Notes on Permutation Groups

Gareth A. Jones
School of Mathematics
University of Southampton
Southampton SO17 1BJ, U.K.
G.A.Jones@maths.soton.ac.uk

Abstract

These are notes for the Summer School on Coherent Configurations and Permutation Groups, Novy Smokovec, September 2014. The topics of the lectures are:

1. Basic examples and definitions I
2. Basic examples and definitions II
3. Invariant relations and permutation groups
4. Primitive and imprimitive groups
5. Multiply transitive groups
6. Representation theory and character theory: general concepts
7. Representation theory and character theory for permutation groups
8. The centraliser algebra
9. Johnson and Hamming graphs, groups and schemes
10. Permutation groups and maps

There is no single text which supports my lectures on permutation groups. However, the following offer useful background reading:

1. *Groups and Geometry*, by Peter M. Neumann, Gabrielle A. Stoy and Edward C. Thompson, Oxford University Press, 1994.

This is a very readable elementary introduction to group actions, mainly on geometric objects, based on an advanced undergraduate course at Oxford.

2. *Permutation Groups*, by Peter J. Cameron, London Mathematical Society Student Texts 45, Cambridge University Press, 1999.

This is a more advanced approach, with quite a wide scope but concentrating mainly on those areas within permutation groups (including infinite groups and connections with logic) where the author has shown most interest and has made his most significant contributions. There are many exercises, and some sections on computing with permutation groups.

3. *Permutation Groups*, by John D. Dixon and Brian Mortimer, Graduate Texts in Mathematics 163, Springer, 1996.

This is very comprehensive and well-organised, but rather more advanced. It is particularly good on the consequences of the classification of finite simple groups (which means that many deep results can be proved 'by inspection').

1 Basic examples and definitions I

1.1 A motivating example: Petersen's graph

We start with an example, the *Petersen graph* P (the only graph with a whole book devoted to it!). This is a 10-vertex graph of valency 3, consisting of a pentagon and a pentagram, with corresponding pairs of vertices of each joined by a single edge. More precisely, it has vertices v_i, w_i ($i \in \mathbb{Z}_5$), with edges v_iv_{i+1}, w_iw_{i+2} and v_iw_i for all $i \in \mathbb{Z}_5$. This description, together with the usual diagram for P, immediately suggests a dihedral group D_5 of ten automorphisms, generated by a rotation induced by $i \mapsto i+1$ and a reflection induced by $i \mapsto -i$.

Does P have any more automorphisms? More precisely, what is its automorphism group $G := \mathrm{Aut}\, P$, regarded as a permutation group on the set Ω of vertices of P?

If we know that P is the antipodal quotient of the dodecahedral graph D, then this tells us that there is an action of $\mathrm{Aut}\, D$ on P. Now $\mathrm{Aut}\, D = A \times Z$, with $A \cong A_5$ (the alternating group of degree 5) acting as the rotation group of the dodecahedron and $Z \cong C_2$ (a cyclic group of order 2) generated by the antipodal symmetry. We form P as the quotient D/Z, so Z acts trivially on D and there is a faithful action of A on P. We can therefore regard A as a subgroup of G. Thus $|G|$ is divisible by $|A| = 5!/2 = 60$, so (by Cauchy's

Theorem) P has automorphisms of order 3.

Exercise 1.1 Draw P to illustrate an automorphism of order 3.

Since $\mathrm{Aut}\, D$ acts transitively on the 20 vertices of D, it follows that A (and hence G) acts transitively on those of P. Thus the stabilisers G_v of the vertices v of P are all conjugate in G. Our first description of P shows that the vertex v_0 is fixed by an automorphism of order 2, so the same applies to every vertex v. Since 10 is not divisible by 3, an automorphism of order 3 must fix at least one vertex, so again, every vertex v is fixed by an automorphism of order 3. These automorphisms of order 2 and 3 fixing v permute its three neighbours as S_3, so G_v has a normal subgroup K_v of index 6, the kernel of this action of G_v, fixing v and its neighbours. Each neighbour is adjacent to two non-neighbours of v, and it is not hard to see that there is a single non-trivial automorphism of P permuting them, specifically by transposing these three pairs. Thus $|K_v| = 2$, so

$$|G| = |G : G_v|.|G_v : K_v|.|K_v| = 10.6.2 = 120.$$

Which group of order 120 is it? Since G contains a copy of A_5 as a subgroup of index 2, two obvious candidates are $A_5 \times C_2$ and S_5. (In fact, a little group theory shows that these are the only possibilities.)

Let us redefine P as $\overline{L(K_5)}$, the complement of the line graph $L(K_5)$ of the complete graph K_5. (The *line graph* of a graph Γ has vertices corresponding to the edges of Γ, and two vertices of $L(\Gamma)$ are adjacent if and only if the corresponding edges of Γ are incident at some vertex; the *complement* of a graph Γ has the same vertex set as Γ, but its edges correspond to the non-adjacent pairs of vertices of Γ.) Thus the vertices of $\overline{L(K_5)}$ correspond to the edges ij $(= ji)$ of K_5 $(i, j \in \{1, 2, \ldots, 5\})$, with two vertices ij and kl adjacent if and only if the edges ij and kl of K_5 are not incident, that is, the sets $\{i, j\}$ and $\{k, l\}$ are disjoint. This labelling of the vertices of P by pairs ij makes it clear that the automorphism group $\mathrm{Aut}\, K_5 \cong S_5$ acts faithfully on P, by permuting the symbols $i = 1, \ldots, 5$, so G contains a subgroup isomorphic to S_5. Since $|S_5| = 5! = 120 = |G|$, we must have $G \cong S_5$. (This is a particular case of Whitney's Theorem that, with a few small exceptions, a connected graph and its line graph – and hence the complement of the line graph – have the same automorphism group.)

Exercise 1.2 Show directly that $\mathrm{Aut}\, P \not\cong A_5 \times C_2$.

Exercise* **1.3** [Starred exercises are harder.] Illustrate the isomorphism

$\operatorname{Aut} P \cong S_5$ by finding a set of five objects within P which are permuted as S_5 by $\operatorname{Aut} P$.

Of course, if one knows in advance the fact that $P \cong \overline{L(K_5)}$ (as well as Whitney's Theorem) one can see immediately that $\operatorname{Aut} P \cong S_5$. However, I have proved this by a rather laborious route in order to illustrate some of the ideas and methods which may prove useful when encountering new situations. It also illustrates how mathematics is often done, by trial and error, analogy and guess-work, as opposed to the rather tidier and more systematic way it is usually presented in papers and textbooks. One could also identify $\operatorname{Aut} P$ easily with the aid of a suitable computer program. However, I have avoided mentioning these here because, although they can be very useful in verifying correct guesses and conjectures, in rejecting wrong ones, and in suggesting new ones, in general they do little to enhance our understanding. (That is a personal view, which I suspect many will disagree with!)

1.2 Generalisation: S_n acting on unordered pairs

There is an obvious generalisation of this action of S_5 on P, namely the action of the symmetric group $G = S_n$ on the set Ω of unordered distinct pairs (i.e. 2-element subsets) $\alpha = \{i, j\}$ of $[1, n] := \{1, 2, \ldots, n\}$, or equivalently on the set of edges ij $(= ji)$ of the complete graph K_5, or the vertices of its line graph $L(K_n)$ (and of its complement).

Let us assume that $n \geq 3$, so that this action is faithful. It is clearly transitive, so the point-stabilisers

$$G_\alpha = \{g \in G \mid \alpha g = \alpha\}$$

are mutually conjugate subgroups of G. Specifically,

$$G_{ij} = \operatorname{Sym}\{i, j\} \times \operatorname{Sym}\overline{\{i, j\}} \cong S_2 \times S_{n-2},$$

since the permutations of $[1, n]$ fixing the (unordered!) pair ij are those independently permuting the set $\{i, j\}$ and its complement in $[n]$. This subgroup is also the centraliser

$$C_G(t) = \{g \in G \mid gt = tg\}$$

in G of the transposition $t = (i, j)$, that is, the stabiliser of t in the action of G by conjugation on its transpositions, so these two actions of G, having the same point-stabilisers, are isomorphic. (Actions of a group G on two sets are *isomorphic* if there is a bijection between the sets commuting with the actions of G; here the bijection is obvious , namely $\alpha = ij \mapsto t = (i,j)$; transitive actions are isomorphic if and only if they have the same point-stabilisers.)

Although G is transitive on Ω, it is not 2-transitive, except in the rather trivial case $n = 3$. (A permutation group (G, Ω) is *k-transitive* if it is transitive on ordered k-tuples of distinct points; for $k \geq 2$ this is equivalent to G being transitive and each point-stabiliser being $(k-1)$-transitive on the remaining points.) In our case this is because no permutation in G can send two incident pairs ij and ik to two disjoint pairs ij and lm. Thus G has three orbits in its natural action on Ω^2 (i.e. on ordered pairs of unordered pairs!): these consist of the pairs (α, β) in which α and β are equal, incident or disjoint. Equivalently, the stabiliser G_α has three orbits on Ω, consisting of those pairs β of these three types. (More generally, the *rank* of a group G is the number of its orbits on Ω^2; when G is transitive, this is also the number of orbits of a point-stabiliser on Ω, so G is 2-transitive if and only if it has rank 2.)

In the case $n = 4$, the action of $G = S_n$ on pairs is *imprimitive*, meaning that there is a G-invariant equivalence relation on Ω other than the trivial ones, namely the identity and the universal relation. In this case we define two pairs $\alpha, \beta \in \Omega$ to be equivalent if they are equal or disjoint, or equivalently if $G_\alpha = G_\beta$. There are three equivalence classes, each of size 2, permuted by G; this action of G gives rise to the epimorphism $S_4 \to S_3$. This has no analogue for $n > 4$, since in this case the action of G on Ω is *primitive*, meaning that there are no non-trivial G-invariant equivalence relations on Ω. I will give a proof later, but in the meantime, try to prove it yourself:

Exercise 1.4 Prove that if $n \geq 5$ then S_n acts primitively on unordered pairs.

Exercise 1.5 The action of S_n on pairs gives an embedding of S_n in S_N, where $N = \binom{n}{2}$. When is it a subgroup of the alternating group A_N ?

Exercise* 1.6 When $n = 6$, show that there is a natural way in which each distinct pair $\alpha \neq \beta$ in Ω determine a third pair $\gamma \in \Omega$, giving Ω the structure of a projective space over the field $\mathbb{F}_2$, in which the lines are the triples $\{\alpha, \beta, \gamma\}$ (equivalently, $\Omega \cup \{0\}$ is a vector space over $\mathbb{F}_2$ in which $\alpha + \beta = \gamma$). Hence show that S_6 can be embedded in the general linear group $GL_4(\mathbb{F}_2)$.

[If $n = 7$ or $n \geq 9$, then S_n, acting on pairs, is a maximal subgroup of S_N or A_N, where $N = \binom{n}{2}$; $n = 6$ is an exception, with $S_6 < GL_4(\mathbb{F}_2) < S_{15}$.]

Exercise* 1.7 Let S_6 act on unordered partitions 2+2+2 of $[1,6]$ (that is, on unordered triples of subsets $\{A,B,C\}$ of size 2 with union $[1,6]$). Show that this is a transitive action of degree 15 and rank 3. Are the point-stabilisers (a) isomorphic, or (b) conjugate to those in the action of S_6 on pairs? This action is isomorphic to the action of S_6 by conjugation on of its conjugacy classes; which class is this?

Exercise 1.8 Let S_n act on m-element subsets of $[1,n]$, where $3 \le m \le n-3$. What is its rank? Is the action ever imprimitive?

[Kalužnin and Klin [14] showed that for fixed m and sufficiently large n (depending on m), the group S_n, acting on m-element subsets of $[n]$, is a maximal subgroup of S_N or A_N where $N = \binom{n}{m}$: see §9.2.]

2 Basic examples and definitions II

2.1 Regular permutation groups

A permutation group (G,Ω) is *regular* if it is transitive and the point-stabilisers G_α ($\alpha \in \Omega$) are trivial. If we choose an arbitrary element $\alpha \in \Omega$ as a base point, then for each $\beta \in \Omega$ there is a unique element $g = g_\beta \in G$ sending α to β.

Example 2.1 Take $\Omega = G$, and let G act on itself by right multiplication, so each $g \in G$ sends each $a \in G$ to ag. Then gh sends a to $a(gh) = (ag)h$, so we have a group action. One can also let G act on itself by left multiplication, but in this case we need g to send a to $g^{-1}a$ rather than ga, so that gh sends a to $(gh)^{-1}a = h^{-1}(g^{-1}a)$. These actions embed G as two regular subgroups $R(G)$ and $L(G)$ of $\mathrm{Sym}\, G$; they are isomorphic, but are different subgroups if G is non-abelian. By associativity, $g^{-1}(ag') = (g^{-1}a)g'$ for all $a, g, g' \in G$, so $R(G)$ and $L(G)$ commute with each other. Let us write $LR(G)$ for the subgroup $L(G)R(G)$ of $\mathrm{Sym}\, G$ which they generate. (I have just invented this notation, as there seems to be no standard notation for it; please let me know if you can think of something better.]

Exercise 2.1 Show that $L(G) \cap R(G)$ is isomorphic to the centre

$$Z(G) = \{z \in G \mid az = za \text{ for all } a \in G\}$$

of G, and that $LR(G) \cong (G \times G)/K$, where $K = \{(z,z) \mid z \in Z(G)\} \le G \times G$. (Thus if $Z(G) = 1$ then $LR(G) = L(G) \times R(G) \cong G \times G$.)

All regular representations of G have the same point stabilisers (the trivial subgroup), so they are all isomorphic as G-spaces. This means that the set Ω permuted can be identified with G, by choosing a base-point α as above and identifying each β with g_β, so that G is now acting on itself by right multiplication. (Note that this identification is not canonical: it depends on a choice of α to be identified with 1.)

