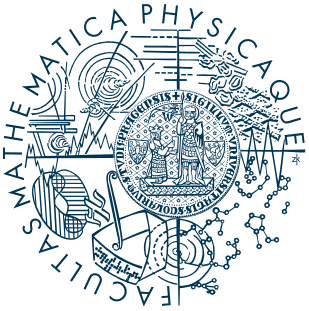
Permutation groups

Peter Zeman

Department of Algebra
Faculty of Mathematics and Physics
Charles University



May 7, 2026

Preface

These are lecture notes for the course NMAL432 Permutation Groups, taught at the Faculty of Mathematics and Physics, Charles University. The lecture notes are largely based on the german lecture notes Permutationsgruppen by Alice C. Niemeyer from RWTH Aachen University. Other sources are

- John D. Dixon, Brian Mortimer – Permutation Groups (1996),
- Peter Cameron – Permutation Groups (1999),
- Helmut Wielandt – Finite Permutation Groups (1964).

Contents

Preface **i**

1 Three motivating examples **1**
1.1 Finite groups of isometries 1
1.2 Automorphism groups of graphs 5
1.3 Isomorphism test for graphs with bounded color classes 6

2 Basic notions **9**
2.1 Actions of groups on sets 9
2.2 Similar actions 12

3 Orbits and constituents **13**
3.1 Invariant sets 13
3.2 Primitivity 15
3.3 Orbitals 18
3.4 Testing isomorphism of cubic graphs 32

4 Wreath products **36**
4.1 Semidirect products 36
4.2 Wreath Products 36
4.3 The imprimitive action 39
4.4 The primitive action 41

5 Socles of primitive permutation groups **48**
5.1 Centralizers and normalizers 48
5.2 The socle 56
5.2.1 Socles of primitive groups 58

Chapter 1

Three 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 $0 \leq \theta < 2\pi$. 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 the following

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

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, provided that 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. First, we reduce this problem to *rooted trees*, which are just trees with a distinguished vertex that has to be preserved by every automorphism.

Let T be a tree. The *center* of a tree is a set of vertices v that minimize the quantity

$$\max_{u \in V(T)} d(v, u),$$

where $d(v,u)$ is the length of the shortest path from v to u in T. Clearly, such vertices lie on every path of maximum length in T, and the center consists of either one or two vertices, based on the parity of this length. Moreover, the center is preserved by every automorphism. If the center consists of one vertex, we can make it a root. If it is of size two, we subdivide the edge between the two vertices by a new vertex, which will be the new root. Thus, we obtain a new rooted tree T_r with a root r such that $\mathrm{Aut}(T_r) \cong \mathrm{Aut}(T)$. On the other hand, if we start with a rooted tree T_r, we can attach a very long path to r that will force the center to be on this path. This gives an unrooted tree T with $\mathrm{Aut}(T) \cong \mathrm{Aut}(T_r)$.

Theorem 1.9 (Jordan, 1869)**.** *The class $\mathcal{T}$ of automorphism groups of trees can be inductively described as follows:*
(1) $\{1\} \in \mathcal{T}$.
(2) If $G, H \in \mathcal{T}$, *then* $G \times H \in \mathcal{T}$.
(3) If $G \in \mathcal{T}$, *then* $G \wr \mathbb{S}_n \in \mathcal{T}$, *for* $n \geq 2$.

Proof. By the argument above, it is sufficient consider only rooted trees. First we need to argue that all the operations (1)–(3) can be realized by some tree, which we do by induction.

Clearly the trivial group is the automorphism group of a tree with one vertex If $G, H \in \mathcal{T}$, then by induction hypothesis there are trees T_G and T_H that realize G and H, respectively. If G and H are not isomorphic then we can construct a tree T with $\mathrm{Aut}(T) \cong G \times H$ by attaching the roots of T_G and T_H to a common new root. If $G \cong H$, this construction creates new automorphisms. We fix this by subdividing one of the newly created edges. Finally, if $G \in \mathcal{T}$ and T_G realizes G, then we can construct T with $\mathrm{Aut}(T) \cong G \wr \mathbb{S}_n$ by attaching the roots of n copies of T_G to a common new root. We proved that every group in the class $\mathcal{T}$ is in fact an automorphism group of some tree.

It remains to show that for a rooted tree T, its automorphism group is isomorphic to a group in $\mathcal{T}$. We again proceed by induction. If T has one vertex, then the statement clearly holds. If T has more vertices, then we remove the root and get a forest of rooted trees. The automorphism group is determined by the formula in Theorem 1.8. It is clear that the only operations that appear in the formula are the direct product and the wreath product with symmetric groups. □

1.3 Isomorphism test for graphs with bounded color classes

In this section, we consider vertex-colored graphs (X, C). The *color class size* of (X, C) is

$$\max \left\{ \, |C^{-1}(c)| \;\middle|\; c \in \mathrm{rg}(C) \, \right\}.$$

We say that a class $\mathcal{C}$ of colored graphs has *bounded color class size* if there is a $k \in \mathbb{N}$ such that all $(X, C) \in \mathcal{C}$ have color class size at most k.

Theorem 1.10 (Babai; Furst, Hopcroft, Luks)**.** *For every class $\mathcal{C}$ of colored graphs of bounded color class size, there is a polynomial time isomorphism test.*

Proof. Suppose that the color class size of all graphs in $\mathcal{C}$ is at most k. We shall devise a polynomial time algorithm that computes the automorphism group of a given graph $(X, C) \in \mathcal{C}$. Observing that the polynomial time reduction from GI to AUT also yields a polynomial time reduction from $\mathrm{GI}(\mathcal{C})$ to $\mathrm{AUT}(\mathcal{C})$, we obtain the desired polynomial time algorithm for $\mathrm{GI}(\mathcal{C})$.

Let $(X, C) \in \mathcal{C}$. Suppose that $\mathrm{rg}(C) = \{c_1, \ldots, c_\ell\}$. For all $i \in [\ell]$, let $V_i := C^{-1}(c_i)$. Then $|V_i| \leq k$ for all $i \in [\ell]$ and the V_i form a partition of $V(X)$. Without loss of generality we assume that $\ell \geq 2$, because otherwise $|V(X)| \leq k$ and we can compute $\mathrm{Aut}(X)$ by brute-force.

Every automorphism of (X, C) maps V_i to V_i for all i. Thus we may view $\mathrm{Aut}(X, C)$ as a subgroup of

$$G_0 := \prod_{i=1}^{\ell} \mathrm{Sym}(V_i).$$

The elements of G_0 are tuples $g = (g_1, \ldots, g_\ell)$, where $g_i \in \mathrm{Sym}(V_i)$, and the action of G_0 on $V(X)$ is defined by

$$v^g = v^{g_i}$$

for the unique $i \in [\ell]$ such that $v \in V_i$.

Let $m := \binom{\ell}{2}$. We choose an arbitrary enumeration $p_1, \ldots, p_m$ of $\binom{[\ell]}{2}$. We inductively define groups $G_1, \ldots, G_m$ such that

$$G_0 \geq G_1 \geq G_2 \geq \cdots \geq G_m.$$

We have defined G_0 above, and for $i \in [m]$ with $p_i = rs$, we let G_i be the set of all

$$g = (g_1, \ldots, g_\ell) \in G_{i-1}$$

such that $(g_r, g_s) \in \mathrm{Aut}(X[V_r \cup V_s])$, where we regard $(g_r, g_s) \in \mathrm{Sym}(V_r) \times \mathrm{Sym}(V_s)$ as an element of $\mathrm{Sym}(V_r \cup V_s)$, as usually acting via

$$v^{(g_r, g_s)} = v^{g_r} \text{ if } v \in V_r \quad \text{and} \quad v^{(g_r, g_s)} = v^{g_s} \text{ if } v \in V_s.$$

Observe that

$$G_m = \mathrm{Aut}(X).$$

Claim 1. For all $i \in [m]$,

$$|G_{i-1} : G_i| \leq (k!)^2.$$

Proof. Let $i \in [m]$ and suppose that $p_i = rs$. Let T be a transversal of G_i in G_{i-1}. Let

$$t = (t_1, \ldots, t_\ell), \quad t' = (t'_1, \ldots, t'_\ell) \in T$$

be distinct.

Suppose for contradiction that $t_r = t'_r$ and $t_s = t'_s$. Then

$$t(t')^{-1} = (t_1(t'_1)^{-1}, \ldots, t_\ell(t'_\ell)^{-1}) \in G_i$$

because

$$(t_r(t'_r)^{-1},\, t_s(t'_s)^{-1}) = (\varepsilon, \varepsilon) \in \mathrm{Aut}(X[V_r \cup V_s]).$$

Hence $G_i t = G_i t'$, which contradicts T being a transversal.

It follows that

$$|T| \leq |\,\mathrm{Sym}(V_r) \times \mathrm{Sym}(V_s)| \leq (k!)^2.$$

□

Let Φ_0 be the set of all transpositions (v, w) with $v, w \in V_i$ for some i. Formally, we identify (v, w) with the element $(g_1, \ldots, g_\ell) \in G_0$ such that $g_i = (v, w) \in \mathrm{Sym}(V_i)$ and $g_j = \varepsilon$ for all $j \neq i$. Then Φ_0 is a generating set of G_0, which we can easily compute from (X, C) in polynomial time.

Note that we can check in polynomial time if a $g \in G_{i-1}$ is in G_i. Thus we can implement a membership oracle for G_i within G_{i-1} in polynomial time. It can be shown that using this, we can compute generating sets for all G_i, and in particular for $G_m = \mathrm{Aut}(X, C)$, in time polynomial in n and $k!$. As k is constant, this proves the theorem. □

Chapter 2

Basic notions

We deal only with finite groups. Throughout the following, all groups are finite, and the sets on which they act are finite as well.

2.1 Actions of groups on sets

Definition 2.1. Let G be a group and Ω a set. A function

$$\omega\colon \Omega \times G \to \Omega, \qquad (\alpha, g) \mapsto \omega(\alpha, g)$$

is called an *action of G on Ω* if the following conditions hold:

1. $\omega(\alpha, 1_G) = \alpha$ for all $\alpha \in \Omega$.
2. $\omega(\alpha, gh) = \omega(\omega(\alpha, g), h)$ for all $\alpha \in \Omega$ and $g, h \in G$.

The set Ω is called a *G-set*, and we say that G *acts on* Ω. Furthermore, $|\Omega|$ is called the *degree* of the action of G on Ω.

Remark 2.2. In general, we use the notation preferred by Wielandt, that is, we write α^g for $\omega(\alpha, g)$. Then the two conditions above can be reformulated as

1. $\alpha^{1_G} = \alpha$ for all $\alpha \in \Omega$.
2. $\alpha^{gh} = (\alpha^g)^h$ for all $\alpha \in \Omega$ and $g, h \in G$.

Definition 2.3. Let G be a group acting on a set Ω. If $\alpha^g = \alpha$ for some $\alpha \in \Omega$ and $g \in G$, then we say that g *fixes the element* α. The set

$$G_{(\Omega)} = \{g \in G \mid \alpha^g = \alpha \text{ for all } \alpha \in \Omega\}$$

is called the *kernel* of the action of G on Ω. If $G_{(\Omega)} = \{1_G\}$, then the action is called *faithful*.

Definition 2.4. Let G be a group and Ω a set. A homomorphism

$$\varphi\colon G \to \mathrm{Sym}(\Omega)$$

is called a *permutation representation of G on Ω*.

Theorem 2.5. *Let G be a group and Ω a set.*

1. *Given an action $\omega\colon \Omega \times G \to \Omega$ of G on Ω, there exists a permutation representation φ of G on Ω defined by*

$$\varphi(g) = \varphi_g, \qquad \text{where } \varphi_g \in \mathrm{Sym}(\Omega) \text{ and } \varphi_g(\alpha) = \omega(\alpha, g).$$

2. *Conversely, a permutation representation φ of G on Ω defines an action $\omega\colon \Omega \times G \to \Omega$ of G on Ω by*

$$\omega(\alpha, g) = \alpha^{\varphi(g)}.$$

Thus, it is not necessary to distinguish between actions of a group G on a set Ω and permutation representations of G on Ω. If G acts faithfully on Ω, then G is isomorphic to $\varphi(G)$.

Example 2.6.

(1) The symmetric group $\mathrm{Sym}(\Omega)$ acts on Ω via the natural action α^g, where $\alpha^g = g(\alpha)$, the image of $\alpha \in \Omega$ under g.

(2) A group acts on itself by right multiplication. Let G be a group and let $\Omega = G$. Define

$$\rho\colon \Omega \times G \to \Omega, \qquad (a, g) \mapsto \rho(a, g) = ag.$$

Then ρ is an action, since $\rho(a, 1_G) = a1_G = a$ for all $a \in \Omega = G$, and

$$\rho(a, gh) = agh = \rho(\rho(a, g), h)$$

for all $a \in \Omega = G$ and $g, h \in G$.
The kernel $G_{(\Omega)}$ of this action is

$$G_{(\Omega)} = \{g \in G \mid ag = a \ \forall a \in \Omega\} = \{g \in G \mid hg = h \ \forall h \in G\} = \{1_G\}.$$

This action is called the *right regular action* of G on Ω.

(3) A group acts on itself by left multiplication. Let G be a group and let $\Omega = G$. Define

$$\omega\colon \Omega \times G \to \Omega, \qquad (a, g) \mapsto \omega(a, g) = g^{-1}a.$$

Then ω is an action, since $\omega(a, 1_G) = 1_G^{-1}a = a$ for all $a \in \Omega = G$, and

$$\omega(a, gh) = (gh)^{-1}a = h^{-1}g^{-1}a = \omega(\omega(a, g), h)$$

for all $a \in \Omega = G$ and $g, h \in G$.
The kernel $G_{(\Omega)}$ of this action is $G_{(\Omega)} = \{1_G\}$.
This action is called the *left regular action* of G on Ω.

(4) Let Ω be a finite set with $|\Omega| = n$ and let $k < n$. Denote by $\binom{\Omega}{k}$ the set of all k-subsets of Ω. If G acts faithfully on Ω, then G also acts on $\binom{\Omega}{k}$, where for $A \in \binom{\Omega}{k}$ the action of $g \in G$ on A is defined by

$$A^g = \{a^g \mid a \in A\}.$$

The kernel $G_{(\Omega)}$ of this action is

$$\begin{aligned} G_{(\Omega)} &= \{g \in G \mid \alpha^g = \alpha \ \forall \alpha \in \Omega\} \\ &= \{g \in G \mid A^g = A \ \forall A \in \tbinom{\Omega}{k}\} \\ &= \{1_G\}. \end{aligned}$$

(5) Let G be a group and $\Omega = G$. Then G acts on Ω by

$$h^g = g^{-1}hg.$$

This action is called the *action of G on itself by conjugation.*
The kernel of this action is

$$\begin{aligned} G_{(\Omega)} &= \{g \in G \mid h^g = h \ \forall h \in \Omega\} \\ &= \{g \in G \mid hg = gh \ \forall h \in G\} \\ &= Z(G). \end{aligned}$$

(6) Let G be a group and Ω the set of all subgroups of G. Then G acts on Ω by

$$H^g = \{h^g \mid h \in H\}.$$

This action is called the *action of G on its subgroups by conjugation.*

(7) Let G be a group and H a subgroup of G. Then G acts on the set Ω of right cosets $\mathcal{R}_{G:H}$ of H in G by right multiplication via

$$(Hx)^g = Hxg.$$

This action is called the *action of G on the right cosets of H.*
The kernel of this action is

$$\begin{aligned} G_{(\Omega)} &= \{g \in G \mid (Hx)^g = Hx \ \forall Hx \in \Omega\} \\ &= \{g \in G \mid Hxg = Hx \ \forall Hx \in \Omega\} \\ &= \{g \in G \mid g \in x^{-1}Hx \ \forall Hx \in \Omega\} \\ &= \bigcap_{x \in G} x^{-1}Hx. \end{aligned}$$

In general, this action is not faithful. The group $G_{(\Omega)}$ is called the *G-core* of H. It is the largest normal subgroup of G contained in H.

(8) Let G be a subgroup of $\mathrm{GL}(n, \mathbb{F})$, the group of invertible $n \times n$ matrices over a field $\mathbb{F}$. Let $V = \mathbb{F}^n$. Then G acts on V by

$$v^g = vg.$$

The kernel of this action is

$$G_{(\Omega)} = \{g \in G \mid vg = v \ \forall v \in V\} = \{I\}.$$

(9) Let G be a subgroup of $\mathrm{GL}(n, \mathbb{F})$ and let $\mathrm{PG}(V)$ be the set of all 1-dimensional subspaces of V. Then G acts on $\mathrm{PG}(V)$ by

$$\langle v \rangle^g = \langle vg \rangle.$$

The kernel of this action is

$$\begin{aligned} G_{(\Omega)} &= \{g \in G \mid \langle vg \rangle = \langle v \rangle \ \forall \langle v \rangle \in \mathrm{PG}(V)\} \\ &= \{aI \mid a \in \mathbb{F}\}. \end{aligned}$$

The group $G/G_{(\Omega)}$ is called the *projective general linear group.*

2.2 Similar actions

If a group G acts on a set Ω, then for $g \in G$ we denote by $\bar{g}_\Omega \colon \Omega \to \Omega$, $\alpha \mapsto \alpha^g$, the map induced by g.

Definition 2.7 (Equivariance)**.** Let the group G act on the sets Ω and Γ. A map $\lambda \colon \Omega \to \Gamma$ is called *G-compatible* (or *equivariant*) if

$$\lambda(\alpha^g) = \lambda(\alpha)^g \qquad \text{for all } \alpha \in \Omega,\ g \in G.$$

This means that the diagram

$$\begin{array}{ccc} \Omega & \xrightarrow{\bar{g}_\Omega} & \Omega \\ {\scriptstyle\lambda}\downarrow & & \downarrow{\scriptstyle\lambda} \\ \Gamma & \xrightarrow{\bar{g}_\Gamma} & \Gamma \end{array}$$

is commutative for all $g \in G$. If, in addition, λ is bijective, then the actions (or the G-sets) are called *G-similar*, and λ is then called a *G-similarity*.

Let G be a group acting on Ω and let H be a group acting on Γ. Then G and H are called *permutation isomorphic* if there exists a bijection $\lambda \colon \Omega \to \Gamma$ and an isomorphism $\varphi \colon G \to H$ such that

$$\lambda(\alpha^g) = \lambda(\alpha)^{\varphi(g)} \qquad \text{for all } \alpha \in \Omega,\ g \in G.$$

Definition 2.8. Let G be a group acting on Ω. The action is called *transitive* if for every pair $(\alpha, \beta) \in \Omega \times \Omega$ there exists $g \in G$ such that $\alpha^g = \beta$.

Theorem 2.9 (Fundamental theorem for transitive G-sets)**.** *Let G be a group.*

(1) Let $H \leq G$. Then G acts transitively on the set $\mathcal{R}_{G:H}$ of right cosets by right multiplication:

$$\mathcal{R}_{G:H} \times G \to \mathcal{R}_{G:H}, \qquad (Ha, g) \mapsto Hag.$$

(2) Let G act transitively on the set Ω, let $\alpha \in \Omega$ and let $G_\alpha := \mathrm{Stab}_G(\alpha)$. Then Ω and $\mathcal{R}_{G:G_\alpha}$ are G-similar as G-sets:

$$\lambda \colon \Omega \to \mathcal{R}_{G:G_\alpha}, \qquad \alpha^g \mapsto G_\alpha g$$

is a G-similarity.

(3) Every transitive G-set Ω determines a conjugacy class $\mathcal{U}_\Omega$ of subgroups of G, namely

$$\mathcal{U}_\Omega := \{G_\alpha \mid \alpha \in \Omega\},$$

and the map

$$\Omega \to \mathcal{U}_\Omega, \qquad \alpha \mapsto G_\alpha$$

is G-equivariant. Moreover, Ω is G-similar to a transitive G-set Γ if and only if $\mathcal{U}_\Omega = \mathcal{U}_\Gamma$.

Chapter 3

Orbits and constituents

3.1 Invariant sets

For a subset $\Delta \subseteq \Omega$ and $g \in G$ we define

$$\Delta^g = \{\delta^g \mid \delta \in \Delta\}.$$

Definition 3.1. Let G be a group acting on a set Ω via $(\alpha, g) \mapsto \alpha^g$. A subset $\Delta \subseteq \Omega$ is called *G-invariant* if $\Delta^g = \Delta$ for all $g \in G$.

