Topics in group and representation theory

Narmada Varadarajan

A "note"

Contents

1 Preliminaries **2**
- 1.1 Subgroup structures . . . 2
- 1.2 Important examples of groups . . . 2
- 1.3 Group homomorphisms . . . 3
- 1.4 Important types of groups and subgroups . . . 5
- 1.5 Group actions . . . 7
- 1.6 Sylow's theorems . . . 8

2 Group structures **8**
- 2.1 Free groups . . . 8
- 2.2 Permutation groups . . . 11
- 2.3 Groups of linear transformations . . . 13
- 2.4 Group extensions . . . 16
- 2.5 p-groups . . . 18

3 Nilpotent and solvable groups **21**
- 3.1 Nilpotent groups . . . 21
- 3.2 Solvable groups . . . 23
- 3.3 The Three-Subgroup Lemma . . . 24
- 3.4 Hall's theorems . . . 26
- 3.5 Supersolvable groups . . . 27

4 Permutation groups **29**
- 4.1 Primitive permutation groups . . . 30
- 4.2 Minimal normal subgroups . . . 31
- 4.3 Wreath products . . . 34
- 4.4 Classification of primitive permutation groups . . . 36
- 4.5 Subgroups of S_n . . . 38

5 Representations of finite groups **39**
- 5.1 Irreducible representations and Maschke's theorem . . . 39
- 5.2 The group algebra . . . 41
- 5.3 Characters and class functions . . . 43
- 5.4 Inner products of characters . . . 44
- 5.5 Induced representations . . . 47

6 Applications of representation theory **49**
6.1 Burnside's theorem . . . 49
6.2 The Frobenius kernel . . . 51
6.3 Induced characters . . . 53
6.4 The order of a finite simple group . . . 53
6.5 Representations of S_n . . . 56
6.6 $SU(2)$ and $SO(3)$ . . . 60

7 Infinite groups **61**
7.1 Burnside groups . . . 61
7.2 Divisible groups . . . 65
7.3 Infinite abelian groups . . . 66
7.4 Free abelian groups . . . 67

References **69**

Index **70**

1 Preliminaries

The purpose of this section is to present key concepts that we will need to use indiscriminately in later sections. Let us keep it brief and proof-free to maximise efficiency. It is assumed that anyone hoping to make sense of this note has taken a first course in group theory, and knows, for example, the definition of a group. We typically write group operations multiplicatively, because most of the groups we deal with will be nonabelian (and it is ridiculous to say $a + b \neq b + a$ additively).

1.1 Subgroup structures

Given a subgroup $H \leq G$, the relation "$x \sim y$ if and only if $xy^{-1} \in H$" defines an equivalence relation. The equivalence classes are called the *left* (resp. *right*) *cosets* of H in G, and are $xH = \{xh : h \in H\}$ (resp. $Hx = \{hy : h \in H\}$). Denote by $|G : H|$ the *index* of H in G, the number of left (resp. right) cosets. From this, we get

Theorem 1.1 (Lagrange's theorem)**.** *If $H \leq G$ are finite groups, $|H|$ divides $|G|$.*

Call $|G|$ the *order* of G. For $S \subset G$, let $\langle S\rangle$ denote the subgroup of G generated by S. When $S = \{x\}$, then $\langle S\rangle = \{x^n : n \in \mathbb{N}\}$. Define the *order* of $x \in G$ as $\operatorname{ord}(x) = \big|\langle x\rangle\big|$.

A group G is called abelian if $xy = yx$ for all $x, y \in G$. A group G is called *cyclic* if $G = \langle x\rangle$; it is clear that every cyclic group is abelian. It is less clear, but true, that every subgroup of a cyclic group is cyclic.

A corollary to Lagrange's theorem is that the order of any element divides the order of the group, so $|G| = n$ implies $g^n = 1$. We say a group is *torsion* if every element has finite order, and *torsion-free* if every element has infinite order.

An exercise in elementary combinatorics says

Proposition 1.2. *If $|G|$ is even, G has an element of order 2.*

The following theorem can also be proven combinatorially,

Theorem 1.3 (Cauchy's theorem)**.** *If a prime p divides the order of G, then G has an element of order p.*

1.2 Important examples of groups

Since we will mostly only study finite groups, the reader should be familiar with the following examples.

(1) For each $n \in \mathbb{N}$, the finite group $\mathbb{Z}_n$ is the set of integers modulo n with addition; this is cyclic.