Now suppose that G, acting on Ω, has a regular normal subgroup N. As above, we can identify Ω with N, so that G permutes N, with N acting on itself by right multiplication. The stabiliser G_1 of the identity element $1 \in N$ is then a complement for N in G (that it, $NG_1 = G$ and $N \cap G_1 = 1$), so G is a semidirect product (or split extension) $N : G_1$ (*ATLAS* [5] notation!) of N by G_1; moreover, the action of G_1 on Ω is identified with its action by conjugation on N.

Exercise 2.2 Prove the statements in the preceding sentence.

Exercise 2.3 What is the stabiliser $LR(G)_1$ in $LR(G)$ of the identity element $1 \in G$? Show that $LR(G)$ acts primitively on G if and only G is simple. *Can it act 2-transitively on G ?

Example 2.2 The dihedral group $G = D_n$ acts on the set Ω of vertices of a regular n-gon; it has a regular normal subgroup $N = C_n$, consisting of the rotations, so one can identify Ω with N. Then $G_\alpha = G_1$ is generated by a reflection fixing the vertex α identified with 1, and this acts by conjugation on N by inverting each element.

Example 2.3 If $\mathbb{F}$ is a field then the *affine group* $G = AGL_d(\mathbb{F})$ acts on the vector space $\Omega = V = \mathbb{F}^d$ by affine transformations $v \mapsto vA + t$, where $A \in GL_d(\mathbb{F})$ and $t \in V$. The translations $v \mapsto v + t$ form a regular normal subgroup isomorphic to V, and the stabiliser of the identity element $0 \in V$ is $GL_d(\mathbb{F})$, so $AGL_d(\mathbb{F}) = V : GL_d(\mathbb{F})$.

Example 2.4 Generalising the preceding example, if G is any group (possibly non-abelian) then its *holomorph* $\mathrm{Hol}\, G$ is the set of permutations $g \mapsto g\theta.t$ of G such that $\theta \in \mathrm{Aut}\, G$ and $t \in G$. Then the 'translations' $g \mapsto gt$ form a regular normal subgroup isomorphic to G (this is just $R(G)$), and automorphisms $g \mapsto g\theta$ form the stabiliser of 1, so $\mathrm{Hol}\, G = G : \mathrm{Aut}\, G$. This group $\mathrm{Hol}\, G$ is the largest subgroup of $\mathrm{Sym}\, G$ containing $R(G)$ as a normal subgroup, so it is the normaliser of $R(G)$ in $\mathrm{Sym}\, G$.

Exercise 2.4 Show that $LR(G)$ is the subgroup $G : \mathrm{Inn}\, G$ of $\mathrm{Hol}\, G$ for which

θ is an inner automorphism of G (one induced by conjugation by an element of G).

Exercise 2.5 Show that if V_4 denotes a Klein four-group $C_2 \times C_2$ (i.e. the elementary abelian group E_4 of order 4) then $\mathrm{Hol}\, V_4 \cong S_4$, and that is p is prime then $\mathrm{Hol}\, C_p \cong AGL_1(\mathbb{F}_p)$.

A permutation group is called *semiregular* if it acts regularly on each of its orbits, i.e. the point-stabilisers are all trivial. For instance, any subgroup of a regular group is semiregular.

Exercise 2.6 Show that if a permutation group commutes with a transitive group, then it is semiregular. What can be said about two commuting transitive groups?

2.2 Orders of groups

It is important to know, or be able to calculate, the orders of various finite permutation groups: for instance, if you know two of the three terms in the orbit-stabiliser equation
$$|G| = |\alpha G|.|G_\alpha|,$$
then you immediately also know the third, or if you think you know all three, then this equation gives a check on whether you are right. Here I have worked put the orders of some of the more important examples of finite groups which will appear in these notes.

By counting the possibilities for successive rows, each linearly independent of its predecessors, one finds that the *general linear group* $GL_d(\mathbb{F}_q) = GL_d(q)$ has order

$$|GL_d(q)| = N := (q^d - 1)(q^d - q)\dots(q^d - q^{d-1}).$$

The factorisation

$$N = q^{d(d-1)/2}(q-1)^d \prod_{i=0}^{d-1}(q^i + q^{i-1} + \cdots + q + 1)$$

is also useful, since the first two terms $q^{d(d-1)/2}$ and $(q-1)^d$ remind you of some important subgroups: if $q = p^e$ where p is prime then the Sylow p-subgroups (e.g. the group U of upper triangular matrices with all diagonal entries equal to 1) have order $q^{d(d-1)/2}$, and the diagonal subgroup D (a direct product of

d copies of the multiplicative group $\mathbb{F}_q^* = \mathbb{F}_q \setminus \{0\})$ has order $(q-1)^d$. Other important subgroups are the normaliser of U, a semi-direct product $U : D$ of U by D, consisting of the upper triangular matrices with non-zero diagonal entries; the group $P \cong S_n$ of permutation matrices; and the group $D : P$ of monomial matrices (those with a single non-zero entry in each row and column).

The Singer subgroups are another important set of subgroups of $GL_d(q)$. The vector space $V = \mathbb{F}_q^d$ acted on by $GL_d(q)$ is an elementary abelian p-group of order $q^d = p^{de}$. It can be identified with the additive group of the field $\mathbb{F}_{q^d}$, so that the multiplicative group $\mathbb{F}_{q^d}^* \cong C_{q^d-1}$ acts by multiplication on V as a group of transformations which are linear over $\mathbb{F}_q$. This gives us a cyclic subgroup of order $q^d - 1$ in $GL_d(q)$, permuting the non-zero vectors transitively. This group and its conjugates are called *Singer subgroups*.

The *special linear group* $SL_d(q) = \{M \in GL_d(q) \mid \det M = 1\}$ is the kernel of the epimorphism $\det : GL_d(q) \to \mathbb{F}_q^*$, so it is a normal subgroup of index $q-1$ and order

$$|SL_d(q)| = \frac{N}{(q-1)}.$$

Its Sylow p-subgroups (where $q = p^e$) are those of $GL_d(q)$, and its diagonal subgroup is a direct product of $d-1$ copies of $\mathbb{F}_q^*$.

The *projective general linear group* $PGL_d(q)$ is the quotient of $GL_d(q)$ by the group of scalar matrices; these have the form λI where $\lambda \in \mathbb{F}_q^*$, so they form a cyclic group of order $q-1$, and hence

$$|PGL_d(q)| = \frac{N}{(q-1)}.$$

The Sylow p-subgroups of $PGL_d(q)$ are isomorphic to those of $GL_d(q)$, the diagonal subgroup is a direct product of $d-1$ copies of $\mathbb{F}_q^*$, and the Singer subgroups of $GL_d(q)$ map onto cyclic subgroups of order $q^{d-1} + \cdots + q + 1$ acting regularly on the points of the geometry. (The last factors of N above correspond to Singer subgroups of $PGL_i(q)$ for $i \leq d$.)

The *projective special linear group* $PSL_d(q)$ is the quotient of $SL_d(q)$ by the group of scalar matrices of determinant 1. These have the form λI where $\lambda \in \mathbb{F}_q^*$ with $\lambda^d = 1$. Since $\mathbb{F}_q^*$ is cyclic, of order $q-1$, the number of such elements λ is the highest common factor $h = (d, q-1)$ of d and $q-1$, so

$$|PSL_d(q)| = \frac{N}{h(q-1)}.$$

In particular, $PSL_2(q)$ has order $q(q-1)(q+1)$ or $q(q-1)(q+1)/2$ as $p = 2$ or $p > 2$.

For any field $\mathbb{F}$, the Galois group Γ of $\mathbb{F}$ (that is, the group of field automorphisms of $\mathbb{F}$) acts naturally on any vector space or projective geometry over $\mathbb{F}$, by acting on coefficients of vectors or points. For instance Γ and $GL_d(\mathbb{F})$ generate a group $\Gamma L_d(\mathbb{F})$ which is a semidirect product $GL_d(\mathbb{F}) : \Gamma$, with Γ acting by conjugation on the normal subgroup $GL_d(\mathbb{F})$ by acting naturally on matrix coefficients. Similarly Γ and $SL_d(\mathbb{F})$ generate $\Sigma L_d(\mathbb{F}) = SL_d(\mathbb{F}) : \Gamma$, and so on.

In the finite case, if $q = p^e$ where p is prime, the Galois group of $\mathbb{F}_q$ is a cyclic group of order e, generated by the *Frobenius automorphism* $t \mapsto t^p$. It follows that $|\Gamma L_d(q)| = Ne$, $|\Sigma L_d(q)| = |P\Gamma L_d(q)| = Ne/(q-1)$, and $|P\Sigma L_d(q)| = Ne/h(q-1)$. Similarly, for the affine groups we have $|AGL_d(q)| = q^d N$, $|A\Gamma L_d(q)| = q^d Ne$, etc.

2.3 Finite simple groups

Many problems in finite group theory, especially those concerning permutation groups, can be reduced to questions about finite simple groups. The classification of these was completed in the early 1980s, as the result of a long series of papers, some of them very long and very difficult. I will summarise the classification very briefly here. For more details, see the excellent book [24] by Wilson, and for very concise information (far from concisely packaged) see [5].

The finite simple groups are

- the cyclic groups C_p of prime order p;
- the alternating groups A_n of degree $n \geq 5$;
- the simple groups of Lie type;
- the 26 sporadic simple groups.

The simple groups of Lie type arise as groups of linear or projective transformations of spaces defined over finite fields. They form a finite number of infinite families, each indexed by a rank (roughly corresponding to the dimension of the space, or the size of the matrices), and the order of the field. The groups $PSL_d(q)$ for $d \geq 2$ and prime powers q form a typical family, all simple except for $PSL_2(2)$ ($\cong S_3$) and $PSL_2(3)$ ($\cong A_4$). Other families include various symplectic, orthogonal and unitary groups, as well as less familiar families such as the Suzuki groups and the Ree groups, the last families to be discovered (around 1960). The most uniform construction and description of these groups is based on Lie algebras, hence the name of these groups.

The sporadic simple groups, as their name suggests, do not fit into any of the preceding four classes. Some of them, such as the Mathieu groups (see §5) and the Conway groups, form small families with related properties, while others are isolated individuals. They range in size from the Mathieu group M_{11}, of order $2^4.3^2.5.11 = 7920$, to the Monster group M of order

$$2^{46}.3^{20}.5^9.7^6.11^2.13^3.17.19.23.29.31.41.47.59.71$$

$$= 808017424794512875886459904961710757005754368000000000$$

$$\approx 8.080 \times 10^{53}.$$

In recent times a number of results, often very powerful, have been proved by inspection of the groups listed above. Such dependence on the classification of finite simple groups is often indicated by writing '(CFSG)'.

3 Invariant relations and permutation groups

3.1 Relations

A *k-relation* on a set Ω is a subset $R \subseteq \Omega^k$. If a group G acts on Ω, then it has a natural product action on Ω^k; we say that R is *G-invariant* if $Rg = R$ for all $g \in G$, i.e. R is a union of orbits of G on Ω^k. We let $k\text{-rel}\, G$ denote the set of all G-invariant k-relations on Ω. The *k-closure* $G^{(k)}$ of G is the set of all $g \in \mathrm{Sym}\,\Omega$ such that $Rg = R$ for all $R \in k\text{-rel}\, G$. Thus $G \leq G^{(k)}$, and we say that G is *k-closed* if $G = G^{(k)}$. Every k-relation can be regarded as a $(k+1)$-relation, by repeating kth coordinates, so

$$G^{(1)} \geq G^{(2)} \geq \cdots \geq G^{(k)} \geq G^{(k+1)} \geq \cdots \geq G.$$

Lemma 3.1 *The automorphism group of a k-relation is k-closed.* □

A 1-relation is just a subset of Ω, so 1-rel G is the set of G-invariant subsets of Ω, i.e. unions of orbits of G on Ω, and $G^{(1)}$ is the cartesian product of the symmetric groups on those orbits.

A 2-relation R is the set of arcs (directed edges) of a directed graph Γ with vertex-set Ω, and it is G-invariant if and only if $G \leq \operatorname{Aut}\Gamma$. The orbits $R_1, \ldots, R_r$ of G on Ω^2 are called (by group-theorists) the *orbitals* of G; they provide *orbital graphs* $\Gamma_1, \ldots, \Gamma_r$, with $G \leq \operatorname{Aut}\Gamma_i$, and the number r of them is called the *rank* of G on Ω. If R_i is an orbit of G then the set $\{(\beta, \alpha)) \mid (\alpha, \beta) \in R_i\}$ is also an orbit, say $R_{i'}$. If $i = i'$ then R_i is *self-paired*, and it is conventional to replace the pairs of arcs between vertices α and β in Γ_i with single undirected edges. If $i \neq i'$ then R_i and $R_{i'}$ are *paired orbits*, and Γ_i and $\Gamma_{i'}$ are directed graphs, related to each other by reversing arcs. If G is transitive on Ω we can take R_1 to be the identity relation; then Γ_1, the *trivial orbital graph*, has a loop at each vertex, and no other edges.

Exercise 3.1 Find the orbital graphs Γ_i for the natural representation of D_n of degree n, for $n = 4, 5, 6$.

Example 3.1 Automorphism groups of graphs are important examples of permutation groups. Any graph is defined by a 2-relation on the vertex set (namely the set of edges, directed or undirected), so its automorphism group is 2-closed.

Example 3.2 Affine and projective geometries of dimension greater than 1 are defined by 3-relations (collinearity), so their automorphism groups are 3-closed.

3.2 Equivalence relations

Equivalence relations (equivalently, partitions of Ω) are important examples of 2-relations, especially when they are G-invariant. For instance, the orbits of G define a G-invariant equivalence relation. Let us assume that G is transitive. In all cases there are two obvious G-invariant equivalence relation: the universal relation, with a single equivalence class, and the identity relation, with all classes singletons; we call these the *trivial* equivalence relations. If there are non-trivial G-invariant equivalence relations, we say that G acts *imprimitively*; otherwise, when there are no non-trivial G-invariant equivalence relations on Ω, we say that G acts *primitively*. Examples of imprimitive actions include the following:

Example 3.3 The symmetry groups of the cube, octahedron, icosahedron and dodecahedron, acting on vertices, preserve the relation of being equal or antipodal (but what about the tetrahedron?).