Let G be a group acting on a set Ω and let Δ be a G-invariant subset of Ω. Then we can restrict the action of G on Ω to an action of G on Δ. For $g \in G$ let g^Δ denote the permutation induced by g on Δ. Then

$$\varphi\colon G \to G^\Delta, \qquad g \mapsto g^\Delta$$

is a homomorphism. We denote by G^Δ the image of φ, that is, the group induced by G on Δ. Thus $G^\Delta \cong G/G_{(\Delta)}$, where $G_{(\Delta)}$ is the kernel of φ, i.e. the kernel of the action of G on Δ.

We call G^Δ the *Δ-constituent* of G. The *transitive constituents of* G are precisely the constituents of G on the orbits of G on Ω.

Definition 3.2. Let G be a group acting on a set Ω via $(\alpha, g) \mapsto \alpha^g$ and let $\Delta \subseteq \Omega$. The *setwise stabilizer* of Δ in G is

$$G_\Delta = \{g \in G \mid \Delta^g = \Delta\}.$$

The *pointwise stabilizer* of Δ in G is

$$\{g \in G \mid \delta^g = \delta \ \forall\, \delta \in \Delta\} = \{g \in G \mid g^\Delta = 1\} = G_{(\Delta)}.$$

Note that for $\Delta = \{\alpha\}$ we have $G_{(\Delta)} = G_\alpha$.

Let again Δ be a G-invariant subset of Ω. It is clear that G_Δ and $G_{(\Delta)}$ are subgroups of G. Moreover, $G_{(\Delta)} \leq G_\Delta$ and $G_{(\Delta)} \trianglelefteq G$, since $G_{(\Delta)}$ is the kernel of a homomorphism.

Lemma 3.3. *Let p be a prime, $G \leq \mathrm{Sym}(\Omega)$ and $\alpha \in \Omega$. If $p^m \mid |\alpha^G|$, then for every p-Sylow subgroup P of G we have $p^m \mid |\alpha^P|$.*

Proof. We have

$$|G : P_\alpha| = |G : P|\,|P : P_\alpha| = |G : P|\,|\alpha^P|.$$

On the other hand,

$$|G : P_\alpha| = |G : G_\alpha|\,|G_\alpha : P_\alpha| = |\alpha^G|\,|G_\alpha : P_\alpha|.$$

Since $p^m \mid |\alpha^G|$, it follows that $p^m \mid |G : P|\,|\alpha^P|$. But P is a p-Sylow subgroup, hence $p \nmid |G : P|$, and therefore $p^m \mid |\alpha^P|$. □

Lemma 3.4. *Let p be a prime, $G \leq \mathrm{Sym}(\Omega)$ and $\alpha \in \Omega$. Let m be the largest natural number such that $p^m \mid |\alpha^G|$. Let $\Delta = \beta^P$ be an orbit of a p-Sylow subgroup P of G on α^G of minimal length. Then $|\Delta| = p^m$.*

Proof. Assume $\Delta = \beta^P$ for some $\beta \in \alpha^G$. Since P is a p-Sylow subgroup, the length of every P-orbit is a power of p. By Lemma 3.3 we have $p^m \mid |\Delta|$. Suppose $p^{m+1} \mid |\Delta|$. The orbits of P on α^G form a partition of α^G. As every orbit length is a power of p and Δ is an orbit of minimal length, it follows that p^{m+1} divides $|\alpha^G|$, contradicting the choice of m. Hence $|\Delta| = p^m$. □

Corollary 3.5. *Let p be a prime, $G \leq \mathrm{Sym}(\Omega)$ and $\alpha \in \Omega$. Let m be the largest natural number such that $p^m \mid |\alpha^G|$. Let $\Delta = \beta^P$ be an orbit of a p-Sylow subgroup P of G on α^G of minimal length. Then $|G_\beta : P_\beta|$ is not divisible by p.*

Proof. Analogously to the proof of Lemma 3.3, we obtain

$$|\beta^G|\,|G_\beta : P_\beta| = |G : P|\,|\beta^P|.$$

Since $p \nmid |G : P|$ and $|\beta^P| = p^m$, it follows that p^m is the highest power of p dividing $|\beta^G|\,|G_\beta : P_\beta|$. But p^m already divides $|\beta^G|$, and hence $p \nmid |G_\beta : P_\beta|$. □

Definition 3.6. Let G be a group and let U, V be subgroups of G. Then U and V are called *G-conjugate* if there exists $g \in G$ such that $U^g = g^{-1}Ug = V$. The *normalizer* of U in G is

$$N_G(U) = \{g \in G \mid gU = Ug\}.$$

For $G \leq \mathrm{Sym}(\Omega)$ define

$$\mathrm{Fix}_\Omega(G) = \{\alpha \in \Omega \mid \alpha^g = \alpha \ \forall\, g \in G\}.$$

Theorem 3.7. *Let $G \leq \mathrm{Sym}(\Omega)$ be transitive and let $\alpha \in \Omega$. Let $U \leq G_\alpha$. Assume that U is conjugate in G_α to every subgroup $V \leq G_\alpha$ which is conjugate to U in G. Then $N_G(U)$ is transitive on $\mathrm{Fix}_\Omega(U)$.*

Proof. Put $\Phi = \mathrm{Fix}_\Omega(U)$ and $N = N_G(U)$. Let $n \in N$ and $\psi \in \Phi$. For $u \in U$ we have

$$(\psi^n)^u = \psi^{nu} = \psi^{nun^{-1}n} = \psi^{u'n} = \psi^n.$$

Thus every $u \in U$ fixes ψ^n, hence $\psi^n \in \mathrm{Fix}_\Omega(U)$. Therefore $\Phi^N = \Phi$.

It remains to show that $N_G(U)$ acts transitively on $\mathrm{Fix}_\Omega(U)$. Let $\beta \in \mathrm{Fix}_\Omega(U)$. Since G is transitive on Ω, there exists $g \in G$ with $\alpha = \beta^g$. Put $V = U^g$. For each $v \in V$ there exists $u \in U$ with $v = u^g$. Then

$$\alpha^v = \alpha^{u^g} = \alpha^{g^{-1}ug} = \beta^{ug} = \beta^g = \alpha,$$

since $\beta \in \mathrm{Fix}_\Omega(U)$. Thus $\alpha^v = \alpha$ for all $v \in V$, so $V \leq G_\alpha$. Hence U and V are conjugate subgroups of G which both lie in G_α. By assumption, there exists $h \in G_\alpha$ with $V^h = U$. Thus $U^{gh} = U$, so $gh \in N_G(U)$. Moreover,

$$\beta^{gh} = \alpha^h = \alpha,$$

since $h \in G_\alpha$. □

Corollary 3.8. *Let $G \leq \mathrm{Sym}(\Omega)$ be transitive and let $\alpha \in \Omega$. Then $N_G(G_\alpha)$ is transitive on $\mathrm{Fix}_\Omega(G_\alpha)$.*

Corollary 3.9. *Let $G \leq \mathrm{Sym}(\Omega)$ be transitive and let $\alpha \in \Omega$. Let P be a p-Sylow subgroup of G_α. Then $N_G(P)$ is transitive on $\mathrm{Fix}_\Omega(P)$.*

3.2 Primitivity

Definition 3.10. Let G be a group acting on a set Ω via $(\alpha, g) \mapsto \alpha^g$. A non-empty subset $\Delta \subseteq \Omega$ is called a *block* (of G) if for all $g \in G$ we have

$$\Delta^g \cap \Delta = \Delta \qquad \text{or} \qquad \Delta^g \cap \Delta = \varnothing.$$

Obviously, Ω and the sets $\{\alpha\}$ for $\alpha \in \Omega$ are always blocks of G. These blocks are called *trivial blocks*. A block with at least two elements is called *minimal* if it contains no proper non-trivial block.

Lemma 3.11. *Let G be a group acting transitively on a set Ω via $(\alpha, g) \mapsto \alpha^g$. Let Γ and Δ be two blocks of G with non-trivial intersection. Then $\Gamma \cap \Delta$ is also a block of G.*

Proof. Let $g \in G$. Since Γ and Δ are blocks, we have either $\Gamma^g = \Gamma$ or $\Gamma^g \cap \Gamma = \varnothing$, and likewise either $\Delta^g = \Delta$ or $\Delta^g \cap \Delta = \varnothing$.

Suppose first that $(\Gamma \cap \Delta)^g \cap (\Gamma \cap \Delta) \neq \varnothing$. Since Γ and Δ are blocks, this implies $\Gamma^g = \Gamma$ and $\Delta^g = \Delta$. Hence $(\Gamma \cap \Delta)^g = \Gamma^g \cap \Delta^g = \Gamma \cap \Delta$. Otherwise, $(\Gamma \cap \Delta)^g \cap (\Gamma \cap \Delta) = \varnothing$. Thus $\Gamma \cap \Delta$ is a block. □

Definition 3.12. Let G be a group acting transitively on a set Ω via $(\alpha, g) \mapsto \alpha^g$. Then G is called *imprimitive* if G possesses a non-trivial block. Otherwise, G is called *primitive*.

A partition Σ of Ω is called *G-invariant* if for every $\Delta \in \Sigma$ and every $g \in G$ we have $\Delta^g \in \Sigma$.

Lemma 3.13. *Let G be a group acting transitively on a set Ω via $(\alpha, g) \mapsto \alpha^g$. A subset Δ is a block of G if and only if*

$$\Sigma = \{\Delta^g \mid g \in G\}$$

is a G-invariant partition of Ω.

Proof. ($\Longrightarrow$) For $\Delta^g \in \Sigma$ and $h \in G$ we have $(\Delta^g)^h = \Delta^{gh} \in \Sigma$. Also, the members of Σ cover Ω because G is transitive: if $\alpha \in \Delta$ and $\omega \in \Omega$, then $\omega = \alpha^g$ for some $g \in G$, so $\omega \in \Delta^g$.

Finally, if $\Delta^g \cap \Delta^h \neq \varnothing$, then applying h^{-1} gives

$$\Delta^{gh^{-1}} \cap \Delta \neq \varnothing.$$

Since Δ is a block, it follows that $\Delta^{gh^{-1}} = \Delta$, hence $\Delta^g = \Delta^h$. Therefore distinct members of Σ are disjoint, so Σ is a partition.

($\Longleftarrow$) Assume that $\Sigma = \{\Delta^g \mid g \in G\}$ is a G-invariant partition of Ω. For any $g \in G$, both Δ and Δ^g lie in the partition Σ, so either they are equal or disjoint. Hence

$$\Delta^g \cap \Delta = \Delta \quad \text{or} \quad \Delta^g \cap \Delta = \varnothing,$$

and therefore Δ is a block. □

Lemma 3.14. *Let G be a group acting transitively on a set Ω via $(\alpha, g) \mapsto \alpha^g$. Let Δ be a block of G. Then G_Δ acts transitively on Δ. In particular,*

$$\Delta = \beta^{G_\Delta} \qquad \text{for every } \beta \in \Delta.$$

Proof. Let $\beta, \gamma \in \Delta$ with $\beta \neq \gamma$. Since G acts transitively on Ω, there exists $g \in G$ with $\beta^g = \gamma$. In particular, $\gamma \in \Delta \cap \Delta^g$. As Δ is a block, it follows that $\Delta = \Delta^g$ and hence $g \in G_\Delta$. Therefore G_Δ acts transitively on Δ. □

Lemma 3.15. *Let G be a group acting on a set Ω via $(\alpha, g) \mapsto \alpha^g$, and let $\alpha \in \Omega$. Let $H \leq G$ with $G_\alpha \leq H$. Then for $\Delta = \alpha^H$ we have*

$$G_\Delta = H.$$

Proof. Since $\Delta = \alpha^H$, clearly $H \leq G_\Delta$.

Let $g \in G_\Delta$, i.e. $\Delta^g = \Delta$. Then for each $\beta \in \Delta$ there exist $h, k \in H$ such that $\beta = \alpha^h$ and

$$\beta = \alpha^{kg}.$$

Hence $kg^{-1} \in G_\alpha \leq H$, and therefore $g \in H$. Thus $G_\Delta \leq H$. □

The following theorem describes a relationship between the subgroups of G that contain a point stabilizer and the blocks of G containing this point (see [2, Theorem 1.5A]).

Theorem 3.16. *Let G be a group acting transitively on a set Ω via $(\alpha, g) \mapsto \alpha^g$ and let $\alpha \in \Omega$. Let $\mathcal{B}$ be the set of all blocks of G containing α and let $\mathcal{S}$ be the set of all subgroups of G containing G_α. Then $\Psi : \mathcal{B} \to \mathcal{S}$ defined by $\Psi(\Delta) = G_\Delta$ is a bijection. The map $\Phi = \Psi^{-1}$ is given by $\Phi(H) = \alpha^H$. Moreover, Ψ is compatible with the inclusion ordering.*

Proof. First we show that for a block Δ containing α we have $\Psi(\Delta) \in \mathcal{S}$. By definition $\Psi(\Delta) = G_\Delta$. Since $\alpha \in \Delta$, for $g \in G_\alpha$ we have

$$\alpha^g = \alpha \in \Delta \cap \Delta^g.$$

As Δ is a block, it follows that $\Delta^g = \Delta$ for all $g \in G_\alpha$. Hence $G_\alpha \leq G_\Delta$, so $G_\Delta \in \mathcal{S}$.

Now we show that for a subgroup H with $G_\alpha \leq H$ the set $\Phi(H)$ is a block of G containing α. Since $\Phi(H) = \alpha^H$, it is obvious that $\Phi(H)$ contains α. Let $\Delta = \Phi(H)$. Assume $\Delta^g \cap \Delta \neq \varnothing$ for some $g \in G$. Then there exists $\beta \in \Omega$ with $\beta \in \Delta^g \cap \Delta$. In particular, $\beta = \alpha^h$ and $\beta = \alpha^{kg}$ for suitable $h, k \in H$. Thus $kgh^{-1} \in G_\alpha \leq H$, hence $g \in H$. But then $\Delta^g = \Delta$ for all $g \in H$, since Δ is an H-orbit. Thus Δ is a block.

It remains to show that $\Psi \circ \Phi = 1$ and $\Phi \circ \Psi = 1$. By Lemma 3.15,

$$\Psi(\Phi(H)) = \Psi(\alpha^H) = G_{\alpha^H} = H.$$

By Lemma 3.14,

$$\Phi(\Psi(\Delta)) = \Phi(G_\Delta) = \alpha^{G_\Delta} = \Delta.$$

Finally we show that Ψ is compatible with the inclusion ordering. Suppose $G_\Delta \leq G_\Gamma$. Then in particular

$$\Delta = \alpha^{G_\Delta} \subseteq \alpha^{G_\Gamma} = \Gamma.$$

Conversely, suppose $\Delta \subseteq \Gamma$. For $g \in G_\Delta$ we have $\Delta \subseteq \Gamma \cap \Gamma^g$. Since Γ is a block, it follows that $\Gamma = \Gamma^g$ and hence $g \in G_\Gamma$. Therefore $G_\Delta \leq G_\Gamma$. □

This immediately yields the following important consequence.

Theorem 3.17. *Let G be a group acting transitively on a set Ω with $|\Omega| \geq 2$. Then the following statements are equivalent:*

(1) G is primitive on Ω.
(2) For every $\alpha \in \Omega$, the stabilizer G_α is a maximal subgroup of G.
(3) For some $\alpha \in \Omega$, the stabilizer G_α is a maximal subgroup of G.

An important example of permutation–isomorphic groups is the following.

Theorem 3.18. *Let G be a group acting transitively on the set Ω, and let $N \trianglelefteq G$. Then the following hold:*

(1) The orbits of N form a block system for G.
(2) The actions of N^Δ on Δ and N^Γ on Γ for two N-orbits Δ, Γ are permutation–isomorphic.
(3) If there exists $\gamma \in \Omega$ with $\gamma^h = \gamma$ for all $h \in N$, then $N \leq G_{(\Omega)}$.
(4) N has at most $[G : N]$ orbits on Ω. If $[G : N]$ is finite, then the number of N-orbits divides $[G : N]$.
(5) If G acts primitively on Ω, then N is either transitive or $N \leq G_{(\Omega)}$.

Proof. (1) Let $\Delta = \alpha^N$ for $\alpha \in \Omega$. Then

$$\Delta^g = (\alpha^N)^g = (\alpha^g)^N.$$

Thus Δ^g is the orbit of α^g under N. Hence the N-orbits partition Ω. Since G acts transitively on Ω, the set $\{\Delta^g \mid g \in G\}$ forms a block system for G.

(2) Let $\Delta = \alpha^N$ and $\Gamma = \beta^N$. Since Δ and Γ are blocks and G is transitive, there exists $g \in G$ with $\Delta^g = \Gamma$. Define $\lambda : \Delta \to \Gamma$ by

$$\lambda(\delta) = \delta^g.$$

This is a bijection.
Define

$$\varphi : N^\Delta \to N^\Gamma, \qquad \varphi(h^\Delta) = (g^{-1}hg)^\Gamma.$$

Then φ is injective, since $\varphi(h^\Delta) = \varphi(k^\Delta)$ iff

$$(g^{-1}hg)^\Gamma = (g^{-1}kg)^\Gamma,$$

which holds exactly when $g^{-1}hk^{-1}g \in N_{(\Gamma)}$. As $\Gamma = \Delta^g$, this is equivalent to $hk^{-1} \in N_{(\Delta)}$, that is, $h^\Delta = k^\Delta$.
The map φ is also surjective because $g^{-1}Ng = N$. Finally, φ is a homomorphism since for $h, k \in N$

$$\varphi(h^\Delta k^\Delta) = \varphi((hk)^\Delta) = (g^{-1}hkg)^\Gamma = (g^{-1}hg)^\Gamma(g^{-1}kg)^\Gamma = \varphi(h^\Delta)\varphi(k^\Delta).$$

Moreover, for $\delta \in \Delta$ and $k \in N$ we have

$$\lambda(\delta^k) = \delta^{kg} = (\delta^g)^{g^{-1}kg} = (\lambda(\delta))^{\varphi(k)}.$$

Thus the actions are permutation–isomorphic.

(3) Suppose there exists $\gamma \in \Omega$ such that $\gamma^h = \gamma$ for all $h \in N$. Then $\gamma^N = \{\gamma\}$. Since the N-orbits form a block system, all N-orbits have size 1, so $N \leq G_{(\Omega)}$.

(4) It is clear that there can be at most $[G : N]$ orbits. If $[G : N]$ is finite, then all N-orbits have the same size, so the number of N-orbits divides $[G : N]$.

(5) If G acts primitively, then either there is only one N-orbit, so N is transitive, or all N-orbits have size 1, and hence $N \leq G_{(\Omega)}$.

□

3.3 Orbitals

The material and proofs in this section are largely taken from the book by Dixon and Mortimer.

Definition 3.19. Let G be a group acting transitively on a set Ω. The orbits of G on $\Omega \times \Omega$ are called the *orbitals* of G on Ω. We denote by $\mathcal{O}(G)$ the set of orbitals of G. A union of orbitals is called a *generalized orbital*. The orbital

$$\Delta_1 = \{(\alpha, \alpha) \mid \alpha \in \Omega\}$$

is called the *diagonal orbital*. For an orbital Δ define

$$\Delta^* = \{(\beta, \alpha) \mid (\alpha, \beta) \in \Delta\}.$$

An orbital is called *self-dual* if $\Delta^* = \Delta$. For an orbital Δ and $\alpha \in \Omega$ let

$$\Delta(\alpha) = \{\beta \in \Omega \mid (\alpha, \beta) \in \Delta\}.$$

For example, the diagonal orbital is self-dual.

Lemma 3.20. *Let G be a group acting transitively on a set Ω and let $\alpha \in \Omega$. The orbitals of G are in bijection with the orbits of G_α on Ω via the map*

$$\varphi \colon \mathcal{O}(G) \to \Omega/G_\alpha, \qquad \Delta \mapsto \Delta(\alpha).$$

Proof. Let $\Delta \in O(G)$. We first show that $\Delta(\alpha)$ is a G_α-orbit. Let $(\beta, \gamma) \in \Delta$. Since G acts transitively on Ω, there exists $g \in G$ with $\beta^g = \alpha$. Hence $(\alpha, \gamma^g) \in \Delta$ and so $\gamma^g \in \Delta(\alpha)$; in particular $\Delta(\alpha) \neq \varnothing$.

