Finite permutation groups: the landscape post-CFSG

Peter J. Cameron
University of St Andrews

GRAW01, 9 January 2020

What is a group?

I have always thought that groups were given to us to act on something.

What is a group?

I have always thought that groups were given to us to act on something.
Over the course of history, a group has been:

What is a group?

I have always thought that groups were given to us to act on something.

Over the course of history, a group has been:

- a symmetry group, the collection of all symmetries of something;

What is a group?

I have always thought that groups were given to us to act on something.
Over the course of history, a group has been:

- a symmetry group, the collection of all symmetries of something;
- a permutation group, a set of permutations of a set Ω closed under composition and inversion and containing the identity;

What is a group?

I have always thought that groups were given to us to act on something.
Over the course of history, a group has been:

- a symmetry group, the collection of all symmetries of something;
- a permutation group, a set of permutations of a set Ω closed under composition and inversion and containing the identity;
- an abstract group, a set G with a binary operation satisfying the (now-standard) group axioms.

What is a group?

I have always thought that groups were given to us to act on something.

Over the course of history, a group has been:

- a symmetry group, the collection of all symmetries of something;
- a permutation group, a set of permutations of a set Ω closed under composition and inversion and containing the identity;
- an abstract group, a set G with a binary operation satisfying the (now-standard) group axioms.

At each stage it was necessary to show that the same class of objects is being considered: for example, every permutation group is the group of symmetries of something, and any abstract group is isomorphic to a permutation group (Cayley's Theorem).

Permutation groups and group actions

A permutation group is a subgroup of the symmetric group $\mathrm{Sym}(\Omega)$ on some set Ω.

Permutation groups and group actions

A permutation group is a subgroup of the symmetric group $\mathrm{Sym}(\Omega)$ on some set Ω.
An action of a group G is a homomorphism from G to the symmetric group $\mathrm{Sym}(\Omega)$.

Permutation groups and group actions

A permutation group is a subgroup of the symmetric group $\mathrm{Sym}(\Omega)$ on some set Ω.

An action of a group G is a homomorphism from G to the symmetric group $\mathrm{Sym}(\Omega)$.

If we understand the abstract structure of a group, we can describe its actions. Conversely, if we know enough about some or all the actions of a group, we can deduce information about its structure.

Permutation groups and group actions

A permutation group is a subgroup of the symmetric group $\mathrm{Sym}(\Omega)$ on some set Ω.

An action of a group G is a homomorphism from G to the symmetric group $\mathrm{Sym}(\Omega)$.

If we understand the abstract structure of a group, we can describe its actions. Conversely, if we know enough about some or all the actions of a group, we can deduce information about its structure.

For the most part, I will consider permutation groups.

Permutation groups and group actions

A permutation group is a subgroup of the symmetric group $\mathrm{Sym}(\Omega)$ on some set Ω.

An action of a group G is a homomorphism from G to the symmetric group $\mathrm{Sym}(\Omega)$.

If we understand the abstract structure of a group, we can describe its actions. Conversely, if we know enough about some or all the actions of a group, we can deduce information about its structure.

For the most part, I will consider permutation groups.

The number $n = |\Omega|$ is the degree of the permutation group G.

I usually assume that it is finite.

Permutation group properties

In any kind of representation of a group, we consider reduction to simpler representations, and the reverse problem of building arbitrary representations from simpler ones.

Permutation group properties

In any kind of representation of a group, we consider reduction to simpler representations, and the reverse problem of building arbitrary representations from simpler ones.
For permutation groups, most of the properties used in this way can be given a uniform definition.

Permutation group properties

In any kind of representation of a group, we consider reduction to simpler representations, and the reverse problem of building arbitrary representations from simpler ones.
For permutation groups, most of the properties used in this way can be given a uniform definition.
A structure of any kind on Ω (graph, order, first-order structure, topological space, or whatever) will be called trivial if it is preserved by the symmetric group $\mathrm{Sym}(\Omega)$, and non-trivial otherwise.

Permutation group properties

In any kind of representation of a group, we consider reduction to simpler representations, and the reverse problem of building arbitrary representations from simpler ones.

For permutation groups, most of the properties used in this way can be given a uniform definition.

A structure of any kind on Ω (graph, order, first-order structure, topological space, or whatever) will be called trivial if it is preserved by the symmetric group $\mathrm{Sym}(\Omega)$, and non-trivial otherwise.

For example,

Permutation group properties

In any kind of representation of a group, we consider reduction to simpler representations, and the reverse problem of building arbitrary representations from simpler ones.
For permutation groups, most of the properties used in this way can be given a uniform definition.
A structure of any kind on Ω (graph, order, first-order structure, topological space, or whatever) will be called trivial if it is preserved by the symmetric group $\mathrm{Sym}(\Omega)$, and non-trivial otherwise.
For example,

- the trivial subsets of Ω are the empty set and Ω;

Permutation group properties

In any kind of representation of a group, we consider reduction to simpler representations, and the reverse problem of building arbitrary representations from simpler ones.
For permutation groups, most of the properties used in this way can be given a uniform definition.
A structure of any kind on Ω (graph, order, first-order structure, topological space, or whatever) will be called trivial if it is preserved by the symmetric group $\mathrm{Sym}(\Omega)$, and non-trivial otherwise.
For example,

- the trivial subsets of Ω are the empty set and Ω;
- the trivial graphs on Ω are the null graph (with no edges) and the complete graph (in which every pair of points forms an edge).

Transitivity

This is the prototype for the way permutation group properties will be introduced.

Transitivity

This is the prototype for the way permutation group properties will be introduced.

The permutation group G on Ω is transitive if it preserves no non-trivial subset of Ω.

Transitivity

This is the prototype for the way permutation group properties will be introduced.

The permutation group G on Ω is transitive if it preserves no non-trivial subset of Ω.

Thus, if G is transitive and $\alpha, \beta \in \Omega$, the only G-invariant subset containing α is the whole of Ω, which also contains β; so there is an element $g \in G$ mapping α to β. (This is the classical definition of transitivity.)

Theorems of Jordan and Fein–Kantor–Schacher

A derangement is a permutation with no fixed points.

