n = 1$ and $n = |G| = |\langle a \rangle|$. In the later case, as $G$ is abelian and $G = \langle a, b \rangle$, we see that $G = \mathbb{Z}_2 \times \mathbb{Z}_2$. The only connected Cayley graphs of $\mathbb{Z}_2 \times \mathbb{Z}_2$ are $C_4$ and $K_4$, which are both Hamiltonian. Assume the result holds for every generating set of size at most $m - 1 \geq 2$, and let $S$ be a self-inverse generating set of $G$ of size $m$.

If $m = 3$, then $S$ contains a self-inverse element $a$, and we define $T := S \setminus \{a\}$. If $m > 3$, then we take $a$ to be arbitrary element of $S$, and define $T := S \setminus \{a, a^{-1}\}$. Observe that in both cases we have that $2 \leq |T| < m$. Let $H = \langle T \rangle$. Then $H$ is abelian group of order at least 3. Let $X = Cay(H, T)$. Then we can apply induction hypothesis on $X$, since it is a connected Cayley graph on abelian group of order at least 3 and its generating set has size less than $m$. Therefore, there exists a Hamilton cycle in the graph $X$. Suppose that this Hamilton cycle is $h_1, h_2 \ldots h_k$, where $H = \{h_1, \ldots, h_k\}$. Let $n$ be the smallest positive integer such that $a^n \in H$. Then $G$ is disjoint union of $H$,$aH$,$a^2H$,$\ldots, a^{n-1}H$. Observe now that $ah_1, ah_2 \ldots ah_k$ is also a cycle, and that each $x$ is adjacent with $ax$. Hence we obtain that $\Gamma$ contains a spanning subgraph isomorphic to $C_k \Box P_n$. By previous Lemma, it follows that there is a Hamilton cycle in $C_k \Box P_n$, hence there is also a Hamilton cycle in $\Gamma$. □

**Example 3.46.** Let $G = \mathbb{Z}_6 \times \mathbb{Z}_4$ in $S = \{(3,1),(3,3),(2,1),(4,3)\}$. Find a Hamilton cycle in graph $Cay(G,S)$.

# 4 Edge-transitive and arc-transitive graphs

Automorphism of a graph is defined as permutation of vertex-set, that preserves edges. Every automorphism of a graph can be also considered as a permutation of edges, that is we can consider natural action of $\mathrm{Aut}(\Gamma)$ on $E(\Gamma)$. For an automorphism $\varphi \in \mathrm{Aut}(\Gamma)$ and an edge $e = \{x, y\}$ we define $\varphi(e) = \{\varphi(x), \varphi(y)\}$.

**Definition 4.1.** A graph $\Gamma = (V, E)$ is said to be *edge-transitive* if $\mathrm{Aut}(\Gamma)$ acts transitively on the edge set, that is for any two edges $\{u, v\}, \{x, y\} \in E$, there exists $\varphi \in \mathrm{Aut}(\Gamma)$ such that $\varphi\{x, y\} = \{u, v\}$.

**Example 4.2.** Complete bipartite graph $K_{m,n}$ is edge-transitive. Furthermore, it is vertex-transitive if and only if $m = n$. Hence there exist edge-transitive graphs which are not vertex-transitive.

We have seen that every Cayley graph is vertex-transitive. Cayley graphs don't need to be edge-transitive.

**Example 4.3.** $Cay(\mathbb{Z}_6, \{\pm 2, 3\})$ is not edge-transitive.

**Example 4.4.** For every odd positive integer $m \geq 3$ graph $Cay(\mathbb{Z}_m \times \mathbb{Z}_2, \{(\pm 1, 0), (0, 1)\})$ is not edge-transitive.

**Theorem 4.5.** Let $\Gamma$ be an edge-transitive graph without isolated vertices. If $\Gamma$ is not vertex-transitive, then $\Gamma$ is bipartite. Moreover, $\mathrm{Aut}(G)$ has two orbits on vertices and these two orbits form a bipartition of $\Gamma$.

