FINITE PERMUTATION GROUPS AND FINITE CLASSICAL GROUPS

NICK GILL

1. Introduction

Throughout this section G is a group. The group G is called *simple* if it is nontrivial and the only normal subgroups of G are $\{1\}$ and G.

> **(E1.1)** *Prove that if G is a finite simple abelian group, then $G \cong C_p$, the cyclic subgroup of order p, where p is a prime.*

This course is motivated by a desire to understand the finite simple groups. As we shall see, when we come to study series, an understanding of the finite simple groups takes us a long way towards understanding all finite groups.

One of the great mathematical achievements of the last century has been the complete classification of the finite simple groups. This classification, the proof of which stretches across thousands of journal articles in work by dozens of authors, can be stated simply.

Theorem 1.1. *(Classification of Finite Simple Groups) A finite simple group is isomorphic to one of the following*

1. *A cyclic group C_p, of order p where p is a prime;*
2. *An alternating group $\mathrm{Alt}(n)$, where $n \geq 5$;*
3. *A finite group of Lie type;*
4. *One of 26 sporadic groups.*

This course is, roughly speaking, split into two halves. In the first half we will study the second type of simple group listed in CFSG, namely the alternating groups $\mathrm{Alt}(n)$. You have already met these groups in an undergraduate course, but there are still many natural questions that one can ask about them: What are their conjugacy classes? What are their automorphism groups? What are their subgroups? We will give at least partial answers to all of these questions.

Our method in studying the alternating groups will be to exploit their natural structure as permutation groups acting on sets with n elements. Thus we will spend quite a bit of time studying permutation groups, which are objects of interest in their own right. [1]

This start will set us up well for the second half of the course when we come to study the finite classical groups. These are a subclass of the groups of Lie type, the others being known as the *exceptional groups of Lie type*. Our analysis of the classical groups follows the original approach of Jordan and, later, Dickson. In other words, we construct the classical groups as quotients of certain subgroups of $\mathrm{GL}(V)$, the set of invertible linear transformations over a finite vector space V. These subgroups have a natural action on the associated vector space V, and we can study this action using permutation group theory in order to deduce properties of the relevant simple groups.

A brief note about what is missing: the two classes of finite simple group that we fail to discuss are the exceptional groups of Lie type, and the 26 sporadic groups. The latter, at least, are a finite set so we might argue that their omission is not so serious. On the other hand the sporadic groups are among the most famous and beautiful objects in finite group theory, so their absence is regretted. Unfortunately, it is their very sporadic-ness that makes them so hard to include – they do not submit

[1] Indeed it is worth noting that group theory first arose, via the work of Galois and his successors, as the study of permutations of sets. In other words, in the beginning, permutation groups were the only objects studied from the subject we now think of as group theory.

easily to a uniform treatment and each sporadic group requires individual attention to be understood properly. The keen student is encouraged to consult [Asc94].

The exceptional groups of Lie type are a different kettle of fish. They form an infinite class of groups and, although they were discovered in a somewhat sporadic way through the first half of the twentieth century, they now form part of a uniform theory of groups of Lie type that has its origins with Chevalley, and later Steinberg, Ree and Tits. This uniform theory has the advantage that it allows one to study all finite groups of Lie type (including the classical groups) in one fell swoop, but it has the disadvantage (at least to my mind) of being somewhat more difficult than the approach we shall take that pertains only to the classical groups.

In any case if one wishes to understand the classical groups properly, one should really understand both approaches as each yields different insight.[2] In this course we will not discuss the approach of Chevalley, but we refer the interested reader to the beautiful book of Carter [Car89].

1.1. **Prerequisites.** I assume that you have done a basic course in group theory and are familiar with the statements of the isomorphism theorems, Lagrange's theorem, Sylow's theorems and the concept of a group action. I also assume that you have seen a definition of the *sign* of a permutation, and have met the symmetric group, $\mathrm{Sym}(\Omega)$, and the alternating group, $\mathrm{Alt}(\Omega)$, for a set Ω.

1.2. **Acknowledgments and sources.** Writing this course has given me an excuse to read a great deal of beautiful mathematical writing, for which I am very grateful.