Theorems of Jordan and Fein–Kantor–Schacher

A derangement is a permutation with no fixed points.

Theorem

Let G be a transitive permutation group of degree $n > 1$.

- *G contains a derangement.*

Theorems of Jordan and Fein–Kantor–Schacher

A derangement is a permutation with no fixed points.

Theorem

Let G be a transitive permutation group of degree $n > 1$.

- *G contains a derangement.*
- *G contains a derangement of prime power order.*

Theorems of Jordan and Fein–Kantor–Schacher

A derangement is a permutation with no fixed points.

Theorem

Let G be a transitive permutation group of degree $n > 1$.

- *G contains a derangement.*
- *G contains a derangement of prime power order.*

The first part, due to Jordan, is elementary: by the Orbit-Counting Lemma, the average number of fixed points of elements of G is 1, and the identity fixes more than 1. See Serre's beautiful paper "On a theorem of Jordan".

Theorems of Jordan and Fein–Kantor–Schacher

A derangement is a permutation with no fixed points.

Theorem

Let G be a transitive permutation group of degree $n > 1$.

- *G contains a derangement.*
- *G contains a derangement of prime power order.*

The first part, due to Jordan, is elementary: by the Orbit-Counting Lemma, the average number of fixed points of elements of G is 1, and the identity fixes more than 1. See Serre's beautiful paper "On a theorem of Jordan".

The second part, due to Fein, Kantor and Schacher, requires the Classification of Finite Simple Groups, together with detailed analysis of all the simple groups. Moreover, it was needed for a result in number theory (on relative Brauer groups of global field extensions).

Theorems of Jordan and Fein–Kantor–Schacher

A derangement is a permutation with no fixed points.

Theorem

Let G be a transitive permutation group of degree $n > 1$.

- *G contains a derangement.*
- *G contains a derangement of prime power order.*

The first part, due to Jordan, is elementary: by the Orbit-Counting Lemma, the average number of fixed points of elements of G is 1, and the identity fixes more than 1. See Serre's beautiful paper "On a theorem of Jordan".

The second part, due to Fein, Kantor and Schacher, requires the Classification of Finite Simple Groups, together with detailed analysis of all the simple groups. Moreover, it was needed for a result in number theory (on relative Brauer groups of global field extensions).

Problem

Is there a more elementary proof of the FKS theorem?

Intransitive groups

The minimal non-empty G-invariant subsets of Ω are called orbits. The argument above shows that, if two points belong to the same orbit, then there is an element of G mapping one to the other; so G has an action on each orbit, and this action is transitive.

Intransitive groups

The minimal non-empty G-invariant subsets of Ω are called orbits. The argument above shows that, if two points belong to the same orbit, then there is an element of G mapping one to the other; so G has an action on each orbit, and this action is transitive.

If G^Δ is the permutation group induced on the orbit Δ by G, then G is not uniquely determined by the transitive constituents G^Δ, but it can be shown that it is a subdirect product of these (smaller) permutation groups.

Intransitive groups

The minimal non-empty G-invariant subsets of Ω are called orbits. The argument above shows that, if two points belong to the same orbit, then there is an element of G mapping one to the other; so G has an action on each orbit, and this action is transitive.

If G^Δ is the permutation group induced on the orbit Δ by G, then G is not uniquely determined by the transitive constituents G^Δ, but it can be shown that it is a subdirect product of these (smaller) permutation groups.

So for many purposes it is enough to study transitive groups.

Group-theoretic interpretation

Let H be a subgroup of G. Then G acts on the set $H\backslash G$ of right cosets Hg (for $g \in G$) by right multiplication. These are the link between the permutation group and abstract group structures: any transitive action of a group G is isomorphic (in an appropriate sense) to an action of this form.

Group-theoretic interpretation

Let H be a subgroup of G. Then G acts on the set $H\backslash G$ of right cosets Hg (for $g \in G$) by right multiplication. These are the link between the permutation group and abstract group structures: any transitive action of a group G is isomorphic (in an appropriate sense) to an action of this form.

In more detail, if $\alpha \in \Omega$, the stabiliser G_α is the set of elements of G fixing α; it is a subgroup of G, and the action of G on the orbit containing α is isomorphic to the action on the set of right cosets of G_α.

Group-theoretic interpretation

Let H be a subgroup of G. Then G acts on the set $H\backslash G$ of right cosets Hg (for $g \in G$) by right multiplication. These are the link between the permutation group and abstract group structures: any transitive action of a group G is isomorphic (in an appropriate sense) to an action of this form.

In more detail, if $\alpha \in \Omega$, the stabiliser G_α is the set of elements of G fixing α; it is a subgroup of G, and the action of G on the orbit containing α is isomorphic to the action on the set of right cosets of G_α.

The isomorphism works as follows: for any element β in the orbit of α, the set $\{g \in G : \alpha g = \beta\}$ is a right coset of G_α, and every right coset arises in this way.

Primitivity

The trivial partitions of Ω are the partition into singletons and the partition with a single part Ω.

Primitivity

The trivial partitions of Ω are the partition into singletons and the partition with a single part Ω.
The permutation group G on Ω is primitive if it is transitive and preserves no non-trivial partition of Ω.

Primitivity

The trivial partitions of Ω are the partition into singletons and the partition with a single part Ω.

The permutation group G on Ω is primitive if it is transitive and preserves no non-trivial partition of Ω.

The reason for including "transitive" in the definition is that a set of size 2 has only the trivial partitions, so even the trivial group preserves no non-trivial partition. This actually matters in investigating the structure of diagonal groups, but in general we prefer primitive groups to be transitive.

Group-theoretic version

As we saw, any transitive action of G is isomorphic to the action on the set of right cosets of the point stabiliser G_α.

Group-theoretic version

As we saw, any transitive action of G is isomorphic to the action on the set of right cosets of the point stabiliser G_α. This action is primitive if and only if G_α is a maximal subgroup of G.