Next we show that $\Delta(\alpha)$ is invariant under G_α. If $\gamma \in \Delta(\alpha)$, then $(\alpha, \gamma) \in \Delta$, and for $g \in G_\alpha$ we have $(\alpha, \gamma^g) \in \Delta^g = \Delta$. Thus $\gamma^g \in \Delta(\alpha)$, so $\Delta(\alpha)$ is a union of G_α-orbits.

It remains to show that $\Delta(\alpha)$ is a single G_α-orbit. Let $\gamma_1, \gamma_2 \in \Delta(\alpha)$. Then $(\alpha, \gamma_1), (\alpha, \gamma_2) \in \Delta$. Since Δ is a G-orbit, there exists $g \in G$ with $(\alpha, \gamma_1)^g = (\alpha, \gamma_2)$. Hence $\alpha^g = \alpha$, so $g \in G_\alpha$, and $\gamma_1^g = \gamma_2$. Thus $\Delta(\alpha)$ is a G_α-orbit.

To see that φ is injective, suppose $\varphi(\Delta) = \varphi(\Psi)$. Then $\Delta(\alpha) = \Psi(\alpha)$. Since both are G_α-orbits, $\Delta(\alpha) = \beta^{G_\alpha} = \Psi(\alpha)$ for some $\beta \in \Delta(\alpha)$. Hence $(\alpha, \beta) \in \Delta \cap \Psi$. But Δ and Ψ are both G-orbits in $\Omega \times \Omega$, so $\Delta = \Psi = (\alpha, \beta)^G$.

Finally, φ is surjective. Let β^{G_α} be a G_α-orbit. Then $\Delta = (\alpha, \beta)^G$ is an orbital of G with $\Delta(\alpha) = \beta^{G_\alpha}$. □

Remark 3.21. Note that $\Delta(\alpha)$ does not depend on the choice of α. Since G acts transitively on Ω, for every $\beta \in \Omega$ there exists $g \in G$ with $\alpha^g = \beta$. Hence

$$G_\beta = G_{\alpha^g} = (G_\alpha)^g.$$

Thus G_β and G_α have the same number of orbits on Ω. Let $(\alpha, \beta) \in \Delta$. Then $(\alpha^g, \beta^g) \in \Delta$ and hence

$$\Delta(\alpha^g) = (\beta^g)^{G_{\alpha^g}} = (\beta^g)^{g^{-1} G_\alpha g} = \beta^{G_\alpha g} = (\beta^{G_\alpha})^g = \Delta(\alpha)^g.$$

Definition 3.22. An orbit of G_α on Ω is called a *suborbit* of G on Ω.

Lemma 3.23. *Let G be a group acting transitively on a set Ω, and let $\alpha \in \Omega$. The map*

$$\psi\colon \mathcal{O}(G) \to G_\alpha \backslash G / G_\alpha, \qquad \Delta \mapsto G_\alpha h G_\alpha \quad \text{for } (\alpha, \alpha^h) \in \Delta$$

from the set of orbitals of G to the set of double cosets of G_α in G is a bijection.

Proof. Since the definition of ψ depends on the choice of $h \in G$, we first show that ψ is well defined. Let $h, k \in G$ with $(\alpha, \alpha^h), (\alpha, \alpha^k) \in \Delta$. Then there exists $g \in G$ with

$$(\alpha, \alpha^h)^g = (\alpha, \alpha^k).$$

In particular $g \in G_\alpha$ and $\alpha^{hg} = \alpha^k$. Thus $hgk^{-1} \in G_\alpha$, and therefore

$$G_\alpha k G_\alpha = (G_\alpha hgk^{-1})k(g^{-1}G_\alpha) = G_\alpha h G_\alpha.$$

Next we show that ψ is injective. Let Δ and Ψ be orbitals with $\psi(\Delta) = \psi(\Psi)$. Then $G_\alpha h G_\alpha = G_\alpha k G_\alpha$ for suitable $h, k \in G$, which holds exactly when $k = g_1 h g_2$ for some $g_1, g_2 \in G_\alpha$. Hence

$$(\alpha, \alpha^k) = (\alpha, \alpha^{g_1 h g_2}) = (\alpha, \alpha^{h g_2}) = (\alpha, \alpha^h)^{g_2}.$$

Thus $(\alpha, \alpha^h) \in \Delta$ and $(\alpha, \alpha^k) \in \Psi$ lie in the same G-orbit, so $\Delta = \Psi$.

Finally we show that ψ is surjective. Let $G_\alpha g G_\alpha$ be a double coset. Then (α, α^g) lies in some orbital Δ, and by definition $\psi(\Delta) = G_\alpha g G_\alpha$. □

In particular, the number of orbitals of G on Ω is equal to the number of orbits that G_α has on Ω, and also equal to the number of double cosets of G_α in G.

Definition 3.24. The number of orbitals of G on Ω is called the *rank* of the group G.

For completeness, we recall a few definitions from graph theory.

Definition 3.25. A *directed graph* (di-graph) is a pair $\Gamma = (\Omega, K)$, where Ω is the set of *vertices* and $K \subseteq \Omega \times \Omega$ is the set of *edges*. The elements of K are called *edges* or *arcs*.

An *undirected graph* is a pair $\Gamma = (\Omega, K)$ where $K \subseteq \binom{\Omega}{2}$. The elements of K are called *edges*, and an ordered pair (α, β) with $\alpha, \beta \in \Omega$ is called an *arc* if $\{\alpha, \beta\} \in K$.

Note that for a digraph the notions of arcs and edges coincide, but edges and arcs may differ for an undirected graph. In particular, an undirected graph cannot have loops.

Definition 3.26. An *automorphism* of a (di-)graph $\Gamma = (\Omega, K)$ is an element $g \in \mathrm{Sym}(\Omega)$ such that

$$e^g \in K \quad \text{if and only if} \quad e \in K.$$

The set of all automorphisms of Γ forms a subgroup of $\mathrm{Sym}(\Omega)$, called the *automorphism group* of Γ.

A subgroup $G \leq \mathrm{Aut}(\Gamma)$ is called

- *G-edge-transitive* if G acts transitively on K,
- *G-vertex-transitive* if G acts transitively on Ω,
- *G-arc-transitive* if G acts transitively on the arcs.

For an orbital Δ we define the directed graph diGraph(Δ) to be the graph with vertex set Ω and edge set Δ. We call diGraph(Δ) the *directed orbital graph* of Δ and uGraph(Δ) the *undirected orbital graph* of Δ.

Definition 3.27. Let $\Gamma = (\Omega, K)$ be a graph. A sequence $(\alpha_1, \alpha_2, \ldots, \alpha_k) \in \Omega^k$ is called an *undirected path* from α to β in Γ if $\alpha_i \neq \alpha_{i+1}$ for $1 \leq i \leq k-1$, $\alpha_1 = \alpha$, $\alpha_k = \beta$, and either

$$\{\alpha_i, \alpha_{i+1}\} \in K$$

if Γ is undirected, or

$$(\alpha_i, \alpha_{i+1}) \in K \quad \text{or} \quad (\alpha_{i+1}, \alpha_i) \in K$$

if Γ is directed, for $1 \leq i < k$.

The path is called a *directed path* if

$$(\alpha_i, \alpha_{i+1}) \in K \qquad \text{for } 1 \leq i < k.$$

The graph Γ is called *connected* if for all $\alpha, \beta \in \Omega$ with $\alpha \neq \beta$ there exists an undirected path from α to β in Γ.

A directed graph Γ is called *strongly connected* if for all $\alpha, \beta \in \Omega$ with $\alpha \neq \beta$ there exists a directed path from α to β in Γ.

Remark 3.28.

(1) A G-vertex-transitive graph Γ with $G \leq \mathrm{Aut}(\Gamma)$ need not be connected. Consider the graph Γ whose two connected components are both K_3. Then

$$\mathrm{Aut}(\Gamma) \cong C_2 \times S_3,$$

since each connected component admits an S_3 and the two components may be interchanged. Nevertheless, G acts vertex-transitively.

(2) We can define an equivalence relation on the vertex set Ω of a graph $\Gamma = (\Omega, K)$ by

$$\alpha \sim \beta \quad \text{if and only if there exists an undirected path from } \alpha \text{ to } \beta \text{ in } \Gamma.$$

The connected components of Γ are exactly the equivalence classes of $\sim$.

The following theorem shows that a transitive group G is also a subgroup of the automorphism group of an orbital graph.

Theorem 3.29. *Let G act transitively on Ω and let Δ be an orbital. Then the following hold:*
(1) G is a subgroup of the automorphism group of diGraph(Δ).
(2) G acts transitively on the vertex set of diGraph(Δ) *and on the edges of* diGraph(Δ).
If Δ is self-dual, then the following also hold:
(1) G is a subgroup of the automorphism group of uGraph(Δ).
(2) G acts transitively on the vertex set of uGraph(Δ) *and on the arcs of* uGraph(Δ).

Proof. Since Δ is an orbit in $\Omega \times \Omega$, it is in particular G-invariant. Hence the statements about the automorphism groups of uGraph(Δ) and diGraph(Δ) and the transitivity follow immediately. □

Theorem 3.30. *Let G act transitively on Ω and let Δ be a non-diagonal orbital with $(\alpha, \beta) \in \Delta$. Then the connected component of the directed graph on Δ containing α is the smallest block $B(\alpha, \beta)$ containing α and β.*

Proof. Let B be the connected component of the directed orbital graph of Δ that contains α. Then B is an equivalence class of the relation $\equiv$ defined by

$$\alpha \equiv \beta \quad \text{if and only if there exists an undirected path from } \alpha \text{ to } \beta \text{ in } \Delta.$$

Since the elements of G are automorphisms of diGraph(Δ), they map undirected paths to undirected paths, and therefore $\equiv$ is G-invariant. By Lemma 2.13, B is a block of G on Ω, and since B contains α and β, it follows that

$$B \supseteq B(\alpha, \beta).$$

Now let $\gamma \in B \setminus \{\alpha\}$. Then there exists an undirected path

$$\alpha = \alpha_0, \ldots, \alpha_t = \gamma$$

from α to γ in diGraph(Δ) for some $t \geq 1$. We claim that for $i = 0, \ldots, t-1$ we have

$$B(\alpha_i, \alpha_{i+1}) = B(\alpha, \beta).$$

For $i = 0$ we have that either (α, α_1) or (α_1, α) is an arc of diGraph(Δ). Since G acts transitively on the edges of diGraph(Δ), there exists $g \in G$ with

$$\{\alpha^g, \beta^g\} = \{\alpha, \alpha_1\}.$$

Hence

$$B(\alpha, \alpha_1) = B(\alpha, \beta)^g.$$

As $B(\alpha, \alpha_1) \cap B(\alpha, \beta)$ contains α, we obtain

$$B(\alpha, \alpha_1) = B(\alpha, \beta).$$

Assume now for some $i \geq 1$ that

$$B(\alpha_{i-1}, \alpha_i) = B(\alpha, \beta).$$

By the same argument as above there exists $g \in G$ with

$$\{\alpha_{i-1}^g, \alpha_i^g\} = \{\alpha_i, \alpha_{i+1}\}.$$

Thus

$$B(\alpha_i, \alpha_{i+1}) = B(\alpha_{i-1}, \alpha_i)^g.$$

Since $B(\alpha_i, \alpha_{i+1}) \cap B(\alpha_{i-1}, \alpha_i)$ contains α_i, we obtain

$$B(\alpha_i, \alpha_{i+1}) = B(\alpha, \beta).$$

By induction it follows that

$$B(\alpha, \beta) = B(\alpha_{t-1}, \gamma),$$

and therefore $\gamma \in B(\alpha, \beta)$. Hence $B = B(\alpha, \beta)$. □

This immediately yields the following theorem of D. G. Higman.

Theorem 3.31. *Let G act transitively on Ω. Then G is primitive on Ω if and only if* diGraph(Δ) *is connected for every orbital Δ which is not the diagonal orbital.*

Definition 3.32. A group G acting transitively on Ω is called *strongly primitive* if the orbital graph diGraph(Δ) is strongly connected for every orbital Δ that is not diagonal.

A *cycle* in a graph is a path whose initial and terminal vertices coincide. The following lemma is [2, Lemma 3.2A].

Lemma 3.33. *Let G be a group acting primitively on Ω. Then:*

(1) diGraph(Δ) *is strongly connected for an orbital Δ that is not diagonal if and only if* diGraph(Δ) *contains at least one non-trivial directed cycle.*

(2) If for every pair α, β with $\alpha \neq \beta$ there exists $g \in G$ that has a finite cycle containing α and β, then G is strongly primitive.

(3) Every finite group is strongly primitive.

Proof. (1) diGraph(Δ) is strongly connected if and only if every two vertices α, β with $\alpha \neq \beta$ lie on a directed cycle.
Conversely, suppose diGraph(Δ) contains at least one directed cycle. Define a relation $\equiv$ on Ω by declaring $\alpha \equiv \beta$ if and only if $\alpha = \beta$ or α and β lie on a non-trivial directed cycle in diGraph(Δ). Then $\equiv$ is an equivalence relation:

- reflexive, since $\alpha \equiv \alpha$,
- transitive, since if $\alpha \equiv \beta$ and $\beta \equiv \gamma$, then there are directed cycles containing α, β and β, γ, which can be combined to obtain a directed cycle containing α, γ,
- symmetric, since a directed cycle containing α, β also contains β, α,
- G-invariant, since Δ is a G-orbit on $\Omega \times \Omega$.

Thus $\equiv$ defines a block system. Since G is primitive and there exists a non-trivial cycle, the relation $\equiv$ must be universal, so every two vertices are equivalent. Hence diGraph(Δ) is strongly connected.

(2) Let Δ be an orbital with $(\alpha, \beta) \in \Delta$ and $\alpha \neq \beta$. By assumption there exists $g \in G$ having a finite cycle containing α and β. Choose a power of g such that $\alpha^{g^k} = \beta$, and set $h = g^k$. Then

$$\alpha, \alpha^h, \alpha^{h^2}, \ldots, \alpha^{h^m} = \alpha$$

forms a directed cycle in diGraph(Δ) containing α and β. Hence diGraph(Δ) is strongly connected by (1).

(3) This follows from (2), since G is transitive and hence we can choose $g \in G$ with $\alpha^g = \beta$. □

Remark 3.34. Statement (3) does not necessarily hold for infinite groups. For example, consider the group

$$G = \mathrm{Aut}(\mathbb{Q}, \leq)$$

of all permutations of $\mathbb{Q}$ that preserve the order $\leq$. Then G has two non-diagonal orbitals, namely

$$\Delta = \{(\alpha, \beta) \mid \alpha < \beta\} \quad \text{and} \quad \Delta^*.$$

It is clear that diGraph(Δ) and diGraph(Δ^*) are connected, but not strongly connected.

Theorem 3.35. *Let G be finite and act transitively on Ω. Then there exists a non-trivial self-dual G-orbital if and only if $|G|$ is even.*

Proof. Suppose Δ is a non-trivial self-dual orbital and let $(\alpha, \beta) \in \Delta$. Since Δ is self-dual, there exists $g \in G$ with

$$(\alpha^g, \beta^g) = (\beta, \alpha).$$

Hence $\alpha^g = \beta$ and $\beta^g = \alpha$. Thus g swaps α and β and therefore has even order. Hence $|G|$ is even.

Conversely, suppose $|G|$ is even. Then G contains an element g of order 2. Thus g swaps two points $\alpha, \beta \in \Omega$ with $\alpha \neq \beta$. The orbital of (α, β) is therefore non-diagonal and self-dual. □

We can now use the previous results to derive some results about the lengths of orbits of stabilizers.

Definition 3.36. Let G act transitively on Ω and suppose that G has k distinct orbitals. The *color graph* $\mathcal{G}$ of G is the directed graph with vertex set Ω and edge set $\Omega \times \Omega$. An edge $(\alpha, \beta) \in \Omega \times \Omega$ is colored with color i if (α, β) lies in the i-th orbital.

Then G acts on its color graph and preserves the coloring of the edges.

Definition 3.37. For subsets $\Sigma, \Lambda \subseteq \Omega \times \Omega$ we define

$$\Sigma \circ \Lambda := \{(\alpha, \beta) \mid (\alpha, \gamma) \in \Sigma,\ (\gamma, \beta) \in \Lambda \text{ for some } \gamma \in \Omega\}.$$

That is, $\Sigma \circ \Lambda$ is the set of all edges in $\Omega \times \Omega$ for which there exists a path of length 2 from α to β whose one edge lies in Σ and the other in Λ.

Lemma 3.38. *Let $\Sigma, \Lambda \subseteq \Omega \times \Omega$ be two G-invariant sets. Then $\Sigma \circ \Lambda$ is also G-invariant.*

Define

$$\Sigma(\alpha) = \{\beta \in \Omega \mid (\alpha, \beta) \in \Sigma\}.$$

Then $\Sigma(\alpha)$ is the set of all neighbours of α in the directed graph of Σ.

For an orbital Δ that is not the diagonal orbital, let $\Gamma = \Delta \cup \Delta^*$. Define $\Gamma^{(0)} = \Delta_1$, the diagonal orbital, and

$$\Gamma^{(k)} = \Gamma \circ \Gamma^{(k-1)}.$$

Example 3.39. Let

$$G = \langle (1,4)(2,5),\ (1,3,5)(2,4,6) \rangle \leq \mathrm{Sym}(6).$$

Then G has the following orbitals:

$$\begin{aligned}
\Delta_1 &= \{(1,1), (2,2), (3,3), (4,4), (5,5), (6,6)\},\\
\Delta_2 &= \{(1,2), (4,5), (3,4), (6,1), (3,1), (5,6), (6,4), (2,3), (5,3), (2,6), (1,5), (4,2)\},\\
\Delta_3 &= \{(1,3), (4,3), (3,5), (6,5), (3,2), (5,1), (6,2), (2,1), (5,4), (2,4), (1,6), (4,6)\},\\
\Delta_4 &= \{(1,4), (4,1), (3,6), (6,3), (5,2), (2,5)\}.
\end{aligned}$$

We see that for $\Gamma = \Delta_3$ the following holds:

$$\begin{aligned}
\Gamma^{(0)} &= \Delta_1,\\
\Gamma^{(1)} &= \Delta_3,\\
\Gamma^{(2)} &= \Delta_3 \circ \Delta_3 = \{(\alpha, \beta) \mid \exists \gamma :\ (\alpha, \gamma), (\gamma, \beta) \in \Delta_3\}\\
&= \{(1,5), (1,2), (2,6), (2,3), (3,4), (3,1), (4,2), (4,5), (5,3), (5,6), (6,4), (6,1)\} = \Delta_2.
\end{aligned}$$

$$\begin{aligned}\Delta_3 \circ \Delta_4 &= \{(\alpha,\beta) \mid \exists\gamma:\ (\alpha,\gamma)\in\Delta_3,\ (\gamma,\beta)\in\Delta_4\}\\ &= \{(1,3),(1,6),(2,1),(2,4),(3,5),(3,2),(4,6),(4,3),(5,1),(5,4),(6,2),(6,5)\} = \Delta_3,\end{aligned}$$

$$\begin{aligned}\Delta_3 \circ \Delta_2 &= \{(\alpha,\beta) \mid \exists\gamma:\ (\alpha,\gamma)\in\Delta_3,\ (\gamma,\beta)\in\Delta_2\}\\ &= \Delta_1 \cup \Delta_4.\end{aligned}$$

The following lemma is [2, Theorem 3.2B(i)].