*Proof.* Let $\{u, v\}$ be an edge of $\Gamma$. Let $U = \{\varphi(u) : \varphi \in \mathrm{Aut}(\Gamma)\}$ and $V = \{\varphi(v) : \varphi \in \mathrm{Aut}(\Gamma)\}$. Since $\Gamma$ is not vertex-transitive, it follows that $U \cap V = \emptyset$. Let $x$ be an arbitrary vertex of $\Gamma$. Since $\Gamma$ has no isolated vertices it follows that there exist $y \in V(\Gamma)$ such that $x \sim y$. Since $\Gamma$ is edge-transitive, there exists $\varphi \in \mathrm{Aut}(\Gamma)$ such that $\varphi\{u, v\} = \{x, y\}$. This shows that $x \in U$ or $x \in V$. Hence $V(\Gamma)$ is disjoint union of $U$ and $V$. Suppose now that there is an edge $\{x, y\}$ where both $x$ and $y$ belong to $U$. Then there exists $\varphi \in \mathrm{Aut}(\Gamma)$ such that $\varphi\{u, v\} = \{x, y\}$. This would imply that $\varphi(v) = x$ or $\varphi(v) = y$ and therefore $x \in V$ or $y \in V$. However, this is impossible, since $U \cap V = \emptyset$. This shows that sets $U$ and $V$ form a bipartition of $\Gamma$. □

**Definition 4.6.** Let $\Gamma$ be a graph. *Arc* in $\Gamma$ is a pair $(u, v)$, where $u$ and $v$ are adjacent vertices of $\Gamma$.

Observe that for any graph $\Gamma$, the number of arcs is twice the number of edges, that is for every edge $\{u, v\}$ there are two arcs $(u, v)$ and $(v, u)$.

**Definition 4.7.** A graph $\Gamma$ is said to be arc-transitive if $\mathrm{Aut}(\Gamma)$ acts transitively on the arc set of $\Gamma$, that is for any two pairs of adjacent vertices $u \sim v$ and $x \sim y$, there exists an automorphism $\varphi \in \mathrm{Aut}(\Gamma)$ such that $\varphi(u) = x$ and $\varphi(v) = y$.

**Proposition 4.8.** Let $\Gamma$ be a graph. If $\Gamma$ is arc-transitive then $\Gamma$ is edge-transitive. Moreover, if $\Gamma$ is without isolated vertices, then $\Gamma$ is vertex-transitive.

Proof is straightforward and is omitted.

**Remark 4.9.** There exist graphs which are vertex-transitive and edge-transitive but not arc-transitive. Such graphs are called half-arc-transitive. The smallest example is a 4-valent graph of order 27 and it so called Doyle-Holt graph.

**Proposition 4.10.** Let $\Gamma$ be a vertex-transitive graph. Then $\Gamma$ is arc-transitive if and only if for an arbitrary vertex $v$, the stabilizer $\mathrm{Aut}(G)_v$ acts transitively on $\Gamma(v)$, the set of neighbour of $v$ in $\Gamma$.

*Proof.* Suppose first that $\Gamma$ is arc-transitive. Let $v \in V(\Gamma)$ and let $a, b \in \Gamma(v)$ be arbitrary. Since $\Gamma$ is arc-transitive, we can map arc $(v, a)$ to arc $(v, b)$, hence there exists automorphism $\varphi$ such that $\varphi(v) = v$ and $\varphi(a) = b$. Hence $\varphi \in \mathrm{Aut}(\Gamma)_v$ and maps $a$ to $b$. This shows that $\mathrm{Aut}(G)_v$ acts transitively on $\Gamma(v)$.

Suppose now that $\mathrm{Aut}(G)_v$ acts transitively on $\Gamma(v)$. Let $(x, y)$ and $(a, b)$ be two arbitrary arc in $\Gamma$. Then there exist automorphism $\varphi_1$ and $\varphi_2$ such that $\varphi_1(x) = v$ and $\varphi_2(y) = v$. Let $c = \varphi_1(y$ and $d = \varphi_2(b)$. Observe that $c, d \in \Gamma(v)$. Then there exists $\varphi_3 \in \mathrm{Aut}(\Gamma)_v$ such that $\varphi_3(c) = d$. It is now easy to verify that $\varphi_2^{-1}\varphi_3\varphi_1$ maps arc $(x, y)$ to arc $(a, b)$. This proves that $\Gamma$ is arc-transitive. □