(2) $\mathbb{Z}_n^\times$, the set of *nonzero* integers coprime to n is a multiplicative group of order $\phi(n)$, where ϕ is the Euler totient function. This is abelian, but not always cyclic[1].

(3) An important related group is the *Klein-four group*, $\mathbb{Z}_2 \times \mathbb{Z}_2$, denoted by V_4.

(4) The *symmetric group of order n*, denoted $\mathrm{Sym}(n)$ or S_n is the group of permutations of n elements. For $n \geq 3$, this is nonabelian. $|S_n| = n!$.

For distinct elements $a_1, \cdots, a_k \in [n]$, let $(a_1 \ldots a_k)$ denote the permutation in S_n that sends $a_i \longrightarrow a_{i+1}$ for $1 \leq i \leq k$, (where $a_{k+1} := a_1$), and fixes all other elements of $[n]$. The permutation (123), for example, denotes the permutation that sends $1 \longrightarrow 2$, $2 \longrightarrow 3$, $3 \longrightarrow 1$, and fixes all other elements. A permutation $\sigma \in S_n$ is called a *k-cycle* if it is of the form $(a_1 a_2 \ldots a_k)$. A permutation $\tau \in S_n$ is called a *transposition* if it is a 2-cycle.

Exercise 1. Disjoint cycles commute.

Exercise 2. Every permutation in S_n has a *cycle decomposition* into a product of disjoint cycles, and this is unique upto reordering.

Exercise 3. The order of a permutation is the least common multiple of the cycle lengths in its cycle decomposition. A permutation $\pi \in S_n$ has prime order p if and only if it is the product of disjoint cycles of length p.

(5) The *alternating group of order n*, A_n, is the subgroup of all permutations that can be written as a product of an even number of transpositions.[2] $|A_n| = n!/2$.

(6) The *dihedral group of order n*, which we will denote by D_n – although some books write D_{2n} – is the group of symmetries of a regular n-gon. This is generated by the rotation r and the reflection s, satisfying

$$D_n = \langle r, s \mid r^n = s^2 = 1, rs = sr^{-1} \rangle.$$

It is clear from the definition that D_n is nonabelian. Further, $|D_n| = 2n$, and it can be written as the set

$$D_n = \{s^i r^j : i = 0, 1, j = 0, \ldots, n-1\}.$$

Along with V_4, the groups $\mathbb{Z}_n : n \leq 5$ make up all groups of order ≤ 5, so every group of order ≤ 5 is abelian. Typically, if we want to prove something for finite groups by induction, the base case $n \leq 5$ will follow trivially from this fact, so it is worth keeping in mind.

Matrix groups will later play an important role. Denote by $GL(V)$ the group of invertible linear transformations of a vector space V, under multiplication; this is the *general linear group*. The *special linear group* $SL(V)$ denotes the subgroup of matrices of determinant 1. When V is a d-dimensional vector space over a field F, we denote these by $GL(d, F)$ and $SL(d, F)$ respectively.

Exercise 4. If $\dim V \geq 2$, $GL(V)$ is not abelian.

1.3 Group homomorphisms

The most simple operations to construct a group (defined here in their most general forms) are the *direct sum* and *direct product*. Given a collection of groups $(G_i)_{i \in I}$, define

$$\bigoplus_{i \in I} G_i = \Big\{ (g_i)_{i \in I} : g_i \in G_i, \text{ and at most finitely many of the } g_i \text{ are not equal to the identity} \Big\}.$$

$$\prod_{i \in I} G_i = \Big\{ (g_i)_{i \in I} : g_i \in G_i \Big\}.$$

[1] $\mathbb{Z}_n^\times$ is cyclic if and only if $n = 2, 4, p^k$ or $2p^k$ for an odd prime p and $k \in \mathbb{N}$.

[2] This definition conceals a nontrivial fact – that the transpositions generate S_n, and that each element is the product of either and even or an odd number of transpositions, but not both.

A finite direct sum is always equal to the finite direct product, so we simply write

$$\bigoplus_{i=1}^{k} G_i = \prod_{i=1}^{k} G_i = G_1 \times \cdots \times G_k.$$

Conversely, can we "build up" any group from "smaller" groups? This is what motivates the definition of a *normal subgroup*.