Group-theoretic version

As we saw, any transitive action of G is isomorphic to the action on the set of right cosets of the point stabiliser G_α.
This action is primitive if and only if G_α is a maximal subgroup of G.
Also, if N is a normal subgroup of G, then the orbits of N form a G-invariant partition; so, if G is primitive, then either N is transitive, or its action is trivial (fixing every point). For $G_\alpha N$ is a subgroup properly containing G_α, hence equal to G; so N contains a set of coset representatives for G_α in G, which means that it is transitive.

Quasi-primitive groups

This leads to a concept which is a weakening of primitivity.

Quasi-primitive groups

This leads to a concept which is a weakening of primitivity. We say that the transitive permutation group G on Ω is quasi-primitive if every normal subgroup of G is either transitive or trivial. Thus, a primitive group is quasi-primitive.

Quasi-primitive groups

This leads to a concept which is a weakening of primitivity. We say that the transitive permutation group G on Ω is quasi-primitive if every normal subgroup of G is either transitive or trivial. Thus, a primitive group is quasi-primitive. In particular, any transitive action of a simple group is quasi-primitive.

Quasi-primitive groups

This leads to a concept which is a weakening of primitivity. We say that the transitive permutation group G on Ω is quasi-primitive if every normal subgroup of G is either transitive or trivial. Thus, a primitive group is quasi-primitive. In particular, any transitive action of a simple group is quasi-primitive.

Problem

Is there a definition of quasi-primitivity in the style used above for transitivity and primitivity, i.e. "G is quasi-primitive if and only if there is no non-trivial G-invariant structure of type X"?

Quasi-primitive groups

This leads to a concept which is a weakening of primitivity. We say that the transitive permutation group G on Ω is quasi-primitive if every normal subgroup of G is either transitive or trivial. Thus, a primitive group is quasi-primitive. In particular, any transitive action of a simple group is quasi-primitive.

Problem

Is there a definition of quasi-primitivity in the style used above for transitivity and primitivity, i.e. "G is quasi-primitive if and only if there is no non-trivial G-invariant structure of type X"?

Many results about primitive groups have been extended to quasi-primitive groups, especially by Cheryl Praeger and her colleagues; but I will not discuss them further.

Imprimitive groups

Suppose that G preserves the non-trivial partition P, and let B be a member of P.

Imprimitive groups

Suppose that G preserves the non-trivial partition P, and let B be a member of P.
Define H to be the permutation group induced on B by its setwise stabiliser, and K the permutation group induced on P by G.

Imprimitive groups

Suppose that G preserves the non-trivial partition P, and let B be a member of P.

Define H to be the permutation group induced on B by its setwise stabiliser, and K the permutation group induced on P by G.

Then G is isomorphic to a subgroup of the wreath product $H \operatorname{Wr} K$, whose base group is a Cartesian product of $|P|$ copies of H (indexed by P), and whose top group is K, acting on the base group by permuting the factors.

Imprimitive groups

Suppose that G preserves the non-trivial partition P, and let B be a member of P.

Define H to be the permutation group induced on B by its setwise stabiliser, and K the permutation group induced on P by G.

Then G is isomorphic to a subgroup of the wreath product $H \operatorname{Wr} K$, whose base group is a Cartesian product of $|P|$ copies of H (indexed by P), and whose top group is K, acting on the base group by permuting the factors.

Again we have a reduction to "smaller" groups. However, I will not discuss this further.

Cartesian structures

Much permutation group theory focuses on describing primitive (or quasi-primitive) groups. However, it is convenient to take one more step.

Cartesian structures

Much permutation group theory focuses on describing primitive (or quasi-primitive) groups. However, it is convenient to take one more step.

A Cartesian structure on Ω is an identification of Ω with X^n for some set X and natural number n; it is non-trivial if $n > 1$. Such a structure can be regarded in various ways; for example, we can think of X^n as a metric space with the Hamming metric d_H, in which the distance between two n-tuples is the number of coordinates in which they differ.

Cartesian structures

Much permutation group theory focuses on describing primitive (or quasi-primitive) groups. However, it is convenient to take one more step.

A Cartesian structure on Ω is an identification of Ω with X^n for some set X and natural number n; it is non-trivial if $n > 1$. Such a structure can be regarded in various ways; for example, we can think of X^n as a metric space with the Hamming metric d_H, in which the distance between two n-tuples is the number of coordinates in which they differ.

If G preserves a Cartesian structure on Ω, then we can define two "smaller" permutation groups H and K, where H is the group induced on the elements of X in a given coordinate by its stabiliser, and K is the group permuting the coordinates; once again we have an embedding of G in the wreath product $H \operatorname{Wr} K$.

Cartesian structures

Much permutation group theory focuses on describing primitive (or quasi-primitive) groups. However, it is convenient to take one more step.

A Cartesian structure on Ω is an identification of Ω with X^n for some set X and natural number n; it is non-trivial if $n > 1$. Such a structure can be regarded in various ways; for example, we can think of X^n as a metric space with the Hamming metric d_H, in which the distance between two n-tuples is the number of coordinates in which they differ.

If G preserves a Cartesian structure on Ω, then we can define two "smaller" permutation groups H and K, where H is the group induced on the elements of X in a given coordinate by its stabiliser, and K is the group permuting the coordinates; once again we have an embedding of G in the wreath product $H \operatorname{Wr} K$.

For more details see the recent book by Praeger and Schneider.

Basic groups

A permutation group G on Ω is basic if it is primitive and preserves no non-trivial Cartesian structure on Ω.

Basic groups

A permutation group G on Ω is basic if it is primitive and preserves no non-trivial Cartesian structure on Ω.
A remarkable theorem due to O'Nan and Scott, extending earlier (and neglected) results of Jordan, asserts the following.

Basic groups

A permutation group G on Ω is basic if it is primitive and preserves no non-trivial Cartesian structure on Ω.
A remarkable theorem due to O'Nan and Scott, extending earlier (and neglected) results of Jordan, asserts the following.

Theorem
A basic permutation group on a finite set Ω is affine, diagonal, or almost simple.

Basic groups

A permutation group G on Ω is basic if it is primitive and preserves no non-trivial Cartesian structure on Ω.
A remarkable theorem due to O'Nan and Scott, extending earlier (and neglected) results of Jordan, asserts the following.

Theorem

A basic permutation group on a finite set Ω is affine, diagonal, or almost simple.