**Example 4.11.** Let $\Gamma = Cay(\mathbb{Z}_{17}, \{1, 2, 4, 8, 16, 15, 13, 9\}$. Then $\Gamma$ is arc-transitive.

*Proof.* Let $S = \{1, 2, 4, 8, 16, 15, 13, 9\}$. Observe that $\mathrm{Aut}(\mathbb{Z}_{17}, S) = \{\varphi_1, \varphi_2, \varphi_4, \varphi_8, \varphi_9, \varphi_{13}, \varphi_{15}, \varphi_{16}\}$ and that it acts transitively on $S$. Observe also that $\Gamma(0) = S$. Recall that $\mathrm{Aut}(\mathbb{Z}_{17}, S) \leq \mathrm{Aut}(\Gamma)_0$. This shows that $\mathrm{Aut}(\Gamma)_0$ acts transitively on neighbours of 0, and hence $\Gamma$ is arc-transitive. □

**Proposition 4.12.** A Cayley graph on Abelian group is arc-transitive if and only if it is edge-transitive.

**Proposition 4.13.** Let $\Gamma$ be a vertex-transitive and edge-transitive graph which is not arc-transitive. Then $\Gamma$ has even valency.

A Cayley graph on cyclic group is called *circulant*

**Exercise 4.14.** Find up to isomorphism all cubic edge-transitive circulants.

# 5 $s$-arc-transitive graphs

**Definition 5.1.** An $s$-arc in a graph is a sequence of vertices $(v_0, \ldots, v_s)$ such that consecutive vertices are adjacent and $v_{i-1} \neq v_i$ when $0 < i < s$. Note that an $s$-arc is permitted to use the same vertex more than once. A graph $\Gamma$ is $s$-arc transitive if its automorphism group is transitive on $s$-arcs, that is for any two $s$-arcs $(v_0, \ldots, v_s)$ and $(u_0, \ldots, u_s)$ there exists $\alpha \in \mathrm{Aut}(\Gamma)$ such that $\alpha(v_i) = u_i$ for $i = 0, \ldots, s$

Observe that 0-arcs are just the vertices and 1-arcs are the usual arcs.

**Example 5.2.** $C_n$ is $s$-arc-transitive for every $s$

**Example 5.3.** $K_n$ is $s$-arc-transitive only for $s = 0, 1, 2$.

**Example 5.4.** Cube $Q_3$ is 2-arc-transitive but not 3-arc-transitive.

**Theorem 5.5.** Let $\Gamma$ be a graph with minimum degree at least 2. Then $\Gamma$ is $(s+1)$-arc-transitive if and only if $\Gamma$ is $s$-arc-transitive and the stabilizer in $\mathrm{Aut}(\Gamma)$ of any $s$-arc $(v_0, \ldots, v_{s-1}, v_s)$ acts transitively on the $\Gamma(v_s) \setminus \{v_{s-1}\}$.

**Example 5.6.** Petersen graph is 3-arc-transitive but not 4-arc-transitive.

**Proposition 5.7.** If $\Gamma$ is an $s$-arc-transitive graph with valency at least three and girth $g$, then $g \geq 2s - 2$.

*Proof.* We may assume that $s \geq 3$, since the condition on the girth is otherwise meaningless. It is easy to see that $\Gamma$ contains a cycle of length $g$ and a path of length $g$ whose end-vertices are not adjacent. Therefore $\Gamma$ contains a $g$-arc with adjacent end-vertices and a $g$-arc with nonadjacent end-vertices; clearly, no automorphism can map one to the other, and so $s < g$. Since $\Gamma$ contains cycles of length $g$, and since these contain $s$- arcs, it follows that any $s$-arc must lie in a cycle of length $g$. Suppose that $u_0, \ldots, u_s$ is an $s$-arc. Denote it by $A$. Since $u_{s-1}$ has valency at least three, it is adjacent to a vertex $w$ other than $u_{s-2}$ and $u_s$, and since the girth of $\Gamma$ is at least $s$, this vertex cannot lie in $A$. Hence we may replace $u_s$ by $w$, obtaining a second $s$-arc $B$ that intersects $A$ in an $(s-1)$-arc. Since $B$ must lie in a circuit of length $g$, we thus obtain a pair of circuits of length $g$ that have at least $s - 1$ edges in common. If we delete these $s - 1$ edges from the graph formed by the edges of the two circuits of length $g$, the resulting graph still contains a cycle of length at most $2g - 2s + 2$. Hence $2g - 2s + 2 > g$, and the result follows. □

