Permutation groups

Peter Zeman

Department of Algebra
Faculty of Mathematics and Physics
Charles University

February 24, 2026

Preface

These are lecture notes for the course NMAL432 Permutation Groups, taught at the Faculty of Mathematics and Physics, Charles University.

Contents

Chapter 1

Two motivating examples

1.1 Finite groups of isometries

A $n \times n$ matrix A is *orthogonal* if $A^T A = I$. Since $\det(A^T A) = (\det A)^2$ the determinant of A is either $+1$ or -1. If A and B are orthogonal, then an easy calculation shows that AB^-1 is orthogonal as well. Therefore, $n \times n$ matrices form a subgroup of GL_n, called the *orthogonal group* O_n. Those elements of O_n which have determinant equal to $+1$ form a subgroup of O_n called the *special orthogonal group* SO_n.

It is easy to see that the linear mapping corresponding to an orthogonal matrix preserves distances in $\mathbb{R}^n$. Coversely, any linear mapping $\mathbb{R}^n \to \mathbb{R}^n$ that preserves lengths, preserves also distances and right angles, and thus maps the standard basis to an orthonormal basis. The matrix representing this mapping has the elements of this basis as its columns, so it is orthogonal.

Two and three dimensions. If $A \in \mathrm{O}_2$, the columns of A are unit vectors and are orthogonal to one another. Suppose that

$$A = \begin{pmatrix} a & c \\ b & d \end{pmatrix}.$$

Then (a, b) lies on the unit circle, giving $a = \cos\theta$, $b = \sin\theta$ for some θ satisfying $0 \le \theta < 2\pi$. Since (c, d) is orthogonal to (a, b) and also lies on the unit circle, we have $c = \cos\varphi$, $d = \sin\varphi$, where either $\varphi = \theta + \pi/2$ or $\varphi = \theta - \pi/2$. We obtain

$$\begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}, \quad \begin{pmatrix} \cos\theta & \sin\theta \\ \sin\theta & -\cos\theta \end{pmatrix}.$$

The first matrix is an element of SO_2 and represents the anticlockwise rotation through θ. The second has determinant -1 and represents the reflection in a line at angle $\theta/2$ to the positive x-axis.

Now suppose that $A \in \mathrm{SO}_3$. The characteristic polynomial $\det(A - \lambda I)$ is a cubic and therefore must have at least one real root, i.e., A has a real eignevalue. Since the determinant is the product of eigenvalues, it follows that $+1$ is an eigenvalue of A. If $\mathbf{v}$ is a corresponding eigenvector, the line through the origin determined by $\mathbf{v}$ is left fixed by A. Also since A preserves right angles, it must map the plane which is perpendicular to $\mathbf{v}$, and which contains the origin, to itself. We can construct an orthonormal basis for $\mathbb{R}^3$ with the unit vector $\mathbf{v}/\|\mathbf{v}\|$ as the first element. The matrix with respect to this new basis corresponding to same mapping as A will be an element of SO_3 taking the form

$$\begin{pmatrix}1 & 0 & 0\\ 0 & b_{11} & b_{12}\\ 0 & b_{21} & b_{22}\end{pmatrix}, \quad B = \begin{pmatrix}b_{11} & b_{12}\\ b_{21} & b_{22}\end{pmatrix} \in \mathrm{SO}_2,$$

So A is a rotation with axis determined by $\mathbf{v}$. Conversely every rotation of $\mathbb{R}^3$ which fixes the origin is represented by a matrix in SO_3.

If $A \in \mathrm{O}_3$, but $A \notin \mathrm{SO}_3$, then $AU \in \mathrm{SO}_3$, where

$$U = \begin{pmatrix}1 & 0 & 0\\ 0 & 1 & 0\\ 0 & 0 & -1\end{pmatrix}.$$

The matrix U represents a reflection in (x, y)-plane. Clearly,

$$A = (AU)U$$

and since AU is a rotation, A is a reflection in the (x, y)-plane followed by a rotation.

Proposition 1.1. $\mathrm{O}_3 \cong \mathrm{SO}_3 \times \mathbb{Z}_2$.

Proof. Let I denote the 3×3 identity matrix. Both I and $-I$ commute with every other matrix in O_3, and together they form a subgroup of O_3 of order 2 isomorphic to $\mathbb{Z}_2$. Define

$$\varphi\colon\ \mathrm{SO}_3 \times \{I, -I\} \to \mathrm{O}_3, \quad \text{by} \quad (A, U) \longmapsto AU,$$

where $A \in \mathrm{SO}_3$ and $U \in \{I, -I\}$.

We have

$$\varphi((A, U)(B, V)) = \varphi(AB, UV) = ABUV = AUBV = \varphi(A, U)\varphi(B, V),$$

for all $A, B \in \mathrm{SO}_3$ and $U, V \in \{I, -I\}$, so φ is a homomorphism.