I will explain the three types of group on the next few slides.

Affine groups

A permutation group G on Ω is affine if there is an identification of Ω with a vector space V over a field $\mathbb{F}$ such that G is contained in the affine general linear group

$$\mathrm{AGL}(V) = \{v \mapsto vA + c : A \in \mathrm{GL}(V), c \in V\}$$

where $\mathrm{GL}(V)$ is the group of invertible linear transformations of V, and G contains the translation group $T = \{v \mapsto v + c : c \in V\}$.

Affine groups

A permutation group G on Ω is affine if there is an identification of Ω with a vector space V over a field $\mathbb{F}$ such that G is contained in the affine general linear group

$$\mathrm{AGL}(V) = \{v \mapsto vA + c : A \in \mathrm{GL}(V), c \in V\}$$

where $\mathrm{GL}(V)$ is the group of invertible linear transformations of V, and G contains the translation group
$T = \{v \mapsto v + c : c \in V\}$.
An affine permutation group is thus a semidirect product of T by H, where H is a subgroup of $\mathrm{GL}(V)$. Now

Affine groups

A permutation group G on Ω is affine if there is an identification of Ω with a vector space V over a field $\mathbb{F}$ such that G is contained in the affine general linear group

$$\mathrm{AGL}(V) = \{v \mapsto vA + c : A \in \mathrm{GL}(V), c \in V\}$$

where $\mathrm{GL}(V)$ is the group of invertible linear transformations of V, and G contains the translation group $T = \{v \mapsto v + c : c \in V\}$.
An affine permutation group is thus a semidirect product of T by H, where H is a subgroup of $\mathrm{GL}(V)$. Now

- G is primitive if and only if H is irreducible on V;

Affine groups

A permutation group G on Ω is affine if there is an identification of Ω with a vector space V over a field $\mathbb{F}$ such that G is contained in the affine general linear group

$$\mathrm{AGL}(V) = \{v \mapsto vA + c : A \in \mathrm{GL}(V), c \in V\}$$

where $\mathrm{GL}(V)$ is the group of invertible linear transformations of V, and G contains the translation group $T = \{v \mapsto v + c : c \in V\}$.
An affine permutation group is thus a semidirect product of T by H, where H is a subgroup of $\mathrm{GL}(V)$. Now

- G is primitive if and only if H is irreducible on V;
- G is basic if and only if H is primitive as linear group, that is, preserves no non-trivial direct sum decomposition of V.

Affine groups

A permutation group G on Ω is affine if there is an identification of Ω with a vector space V over a field $\mathbb{F}$ such that G is contained in the affine general linear group

$$\mathrm{AGL}(V) = \{v \mapsto vA + c : A \in \mathrm{GL}(V), c \in V\}$$

where $\mathrm{GL}(V)$ is the group of invertible linear transformations of V, and G contains the translation group $T = \{v \mapsto v + c : c \in V\}$.
An affine permutation group is thus a semidirect product of T by H, where H is a subgroup of $\mathrm{GL}(V)$. Now

- G is primitive if and only if H is irreducible on V;
- G is basic if and only if H is primitive as linear group, that is, preserves no non-trivial direct sum decomposition of V.

Further study of affine groups uses Aschbacher's Theorem on subgroups of linear groups.

Diagonal groups

Let T be a non-abelian finite simple group, and d a natural number greater than 1. A permutation group G is diagonal if its socle (product of minimal normal subgroups) is isomorphic to T^d acting on the cosets of its diagonal subgroup $\{(t, t, \ldots, t) : t \in T\}$.

Diagonal groups

Let T be a non-abelian finite simple group, and d a natural number greater than 1. A permutation group G is diagonal if its socle (product of minimal normal subgroups) is isomorphic to T^d acting on the cosets of its diagonal subgroup $\{(t, t, \ldots, t) : t \in T\}$.
In the case $d = 2$, there is a simpler description: $T \times T$ acts on T by left and right multiplication:

$$(g, h) : t \mapsto g^{-1}th.$$

Diagonal groups

Let T be a non-abelian finite simple group, and d a natural number greater than 1. A permutation group G is diagonal if its socle (product of minimal normal subgroups) is isomorphic to T^d acting on the cosets of its diagonal subgroup $\{(t, t, \ldots, t) : t \in T\}$.
In the case $d = 2$, there is a simpler description: $T \times T$ acts on T by left and right multiplication:

$$(g, h) : t \mapsto g^{-1}th.$$

The normaliser of T^d in the symmetric group also contains

- automorphisms of T (acting componentwise);
- the symmetric group S_d, permuting the components.

Diagonal groups

Let T be a non-abelian finite simple group, and d a natural number greater than 1. A permutation group G is diagonal if its socle (product of minimal normal subgroups) is isomorphic to T^d acting on the cosets of its diagonal subgroup $\{(t, t, \ldots, t) : t \in T\}$.
In the case $d = 2$, there is a simpler description: $T \times T$ acts on T by left and right multiplication:

$$(g, h) : t \mapsto g^{-1}th.$$

The normaliser of T^d in the symmetric group also contains

- automorphisms of T (acting componentwise);
- the symmetric group S_d, permuting the components.

In the case $d = 3$, the full diagonal group is the automorphism group of the Latin square graph associated with the Cayley table of T.

Almost simple groups

The group G is almost simple if $T \leq G \leq \mathrm{Aut}(T)$ for some non-abelian simple group T, where T is embedded in $\mathrm{Aut}(T)$ as its group of inner automorphisms.

Almost simple groups

The group G is almost simple if $T \leq G \leq \mathrm{Aut}(T)$ for some non-abelian simple group T, where T is embedded in $\mathrm{Aut}(T)$ as its group of inner automorphisms.

The Schreier conjecture, whose truth follows from the Classification of Finite Simple Groups, asserts that the outer automorphism group $\mathrm{Aut}(T)/T$ is "very small", so that G is pinned down quite precisely.