Example 3.4 If V is a vector space, then generating the same 1-dimensional subspace is a $GL(V)$-invariant equivalence relation on $V \setminus \{0\}$, non-trivial if the underlying field is not $\mathbb{F}_2$ (but what if it is $\mathbb{F}_2$?).

Example 3.5 let S_4 act on pairs, and define two pairs to be equivalent if they are equal or disjoint (but what about $n \neq 4$?).

If G is imprimitive then the equivalence classes are called *blocks of imprimitivity*; these are permuted by G, giving a second action of G, of degree dividing $n = |\Omega|$. In the examples above we get the action on diagonals, on the associated projective geometry, and the epimorphism $S_4 \to S_3$ with kernel V_4.

If G is an imprimitive but transitive group of degree n, with a G-invariant equivalence relation R, then the blocks all have constant size c (a proper divisor of n), and there are d of them, say $B_1, \ldots, B_d$, where $n = cd$. (Thus a transitive group of prime degree must be primitive.) Since G preserves R we have $G \leq \operatorname{Aut} R$, so it is useful to understand the full automorphism group of R, the largest subgroup of $\operatorname{Sym}\Omega$ preserving R.

There is a normal subgroup $K \cong S_c \times \cdots \times S_c = S_c^d$ in $\operatorname{Aut} R$, the kernel of its action on the set of blocks, with the i-th direct factor permuting the points in B_i and fixing those in the other blocks. Choosing bijections $B_1 \to \ldots \to B_d$ gives a complement S_d, permuting the blocks transitively, with each of its orbits on Ω meeting each B_i in a single point. This group acts by conjugation on K, permuting the direct factors naturally, so $\operatorname{Aut} R$ is isomorphic to the *wreath product* $S_c \wr S_d = K : S_d$ (a semidirect product of K by S_d). This action of $S_c \wr S_d$ is called the *imprimitive action*, to distinguish it from another important action of this group which will appear later.

Now our transitive but imprimitive group G is contained in $\operatorname{Aut} R = S_c \wr S_d$. The kernel of its action on the blocks is $G \cap K$, a subgroup of $K = S_c \times \cdots \times S_c$ which is normal in G, and the permutation group induced by G on the blocks is a subgroup $\overline{G} \cong G/(G \cap K)$ of S_d.

This shows how imprimitive groups can be reduced to permutation groups of lower degree, so we concentrate on primitive groups. Next we consider some criteria to recognise when a transitive group is primitive.

If G acts transitively on Ω, and $\alpha \in \Omega$, then the G-invariant equivalence relations R on Ω correspond to the subgroups H of G such that $G_\alpha \leq H \leq G$: given H, define $B = \alpha H$ and check that the images of B under G form a G-invariant partition of Ω; conversely, given R, define H to be the set of elements of G sending α to some equivalent point. The identity and universal relations R correspond to the subgroups $H = G_\alpha$ and G, so we have:

Proposition 3.2 *A transitive permutation group G is primitive if and only if some (and hence each) point-stabiliser G_α is a maximal subgroup of G.* □

Exercise 3.2 Show that the alternating group A_5 has primitive permutation representations of degrees $5, 6$ and 10, and has imprimitive but transitive representations of degrees $12, 15, 20, 30$ and 60.

Theorem 3.3 (Higman [10], Sims [19]) *A transitive permutation group G is primitive if and only if each non-trivial orbital graph for G is connected.*

Proof. If some non-trivial orbital graph is not connected, its connected components, which are permuted by G, form blocks of imprimitivity for G. Conversely, let R be a non-trivial G-invariant equivalence relation, containing (α, β) for some $\alpha \neq \beta$, and let Γ be the orbital graph coresponding to the orbit of G on Ω^2 containing (α, β); then each connected component of Γ is contained in an equivalence class for R, so Γ is not connected. □

Exercise 3.3 Use this theorem to show that the natural action of D_n for $n \geq 3$, on vertices of an n-gon, is primitive if and only if n is prime, and that the action of S_n $(n \geq 3)$ on pairs is primitive if and only if $n \neq 4$.

Example 3.6 The *Hamming graph* $H_d(c)$, for integers $c, d \geq 2$, has vertex set

$$\Omega = \mathbb{Z}_c \times \cdots \times \mathbb{Z}_c = \mathbb{Z}_c^d,$$

with two vertices joined by an edge if and only if they differ in one coordinate. Thus there are c^d vertices, each of valency $(c-1)d$. The distance of a vertex $v = (a_1, \ldots, a_d)$ from the vertex $0 = (0, \ldots, 0)$ is equal to its *weight* $\mathrm{wt}\, v$, that is, the number of coordinates $a_i \neq 0$. The wreath product $G = S_c \wr S_d = (S_c \times \cdots \times S_c) : S_d$ acts on $H_d(c)$ as a group of automorphisms, transitive on Ω: for $i = 1, \ldots, d$ each of the d direct factors S_c permutes the values $a_i \in \mathbb{Z}_c$ of the coordinates in the ith coordinate position, while S_d acts on each vector by permuting its coordinates $a_1, \ldots, a_d$. (I shall show in §9 that $\mathrm{Aut}\, H_d(c) = S_c \wr S_d$, but you could try that now.) This is called the *product action* of $S_c \wr S_d$, to distinguish it from the imprimitive action of degree cd discussed earlier; it is also sometimes called the *exponentiation* $S_c \uparrow S_d$.

Exercise 3.4 How can the product action of $S_c \wr S_d$ of degree c^d be obtained from its imprimitive action of degree cd ?

Exercise 3.5 Describe the orbitals for $S_c \wr S_d$ in its product action.

Exercise 3.6* For which c and d is the product action of $S_c \wr S_d$ primitive?.

4 Primitive permutation groups

4.1 Normal subgroups of primitive groups

Proposition 4.1 *Every 2-transitive permutation group is primitive.*

Proof. Either show directly that there are no non-trivial invariant equivalence relations, using 2-transitivity to send two equivalent points to two inequivalent points, or use the fact that the only non-trivial orbital graph is a complete graph, and is therefore connected. □

The converse is false, e.g. consider S_n acting on pairs for $n > 4$.

Example 4.1 The group $PGL_2(q)$ acts 3-transitively by Möbius transformations

$$t \mapsto \frac{at+b}{ct+d} \quad (a, b, c, d \in \mathbb{F}_q,\ ad - bc \neq 0)$$

on the projective line $\mathbb{P}^1(\mathbb{F}_q) = \mathbb{F}_q \cup \{\infty\}$, and its subgroup $PSL_2(q)$ (where $ad - bc = 1$) acts 2-transitively, so they both act primitively.

Exercise 4.1 Prove that $PGL_2(q)$ and $PSL_2(q)$ are respectively 3- and 2-transitive on $\mathbb{P}^1(\mathbb{F}_q)$.

Proposition 4.2 *If N is a normal subgroup of a permutation group G, then G permutes the orbits of N.*

Proof. $\alpha N g = \alpha g N$. □

Corollary 4.3 *A non-trivial normal subgroup of a primitive permutation group G must be transitive.*

Proof. Otherwise, the orbits of N are blocks of imprimitivity. □

Corollary 4.4 *A primitive permutation group G has at most two minimal (non-trivial) normal subgroups. If it has two, they are the left and right regular representations of the same non-abelian group M.*

Proof. Let M_1 and M_2 be distinct minimal normal subgroups of G. The subgroup $[M_1, M_2]$ of G generated by the commutators $[g_1, g_2] := g_1^{-1} g_2^{-1} g_1 g_2$ ($g_i \in M_i$) is a normal subgroup of G contained in each M_i; by minimality it is trivial, so $g_2 g_1 = g_1 g_2$ and thus M_1 and M_2 commute. By Corollary 4.3 they are both transitive, with transitive centralisers, so they both act regularly (see Exercise 2.6), as the left and right regular representations of the same group M, which is non-abelian since $M_1 \neq M_2$. There can be no third minimal normal subgroup M_3, since we could apply the above argument to M_1 and M_3, giving $M_3 = M_2$. $\square$

Example 4.2 The affine group $AGL_d(\mathbb{F})$ over any field $\mathbb{F}$ is 2-transitive and hence primitive on the vector space $V = \mathbb{F}^d$; it has a unique minimal normal subgroup M, consisting of the translations.

Example 4.3 Let $G = S \times S$ for some non-abelian simple group S. Let G act on $\Omega = S$ by left and right multiplication, each $(g, h) \in S \times S$ sending each $a \in S$ to $g^{-1}ah$. Then G acts faithfully and primitively on Ω, and $M_1 := S \times 1$ and $M_2 := 1 \times S$ are minimal normal subgroups of G. (See §2.1, especially Exercise 2.3.)

In order to apply the above results we need to know the possible structure of a minimal normal subgroup. First we need some definitions. A subgroup K of a group G is *characteristic* if it is invariant under all automorphisms of G; examples include the centre $Z(G)$ and the derived group G'. This is a stronger condition than being normal (invariance under inner automorphisms of G).

Being a normal subgroup is not a transitive relation; instead we have:

Lemma 4.5 *If K is a characteristic subgroup of a normal subgroup N of a group G, then K is a normal subgroup of G.*

Proof. Each element of G, acting by conjugation, induces an automorphism of N, which must leave K invariant. $\square$

Exercise 4.2 Give an example in which K is a normal subgroup of N and N is a normal subgroup of G, but K is not a normal subgroup of G.

It follows from Lemma 4.5 that a minimal normal subgroup M of a group G must be *characteristically simple*, that is, it has no characteristic subgroups other than itself and 1. It can be shown that a *finite* characteristically simple group is isomorphic to $S \times \cdots \times S = S^d$ for some simple group S and integer $d \geq 1$. In particular, if M is abelian then so is S, so $S \cong C_p$ for some prime p; then M is an elementary abelian p-group C_p^d, and (written additively) can be regarded as a d-dimensional vector space over the field $\mathbb{F}_p$.

The following exercises show why we need to assume finiteness of G at this point.

Exercise 4.3 Give an example of an infinite group with no minimal normal subgroups.

Exercise 4.4 Show that the additive group of any field is characteristically simple. (The same applies to division algebras – non-commutative versions of fields.)

4.2 Structure of a finite primitive group

Let G be a finite primitive permutation group, so by Corollary 4.4 it has at most two minimal normal subgroups. We consider the different possibilities.

Case 1 If G has a unique minimal normal subgroup M, then the centraliser $C := C_G(M)$ of M in G, the kernel of the action of G by conjugation on M, is a normal subgroup of G, so either $C \geq M$ or $C = 1$.

Case 1a If $C \geq M$ then M is abelian, so being transitive it must act regularly, and being characteristically simple it is isomorphic to C_p^d, giving

$$M \leq G \leq \operatorname{Hol} M = AGL_d(p).$$

Then $G = M : G_0$ where $M \cong \mathbb{F}_p^d$ and G_0 is a subgroup of $GL_d(p)$ acting irreducibly (i.e. with no proper invariant subspaces, see $6) on M.

Case 1b If $C = 1$ then M (and hence S) is non-abelian and G acts faithfully by conjugation on M, giving

$$M \leq G \leq \operatorname{Aut} M.$$

The automorphisms of $M = S^d$ permute the direct factors. It follows that $\operatorname{Aut} M$ has a normal subgroup $(\operatorname{Aut} S)^d$, the kernel of its action permuting the factors, with each factor $\operatorname{Aut} S$ acting naturally on the corresponding factor S of S^d, and this has a complement S_d permuting the direct factors. Thus $\operatorname{Aut} S^d$ is a wreath product $\operatorname{Aut} S \wr S_d$, and

$$G \leq \operatorname{Aut} M \cong \operatorname{Aut} S \wr S_d.$$

The automorphism groups $\operatorname{Aut} S$ of the finite simple groups S are all known; for instance, here we could have $S = A_c$ ($c \geq 5$) and $\operatorname{Aut} S = S_c$ if $c \neq 6$.

Case 2 If G has two minimal normal subgroups, they are isomorphic to $M = S^d$ for some non-abelian finite simple group S, and

$$M \times M \leq G \leq \operatorname{Hol} M = M : \operatorname{Aut} M.$$

For instance, see Example 4.3 with $d = 1$. As in Case (1b), $\mathrm{Aut}\, M \cong \mathrm{Aut}\, S \wr S_d$ and $\mathrm{Aut}\, S$ is known.

As a by-product of this analysis, we have:

Theorem 4.6 *A finite solvable primitive permutation group must have prime power degree.*

Proof. In the preceding argument, if G is solvable then a minimal normal subgroup M is also solvable; being characteristically simple, it must be an elementary abelian p-group for some prime p, acting regularly, so G is a subgroup of $AGL_d(p)$, of degree p^d, for some prime p, as in Case 1a. □

Example 4.4 $AGL_1(q)$, acting on $\mathbb{F}_q$, is primitive (being 2-transitive) and also solvable (because the translations form an abelian normal subgroup, with an abelian quotient). The group $A\Gamma L_1(q)$ is also primitive and solvable.

The O'Nan-Scott Theorem (see [3, Ch. 4] or [8, Ch. 4] for details) takes a closer look at *all* the minimal normal subgroups M of G, and the subgroup they generate (the *socle* of G), in order to give a more precise description of the primitive groups G than that outlined above (the full statement and proof are too detailed to cover here). In most practical applications, the most important cases are Case 1a, when G is *affine*, i.e. $G \leq AGL_d(p)$ with M the translation group, and Case 1b with $d = 1$, when G is *almost simple*, i.e. $S \leq G \leq \mathrm{Aut}\, S$ for some non-abelian simple group $S = M$. In the latter case the quotient $\mathrm{Aut}\, S/S$, the outer automorphism group $\mathrm{Out}\, S$ of S, is usually very small, allowing few possibilities for G; for instance $\mathrm{Out}\, A_n \cong C_2$, giving $G = A_n$ or S_n, for all $n \geq 5$ except $n = 6$, where $\mathrm{Out}\, A_6 \cong V_4$.

