n groups

2. Permutation groups

Throughout this section, assume that G is a group that acts (on the right) on some set Ω. Equivalently, there exists a group homomorphism $\phi : G \to \mathrm{Sym}(\Omega)$, the set of permutations on the set Ω. Recall that

- for $\omega \in \Omega$, $G_\omega := \{g \in g \mid \omega^g = \omega\}$, is the *stabilizer* of ω;
- $G_{(\Omega)} := \bigcap_{\omega \in \Omega} G_\omega$ is the *kernel* of the action;
- for $\omega \in \Omega$, $\omega^G := \{\omega^g \mid g \in G\}$ is the *orbit* of ω.

Note that $G_{(\Omega)}$ is precisely the kernel of ϕ.
We say that the action of G on Ω is

- *faithful*, if $G_{\Omega)} = \{1\}$; equivalently, ϕ is a monomorphism and we think of G as a subgroup of $\mathrm{Sym}(\Omega)$;
- *transitive*, if $\omega^G = \Omega$ for some (and hence all) $\omega \in \Omega$.

Remark. When a group theorist speaks of a 'permutation group', they mean an abstract group G accompanied by some fixed embedding of G in $\mathrm{Sym}(\Omega)$, for some set Ω. Equivalently, they mean an abstract group G accompanied by some faithful action. Indeed for a long time this was the only context in which groups were studied, in the immediate aftermath of the work of Galois.

Example 1. Let H be any subgroup of G. The group G acts transitively on $H\backslash G$, the set of right cosets of H via right multiplication.

o action

(E8*) *Prove that any transitive action is isomorphic to an action of this kind, i.e. given a transitive action of G on Ω, there exists a subgroup $H \leq G$ such that the action of G on Ω is isomorphic to the action of G on $H\backslash G$. You may need to recall what it means for two group actions to be isomorphic.*

Recall that when G is finite the Orbit-Stabilizer Theorem asserts that, for all $\omega \in \Omega$,

$$|G| = |G_\omega| \cdot |\omega^G|.$$

(E9) *Use (E8) to prove the orbit-stabilizer theorem.*

tab conj

(E10) *Prove that if G acts transitively on Ω and G_ω is a stabilizer, then the set of all stabilizers equals the set of all conjugates of G_ω. Under what conditions is the action of G by conjugation on this set of conjugates is isomorphic to the action of G on Ω?*

(E11) *What conditions on H result in the action of G on $H\backslash G$ being faithful?*

(E12*) *Let G be a finite group acting transitively on a set Ω. Show that the average number of fixed points of the elements of G is 1, i.e.*

$$\frac{1}{|G|} \sum_{g \in G} |\{\omega \in \Omega \mid \omega^g = \omega\}| = 1.$$

Example 2. Let $3 \leq n \in \mathbb{Z}^+$ and let $G := D_{2n}$, the dihedral group of order $2n$. In other words

$$G := \langle g, h \mid g^n = h^2 = 1, h^{-1}gh = g^{-1} \rangle.$$

Define Ω to be the corners of an n-gon which we might as well label $1, \ldots, n$. We can define g to act like the permutation $(1, 2, \ldots, n)$ and h to reflect the polygon through a line passing through 1; see Figure 1 for an example when $n = 5$. Thus

$$h := (2, n)(3, n-1) \ldots \left(\lfloor \frac{n+2}{2} \rfloor, \lceil \frac{n+2}{2} \rceil \right).$$

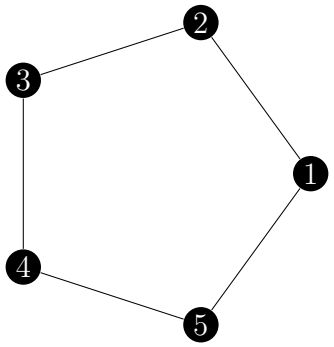

FIGURE 1. D_{10} acts on the pentagon with $g = (1, 2, 3, 4, 5)$ and $h = (2, 5)(3, 4)$.