Almost simple groups

The group G is almost simple if $T \leq G \leq \mathrm{Aut}(T)$ for some non-abelian simple group T, where T is embedded in $\mathrm{Aut}(T)$ as its group of inner automorphisms.
The Schreier conjecture, whose truth follows from the Classification of Finite Simple Groups, asserts that the outer automorphism group $\mathrm{Aut}(T)/T$ is "very small", so that G is pinned down quite precisely.
However, in contrast to the other two classes in the O'Nan–Scott theorem, the action of G is not prescribed here. So this is the case where most of the mystery resides.

Multiply-transitive groups

A permutation group G on Ω is 2-transitive if it preserves no non-trivial directed graph on Ω. Equivalently, any ordered pair of distinct points of Ω can be mapped to any other such pair by some element of G.

Multiply-transitive groups

A permutation group G on Ω is 2-transitive if it preserves no non-trivial directed graph on Ω. Equivalently, any ordered pair of distinct points of Ω can be mapped to any other such pair by some element of G.
More generally G is t-transitive if any t-tuple of distinct points can be mapped to any other by an element of G. (We assume that $|\Omega| \geq t$.) Note that t-transitivity implies $(t-1)$-transitivity.

Multiply-transitive groups

A permutation group G on Ω is 2-transitive if it preserves no non-trivial directed graph on Ω. Equivalently, any ordered pair of distinct points of Ω can be mapped to any other such pair by some element of G.

More generally G is t-transitive if any t-tuple of distinct points can be mapped to any other by an element of G. (We assume that $|\Omega| \geq t$.) Note that t-transitivity implies $(t-1)$-transitivity.

The symmetric group of degree n is n-transitive, and the alternating group is $(n-2)$-transitive. In the nineteenth century, Mathieu discovered two additional 5-transitive groups, M_{12} and M_{24}, and two 4-transitive groups, M_{11} and M_{23}.

Multiply-transitive groups

A permutation group G on Ω is 2-transitive if it preserves no non-trivial directed graph on Ω. Equivalently, any ordered pair of distinct points of Ω can be mapped to any other such pair by some element of G.

More generally G is t-transitive if any t-tuple of distinct points can be mapped to any other by an element of G. (We assume that $|\Omega| \geq t$.) Note that t-transitivity implies $(t-1)$-transitivity.

The symmetric group of degree n is n-transitive, and the alternating group is $(n-2)$-transitive. In the nineteenth century, Mathieu discovered two additional 5-transitive groups, M_{12} and M_{24}, and two 4-transitive groups, M_{11} and M_{23}.

Mathieu knew that primitive groups other than S_n and A_n exist for $5 \leq n \leq 33$; but for $n = 22$, it is necessary to construct M_{22} to show this.

Multiply-transitive groups, again

For a century, one of the defining problems of permutation group theory was the existence question for 6-transitive groups other than symmetric and alternating groups. Wielandt found a bound of about $\log n$ for the transitivity degree of such a group of degree n. He also showed the non-existence of 8-transitive groups modulo the Schreier conjecture; this was improved to 7 by Nagao and 6 by O'Nan.

Multiply-transitive groups, again

For a century, one of the defining problems of permutation group theory was the existence question for 6-transitive groups other than symmetric and alternating groups. Wielandt found a bound of about $\log n$ for the transitivity degree of such a group of degree n. He also showed the non-existence of 8-transitive groups modulo the Schreier conjecture; this was improved to 7 by Nagao and 6 by O'Nan.

Burnside knew that a 2-transitive group must be affine or almost simple. (This special case of the O'Nan–Scott theorem was probably known to Jordan but forgotten.)

Multiply-transitive groups, again

For a century, one of the defining problems of permutation group theory was the existence question for 6-transitive groups other than symmetric and alternating groups. Wielandt found a bound of about $\log n$ for the transitivity degree of such a group of degree n. He also showed the non-existence of 8-transitive groups modulo the Schreier conjecture; this was improved to 7 by Nagao and 6 by O'Nan.

Burnside knew that a 2-transitive group must be affine or almost simple. (This special case of the O'Nan–Scott theorem was probably known to Jordan but forgotten.)

With the combined efforts of many people including Curtis, Kantor, Seitz, Howlett, Hering, and Liebeck, and the Classification of Finite Simple Groups, we know have:

Multiply-transitive groups, again

For a century, one of the defining problems of permutation group theory was the existence question for 6-transitive groups other than symmetric and alternating groups. Wielandt found a bound of about $\log n$ for the transitivity degree of such a group of degree n. He also showed the non-existence of 8-transitive groups modulo the Schreier conjecture; this was improved to 7 by Nagao and 6 by O'Nan.

Burnside knew that a 2-transitive group must be affine or almost simple. (This special case of the O'Nan–Scott theorem was probably known to Jordan but forgotten.)

With the combined efforts of many people including Curtis, Kantor, Seitz, Howlett, Hering, and Liebeck, and the Classification of Finite Simple Groups, we know have:

Theorem

All finite 2-transitive groups are known. In particular, the only 6-transitive groups are symmetric and alternating groups.

Footnote to Mathieu

Mathieu may have thought that primitive groups of degree n (other than S_n or A_n) would exist for all, or almost all, n. But there is none of degree 34. With Peter Neumann and Dave Teague, I showed (using CFSG) that degrees of such groups are rare; if $e(x)$ is the number of them less than x, then

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

Footnote to Mathieu

Mathieu may have thought that primitive groups of degree n (other than S_n or A_n) would exist for all, or almost all, n. But there is none of degree 34. With Peter Neumann and Dave Teague, I showed (using CFSG) that degrees of such groups are rare; if $e(x)$ is the number of them less than x, then

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

(Here $\pi(x)$ is the number of primes less than x. The difference between $\pi(x)$ and its analytic approximation $x/\log x$ swamps out the next term in the asymptotic expansion.)

Footnote to Mathieu

Mathieu may have thought that primitive groups of degree n (other than S_n or A_n) would exist for all, or almost all, n. But there is none of degree 34. With Peter Neumann and Dave Teague, I showed (using CFSG) that degrees of such groups are rare; if $e(x)$ is the number of them less than x, then

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

(Here $\pi(x)$ is the number of primes less than x. The difference between $\pi(x)$ and its analytic approximation $x/\log x$ swamps out the next term in the asymptotic expansion.)
All primitive groups of degree smaller than 4096 have been determined; these groups are available in the computer algebra systems Magma and GAP. (This would be completely out of reach without CFSG.)