Lemma 3.40. *Let G act transitively on Ω. Let $\Sigma, \Lambda \subseteq \Omega\times\Omega$ and suppose that Λ is G-invariant. Then*

$$|(\Sigma \circ \Lambda)(\alpha)| \le |\Sigma(\alpha)|\,|\Lambda(\alpha)|.$$

Proof. We have

$$\begin{aligned}(\Sigma \circ \Lambda)(\alpha) &= \{\beta\in\Omega \mid (\alpha,\beta)\in\Sigma\circ\Lambda\}\\ &= \{\beta\in\Omega \mid \exists\gamma \text{ with } (\alpha,\gamma)\in\Sigma \text{ and } (\gamma,\beta)\in\Lambda\}\\ &= \bigcup_{\gamma\in\Sigma(\alpha)} \Lambda(\gamma).\end{aligned}$$

Since Λ is G-invariant, for $g\in G$ we have

$$\begin{aligned}(\Lambda(\alpha))^g &= \{\beta\in\Omega \mid (\alpha,\beta)\in\Lambda\}^g\\ &= \{\beta^g\in\Omega \mid (\alpha,\beta)\in\Lambda\}\\ &= \{\beta^g\in\Omega \mid (\alpha^g,\beta^g)\in\Lambda^g\}\\ &= \{\beta'\in\Omega \mid (\alpha^g,\beta')\in\Lambda\}\\ &= \Lambda(\alpha^g).\end{aligned}$$

By transitivity of G on Ω, it follows that $|\Lambda(\gamma)| = |\Lambda(\alpha)|$ for all $\gamma\in\Omega$. Hence

$$|(\Sigma \circ \Lambda)(\alpha)| \le \sum_{\gamma\in\Sigma(\alpha)} |\Lambda(\gamma)| = |\Sigma(\alpha)|\,|\Lambda(\alpha)|.$$

□

Theorem 3.41. *Let G be primitive and let Δ be a non-diagonal orbital of G. Then the following hold:*

(1) For $\Gamma = \Delta\cup\Delta^*$,

$$\bigcup_{k\ge 0} \Gamma^{(k)} = \Omega\times\Omega.$$

(2) If G has finite rank r, then

$$\bigcup_{0\le k\le r-1} \Gamma^{(k)} = \Omega\times\Omega.$$

(3) If diGraph(Δ) *is strongly connected, then the above statements also hold for $\Gamma = \Delta$.*

Proof. (1) We have

$$\Gamma^{(k)} = \{(\alpha, \beta) \in \Omega \times \Omega \mid \exists \gamma : (\alpha, \gamma) \in \Gamma,\ (\gamma, \beta) \in \Gamma^{(k-1)}\}. \tag{3.3.1}$$

This is precisely the set of all pairs of vertices that are joined by a path of length k in diGraph(Γ), and hence also the set of all pairs of vertices joined by a path of length k in the undirected graph uGraph(Δ).
Now let $(\varepsilon, \delta) \in \Omega \times \Omega$. Since G is primitive, Theorem 3.31 implies that diGraph(Γ) is connected. Hence there exists k such that there is a path of length k from ε to δ in uGraph(Δ). Therefore

$$(\varepsilon, \delta) \in \bigcup_{k \geq 0} \Gamma^{(k)}.$$

(2) Define

$$\Phi(s) = \bigcup_{0 \leq k \leq s} \Gamma^{(k)}.$$

Then $\Phi(s)$ is the set of all pairs (α, β) of vertices for which there exists a path in Γ of length at most s from α to β. In particular,

$$\Phi(0) \subseteq \Phi(1) \subseteq \cdots .$$

Assume that $\Phi(t) = \Phi(t-1)$ for some $t \geq 1$. Then

$$\Gamma^{(t+1)} = \Gamma^{(t)} \circ \Gamma \subseteq \Phi(t) \circ \Gamma = \Phi(t-1) \circ \Gamma \subseteq \Phi(t),$$

and hence $\Phi(t+1) = \Phi(t)$, because by definition

$$\Phi(t+1) = \bigcup_{0 \leq k \leq t+1} \Gamma^{(k)} = \Gamma^{(t+1)} \cup \left(\bigcup_{0 \leq k \leq t} \Gamma^{(k)} \right) = \Gamma^{(t+1)} \cup \Phi(t) \subseteq \Phi(t).$$

It follows that $\Phi(s) = \Phi(t-1)$ for all $s \geq t$, and in particular, by part (1), that $\Phi(t-1) = \Omega \times \Omega$.
It remains to show that $\Phi(r) = \Phi(r-1)$. Since each orbital of G is an orbit of G on $\Omega \times \Omega$, every G-invariant subset of $\Omega \times \Omega$ is a union of orbitals. Now each $\Gamma^{(k)}$ is G-invariant, and hence so is each $\Phi(s)$. Therefore each $\Phi(s)$ is a union of orbitals. As the sets $\Gamma^{(k)}$ cover $\Omega \times \Omega$, for each orbital there exists some k such that it is contained in $\Gamma^{(k)}$. Since G has exactly r orbitals, there can be at most r distinct sets among the $\Phi(s)$. In particular,

$$\Phi(r-1) = \Omega \times \Omega.$$

(3) Clear.

□

The following lemma is [2, Theorem 3.2B(iii)].

Lemma 3.42. *Let G be primitive on Ω with finite rank r, and suppose that G has a suborbit of finite length m with $m > 1$. Then Ω is finite and*

$$|\Omega| \leq 1 + m + \cdots + m^{r-1} = \frac{m^r - 1}{m - 1}.$$

Proof. Let $\alpha \in \Omega$. By Lemma 3.20 we can find an orbital Δ of G such that G_α has an orbit $\Delta(\alpha)$ of length m. Since $m > 1$, Δ is not the diagonal orbital. We first show that diGraph(Δ) is strongly connected.

Let E_α be the set of all $\gamma \in \Omega$ for which there exists a directed path in diGraph(Δ) from α to γ.

Now $\Delta^{(k)}$ is the set of all directed paths of length k in diGraph(Δ), and hence $\Delta^{(k)}(\alpha)$ is the set of all endpoints of directed paths of length k in diGraph(Δ) which start at α. Thus

$$E_\alpha = \bigcup_{0 \le k} \Delta^{(k)}(\alpha),$$

since every endpoint of a path has to lie on a path of length k for some k.

Since the sets $\Delta^{(k)}(\alpha)$ are also G_α-invariant, they are unions of G_α-orbits. But there are only r such G_α-orbits in total, and therefore

$$E_\alpha = \bigcup_{0 \le k < r} \Delta^{(k)}(\alpha).$$

(Argue as in the previous lemma with the sets $\Psi(s) = \bigcup_{0 \le k \le s} \Delta^{(k)}(\alpha)$.) In particular, E_α is finite, since every $\Delta^{(k)}(\alpha)$ is finite by Lemma 3.40.

Furthermore, for $g \in G$ we have

$$(E_\alpha)^g = E_{\alpha^g}.$$

Since G is transitive, it follows that

$$|E_\alpha| = |E_\beta| \qquad \text{for all } \beta \in \Omega.$$

Now $|\Delta(\alpha)| = m > 1$, so $|E_\alpha| > 1$.

Choose $\beta \in E_\alpha \setminus \{\alpha\}$. Then E_β is the set of all endpoints of directed paths beginning at β. But there exists a directed path in diGraph(Δ) from α to β, and hence all these endpoints also lie on directed paths beginning at α. Therefore

$$E_\beta \subseteq E_\alpha.$$

Since these are finite sets of the same cardinality, we have

$$E_\beta = E_\alpha.$$

In particular, $\beta \in E_\alpha$ and $\alpha \in E_\beta$, so there exists a directed cycle on which both α and β lie. By Lemma 3.33 it follows that diGraph(Δ) is strongly connected.

By Theorem 3.41(3) and (2), we now have

$$\Omega \times \Omega = \bigcup_{0 \le k < r} \Delta^{(k)},$$

and hence $E_\alpha = \Omega$. It follows that

$$|\Omega| \le \sum_{0 \le k < r} |\Delta^{(k)}(\alpha)| \le \sum_{0 \le k < r} m^i,$$

by Lemma 3.40. □

Definition 3.43. Let G be a finite transitive permutation group of degree n. The list of *subdegrees* is the list of orbit lengths of a point stabilizer on Ω.

The list of subdegrees is an invariant of G. We will always list them in increasing order, i.e.

$$n_1 = 1 \leq n_2 \leq \cdots \leq n_r,$$

where r is the rank of G.

Lemma 3.44. *Let G be a finite group acting faithfully and transitively on Ω, and let $\alpha \in \Omega$. Then $\mathrm{Fix}_\Omega(G_\alpha)$ is a block for G. In particular, if G is primitive, then either $\mathrm{Fix}_\Omega(G_\alpha) = \{\alpha\}$ or $G_\alpha = 1$ and the degree $n := |\Omega|$ is a prime.*

Proof. Exercise. □

The next lemma tells us that in a finite, primitive and non-regular permutation group, the stabilizer of any point fixes only that point.

Lemma 3.45. *Let $G \leq \mathrm{Sym}(\Omega)$ be a finite primitive group that is not regular on Ω. Then $n_i > 1$ for all i with $i > 1$.*

Proof. Exercise. □

The following theorem is [2, Lemma 3.2B(i)].

Theorem 3.46. *Let $G \leq \mathrm{Sym}(\Omega)$ be a finite primitive group which is not regular on Ω, with $|\Omega| = n$. Suppose G has rank $r > 2$ and subdegrees*

$$n_1 = 1 \leq n_2 \leq \cdots \leq n_r.$$

Then

$$n_{i+1} \leq n_i(n_2 - 1) \qquad \text{for all } 2 \leq i < r.$$

Proof. We argue similarly as in the previous lemma. Fix $\alpha \in \Omega$. By Lemma 3.20, the orbitals $\Delta_1, \ldots, \Delta_r$ of G correspond to the orbits of G_α on Ω, and we may order them such that $|\Delta_i(\alpha)| = n_i$ for each i. Thus

$$1 = n_1 = |\Delta_1(\alpha)| \leq n_2 = |\Delta_2(\alpha)| \leq \cdots \leq |\Delta_r(\alpha)| = n_r.$$

Consider

$$\Gamma = \Delta_2 \circ \Delta_2^*.$$

Then

$$\Gamma = \{(\alpha, \beta) \mid \exists \gamma : \ (\alpha, \gamma), (\beta, \gamma) \in \Delta_2\}.$$

Since $n_2 > 1$ (by Lemma 3.45), Δ_2 is a non-diagonal orbital.

Now consider the color graph $\mathcal{G}$ of G. We look at paths of the form

$$\alpha = \alpha_0, \alpha_1, \alpha_2, \ldots, \alpha_k,$$

such that $(\alpha_i, \alpha_{i+1}) \in \Delta_2$ when i is even, and $(\alpha_i, \alpha_{i+1}) \in \Delta_2^*$ when i is odd. We call such a path an *alternating path* of length k.

Since $\Gamma = \Delta_2 \circ \Delta_2^*$ and $n_2 > 1$, the set Γ contains a non-diagonal orbital. Hence by Theorem 3.41(2),

$$\bigcup_{0 \le k \le r-1} \Gamma^{(k)} = \Omega \times \Omega.$$

Thus for every $\beta \in \Omega$ there exists an alternating path from α to β of length at most $r-1$.

Let $2 \le i < r$ and we prove $n_{i+1} \le n_i(n_2 - 1)$. Let k be the length of a shortest alternating path from α to a vertex β with $(\alpha, \beta) \in \Delta_j$ and $j > i$. Consider such a path

$$\alpha = \alpha_0, \alpha_1, \ldots, \alpha_k = \beta.$$

Then $k \ge 2$, since $(\alpha, \beta) \notin \Delta_2$. By minimality of k, we have $(\alpha, \alpha_{k-1}) \in \Delta_t$ for some $t \le i$.

Suppose k is odd. Then $\Delta_j(\alpha)$ is a G_α-orbit containing β. For any $\delta \in \Delta_j(\alpha)$, say $\delta = \beta^g$ with $g \in G_\alpha$, we obtain another alternating path

$$\alpha = \alpha_0^g, \alpha_1^g, \ldots, \alpha_{k-1}^g, \beta^g = \delta$$

of length k.

Since $\Delta_t(\alpha)$ is also a G_α-orbit, we have $\alpha_{k-1}^g \in \Delta_t(\alpha)$. Thus every $\delta \in \Delta_j(\alpha)$ arises from an alternating path whose predecessor lies in $\Delta_t(\alpha)$.

Now count possibilities for δ. There are at most $n_t = |\Delta_t(\alpha)|$ choices for the predecessor α_{k-1}. From each such predecessor there are n_2 edges in Δ_2, but one of them leads back to α_{k-2}, so there are at most $n_2 - 1$ possible next vertices. Hence

$$n_j \le n_t(n_2 - 1) \le n_i(n_2 - 1).$$

If k is even, interchange the roles of Δ_2 and Δ_2^* and argue similarly.

Since $j \ge i + 1$, this yields

$$n_{i+1} \le n_i(n_2 - 1).$$

□

One can in fact prove more, for example that $\gcd(n_r, n_i) \ne 1 \quad \text{for } 2 \le i \le r$.

Brief overview

We know that the orbits of G on $\Omega \times \Omega$ are in bijection with the orbits of G_α on Ω. If G acts transitively on Ω, then G always has rank at least 2, since Δ_1 is an orbital and there is at least one more. If there is exactly one more, then G is *2-transitive*, since G_α acts transitively on $\Omega \setminus \{\alpha\}$. Thus the transitive groups of rank 2 are exactly the 2-transitive groups.

Burnside showed that a finite 2-transitive group G is either almost simple (i.e. $T \cong \mathrm{Inn}(T) \le G \le \mathrm{Aut}(T)$, where T is simple), or a subgroup of $\mathrm{AGL}(V)$.

The next interesting case is therefore that of rank 3 groups. Higman already studied rank 3 groups in 1964. A group of rank 3 can be primitive or imprimitive.

The primitive groups of rank 3 have been completely classified in work of Bannai (1972), Cameron (1981), Liebeck and Saxl (1986), Liebeck (1987), and Dempwolff (2001).

A primitive rank 3 group is either

1. an almost simple group,
2. a subgroup of an affine group $\mathrm{AGL}(d, p)$ for a prime p,

3. a subgroup of $H \wr S_2$ acting on Δ^2 via the product action, where H is a 2-transitive group on Δ.

An important generalization of primitive groups are the *quasiprimitive* groups, introduced by Cheryl Praeger.

Definition 3.47. A group acts *quasiprimitively* on Ω if every non-trivial normal subgroup of G acts transitively on Ω.

We know that the orbits of a normal subgroup are blocks; however, there may also be blocks that do not arise in this way. Thus in a quasiprimitive group, not all blocks are orbits of normal subgroups.

Devillers, Giudici, Li, Pearce and Praeger published a paper in 2011 titled: "On imprimitive rank 3 permutation groups" (*J. Lond. Math. Soc. (2) 84 (3)*).

They write in their abstract: "A classification is given of rank 3 group actions which are quasiprimitive but not primitive. There are two infinite families and a finite number of individual imprimitive examples. When combined with earlier work of Bannai, Kantor, Liebler, Liebeck and Saxl, this yields a classification of all quasiprimitive rank 3 permutation groups".

Further properties of point stabilizers

Lemma 3.48. *(Exercise 1.5.5 in Dixon–Mortimer.) Let G act primitively on Ω and let $\Delta \subseteq \Omega$ contain at least two points. Then for every pair $\alpha, \beta \in \Omega$ with $\alpha \neq \beta$ there exists $g \in G$ such that*

$$\left|\{\alpha, \beta\} \cap \Delta^g\right| = 1.$$

Proof. Define a relation on Ω by $\alpha \sim \beta$ if and only if for all $g \in G$ we have

$$\{\alpha, \beta\} \cap \Delta^g = \{\alpha, \beta\} \quad \text{or} \quad \{\alpha, \beta\} \cap \Delta^g = \varnothing.$$

We show that this is a G-invariant equivalence relation.

It is clearly reflexive and symmetric. Now suppose $\alpha \sim \beta$ and $\beta \sim \gamma$. Then for all $g \in G$,

$$\{\alpha, \beta\} \cap \Delta^g \in \{\{\alpha, \beta\}, \varnothing\} \quad \text{and} \quad \{\beta, \gamma\} \cap \Delta^g \in \{\{\beta, \gamma\}, \varnothing\}.$$

Hence also for all $g \in G$,

$$\{\alpha, \gamma\} \cap \Delta^g \in \{\{\alpha, \gamma\}, \varnothing\},$$

and thus $\alpha \sim \gamma$.

The relation is G-invariant: if $\alpha \sim \beta$ and $g \in G$, then for all $h \in G$,

$$\{\alpha^g, \beta^g\} \cap \Delta^h = \{\alpha^g, \beta^g\} \cap \Delta^{hg^{-1}} \in \{\varnothing, \{\alpha^g, \beta^g\}\}.$$

Hence $\alpha^g \sim \beta^g$.

Thus $\sim$ is a G-invariant equivalence relation, i.e. it defines a block system. Since G is primitive, it must be trivial. As Δ contains at least two points, the relation cannot be universal, so it must be equality.

Therefore, for every $\alpha \neq \beta$ there exists $g \in G$ such that

$$\left|\{\alpha, \beta\} \cap \Delta^g\right| = 1.$$

□

Definition 3.49. Let G be a group. A group S is called a *section* of G if there exists a subgroup $U \leq G$ and a normal subgroup $N \trianglelefteq U$ (i.e. $N \leq U \leq G$) such that

$$U/N \cong S.$$

Theorem 3.50. *Let $G \leq \mathrm{Sym}(\Omega)$ be a finite primitive group and $\alpha \in \Omega$. Let Γ be a non-trivial orbit of G_α. Then every simple group that occurs as a section of G_α is isomorphic to a section of G_α^Γ. In particular, every composition factor of G_α already occurs in G_α^Γ.*

Proof. Let $\{1\} < H \leq G_\alpha$ and $\beta \in \Gamma$. We first show that there exists $g \in G$ such that $g^{-1}Hg$ fixes α but not β.

Let $\Delta = \mathrm{Fix}(H)$. Then $\Delta \neq \Omega$ since $H \neq \{1\}$. If $\beta \notin \Delta$, we can take $g = 1$. Otherwise $\beta \in \Delta$. Since G is primitive, any subset $\Delta \neq \Omega$ containing two points α, β cannot be a block. Hence there exists $g \in G$ such that

$$\alpha \in \Delta^g = \mathrm{Fix}(g^{-1}Hg) \quad \text{and} \quad \beta \notin \Delta^g.$$

Now let S be simple and isomorphic to a section of G_α. Choose $H \leq G_\alpha$ minimal such that $S \cong H/K$ for some normal subgroup $K \trianglelefteq H$. Since S is simple, K is a maximal normal subgroup of H.

If $N \trianglelefteq H$ with $N \not\leq K$, then

$$S \cong H/K = NK/K \cong N/(N \cap K).$$

This would contradict minimality of H, since $N < H$. Hence every proper normal subgroup of H is contained in K.

In particular, every homomorphic image of H has a section isomorphic to S, since the kernel must lie in K.

Now choose $g \in G$ such that $g^{-1}Hg \leq G_\alpha$ and $(g^{-1}Hg)^\Gamma \neq \{1\}$ (since β is not fixed). Then G_α^Γ contains $(g^{-1}Hg)^\Gamma$ and hence also the section

$$(g^{-1}Hg)/(g^{-1}Kg) \cong S.$$

□

Corollary 3.51. *Let G be finite, primitive and non-regular on Ω, and let $\Gamma \neq \{\alpha\}$ be an orbit of G_α. Then the following hold:*

(1) If p is a prime divisor of $|G_\alpha|$, then p also divides $|G_\alpha^\Gamma|$.

(2) If G_α^Γ is solvable, then so is G_α.

Theorem 3.52. *Let $G \leq \mathrm{Sym}(\Omega)$ be finite and transitive of degree n, and let P be a non-trivial Sylow p-subgroup of G. Then*

$$|\mathrm{Fix}(P)| < \frac{n}{2}.$$

Proof. If $n \leq 3$, the statement is easily checked since $n/2 \leq 3/2$ and $|\mathrm{Fix}(P)| \leq 1$. We argue by induction on n, so assume $n > 3$.

(a) G primitive. If P fixes no point, we are done. So assume P fixes a point α and let $\Omega_1 = \{\alpha\}, \Omega_2, \ldots, \Omega_r$ be the orbits of G_α on Ω, with $n_i := |\Omega_i|$ and $n_1 = 1$.

Since $1 \neq P \leq G_\alpha$ and G_α is maximal, it follows that $p \mid |G_\alpha|$. By Corollary 3.51, $p \mid |G_\alpha^{\Omega_i}|$ for all $i > 1$, so P acts non-trivially on each Ω_i with $i > 1$.

By induction (applied to G_α acting on Ω_i),

$$|\operatorname{Fix}(P) \cap \Omega_i| \leq \frac{n_i - 1}{2} \quad \text{for all } i > 1.$$

Hence

$$|\operatorname{Fix}(P)| \leq 1 + \sum_{i=2}^{r} \frac{n_i - 1}{2} = \frac{n - r + 2}{2} \leq \frac{n}{2}.$$

We must exclude equality. Since $P \leq G_\alpha$, we have $p \nmid [G : G_\alpha] = n$. Every P-orbit has size divisible by p, so $p \mid |\operatorname{supp}(P)|$. If equality held, then

$$|\operatorname{supp}(P)| = n - |\operatorname{Fix}(P)| = \frac{n}{2},$$

which is divisible by p, contradicting $p \nmid n$. Thus $|\operatorname{Fix}(P)| < n/2$.