Definition 1.4. N is a *normal subgroup* of G, denoted $N \lhd G$, if $\forall g \in G$, $gNg^{-1} \subset N$.

Equivalently, say $x \sim y$ if for some $g \in G$, $x = gyg^{-1}$. We say x and y are *conjugate* (in G), and the equivalence classes of this relation are called *conjugacy classes*. Then N is a normal subgroup of G if and only if N is a subgroup and N is a union of conjugacy classes.

Exercise 5. If G is a direct sum of groups $G = A \times B$, then $A \lhd G$ and $B \lhd G$.

Exercise 6. Every subgroup of an abelian group is normal.

Proposition 1.5. *Any subgroup of index* 2 *is normal.*

Why are normal subgroups important?

Definition 1.6. A function $\varphi : G \longrightarrow H$ is a *(group) homomorphism* if $\varphi(gh) = \varphi(g)\varphi(h)$ for all $g, h \in G$. If φ is also a bijection, call it an *isomorphism*, and write $G \cong H$.

Given $N \leq G$, we can define a natural operation on the set of cosets G/N by

$$(gN)(hN) = (gh)N.$$

This is well-defined if and only if N is a normal subgroup, in which case we call G/N a *quotient group* of G.

That is, given a homomorphism $\varphi : G \longrightarrow H$, define its kernel

$$\ker\varphi = \{g \in G : \varphi(g) = 1\}.$$

$\ker\varphi$ is a normal subgroup of G, and this is a one-to-one correspondence between normal subgroups of G and kernels of homomorphisms of G.

(*) For $n \in \mathbb{N}_{>0}$, the map $\pi_n : \mathbb{Z} \longrightarrow \mathbb{Z}_n$, $\pi_n(a) = a \mod n$ is a homomorphism $\mathbb{Z} \longrightarrow \mathbb{Z}_n$. Its kernel is the subgroup $n\mathbb{Z}$.

(*) A_n is the kernel of the *sign* homomorphism $S_n \longrightarrow \{\pm 1\} \cong \mathbb{Z}_2$, which sends a permutation to -1 if it is the product of an odd number of transpositions, and 1 otherwise.

(*) $SL(V)$ is the kernel of the determinant homomorphism $\det : GL(V) \longrightarrow F$, the base field.

Exercise 7. If $N \lhd G$ and $H \leq G$, then $N \cap H \lhd H$. If $H \lhd G$, then $N \cap H \lhd G$.

Definition 1.7. We say G is an *extension* of K by H, if G has a normal subgroup isomorphic to K such that the quotient group is isomorphic to H.

Unfortunately, it is not always true that $G \cong N \oplus G/N$.

Exercise 8. For $n \geq 3$, S_n is not isomorphic to $A_n \oplus \mathbb{Z}_2$.[3]

Nevertheless, the three isomorphism theorems, though seemingly simple, prove to be powerful tools.

Theorem 1.8 (First isomorphism theorem)**.** *Let $\varphi : G \longrightarrow H$ be a group homomorphism.*

$$G/\ker\varphi \cong \mathrm{Im}\varphi.$$

[3] S_n does not have a normal subgroup of order 2.

Given two subgroups $H, K \leq G$, define their *product* denote by HK as

$$HK = \{hk : h \in H, k \in K\}.$$

This is not always a subgroup! The subgroup *generated* by H and K will be denoted $\langle H, K \rangle$.

Exercise 9. $H = \{1, s\}$ and $K = \{1, r^2\}$ are subgroups of D_4, but HK is not.

Exercise 10. For $H, K \leq G$, HK is a subgroup of G if and only if $HK = KH$.

Exercise 11. If $K \lhd G$ and $H \leq G$, then HK is a subgroup of G. If $H \lhd G$ as well, then $HK \lhd G$.

Theorem 1.9 (Second isomorphism theorem)**.** *Let $N \lhd G$, and $H \leq G$. Then,*

$$HN/N \cong H/H \cap N.$$

Theorem 1.10 (Third isomorphism theorem)**.** *If H and K are normal subgroups of G such that $H \leq K \leq G$, then K/H is a normal subgroup of G/H, and*

$$G/H \big/ K/H \cong G/K.$$

Exercise 12. There is a one-to-one correspondence between subgroups of G/H and subgroups of G containing H.

Exercise 13. Suppose $H \lhd G$, and for some $K \leq G$, $HK/H \lhd G/H$. Then $HK \lhd G$. That is, any normal subgroup in G/H "lifts" to a normal subgroup in G containing H.