(E13) *Check that this gives a well-defined action of G on Ω that is both faithful and transitive. What are the stabilizers in this action?*

d10

2.1. **Multiple transitivity.** As soon as we have an action of a group G on a set Ω, we can define others. For instance, define an action of G on $\Omega^2 = \Omega \times \Omega$ via

$$(\omega_1, \omega_2)^g := (\omega_1^g, \omega_2^g),$$

for all $g \in G$.

In fact this defines a natural action on the set of distinct pairs,

$$\Omega^{(2)} := \{(\omega_1, \omega_2) \mid \omega_1 \neq \omega_2\}.$$

We say that the *original* action of G on Ω is 2-*transitive* if the induced action of G on $\Omega^{(2)}$ is transitive. One defines k-*transitivity* for $2 \geq k \in \mathbb{Z}^+$ similarly. It is convenient to define an action to be 1-*transitive* if and only if it is transitive.

(E14*) *For which values of n is the action of D_{2n} on an n-gon, 2-transitive?*

(E15) *Show that, for $k \geq 2$, if an action is k-transitive, then it is $k-1$-transitive.*

(E16) *Let $G = S_n$, the symmetric group on n letters. What is the largest value of k for which G is k-transitive? What about $G = A_n$, the alternating group on n letters?*

2.2. **Blocks and primitivity.** A G-*congruence* on Ω is an equivalence relation $\sim$ on Ω such that

$$\alpha \sim \beta \implies \alpha^g \sim \beta^g$$

for all $g \in G$. Any action always admits two G-congruences which we call *trivial*, as follows:

- Define $\alpha \sim_1 \beta$ if and only if $\alpha = \beta$;
- Define $\alpha \sim_2 \beta$ always.

The equivalence classes of a G-congruence are called *blocks*. Note that, for $\sim_1$, there are $|\Omega|$ blocks all of cardinality 1 while, for $\sim_2$, there is one block of cardinality $|\Omega|$.

The action of G on Ω is called *primitive* if the only G-congruences on Ω are the trivial ones. We call the action *imprimitive* if it is not primitive. (I may also write things like "G acts primitively on the set Ω", and will trust you to figure out what I mean.)

al trans

Lemma 2. *Suppose that G acts primitively on Ω and let $N \trianglelefteq G$ with $N \not\leq G_{(\Omega)}$. Then N acts transitively on Ω.*

Proof. Let $\Lambda_1, \ldots, \Lambda_k$ be the orbits of N on Ω. Define an equivalence relation $\sim$ on Ω such that $\alpha \sim \beta$ if and only if there exists i such that $\alpha, \beta \in \Lambda_i$. Now suppose that $\alpha \sim \beta$. By definition $\beta = \alpha^n$ for some $n \in N$. Let $g \in G$ and observe that

$$\beta^g = (\alpha^n)^g = (\alpha^g)^{g^{-1}ng}.$$

Since N is normal, $g^{-1}ng \in N$ and we conclude that $\alpha^g \sim \beta^g$ and hence $\sim$ is a G-congruence on Ω.

Since G is primitive, $\sim$ must be one of the two trivial G-congruences, $\sim_1$ or $\sim_2$. Since $N \not\leq G_{(\Omega)}$ we conclude that $|\Lambda_i| \geq 2$ for some $i = 1, \ldots, k$ and so $\sim \neq \sim_1$. We conclude that $\sim = \sim_2$ which implies, in particular that $k = 1$ and N acts transitively on Ω.

□

Taking N to equal G in this lemma we observe, in particular, that if $|\Omega| > 2$ and an action is primitive, then it is transitive.

(E17) *Prove that if an action is transitive and $\sim$ is a G-congruence, then all of the blocks associated with $\sim$ have the same cardinality.*

(E18) *Prove that if an action is 2-transitive, then it is primitive.*

(E19*) *Prove that G acts primitively on Ω if and only if G acts transitively and any stabilizer, G_ω, is a maximal subgroup of G.*

2.3. **Iwasawa's Criterion.** The point of the material covered so far has been to allow us to state a famous lemma of Iwasawa which gives a criterion for a finite permutation group to be simple.

iwasawa **Lemma 3.** (Iwasawa's criterion) *Let G be a finite group acting primitively on a set Ω. Let $\omega \in \Omega$ and assume that G_ω has a normal subgroup A which is abelian such that*

$$\langle A^g \mid g \in G \rangle = G$$

If $K \lhd G$, either $K \leq G_{(\Omega)}$ or $G' \leq K$. In particular if G is perfect and faithful on Ω, then G is simple.