(b) G imprimitive. Let $\Sigma = \{\Delta_1, \ldots, \Delta_m\}$ be a block system with each block of size d, so $n = md$ and $1 < d < n$. Let K be the kernel of the action of G on Σ.

Since each Δ_i is a block, if $\Delta_i \cap \operatorname{Fix}(P) \neq \varnothing$ then $P \leq G_{\Delta_i}$, so P fixes at least $|\operatorname{Fix}(P)|/d$ blocks setwise. In particular,

$$\frac{|\operatorname{Fix}(P)|}{d} \leq |\operatorname{Fix}_\Sigma(P)|.$$

(i) If $P \not\leq K$, then P acts non-trivially on Σ, and by induction (applied to G^Σ),

$$\frac{|\operatorname{Fix}(P)|}{d} \leq |\operatorname{Fix}_\Sigma(P)| < \frac{m}{2},$$

so $|\operatorname{Fix}(P)| < md/2 = n/2$.

(ii) If $P \leq K$, then P acts trivially on Σ. Since all groups K^{Δ_i} are isomorphic, each has order divisible by p. If $\Delta_i \subseteq \operatorname{Fix}(P)$, then P acts trivially on Δ_i, and hence all Sylow p-subgroups of K act trivially on Δ_i, a contradiction since $p \mid |K^{\Delta_i}|$. Thus P acts non-trivially on each Δ_i, and by induction (applied to G_{Δ_i} on Δ_i),

$$|\operatorname{Fix}(P)| < \frac{md}{2} = \frac{n}{2}.$$

□

Lemma 3.53. *Let P be a transitive p-subgroup of $\operatorname{Sym}(\mathcal{A})$ with $|\mathcal{A}| > 1$. Then any minimal P-block system consists of exactly p blocks. Furthermore, the subgroup P' which stabilizes all of the blocks has index p in P.*

Proof. Let $\mathcal{B} = \{B_1, \ldots, B_m\}$ be a minimal nontrivial block system for the action of P on $\mathcal{A}$. Since P is transitive on $\mathcal{A}$, it is also transitive on the set of blocks, so the induced action of P on $\mathcal{B}$ is transitive. Let P' be the kernel of this action, that is, the subgroup of P fixing each block setwise. Then

$$P/P'$$

acts faithfully and transitively on $\mathcal{B}$.

We claim that this action is primitive. Indeed, if there were a nontrivial block system for the action of P/P' on $\mathcal{B}$, then by taking unions of the corresponding blocks in $\mathcal{A}$ we would obtain

a P-block system on $\mathcal{A}$ strictly coarser than the partition into points and strictly finer than $\mathcal{B}$. This contradicts the minimality of $\mathcal{B}$.

Thus P/P' is a primitive p-group on the set $\mathcal{B}$. We now show that any primitive p-group has degree p. Since P/P' is a nontrivial finite p-group, its center is nontrivial. Let

$$1 \neq z \in Z(P/P').$$

Because the action is primitive, any nonidentity central element cannot fix a point of $\mathcal{B}$: if z fixed some block B_i, then for every $g \in P/P'$,

$$z(g(B_i)) = g(z(B_i)) = g(B_i),$$

so z would fix every point of $\mathcal{B}$, contrary to $z \neq 1$. Hence z is fixed-point-free.

Now the cycles of a permutation of p-power order all have lengths that are powers of p. Since z is fixed-point-free, all cycles of z have length at least p. Because z lies in the center, its orbits form a block system for the primitive action of P/P' on $\mathcal{B}$. Primitivity therefore forces these orbits to be the whole of $\mathcal{B}$. Thus z is transitive on $\mathcal{B}$, so $\mathcal{B}$ has size equal to the order of the cyclic group generated by z on $\mathcal{B}$, which must be p. Therefore,

$$m = |\mathcal{B}| = p.$$

Finally, since P/P' acts faithfully and transitively on the p blocks, we have

$$|P : P'| = |P/P'| = |\mathcal{B}| = p.$$

Equivalently, P' has index p in P. □

3.4 Testing isomorphism of cubic graphs

We follow the paper of Luks. We demonstrate that the problem of testing isomorphism of cubic graphs is polynomial-time reducible to the Color Automorphism Problem for 2-groups. The first step is a modification of the reduction of the graph isomorphism problem to an automorphism problem.

Proposition 3.54. *Testing isomorphism of cubic graphs is polynomial-time reducible to the problem of determining generators for* $\mathrm{Aut}(X)_e$*, where* X *is a connected cubic graph and* e *is a distinguished edge.*

Proof. Assume we have a polynomial-time algorithm which returns generators for any such $\mathrm{Aut}(X)_e$. It suffices to be able to compare two connected cubic graphs X_1, X_2. Fix an edge $e_1 \in E(X_1)$. For each edge $e_2 \in E(X_2)$ we can test whether there is an isomorphism from X_1 to X_2 which maps e_1 to e_2 as follows. Construct a connected cubic graph X from the disjoint union $X_1 \cup X_2$ by

(1) inserting new vertices v_1 in e_1 and v_2 in e_2, and
(2) joining v_1 to v_2 with a new edge e.

Then there is an isomorphism from X_1 to X_2 mapping e_1 to e_2 if and only if some element of $\mathrm{Aut}(X)_e$ transposes v_1 and v_2. Furthermore, if such automorphisms exist, any set of generators of $\mathrm{Aut}(X)_e$ will contain one. □

We now fix a connected cubic graph X with $|V(X)| = n$. The group $\mathrm{Aut}(X)_e$ is determined through a natural sequence of successive approximations, $\mathrm{Aut}(X_r)_e$, $r = 1, 2, \ldots$, where X_r is the subgraph consisting of all vertices and all edges of X which appear in paths of length at most r through e. So $X_1 = e$ itself and $X_{n-1} = X$. The groups are related via the induced homomorphisms

$$\pi_r : \mathrm{Aut}(X_{r+1})_e \to \mathrm{Aut}(X_r)_e,$$

in which $\pi_r(\sigma)$ is the restriction of σ to X_r. Thus, assuming we know $\mathrm{Aut}(X_r)_e$, the determination of $\mathrm{Aut}(X_{r+1})_e$ breaks up into two problems:

(i) Find a set $\mathcal{K}$ of generators for K_r, the kernel of π_r.
(ii) Find a set $\mathcal{S}$ of generators for $\pi_r(\mathrm{Aut}(X_{r+1})_e)$, the image of π_r.

Then, if $\mathcal{S}'$ is any pullback of $\mathcal{S}$ in $\mathrm{Aut}(X_{r+1})_e$, that is, $\pi_r(\mathcal{S}') = \mathcal{S}$, then $\mathcal{K} \cup \mathcal{S}'$ generates $\mathrm{Aut}(X_{r+1})_e$. It turns out that the essential, and difficult, problem is (ii).

To investigate these problems we consider $V(X_{r+1}) \setminus V(X_r)$. Each vertex in this set is connected to one, two or three vertices in X_r. We codify this relationship as follows: Let $\mathcal{A}$ denote the collection of all subsets of $V(X_r)$ of size one, two, or three. Define

$$f\colon V(X_{r+1}) \setminus V(X_r) \to \mathcal{A}$$

by

$$f(v) = \{\, w \in V(X_r) \mid \{v, w\} \in E(X) \,\}.$$

We call v, v', for $v \neq v'$, *twins* if $f(v) = f(v')$ (note: triplets cannot exist). In the above example v_3 and v_4 are twins, v_1 and v_2 are not. Now,

$$\sigma \in \mathrm{Aut}(X_{r+1})_e \quad \Longrightarrow \quad f(\sigma(v)) = \sigma(f(v)). \tag{$*$}$$

Thus, in particular, if $\sigma \in K_r$ (i.e. σ fixes all elements of X_r) then $f(v) = f(\sigma(v))$; so either $v = \sigma(v)$ or v and $\sigma(v)$ are twins. It follows that K_r is precisely the elementary abelian 2-group generated by the transpositions in each pair of twins.

Since

$$|\,\mathrm{Aut}(X_{r+1})_e| = |\,\mathrm{Im}\,\pi_r| \cdot |K_r|,$$

an induction argument recovers the following result.

Proposition 3.55 (Tutte)**.** *For each r, $\mathrm{Aut}(X_r)_e$ is a 2-group.*

To get at (ii), observe that $(*)$ implies any $\sigma \in \pi_r(\mathrm{Aut}(X_{r+1})_e)$ stabilizes the set of fathers with one son, i.e.,

$$\mathcal{A}_1 = \{a \in \mathcal{A} \mid a = f(v) \text{ for some unique } v \in V(X_{r+1}) \setminus V(X_r)\}.$$

Furthermore any $\sigma \in \pi_r(\mathrm{Aut}(X_{r+1})_e)$ must stabilize the subset of $\mathcal{A}$ consisting of the fathers of twins, i.e.,

$$\mathcal{A}_2 = \{a \in \mathcal{A} \mid a = f(v_1) = f(v_2) \text{ for some } v_1 \neq v_2\}.$$

Now, aside from the edges from $V(X_{r+1}) \setminus V(X_r)$, there are elements of $E(X_{r+1}) \setminus E(X_r)$ which join two vertices in $V(X_r)$. These correspond to the subset of $\mathcal{A}$,

$$\mathcal{A}' = \big\{\{w_1, w_2\} \in \mathcal{A} \mid \{w_1, w_2\} \in E(X_{r+1})\big\}.$$

An element of $\pi_r(\mathrm{Aut}(X_{r+1})_e)$ must also stabilize $\mathcal{A}'$. However, we have now summarized the condition that $\sigma \in \mathrm{Aut}(X_r)_e$ be in the image of π_r.

Proposition 3.56. *$\pi_r(\mathrm{Aut}(X_{r+1})_e)$ is precisely the set of those $\sigma \in \mathrm{Aut}(X_r)_e$ which stabilize each of the collections $\mathcal{A}_1, \mathcal{A}_2, \mathcal{A}'$.*

Proof. We need only now show that, if σ stabilizes $\mathcal{A}_1, \mathcal{A}_2, \mathcal{A}'$, it does indeed extend to an element of $\mathrm{Aut}(X_{r+1})_e$. For such σ, we define the extension as follows.

For each "only child" v, $f(v) \in \mathcal{A}_1$ implies $\sigma(f(v)) \in \mathcal{A}_1$, so map v to the unique vertex corresponding to $\sigma(f(v))$.

For each pair of twins v, v', $f(v) \in \mathcal{A}_2$ implies $\sigma(f(v)) \in \mathcal{A}_2$, so map $\{v, v'\}$ to the twin pair corresponding to $\sigma(f(v))$ in either order.

By construction, this extension stabilizes the set of edges between $V(X_r)$ and $V(X_{r+1}) \setminus V(X_r)$ (note that $f(v)$ and $\sigma(f(v))$ automatically have the same cardinality as subsets of $V(X_r)$). That it stabilizes the "new" edges between "old" points was implicit, before the extension, in the condition $\sigma(\mathcal{A}') = \mathcal{A}'$. □

Let $\mathcal{A}_0 = \mathcal{A} \setminus (\mathcal{A}_1 \cup \mathcal{A}_2)$. In order to isolate the essential problem, we color the set $\mathcal{A}$ with six colors to distinguish the six disjoint regions

$$\mathcal{A}_0 \cap \mathcal{A}', \quad \mathcal{A}_1 \cap \mathcal{A}', \quad \mathcal{A}_2 \cap \mathcal{A}', \quad \mathcal{A}_0 \setminus \mathcal{A}', \quad \mathcal{A}_1 \setminus \mathcal{A}', \quad \mathcal{A}_2 \setminus \mathcal{A}'.$$

We are now looking for the color preserving elements in $\mathrm{Aut}(X_r)_e$ in its action on $\mathcal{A}$. Thus cubic graph isomorphism is polynomial-time reducible to the following:

Problem 1. **Input:** A set of generators for a 2-subgroup G of $\mathrm{Sym}(\mathcal{A})$, where $\mathcal{A}$ is a colored set. **Find:** A set of generators for the subgroup $\{\sigma \in G \mid \sigma \text{ is color preserving}\}$.

The presence of a group action on a set suggests two divide-and-conquer mechanisms: the decomposition of the set into orbits and, in the transitive case, the decomposition of the set into blocks of imprimitivity. Both of these come into play in the algorithm for *Problem 1* but they require a generalization of the problem that admits a recursive procedure.

We fix a colored set $\mathcal{A}$ with n elements. The number and distribution of colors is unimportant. For $a, b \in \mathcal{A}$, the relation "a has the same color as b" will be abbreviated $a \sim b$. Suppose $B \subseteq \mathcal{A}$ and $K \leq \mathrm{Sym}(\mathcal{A})$. Set

$$\mathcal{C}_B(K) = \{\sigma \in K \mid \text{for all } b \in B,\ \sigma(b) \sim b\}.$$

The following properties are immediate:

(i) $\mathcal{C}_B(K \cup K') = \mathcal{C}_B(K) \cup \mathcal{C}_B(K')$.
(ii) $\mathcal{C}_{B \cup B'}(K) = \mathcal{C}_{B'}(\mathcal{C}_B(K))$.

The generalization we need of Problem 1 is:

Problem 2. **Input:** Generators for a 2-subgroup $G \leq \mathrm{Sym}(\mathcal{A})$, a G-stable subset $B \subseteq \mathcal{A}$, and $\sigma \in \mathrm{Sym}(\mathcal{A})$. **Find:** $\mathcal{C}_B(\sigma G)$.

Problem 1 is the special case $B = \mathcal{A}$, $\sigma = 1$. We observe first that

Lemma 3.57. *If $\mathcal{C}_B(\sigma G)$ is not empty then it is a left coset of the subgroup $\mathcal{C}_B(G)$.*

Proof. The G-stability of B guarantees that $\mathcal{C}_B(G)$ is a subgroup. If $\sigma_0 \in \mathcal{C}_B(\sigma G)$, then in particular $\sigma_0 = \sigma\tau_0$ for some $\tau_0 \in G$. For $\tau \in G$, $b \in B$, we know $\tau(b) \in B$ and so $\sigma_0(\tau(b)) \sim \tau(b)$. Thus $\sigma_0\tau \in \mathcal{C}_B(\sigma G)$ if and only if $\tau \in \mathcal{C}_B(G)$. That is,

$$\mathcal{C}_B(\sigma G) = \sigma_0 \mathcal{C}_B(G).$$

□

By the lemma, we expect the program for *Problem 2* to accept, as input, a coset of a group and return an answer of $\emptyset$ or a coset of a group. The cosets would each be specified by a pair consisting of a representative element and a set of generators for the group.

The algorithm for Problem 2 proceeds as follows. If B is the union of G-stable subsets B', B'' then

$$\mathcal{C}_B(\sigma G) = \mathcal{C}_{B'}\big(\mathcal{C}_{B''}(\sigma G)\big).$$

If not, that is, if G acts transitively on B, we recall Lemmas 1.1, 1.3 and write B as the union of two G-blocks, $B = B' \cup B''$. Note, we do not, this time, attempt to compute $\mathcal{C}_{B'}(\sigma G)$ directly; B' is not G-stable. However, we can find in polynomial (in n) time the subgroup H of G which stabilizes B', B''. Then

$$G = H \cup \tau H$$

and so

$$\begin{aligned}\mathcal{C}_B(\sigma G) &= \mathcal{C}_B(\sigma H) \cup \mathcal{C}_B(\sigma\tau H)\\ &= \mathcal{C}_{B'}\big(\mathcal{C}_{B''}(\sigma H)\big) \cup \mathcal{C}_{B'}\big(\mathcal{C}_{B''}(\sigma\tau H)\big).\end{aligned}$$

It is important to observe that Lemma 2.4 guarantees, when both subanswers $\mathcal{C}_B(\sigma H)$ and $\mathcal{C}_B(\sigma\tau H)$ are non-empty, that they must paste together neatly to a single coset of $\mathcal{C}_B(G)$. In such a case, we would have

$$\mathcal{C}_B(\sigma H) = \rho_1 \mathcal{C}_B(H), \qquad \mathcal{C}_B(\sigma\tau H) = \rho_2 \mathcal{C}_B(H),$$

and the main answer would be expressed

$$\mathcal{C}_B(\sigma G) = \rho_1 \langle \mathcal{C}_B(H), \rho_1^{-1}\rho_2 \rangle.$$

(The answer must include the right-hand side since $\mathcal{C}_B(H)$ and $\rho_1^{-1}\rho_2$ are contained in $\mathcal{C}_B(G)$; on the other hand, the right-hand side clearly contains the two subanswers.)

We have shown how, in the intransitive case, the set breaks into disjoint pieces and we solve one problem on each piece. And, in the transitive case, the computation of $\mathcal{C}_B(\sigma G)$ involves four recursive calls to similar problems on sets B', B'' of half the size. It remains only to examine the case $|B| = 1$. But, if $B = \{b\}$ and $Gb = B$ then

$$\mathcal{C}_B(\sigma G) = \begin{cases} \sigma G & \text{if } \sigma(b) \sim b,\\ \emptyset & \text{if } \sigma(b) \not\sim b.\end{cases}$$

So this is resolved in constant time. Standard induction arguments show that the total algorithm requires only polynomial time.

Chapter 4

Wreath products

4.1 Semidirect products

As a reminder, we define once again the semidirect product of two groups K and H.

Definition 4.1. A group G is called the *semidirect product* of two groups K and H if:

- $K \trianglelefteq G$,
- $K \cap H = \{1\}$,
- $K \cdot H = G$.

We use the notation $K \rtimes H$.

Then every element $g \in G$ can be written uniquely as $g = kh$ with $k \in K$ and $h \in H$. Conversely, given groups K, H, and a homomorphism

$$\varphi : H \to \mathrm{Aut}(K),$$

we can define the semidirect product of K and H as

$$K \rtimes H = \{(k, h) \mid k \in K,\ h \in H\},$$

where

$$(k_1, h_1) \cdot (k_2, h_2) = \big(k_1 (k_2)^{\varphi(h_1^{-1})},\ h_1 h_2\big).$$

Theorem 4.2. *Let G be a group. Then G has a normal subgroup N and a subgroup U with $G/N \cong U$ if and only if G is isomorphic to a semidirect product $G \cong K \rtimes H$.*

4.2 Wreath Products

Every group that acts faithfully on a set Ω can be embedded into the symmetric group $\mathrm{Sym}(\Omega)$. We now first describe imprimitive subgroups of $\mathrm{Sym}(\Omega)$.

For sets Δ and Γ we denote by Δ^Γ the set of all maps from Γ to Δ.

Lemma 4.3. *Let $(K, *)$ be a group and let Γ be a set. Then the set K^Γ of all maps from Γ to K is again a group with respect to pointwise multiplication of maps.*

Proof. We show that $(K^\Gamma, \cdot)$ is a group, where the multiplication $f_1 \cdot f_2 \colon \Gamma \to K$ is defined by

$$\gamma \mapsto f_1(\gamma) * f_2(\gamma).$$

It is clear that $f_1 \cdot f_2$ is again in K^Γ. The identity in K^Γ is evidently the map $1 \colon \gamma \mapsto 1_K$. Associativity of the multiplication is immediate, since K is a group. Let $f_1 \in K^\Gamma$. Then the map

$$f_1^{-1} \colon \Gamma \to K : \gamma \mapsto \big(f_1(\gamma)\big)^{-1}$$

is an element of K^Γ and satisfies

$$f_1 \cdot f_1^{-1} = f_1^{-1} \cdot f_1 = 1.$$

□

Now let H be a group acting on Γ. Then we can define an action of H on K^Γ by $(f, h) = f^h$, where f^h is defined by

$$f^h \colon \Gamma \to K : \gamma \mapsto f(\gamma^{h^{-1}}).$$

We first show that this indeed defines an action of H on K^Γ. Let $f \in K^\Gamma$. Then $f^{1_H} = f$, and for $h_1, h_2 \in H$ we have

$$\begin{aligned} f^{h_1 h_2}(\gamma) &= f(\gamma^{(h_1 h_2)^{-1}}) \\ &= f\big((\gamma^{h_2^{-1}})^{h_1^{-1}}\big) \\ &= f^{h_1}(\gamma^{h_2^{-1}}) \\ &= \big(f^{h_1}\big)^{h_2}(\gamma). \end{aligned}$$

In particular, the action of H on K^Γ yields a homomorphism $\varphi \colon H \to \mathrm{Aut}(K^\Gamma)$.