Vigyázz. Suppose $H \leq G$ and $x, y \in H$. Clearly, if x and y are conjugate in H, then they are conjugate in G, but the converse is not true.

Exercise 14. If the cycle decomposition of π in S_n contains l_i cycles of length i, for $1 \leq i \leq n$, define the *cycle type* of π as $(l_1, \ldots, l_n)$. Show that two permutations are conjugate in S_n if and only if they have the same cycle type.[4]

A natural question to ask is: if $M \lhd N$, and $N \lhd G$, is $M \lhd G$? Unfortunately, this is not true.

Exercise 15. $\langle s, r^2 \rangle \lhd D_4$, and $\langle s \rangle \lhd \langle s, r^2 \rangle$, but $\langle s \rangle$ is not normal in D_4.

However, we say a subgroup H is *characteristic* in G, denoted $H \mathrm{char} G$, if H is fixed by every automorphism[5] of G.

Proposition 1.11. *If $M \mathrm{char} N$ and $N \lhd G$, then $M \lhd G$.*

1.4 Important types of groups and subgroups

The theory of finite – in fact, finitely generated – abelian groups is well-studied.

Theorem 1.12 (Fundamental theorem of finitely generated abelian groups)**.** *If G is a finitely generated abelian group, $\exists$ prime powers $p_1^{a_1}, \ldots, p_k^{a_k}$ (not necessarily all distinct) and $n \geq 0$ such that,*

$$G \cong \mathbb{Z}^n \oplus \bigoplus_{i=1}^{k} \mathbb{Z}_{p_i^{a_i}}.$$

Exercise 16. If the prime factorisation of $n \in \mathbb{N}$ is $n = p_1^{\alpha_1} \ldots p_k^{\alpha_k}$, then $\mathbb{Z}_n \cong \mathbb{Z}_{p_1^{\alpha_1}} \ldots \mathbb{Z}_{p_k^{\alpha_k}}$.

For a prime p, we say G is a *p-group* if the order of every element of G is a power of p. G may be infinite: for example, the group of all p^kth roots of unity, as k runs over all natural numbers, is called the *quasicylic group C_p^∞*.

Almost on the other end of the spectrum from abelian groups, we have *simple groups*, which contain no nontrivial normal subgroups.

Proposition 1.13. *The only abelian finite simple groups are $\mathbb{Z}_p$, for p prime.*

[4]Hint: if $\rho = \tau^{-1}\sigma\tau$, then $\rho(\tau^{-1}(i)) = \sigma(i)$ for all $i = 1, \ldots, n$.

[5]An isomorphism $G \to G$.

For $n \geq 5$, the alternating groups A_n are simple, and they are the only normal subgroups of S_n. A_5 is even the smallest nonabelian finite simple group.

In order to **c**lassify all **f**inite **s**imple **g**roups, we want to define some subgroups that exist and are normal in any group G, thus showing that in any nonabelian finite simple group these subgroups are trivial.

For two elements $g, h \in G$, define their *commutator*

$$[g, h] = ghg^{-1}h^{-1},$$

and the *commutator subgroup* of G,

$$[G, G] = \langle [g, h] : g, h \in G \rangle.$$

Vigyázz. $[G, G]$, sometimes also denoted G', is the subgroup *generated* by all commutators of G. In general, the *set* of all commutators need not be closed under the group operation.

Then,

(*) $[G, G] \lhd G$.

(*) $G/[G, G]$ is abelian.

(*) If G/N is abelian, then $[G, G] \leq N$. Conversely, if $[G, G] \leq N$, then $N \lhd G$ and G/N is abelian.

Define the *center* of G

$$Z(G) = \{x \in G : gx = xg, \forall g \in G\}.$$

Equivalently, this is the set of all elements whose conjugacy class has exactly one element. $Z(G) \lhd G$. It is important to know and easy to show that $Z(G)$ and $[G, G]$ are characteristic in G. Further, each characterises how far G is from being abelian; G is abelian if and only if $Z(G) = G$, and if and only if $[G, G] = 1$.

Exercise 17. What is $Z(S_n)$? What is $[S_n, S_n]$?

Exercise 18. Give an example of a group G with a subgroup $H \leq G$ such that $Z(H) \neq Z(G) \cap H$. Which inclusion is always true?