(E20) *Use Iwasawa's criterion to show that A_5 is simple.*

(E21*) *Now use Iwasawa's criterion to show that A_n is simple for $n \geq 5$. Hint: consider the action on unordered triples from $\{1, \ldots, n\}$.*

Proof. Let K be a normal subgroup of G that is not contained in $G_{(\Omega)}$. Lemma 2 implies, therefore, that K acts transitively on Ω and hence $G = G_\omega K$ (use the Orbit-Stabilizer Theorem to see this). Thus, for all $g \in G$, there exists $g_1 \in G_\omega, k \in K$ such that $g = g_1 k$ and this implies, in particular, that

$$\{A^g \mid g \in G\} = \{A^k \mid k \in K\}.$$

Now, since $\langle A^k \mid k \in K \rangle \leq AK \leq G$ we conclude that $G = AK$. Then

$$G/K = AK/K \cong A/A \cap K.$$

Since the right hand side is a quotient of an abelian group it must itself be abelian, and we conclude that G/K is abelian. Hence, by (E3), $K \geq G'$. □

(E22*) *Prove the following variant on Iwasawa's criterion: Suppose that G is a finite perfect group acting faithfully and primitively on a set Ω, and suppose that the stabilizer of a point has a normal soluble subgroup S, whose conjugates generate G. Then G is simple.*

s: sdp

2.4. **Groups acting on groups.** Given a group G with a composition series, one can (in theory) calculate its composition factors. What about the reverse process? Suppose we are given a multiset of composition factors, how does one construct a group G to which they correspond? In general there are many ways to do this, and we briefly outline one such here.[1]

Let H and K be groups. Recall that an *automorphism* of K is simply a group isomorphism $K \to K$. The set of all automorphisms of K forms a group, which we label $\mathrm{Aut}(K)$. Now let $\phi : H \to \mathrm{Aut}(K)$ be a group homomorphism. We define $G := K \rtimes_\phi H$ to be the group whose elements are the elements of $H \times K$, with group multiplication given by

$$(h_1, k_1)(h_2, k_2) = (h_1 \cdot h_2, k_1^{\phi(h_2)} \cdot k_2).$$

(E23*) *Check that this gives a well-defined group. If ϕ is the trivial homomorphism, what is $K \rtimes_\phi H$?*

The next lemma lists some basic properties of this construction.

Lemma 4. *Let $G = K \rtimes_\phi H$.*

(1) *The subset $K_0 := \{(1, k) \mid k \in K\}$ is a normal subgroup of $K \rtimes_\phi H$ that is isomorphic to K;*
(2) *The subset $H_0 := \{(h, 1) \mid h \in H\}$ is a subgroup of $K \rtimes_\phi H$ that is isomorphic to K;*
(3) *$G/K_0 \cong H$;*
(4) *The natural conjugation action of H_0 on K_0 is isomorphic to the action of H on K given by ϕ.*

Proof. **(E24*)** *Prove this.* □

In what follows I will tend to identify the groups K_0 and K, and the groups H_0 and H. This allows me to abuse notation and think of $K \rtimes_\phi H$ as a semi-direct product of two of its *subgroups*, a point of view that is helpful. Usually, too, the homomorphism ϕ is obvious from the context, so I will tend to write the semidirect product as $K \rtimes H$.

Suppose that G is a group with normal subgroup K such that $G/K \cong H$. In this case we write $G = K.H$ and call G *an extension of K by H*.[2] A semi-direct product $G := K \rtimes H$ is an example of a group $K.H$, but it is important to note that not all groups $K.H$ can be expressed as a semi-direct product. In the literature groups $K.H$ that can be expressed as a semi-direct product are called *split extensions* and are sometimes denoted $K : H$; those that can't be expressed as a semi-direct product are called *non-split extensions*.[3]

Remark. In the particular case where groups K and H are simple, any group $K.H$, in particular any semi-direct product $K \rtimes H$, is an example of a group with composition factors $\{H, K\}$. Thus semi-direct products allow us to 'construct a group from its composition factors', as we set out to do at the start of this section.