## 5.1 Cubic-arc-transitive graphs

A graph is said to be *cubic* if it is 3-regular, that is if each vertex has degree 3. In 1947 Tutte showed that for any $s$-arc transitive cubic graph, $s \leq 5$. This was, eventually, the stimulus for a lot of work. One outcome of this was a proof, by Richard Weiss, that for any $s$-arc transitive graph, $s \leq 7$. This is a very deep result, the proof of which depends on the classification of the finite simple groups.

**Definition 5.8.** A graph $\Gamma$ is $s$-arc regular if it is $s$-arc-transitive and stabilizer in $\mathrm{Aut}(\Gamma)$ of any $s$-arc is trivial, or equivalently, the automorphism group $\mathrm{Aut}(\Gamma)$ acts regularly on the set of all $s$-arcs of $\Gamma$.

**Lemma 5.9.** Let $\Gamma$ be a connected cubic graph that is $s$-arc transitive, but not $(s+1)$-arc transitive. Then $\Gamma$ is $s$-arc regular.

**Theorem 5.10** (Tutte)**.** If $\Gamma$ is an $s$-arc regular cubic graph, then $s \leq 5$.

**Corollary 5.11.** If $\Gamma$ is cubic arc-transitive graph then $|Aut(\Gamma)| = |V(\Gamma)| \cdot 3 \cdot 2^{s-1}$ for some $s \in \{1, 2, 3, 4, 5\}$.

**Example 5.12.** Petersen graph is 3-arc-regular.

# 6 Distance-transitive graphs

**Definition 6.1.** A connected graph $\Gamma$ is *distance-transitive* if given any two ordered pairs of vertices $(u, u')$ and $(v, v')$ such that $d(u, u') = d(v, v')$, there is an auto- morphism $\alpha$ of $\Gamma$ such that $\alpha(v, v') = (u, u')$.

**Example 6.2.** Complete graph $K_n$ is distance-transitive.

For a connected graph $\Gamma$ and a vertex $v \in V(\Gamma)$ let $\Gamma_i(v)$ be the set of vertices at distance $i$ from $v$, that is $\Gamma_i(v) = \{u \in V(\Gamma) \mid d(u, v) = i\}$. Observe that for any connected graph $\Gamma$ with diameter $d$ we have that $V(\Gamma)$ is partitioned into sets $\Gamma_0(v)$, $\Gamma_1(v)$, ..., $\Gamma_d(v)$. The following theorem gives a characterization of distance-transitive graphs, based on the action of automorphism group on sets $\Gamma_i(v)$. This partition is called *distance-partition* of $\Gamma$.

**Theorem 6.3.** Let $\Gamma$ be a connected graph. Then $\Gamma$ is distance transitive if and only if the following conditions hold:

1. $\Gamma$ is vertex-transitive;
2. $\mathrm{Aut}(\Gamma)_v$ acts transitively on each of sets $\Gamma_i(v)$ $(i = 1, \ldots, diam(\Gamma))$, for any vertex $v \in V(\Gamma)$.

**Corollary 6.4.** Let $\Gamma$ be a connected distance-transitive graph. Then $\Gamma$ is arc-transitive.

**Example 6.5.** Petersen graph is distance-transitive.

We would like to note that distance-transitive graphs are not necessarily $s$-arc-transitive for higher values of $s$.

**Example 6.6.** A cube graph $Q_3$ is distance-transitive, it has diameter 3, but it is not 3-arc-transitive.

**Example 6.7.** Let $G = \mathbb{Z}_{17}$ and $S = \{1, 2, 4, 8, 9, 13, 15, 16\}$ and let $\Gamma = Cay(G, S)$. Then $\Gamma$ is distance-transitive with diameter 2.

**Example 6.8.** Let $p \equiv 1 \pmod 4$ be a prime, and let $G = \mathbb{Z}_p$. Let $S = \{x^2 : x \in 1, \ldots, p-1$. Observe that $S = -S$ and that $|S| = (p-1)/2$. Let $\Gamma = Cay(G, S)$. Then $\Gamma$ is distance-transitive with diameter 2.