4.3 Prevalence of alternating and symmetric groups

There are primitive permutation groups of every finite degree n, namely the natural representations of S_n and A_n, and we have seen some examples of others. Surprisingly, for 'most' n there are no others: the set of n for which there are other primitive groups of degree n has asymptotic density zero!

Theorem 4.7 (Cameron-Neumann-Teague) *Let $e(x)$ denote the number of integers $n < x$ for which there is a primitive group of degree n other than S_n or A_n. Then*

$$e(x) = 2\pi(x) + (1 + \sqrt{2})x^{1/2} + O(x^{1/2}/\log x).$$

Here $\pi(x)$ is the number of primes $p < x$, so $\pi(x) \sim x/\log x$ by the Prime Number Theorem, and hence

$$\frac{e(x)}{x} \sim \frac{2}{\log x} \to 0 \quad \text{as } x \to \infty.$$

In this theorem, primitive groups C_p and $PGL_2(p)$ of degree $n = p < x$ and $n = p + 1 < x$ each contribute asymptotically $\pi(x)$, while $S_c \wr S_2$ in its product action of degree $n = c^2 < x$, and S_m acting on pairs, of degree $n = m(m-1)/2 < x$, justify the terms $x^{1/2}$ and $\sqrt{2}x^{1/2}$. The remaining (difficult) part of the proof uses the O'Nan-Scott Theorem to show that the set of degrees of the remaining primitive groups, other than S_n and A_n, has sufficiently small density. For instance, degrees $n = c^d < x$ (arising from $S_c \wr S_d$) with $d \geq 3$ contribute at most

$$\lfloor x^{1/3} \rfloor + \lfloor x^{1/4} \rfloor + \cdots = O(x^{1/3} \log x)$$

to $e(x)$. See [3, §4.9] for a more detailed outline proof.

Another surprising result on the prevalence of alternating and symmetric groups is the following:

Theorem 4.8 (Dixon) *Let permutations x and y be chosen from S_n, randomly and independently, with uniform distribution, and let $G = \langle x, y \rangle$ be the subgroup they generate. Then the probabilities*

$$\Pr(G = S_n) \to 3/4 \quad \textit{and} \quad \Pr(G = A_n) \to 1/4$$

as $n \to \infty$.

Of course, $1/4$ is the probability that x and y are both even, so that $G \leq A_n$. Convergence is surprisingly rapid. The proof depends on knowing enough about the maximal subgroups of S_n and A_n (see [3, §4.6] or [8, §8.5]) to estimate the probability that none of them contains both x and y.

Exercise 4.5 Use GAP or MAPLE to test Theorem 4.8, by choosing a large number of random pairs of permutations and finding the groups they generate.

5 Multiply transitive groups

A permutation group G, acting on Ω is *k-transitive* if it acts transitively on k-tuples of distinct points in Ω; this means that if $(\alpha_1, \ldots, \alpha_k)$ and $(\beta_1, \ldots, \beta_k)$ in Ω^k satisfy $\alpha_i \neq \alpha_j$ and $\beta_i \neq \beta_j$ for all $i \neq j$, then there exists some $g \in G$ such that $\alpha_i g = \beta_i$ for $i = 1, \ldots, k$. If g is unique, so that G acts regularly on k-tuples of distinct points, we say that G is *sharply k-transitive*. If G is k-transitive then it is also $(k-1)$-transitive, since one can simply ignore kth terms. Clearly 1-transitivity is the same as transitivity.

Example 5.1 The symmetric group S_n, acting naturally, is sharply n-transitive. The alternating group A_n is sharply $(n-2)$-transitive: there are two permutations sending α_i to β_i for $i = 1, \ldots, n-2$, differing by a transposition, so one is even and the other is odd. The general linear group $GL_d(\mathbb{F})$ is transitive on non-zero vectors, and is 2-transitive if and only if $|\mathbb{F}| = 2$.

Exercise 5.1 Show that the projective general linear group $PGL_d(\mathbb{F})$ is 2-transitive on points, and is 3-transitive if and only if $d = 2$, in which case it is sharply 3-transitive. Can $GL_d(\mathbb{F})$ be 3-transitive on non-zero vectors?

Lemma 5.1 *A permutation group G is k-transitive for some $k \geq 2$ if and only if it is transitive and a point-stabiliser G_α is $(k-1)$-transitive on the remaining points.*

Proof. Easy exercise. □

Example 5.2 The affine general linear group $AGL_2(\mathbb{F})$ is transitive on $V = \mathbb{F}^d$, and the stabiliser of 0 is $GL_d(\mathbb{F})$, so $AGL_d(\mathbb{F})$ is 2-transitive on V, and 3-transitive if $|\mathbb{F}| = 2$.

As a consequence of the classification of finite simple groups, the finite k-transitive groups are all known for each $k \geq 2$ (see [8, Chapter 7]). A first step in their classification is the following theorem of Burnside [2, §154], an early precursor of the O'Nan-Scott Theorem:

Theorem 5.2 (Burnside) *A finite 2-transitive permutation group G is either affine or almost simple.*

In other words, if G is finite and 2-transitive, then either $G \leq AGL_d(p)$ for some prime p and $d \geq 1$, with G_0 a subgroup of $GL_d(p)$ acting transitively on non-zero vectors, or $S \leq G \leq \operatorname{Aut} S$ for some non-abelian finite simple group S. In the first case, the relevant linear groups G_0, and hence the 2-transitive affine groups G, are known: obvious examples include $G_0 = GL_d(p)$ for $d \geq 1$, and $SL_d(p)$ for $d \geq 2$. In the second case, with just one exception, the simple group S is also 2-transitive; this means that it is sufficient to classify the 2-transitive representations of the non-abelian finite simple groups, and the classification of finite simple groups allows this: see [3, Table 7.4] or [8, §7.7], for instance. (The exception here is a 2-transitive representation of degree 28 of $G = P\Gamma L_2(8)$, with $S = PSL_2(8)$ of rank 3.)

There are other examples of 2- and 3-transitive groups, besides those listed above, but apart from alternating and symmetric groups there are only four finite 4-transitive groups, and two finite 5-transitive groups. These are all Mathieu groups, finite simple groups which arise most naturally as the automorphism groups of Steiner systems [8, §6.3].

A *Steiner system* $\mathcal{S} = \mathcal{S}(t, k, n)$, for integers $t < k < n$, is an n-element set Ω with a collection of k-element subsets $B \subset \Omega$, called *blocks*, such that each set of t elements of Ω is contained in a unique block.

Example 5.3 The affine geometry $V = \mathbb{F}_q^d$ is a Steiner system $\mathcal{S}(2, q, q^d)$ with the affine lines as blocks. The associated projective geometry is a Steiner system $\mathcal{S}(2, q+1, (q^d - 1)/(q-1))$, with the projective lines as blocks.

The deceptively simple definition of a Steiner system imposes quite strong restrictions on the parameters t, k and n. There are $\binom{n}{t}$ t-element subset of Ω, each determine a unique block; each block has $\binom{k}{t}$ t-element subsets, so if there are b blocks then

$$\binom{n}{t} = b\binom{k}{t}.$$

Thus $\binom{n}{t}$ is divisible by $\binom{k}{t}$. It is easy to check that deleting a point $\alpha \in \Omega$ gives a Steiner system $\mathcal{S}(t-1, k-1, n-1)$ in which the blocks are the sets $B \setminus \{\alpha\}$ where B is a block of $\mathcal{S}$ containing α, so $\binom{n-1}{t-1}$ is divisible by $\binom{k-1}{t-1}$. Iterating gives further restrictions.

Exercise 5.2 Show that if a Steiner system $\mathcal{S}(2, 3, n)$ exists then $n \equiv 1$ or 3 mod (6). (These conditions are also known to be sufficient.)

The automorphism group $\operatorname{Aut} \mathcal{S}$ of a Steiner system $\mathcal{S}$ is the subgroup of $\operatorname{Sym} \Omega$ preserving the set of blocks. One can show that there is a unique Steiner system $\mathcal{S}(5, 6, 12)$: there are several constructions, for instance take

$\Omega = \mathbb{P}^1(\mathbb{F}_{11}) = \mathbb{F}_{11} \cup \{\infty\}$, take $B = \{0, 1, 3, 4, 5, 9\}$, the set of perfect squares in $\mathbb{F}_{11}$, and let the blocks be the images of B under the group $PSL_1(11)$ of projective transformations of Ω. The automorphism group of $\mathcal{S}$ is a sharply 5-transitive simple group of order $12.11.10.9.8 = 95040$; this is the Mathieu group M_{12}. Deleting a point gives the unique Steiner system $\mathcal{S}(4, 5, 11)$; its automorphism group, the stabiliser of a point in M_{12}, is a sharply 4-transitive simple group of order $11.10.9.8 = 7920$; this is the Mathieu group M_{11}.

Exercise 5.3. In $\mathcal{S}(5, 6, 12)$, how many blocks are there? How many blocks contain one, two, three or four given points?

Similarly, there is a unique Steiner system $\mathcal{S}(5, 8, 24)$, the Witt design W_{24}; its automorphism group is a 5-transitive simple group of order

$$24.23.22.21.20.48 = 2^{10}.3^3.5.7.11.23 = 244,823,040,$$

the Mathieu group M_{24}, and the stabilisers of a point and of two points are the 4- and 3-transitive simple Mathieu groups M_{23} and M_{22}. These five sporadic simple groups were discovered in the 19th century by Mathieu; they also arise in connection with other structures such as error-correcting codes, lattices, and Hadamard matrices. For instance, the extended Golay code $\mathcal{G}_{24}$ of length 24 is the 12-dimensional linear subspace of the power set $\mathcal{P}(\Omega)$ of Ω spanned by the blocks. The remaining 21 sporadic simple groups were not discovered until about 100 years later, between 1966 and 1976

Exercise 5.4 Show that in a Steiner system $\mathcal{S}(5, 8, 24)$, every element lies in 253 blocks, every two elements lie in 77 blocks, every three elements lie in 21 blocks, and every four elements lie in five blocks.

Exercise 5.5* Give an example of an infinite permutation group which is transitive on m-element subsets for every $m \in \mathbb{N}$, but which is not 2-transitive. Find another one which is 2- but not 3-transitive.

6 Representation theory and character theory: general concepts

Here I will give a very brief summary of representation theory, an immense subject; for detailed background, see [6] or [9], and for a fairly short and very elegant introduction see [18]. In the next section I shall apply some of this theory to permutation groups.

A (linear) *representation* of a group G over a field $\mathbb{F}$ is an action $V \times G \to V$ by linear transformations of a vector space V of finite dimension $d \geq 1$ over $\mathbb{F}$, or equivalently a homomorphism $\rho : G \to GL(V)$; by choosing a basis for V, one can regard it as a homomorphism $\rho : G \to GL_d(\mathbb{F})$. We call d the *degree* or *dimension* of ρ, and we call V a *G-module.* (It is sometimes called an *$\mathbb{F}G$-module*, since one can extend the action of G by linearity to the group algebra $\mathbb{F}G = \{\sum_{g\in G} a_g g \mid a_g \in \mathbb{F}\}$, making V a module over this ring.)

A *G-homomorphism* is a homomorphism $V_1 \to V_2$ between G-modules, commuting with the actions of G on V_1 and V_2; it is a *G-isomorphism* if it is invertible, in which case the two representations of G are *equivalent.* This corresponds to conjugacy of the images of G in $GL_d(\mathbb{F})$.

A *G-submodule* U of V is a linear subspace which is invariant under the action of G , giving representations of G on U and on the quotient module V/U. Obvious examples include $U = 0$ and $U = V$. We say that V and ρ are *reducible* if there is a G-submodule $U \neq 0, V$; otherwise, they are *irreducible.* When V is reducible, by extending a basis of U to a basis of V one can represent G by block matrices of the form

$$\begin{pmatrix} A & 0 \\ * & B \end{pmatrix},$$

with matrices A and B representing the actions of G on U and V/U.

Example 6.1 Let the representation $\rho : G = \mathbb{Z} \to GL_2(\mathbb{F})$ be given by

$$i \mapsto \begin{pmatrix} 1 & 0 \\ i & 1 \end{pmatrix},$$

for each $i \in \mathbb{Z}$, so i acts on the standard basis by $e_1 \mapsto e_1, e_2 \mapsto ie_1 + e_2$. The subspace $U = \langle e_1 \rangle$ is a G-submodule, so ρ is reducible.

We say that V and ρ are *decomposable* if $V = U_1 \oplus U_2$ for G-submodules $U_i \neq 0, V$; otherwise they are *indecomposable.* Again, in the decomposable case we can represent G by block matrices, this time of the form

$$\begin{pmatrix} A & 0 \\ 0 & B \end{pmatrix},$$

with A and B representing the actions of G on U_1 and U_2.

Exercise 6.1 Represent a cyclic group $G = C_n$ on $V = \mathbb{R}^2$ by rotation matrices, where $n \geq 3$. Show that V is indecomposable, but if we extend the representation to $\mathbb{C}^2$, usng the same matrices, it is decomposable.

Clearly, decomposable representations are reducible; equivalently, irreducible representations are indecomposable. However the converse is false:

Example 6.2 For a reducible but indecomposable representation, one could take $G = \mathbb{Z} \to GL_2(\mathbb{F})$ as in Example 6.1, for any field $\mathbb{F}$. Alternatively, one could take $G = \mathbb{Z}_n \to GL_2(\mathbb{F})$, where $\operatorname{char} \mathbb{F} = p$ divides n, using the same matrices.

These examples illustrate the two main obstructions to the converse: infinite groups, and fields of characteristic dividing the order of a finite group.

Theorem 6.1 (Maschke's Theorem) *If G is a finite group and* $\operatorname{char} \mathbb{F}$ *is* 0 *or coprime to $|G|$, then every G-submodule of a G-module V has a G-invariant complement.* $\square$

(In other words, every reducible G-module is decomposable.)