I want to record in particular the extensive use I have made of unpublished lecture notes of Jan Saxl (Cambridge), Tim Penttila (UWA, now Colorado) and Michael Giudici (UWA), as well as published work (or work available online) of Peter Cameron [Cama, Camb], Dixon and Mortimer [DM96], Joanna Fawcett [Faw] and Harold Simmons [Sim].

The just-cited texts are all well worth reading. The keen student may also be interested in the following:

(1) *La géométrie des groupes classiques* by Jean Dieudonné[Die63]. This is a classic, written in French.
(2) *The subgroup structure of the finite classical groups* by Kleidman and Liebeck[KL90]. This proves a refined version of Aschbacher's theorem on the subgroup structure of the finite classical groups. It also contains a wealth of other information on these groups (and other almost simple groups).
(3) *The geometry of the classical groups* by Donald Taylor [Tay92]. This covers all the material in the second half of this course plus a fair bit more.
(4) *Finite permutation groups* by Wielandt. Another classic which gives a good sense of the major themes in the development of the theory of finite permutation groups.

[2]This is most clearly exhibited when one studies the subgroup structure of the classical groups. Subgroups that are not almost simple are exhibited very clearly by the theorem of Aschbacher [Asc84] which uses the classical theory of Jordan, whereas almost simple groups are often most clearly seen using the approach of Chevalley et al.

2. A little category theory

A *category* $\mathbf{C}$ consists of

- a class *Obj* of entities called *objects*.
- a class *Arw* of entities called *arrows*.
- two assignments *source* : $Arw \longrightarrow Obj$ and *target* : $Arw \longrightarrow Obj$. These assignments are represented in the obvious way:
$$A \xrightarrow{f} B$$
indicates that f is an arrow with *source* A and *target* B.
- an assignment $1 : Obj \longrightarrow Arw$ which, given an object A in $\mathbf{C}$, yields an arrow 1_A satisfying
$$A \xrightarrow{1_\mathrm{A}} A$$
(In other words the *source* and *target* assignments of the distinguished arrow 1_A are A itself.)
- a partial composition $Arw \times Arw \longrightarrow Arw$ which has the following range of definition: Two arrows
$$A \xrightarrow{f} B_1 \text{ and } B_2 \xrightarrow{g} C$$
are composable, in that order, precisely when B_1 and B_2 are the same object. The resulting arrow has form
$$A \xrightarrow{fg} C.$$

In addition the category $\mathbf{C}$ must satisfy the following conditions:

(C1) Suppose we are given a diagram as follows:
$$A \xrightarrow{f} B \xrightarrow{g} C \xrightarrow{h} D.$$
We require that $(fg)h = f(gh)$. (In other words, composition is associative.)

(C2) Consider an arbitrary arrow f and the two compatible identity arrows, as follows:
$$A \xrightarrow{1_A} A \xrightarrow{f} B \xrightarrow{1_B} B.$$
We require that $f1_B = f = 1_A f$.

Some notes:

- We use words like ‘class’ and ‘assignment’ to allow for the possibility that *Obj* and *Arw* are not sets. If they were sets (in which case $\mathbf{C}$ is called a *small category*), then ‘assignment’ would be the same as ‘function’.
- When we write ‘fg’ for the composition of arrows f and g, we are simply fixing some notation – do not confuse this with composition of functions (although for many categories, arrows are indeed functions of a kind). You should also note our ordering which is somewhat unconventional, but which is chosen to be consistent with our later convention of studying groups *acting on the right*.
- A final piece of notation: given two objects A and B in $\mathbf{C}$, we write $\mathrm{Hom}_{\mathbf{C}}[A, B]$ for the class of all arrows with source A and target B, and we call this the *hom-class from A to B*.

2.1. **Examples of categories.** We briefly discuss some examples of categories. The first type we shall study – categories of structured sets – are far and away the easiest. In fact we will not use any other type of category in our ensuing work, but it will be worth at least mentioning some other types for the sake of our mathematical education.

2.1.1. *Structured sets.* In these categories, each object is a 'structured set', i.e. a set equipped with some extra gadgetry, and arrows are functions between the carrying sets which respect this gadgetry. Rather than making such a notion precise[3], let us list some examples:

Example 1.