**Example 6.9.** Let $p$ be a prime, and $q = p^n$ such that $q \equiv 1 \pmod 4$. Let $\mathbb{F}_q$ be the field of order $q$. Let $S$ be the set of all non-zero squares in $\mathbb{F}_q$, that is $S = \{x^2 \mid x \in \mathbb{F}_q \setminus \{0\}\}$. Let $G$ be the additive group of the field $\mathbb{F}_q$, that is $G = (\mathbb{F}_q, +)$. The graph $\Gamma = Cay(G, S)$ is called Paley graph. Prove that Paley graphs are distance-transitive.

Suppose that $\Gamma$ is a connected distance-transitive graph and $u \in V(\Gamma)$. Since the cells of the distance partition $\Gamma_i(u)$ are orbits of $\mathrm{Aut}(\Gamma)_u$, every vertex in $\Gamma_i(u)$ is adjacent to the same number of other vertices, say $a_i$, in $\Gamma_i(u)$. Similarly, every vertex in $\Gamma_i(u)$ is adjacent to the same number, say $b_i$, of vertices in $\Gamma_{i+1}(u)$ and the same number, say $c_i$, of vertices in $\Gamma_{i-1}(u)$. The graph X is regular, and its valency is given by $b_0$, so if the diameter of $\Gamma$ is $d$, we have

$$c_i + a_i + b_i = b_0, \quad i = 0, 1, ..., d.$$

These numbers are called the parameters of the distance-transitive graph, and determine many of its properties.

Distance transitivity is a symmetry property in that it is defined in terms of the existence of certain automorphisms of a graph. These automorphisms impose regularity properties on the graph, namely that the numbers $a_i$, $b_i$, and $c_i$ are well-defined. There is an important combinatorial analogue to distance transitivity, which simply asks that the numerical regularity properties hold, whether or not the automorphisms exist. Given any graph $\Gamma$ we can compute the distance partition from any vertex $u$, and it may occur "by accident" that every vertex in $\Gamma_i(u)$ is adjacent to a constant number of vertices in $\Gamma_{i-1}(u)$,$\Gamma_i(u)$ and $\Gamma_{i+1}(u)$, regardless of whether there are any automorphisms that force this to occur. Such graphs are called *distance-regular* graphs.

**Proposition 6.10.** Every distance-transitive graph is distance-regular.

A special case are distance-regular graphs of diameter 2. Such graphs are called strongly regular graphs.

**Exercise 6.11.** Let $\Gamma$ be a distance-regular graph with diameter 2. Prove that there exist parameters $(n, k, \lambda, \mu)$ such that $\Gamma$ has order $n$, it is $k$-regular, every edge lies on $\lambda$ triangles (in other words every pair of adjacent vertices have $\lambda$ common neighbours), and every pair of distinct non-adjacent vertices have $\mu$ common neighbours. A graph $\Gamma$ is said to be strongly regular with parameters $(n, k, \lambda, \mu)$.

**Example 6.12.** Prove that the complement of a strongly regular graph is strongly regular.

**Example 6.13.** Let $\Gamma$ be a connected vertex-transitive graph, and suppose that $\mathrm{Aut}(G)_v$ have exactly three orbits in its action on $V(\Gamma)$. Prove that $\Gamma$ is distance-transitive.

**Example 6.14.** The graph $L(K_n)$ (that is the line graph of $K_n$) is strongly regular with parameters $(n(n-1)/2, 2n-4, n-2, 4)$.

**Example 6.15.** The graph $L(K_{n,n})$ is strongly regular with parameters $(n^2, 2n-2, n-2, 2)$.

**Exercise 6.16.** Let $G = \mathbb{Z}_4 \times \mathbb{Z}_4$ and let $S = \{\pm(1,0), \pm(0,1), \pm(1,1)\}$. The graph $\Gamma = Cay(G, S)$ is called Shrikhande graph. Prove that it is strongly regular, but not distance-transitive.