Exercise 19. If $G = A \times B$, then $Z(G) = Z(A) \times Z(B)$.

Given a set $S \subset G$, define its *centralizer* and *normalizer* respectively

$$C_G(S) = \{g \in G : gs = sg, \forall s \in S\},$$

$$N_G(S) = \{g \in G : gS = Sg\}.$$

When $S = \{x\}$, we abuse notation a little and write $C_G(x)$ and $N_G(x)$.

Proposition 1.14. *$C_G(S)$ and $N_G(S)$ are always subgroups of G, and $C_G(S) \lhd N_G(S)$. When S is a subgroup of G, $S \leq N_G(S)$ and $N_G(S)$ is the largest subgroup of G in which S is normal. $S \leq C_G(S)$ exactly when S is abelian.*

For $g \in G$, define $\varphi_g : G \to G$ by

$$\varphi_g(x) = g^{-1}xg.$$

This is an isomorphism from $G \to G$, or an *automorphism*. Denote by $Aut(G)$ the group of all automorphisms of G, and by $Inn(G) = \{\varphi_g : g \in G\}$ the subgroup of all *inner automorphisms*. Then,

$$G/Z(G) \cong Inn(G).$$

Proposition 1.15. *G is abelian if and only if $Inn(G)$ is cyclic.*[6]

Recall that a subgroup $H \leq G$ is called *characteristic* if it is invariant under $Aut(G)$. A characteristic subgroup is necessarily normal (invariant under $Inn(G)$), but the converse need not hold.

Exercise 20. Give an example of a group G with a normal subgroup which is not characteristic.[7]

[6]This is a misleading way to state the proposition. Of course, if G is abelian, then $Inn(G)$ is trivial. The crucial observation is that if G is nonabelian, then $Inn(G)$ is not cyclic.

[7]Hint: the smallest such example satisfies $|G| \leq 5$.

1.5 Group actions

We say G is a *permutation group* if G is isomorphic to a subgroup of some symmetric group. We say a group G *acts* on a set Ω if there is a homomorphism $\varphi : G \to S_\Omega$, $g \to \varphi_g$. Alternatively, each $g \in G$ defines a permutation of Ω so that

$$\omega 1 = \omega,$$
$$(\omega g)h = \omega(gh), \quad \forall g, h \in G.$$

Vigyázz. We write a group action as a *right* group action, and will hopefully keep this consistent throughout the note.

Definition 1.16. Let G act on Ω. Define

(1) the *orbit* of $\omega \in \Omega$ denoted by $\omega G := \{\omega g : g \in G\}$,

(2) the stabilizer of ω, $G_\omega := \{g \in G : \omega g = \omega\}$, sometimes denoted by $Stab_G(\omega)$,

(3) the *kernel* of the action, $\{g \in G : \omega g = \omega, \forall \omega \in \Omega\}$.

Example 1.17. D_n acts on the set $\{1, \dots, n\}$ by identifying it with the vertices of a regular n-gon. The orbit of each element is the full set $\{1, \dots, n\}$. The stabilizer of an element is a subgroup of the form $\{1, sr^i\}$. The kernel of the action is the identity subgroup.

Example 1.18. Given a subgroup $H \leq G$, G acts on the cosets $G : H$ by right multiplication. The orbit of each coset Hg is the full coset space $G : H$. The stabilizer of the coset Hg is the conjugate subgroup $g^{-1}Hg$. The kernel of the action is called the *core* of H: this is the largest normal subgroup of G contained in H.

Example 1.19. Let G act on itself by conjugation, i.e. $h \cdot \varphi_g = g^{-1}hg$. The orbit of each element is its conjugacy class. The stabilizer of an element h is $C_G(h)$. The kernel of the action is $Z(G)$.

Some properties that are easy to check:

(*) $\omega g_1 = \omega g_2 \iff G_\omega g_1 = G_\omega g_2$.

(*) $G_{\omega g} = g^{-1} G_\omega g$, i.e. any two stabilizers are conjugate in G.[8]

(*) $\ker(\varphi) = \bigcap_\omega G_\omega$.

The following result is easy to prove but surprisingly fundamental for many nontrivial results that will follow later.

Lemma 1.20 (The orbit-stabilizer lemma)**.** $|\omega G| = |G : G_\omega|$.

Exercise 21. The size of each conjugacy class of G divides $|G|$.