Category	Objects	Arrows
Set	sets	functions
Pfn	sets	partial functions
Grp	groups	morphisms
AGrp	abelian groups	morphisms
Rng	rings	morphisms
Field	fields	morphisms
Pos	posets	monotone maps
Top	topological spaces	continuous maps
$\mathbf{Vect}_K$	vector spaces over a field K	linear transformation
$\mathbf{Mod}-R$	right R-modules over a ring R	morphisms
$R-\mathbf{Mod}$	left R-modules over a ring R	morphisms

(E2.1) *Prove that* **Set**, **Pfn**, **Grp**, **Top** *and* $\mathbf{Vect}_K$ *are categories.*

D is a *subcategory* of a category **C** if the class of objects (resp. arrows) of **D** is a subset of the class of objects (resp. arrows) of **C** and, moreover, **D** is a category. **D** is a *full subcategory* of a category **C** if it is a subcategory and, moreover, if for all objects X, Y of **D**, $\mathrm{Hom}_{\mathbf{D}}[X,Y] = \mathrm{Hom}_{\mathbf{C}}[X,Y]$.

(E2.2) *Which categories in Example 1 are (full) subcategories of some other category in Example 1?*

Another example of a structured-set category that is well-studied within permutation group theory is the following:

Example 2. Our category is called **SimpleGraph**.

Objects: An object is a pair (V, E) where V is a set (the 'vertices') and E is a set of subsets of V, each element of E having cardinality at most 2 (the 'edges').

Arrows: Consider an arrow

$$(V, E) \xrightarrow{f} (V', E').$$

Then f is just a function $V \to V'$ such that

$$\{e_1, e_2\} \in E \implies \{f(e_1), f(e_2)\} \in E'.$$

In combinatorics, f would be called a a *graph morphism*.

An easy variant of **SimpleGraph** is the category **SimpleDigraph** whose objects are 'directed graphs'. In this category objects are pairs (V, E) where V is a set and E is a multiset of ordered pairs of elements of V. One defines arrows in the obvious way.

(E2.3) *Complete the definition of* **SimpleDigraph** *and prove that it is a category.*

(E2.4) *Give the 'right' definition of the category* **Graph** *corresponding to graphs that are not necessarily simple, i.e. which may have multiple edges between vertices.*

The final such structured-set category we consider will turn out to be important in the second half of the course when we study the classical groups.

Example 3. Let us begin with the category $\mathbf{Vect}_K$ defined above. We will study a couple of variants of $\mathbf{Vect}_K$:

Variant 1: More arrows

A *semilinear transformation* from V to W is a map $T : V \to W$ such that

[3]The precise notion is that of a *concrete category*. This is a category equipped with a faithful functor to the category **Set**.

(1) $(v_1 + v_2)T = v_1T + v_2T$ for all $v_1, v_2 \in V$;
(2) there exists an automorphism α of k such that

$$(cv)T = c^\alpha(vT)$$

for all $c \in k, v \in V$.[4]

Our new category is called $\mathbf{VectS}_K$. The objects are vector spaces over K; arrows are semilinear transformations. Clearly $\mathbf{Vect}_K$ is a subcategory of $\mathbf{VectS}_K$.

Variant 2: Dot product

Let us specify $K = \mathbb{R}$ (an analogous discussion holds for $K = \mathbb{C}$). If V is a finite-dimensional vector space over $\mathbb{R}$, then V can be equipped with a Euclidean inner product as follows: choose a basis $\{b_1, \dots, b_n\}$ for V and define the inner product of two vectors $x, y \in V$ to be

$$x \cdot y := \sum_{i=1}^{n} x_i y_i,$$

where $x = \sum x_i b_i$ and $y = \sum y_i b_i$.[5]

We will define three new categories. All have the same set of objects: these are pairs $(V, \cdot)$ where V is a finite dimensional vector space over $\mathbb{R}$ and $\cdot$ is a Euclidean inner product on V (in other words, objects are *Euclidean spaces*).

$\mathbf{IVect}_\mathbb{R}$: an arrow $(V_1, \cdot) \xrightarrow{f} (V_2, \cdot)$ is a linear transformation $f : V_1 \to V_2$ such that, for all $v, w \in V_1$,

$$vf \cdot wf = v \cdot w.$$

Note that the dots on each side of this equation represent different inner products.