## 6.1 Eigenvalues of strongly regular graphs

Let $\Gamma$ be a graph of order $n$ with vertex set $\{v_1, \ldots, v_n\}$. Adjacency matrix $A = A(\Gamma)$ is $n$-by-$n$ matrix with value $A_{i,j}$ equal to 1 if and only if $\{v_i, v_j\} \in E(\Gamma)$. Observe that adjacency matrix is a symmetric matrix, that is $A^T = A$. Such matrices have several nice properties.

**Lemma 6.17.** All eigenvalues of a real symmetric matrix are real.

*Proof.* Suppose that $\alpha \in \mathbb{C}$ is an eigenvalue of a symmetric matrix $A$. Let $x \neq 0$ be a corresponding eigenvector. Then $Ax = \alpha x$. Then $x^*Ax = x^*\alpha x = \alpha x^*x$. On the other hand $\alpha x^*x = x^*\alpha x = x^*Ax = (x^*Ax)^* = \overline{\alpha} x^*x$. Therefore, $\alpha = \overline{\alpha}$, hence $\alpha$ is real. □

**Lemma 6.18.** Let $A$ be a symmetric real matrix. Then $A$ is diagonalizable.

**Exercise 6.19.** Let $\Gamma$ be a connected $k$-regular graph. Then $k$ is an eigenvalue of $A(\Gamma)$ with multiplicity one.

*Proof.* Let $\Gamma$ be a connected $k$-regular graph of order $n$, and let $\{v_1, \ldots, v_n\}$ be the vertex set of $\Gamma$. Let $A$ be its adjacency matrix. Then it is easy to see that $A \cdot \mathbf{1} = k\mathbf{1}$, hence $k$ is an eigenvalue. Suppose that $x$ is an eigenvector of $A$ corresponding to $k$. Let $x = (x_1, \ldots, x_n)^T$. Since $x$ is eigenvector corresponding to eigenvalue $k$, it follows that $Ax = kx$. Let $x_j$ be the maximum of $x_1, \ldots, x_n$, that is $x_i \leq x_j$ for every $i \in \{1, \ldots, n\}$. Then

$$kx_j = (kx)_j = (Ax)_j = \sum A_{j,i}x_i = \sum_{v_i \in \Gamma_i(v_j)} x_i \leq kx_j.$$

Therefore, we conclude that $x_i = k_j$ for every $i$ such that $v_i \in \Gamma(v_j)$. The connectedness of $\Gamma$ now implies that all $x_i$ must be equal to $x_j$, hence $x = x_j\mathbf{1}$. This shows that the multiplicity of $k$ as an eigenvalue if 1. □

Suppose $A$ is the adjacency matrix of the $(n, k, \lambda, \mu)$ strongly regular graph $\Gamma$. We can determine the eigenvalues of the matrix $A$ from the parameters of $\Gamma$ and thereby obtain some strong feasibility conditions. The $uv$-entry of the matrix $A^2$ is the number of walks of length two from the vertex $u$ to the vertex $v$. In a strongly regular graph this number is determined only by whether $u$ and $v$ are equal, adjacent, or distinct and nonadjacent. Therefore, we get the equation

$$A^2 = kI + \lambda A + \mu(J - I - A)$$

Where $J$ denotes all 1 matrix. The above equation can be rewritten as

$$A^2 - (\lambda - \mu)A - (k - \mu)I = \mu J.$$

We can use this equation to determine the eigenvalues of A. Since $\Gamma$ is regular with valency $k$, it follows that $k$ is an eigenvalue of $A$ with eigenvector $(1, \ldots, 1)$. Any other eigenvector of $A$ is orthogonal to $(1, \ldots, 1)$ (this follows since $A$ is symmetric matrix, that is $A^T = A$). Let $z$ be an eigenvector for $A$ with eigenvalue $\theta \neq k$. Then

$$A^2z - (\lambda - \mu)Az - (k - \mu)Iz = \mu Jz = 0,$$

so

$$\theta^2 - (\lambda - \mu)\theta - (k - \mu) = 0.$$

Therefore, the eigenvalues of $A$ different from $k$ must be zeros of the quadratic

$$x^2 - (\lambda - \mu)x - (k - \mu).$$

If we set $\Delta = (\lambda - \mu)^2 + 4(k - \mu)$ (the discriminant of the quadratic) and denote the two zeros of this polynomial by $\tau$ and $\theta$, we get

$$\tau = \frac{\lambda - \mu - \sqrt{\Delta}}{2}$$

and

$$\theta = \frac{\lambda - \mu + \sqrt{\Delta}}{2}$$

Now, $\tau\theta = (\mu - k)$, and so, provided that $\mu < k$, we get that $\tau$ and $\theta$ are nonzero with opposite signs. We see that the eigenvalues of a strongly regular graph are determined by its parameters (although strongly regular graphs with the same parameters need not be isomorphic). The multiplicities of the eigenvalues are also determined by the parameters.