(E25) *Find an example of a group $G = K.H$ (where K and H are both non-trivial finite groups) which is non-split. Hint: there is precisely one example with $|G| \leq 7$, and it is abelian. The smallest non-abelian examples have $|G| = 8$.*

(E26) *Write down as many groups as you can which have composition factors $\{C_2, A_6\}$. Identify those that can be written as split extensions.*

[1] This section is a little terse; more detail can be found in [Ros94].

[2] **Warning**: Some authors call this *an extension of H by K*.

[3] If you know about short exact sequences, then this terminology will make sense to you. If you don't, I recommend you look 'em up.

Understanding the automorphism group of a group is sometimes important. For any group G there is a homomorphism

$$\phi : G \to \mathrm{Aut}(G), g \mapsto \phi_g$$

where $\phi_g : G \to G, h \mapsto g^{-1}hg$. In other words, the natural action of a group on itself by conjugation induces a set of group automorphisms. We define $\mathrm{Inn}(G) := \mathrm{Im}(\phi)$ and call $\mathrm{Inn}(g)$ *the set of inner automorphisms of* G.

ut group

Lemma 5. (1) $\mathrm{Inn}(G) \trianglelefteq \mathrm{Aut}(G)$;
(2) $\ker(\phi) = Z(G)$.

Proof. **(E27)** *Prove this.* □

Note, in particular, that if $Z(G)$ is trivial, then G embeds into its own automorphism group. In particular this allows us to define the notion of an *almost simple group*: it is a group G with a simple normal subgroup S such that

$$S \leq G \leq Aut(S).$$

3. Fields and Vector Spaces

We will need some background knowledge concerning linear algebra over an arbitrary field. I will assume that you are familiar with the definition of a field, a vector space, and with some basic facts about polynomials over fields; in particular I will also assume the following basic result, which is *Vandermonde's Theorem.*

of roots

Proposition 6. *Let $f \in k[X]$ be a polynomial of degree $n \geq 0$ with coefficients in a field k. Then f has at most n roots.*

3.1. **A diversion into division rings.** There is a natural definition of the notion of a field, namely a *division ring*, in which one does not require that multiplication is commutative. Much of what will be discussed below applies in this setting but not all. We give an example of a division ring next and briefly mention some things to beware of in this more general setting.

Example 3. The real octonions, $\mathbf{H}$, are defined to be a 4-dimensional vector space over the real numbers, $\mathbb{R}$. Addition is defined to be the usual addition of vectors.

To define multiplication we introduce some notation: we write a vector (a, b, c, d) as $a + bi + cj + dk$, we define multiplication by a vector $a + 0i + 0j + 0k$ as the usual scalar multiplication, we define the multiplication of basis vectors as

$$i^2 = j^2 = k^2 = -1,\ ij = k,\ ji = -k,\ jk = i,\ kj = -i,\ ki = j,\ ik = -j,$$

and we use distributivity to extend this definition so that multiplication is defined for all pairs of octonions.

(E28) *Check that $\mathbb{H}$ is a division ring.*

(E29*) *Show that Proposition 6 does not hold in $\mathbb{H}$.*

One cannot immediately talk of a vector space over a division ring - one distinguishes between *left* and *right* vector spaces. For instance, for a division ring k, a left vector space is a left unital k-module.

Our choice to eschew the generality offered by division rings is justified by our desire to focus on finite fields, and by the following classical result.

Theorem 7. (Wedderburn's theorem) *A finite division ring is a field.*

3.2. **Back to fields.** Throughout this section k is a field; we write $k^* := k\backslash\{0\}$.

t cyclic

Lemma 8. *Any finite subgroup of the multiplicative group $(k^*, \cdot)$ is cyclic.*

Proof. Let H be a minimal non-cyclic subgroup of $(k^*, \cdot)$. Our knowledge of abelian groups implies that $H \cong C_p \times C_p$ for some prime p. Now every element of H satisfies the polynomial $X^p = 1$ which is a contradiction of Proposition 6. □

Of course, if k is finite, then this result implies that $(k^*, \cdot)$ is cyclic. In this case we call those elements of k^* that generate $(k^*, \cdot)$ the *primitive elements*.