Definition 4.4. Let H and K be groups, and let Γ be a set on which H acts. The semidirect product

$$K^\Gamma \rtimes H = \{(f, h) \mid f \in K^\Gamma,\ h \in H\},$$

where

$$(f_1, h_1) \cdot (f_2, h_2) = \big(f_1 (f_2)^{h_1^{-1}},\ h_1 h_2\big),$$

is called the *wreath product* of K with H, written $K \wr_\Gamma H$. The subgroup

$$B = \{(f, 1) \mid f \in K^\Gamma\}$$

is called the *base group*.

Remark 4.5. 1. It is easy to see that

$$(f, h)^{-1} = \big((f^{-1})^h,\ h^{-1}\big),$$

since

$$\begin{aligned} (f, h)(f, h)^{-1} &= (f, h)\big((f^{-1})^h,\ h^{-1}\big) \\ &= \Big(f\big(((f^{-1})^h)^{h^{-1}}\big),\ hh^{-1}\Big) = (ff^{-1}, 1_H) = (1_K, 1_H). \end{aligned}$$

2. The wreath product of K and H depends on the action of H on Γ. To make this explicit, the wreath product is denoted by $K \wr_\Gamma H$. If H acts regularly on itself by right multiplication, then this is the *standard wreath product*, and we omit Γ. Often Γ is also omitted when it is clear from the context which action of H on Γ is meant. In the standard wreath product $K \wr H$, for $f \in K^H$ the action of H on f is defined by

$$f^h \colon a \mapsto f(ah^{-1}).$$

This corresponds to right multiplication, since for $\gamma \in \Gamma = H$ we have

$$f^h(\gamma) = f(\gamma^{h^{-1}}) = f(\gamma h^{-1}).$$

3. Consider the case where Γ is a finite set, say $m = |\Gamma|$. In this case $K^\Gamma \cong K^m$, since every map $f \in K^\Gamma$ can be described by its values $(f_1, \ldots, f_m)$, where the $f_i \in K$ are defined by $f_i = i^f$. Hence, when Γ is finite, we write the elements $(f, h) \in K \wr_\Gamma H$ in the form

$$(f, h) = (f_1, \ldots, f_m; h),$$

where $i^f = f_i$ for $1 \leq i \leq m$. Thus the wreath product of K and H is defined as

$$K \wr_\Gamma H := K^\Gamma \rtimes H = \{(f_1, \ldots, f_m, h) \mid f_i \in K,\ h \in H\},$$

with multiplication on $K \wr_\Gamma H$ given by

$$(f_1, \ldots, f_m, h_1)(f'_1, \ldots, f'_m, h_2) = \big(f_1 f'_{1^{h_1}}, \ldots, f_m f'_{m^{h_1}}, h_1 h_2\big).$$

The following theorem shows that the standard wreath product has a universal property: every extension G of N by H (that is, there exists an exact sequence $1 \to N \to G \to H \to 1$) can be embedded into the standard wreath product $N \wr H$ of the groups N and H. Thus the wreath product contains a copy of every extension of N by H. This theorem was first proved by Krasner and Kaloujnine in 1951.

Theorem 4.6 (The universal embedding theorem)**.** *Let G be a (finite) group, let $N \trianglelefteq G$, and let $H = G/N$. Then there exists a monomorphism $\Phi \colon G \to N \wr H$ such that*

$$\Phi(N) = \Phi(G) \cap B.$$

Proof. Let $\psi \colon G \to H$ be a homomorphism with $N = \ker \psi$. Let

$$T = \{t_u \mid u \in H\}$$

be a system of representatives for the right cosets of N in G such that $\psi(t_u) = u$ for all $u \in H$.

For $g \in G$ we then have

$$\psi(t_u g) = \psi(t_u)\psi(g) = u\psi(g) = \psi(t_{u\psi(g)}),$$

and hence

$$t_u g t_{u\psi(g)}^{-1} \in \ker \psi = N.$$

For $g \in G$ define the function

$$f_g \colon H \to N : u \mapsto t_u g t_{u\psi(g)}^{-1}.$$

Then we can define an embedding of G into $N \wr H$ by

$$\Phi\colon g \mapsto (f_g, \psi(g)).$$

One checks easily that

$$\begin{aligned} f_{g_1g_2}(u)\, t_{u\psi(g_1g_2)} &= t_u g_1 g_2 \\ &= t_u g_1 t_{u\psi(g_1)}^{-1} \cdot t_{u\psi(g_1)} g_2 \\ &= f_{g_1}(u) \cdot t_{u\psi(g_1)} g_2 \\ &= f_{g_1}(u) \cdot f_{g_2}(u\psi(g_1))\, t_{u\psi(g_1)\psi(g_2)} \\ &= f_{g_1}(u) \cdot f_{g_2}^{\psi(g_1)^{-1}}(u)\, t_{u\psi(g_1)\psi(g_2)}. \end{aligned}$$

Hence

$$f_{g_1g_2} = f_{g_1} f_{g_2}^{\psi(g_1)^{-1}}.$$

Thus Φ is a homomorphism: let $g_1, g_2 \in G$. Then

$$\begin{aligned} \Phi(g_1g_2) &= (f_{g_1g_2}, \psi(g_1g_2)) \\ &= \left(f_{g_1} f_{g_2}^{\psi(g_1)^{-1}}, \psi(g_1)\psi(g_2)\right) \\ &= (f_{g_1}, \psi(g_1))(f_{g_2}, \psi(g_2)) = \Phi(g_1)\Phi(g_2). \end{aligned}$$

Moreover, $\ker \Phi = 1$, since $\Phi(g) = 1$ means that $f_g = 1$ and $\psi(g) = 1$, and hence

$$g = t_1^{-1} f_g(1) t_{1\psi(g)} = 1.$$

Thus Φ is injective.

Finally, $\Phi(g) \in B$ if and only if $\psi(g) = 1$, and this holds if and only if $g \in N$. Therefore

$$\Phi(N) = \Phi(G) \cap B.$$

□

4.3 The imprimitive action

Remark 4.7. Let K and H be groups, let Δ and Γ be non-empty finite sets, and suppose that K acts on Δ and H acts on Γ. Let $\Gamma = \{1, \ldots, m\}$. Set

$$\Delta_i := \Delta \times \{i\}$$

and identify

$$\Delta \times \Gamma = \bigcup_{i=1}^{m} \Delta_i.$$

Then the wreath product $K \wr_\Gamma H$ of K and H acts naturally on $\Delta \times \Gamma$ as follows. The top group T is defined by the action of H on $\Delta \times \Gamma$ via

$$(\delta, i)^h = (\delta, i^h).$$

The base group B is defined by the action of K^Γ on $\Delta \times \Gamma$ via

$$(\delta, i)^{(g_1,\ldots,g_m)} = (\delta^{g_i}, i).$$

The wreath product $K \wr_\Gamma H$ is the group generated by B and T, and consists of all products bt with $b \in B$ and $t \in T$.

This corresponds to the action of H on K^Γ described above, since a function $g \in K^\Gamma$ is described by its values, in particular $g(i) = g_i$. Hence for $h \in H$ the map g^h is given by

$$g^h(i) = g(i^{h^{-1}}) = g_{i^{h^{-1}}}.$$

Thus, by the definition of the multiplication, we have

$$hg = g^{h^{-1}}h.$$

We see that

$$\big((\delta, i)^h\big)^{(g_1,\ldots,g_m)} = (\delta, i^h)^{(g_1,\ldots,g_m)} = (\delta^{g_{i^h}}, i^h),$$

while

$$(\delta, i)^{(g_1^{h^{-1}},\ldots,g_m^{h^{-1}})h} = (\delta^{g_i^{h^{-1}}}, i)^h = (\delta^{g_i^{h^{-1}}}, i^h).$$

Example 4.8. Consider $\mathbb{Z}_2 \wr S_3$. Then $\Delta = \{1, 2\}$ and $\Gamma = \{1, 2, 3\}$, so $m = 3$. The group $K = \mathbb{Z}_2$ is generated by $(1, 2)$. The group $H = S_3$ is generated by $\{(1, 2), (1, 2, 3)\}$. The wreath product acts on the set

$$\Omega = \{(1, 1), (2, 1), (1, 2), (2, 2), (1, 3), (2, 3)\}.$$

The base group is generated by the permutations

$$b_1 = ((1, 2), (), (), 1_H), \qquad b_2 = ((), (1, 2), (), 1_H), \qquad b_3 = ((), (), (1, 2), 1_H).$$

These act as

$$b_1 = \begin{pmatrix} (1,1) & (2,1) & (1,2) & (2,2) & (1,3) & (2,3) \\ (2,1) & (1,1) & (1,2) & (2,2) & (1,3) & (2,3) \end{pmatrix},$$

$$b_2 = \begin{pmatrix} (1,1) & (2,1) & (1,2) & (2,2) & (1,3) & (2,3) \\ (1,1) & (2,1) & (2,2) & (1,2) & (1,3) & (2,3) \end{pmatrix},$$

$$b_3 = \begin{pmatrix} (1,1) & (2,1) & (1,2) & (2,2) & (1,3) & (2,3) \\ (1,1) & (2,1) & (1,2) & (2,2) & (2,3) & (1,3) \end{pmatrix}.$$

The top group is generated by the permutations

$$h_1 = (1_B, (1, 2)) \qquad \text{and} \qquad h_2 = (1_B, (1, 2, 3)),$$

which act as follows:

$$h_1 = \begin{pmatrix} (1,1) & (2,1) & (1,2) & (2,2) & (1,3) & (2,3) \\ (1,2) & (2,2) & (1,1) & (2,1) & (1,3) & (2,3) \end{pmatrix},$$

$$h_2 = \begin{pmatrix} (1,1) & (2,1) & (1,2) & (2,2) & (1,3) & (2,3) \\ (1,2) & (2,2) & (1,3) & (2,3) & (1,1) & (2,1) \end{pmatrix}.$$

If we renumber the points of Ω as $\{1,2,3,4,5,6\}$, then we obtain the permutations

$$b_1 = (1,2), \qquad b_2 = (3,4), \qquad b_3 = (5,6),$$
$$h_1 = (1,3)(2,4) \qquad \text{and} \qquad h_2 = (1,3,5)(2,4,6).$$

We see immediately that $\mathbb{Z}_2 \wr S_3$ acts imprimitively and that

$$\{\{1,2\},\{3,4\},\{5,6\}\}$$

is a block system.

In general, the wreath product defined in this way acts imprimitively on $\Delta \times \Gamma$, and the blocks are the sets Δ_i. The base group permutes the elements of each Δ_i, while the top group permutes the Δ_i among themselves. The order of the wreath product is $|K|^m|H|$.

Lemma 4.9. *Let Ω be a set with $|\Omega| = n$, and let there be given an unordered partition of Ω into m blocks, each of size b. Then the stabilizer of this partition in S_n is isomorphic to $S_b \wr S_m$.*

If we do not assume that Γ is finite, then we can define the *imprimitive action on* $\Delta \times \Gamma$ in full generality by

$$(\delta,\gamma)^{(f,h)} = \left(\delta^{f(\gamma)}, \gamma^h\right).$$

4.4 The primitive action

There is another important action of wreath products on sets, namely the so-called *product action*. This action is not always primitive, but it is very often primitive. Let again K and H be finite groups, let Δ and Γ be non-empty finite sets, and suppose that K acts on Δ and H acts on Γ. Let $\Gamma = \{1,\ldots,m\}$. Then the wreath product

$$K \wr_\Gamma H = K^m \rtimes H$$

acts on the set Δ^Γ of all maps from Γ to Δ. This set has cardinality $|\Delta|^m$.

Let $\pi \in \Delta^\Gamma$. Then we may represent π by the vector of length m of its values, that is, if $\Gamma = \{1,\ldots,m\}$, then π is determined by

$$(\pi(1),\ldots,\pi(m)).$$

Write $\pi_i = \pi(i)$. Then the base group B acts componentwise on Δ^Γ via

$$(\pi_1,\ldots,\pi_m)^{(g_1,\ldots,g_m)} = (\pi_1^{g_1},\ldots,\pi_m^{g_m}).$$

The top group acts by

$$(\pi_1,\ldots,\pi_m)^h = (\pi_{1^{h^{-1}}},\ldots,\pi_{m^{h^{-1}}}).$$

This is indeed an action. For this we must verify that

$$\begin{aligned}
(\pi_1,\ldots,\pi_m)^{ab} &= (\pi(1),\ldots,\pi(m))^{ab} \\
&= \left(\pi(1^{(ab)^{-1}}),\ldots,\pi(m^{(ab)^{-1}})\right) \\
&= \left(\pi(1^{b^{-1}a^{-1}}),\ldots,\pi(m^{b^{-1}a^{-1}})\right) \\
&= \left(\pi(1^{a^{-1}}),\ldots,\pi(m^{a^{-1}})\right)^b \\
&= \left((\pi(1),\ldots,\pi(m))^a\right)^b \\
&= \left((\pi_1,\ldots,\pi_m)^a\right)^b,
\end{aligned}$$

where a and b are elements of the top group of the wreath product.

Example 4.10. We consider again $\mathbb{Z}_2 \wr S_3$ and let this wreath product act on Δ^Γ via the product action, where

$$\Delta^\Gamma = \{(1,1,1),(1,1,2),(1,2,1),(1,2,2),(2,1,1),(2,1,2),(2,2,1),(2,2,2)\}.$$

Then the action of the base group is given by

$$b_1 = \begin{pmatrix} (1,1,1) & (1,1,2) & (1,2,1) & (1,2,2) & (2,1,1) & (2,1,2) & (2,2,1) & (2,2,2) \\ (2,1,1) & (2,1,2) & (2,2,1) & (2,2,2) & (1,1,1) & (1,1,2) & (1,2,1) & (1,2,2) \end{pmatrix},$$

$$b_2 = \begin{pmatrix} (1,1,1) & (1,1,2) & (1,2,1) & (1,2,2) & (2,1,1) & (2,1,2) & (2,2,1) & (2,2,2) \\ (1,2,1) & (1,2,2) & (1,1,1) & (1,1,2) & (2,2,1) & (2,2,2) & (2,1,1) & (2,1,2) \end{pmatrix},$$

$$b_3 = \begin{pmatrix} (1,1,1) & (1,1,2) & (1,2,1) & (1,2,2) & (2,1,1) & (2,1,2) & (2,2,1) & (2,2,2) \\ (1,1,2) & (1,1,1) & (1,2,2) & (1,2,1) & (2,1,2) & (2,1,1) & (2,2,2) & (2,2,1) \end{pmatrix},$$

and the top group acts via

$$h_1 = \begin{pmatrix} (1,1,1) & (1,1,2) & (1,2,1) & (1,2,2) & (2,1,1) & (2,1,2) & (2,2,1) & (2,2,2) \\ (1,1,1) & (1,1,2) & (2,1,1) & (2,1,2) & (1,2,1) & (1,2,2) & (2,2,1) & (2,2,2) \end{pmatrix},$$

$$h_2 = \begin{pmatrix} (1,1,1) & (1,1,2) & (1,2,1) & (1,2,2) & (2,1,1) & (2,1,2) & (2,2,1) & (2,2,2) \\ (1,1,1) & (2,1,1) & (1,1,2) & (2,1,2) & (1,2,1) & (2,2,1) & (1,2,2) & (2,2,2) \end{pmatrix}.$$

That is, on

$$\Omega = \{1,2,3,4,5,6,7,8\}$$

we obtain the permutations

$$b_1 = (1,5)(2,6)(3,7)(4,8),$$
$$b_2 = (1,3)(2,4)(5,7)(6,8),$$
$$b_3 = (1,2)(3,4)(5,6)(7,8),$$
$$h_1 = (3,5)(4,6),$$
$$h_2 = (2,5,3)(4,6,7).$$

Note that this action is not primitive, since $\{1,4,6,7\}$ is a block. However, the action of $K \wr_\Gamma H$ on Δ^Γ is very often primitive, as we shall soon see.

Now let K and H be groups such that K acts on Δ and H acts on Γ. We now define, in complete generality (that is, also for Γ infinite), the action of $K \wr_\Gamma H$ on Δ^Γ, and we no longer assume that Γ is finite. Let

$$G = K \wr_\Gamma H.$$

Then G is the semidirect product

$$K^\Gamma \rtimes H,$$

that is, the set of pairs (f,h) with $f \in K^\Gamma$ and $h \in H$.

The action of (f,h) on $\Omega = \Delta^\Gamma$ is then defined as follows. Let $\varphi \in \Omega$ and $(f,h) \in G$. Then $\varphi\colon \Gamma \to \Delta$ and $f\colon \Gamma \to K$. Define

$$\varphi^{(f,h)}\colon \Gamma \to \Delta : \gamma \mapsto \varphi(\gamma^{h^{-1}})^{f(\gamma^{h^{-1}})}.$$

In this way, the action of (f,h) on $\varphi \in \Omega$ is defined using the action of K on Δ.

We now show that this defines an action of G on Ω. Since the multiplication in G is given by

$$(f_1,h_1)(f_2,h_2) = \big(f_1 f_2^{h_1^{-1}}, h_1h_2\big),$$

we must show that for every $\varphi \in \Omega$ and $(f_1,h_1),(f_2,h_2) \in G$,

$$\big(\varphi^{(f_1,h_1)}\big)^{(f_2,h_2)} = \varphi^{(f_1 f_2^{h_1^{-1}},h_1h_2)}.$$

So let $\gamma \in \Gamma$. Then

$$\begin{aligned}
\big(\big(\varphi^{(f_1,h_1)}\big)^{(f_2,h_2)}\big)(\gamma) &= \big(\varphi^{(f_1,h_1)}\big)(\gamma^{h_2^{-1}})^{f_2(\gamma^{h_2^{-1}})} \\
&= \varphi(\gamma^{h_2^{-1}h_1^{-1}})^{f_1(\gamma^{h_2^{-1}h_1^{-1}})f_2(\gamma^{h_2^{-1}})} \\
&= \varphi(\gamma^{h_2^{-1}h_1^{-1}})^{f_1(\gamma^{h_2^{-1}h_1^{-1}})f_2(\gamma^{h_2^{-1}})} \\
&= \varphi(\gamma^{h_2^{-1}h_1^{-1}})^{f_1(\gamma^{h_2^{-1}h_1^{-1}})f_2^{h_1^{-1}}(\gamma^{h_2^{-1}h_1^{-1}})} \\
&= \varphi(\gamma^{(h_1h_2)^{-1}})^{(f_1 f_2^{h_1^{-1}})(\gamma^{(h_1h_2)^{-1}})} \\
&= \big(\varphi^{(f_1 f_2^{h_1^{-1}},h_1h_2)}\big)(\gamma).
\end{aligned}$$

Hence

$$\big(\varphi^{(f_1,h_1)}\big)^{(f_2,h_2)} = \varphi^{(f_1 f_2^{h_1^{-1}},h_1h_2)}.$$

The action of the wreath product is faithful if and only if the actions of K on Δ and of H on Γ are faithful. The degree of the wreath product is $|\Delta|^{|\Gamma|}$.

Lemma 4.11. *Let G be a primitive permutation group of degree at least 2 on a set Ω. Then G is non-regular if and only if there exists $\alpha \in \Omega$ such that*

$$G_\alpha = N_G(G_\alpha).$$

Proof. "$\Leftarrow$". If G acts regularly on Ω, then $G_\alpha = \{1\}$ for all $\alpha \in \Omega$, and hence

$$N_G(G_\alpha) = G \neq G_\alpha.$$

Thus, if there exists $\alpha \in \Omega$ such that $N_G(G_\alpha) = G_\alpha$, then G is not regular.

"$\Rightarrow$". Now suppose that G is not regular on Ω. Since G is transitive, there exists $\alpha \in \Omega$ such that

$$G_\alpha \neq \{1\}.$$

We show that then $G_\alpha = N_G(G_\alpha)$.