**Exercise 6.20.** Determine the multiplicities of eigenvalues of an $(n, k, \lambda, \mu)$ strongly regular graph.

**Theorem 6.21.** A connected regular graph with exactly three distinct eigenvalues is strongly regular.

*Proof.* Suppose that $\Gamma$ is connected and regular with eigenvalues $k, \theta$, and $\tau$, where $k$ is the valency of $\Gamma$, and let $n$ be the order of $\Gamma$. Let $A$ be the adjacency matrix of $G$. Since $A$ is symmetric, the sum of multiplicities of its eigenvalues equals $n$. Moreover, since $\Gamma$ is connected, eigenvalue $k$ has multiplicity 1. Define matrix $M$ with

$$M := \frac{1}{(k-\theta)(k-\tau)}(A - \theta I)(A - \tau I)$$

Observe that kernel of $M$ consists precisely of eigenvectors of $A$ corresponding to $\theta$ or $\tau$, hence kernel of $M$ has dimension $n - 1$. Moreover, we have

$$\begin{aligned} M \cdot [1, \ldots, 1]^T &= \frac{1}{(k-\theta)(k-\tau)}(A - \theta I)(A - \tau I) \cdot [1, \ldots, 1]^T \\ &= \frac{1}{(k-\theta)(k-\tau)}(A - \theta I)((A \cdot [1, \ldots, 1]^T - \tau \cdot [1, \ldots, 1]^T)) \\ &= \frac{1}{(k-\theta)(k-\tau)}(A - \theta I)((k - \tau) \cdot [1, \ldots, 1]^T)) \\ &= \frac{1}{(k-\theta)}(A - \theta I) \cdot [1, \ldots, 1]^T = [1, \ldots, 1]^T. \end{aligned}$$

This implies that $M = \frac{1}{n}J$ (explain why).

We have shown that $J$ is a quadratic polynomial in $A$, and thus $A^2$ is a linear combination of $I$, $J$, and $A$. Accordingly, $\Gamma$ is strongly regular. □

**Exercise 6.22.** Let $\Gamma$ be a Moore graph with valency $k$ and diameter 2. Prove that $k \in \{2, 3, 7, 57\}$.

*Proof.* Observe that a Moore graph with valency $k$ and diameter 2 is $(k^2 + 1, k, 0, 1)$ strongly regular. Calculate the eigenvalues and the corresponding multiplicities. Use the fact that multiplicities of eigenvalues are integers. □

**Exercise 6.23.** Let $\Gamma$ be a connected graph of order 25 and let $A$ be its adjacency matrix. If $A^2 + A - 6I = 6J$, prove that $\Gamma$ is strongly regular, and determine its parameters $(n, k, \lambda, \mu)$.

*Proof.* Observe that we can rewrite the given equality as:

$$A^2 = 12I + 5A + 6(J - I - A).$$

This means that for vertex $v \in V(\Gamma)$, the number of walks of length 2 between $v$ and $v$ is 12. Hence $\Gamma$ is regular with valency 12. Similarly we see that for two adjacent vertices $u$ and $v$ the number of common neighbours is 5 and for two non-adjacent vertices, the number of their common neighbours is 6. Therefore, $\Gamma$ is $(25, 12, 5, 6)$-strongly regular graph. □

**Exercise 6.24.** Let $\Gamma$ be a connected graph of order 21 and let $A$ be its adjacency matrix such that $A^2 - A - 6I = 4J$.

(a) Prove that $\Gamma$ is strongly regular graph;

(b) Determine parameters $(n, k, \lambda, \mu)$ of $\Gamma$;

(c) Determine eigenvalues of $A$ and their multiplicities.