If $\varphi(A, U) = \varphi(B, V)$, then $AU = BV$, giving $\det(AU) = \det(BV)$. But

$$\det(AU) = \det(A)\det(U) = \det(U)$$

because $A \in \mathrm{SO}_3$, and similarly $\det(BV) = \det(V)$. Hence $U = V$, $A = B$, and we conclude that φ is injective. It only remains to check that φ is surjective. Given $A \in \mathrm{O}_3$, either $A \in \mathrm{SO}_3$, in which case $A = \varphi(A, I)$, or $A(-I) \in \mathrm{SO}_3$ and $A = \varphi(A(-I), -I)$. Thus, φ is an isomorphism. □

Remark 1.2. The same argument shows that $\mathrm{O}_n \cong \mathrm{SO}_n \times \mathbb{Z}_2$ only *when n is odd*. The map φ is not an isomorphism for an even n since then we have $\operatorname{Ker} \varphi = \{(I, I), (-I, -I)\}$. In fact, for even $n \geq 4$ the statement is not true: for instance, the groups O_n and $\mathrm{SO}_n \times \mathbb{Z}_2$ have centers of different orders, two and four, respectively. And for $n = 2$, the group SO_2 is abelian, so $\mathrm{SO}_2 \times \mathbb{Z}_2$ has much larger center than O_2.

Theorem 1.3. *A finite subgroup of O_2 is either cyclic or dihedral.*

Proof. Let G be a finite non-trivial subgroup of O_2. First, suppose that G lies inside SO_2 so that each element of G represents a rotation of the plane. Write A_θ for the matrix which represents the anticlockwise rotation through θ about the origin, where $0 \leq \theta < 2\pi$, and choose $A_\varphi \in G$ so that φ is positive and as small as possible.

Given $A_\theta \in G$, divide θ by φ to produce

$$\theta = k\varphi + \psi$$

where $k \in \mathbb{Z}$ and $0 \leq \psi < \varphi$. Then

$$A_\theta = A_{k\varphi+\psi} = (A_\varphi)^k A_\psi \qquad \text{and} \qquad A_\psi = (A_\varphi)^{-k} A_\theta.$$

Since A_θ and A_φ both lie in G, we see that A_ψ is also in G. This gives $\psi = 0$, since otherwise we contradict our choice of φ. Therefore, G is generated by A_φ and is cyclic.

If G is not contained inside SO_2, we set $H = G \cap \mathrm{SO}_2$. Then H is a subgroup of G which has index 2, and by the first part H is cyclic because it is contained in SO_2. Choose a generator A for H and an element B from $G \setminus H$. As B represents a reflection we have $B^2 = I$. If $A = I$, then G consists of I and B and is a cyclic group of order 2. Otherwise, the order of A is an integer $n \geq 2$. The elements of G are now

$$I,\ A,\ \ldots,\ A^{n-1},\ B,\ AB,\ \ldots,\ A^{n-1}B$$

and they satisfy $A^n = I$, $B^2 = I$, $BA = A^{-1}B$. The presentation

$$\langle A, B \mid A^n = I, B^2 = I, BA = A^{-1}B \rangle$$

determines the dihedral group $\mathbb{D}_n$. □

Theorem 1.4. *A finite subgroup of* SO_3 *is isomorphic either to a cyclic group, a dihedral group, or the rotational symmetry group of one of the Platonic solids.*

Proof. Let G be a finite subgroup of SO_3. Each element of G, other than the identity, represents a rotation of $\mathbb{R}^3$ about an axis which passes through the origin. We will work with rotations rather than the corresponding matrices. The two points where the axis of a rotation $g \in G$ meets the unit sphere are called the *poles* of g. These poles are the only points on the unit sphere which are fixed by the given rotation.

Let X denote the set of all poles of all elements of $G \setminus \{e\}$. Suppose $x \in X$ and $g \in G$. Let x be a pole of the element $h \in G$. Then

$$(ghg^{-1})(g(x)) = g(h(x)) = g(x),$$

which shows that $g(x)$ is a pole of ghg^{-1} and hence $g(x) \in X$. Therefore, we have an action of G on X. The idea of the proof is to apply the orbit-counting lemma to this action and show that X has to be a particularly nice configuration of points.

Let N denote the number of distinct orbits, choose a pole from each orbit, and call these poles $x_1, x_2, \ldots, x_N$. Every element of $G \setminus \{e\}$ fixes precisely two poles, while the identity fixes them all, so the orbit-counting lemma gives

$$N = \frac{1}{|G|}(2(|G|-1) + |X|) = \frac{1}{|G|}\left(2(|G|-1) + \sum_{i=1}^{N} |x_i^G|\right).$$

This rearranges to

$$\begin{aligned} 2\left(1-\frac{1}{|G|}\right) &= N - \frac{1}{|G|}\sum_{i=1}^{N}|x_i^G| \\ &= N - \sum_{i=1}^{N}\frac{1}{|G_{x_i}|} \\ &= \sum_{i=1}^{N}\left(1-\frac{1}{|G_{x_i}|}\right). \end{aligned}$$

Assuming G is not the trivial group, the left-hand side of the above expression is greater than or equal to 1 and less than 2. But each stabilizer G_x has order at least 2 so that

$$\frac{1}{2} \leq 1 - \frac{1}{|G_{x_i}|} < 1,$$

for $1 \leq i \leq N$. Therefore, N is either 2 or 3.