Set-transitivity

In their foundational book on game theory, von Neumann and Morgenstern asked (in connection with their definition of "fair" n-player games), which permutation groups of degree n are set-transitive, that is, transitive on subsets of size t for $0 \leq t \leq n$? The question was answered by Chevalley (unpublished as far as I know); a solution was published by Beaumont and Peterson (with no reference to von Neumann and Morgenstern). Apart from symmetric and alternating groups, there are just four such groups, with degrees 5, 6, 9, 9 respectively.

Set-transitivity

In their foundational book on game theory, von Neumann and Morgenstern asked (in connection with their definition of "fair" n-player games), which permutation groups of degree n are set-transitive, that is, transitive on subsets of size t for $0 \le t \le n$? The question was answered by Chevalley (unpublished as far as I know); a solution was published by Beaumont and Peterson (with no reference to von Neumann and Morgenstern). Apart from symmetric and alternating groups, there are just four such groups, with degrees 5, 6, 9, 9 respectively.

More generally a permutation group is 2-set transitive, or 2-homogeneous, if it preserves no non-trivial graph on Ω, that is, acts transitively on the 2-element subsets of Ω.

Set-transitivity

In their foundational book on game theory, von Neumann and Morgenstern asked (in connection with their definition of "fair" n-player games), which permutation groups of degree n are set-transitive, that is, transitive on subsets of size t for $0 \leq t \leq n$? The question was answered by Chevalley (unpublished as far as I know); a solution was published by Beaumont and Peterson (with no reference to von Neumann and Morgenstern). Apart from symmetric and alternating groups, there are just four such groups, with degrees 5, 6, 9, 9 respectively.

More generally a permutation group is 2-set transitive, or 2-homogeneous, if it preserves no non-trivial graph on Ω, that is, acts transitively on the 2-element subsets of Ω.

Further, G is t-set transitive, or t-homogeneous, if it acts transitively on the t-element subsets of Ω. Note that t-homogeneity is equivalent to $(n-t)$-homogeneity (where $n = |\Omega|$), so we may assume that $t \leq n/2$.

t-homogeneity

A pioneering paper of Livingstone and Wagner investigated these concepts. They showed using representation theory that t-homogeneity implies $(t-1)$-homogeneity for $2 \leq t \leq n/2$. They showed further that such groups are t-transitive for $t \geq 5$.

t-homogeneity

A pioneering paper of Livingstone and Wagner investigated these concepts. They showed using representation theory that t-homogeneity implies $(t-1)$-homogeneity for $2 \leq t \leq n/2$. They showed further that such groups are t-transitive for $t \geq 5$. If G is 2-homogeneous but not 2-transitive, then no pair of points can be interchanged, so G has odd order. By the Feit–Thompson theorem, G is soluble, from which it follows that it is affine, and that $\langle G, -I \rangle$ is 2-transitive. Thus all such groups are known. (This was done independently by Kantor and Berggren.)

t-homogeneity

A pioneering paper of Livingstone and Wagner investigated these concepts. They showed using representation theory that t-homogeneity implies $(t-1)$-homogeneity for $2 \leq t \leq n/2$. They showed further that such groups are t-transitive for $t \geq 5$.
If G is 2-homogeneous but not 2-transitive, then no pair of points can be interchanged, so G has odd order. By the Feit–Thompson theorem, G is soluble, from which it follows that it is affine, and that $\langle G, -I \rangle$ is 2-transitive. Thus all such groups are known. (This was done independently by Kantor and Berggren.)
More generally Kantor determined all the t-homogeneous but not t-transitive groups for $2 \leq t \leq 4$.

Other properties

There are several other classes of primitive permutation groups, defined by other types of combinatorial structure, with the usual template: G is "X-free" if it preserves no non-trivial X-structure on Ω. I will talk about several of these, arising from automata theory and semigroup theory, in my next talk.

Other properties

There are several other classes of primitive permutation groups, defined by other types of combinatorial structure, with the usual template: G is "X-free" if it preserves no non-trivial X-structure on Ω. I will talk about several of these, arising from automata theory and semigroup theory, in my next talk.

I will finish up the present talk by describing a recent result along these lines by Sean Eberhard and me.

Other properties

There are several other classes of primitive permutation groups, defined by other types of combinatorial structure, with the usual template: G is "X-free" if it preserves no non-trivial X-structure on Ω. I will talk about several of these, arising from automata theory and semigroup theory, in my next talk.
I will finish up the present talk by describing a recent result along these lines by Sean Eberhard and me.
This also allows me to introduce a very important combinatorial tool in the study of permutation groups.

Coherent configurations

Coherent configurations have several mathematical origins. They were introduced by Donald Higman to extend work of Schur and Wielandt on permutation groups; by Weisfeiler and Leman for the graph isomorphism problem; and by Bose for use in design and analysis of experiments in statistics.

Coherent configurations

Coherent configurations have several mathematical origins. They were introduced by Donald Higman to extend work of Schur and Wielandt on permutation groups; by Weisfeiler and Leman for the graph isomorphism problem; and by Bose for use in design and analysis of experiments in statistics.

A binary relation on a set Ω (a subset of $\Omega \times \Omega$) can be represented by a zero-one relation matrix with rows and columns indexed by Ω: the (α, β) entry is 1 if (α, β) satisfies the relation and zero otherwise.

Coherent configurations

Coherent configurations have several mathematical origins. They were introduced by Donald Higman to extend work of Schur and Wielandt on permutation groups; by Weisfeiler and Leman for the graph isomorphism problem; and by Bose for use in design and analysis of experiments in statistics.

A binary relation on a set Ω (a subset of $\Omega \times \Omega$) can be represented by a zero-one relation matrix with rows and columns indexed by Ω: the (α, β) entry is 1 if (α, β) satisfies the relation and zero otherwise.

Now a coherent configuration is a set $\mathcal{C}$ of binary relations on Ω such that

Coherent configurations

Coherent configurations have several mathematical origins. They were introduced by Donald Higman to extend work of Schur and Wielandt on permutation groups; by Weisfeiler and Leman for the graph isomorphism problem; and by Bose for use in design and analysis of experiments in statistics.