Example 6.3 Represent a permutation group G of degree n by permutation matrices, permuting the standard basis $e_1, \ldots, e_n$ of $V = \mathbb{F}^n$. Then there are G-invariant subspaces

$$V_0 = \{(a_1, \ldots, a_n) \in V \mid a_1 = \cdots = a_n\},$$

of dimension 1, and

$$V^0 = \{(a_1, \ldots, a_n) \in V \mid a_1 + \cdots + a_n = 0\},$$

of codimension 1. If $\operatorname{char} \mathbb{F}$ is 0 or does not divide n, then $V = V_0 \oplus V^0$, but if $\operatorname{char} \mathbb{F}$ divides n then $V_0 \leq V^0$ (giving a representation of G on V^0/V_0).

In this example, the 1-dimensional modules V_0 and V/V^0 are both fixed by G. Every group has such a representation $g \mapsto I \in GL_1(\mathbb{F})$ for all $g \in G$; it is called the *principal representation*.

Maschke's Theorem divides the representation theory of finite groups into two areas: *ordinary* and *modular representation theory* study the cases where $\mathbb{F}$ and G do or do not satisfy the hypotheses of the theorem. The latter theory is usually harder (since extensions of G-modules need not split), but sometimes more effective, especially when dealing with properties of groups associated with a particular prime p, such as its Sylow p-subgroups, or its permutation representations of degrees divisible by p.

A simple argument, by induction on the dimension, using Maschke's Theorem, gives:

Theorem 6.2 *If G is a finite group and $\operatorname{char}\mathbb{F}$ is 0 or coprime to $|G|$, then every G-module (or representation of G) is a direct sum of irreducible G-submodules (or representations of G).* □

From now on we will take $\mathbb{F} = \mathbb{C}$. In addition to having characteristic 0, so that Maschke's Theorem applies to every finite group G, this field has the advantage that it is algebraically closed, so in particular it contains the eigenvalues of all elements of any finite group. (Actually, the field $\overline{\mathbb{Q}}$ of all algebraic numbers would do equally well.) Then one can prove:

Theorem 6.3 *The number of irreducible representations of G (up to G-isomorphism) is equal to the number k of conjugacy classes of G. Their degrees $n_1, \ldots, n_k$ all divide $|G|$, and satisfy*

$$n_1^2 + \cdots + n_k^2 = |G|.$$

Corollary 6.4 *If G is abelian then it has $|G|$ irreducible representations, all of them of degree* 1.

Proof. Since $k = |G|$ we have $n_i = 1$ for each $i = 1, \ldots, k$. □

Example 6.4 If $G = C_n = \langle a \mid a^n = 1\rangle$ there are n 1-dimensional irreducible representations; they are obtained by sending a to $(\zeta^j) \in GL_1(\mathbb{C})$ for $j = 0, 1, \ldots, n-1$, where $\zeta = \exp(2\pi i/n)$. The faithful representations are those with j coprime to n.

Exercise 6.2 Show that the number of 1-dimensional representations of a group G (all necessarily irreducible) is equal to the index $|G : G'|$ in G of its commutator subgroup $G' = [G, G]$.

If G is small, it is often easy to find all its irreducible representations.

Example 6.5 Let $G = A_4$. This has four conjugacy classes: the identity, the three double transpositions, and two mutually inverse classes of four 3-cycles (note that $(1, 2, 3)$ is conjugate to $(1, 3, 2)$ in S_4 but not in A_4). The first two classes form a normal Klein four-group V_4, with $G/V_4 \cong C_3$, so by composing the quotient map $G \mapsto G/V_4$ with the three 1-dimensional irreducible representations of C_3 (see Example 6.4) we obtain three non-faithful 1-dimensional irreducible representations of G. Now there are four conjugacy classes, so there should be a fourth irreducible representation of G, and since $|G| = 12$, Theorem 6.3 implies that it must have degree 3. There is a rather obvious 3-dimensional space for A_4 to act on, namely $\mathbb{R}^3$ (as the rotation group of a tetrahedron). This is not a complex representation, but we can regard the same matrices as acting on the larger space $\mathbb{C}^3 \supset \mathbb{R}^3$. (In more sophisticated language we are letting G act on the tensor product $\mathbb{R}^3 \otimes \mathbb{C}$.) If this representation were reducible it would be a direct sum of irreducible representations of lower degrees; but these all have V_4 in their kernel, whereas this representation is faithful, so it must be irreducible. (One can obtain an equivalent representation on the codimension 1 submodule V^0 of the natural permutation module $V = \mathbb{C}^4$; see Example 6.3.)

Exercise 6.3 Find all the irreducible representations over $\mathbb{C}$ of the dihedral groups $D_n = \langle a, b \mid a^n = b^2 = (ab)^2 = 1\rangle$. (Hint: consider n odd and n even separately, in that order.)

Knowing all the irreducible representations of G can mean storing and handling a massive amount of data. For instance, each n_i-dimensional representation requires n_i^2 matrix entries for each of the $|G|$ elements of G, giving a total of

$$\sum_{i=1}^{j} |G|n_i^2 = |G|^3$$

matrix entries, the same as the number of entries in the multiplication table of G. Fortunately, for most purposes it is sufficient to know just the traces of the matrices. (The *trace* $\operatorname{tr} M$ of a matrix M is the sum of its diagonal entries, equal to the sum of its eigenvalues, counting multiplicities.)

If ρ is a representation of G, its *character* $\chi = \chi_\rho$ is the function

$$G \to \mathbb{C}, \quad g \mapsto \operatorname{tr} \rho(g).$$

Conjugate matrices have the same eigenvalues, and hence the same trace, so this is independent of the choice of basis. This also shows that χ is a *class-function*, that is, it is constant on the conjugacy classes of G. Similarly, equivalent representations of G have the same character, and conversely:

Theorem 6.5 *Two representations of a finite group G are equivalent if and only if they have the same character.*

Thus, in order to understand the representation theory of a finite group G it is very helpful to know the values of its irreducible characters (those corresponding to its irreducible representations). These are encoded in the *character table* of G, a $k \times k$ array, with rows and columns indexed by the irreducible characters χ_i and the conjugacy classes $\mathcal{C}_j$ of G, and with entry $\chi_i(g_j)$ for $g_j \in \mathcal{C}_j$ in the ith row and jth column.

Example 6.6 Let $G = A_4$. In Example 6.5 we found the irreducible representations $\rho_1, \ldots, \rho_4$ of G. If $\mathcal{C}_1, \ldots, \mathcal{C}_4$ denote the classes containing the identity, the double transpositions and the 3-cycles (two classes), then the character table of A_4 is as follows, where $\zeta = \exp(2\pi i/3)$:

	$\mathcal{C}_1$	$\mathcal{C}_2$	$\mathcal{C}_3$	$\mathcal{C}_4$
χ_1	1	1	1	1
χ_2	1	1	ζ	$\overline{\zeta}$
χ_3	1	1	$\overline{\zeta}$	ζ
χ_4	3	-1	0	0

Exercise 6.4 Find the character tables for the dihedral groups D_n.

Exercise 6.5 How many irreducible representations does S_4 have, and what are their degrees? *Find these representations, and hence find the character table for S_4. (This last part will become easier after the next section.)

There are various *orthogonality relations* satisfied by character tables. I will just mention the orthonormality of the irreducible characters. For any two class functions $\phi, \psi : G \to \mathbb{C}$, define

$$(\phi, \psi) = \frac{1}{|G|} \sum_{g \in G} \phi(g)\overline{\psi(g)}.$$

Then it can be shown that the irreducible characters χ_i of G satisfy

$$(\chi_i, \chi_j) = \delta_{ij},$$

where δ_{ij} is the Kronecker delta, equal to 1 or 0 as $i = j$ or not.

Exercise 6.6 Show that a representation ρ of G is irreducible if and only if its character χ satisfies $(\chi, \chi) = 1$.

7 Representation theory and character theory for permutation groups

7.1 Characters of permutation groups

Let us represent a finite permutation group G of degree n on a set Ω by permutation matrices over an algebraically closed field $\mathbb{F}$ of characteristic 0, e.g. $\mathbb{C}$ or $\overline{\mathbb{Q}}$ (the field of algebraic numbers), giving a faithful representation

$$\rho : G \to GL(V) = GL_d(\mathbb{F}), \quad g \mapsto M(g)$$

where $M(g)$ is the permutation matrix representing g, and $V = \mathbb{F}^d$.

Adding diagonal entries of $M(g)$ ($= 1$ or 0, corresponding to points fixed or not fixed by g) gives the trace

$$\mathrm{tr}(M(g)) = \pi(g) := |\{\alpha \in \Omega \mid \alpha g = \alpha\}|,$$

so ρ has character $\chi_\rho = \pi$, called the *permutation character*. One can decompose π as

$$\pi = m_1\chi_1 + \cdots + m_k\chi_k$$

where $\chi_1, \ldots, \chi_k$ are the irreducible characters of G, with integer multiplicities $m_i \geq 0$. We will always take χ_1 to be the principal character $\chi_1(g) = 1$ for all $g \in G$, obtained from the principal representation $\rho_1 : G \to GL_1(\mathbb{C})$. Since $\chi_1, \ldots, \chi_k$ are orthonormal, the multiplicity of χ_1 in π is

$$m_1 = (\pi, \chi_1) = \frac{1}{|G|}\sum_{g \in G} \pi(g),$$

which is the number of orbits of G by Burnside's (or the Cauchy-Frobenius) Lemma.

Exercise 7.1 Use a double-counting argument to prove Burnside's Lemma, that the number of orbits of a permutation group is equal to the average number of fixed points of its elements.

In particular, for a transitive group G we have $m_1 = 1$, so

$$\pi = \chi_1 + m_2\chi_2 + \cdots + m_k\chi_k.$$

Similarly,

$$(\pi, \pi) = \frac{1}{|G|}\sum_{g \in G} \pi(g)\overline{\pi(g)} = \frac{1}{|G|}\sum_{g \in G} \pi(g)^2$$

(since $\pi(g) \in \mathbb{N} \subset \mathbb{R}$), with

$$\pi(g)^2 = |\{(\alpha, \beta) \in \Omega^2 \mid (\alpha, \beta)g = (\alpha, \beta)\},$$

so (π, π) is the number of orbits of G on Ω^2, that is, the rank of G. But the orthonormality of the characters χ_i gives

$$(\pi, \pi) = \sum_{i,j} m_i m_j (\chi_i, \chi_j) = \sum_{i,j} m_i m_j \delta_{ij} = \sum_i m_i^2,$$

so G has rank

$$r = \sum_{i=1}^{k} m_i^2.$$

For a transitive group we have $m_1 = 1$, so

$$r = 1 + \sum_{i=2}^{k} m_i^2.$$

Now a transitive group G is 2-transitive if and only if it has rank $r = 2$, so 2-transitivity is equivalent to

$$\pi = \chi_1 + \chi_i$$

for some non-principal irreducible character χ_i (afforded by the G-submodule V^0 of the permutation module V). To put this another way, if G is 2-transitive then the class function $\pi - \chi_1 = \pi - 1$ is a non-principal irreducible character of G. Similarly, for a transitive group of rank 3 we have $\pi = \chi_1 + \chi_i + \chi_j$ for some distinct irreducible characters χ_i and χ_j.

7.2 Application to S_4

Let us return to Exercise 6.5. The group $G = S_4$ has five conjugacy classes $\mathcal{C}_1, \ldots, \mathcal{C}_5$: these consist of the identity, the i-cycles for $i = 2, 3, 4$, and the double-transpositions, so there are five irreducible representations. Since $G' = A_4$, of index 2, two of these have degree $n_1 = n_2 = 1$. These are the principal representation $\rho_1 : g \mapsto (1)$ and the alternating representation $\rho_2 : g \mapsto (\mathrm{sgn}(g))$. Since $\sum n_i^2 = |G| = 24$ we have $n_3^2 + n_4^2 + n_5^2 = 22$ and hence $n_3 = 2$, $n_4 = n_5 = 3$. The epimorphism $S_4 \to S_3 \cong D_3$, composed with the 2-dimensional irreducible representation of D_3, gives a 2-dimensional irreducible representation ρ_3 of S_4 with kernel V_4. The action of S_4 as the rotation group of a cube, extended from $\mathbb{R}^3$ to $\mathbb{C}^3$, gives a 3-dimensional irreducible representation ρ_4. The natural permutation representation has dimension 4, and being doubly transitive it has an irreducible summand of dimension 3, giving an irreducible representation ρ_5 of degree $n_5 = 3$. This is not equivalent to ρ_4 since if g is a 4-cycle then $\chi_5(g) = -1$ whereas $\chi_4(g) = 1$. Calculating all traces (check this!), we find that the character table of S_4 is:

	$\mathcal{C}_1$	$\mathcal{C}_2$	$\mathcal{C}_3$	$\mathcal{C}_4$	$\mathcal{C}_5$
χ_1	1	1	1	1	1
χ_2	1	-1	1	-1	1
χ_3	2	0	-1	0	2
χ_4	3	-1	0	1	-1
χ_5	3	1	0	-1	-1

Exercise 7.2* In A_5, let $\mathcal{C}_1, \ldots, \mathcal{C}_5$ be the conjugacy classes consisting of the identity, the double transpositions, the 3-cycles, and the two classes of 5-cycles. Find the irreducible representations of A_5, and show that its character table is:

	$\mathcal{C}_1$	$\mathcal{C}_2$	$\mathcal{C}_3$	$\mathcal{C}_4$	$\mathcal{C}_5$
χ_1	1	1	1	1	1
χ_2	3	-1	0	ϕ	ψ
χ_3	3	-1	0	ψ	ϕ
χ_4	4	0	1	-1	-1
χ_5	5	1	-1	0	0

where $\phi, \psi = (1 \pm \sqrt{5})/2$. (Hint: A_5 is isomorphic to the rotation group of a icosahedron or dodecahedron, and also to $PSL_2(5)$.)