$\mathbf{SVect}_\mathbb{R}$: an arrow $(V_1, \cdot) \xrightarrow{f} (V_2, \cdot)$ is a linear transformation $f : V_1 \to V_2$ for which there exists a $c \in \mathbb{R}$ such that for all $v, w \in V_1$,

$$vf \cdot wf = c(v \cdot w).$$

$\mathbf{SSVect}_\mathbb{R}$: an arrow $(V_1, \cdot) \xrightarrow{f} (V_2, \cdot)$ is a semilinear transformation $f : V_1 \to V_2$ for which there exists a $c \in \mathbb{R}$ such that for all $v, w \in V_1$,

$$vf \cdot wf = c(v \cdot w).$$

The reason for the names of these categories will become clear when we come to the study of isomorphisms.

(E2.5) *Prove that* $\mathbf{VectS}_K$ *and* $\mathbf{IVect}_\mathbb{R}$ *are categories.*

Our final example is not exactly a category of structured sets, but it has very much the same flavour. It will be crucial in what follows.

Example 4. Our category is called $\mathbf{G} - \mathbf{Set}$.

Objects: An object is a triple (G, Ω, ϕ) where G is a group, Ω is a set and ϕ is an action of G on ϕ, i.e. ϕ is a map $G \times \Omega \to \Omega$ satisfying the usual axioms.

Arrows: An arrow $(G, \Omega, \phi) \longrightarrow (H, \Gamma, \psi)$ is a pair (α, β) where $\alpha : G \to H$ is a group morphism and $\beta : \Omega \to \Gamma$ is a total function. We require moreover that the following diagram commutes:

---

[4]We will formally define the notion of 'automorphism' for a category $\mathbf{C}$ shortly; in particular a *field automorphism* is an automorphism for the category **Field**. For now it may help to consider the example $K = \mathbb{C}$ and consider the complex-conjugation map $z \to \overline{z}$. This is a field automorphism of $\mathbb{C}$.

[5]A better definition of a Euclidean inner product is that it is a non-trivial bilinear map $V \times V \to \mathbb{R}$. (This is 'better' because it does not involve a choice of basis.)

$$\begin{tikzcd} G \times \Omega \arrow[r, "\phi"] \arrow[d, "(\alpha,\beta)"'] & \Omega \arrow[d, "\beta"] \\ H \times \Gamma \arrow[r, "\psi"] & \Gamma \end{tikzcd}$$

(E2.6) *Prove that **G-Set** is a category.*

2.1.2. *More exotic categories.* The categories that we have met so far are all of a sort. Category theory was developed not to deal with these, but to deal with categories that crop in far more exotic ways. So one might consider, say, function categories, or categories of presheaves of a given category, or categories of chain complexes, etc.

Rather than discuss the aforementioned exotic categories which are important for many reasons, I will discuss an unimportant example that has the advantage of being easy to define and gives a tiny flavour of what is possible.

Example 5. The objects are finite sets. An arrow

$$A \xrightarrow{f} B$$

is a function

$$f : A \times B \to \mathbb{R}.$$

For each pair of arrows,

$$A \xrightarrow{f} B \xrightarrow{g} C,$$

we define

$$fg : A \times C \to \mathbb{R},\ (a, c) \mapsto \sum_{b \in B} f(a, b)g(b, c).$$

(E2.7) *Prove that Example 5 yields a category.*

2.2. **Isomorphisms and automorphisms.** A pair of arrows

$$A \xrightarrow{f} B \text{ and } B \xrightarrow{g} A$$

such that

$$fg = 1_A \text{ and } gf = 1_B$$

form an *inverse pair of isomorphisms*. Each arrow is an isomorphism.

An arrow

$$A \xrightarrow{f} A$$

(i.e. an arrow with *source* and *target* equal) is called an *endormorphism*. An arrow that is both an endomorphism and an isomorphism is called an *automorphism*.

Given an object X, the set of all automorphisms of X is a group under composition. We call this group *the automorphism group of* X and denote it $\mathrm{Aut}(X)$.