Example 4. Let p be a prime and define $\mathbb{F}_p := \mathbb{Z}/p\mathbb{Z}$, the integers modulo p, with the usual addition and multiplication. Then $\mathbb{F}_p$ is a field.

r fields

Lemma 9. *Let $q = p^a$ where p is a prime and a is a positive integer. Then there exists a finite field of order q.*

Proof. (Sketch) The previous example gives the result for $a = 1$. Now let $f(X) \in \mathbb{F}_p[X]$ be an irreducible monic polynomial of degree at least 2. Since $\mathbb{F}_p[X]$ is a Principal Ideal Domain we conclude that $I := \langle f(X)\rangle$ is a maximal ideal of $\mathbb{F}_p[X]$ and we conclude that $\mathbb{F}_p[X]/I$ is a field. Since every element of $\mathbb{F}_p[X]/I$ contains a unique (and distinct) polynomial of degree less than a, we conclude that $\mathbb{F}_p[X]/I$ is a field of order p^a.

It remains to show that, for every p and every $a > 1$, there exists a monic irreducible polynomial of degree a over $\mathbb{F}_p$. We omit this part. □

A variant of the preceding result, using the theory of splitting fields can be found at https://kconrad.math.uconn.edu/blurbs/galoistheory/finitefields.pdf

Given a monic irreducible $f(X) \in \mathbb{F}_p[X]$, one can do computations in $F := k[X]/\langle f(X)\rangle$ by observing that

$$F := \{c_{a-1}X^{a-1} + c_{a-2}X^{a-2} + \cdots + c_1X + c_0 + \langle f(x)\rangle \mid c_0, \ldots, c_{a-1} \in \mathbb{F}_p\}.$$

(We are using the fact, mentioned in the proof, that every element of $\mathbb{F}_p[X]/I$ contains a unique (and distinct) polynomial of degree less than a.)

Now one represents the element $c_{a-1}X^{a-1} + c_{a-2}X^{a-2} + \cdots + c_1X + c_0 + \langle f(x)\rangle \in F$ by the string

$$c_{a-1}\alpha^{a-1} + c_{a-2}\alpha^{a-2} + \cdots + c_1\alpha + c_0$$

where α is just a convenient symbol. Addition and multiplication on the resulting set of polynomials in α are just the usual addition and multiplication of polynomials, with the extra rule that $f(\alpha) = 0$.

(E30*) *Show that $X^2 + 1 \in \mathbb{F}_3[X]$ is irreducible, and compute the addition and multiplication tables for $\mathbb{F}_9 := \mathbb{F}_3[x]/\langle X^2 + 1\rangle$.*

(E31*) *Show that $X^3 + X + 1 \in \mathbb{F}_2[X]$ is irreducible, and compute the addition and multiplication tables for $\mathbb{F}_8 = \mathbb{F}_2[x]/\langle X^3 + X + 1\rangle$.*

er order

Lemma 10. *Any finite field k has order p^a where p is a prime and a is a positive integer.*

Proof. Consider the set

$$k_0 := \{1, 1 + 1, 1 + 1 + 1, \ldots\}.$$

This is a closed subring of k of order n, say. Furthermore, $k \cong \mathbb{Z}/n\mathbb{Z}$. Now, since k contains no zero-divisors, neither does k_0 and so $n = p$, a prime. This implies that k_0 is a subfield of k of order p and so k is a vector space over k_0 of dimension a, say. Thus $|K| = p^a$ as required. □

Note that we have shown that k has a unique subfield, k_0, of order p. This is the *prime subfield* of k, and any subfield of k must contain k_0 (as is clear from its definition).