Clearly,

$$G_\alpha \leq N_G(G_\alpha).$$

Now let $h \in N_G(G_\alpha)$. Then for every $g \in G_\alpha$ we have

$$h^{-1}gh \in G_\alpha.$$

Hence for every $g \in G_\alpha$,

$$\alpha^{h^{-1}gh} = \alpha.$$

Therefore, for every $g \in G_\alpha$,

$$(\alpha^{h^{-1}})^g = \alpha^{h^{-1}}.$$

In particular,

$$\alpha^{h^{-1}} \in \mathrm{Fix}_\Omega(G_\alpha).$$

But by Lemma 2.43, the set $\mathrm{Fix}_\Omega(G_\alpha)$ is a block. Since G is primitive, it follows that

$$\mathrm{Fix}_\Omega(G_\alpha) = \Omega \qquad \text{or} \qquad \mathrm{Fix}_\Omega(G_\alpha) = \{\alpha\}.$$

Since $G_\alpha \neq \{1\}$, we cannot have $\mathrm{Fix}_\Omega(G_\alpha) = \Omega$. Hence

$$\mathrm{Fix}_\Omega(G_\alpha) = \{\alpha\}.$$

Therefore

$$\alpha^{h^{-1}} = \alpha,$$

so $h \in G_\alpha$. Thus

$$N_G(G_\alpha) \leq G_\alpha.$$

Consequently,

$$G_\alpha = N_G(G_\alpha).$$

□

Theorem 4.12 (Lemma 2.7A in Dixon–Mortimer)**.** *Let K and H be non-trivial groups, let Δ and Γ be non-empty sets, and suppose that K acts faithfully on Δ and H acts faithfully on Γ. Let $\Omega = \Delta^\Gamma$. Then the wreath product*

$$G = K \wr_\Gamma H$$

acts primitively on Ω in the product action if and only if

1. *K acts primitively but not regularly on Δ, and*
2. *Γ is finite and H acts transitively on Γ.*

Proof. Let B be the base group of G and set

$$H_0 = \{(1, h) \in G \mid h \in H\}.$$

Then $G = BH_0$.

For $\delta \in \Delta$ define $\varphi_\delta \in \Omega$ to be the function that maps every point of Γ to δ, that is,

$$\varphi_\delta \colon \Gamma \to \Delta : \gamma \mapsto \delta.$$

Recall that the action of G on Δ^Γ is given by

$$\varphi^{(f,h)} \colon \Gamma \to \Delta : \gamma \mapsto \varphi(\gamma^{h^{-1}})^{f(\gamma^{h^{-1}})}.$$

Then $(f,h) \in \mathrm{Stab}_G(\varphi_\delta)$ if and only if $\varphi_\delta^{(f,h)} = \varphi_\delta$. This is the case if and only if

$$\forall \gamma \in \Gamma : \varphi_\delta(\gamma^{h^{-1}})^{f(\gamma^{h^{-1}})} = \varphi_\delta(\gamma) \iff \forall \gamma \in \Gamma : \delta^{f(\gamma^{h^{-1}})} = \delta.$$

Since $\{\gamma^{h^{-1}} \mid \gamma \in \Gamma\} = \Gamma$, it follows that

$$\mathrm{Stab}_G(\varphi_\delta) = \{(f,h) \in G \mid \varphi_\delta^{(f,h)} = \varphi_\delta\} = \{(f,h) \in G \mid f(\gamma) \in K_\delta \text{ for all } \gamma \in \Gamma\}.$$

Now by Theorem 3.17 the group G is primitive if and only if G is transitive and $\mathrm{Stab}_G(\varphi_\delta)$ is a maximal subgroup of G.

We first show that conditions (1) and (2) are necessary.

- If H is not transitive, let Σ be an orbit of H on Γ. Then

  $$M = \{(f,1) \in B \mid f(\gamma) \in K_\delta \text{ for all } \gamma \in \Sigma\}$$

  is a proper subgroup of B and is normalized by H_0. Moreover,

  $$\mathrm{Stab}_G(\varphi_\delta) < MH_0 < G,$$

  hence G is not primitive.

- If Γ is infinite, define

  $$B_0 = \{(f,1) \in B \mid f \text{ has finite support on } \Gamma\}.$$

  Then $B_0 \trianglelefteq G$ and

  $$\mathrm{Stab}_G(\varphi_\delta) < \mathrm{Stab}_G(\varphi_\delta)B_0 < G,$$

  so again G is not primitive.

- If K does not act transitively on Δ, let Π be an orbit of K. Then G is not transitive on Δ^Γ: let

  $$\psi \colon \Gamma \to \Delta$$

  be a constant function with value $\eta \in \Pi$. Then

  $$\psi^{(f,h)} \colon \gamma \mapsto \psi(\gamma^{h^{-1}})^{f(\gamma^{h^{-1}})} \in \Pi^{f(\gamma^{h^{-1}})} = \Pi,$$

  so ψ cannot be mapped to a constant function whose image lies in $\Delta \setminus \Pi$. Hence in particular G is not primitive.

- If K is transitive on Δ but not primitive, choose R with

  $$K_\delta < R < K.$$

  Then the subgroup

  $$\{(f,h) \in G \mid f(\gamma) \in R \text{ for all } \gamma \in \Sigma\}$$

  is properly contained in G and properly contains $\mathrm{Stab}_G(\varphi_\delta)$, hence G is not primitive.

- If K is regular on Δ, then the subgroup

$$D = \{(f, 1) \in B \mid f(\gamma) = f(\gamma') \text{ for all } \gamma, \gamma' \in \Gamma\}$$

is normalized by H_0, and thus

$$\mathrm{Stab}_G(\varphi_\delta) < DH_0 < G,$$

so again G is not primitive.

This proves necessity.

Now assume that (1) and (2) hold, and we must show that G is primitive. It is easy to see that B is transitive, and hence G is also transitive.

We now use the fact that a group is primitive if and only if the stabilizer of a point is a maximal subgroup, see Theorem 3.17. Therefore it suffices to show that

$$S := \mathrm{Stab}_G(\varphi_\delta)$$

is a maximal subgroup.

Suppose

$$S < M \leq G.$$

Now $G = BH_0$, and since $H_0 \leq S$, it follows that $G = BS$. Hence

$$M = M \cap G = M \cap (BS) = (M \cap B)S,$$

because $S < M$. In particular,

$$S \cap B < M \cap B.$$

Therefore there exists

$$(f, 1) \in M \cap B$$

that does not lie in $S \cap B$. So there exists $\gamma_0 \in \Gamma$ with

$$f(\gamma_0) \notin K_\delta.$$

But since K acts primitively and non-regularly on Δ, it follows from Theorem 4.11 that

$$K_\delta = N_K(K_\delta).$$

Hence

$$f(\gamma_0) \notin N_K(K_\delta),$$

and there exists $k \in K_\delta$ such that

$$f(\gamma_0)^{-1} k f(\gamma_0) \notin K_\delta.$$

Define $g \in K^\Gamma$ by

$$g(\gamma_0) = k \qquad \text{and} \qquad g(\gamma) = 1 \text{ for all } \gamma \in \Gamma \setminus \{\gamma_0\}.$$

Then

$$(g, 1) \in S.$$

Set

$$y := [f, g].$$

Then

$$(y, 1) = \big((f^{-1}gf) \cdot g, 1\big) \in MS.$$

Moreover, by pointwise multiplication,

$$y(\gamma_0) = \big(f(\gamma_0)^{-1} g(\gamma_0) f(\gamma_0)\big) \cdot g(\gamma_0) \in K \setminus K_\delta,$$

and

$$y(\gamma) = 1 \text{ for all } \gamma \in \Gamma \setminus \{\gamma_0\}.$$

Now K is primitive, and hence K_δ is a maximal subgroup. Since $y(\gamma_0) \notin K_\delta$, we have

$$K = \langle K_\delta, y(\gamma_0) \rangle.$$

Therefore M contains the subgroup

$$B(\gamma_0) = \{(f, 1) \in B \mid f(\gamma) = 1 \text{ for all } \gamma \in \Gamma \setminus \{\gamma_0\}\}.$$

Now

$$(1, h)B(\gamma_0)(1, h)^{-1} = B(\gamma_0^h)$$

for all $h \in H$. Since $H_0 \leq M$ and since H acts transitively on Γ, it follows that

$$B(\gamma) \leq S$$

for all $\gamma \in \Gamma$. Furthermore, Γ is finite, and hence

$$B = \prod_{\gamma \in \Gamma} B(\gamma) \leq M.$$

In particular,

$$M = BH_0 = G.$$

This shows that S is maximal, and therefore G is primitive. □

Chapter 5

Socles of primitive permutation groups

5.1 Centralizers and normalizers

The following proofs are due to Cheryl Praeger.

Theorem 5.1. *Let $G \leq \mathrm{Sym}(\Omega)$ and let*

$$C = C_{\mathrm{Sym}(\Omega)}(G).$$

Then for $\alpha \in \Omega$,

$$\alpha^C = \{\beta \mid G_\alpha = G_\beta\}.$$

Proof. Let

$$\Delta = \{\beta \mid G_\alpha = G_\beta\}.$$

First we show that $\alpha^C \subseteq \Delta$.

Let $\beta = \alpha^c$ for some $c \in C$. Then for $g \in G_\alpha$ we have

$$\beta^g = \alpha^{cg} = \alpha^{gc} = \alpha^c = \beta,$$

and hence $G_\alpha \leq G_\beta$. Since $\alpha = \beta^{c^{-1}}$, one sees similarly that $G_\beta \leq G_\alpha$. Thus $G_\beta = G_\alpha$ and $\beta \in \Delta$. Therefore $\alpha^C \subseteq \Delta$.

Now we show that $\Delta \subseteq \alpha^C$.

Let $\beta \in \Delta$. We construct an element $h \in C$ with $\alpha^h = \beta$. For

$$\gamma \notin \alpha^G \cup \beta^G$$

set $\gamma^h = \gamma$. For $g \in G$ set

$$(\alpha^g)^h = \beta^g.$$

If $\alpha^G = \beta^G$, then h is already defined on every $\gamma \in \Omega$. Otherwise $\alpha^G \neq \beta^G$, and we define additionally

$$(\beta^g)^h = \alpha^g.$$

It remains to show that h is well defined, lies in $\mathrm{Sym}(\Omega)$, and satisfies $h \in C_{\mathrm{Sym}(\Omega)}(G)$.

Now

$$\alpha^x = \alpha^y$$

if and only if

$$xy^{-1} \in G_\alpha = G_\beta,$$

which holds if and only if

$$\beta^x = \beta^y.$$

Using this, we can show that h is injective. Suppose

$$\gamma^h = \delta^h$$

for $\gamma, \delta \in \Omega$.

If $\gamma, \delta \notin \alpha^G \cup \beta^G$, then $\gamma = \delta$.

If $\gamma \notin \alpha^G \cup \beta^G$ and $\delta \in \alpha^G \cup \beta^G$, then also

$$\gamma^h \notin \alpha^G \cup \beta^G \quad \text{and} \quad \delta^h \in \alpha^G \cup \beta^G,$$

so $\gamma^h = \delta^h$ is impossible.

If $\gamma, \delta \in \alpha^G$, say $\gamma = \alpha^g$ and $\delta = \alpha^k$, then by the observation above, from

$$\beta^g = \gamma^h = \delta^h = \beta^k$$

it follows that

$$\alpha^g = \alpha^k,$$

and hence $\gamma = \delta$.

If $\alpha^G = \beta^G$, we are done. Otherwise note that h maps the orbit α^G onto β^G and β^G onto α^G. Hence it is not possible that $\gamma^h = \delta^h$ when γ and δ lie in different orbits.

Finally, if $\gamma, \delta \in \beta^G$, argue as in the case where they lie in α^G. One also checks easily that h is surjective, since for every $\gamma \in \Omega$ one can construct a preimage.

Therefore h is a permutation of Ω. It remains to show that for $x \in G$ we have $xh = hx$. It suffices to show that

$$\gamma^{xh} = \gamma^{hx}$$

for all $\gamma \in \Omega$.

If $\gamma \notin \alpha^G \cup \beta^G$, then

$$\gamma^{hx} = \gamma^x = \gamma^{xh},$$

since also $\gamma^x \notin \alpha^G \cup \beta^G$.

If $\gamma \in \alpha^G$, say $\gamma = \alpha^y$ for some $y \in G$, then

$$\gamma^{xh} = \alpha^{yxh} = \beta^{yx} = (\alpha^{yh})^x = \gamma^{hx}.$$

If $\alpha^G = \beta^G$, this is enough. If $\alpha^G \neq \beta^G$, and $\gamma = \beta^y \in \beta^G$, then

$$\gamma^{xh} = \beta^{yxh} = \alpha^{yx} = (\beta^{yh})^x = \gamma^{hx}.$$

Thus $hx = xh$. It follows that $h \in C$, and hence $\beta \in \alpha^C$. Therefore

$$\Delta = \alpha^C.$$

□

Example 5.2. 1. Let

$$G = \langle (1,2)(3,4) \rangle.$$

Then G is semiregular of degree 4. Hence

$$G_\alpha = \{1\} \qquad \text{for all } \alpha \in \{1, \ldots, 4\}.$$

Therefore the centralizer of G in S_4 must be transitive.

The centralizer of G in S_4 is

$$C = \langle (1,3)(2,4), (1,2) \rangle,$$

and is isomorphic to D_8, the dihedral group of order 8.

2. Let

$$G = \langle (1,3,2,4), (1,2) \rangle.$$

The centralizer of G in S_4 is

$$C = \langle (1,2)(3,4) \rangle.$$

One sees that C does not act transitively on $\{1, \ldots, 4\}$. In fact,

$$G_1 = \langle (3,4) \rangle$$

fixes the points 1 and 2, that is,

$$1^C = \{\beta \mid G_1 = G_\beta\} = \{1,2\}.$$

3. Let

$$G = \langle (1,3,2,4) \rangle.$$

Then G is regular, so the centralizer C of G in S_4 is transitive and

$$C = G.$$

Corollary 5.3. *Let $G \leq \mathrm{Sym}(\Omega)$ and let C be the centralizer of G in $\mathrm{Sym}(\Omega)$. Then:*

1. *G is semiregular if and only if C is transitive.*
2. *If G is transitive, then C is semiregular.*
3. *If G is regular, then C is also regular.*
4. *If G is transitive and abelian, then G is regular and $C = G$.*
5. *If G is finite and primitive, then either $C = \{1\}$ or $G = C$ is cyclic of prime order.*

Proof. 1. This follows immediately from the preceding theorem, once one observes that

$$G_\alpha = G_\beta \text{ for all } \alpha, \beta \in \Omega$$

means that

$$G_\alpha = \{1\}.$$

2. Let G be transitive and let H be the centralizer of C in $\mathrm{Sym}(\Omega)$. Then

$$G \leq H,$$

and hence H is transitive. Therefore, by (1), C is semiregular.

3. If G is regular, then by (1) and (2) it follows that C is also regular.

4. If G is transitive, then by (2), C is semiregular. Since G is abelian, we have

$$G \leq C.$$

Hence C is transitive, and therefore C is regular. By (1), G is then semiregular. Since G is transitive, it follows that G is regular. But then

$$C = G.$$

5. If G is primitive, then by Lemma 2.43 either

$$\mathrm{Fix}(G_\alpha) = \{\alpha\}$$

for all $\alpha \in \Omega$, and then by Theorem 5.1,

$$\alpha^C = \{\alpha\}$$

for all $\alpha \in \Omega$, that is,

$$C = 1,$$

or else

$$\mathrm{Fix}(G_\alpha) = \Omega$$

and n is a prime. Hence

$$G_\alpha = \{1\}.$$

Therefore

$$|G| = |G : G_\alpha| = n,$$

so G is a cyclic group of prime order n. By (4) it now follows that

$$G = C.$$

□

According to part (3) of this corollary, a regular permutation group G has a regular centralizer C in $\mathrm{Sym}(\Omega)$. One can also give an exact description of the normalizer in $\mathrm{Sym}(\Omega)$ of a regular group. This is important for understanding the action of a permutation group on a regular normal subgroup.

Definition 5.4. Let G be a group, and let $\rho(G) \leq \mathrm{Sym}(G)$ be the permutation group induced by the right regular action of G on itself. The *holomorph* $\mathrm{Hol}(G)$ of G is

$$\mathrm{Hol}(G) = N_{\mathrm{Sym}(G)}(\rho(G)) = \{h \in \mathrm{Sym}(G) \mid (\rho(G))^h = \rho(G)\}.$$

Lemma 5.5. *Let G be a group acting on itself by right multiplication ρ. Then*

$$\mathrm{Hol}(G) = N_{\mathrm{Sym}(G)}(\rho(G)) \cong \rho(G) \rtimes \mathrm{Aut}(G).$$

Proof. First, $\mathrm{Aut}(G)$ acts naturally on G via

$$G \times \mathrm{Aut}(G) \to G : (g, \sigma) \mapsto \sigma(g).$$

Let

$$A \leq \mathrm{Sym}(G)$$

be the permutation group on G induced by this action of $\mathrm{Aut}(G)$.

Now set

$$H = N_{\mathrm{Sym}(G)}(\rho(G)).$$

Since $\rho(G)$ is a transitive normal subgroup of H, it follows that

$$H = \rho(G)H_\alpha \qquad \text{for } \alpha = 1_G \in G.$$

Because $\rho(G)$ is regular, we have

$$H_\alpha \cap \rho(G) = 1,$$

and hence H is the semidirect product

$$H = \rho(G) \rtimes H_\alpha.$$

Now let $g, \beta \in G$ and $\sigma \in \mathrm{Aut}(G)$. Then

$$\begin{aligned} \beta^{\sigma^{-1}\rho(g)\sigma} &= \sigma\big(\rho(g)(\sigma^{-1}(\beta))\big) \\ &= \sigma\big(\sigma^{-1}(\beta)g\big) \\ &= \beta\sigma(g) \\ &= \rho(\sigma(g))(\beta). \end{aligned}$$

Therefore

$$\sigma^{-1}\rho(g)\sigma = \rho(\sigma(g)) \in \rho(G).$$

So

$$A \leq N_{\mathrm{Sym}(G)}(\rho(G)) = H.$$

Moreover, every $\sigma \in A$ fixes $\alpha = 1_G$, so

$$A \leq H_\alpha.$$

Conversely, let

$$h \in H_\alpha.$$

Since h normalizes $\rho(G)$, conjugation by h induces an automorphism of $\rho(G)$, and hence an automorphism of G. Define

$$\varphi\colon H_\alpha \to \mathrm{Aut}(G)$$

by letting $\varphi(h)$ be the automorphism induced by conjugation with h.

It remains to show that φ is an isomorphism.

We have already seen that for $\sigma \in A \leq H_\alpha$,

$$\rho(g)^{\varphi(\sigma)} = \rho(\sigma(g)) \qquad \text{for all } g \in G,$$

so φ is surjective.

Now

$$\ker \varphi = C_{H_\alpha}(\rho(G)).$$

Let

$$C := C_{\mathrm{Sym}(G)}(\rho(G)).$$

By Theorem 5.3, since $\rho(G)$ is regular, its centralizer C is also regular. Hence

$$\ker \varphi = C_{H_\alpha}(\rho(G)) = C \cap H_\alpha = \{1\}.$$

Thus φ is injective, and therefore an isomorphism. So

$$H_\alpha \cong \mathrm{Aut}(G).$$

Finally,

$$H = \rho(G) \rtimes H_\alpha \cong \rho(G) \rtimes \mathrm{Aut}(G).$$

This proves the claim. □

Let G be a group, $H \leq G$, and $K = N_G(H)$. Let Γ be the set of right cosets of H in G. Then G acts on Γ by $(Ha)^g = Hag$, and we denote the associated permutation representation by ρ. Further, K acts on Γ by $(Ha)^k = k^{-1}Ha = Hk^{-1}a$. We denote the associated permutation representation of K on Γ by λ.

Lemma 5.6 (Lemma 4.2A in Dixon–Mortimer)**.** *Let G be a group, $H \leq G$, and $K = N_G(H)$. Let Γ be the set of right cosets of H in G, and let ρ and λ be as defined above. Then:*

1. $\mathrm{Ker}(\lambda) = H$ *and* $\lambda(K)$ *is semiregular on* Γ.
2. $C_{\mathrm{Sym}(\Gamma)}(\rho(G)) = \lambda(K)$.

Proof. 1. We first show that $\mathrm{Ker}(\lambda) = H$. Now $k \in \mathrm{Ker}(\lambda)$ if and only if $k^{-1}Ha = Ha$ for all $Ha \in \Gamma$. This holds if and only if $k^{-1} \in H$.