A binary relation on a set Ω (a subset of $\Omega \times \Omega$) can be represented by a zero-one relation matrix with rows and columns indexed by Ω: the (α, β) entry is 1 if (α, β) satisfies the relation and zero otherwise.

Now a coherent configuration is a set $\mathcal{C}$ of binary relations on Ω such that

- the relations in $\mathcal{C}$ partition $\Omega \times \Omega$;

Coherent configurations

Coherent configurations have several mathematical origins. They were introduced by Donald Higman to extend work of Schur and Wielandt on permutation groups; by Weisfeiler and Leman for the graph isomorphism problem; and by Bose for use in design and analysis of experiments in statistics.

A binary relation on a set Ω (a subset of $\Omega \times \Omega$) can be represented by a zero-one relation matrix with rows and columns indexed by Ω: the (α, β) entry is 1 if (α, β) satisfies the relation and zero otherwise.

Now a coherent configuration is a set $\mathcal{C}$ of binary relations on Ω such that

- the relations in $\mathcal{C}$ partition $\Omega \times \Omega$;
- a subset of the relations partitions the diagonal $\{(\alpha, \alpha) : \alpha \in \Omega\}$;

Coherent configurations

Coherent configurations have several mathematical origins. They were introduced by Donald Higman to extend work of Schur and Wielandt on permutation groups; by Weisfeiler and Leman for the graph isomorphism problem; and by Bose for use in design and analysis of experiments in statistics.

A binary relation on a set Ω (a subset of $\Omega \times \Omega$) can be represented by a zero-one relation matrix with rows and columns indexed by Ω: the (α, β) entry is 1 if (α, β) satisfies the relation and zero otherwise.

Now a coherent configuration is a set $\mathcal{C}$ of binary relations on Ω such that

- the relations in $\mathcal{C}$ partition $\Omega \times \Omega$;
- a subset of the relations partitions the diagonal $\{(\alpha, \alpha) : \alpha \in \Omega\}$;
- the converse of a relation in $\mathcal{C}$ is in $\mathcal{C}$;

Coherent configurations

Coherent configurations have several mathematical origins. They were introduced by Donald Higman to extend work of Schur and Wielandt on permutation groups; by Weisfeiler and Leman for the graph isomorphism problem; and by Bose for use in design and analysis of experiments in statistics.

A binary relation on a set Ω (a subset of $\Omega \times \Omega$) can be represented by a zero-one relation matrix with rows and columns indexed by Ω: the (α, β) entry is 1 if (α, β) satisfies the relation and zero otherwise.

Now a coherent configuration is a set $\mathcal{C}$ of binary relations on Ω such that

- the relations in $\mathcal{C}$ partition $\Omega \times \Omega$;
- a subset of the relations partitions the diagonal $\{(\alpha, \alpha) : \alpha \in \Omega\}$;
- the converse of a relation in $\mathcal{C}$ is in $\mathcal{C}$;
- the linear span of the relation matrices is closed under matrix multiplication.

Association schemes

The relation matrices of a coherent configuration over $\mathbb{C}$ form a semisimple algebra, the Bose–Mesner algebra of the configuration.

Association schemes

The relation matrices of a coherent configuration over $\mathbb{C}$ form a semisimple algebra, the Bose–Mesner algebra of the configuration.

The orbits on $\Omega \times \Omega$ of a permutation group G on Ω form a coherent configuration; such a configuration is called Schurian.

This was Higman's motivation for studying these things. The Bose–Mesner algebra of a Schurian scheme is the centraliser algebra of the permutation group.

Association schemes

The relation matrices of a coherent configuration over $\mathbb{C}$ form a semisimple algebra, the Bose–Mesner algebra of the configuration.

The orbits on $\Omega \times \Omega$ of a permutation group G on Ω form a coherent configuration; such a configuration is called Schurian. This was Higman's motivation for studying these things. The Bose–Mesner algebra of a Schurian scheme is the centraliser algebra of the permutation group.

If all the matrices are symmetric, the configuration is called an association scheme. Following Bose, statisticians were interested only in association schemes, since covariance matrices are always symmetric, and statistical data consists of real numbers.

AS-free groups

The trivial coherent configurations are the partition into singletons and the 2-part partition whose relation matrices are I and $J - I$ (where J is the all-1 matrix).

AS-free groups

The trivial coherent configurations are the partition into singletons and the 2-part partition whose relation matrices are I and $J - I$ (where J is the all-1 matrix).
So, if we define G to be CC-free if it preserves no non-trivial coherent configuration, the CC-free groups would be the 2-transitive groups.

AS-free groups

The trivial coherent configurations are the partition into singletons and the 2-part partition whose relation matrices are I and $J - I$ (where J is the all-1 matrix).

So, if we define G to be CC-free if it preserves no non-trivial coherent configuration, the CC-free groups would be the 2-transitive groups.

However, for association schemes, the question is more subtle. Call a permutation group G AS-free if it preserves no non-trivial association scheme (symmetric coherent configuration) on Ω.

Problem

Which transitive permutation groups are AS-free?

AS-free groups

The trivial coherent configurations are the partition into singletons and the 2-part partition whose relation matrices are I and $J - I$ (where J is the all-1 matrix).
So, if we define G to be CC-free if it preserves no non-trivial coherent configuration, the CC-free groups would be the 2-transitive groups.
However, for association schemes, the question is more subtle.
Call a permutation group G AS-free if it preserves no non-trivial association scheme (symmetric coherent configuration) on Ω.

Problem

Which transitive permutation groups are AS-free?

The 2-homogeneous groups are AS-free; but there are others!

AS-free groups, continued

If G is transitive but imprimitive, it preserves a partition of Ω, and so preserves the divisible association scheme whose relations are "equal", "different but in the same part", and "other". So an AS-free group is primitive.

AS-free groups, continued

If G is transitive but imprimitive, it preserves a partition of Ω, and so preserves the divisible association scheme whose relations are "equal", "different but in the same part", and "other". So an AS-free group is primitive.
If G is primitive but not basic, it preserves a Hamming association scheme, whose relations are defined by the values of the Hamming metric. So an AS-free group is basic.