If $N = 2$, the above equations give

$$2 = |x_1^G| + |x_2^G|$$

and there can only be two poles. These poles determine an axis L and every element of $G \setminus \{e\}$ must be a rotation about this axis. The plane which passes through the origin and which is perpendicular to L is rotated on itself by G. Therefore, G is isomorphic to a subgroup of SO_2 and has to be cyclic by Theorem 1.3.

If $N = 3$, writing x, y, z instead of x_1, x_2, x_3, we have

$$2\left(1-\frac{1}{|G|}\right) = 3 - \left(\frac{1}{|G_x|}+\frac{1}{|G_y|}+\frac{1}{|G_z|}\right)$$

and, therefore,

$$1 + \frac{2}{|G|} = \frac{1}{|G_x|}+\frac{1}{|G_y|}+\frac{1}{|G_z|}.$$

The sum of the three terms on the right-hand side is greater than 1, so there are only four possibilities for $(|G_x|, |G_y|, |G_z|)$:

$$(2,2,n), \quad \text{for any } n \geq 2, \quad (2,3,3), \quad (2,3,4), \quad (2,3,5).$$

From this it is possible to deduce the theorem. The theorem follows by carefully analyzing these case, we omit this part here. □

Remark 1.5. The rotational symmetry group of the tetrahedron is isomorphic to $\mathbb{A}_4$. Cube and octahedron have rotational symmetry group isomorphic to $\mathbb{S}_4$. Dodecahedron and icosahedron have rotational symmetry group isomorphic to $\mathbb{A}_5$.

Corollary 1.6. *If G is a finite subgroup of O_3, then G is isomorphic to a subgroup of one the following groups: $\mathbb{Z}_n \times \mathbb{Z}_2$, $n \geq 1$, $\mathbb{D}_n \times \mathbb{Z}_2$, $n \geq 2$, $\mathbb{A}_4 \times \mathbb{Z}_2$, $\mathbb{S}_4 \times \mathbb{Z}_2$, $\mathbb{A}_5 \times \mathbb{Z}_2$.*

1.2 Automorphism groups of graphs

Recall that a *(simple) graph* is a tuple $X = (V, E)$ such that $E \subseteq \binom{V}{2}$. An *automorphism* of X is a bijection $f \colon V \to V$ such that $\{x, y\} \in E \iff \{f(x), f(y)\} \in E$. The group of all automorphisms of X is denoted by $\mathrm{Aut}(X)$.

Theorem 1.7 (Frucht's theorem)**.** *For every finite group G, there is a graph X such that $G \cong \mathrm{Aut}(X)$.*

It is reasonable to consider what finite groups can be realized as automorphism groups of some restricted class of graphs. For instance, we can consider the class $\mathcal{T}$ of finite groups that can be realized as automorphism groups of trees.

Disconnected graphs. In order to characterize the groups belonging to $\mathcal{T}$, we will first derive a useful formula. Suppose that we have a disconnected graph X. We would like to be able to express its automorphism group in terms of its connected components. If X is a disjoint union of two non-isomorphic connected components Y and Y', then clearly $\mathrm{Aut}(X) \cong \mathrm{Aut}(Y) \times \mathrm{Aut}(Y')$. However, if X consists of, say, $k \geq 2$ copies of the same graph Y, then $\mathrm{Aut}(X)$ can no longer be expressed as a direct product.

In order to deal with this situation, we use the wreath product. Suppose that G acts on the set Ω. For each $\omega \in \Omega$, take a copy H_ω of a group H. The *wreath product* $H \wr G$ is the semidirect product of

$$K = \prod_{\omega \in \Omega} H_\omega$$

by G, where the homomorphism $G \to \mathrm{Aut}(K)$, required for the semidirect product, is defined naturally by the action of G on the coordinates of K.

As an example, we can apply this to the situation described above. In particular, we get that

$$\mathrm{Aut}(X) \cong \mathrm{Aut}(Y) \wr \mathbb{S}_k.$$

In general, we have the following formula.

Theorem 1.8. *Let $X_1, \ldots, X_n$ be pairwise non-isomorphic graphs and let X be the disconnected graph consisting of $k_i \in \mathbb{N}$ copies of the graph X_i, for $i = 1, \ldots, n$. Then*

$$\mathrm{Aut}(X) \cong \prod_{i=1}^{n} \mathrm{Aut}(X_i) \wr \mathbb{S}_{k_i}.$$

Using Theorem 1.8, one can easily determine the automorphism group if the automorphism groups of the connected components are known. We note that this can be further generalized to 2-connected and 3-connected components.

Trees. We are ready to characterize automorphism groups of trees.

Chapter 2

Basic notions