The following theorem summarizes some of what we have proved about finite fields so far. The last phrase "and is unique up to isomorphism" has not been proved, but we will take it as a fact in what follows.

e fields

Theorem 11. *For every prime p and every positive integer a, there is a finite field of order $q = p^a$. This field is unique up to isomorphism.*

In what follows we will write $\mathbb{F}_q$ for the field of order $q = p^a$. We close this section with a useful result that we prove using Galois theory.

elds aut

Proposition 12. *Let $q = p^a$.*

1. *The automorphism group of $\mathbb{F}_q$ is cyclic of of order a, and is generated by the* Frobenius automorphism*, $\sigma : x \mapsto x^p$.*
2. *For every divisor b of a, there is a unique subfield of $\mathbb{F}_q$ of order p^b, consisting of all solutions of $x^{p^b} = x$, and these are all the subfields of $\mathbb{F}_q$.*

Proof. Write $\mathbb{F}_p$ for the prime subfield of $\mathbb{F}_q$, and observe that the degree of $\mathbb{F}_q$ over $\mathbb{F}_p$ is a. The Frobenius map, σ, is an $\mathbb{F}_p$-automorphism of $\mathbb{F}_q$, and has order a. Thus $\mathrm{Aut}(\mathbb{F}_q/\mathbb{F}_p) \geq a = |\mathbb{F}_q : \mathbb{F}_p|$.

By Galois theory we know that, given a field extension K/F, $\mathrm{Aut}(K/F) \leq |K : F|$ with equality if and only if K/F is a Galois extension. We conclude that $\mathbb{F}_q$ is a Galois extension of Fp and that

$$\mathrm{Aut}(\mathbb{F}_q/\mathbb{F}_p) = \mathrm{Gal}(\mathbb{F}_q/\mathbb{F}_p) = \langle\sigma\rangle \cong C_a,$$

the cyclic group of order a.

The subgroups of $\langle\sigma\rangle$ are $\langle\sigma^{a/b}\rangle$ where b ranges through the divisor of a, and Galois theory implies that the subfields of $\mathbb{F}_q$ are, therefore, the the fixed fields of $\sigma^{a/b}$, as b ranges through the divisors of a. These are precisely the subfields of order p^b consisting of all solutions of $x^{p^b} = x$. □

3.3. **Vector spaces.** Let V and W be vector spaces over some field k. A *semilinear transformation* from V to W is a map $T : V \to W$ such that

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 $c \in k, v \in V$.

The automorphism α is called the *associated automorphism* of T. If T is not identically zero, then α is uniquely determined by T. If $\alpha = 1$ then T is a *linear transformation* between V and W.

We are mainly interested in the situation where $V = W$ (in which case we talk of 'semilinear transformations on V'). In this case if T is one-to-one and onto, then the inverse map is also a semilinear transformation and we say that T is *invertible*.

We can think of semilinear transformations on V in a different way: first fix a basis B of V. if α is an automorphism of K, then extend the action to V coordinate-wise, by defining

$$(c_1, \ldots, c_n)^\alpha := (c_1^\alpha, \ldots, c_n^\alpha).$$

We call this a *field automorphism of V with respect to B*; note that it is, in particular, a semilinear transformation from V to V.

Lemma 13. *Fix a basis B of V. Any semilinear transformation on V is a composition of a linear transformation and a field automorphism of V with respect to B.*

(E32*) *Prove this.*

Suppose that V has dimension n over k; recall that all vector spaces of dimension n over k are mutually isomorphic (this will justify our next notation). We define

(1) $\mathrm{E}nd(V)$, or $\mathrm{M}_n(k)$, to be the set of all linear transformations on V;
(2) $\mathrm{GL}(V)$, or $\mathrm{GL}_n(k)$ is the set of all invertible linear transformations on V;
(3) $\mathrm{SL}(V)$, of $\mathrm{SL}_n(k)$ is the set of all linear transformations on V of determinant 1;
(4) $\Gamma\mathrm{L}(V)$, or $\Gamma\mathrm{L}_n(k)$ is the set of all invertible semilinear transformations on V.

All of these are groups under the operation of composition. All act naturally on the vector space V (hence our decision to define transformations on the right).

(E33*) *Prove that* $\Gamma\mathrm{L}_n(k) \cong \mathrm{GL}_n(k) \rtimes_\phi \mathrm{Aut}(k)$. *You will need to choose an appropriate homomorphism* $\phi : \mathrm{Aut}(k) \to \mathrm{Aut}(\mathrm{GL}_n(K))$ *to make this work. You may find it convenient to fix a basis for* V *– so you can express elements of* $\mathrm{GL}_n(k)$ *as matrices – before you choose* ϕ.