Consider the specific situation when X is an object in C, a category of structured sets. Thus X can be thought of as a set (which we call Ω for now, to distinguish it from X), plus some extra gadgetry, the 'furnishings' of the object. An automorphism of X will necessarily be a permutation of the underlying set Ω. This means, in particular, that $\mathrm{Aut}(X)$ is group-isomorphic to a subgroup of $\mathrm{Sym}(X)$, the symmetric group on X.

Example 6. In many cases $\mathrm{Aut}(X)$ is an object we have encountered before. For example

Category	$\mathrm{Aut}(X)$
Set	$\mathrm{Sym}(X)$, the symmetric group on X
Grp	$\mathrm{Aut}(X)$
Top	???
$\mathbf{Vect}_K$	$\mathrm{GL}(X)$, the general linear group of X

(E2.8) *What is* $\mathrm{Aut}(X)$ *when* X *is an object in* **Top***?*

In a category an arrow $A \xrightarrow{f} B$ is called

- *monic* if, for each pair of arrows $X \underset{h}{\overset{g}{\rightrightarrows}} A$, we have
$$gf = hf \Longrightarrow g = h;$$
- *epic* if, for each pair of arrows $B \underset{h}{\overset{g}{\rightrightarrows}} X$, we have
$$fg = fh \Longrightarrow g = h.$$

(E2.9) *Show that*

(1) *an isomorphism is monic and epic;*
(2) *if C is a structured set (so that each arrow is carried by a total function between the carriers of the two objects), then*
$$\textit{injective} \Longrightarrow \textit{monic, and surjective} \Longrightarrow \textit{epic};$$
(3) *epic does not imply surjective in* **Ring***;*
(4) *bijective does not imply isomorphism in* **Top***.*

Example 7. An isomorphism in **G-Set** is a *permutation isomorphism*. We will discuss these in greater detail in due course.

Example 8. If $X = (V, E)$ is an object in **SimpleGraph**, then $\mathrm{Aut}(X)$, the group of automorphisms of the graph X, is the set of all bijective functions $f : V \to V$ that are arrows in **SimpleGraph** and whose inverse is an arrow in **SimpleGraph**.

(E2.10) *What are automorphisms in* **Graph***? Can you see why one needs a different definition in this context?*

Example 9. Consider the variants on $\mathbf{Vect}_K$ which we defined earlier. For the first objects V are vector spaces, for the remaining three, objects $\mathbb{R}^n$ are Euclidean spaces (real vector spaces equipped with a Euclidean inner product).

(1) $\mathbf{VectS}_K$: $\mathrm{Aut}(V)$ is the set of all invertible semilinear transformations of V, often denoted $\Gamma\mathrm{L}(V)$.
(2) $\mathbf{IVect}_{\mathbb{R}}$: an arrow is an invertible linear transformation $f : V \to V$ such that $vf \cdot wf = v \cdot w$ for all $v, w \in V$. In other words f is an *isometry* of $\mathbb{R}^n$, and $\mathrm{Aut}(\mathbb{R}^n)$ is the *orthogonal group* of $\mathbb{R}^n$, denoted $O(\mathbb{R}, n)$ or, simply $O(n)$ in the literature.
(3) $\mathbf{SVect}_{\mathbb{R}}$: an arrow is an invertible linear transformation $f : V \to V$ for which there exists $c \in \mathbb{R}$ such that $vf \cdot wf = c(v \cdot w)$ for all $v, w \in V$. In other words f is a *similarity* of $\mathbb{R}^n$, and $\mathrm{Aut}(\mathbb{R}^n)$ is the *similarity group of* $\mathbb{R}^n$.
(4) $\mathbf{SSVect}_{\mathbb{R}}$: an arrow is an invertible semilinear transformation $f : V \to V$ for which there exists $c \in \mathbb{R}$ such that $vf \cdot wf = c(v \cdot w)$ for all $v, w \in V$. In other words f is a *semisimilarity* of $\mathbb{R}^n$, and $\mathrm{Aut}(\mathbb{R}^n)$ is the *semisimilarity group of* $\mathbb{R}^n$.[6]

[6]This category is, in fact, the same as the previous, since $\mathbb{R}$ admits no automorphisms! Of course this construction will also work for $\mathbb{C}$ or, indeed, any field you care to mention... And in these cases this category is interesting (as we shall see).