7.3 Application to groups of prime degree

If R is a regular permutation group, then $\pi(g) = 0$ for all $g \neq 1$ in R, and $\pi(g) = |R|$ for $g = 1$, so each irreducible character χ_i of R has multiplicity $m_i = (\pi, \chi_i) = \chi_i(1)$ in π, which is the degree n_i of χ_i; thus $\pi = \sum_i n_i \chi_i$. For instance, if R is abelian then each degree $n_i = 1$, so $\pi = \sum_i \chi_i$.

Here are some useful general results:

a) if a permutation group G has a regular abelian subgroup R, then the permutation character π of G is multiplicity-free (each multiplicity $m_i = 0$

or 1); this is because $\pi\mid_R$, the character of the regular representation of R, is multiplicity-free, as shown above.
b) characters of G which are conjugate under the Galois group of $\overline{\mathbb{Q}}$ have the same multiplicities in π; this is because π, taking integer values, is invariant under all field automorphisms.

From now on suppose that G is a transitive permutation group of prime degree p. Then p divides $|G|$, so by Cauchy's Theorem G has an element of order p. This must be a cycle of length p, so it generates a regular subgroup $P \cong C_p$. Hence π is multiplicity free.

Now $\pi\mid_P$ is the regular representation of P, the sum of all its irreducible representations since P is abelian. These are realised over the cyclotomic field of p-th roots of 1, and the non-principal characters are conjugate under the Galois group (isomorphic to C_{p-1}) of that field. it follows that the non-principal irreducible characters of G in π are also conjugate under this group, and in particular they have the same degrees.

Burnside used these ideas to prove the following (see [8, §3.5] for a later proof due to Schur):

Theorem 7.1 *If G is a transitive permutation group of prime degree p, then either $G \leq AGL_1(p)$ or G is 2-transitive.*

In the case $G \leq AGL_1(p)$ we have $G = C_p : C_m$ where m divides $p-1$. In the 2-transitive case, it follows from the classification of finite simple groups that G is one of the following

- $AGL_1(p)$ for a prime $p \geq 3$ (the only solvable examples);
- A_p or S_p for a prime $p \geq 5$;
- $PSL_2(11)$, M_{11} or M_{23} of degree $p = 11, 11$ or 23;
- a projective group with $PSL_d(q) \leq G \leq P\Gamma L_d(q)$, of prime degree $p = (q^d-1)/(q-1)$.

Here $PSL_2(11)$ acts on the cosets of a subgroup of index 11, isomorphic to A_5 (a fact already known to Galois!); the Mathieu groups M_{11} and M_{23} act on the points of their Steiner systems (see §5). Primes $p = (q^d-1)/(q-1)$ include the Mersenne primes of the form 2^d-1 with $q = 2$, the Fermat primes of the form 2^e+1 with $d = 2$ and $q = 2^e$, and others such as 13, with $q = d = 3$; it is unknown whether there are infinitely many of them.

Exercise 7.3 Prove that if $(q^d-1)/(q-1)$ is prime then d is prime.

8 The centraliser algebra

8.1 Definition and basic properties

Let (G, Ω) be a permutation group of degree n, and let $\mathbb{F}$ be any field. We define the *centraliser algebra* $\mathcal{V} = \mathcal{V}(G, \Omega)$ of (G, Ω) over $\mathbb{F}$ to be the set of all $n \times n$ matrices A over $\mathbb{F}$ such that $AM(g) = M(g)A$ for all $g \in G$, where $M(g)$ is the permutation matrix for g. Clearly $\mathcal{V}$ is closed under linear combinations and matrix products, so it is indeed an algebra over $\mathbb{F}$.

The permutation matrices $M(g)$ $(g \in G)$ act on the right and left of all $n \times n$ matrices over $\mathbb{F}$ by permuting rows and columns, giving an action $g : A \mapsto g^{-1}Ag$ of G, and a matrix A commutes with all such $M(g)$ if and only if it is fixed under this action, that is, its entries are constant on the orbits of G on Ω^2. It follows that $\mathcal{V}$ has a *standard basis* $A_1, \ldots, A_r$, where $r = |2\text{-orb}(G, \Omega)|$ is the rank of (G, Ω), and each A_i is the adjacency matrix $A(\Gamma_i)$ of the orbital graph $\Gamma_i = (\Omega, R_i)$ of an orbital $R_i \subset \Omega^2$ of G. I will generally assume that G is transitive on Ω, in which case it is conventional to take R_1 to be the diagonal of Ω^2, corresponding to the identity relation, so that A_1 is the $n \times n$ identity matrix $I = I_n$.

Notice that $\sum_i A_i = J$ (the $n \times n$ matrix with all entries equal to 1). Reflecting Ω^2 in the diagonal (i.e. taking transposes A^t of matrices A) sends orbitals of G to orbitals of G, so for each i there exists i' such that $A_i^t = A_{i'}$. We say that R_i is a *self-paired* orbital if $i' = i$ (so that Γ_i is undirected), otherwise R_i and $R_{i'}$ are *paired* orbitals (so that Γ_i and $\Gamma_{i'}$ are directed graphs, each the reverse of the other).

Since $\mathcal{V}$ is an algebra, each product of standard basis elements is a linear combination of standard basis elements. It follows that there are *structure constants* $p_{ij}^k \in \mathbb{F}$ defined by

$$A_i A_j = \sum_{k=1}^{r} p_{ij}^k A_k \quad (i, j \in \{1, \ldots, r\}).$$

These structure constants have a simple and very useful combinatorial interpretation. For any $\alpha, \beta \in \Omega$, the (α, β) entry of $A_i A_j$ is the number of directed walks $\alpha \to \gamma \to \beta$ of length 2 from α to β, with $(\alpha, \gamma) \in R_i$ and $(\gamma, \beta) \in R_j$. (Here we regard the undirected edges of a self-paired orbital graph as pairs of oppositely directed edges.) In particular, if we choose α and β so that $(\alpha, \beta) \in R_k$, then we see the following very interesting facts:

- p_{ij}^k is the number of such walks from α to β;
- p_{ij}^k is otherwise independent of this choice of α and β;
- p_{ij}^k is a non-negative integer.

Example 8.1 Let $G = D_5$ acting naturally on vertices of a pentagon, so $r = 3$. The orbitals are the sets R_1, R_2 and R_3 of pairs of vertices which are identical, adjacent or non-adjacent in the pentagon. Counting walks gives

$$A_2^2 = 2A_1 + A_3, \quad A_3^2 = 2A_1 + A_2 \quad \text{and} \quad A_2A_3 = A_3A_2 = A_2 + A_3.$$

(Of course, A_1 acts as the multiplicative identity.)

Example 8.2 Let $G = S_n$ acting on unordered pairs, so $r = 3$. The orbitals are the sets R_1, R_2 and R_3 of pairs (α, β) with $|\alpha \cap \beta| = 2, 1$ and 0. Then

$$A_2^2 = 2(n-2)A_1 + (n-2)A_2 + 4A_3.$$

Exercise 8.1 Verify this equation, and calculate the remaining structure constants in Example 8.2.

Exercise 8.2 Show that if all orbitals of (G, Ω) are self-paired, then $\mathcal{V}(G, \Omega)$ is commutative.

8.2 S-rings

Assume that G, acting with degree n on Ω, has a regular subgroup R. By identifying some arbitrary $\alpha \in \Omega$ with $1 \in R$ we can identify Ω with R, so that G acts on R (see §2.1). We can then identify $\mathbb{F}^n$ with the group algebra $\mathbb{F}R$. This is a vector space over $\mathbb{F}$ with basis R, so it is isomorphic to $\mathbb{F}^n$, but it is also a ring, with a product obtained by extending the group product in R by linearity, so it is an algebra over $\mathbb{F}$. The group G acts on $\mathbb{F}R$ by permuting its basis vectors (the elements of R), so the subgroup G_1 fixing 1 also acts on $\mathbb{F}R$. We define the *S-ring* $\mathcal{S} = \mathcal{S}(G, R)$ to be the subset of $\mathbb{F}R$ fixed by G_1. (S stands for Schur, who introduced this idea.) This is an r-dimensional linear subspace of $\mathbb{F}R$; it has a basis consisting of the sums B_i of the elements of R in the orbits Δ_i of G_1 on R corresponding to R_i, for $i = 1, \ldots, r$; what is really useful is that $\mathcal{S}(G, R)$ is also a subring of $\mathbb{F}R$, so it is an algebra over $\mathbb{F}$ (see [8, Lemma 3.5B]). Even better, we have:

Theorem 8.1 *There is an isomorphism $\mathcal{V}(G,\Omega) \to \mathcal{S}(G,R)$ of $\mathbb{F}$-algebras given by $A_i \mapsto B_i$.*

Proof. It is sufficient to check that

$$B_iB_j = \sum_k p_{ij}^k B_k \quad (i,j,k \in \{1,\dots,r\})$$

in $\mathbb{F}R$, that is, each element of the subset Δ_k of R arises p_{ij}^k times as a product of an element of Δ_i and an element of Δ_j. □

One advantage of this isomorphism is that the group structure of R makes calculations easier in $\mathcal{S}(G,R)$ than in $\mathcal{V}(G,\Omega)$. For instance, if G contains a regular abelian subgroup then $\mathcal{V}(G,\Omega)$ is commutative, since it is isomorphic to a subalgebra of $\mathbb{F}R$.

Example 8.3 Let $G = D_5 = \langle a, b \mid a^5 = b^2 = (ab)^2 = e\rangle$, acting naturally with degree $n = 5$, with a regular subgroup $R = C_5 = \langle a \rangle$. (I use e for the identity element of G to distinguish it from the element $1 \in \mathbb{F}$.) Then $B_1 = e$, $B_2 = a + a^{-1}$ and $B_3 = a^2 + a^{-2}$, and the structure constants are given by

$$\begin{aligned}
B_2^2 &= (a+a^{-1})(a+a^{-1}) = a^2 + 2e + a^{-2} = 2B_1 + B_3,\\
B_3^2 &= (a^2+a^{-2})(a^2+a^{-2}) = a^4 + 2e + a^{-4} = 2B_1 + B_2,\\
B_2B_3 = B_3B_2 &= (a+a^{-1})(a^2+a^{-2}) = a^3 + a + a^{-1} + a^{-3} = B_2 + B_3.
\end{aligned}$$

(Of course B_1, like A_1 in $\mathcal{V}(G,\Omega)$, acts as the multiplicative identity.) Notice the isomorphism $B_i \mapsto A_i$ between this example and Example 8.1.

The analogue of Theorem 3.3 about the connectivity of orbital graphs is that G acts primitively on Ω if and only if the support of each element of $\mathcal{S}(G,R)$ either generates R or is contained in $\{e\}$.

Exercise 8.3 Find the structure constants for $\mathcal{S}(G,R)$ where $G = D_6$ acting naturally, with $R = C_6$. Verify the above statement about supports and primitivity in this case.

Exercise 8.4* Find a non-abelian regular subgroup R' of D_6, and find the basis elements and structure constants for $\mathcal{S}(G,R')$.

Exercise 8.5* Let S_n act on unordered distinct pairs. For which $n = 3,\dots,8$ does it contain a regular subgroup? Show that if n is a prime power and $n \equiv 3$ mod (4) then there is a regular subgroup.

8.3 B-groups

A group H is called a *B-group* (after Burnside) if every primitive group G containing a regular subgroup $R \cong H$ is 2-transitive. Many finite groups are B-groups: for 'most' n the only primitive groups of degree n are the alternating and symmetric groups (see Theorem 4.7), and these are 2-transitive, so any group H of such an order n must be a B-group. To prove that a group H is not a B-group, it is sufficient to find a *simply primitive* group G (one which is primitive but not 2-transitive), with a regular subgroup $R \cong H$.

Example 8.4 If p is an odd prime then the group $H = C_p$ is not a B-group: its regular representation is simply primitive, so we can take $G = H$. (If $p > 3$ we could use D_p, and possibly other subgroups of $AGL_1(p)$.)

Exercise 8.6 Show that if H is an elementary abelian p-group of order $q = p^d$ for some odd prime p, then H is not a B-group.

Exercise 8.7* Show that if $H = H_1 \times \cdots \times H_d$ where $|H_1| = \ldots = |H_d| = c \geq 3$ and $d \geq 2$ then H is not a B-group. (This is a theorem of Dorothy Manning [16], giving counterexamples to a conjecture of Burnside that every abelian group which is not elementary abelian is a B-group; see [22, §25].)