To show that $\lambda(K)$ acts semiregularly, assume $k^{-1}Ha = Ha$. This is again equivalent to $k^{-1} \in H$, that is, to $k \in \mathrm{Ker}(\lambda)$.

2. First we show that $\lambda(K) \leq C_{\mathrm{Sym}(\Gamma)}(\rho(G))$. Let $\lambda(k) \in \lambda(K)$. Then

$$(Ha)^{\rho(g)\lambda(k)} = (Hag)^{\lambda(k)} = k^{-1}(Hag) = (k^{-1}Ha)g = (Ha)^{\lambda(k)\rho(g)}.$$

Hence $\rho(g)\lambda(k) = \lambda(k)\rho(g)$, so $\lambda(K) \leq C_{\mathrm{Sym}(\Gamma)}(\rho(G))$.

Now let $x \in C_{\mathrm{Sym}(\Gamma)}(\rho(G))$. Choose $b \in G$ such that $H^x = Hb$. Then for all $Ha \in \Gamma$,

$$(Ha)^x = H^{\rho(a)x} = H^{x\rho(a)} = Hba.$$

Thus for all $a \in H$ we have $Hb = Hba$, so $b \in N_G(H) = K$. Since $(Ha)^x = Hba = bHa$, it follows that $x = \lambda(b^{-1})$. Therefore $C_{\mathrm{Sym}(\Gamma)}(\rho(G)) \leq \lambda(K)$.

□

Theorem 5.7 (See also Lemma 4.2.4(iv) in Dixon–Mortimer)**.** *Let G be a group, let $H \leq G$, and let $K = N_G(H)$. Let Γ be the set of right cosets of H in G, and let ρ and λ be as defined above. Then:*

1. $H^{\lambda(K)} = H^{\rho(K)}$.
2. *If $\lambda(K)$ is transitive, then $K = G$ and $\lambda(G)$ and $\rho(G)$ are conjugate in* $\mathrm{Sym}(\Gamma)$.

Proof. 1. The orbit $H^{\rho(K)}$ is the set of right cosets of H in K. But this is also the orbit $H^{\lambda(K)}$.

2. If $\lambda(K)$ is transitive, then by (1),

$$\Gamma = H^{\lambda(K)} = H^{\rho(K)}.$$

Thus for every coset Ha there exists $k \in K$ with $Hk = H^{\rho(k)} = Ha$. Hence $a \in HK \leq K$ for all $a \in G$, so $K = G$. By definition of K, it follows that $H \trianglelefteq G$.

Define $t \in \mathrm{Sym}(\Gamma)$ by

$$(Ha)^t := Ha^{-1}.$$

Since $H \trianglelefteq G$, this is well-defined. Also $t^2 = 1$, so $t^{-1} = t$. We claim that

$$t^{-1}\lambda(g)t = \rho(g) \qquad \text{for all } g \in G.$$

Indeed,

$$(Ha)^{t^{-1}\lambda(g)t} = (Ha^{-1})^{\lambda(g)t} = (g^{-1}Ha^{-1})^t = (Hg^{-1}a^{-1})^t = Hag = (Ha)^{\rho(g)}.$$

Therefore $\lambda(G)$ and $\rho(G)$ are conjugate in $\mathrm{Sym}(\Gamma)$.

□

Corollary 5.8. *Let G be a group, and let ρ and λ be the right and left regular actions of G on itself. Then:*

1. $C_{\mathrm{Sym}(G)}(\rho(G)) = \lambda(G)$.
2. $C_{\mathrm{Sym}(G)}(\lambda(G)) = \rho(G)$.
3. $\lambda(G)$ *and* $\rho(G)$ *are conjugate in* $\mathrm{Sym}(G)$.
4. $\lambda(G) \cap \rho(G) = Z(G)$.

Proof. 1. For (1), choose $H = \{1\}$ in **??**.

2. Similarly to (1).

3. This follows from Theorem 5.7(2).

4. Let $z \in \lambda(G) \cap \rho(G)$. Then there exist $g, h \in G$ with $z = \lambda(g) = \rho(h)$. For $a \in G$ we have

$$ah = a^{\rho(h)} = a^z = a^{\lambda(g)} = g^{-1}a.$$

In particular, taking $a = 1$ gives $h = g^{-1}$, and hence $h \in Z(G)$. Conversely, if $z \in Z(G)$, then $\rho(z) = \lambda(z^{-1})$, and so $z \in \rho(G) \cap \lambda(G)$.

□

Let G be a permutation group on a set Ω, and let N be a regular normal subgroup of G. The next theorem shows, together with Theorem 5.5, that the action of a permutation group G on Ω is similar to the action of a subgroup of $\mathrm{Hol}(N)$ on N. In other words, we can embed G into the holomorph of the regular normal subgroup.

Theorem 5.9. *Let G be a permutation group on Ω, and let $N \trianglelefteq G$ be a regular normal subgroup. Let $\alpha \in \Omega$. Then $G = NG_\alpha$, $N \cap G_\alpha = \{1\}$, and G_α is isomorphic to a subgroup of* $\mathrm{Aut}(N)$.

In particular, Ω may be identified with N in such a way that:

1. *1 is identified with α;*
2. *N acts on Ω by right multiplication;*
3. *G_α acts on Ω by conjugation;*
4. *this induces an action of G on N similar to the action of G on Ω.*

Proof. 1. Since N is transitive, $\Omega = \alpha^N$. Define $\psi\colon \Omega \to N$ by $\alpha^n \mapsto n$ for $n \in N$. This map is well defined, since $N_\alpha = 1$. Under this identification, 1 corresponds to α.

2. Thus the actions of N on Ω and of N on itself by right multiplication are similar, because for all $x \in N$ and all $\omega = \alpha^n \in \Omega$,

$$\psi(\omega)^{\rho(x)} = n^{\rho(x)} = nx = \psi(\alpha^{nx}) = \psi(\omega^x).$$

3. Now we show that the action of G_α on Ω is similar to the action of G_α on N by conjugation. Let $g \in G_\alpha$ and $\beta = \alpha^n \in \Omega$. Since $\alpha = \alpha^{g^{-1}}$, we have

$$\psi(\beta^g) = \psi(\alpha^{ng}) = \psi(\alpha^{g^{-1}ng}) = g^{-1}ng.$$

Hence $\psi(\beta) = n$ and $\psi(\beta^g) = g^{-1}ng = \psi(\beta)^g$.

Since N is transitive, $G = NG_\alpha$, and since N is regular, $N \cap G_\alpha = 1$.

4. Finally, define an action of G on N as follows. Each $g \in G$ has a unique expression $g = mh$ with $m \in N$ and $h \in G_\alpha$. Set

$$n^g := h^{-1}nmh.$$

Then the action of G on Ω is similar to the action of G on N, because for $g = mh$,

$$\psi((\alpha^n)^g) = \psi(\alpha^{ng}) = \psi(\alpha^{h^{-1}nmh}) = h^{-1}nmh = n^{mh} = \psi(\alpha^n)^g.$$

□

Remark 5.10. If Ω is finite and G is transitive on Ω, then $\alpha^C = \mathrm{Fix}_\Omega(G_\alpha)$.

Proof. One always has $\alpha^C \subseteq \mathrm{Fix}_\Omega(G_\alpha)$, since $\alpha^{cg} = \alpha^{gc} = \alpha^c$ for $g \in G_\alpha$. If Ω is finite and $\omega \in \mathrm{Fix}_\Omega(G_\alpha)$, then $G_\alpha \leq G_\omega$. Since G is transitive, $G_\alpha = G_\omega$, and hence by Theorem 5.1, $\omega \in \alpha^C$. □

The next theorem shows that the centralizer can be found as a section in G. This proof is also due to Cheryl Praeger.

Theorem 5.11. *Let G be a transitive permutation group on a finite set Ω, let $C = C_{\mathrm{Sym}(\Omega)}(G)$, let $\alpha \in \Omega$, and let $N = N_G(G_\alpha)$. Then*

$$C \cong N/G_\alpha.$$

Moreover, N and C act on

$$\alpha^C = \{\beta \mid G_\alpha = G_\beta\},$$

and both actions are similar to the regular action of N/G_α on itself by right multiplication.

Proof. TODO □

5.2 The socle

We follow Dixon–Mortimer.

Definition 5.12. Let G be a non-trivial group. A normal subgroup $N \trianglelefteq G$ is called a *minimal normal subgroup* if $N \neq 1$ and, whenever

$$1 \neq M \trianglelefteq G \quad \text{with} \quad M \leq N,$$

it follows that $M = N$.

The *socle* $\mathrm{soc}(G)$ of G is the subgroup generated by all proper minimal normal subgroups of G, or 1 if G has no minimal normal subgroups.

Theorem 5.13 (Theorem 4.3A in Dixon–Mortimer)**.** *Let G be a finite, non-trivial group.*

1. *Let K be a minimal normal subgroup of G, and let L be any normal subgroup of G. Then either $K \leq L$ or*
$$\langle K, L\rangle = K \times L.$$
2. *There exist minimal normal subgroups $K_1, \ldots, K_m$ of G such that*
$$\mathrm{soc}(G) = K_1 \times \cdots \times K_m.$$
3. *Every minimal normal subgroup $K \trianglelefteq G$ is a direct product*
$$K = T_1 \times \cdots \times T_k,$$
where each $T_i \trianglelefteq K$ is simple, and all T_i are conjugate under G.
4. *If the groups K_i in (2) are all non-abelian, then $K_1, \ldots, K_m$ are the only minimal normal subgroups of G.*
5. *If the groups T_i in (3) are all non-abelian, then $T_1, \ldots, T_k$ are the only minimal normal subgroups of K.*

Proof. 1. Since $K \cap L \trianglelefteq G$ and K is minimal, either $K \cap L = K$ or $K \cap L = 1$. In the first case $K \leq L$, and in the second case

$$\langle K, L\rangle = K \times L,$$

since the intersection is trivial and both K and L are normal.

2. Since G is finite, we may choose a subset $\mathcal{M}$ of the set of all minimal normal subgroups of G, maximal with the property that the subgroup S generated by the members of $\mathcal{M}$ is their direct product. We show that S contains every minimal normal subgroup of G.

   Clearly $S \trianglelefteq G$, since it is generated by normal subgroups. Let K be a minimal normal subgroup of G. By (1), either $K \leq S$ or $S \times K$ is a normal subgroup of G. The latter is impossible by the maximality of $\mathcal{M}$. Hence $K \leq S$. Therefore $S = \mathrm{soc}(G)$.

3. Let T be a minimal normal subgroup of K. Then for each $g \in G$, the conjugate $T^g \leq K$ is again a minimal normal subgroup of K. Choose a subset $\mathcal{L} \subseteq T^G$ of pairwise G-conjugate minimal normal subgroups of K, maximal with the property that the subgroup L generated by the members of $\mathcal{L}$ is their direct product.

   We show that $\mathcal{L}$ contains all G-conjugates of T. Let T^g be such a conjugate. By (1), either $T^g \leq L$ or $T^g \times L$ is a normal subgroup of K. The latter is impossible by the maximality of $\mathcal{L}$. Thus $T^g \leq L$. Hence L contains all G-conjugates of T, so in particular $L \trianglelefteq G$.

   Since $1 \neq L \leq K$ and K is a minimal normal subgroup of G, it follows that $K = L$. Thus K is a direct product of the G-conjugates in $\mathcal{L}$.

   Finally, for each $T_i \in \mathcal{L}$, every normal subgroup of T_i is also normal in K, because the other factors T_j with $j \neq i$ commute with T_i. Since T_i is minimal normal in K, it follows that T_i is simple.

□

Corollary 5.14. *Every minimal normal subgroup N of a finite group G is either an elementary abelian p-group for some prime p, or $Z(N) = 1$.*

Proof. Let N be a minimal normal subgroup of G. Since $Z(N)$ is a characteristic subgroup of N, it is also normal in G. Hence

$$Z(N) = N \quad \text{or} \quad Z(N) = 1.$$

Suppose that $Z(N) = N$. Then N is abelian. By Theorem 5.13(3), N is a direct product of isomorphic simple groups. Since N is abelian, these simple groups must be cyclic of prime order. Therefore N is an elementary abelian p-group for some prime p. □

Lemma 5.15. *Let $T_1, \ldots, T_m$ be non-abelian simple groups. Let H be a group with pairwise distinct normal subgroups $K_1, \ldots, K_m$ such that*

$$H/K_i \cong T_i \quad \textit{for } 1 \leq i \leq m$$

and

$$\bigcap_{i=1}^{m} K_i = 1.$$

Then

$$H \cong T_1 \times \cdots \times T_m.$$

Proof. We argue by induction on m. For $m = 1$, we have $K_1 = 1$, so

$$H = H/K_1 \cong T_1.$$

Now let $m > 1$, and set

$$\bar{K} := \bigcap_{i=1}^{m-1} K_i, \qquad \bar{H} := H/\bar{K}, \qquad \bar{K}_i := K_i/\bar{K} \quad (1 \leq i \leq m-1).$$

Then

$$\bar{H}/\bar{K}_i \cong (H/\bar{K})/(K_i/\bar{K}) \cong H/K_i \cong T_i$$

and

$$\bigcap_{i=1}^{m-1} \bar{K}_i = 1.$$

Hence by induction,

$$\bar{H} \cong T_1 \times \cdots \times T_{m-1}.$$

In particular, by the following lemma, $\bar{H}$ has only $m-1$ maximal normal subgroups, whereas H has m, so $H \ncong \bar{H}$. Thus $\bar{K} \neq 1$.

By assumption,

$$\bar{K} \cap K_m = 1.$$

Since $H/K_m \cong T_m$ is simple, K_m is maximal normal in H, and therefore

$$H = \bar{K}K_m = \bar{K} \times K_m.$$

Moreover,

$$\bar{K} \cong H/K_m \cong T_m$$

and

$$K_m \cong H/\bar{K} \cong \bar{H} \cong T_1 \times \cdots \times T_{m-1}.$$

Thus

$$H \cong T_1 \times \cdots \times T_m.$$

□

Lemma 5.16. *Let*

$$G = T_1 \times \cdots \times T_m,$$

where the T_i are non-abelian simple groups. Then the T_i are the only minimal normal subgroups of G, and G has exactly m maximal normal subgroups, namely

$$C_G(T_i) \qquad \text{for } i = 1, \ldots, m.$$

5.2.1 Socles of primitive groups

The results obtained so far about socles were for general groups. We now apply them to primitive groups and obtain very strong consequences. Let $G \leq \mathrm{Sym}(\Omega)$ be a primitive group. By Theorem 2.18, if $H \trianglelefteq G$, then H is transitive. In particular, every non-trivial normal subgroup of G is transitive.

The next theorem shows that the socle of a finite primitive group is either regular and elementary abelian, itself a non-abelian minimal normal subgroup, regular or non-regular, or regular, non-abelian, and a direct product of two minimal normal subgroups. It is therefore natural to distinguish the cases where the socle is regular and where the socle is non-regular.

Theorem 5.17 (Theorem 4.3B [2]). *Let $G \leq \mathrm{Sym}(\Omega)$ be a finite primitive group, and let $K \trianglelefteq G$ be a minimal normal subgroup. Then exactly one of the following holds:*

1. *There exist a prime p and $d \in \mathbb{N}$ such that K is a regular elementary abelian group of order p^d, and*
$$\mathrm{soc}(G) = K = C_G(K).$$
2. *K is a regular non-abelian group, $C_G(K)$ is also a minimal normal subgroup of G, and*
$$\mathrm{soc}(G) = K \times C_G(K).$$
3. *K is non-abelian, $C_G(K) = 1$, and*
$$\mathrm{soc}(G) = K.$$

Proof. Homework Set $C = C_G(K)$. We first show that $C \trianglelefteq G$. Let $g \in G$ and $z \in C_G(K)$. Then for $k \in K$ we have

$$kz^g = kg^{-1}zg = g^{-1}(gkg^{-1})zg = g^{-1}k'zg = g^{-1}zk'g = g^{-1}zgkg^{-1}g = z^g k,$$

and hence $z^g \in C_G(K)$.

Now by Theorem 5.13(1) every minimal normal subgroup L of G distinct from K is contained in C, since then L commutes with K. Therefore $\mathrm{soc}(G) = KC$, and hence $\mathrm{soc}(G)$ is either K or $K \times C$, according as $K \leq C$ or not.

By Theorem 2.18, every normal subgroup of G is either 1 or transitive. In particular, K is transitive, and either $C = 1$ or C is transitive.

If C is transitive, then in particular $C \leq C_{\mathrm{Sym}(\Omega)}(K)$ is transitive. Hence by Theorem 5.3(1), K is semiregular. Since K is transitive, it follows that K is regular. Now C is isomorphic to $C_{\mathrm{Sym}(\Omega)}(K)$ and conjugate to K in $\mathrm{Sym}(\Omega)$. Moreover, C must be a minimal normal subgroup of G, since every proper subgroup of C is not transitive. Since every non-trivial normal subgroup of a regular group is not transitive, whereas every normal subgroup of G is transitive, it follows that C has no non-trivial normal subgroups and hence is minimal normal.

If $C = K$, then K is abelian, and by Theorem 5.14 we are in case (1).

If $\mathrm{soc}(G) = K \times C$, then we are in case (2).

If $C = 1$, then we are in case (3). □

Note that the proof of the previous theorem shows that in case (1) or (3) the socle $\mathrm{soc}(G)$ is the unique minimal normal subgroup of G. In case (2), Theorem 4.13(4) implies that K and C are the only minimal normal subgroups of G, that is, G has exactly two minimal normal subgroups.

The following corollary shows that for a finite primitive group with socle H, the normalizer of H in $\mathrm{Sym}(\Omega)$ plays an important role, since it contains H as a minimal normal subgroup, and this is even the unique minimal normal subgroup if H is non-regular.

Corollary 5.18 (Corollary 4.3B [2]). *Let G be a finite primitive group on Ω, let $H = \mathrm{soc}(G)$, and let $N = N_{\mathrm{Sym}(\Omega)}(H)$. Then:*

1. *H is a direct product of isomorphic simple groups.*
2. *H is a minimal normal subgroup of N.*

3. If H is non-regular, then H is the unique minimal normal subgroup of N.

Proof. Homework.

1. We consider the cases of Theorem 5.17. In case (1) the statement is immediate. In cases (2) and (3) it follows from Theorem 5.13(3).

2. We have $G \leq N$, since $H \trianglelefteq G$. As G is primitive, so is N, and $H \trianglelefteq N$. In cases (1) and (3), $H = K$ is a minimal normal subgroup of G, and hence also of N.

   In case (2), let $C = C_G(K)$. Then C is conjugate in $\mathrm{Sym}(\Omega)$ to K, so $C = t^{-1}Kt$ for some $t \in \mathrm{Sym}(\Omega)$. Hence $t^{-1}Kt$ centralizes K, and therefore $t^{-1}Ct = t^{-2}Kt^2 \leq K$, since $t^{-1}Kt = C$ centralizes K. Indeed,

   $$t^{-2}kt^2 \cdot t^{-1}k't = t^{-1}(t^{-1}kt)k't = t^{-1}k'(t^{-1}kt)t = t^{-1}k'tt^{-2}kt^2.$$

   Comparing orders, we get $t^{-1}Ct = K$. Thus conjugation by t interchanges K and C, so C is also a minimal normal subgroup of N.

3. If H is non-regular, then by Theorem 5.17 we are in case (3). Hence $H = K$ is the unique minimal normal subgroup of G, and therefore also of N.

□

Summary

Let G be a finite primitive permutation group acting on Ω, let $H = \mathrm{soc}(G)$, let $N = N_{\mathrm{Sym}(\Omega)}(H)$, and let K be a minimal normal subgroup of G. Then

$$H = T_1 \times \cdots \times T_m,$$

where the T_i are simple, pairwise isomorphic, and satisfy $T_i \trianglelefteq H$, and exactly one of the following holds:

- $\mathrm{soc}(G) = K$ is a regular minimal normal subgroup of G, and
  $$\mathrm{soc}(G) = C_G(K) \cong \mathbb{Z}_p^d.$$
- $\mathrm{soc}(G) = K \times C_G(K)$ for a regular, non-abelian minimal normal subgroup K of G, similar to the minimal normal subgroup $C_G(K)$.
- $\mathrm{soc}(G) = K$ is a non-abelian minimal normal subgroup of G and $C_G(K) = 1$. If K is non-regular, then K is the unique minimal normal subgroup of N.