AS-free groups, continued

If G is transitive but imprimitive, it preserves a partition of Ω, and so preserves the divisible association scheme whose relations are "equal", "different but in the same part", and "other". So an AS-free group is primitive.
If G is primitive but not basic, it preserves a Hamming association scheme, whose relations are defined by the values of the Hamming metric. So an AS-free group is basic.
By O'Nan–Scott, it is affine, diagonal or almost simple.

AS-free groups, continued

If G is transitive but imprimitive, it preserves a partition of Ω, and so preserves the divisible association scheme whose relations are "equal", "different but in the same part", and "other". So an AS-free group is primitive.
If G is primitive but not basic, it preserves a Hamming association scheme, whose relations are defined by the values of the Hamming metric. So an AS-free group is basic.
By O'Nan–Scott, it is affine, diagonal or almost simple.
An affine AS-free group must be 2-homogeneous. For the Bose–Mesner algebra of the coherent configuration are contained in the group algebra of the (abelian) translation group, from which it is easy to see that the configuration can be symmetrised by adding relation matrices to their transposes if necessary.

The final result

A 2-factor diagonal group has socle $T \times T$ (T simple), acting by left and right multiplication. It preserves the conjugacy class scheme, in which x and y are in the relation corresponding to the class C if $x^{-1}y \in C \cup C^{-1}$. So these groups are not AS-free.

The final result

A 2-factor diagonal group has socle $T \times T$ (T simple), acting by left and right multiplication. It preserves the conjugacy class scheme, in which x and y are in the relation corresponding to the class C if $x^{-1}y \in C \cup C^{-1}$. So these groups are not AS-free.

A 3-factor diagonal group, as we saw, is the automorphism group of the Latin square graph of the Cayley table of T. This graph is strongly regular, which means that the relations "equal", "adjacent" and "non-adjacent" form an association scheme. Eberhard and I were able to generalise this to construct association schemes for d-factor diagonal groups for all $d \geq 3$. So these groups are not AS-free.

The final result

A 2-factor diagonal group has socle $T \times T$ (T simple), acting by left and right multiplication. It preserves the conjugacy class scheme, in which x and y are in the relation corresponding to the class C if $x^{-1}y \in C \cup C^{-1}$. So these groups are not AS-free.

A 3-factor diagonal group, as we saw, is the automorphism group of the Latin square graph of the Cayley table of T. This graph is strongly regular, which means that the relations "equal", "adjacent" and "non-adjacent" form an association scheme. Eberhard and I were able to generalise this to construct association schemes for d-factor diagonal groups for all $d \geq 3$. So these groups are not AS-free.

Hence we have:

The final result

A 2-factor diagonal group has socle $T \times T$ (T simple), acting by left and right multiplication. It preserves the conjugacy class scheme, in which x and y are in the relation corresponding to the class C if $x^{-1}y \in C \cup C^{-1}$. So these groups are not AS-free.
A 3-factor diagonal group, as we saw, is the automorphism group of the Latin square graph of the Cayley table of T. This graph is strongly regular, which means that the relations "equal", "adjacent" and "non-adjacent" form an association scheme. Eberhard and I were able to generalise this to construct association schemes for d-factor diagonal groups for all $d \geq 3$. So these groups are not AS-free.
Hence we have:

Theorem

A transitive AS-free permutation group is either 2-homogeneous or almost simple.

Almost simple groups

Perhaps surprisingly, there do exist almost simple AS-free groups, though only a few are known at present. These are:

Almost simple groups

Perhaps surprisingly, there do exist almost simple AS-free groups, though only a few are known at present. These are:

- $\mathrm{PSL}(3,3)$, acting on the right cosets of $\mathrm{PO}(3,3)$ (a subgroup isomorphic to S_4), with degree 234;

Almost simple groups

Perhaps surprisingly, there do exist almost simple AS-free groups, though only a few are known at present. These are:

- $\mathrm{PSL}(3,3)$, acting on the right cosets of $\mathrm{PO}(3,3)$ (a subgroup isomorphic to S_4), with degree 234;
- M_{12}, degree 1320;

Almost simple groups

Perhaps surprisingly, there do exist almost simple AS-free groups, though only a few are known at present. These are:

- $\mathrm{PSL}(3,3)$, acting on the right cosets of $\mathrm{PO}(3,3)$ (a subgroup isomorphic to S_4), with degree 234;
- M_{12}, degree 1320;
- J_1, degree 1463, 1540 or 1596;

Almost simple groups

Perhaps surprisingly, there do exist almost simple AS-free groups, though only a few are known at present. These are:

- $\mathrm{PSL}(3,3)$, acting on the right cosets of $\mathrm{PO}(3,3)$ (a subgroup isomorphic to S_4), with degree 234;
- M_{12}, degree 1320;
- J_1, degree 1463, 1540 or 1596;
- J_2, degree 1800.

Almost simple groups

Perhaps surprisingly, there do exist almost simple AS-free groups, though only a few are known at present. These are:

- $\mathrm{PSL}(3,3)$, acting on the right cosets of $\mathrm{PO}(3,3)$ (a subgroup isomorphic to S_4), with degree 234;
- M_{12}, degree 1320;
- J_1, degree 1463, 1540 or 1596;
- J_2, degree 1800.

Problem

Make some sense of almost simple AS-free groups!

References

M. Aschbacher, On the maximal subgroups of the finite classical groups, *Invent. Math.* **76** (1984), 469–514.

P. J. Cameron and S. Eberhard, Association schemes for diagonal groups, *Austral. J. Combinatorics* **75** (2019), 357–364.

B. Fein, W. M. Kantor and M. Schacher, Relative Brauer Groups II, *J. Reine Angew. Math.* **328** (1981), 39–57.

C. E. Praeger and C. Schneider, *Permutation Groups and Cartesian Decompositions*, LMS Lecture Notes **449**, Cambridge, 2018.

J.-P. Serre, On a theorem of Jordan, *Bull. Amer. Math. Soc.* **40** (2003), 429–440.