Burnside [2] used character theory to show that if $n = p^e$ for some prime p and $e \geq 2$ then the cyclic group C_n is a B-group. Schur [17] used S-rings to extend this result to all composite degrees n. The proof is complicated, so here instead is a simple case:

Theorem 8.2 *If $n = 2p$ for some prime $p > 2$ then C_n is a B-group.*

Before proving this we need a very useful idea. It is convenient to choose $\mathbb{F}$ to have characteristic 0. If $B = \sum_{g \in R} a_g g \in \mathbb{F}R$ and $m \in \mathbb{Z}$ define

$$B^{(m)} = \sum_{g \in R} a_g g^m.$$

Lemma 8.3 *Let G contain a regular abelian subgroup R, let $\mathcal{S} = \mathcal{S}(G, R)$, and let m be coprime to the degree $n = |R|$ of G.*

(i) *If $B \in \mathcal{S}$ then $B^{(m)} \in \mathcal{S}$.*

(ii) *If B is a basis element of $\mathcal{S}$ then so is $B^{(m)}$.*

Proof. By taking linear combinations, it is sufficient to prove (i) when B is a basis element, so that

$$B = \sum_{g \in S} g$$

for some $S \subseteq R$. Since $B^{(mm')} = B^{(m)(m')}$ we may assume that m is prime. Now $\mathcal{S}$ contains

$$B^m = \Big(\sum_{g \in S} g\Big)^m,$$

and since R is abelian one can expand this by the multinomial theorem. Since m is prime, every multinomial coefficient

$$\binom{m}{a, b, \ldots, k} = \frac{m!}{a!b!\ldots k!} \qquad (a + b + \cdots + k = m)$$

is divisible by m, except for $\binom{m}{m} = 1$, so

$$B^m = \sum_{g \in S} g^m + C = B^{(m)} + C,$$

where all coefficients appearing in C are integers divisible by m. Now $g \mapsto g^m$ is an automorphism of R, so $B^{(m)}$ is a simple element of $\mathbb{F}R$. Writing B^m as a linear combination of basis elements of $\mathcal{S}$ and comparing coefficients, we see (this is the Schur-Wielandt principle) that $B^{(m)} \in \mathcal{S}$. Thus $B^{(m)}$ is a sum of basis elements, and applying the same argument to them, replacing m with its multiplicative inverse mod (n), shows that it is a single basis element. $\square$

Proof of Theorem 8.2. Suppose that G is a primitive group of degree $n = 2p$ containing a regular subgroup $R \cong C_n$, and G is not 2-transitive, so it has rank $r \geq 3$. We can write

$$R = \langle a \mid a^p = e\rangle \times \langle b \mid b^2 = e\rangle \cong C_p \times C_2,$$

so that a^i and $a^i b$ have order p and $2p$ for $i = 1, \ldots, p-1$. Let $\mathcal{S} = \mathcal{S}(G, R)$ and let B be the basis element containing the unique involution $b \in R$. Since b generates a proper subgroup of R, primitivity implies that B contains other elements a^i or $a^i b$ where $i = 1, \ldots, p-1$.

First suppose that $a^i b \in B$ for some $i = 1, \ldots, p-1$. Given any $j = 1, \ldots, p-1$, there is an integer m coprime to $2p$ such that $im \equiv j$ mod (p). By Lemma 8.1, $B^{(m)}$ is a basis element of $\mathcal{S}$. Since $B^{(m)}$ contains

$b^m = b$, this basis element is B; it also contains $(a^i b)^m = a^{im} b = a^j b$, so this shows that B contains $a^j b$ for all $j = 1, \ldots, p-1$. Since G has rank $r \geq 3$, the remaining non-trivial basis elements must consist of powers of a, contradicting primitivity.

It follows that B consists of b and certain non-identity powers of a, and a similar application of Lemma 8.1 shows that it contains all of them, so $B = \sum_{i=1}^{p-1} a^i + b$. Therefore $\mathcal{S}$ contains

$$B^2 = (p-2) \sum_{i=1}^{p-1} a^i + 2 \sum_{i=1}^{p-1} a^i b + pe.$$

But this is impossible, since the elements a^i and b of the basis element B have different coefficients ($p-2$ and 0) in this expression. $\square$

This is a very simple example of the sort of arguments which can be used to show that various groups are B-groups. They are much harder for non-abelian regular subgroups R, since Lemma 8.1 does not then apply.

Exercise 8.8* Show that if $n = pq$ for distinct primes p and q, then C_n is a B-group.

9 The Hamming and Johnson graphs, groups and schemes

9.1 The Hamming graphs, groups and schemes

Recall from Example 3.6 that the Hamming graph $H_d(c)$, for integers $c, d \geq 2$, has vertex set $\Omega = \mathbb{Z}_c^d$, with two vertices joined by an edge if and only if they differ in one coordinate. Thus there are c^d vertices, each of valency $(c-1)d$. The graph-theoretic distance of a vertex $\alpha = (a_1, \ldots, a_d)$ from the vertex $0 = (0, \ldots, 0)$ is equal to its *weight* $\mathrm{wt}\,\alpha$, the number of coordinates $a_i \neq 0$.

The wreath product $S_c \wr S_d$ acts on $H_d(c)$ as a group of automorphisms, transitive on the vertices: for $i = 1, \ldots, d$ the ith direct factor S_c in the normal subgroup $K = S_c^d$ permutes the values $a_i \in \mathbb{Z}_c$ of the coordinates in the ith coordinate position, while S_d acts on each vector by permuting its coordinates $a_1, \ldots, a_d$.

Lemma 9.1 $\mathrm{Aut}\, H_d(c) = S_c \wr S_d$.

Proof. Let $g \in G := \mathrm{Aut}\, H_d(c)$. It is sufficient to show that $g \in W := S_c \wr S_d$. The idea is to continue composing g with elements of W until the resulting product gw ($w \in W$) fixes every vertex, and is therefore the identity, so that $g = w^{-1} \in W$.

By composing g with a suitable element of the subgroup S_c^d of W we may assume that g fixes the vertex 0. The neighbours of 0 form d mutually non-adjacent cliques (complete graphs K_{c-1}); these are permuted by g, and by composing g with an element of the subgroup S_d of W we may assume that g leaves these invariant. By composing g again with an element of S_c^d fixing the vertex 0, we may assume that g fixes each of these cliques, so that it fixes all the vertices of weight 1. Now each vertex of weight 2 has two neighbours of weight 1, and is their unique common neighbour of weight 2, so it must also be fixed by g. Continuing this type of argument through successive weights $3, 4, \ldots, d$, we find that g fixes every vertex, so g is the identity. $\square$

Exercise 9.1 Explain more carefully what is meant by 'Continuing this type of argument ...'.

The group $G = \mathrm{Aut}\, H_d(c) = S_c \wr S_d$ has rank $d+1$: the orbits of G_0 are the sets Δ_i of vectors of weight i for $i = 0, \ldots, d$, with $|\Delta_i| = \binom{d}{i}(c-1)^i$ since there are $\binom{d}{i}$ choices for which i coordinates are to be non-zero, and $c-1$ non-zero values for each of them. This is therefore the valency of the orbital graph Γ_i, in which two vertices are adjacent if and only if they differ in exactly i coordinate places, so that they have Hamming distance i. This is a symmetric relation, so each Γ_i is an undirected graph: it is in fact the distance i graph of $H_d(c)$.

The adjacency matrices A_i ($i = 0, \ldots, d$) are the basis elements of the centraliser algebra $\mathcal{V}(G, \Omega)$, called the *Hamming scheme*. To compute its structure constants p_{ij}^k, for $i, j, k \in \{0, 1, \ldots, d\}$, one has to take two vertices α and β which are distance k apart, and count how many vertices γ are at distance i from α and distance j from β. Without loss of generality one can take $\alpha = (0, \ldots, 0)$ and $\beta = (1, \ldots, 1, 0, \ldots, 0)$, where β has k entries equal to 1. The counting is easy when d is small:

Example 9.1 Let $d = 2$, so $r = 3$ with $|\Delta_1| = 2(c-1)$ and $|\Delta_2| = (c-1)^2$. Let us calculate p_{22}^1, the coefficient of A_1 in A_2^2. Since $k = 1$ we take $\alpha = (0,0)$ and $\beta = (1,0)$. Then $\gamma = (c_1, c_2)$ is distance $i = 2$ from α if and only if $c_1, c_2 \neq 0$, and it is distance $j = 2$ from β if and only if $c_1 \neq 1$ and $c_2 \neq 0$. Thus we can have $c_1 = 2, 3, \ldots c-1$ (giving $c-2$ possibilities), and $c_2 = 1, 2, \ldots c-1$

(giving $c-1$ possibilities), so $p^1_{22} = (c-1)(c-2)$. The remaining coefficients p^k_{ij} can be found by similar arguments, giving

$$A_1^2 = 2(c-1)A_0 + (c-2)A_1 + 2A_2,$$

$$A_2^2 = (c-1)^2 A_0 + (c-1)(c-2)A_1 + (c-2)^2 A_2,$$

$$A_1 A_2 = A_2 A_1 = (c-1)A_1 + 2(c-2)A_2.$$

Exercise 9.2 Verify the above equations.

Exercise 9.3 Find the corresponding equations when $d = 3$.

The calculations become more laborious as d increases, and it is better to look for general formulae, valid for all d. The vertices $\gamma = (c_1, \ldots, c_d)$ at distance i from α are those of weight i, with i coordinates $c_i \neq 0$. Such a vertex has distance j from β if and only if, for some integer s, there are $j - s$ coefficients $c_1, \ldots, c_k$ distinct from 1, and s coefficients $c_{k+1}, \ldots, c_d$ distinct from 0. This is equivalent to the following

- $c_1, \ldots, c_k$ have exactly $k - i + s$ terms equal to 0,
- $c_1, \ldots, c_k$ have exactly $k - j + s$ terms equal to 1,
- $c_1, \ldots, c_k$ have exactly $i + j - k - 2s$ terms not equal to 0 or 1,
- $c_{k+1}, \ldots, c_d$ have exactly $d - k - s$ terms equal to 0,
- $c_{k+1}, \ldots, c_d$ have exactly s terms not equal to 0.

For each s, the number of ways of partitioning $c_1, \ldots, c_k$ into these three sets, taking values $0, 1$ and all other values, is given by the trinomial coefficient

$$\binom{k}{k-i+s,\, k-j+s,\, i+j-k-2s} = \frac{k!}{(k-i+s)!(k-j+s)!(i+j-k-s)!},$$

while the number of ways of partitioning $c_{k+1}, \ldots, c_d$ into two sets, with values 0 and all others, is given by the binomial coefficient

$$\binom{d-k}{d-k-s,\, s} = \frac{(d-k)!}{(d-k-s)!s!},$$

so the total number of partitions of $c_1, \ldots, c_d$ is

$$\binom{k}{k-i+s, k-j+s, i+j-k-2s}\binom{d-k}{d-k-s, s}.$$

For each partition there are

$$(c-2)^{i+j-k-2s}(c-1)^s$$

free choices for the coefficients, so the number of possibilities for a given s is

$$\binom{k}{k-i+s, k-j+s, i+j-k-2s}\binom{d-k}{d-k-s, s}(c-2)^{i+j-k-2s}(c-1)^s.$$

Summing this expression over all possible values of s gives p_{ij}^k.

Exercise 9.4 Show that the range of possible values of s is

$$s_* := \max(0, i-k, j-k) \leq s \leq s^* = \min(d-k, i, j, \frac{1}{2}(i+j-k)).$$

If $s_* > s^*$ then no such vertex γ exists and we have $p_{ij}^k = 0$.

Exercise 9.5 Show that if p_{ij}^k is not identically zero then it is a polynomial in c, of degree j, i or $i+j-k$ as $\max(i,j,k) = i, j$ or k.

These structure constants were used by Soomro and the author in [13] to show that, for fixed $d \geq 2$, the group $G = S_c \wr S_d$ is a maximal subgroup of A_n or S_n, where $n = c^d$, for all sufficiently large c (depending on d). A contribution to that paper by Peter Neumann verified the conjecture of the authors that this is in fact true for all $c \geq 5$, independent of d. (If $c \leq 4$ then S_c is solvable, with a regular normal subgroup, and it follows that G is a proper subgroup of an affine group).

In modern terminology, the structure constants were used to eliminate mergings of the Hamming scheme which might correspond to simply transitive groups $G^* > G$, while doubly transitive groups $G^* > G$ were eliminated by a theorem of Bochert (see [22, §15]) that a doubly transitive group, which does not contain the alternating group, cannot have non-identity elements with a large number of fixed points. Neumann's contribution used different methods, based on the analysis of minimal normal subgroups outlined in §4. Soon afterwards, Liebeck, Praeger and Saxl [15] gave a complete classification of the maximal subgroups of the alternating and symmetric groups.

Exercise 9.6 When is $S_c \wr S_d$, in its product action, a subgroup of the alternating group A_n ($n = c^d$)?

9.2 The Johnson graphs, groups and schemes

One can view the family of Hamming graphs, with their corresponding groups and association schemes, as being based on the set of ordered d-tuples from a c-element set. By replacing these with *unordered* d-tuples, that is, with d-element subsets, we obtain the family of Johnson graphs, groups and schemes.

Let $G = S_c$, acting naturally with degree $\binom{c}{d}$ on the set Ω of d-element subsets α of $\mathbb{Z}_c$ where $c \geq 2d$. Then the rank is $r = d + 1$, and the orbitals of G are the sets

$$R_i = \{(\alpha, \beta) \in \Omega^2 \mid |\alpha \cap \beta| = d - i\} \quad (i = 0, \ldots, d).$$

The *Johnson graph* $J_d(c)$ is the orbital graph $\Gamma_1 = (\Omega, R_1)$ (which is undirected), and the remaining orbital graphs Γ_i are its distance i graphs.

Exercise 9.7* Show that $\operatorname{Aut}\Gamma_1 = G$ if $c > 2d$. What happens if $c = 2d$?

An analysis similar to that for the Hamming graphs shows that the structure constants are given as sums of products of binomial coefficients:

$$p_{ij}^k = \sum_{s=s_*}^{s^*} \binom{d-k}{s} \binom{k}{d-i-s} \binom{k}{d-j-s} \binom{c-d-k}{s+i+j-d}$$

where

$$s_* = \max(0, d-i-j, d-j-k, d-k-i)$$

and

$$s^* = \min(d-i, d-j, d-k, c-i-j-k).$$

Exercise 9.8* Verify the above formula for p_{ij}^k.

For fixed d, each p_{ij}^k is a polynomial in c, a fact used by Kalužnin and Klin [14] to show that if c is sufficiently large (depending on d) then S_c, in its action on Ω, is a maximal subgroup of A_n or S_n where $n = \binom{c}{d}$.

Exercise 9.9 When is S_c, in its action on d-element subsets, a subgroup of A_n ($n = \binom{c}{d}$)?

Exercise 9.10 Show that if $c = 2d$ then S_c, in its action on d-element subsets, is not a maximal subgroup of A_n or S_n.

10 Permutation groups and maps

In this section I will describe an important class of permutation groups called Frobenius groups, and I will show how they have been used to solve a problem concerning maps on surfaces.

10.1 Frobenius groups

A permutation group G, acting on Ω, is called a *Frobenius group* if it is transitive and $G_{\alpha,\beta} = 1$ for all $\alpha \neq \beta$ in Ω; to avoid trivial cases, we also require that G does not act regularly, that is, $G_\alpha \neq 1$.

Example 10.1 The simplest example of a Frobenius group is $G = D_n$, acting naturally with odd degree n. (Why not even n?)

Example 10.2 Another example of a Frobenius group is $G = AGL_1(q)$, acting naturally on $\Omega = \mathbb{F}_q$, where $q > 2$. (Why not $q = 2$?)

Example 10.3 More generally, one could take $G = V : G_0 \leq AGL(V)$ with G_0 ($\neq 1$) a subgroup of $GL(V)$ acting semi-regularly on $V \setminus \{0\}$. For a specific example, it is known that $PSL_2(p)$ has subgroups $A \cong A_5 \cong PSL_2(5)$ for each prime $p \equiv \pm 1$ mod (5); these lift to subgroups $B \cong SL_2(5)$ (the binary icosahedral group) in $SL_2(p)$; now $SL_2(5)$ is perfect, so B fixes no non-zero vectors in its natural action on $V = \mathbb{F}_p^2$, and hence the subgroup $G = V : B$ of $AGL_2(p)$ acts on V as a Frobenius group (sharply 2-transitive if $p = 11$).

Exercise 10.1 Prove that in Example 10.1, B fixes no non-zero vectors.

If G is a Frobenius group of degree n on Ω then $G_\alpha \cap G_\beta = 1$ for all $\alpha \neq \beta$ in Ω. It follows that there are $1 + n(|G_\alpha| - 1) = |G| - (n-1)$ elements of G (including the identity) with fixed points in Ω, so there are $n - 1$ elements with no fixed points. These, together with the identity, form a normal subset N of order n in G. What is less obvious is that N is a normal *subgroup* of G. (The proof, due to Frobenius, uses character theory to construct a representation of G with kernel N.) This subgroup is called the *Frobenius kernel* of G; any point-stabiliser G_α is called a *Frobenius complement*, since $G = NG_\alpha$ with $N \cap G_\alpha = 1$. This shows that N acts regularly on Ω. Thus G has a regular normal subgroup N, so $G \leq \operatorname{Hol} N$ (see Example 2.4).

A deep theorem of Thompson [20] shows that N is nilpotent, so it is a direct product of its Sylow p-subgroups for the different primes p dividing N. In particular, if G is primitive then N must be characteristically simple (see

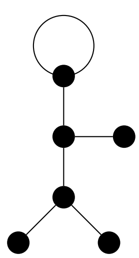
§4.1, §4.2), and so must be an elementary abelian p-group for some prime p, so that $G \leq AGL_d(p)$ where $n = p^d$. The structure of a Frobenius complement is also restricted: its Sylow p-subgroups are cyclic for odd primes p, while the Sylow 2-subgroups are cyclic or quaternion groups; also, G_α has at most one non-abelian composition factor, isomorphic to A_5, as in Example 10.2 with $B/Z(B) \cong A \cong A_5$. (See [8, §3.4] for more details and proofs.)

10.2 Maps

A *map* $\mathcal{M}$ is an embedding of a connected graph $\mathcal{G}$ in a surface $\mathcal{S}$ such that the faces (connected components of $\mathcal{S} \setminus \mathcal{G}$) are simply connected (homeomorphic to discs). For simplicity I will assume that $\mathcal{G}$ is finite, and that $\mathcal{S}$ is compact, connected, oriented and without boundary.

Example 10.4 The regular solids can be regarded as maps on the sphere.

Using an idea that goes back to Hamilton (1856), a map $\mathcal{M}$ can be defined by a pair of permutations x, y of the set Ω of arcs (directed edges, sometimes called darts) of $\mathcal{M}$: the permutation x rotates arcs around the vertex to which they point, using the local orientation to send each arc to the next one, while y is the involution which reverses the direction of each arc. (Note that x and y are not, in general, automorphisms of $\mathcal{M}$, since they do not preserve incidence.) By connectedness, the subgroup $G = \langle x, y \rangle$ of $\mathrm{Sym}\,\Omega$ which they generate is transitive. The vertices, edges and faces of $\mathcal{M}$ correspond to the cycles x, y and of $z := (xy)^{-1}$ on Ω (check that z follows the orientation around faces). Conversely, any transitive group with generators x and y satisfying $y^2 = 1$ determines a map (in fact, on a Riemann surface defined over an algebraic number field: see [12] for example).



Émile Léonard Mathieu, 1835–1890.

Figure 1: Monsieur Mathieu

Example 10.5 In Figure 1, drawn on the sphere, $|\Omega| = 12$ and $G = \langle x, y\rangle$ is the Mathieu group $M_{12} < S_{12}$, a sporadic simple group of order 95040, isomorphic to $\mathrm{Aut}\,\mathcal{S}(5, 6, 12)$.

Exercise 10.2 Use GAP (or any other computational tool) to verify that $G = M_{12}$ in Example 10.5.

Two maps, corresponding to groups $G = \langle x, y\rangle$ and $G' = \langle x', y'\rangle$, are isomorphic if and only if there is an isomorphism $G \to G'$ taking x to x' and y to y', or equivalently some element of $\mathrm{Sym}\,\Omega$ conjugates x to x', and y to y'. The automorphism group (preserving orientation) A of $\mathcal{M}$ is the group of all $g \in \mathrm{Sym}\,\Omega$ commuting with x and y, that is, A is the centraliser $C(G)$ of G in $\mathrm{Sym}\,\Omega$. Since A commutes with the transitive group G it acts semi-regularly on Ω.

The most symmetric maps are the *regular* maps, those for which A acts transitively (and hence regularly) on arcs. In this case G also acts regularly, so A and G are the left and right regular representations of the same group (see §2.1, especially Exercise 2.6).

Example 10.6 The regular solids are regular maps on the sphere, with orientation-preserving automorphism groups $A \cong A_4$ (for the tetrahedron), S_4 (for the cube and the octahedron) and A_5 (for the dodecahedron and the icosahedron).

10.3 Regular embeddings of complete graphs

A major problem in the theory of maps is to classify all the regular embeddings of a given class of graphs. These graphs must be arc-transitive in order to have such embeddings, so the complete graphs K_n are obvious candidates.

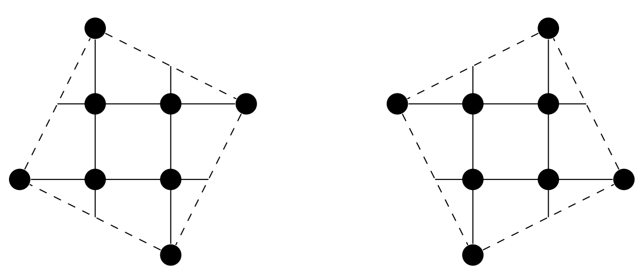


Figure 2: Two regular torus embeddings of K_5

Example 10.7 Figure 2 shows two regular embeddings of K_5, mirror images of each other; in each case, opposete sides of the outer square are identified to form a torus. They both have

$$G \cong A \cong AGL_1(5) \cong C_5 : C_4.$$

Exercise 10.3 For each map in Figure 2, label the vertices with the elements of $\mathbb{F}_5$ so that the automorphism group acts on the labels as $AGL_1(5)$.

It is known that regular embeddings of K_n exist for $n = 1, 2, 3, 4$ (on the sphere), $5, 7$ (on the torus), 8 (on a surface of genus 7), 9 (genus 10), and so on, but not for $n = 6$ or 10. Here is the explanation:

Theorem 10.1 (Biggs [1]) *The complete graph K_n has a regular embedding if and only if n is a prime power.*

Outline proof. If n is a prime power, construct a map $\mathcal{M}$ by taking the vertex-set to be $\mathbb{F}_n$, choosing a generator ζ for the multiplicative group $\mathbb{F}_n^* \cong C_{n-1}$, and joining each vertex v to its neighbours $v+1, v+\zeta, v+\zeta^2, \ldots, v+\zeta^{n-2}$, with that cyclic order defining the orientation of the surface around v (this is an example of the Cayley map construction). One can check that the embedded graph is isomorphic to K_n, and that the automorphism group is isomorphic to $AGL_1(n)$, acting sharply 2-transitively on the vertices and hence regularly on the arcs.

Conversely, if $\mathcal{M}$ is a regular embedding of K_n then its automorphism group A must act regularly on the arcs, and hence sharply 2-transitively on the vertices. Thus A acts on the vertices as a primitive Frobenius group, so the degree n is a prime power (see §10.1). $\square$

Corollary 10.2 (James and Jones [11]) *For each prime power $n = p^e$, the complete graph K_n has $\phi(n-1)/e$ regular embeddings, up to orientation-preserving isomorphism, where ϕ is Euler's totient function.*

Outline proof. As above, the automorphism group A of a regular embedding of K_n ($n = p^e$) acts on the vertices as a sharply 2-transitive finite group. Such groups were classified by Zassenhaus [25] in 1936: they are all 1-dimensional affine groups over near-fields (generalisations of fields), see [8, §7.6]. In our case the stabiliser of a vertex v is cyclic (consisting of rotations around v), and the groups in Zassenhaus's list with this property are the affine groups

$AGL_1(n)$ over finite fields $\mathbb{F}_n$. One now checks that the group $A = AGL_1(n)$ has $\phi(n-1)n(n-1)$ generating pairs x, y with $y^2 = 1$, leading to regular embeddings of K_n. Since the group $\mathrm{Aut}\, A = A\Gamma L_1(n)$, of order $en(n-1)$, permutes these pairs semi-regularly (why?), it has $\phi(n-1)/e$ orbits on them, so this is the number of isomorphism classes of regular embeddings. $\square$

In fact, the full proof shows that the regular embeddings of K_n are those constructed by Biggs: $\phi(n-1)$ is the number of different choices for the generator ζ of the cyclic group $\mathbb{F}_n^* \cong C_{n-1}$; two of these determine isomorphic maps if and only if they are conjugate under the Galois group of $\mathbb{F}_n$, a cyclic group of order e generated by the Frobenius automrphism $t \mapsto t^p$; this group acts semi-regularly on generators ζ, so dividing by e gives the number of its orbits and hence the number of Biggs maps.

Example 10.8 Let $n = 5$. Then $\phi(n-1) = \phi(4) = 2$, and $e = 1$, so there are two regular embeddings of K_5. These are the maps shown in Figure 2, and if your solution to Exercise 10.3 is correct, they should correspond to the two generators of the multiplicative group $\mathbb{F}_5^*$.

References

[1] N. L. Biggs, Automorphisms of imbedded graphs, *J. Combin. Theory Ser. B* 11 (1971), 132–138.

[2] W. Burnside, *Theory of Groups of Finite Order* (2nd ed.), Cambridge University Press, 1911; reprinted Dover, 1955.

[3] P. J. Cameron, *Permutation Groups*, London Mathematical Society Student Texts 45, Cambridge University Press, 1999.

[4] P. J. Cameron, P. M. Neumann and D. N. Teague, On the degrees of primitive permutation groups, *Math. Z.* 180 (1982), 141–149.

[5] J. H. Conway, R. T. Curtis, S. P. Norton, R. A. Parker and R. A. Wilson, *ATLAS of Finite Groups*, Clarendon Press, Oxford, 1985.

[6] C. W. Curtis and I. Reiner, *Representation Theory of Finite Groups and Associative Algebras*, Wiley, New York, 1962.

[7] J. D. Dixon, The probability of generating the symmetric group, *Math. Z.* 110 (1969), 199–205.

[8] J. D. Dixon and B. Mortimer, *Permutation Groups*, Graduate Texts in Mathematics 163, Springer, 1996.

[9] W. Fulton and J. Harris, *Representation Theory: a First Course*, Springer, 2004.

[10] D. G. Higman, Intersection matrices for finite permutation groups, *J. Algebra* 6 (1967), 22–42.

[11] L. D. James and G. A. Jones, Regular orientable imbeddings of complete graphs, *J. Combin. Theory Ser. B* 39 (1985), 353–367.

[12] G. A. Jones and D. Singerman, Belyi functions, hypermaps and Galois groups, *Bull. London Math. Soc.* 28 (1996) 561–590.

[13] G. A. Jones and K. D. Soomro, The maximality of certain wreath products in alternating and symmetric groups, *Quart. J. Math'Oxford* (2) 37 (1986), 419–435.

[14] L. A. Kalužnin and M. H. Klin, On certain maximal subgroups of symmetric and alternating groups, *Mat. Sbornik* 87 (129) (1972), 91–121 (Russian); *Math. USSR Sbornik* 16 (1972), 95–123 (English transl.).

[15] M. W. Liebeck, C. E. Praeger and J. Saxl, The classification of the maximal subgroups of the finite alternating and symmetric groups, *J. Algebra* 111 (1987), 365–383.

[16] D. Manning, On simply transitive groups with transitive abelian subgroups of the same degree, *Trans. Amer. Math. Soc.* 40 (1936), 324–342.

[17] I. Schur, Zur Theorie der einfach transitiven Permutationsgruppen *S. B. Preuss. Akad. Wiss., Phys.-Math. Kl.* 1933 (1933), 598–623.

[18] J-P. Serre, *Linear Representations of Finite Groups*, Springer, 1977.

[19] C. C. Sims, Graphs and permutation groups, *Math. Z.* 95 (1967), 76–86.

[20] J. G. Thompson, Finite groups with fixed point free automorphisms of prime order, *Proc. Nat. Acad. Sci. USA* 45 (1959), 578–581.

[21] H. Whitney, Congruent graphs and the connectivity of graphs, *Amer. J. Math.* 54 (1932),150–168.

[22] H. Wielandt, *Finite Permutation Groups*, Academic Press, New York, 1964.

[23] H. Wielandt, *Permutation Groups through Invariant Relations and Invariant Functions*, lecture notes, Ohio State Univ., Columbus, Ohio, 1969.

[24] R. A. Wilson, *The Finite Simple Groups*, Springer, 2009.

[25] H. Zassenhaus, Über endliche Fastkörper, *Abh. Math. Sem. Univ. Hamburg* 11 (1936), 187–220.