Exercise 22. Let $\sigma \in A_n$. Let σ^{S_n} and σ^{A_n} denote its conjugacy classes in S_n and A_n respectively.

(a) If $C_{A_n}(\sigma) \subsetneq C_{S_n}(\sigma)$, then $\sigma^{A_n} = \sigma^{S_n}$.

(b) If $C_{A_n}(\sigma) = C_{S_n}(\sigma)$, then σ^{S_n} splits into two conjugacy classes of equal size in A_n, one of which is σ^{A_n}.

(c) List the conjugacy classes of S_5 and A_5.

(d) Show that A_5 has no nontrivial normal subgroups.

An action is

(*) *faithful* if its kernel is trivial,

(*) *transitive* if it has only one orbit[9],

(*) *semi-regular* if the stabilizer of every element is trivial, and

[8]This is an important fact! Typically when we have a property for one stabilizer, it will be true for all stabilizers.

[9]$\forall \alpha, \beta \in \Omega$, $\alpha g = \beta$ for some $g \in G$.

(*) *regular* if it is semi-regular and transitive.

Equivalently, it is regular if

$$\forall \alpha, \beta \in \Omega, \exists! g \in G : \quad \alpha g = \beta.$$

Note that any semi-regular action is faithful.

Exercise 23. Suppose G acts transitively on Ω. Define a bijection from the coset space of G_ω to Ω; $f : (G : G_\omega) \to \Omega$ by $f(G_\omega x) = \omega x$. Then the action of G on the cosets $G : G_\omega$ by right multiplication is equivalent to the action of G on Ω, i.e. $f(G_\omega)x = f(G_\omega x)$ for all $x \in G$.

If G acts transitively on Ω, then the orbit-stabilizer lemma implies that $|\Omega|$ divides $|G|$. If G acts regularly on Ω, $|G| = |\Omega|$, and for any fixed $\alpha \in \Omega$, we have a bijection $g \to \alpha g$. So any regular action of G is essentially the *right regular action* (the action of G on itself by right multiplication). This gives us an injective homomorphism $G \to \mathrm{Sym}(|G|)$, so that

Theorem 1.21 (Cayley's theorem)**.** *Every group is isomorphic to a permutation group.*

From now on, instead of writing "G acts on Ω and the action is faithful", we will write $G \leq S_\Omega$.

1.6 Sylow's theorems

Sylow's theorems provide a sort of converse to Lagrange's theorem. Let G be a finite group, and let p be a prime such that the highest power of p dividing $|G|$ is p^k. Say H is a *Sylow p-subgroup* of G if $|H| = p^k$.

Theorem 1.22 (Sylow's theorems)**.** *Let $|G| = p^k m$, $(m, p) = 1$.*

(1) G has a Sylow p-subgroup.

(2) Any two Sylow p-subgroups of G are conjugate.

(3) The number of Sylow p-subgroups of G divides m and is congruent to $1 \mod p$.

An easy observation:

Corollary 1.23. *Every finite abelian group is the direct sum of its Sylow p-subgroups.*

Exercise 24. What are the Sylow p-subgroups of D_n?

A useful observation is the following corollary, which we will use in later proofs.

Corollary 1.24. *If G is a group of order pq, where p, q are primes and $p > q$, then G has a unique subgroup of order p and this is normal in G. As a result, G is solvable.* [10]

2 Group structures

2.1 Free groups

Recall that we wrote the dihedral group as

$$D_n = \langle r, s \mid r^n = s^2 = 1, rs = sr^{-1} \rangle.$$

What if we just wrote

$$G = \langle r, s \rangle$$

and left the rest to fate? This is the idea of a *free group*.

Given a set X, we consider all finite words $x_1 x_2 \ldots x_n$ over X, with the operation of concatenation. Of course, we would like some words such as xx^{-1} to be 1, where 1 denotes the empty word. Extending the $^{-1}$ to words, if $w_1 = x_1 \ldots x_k$, define $w_1^{-1} = x_k^{-1} \ldots x_1^{-1}$. Then define an equivalence relation $w_1 \sim w_2$ if and only if $w_1 w_2^{-1} = 1$.

[10] We will define solvability later.

Definition 2.1. The *free group* generated by X is

$$F(X) = {\{\text{ finite words over } X\}}/{\sim}.$$

When $|X| = n$ is finite, we may equivalently write F_n to denote a free group on n elements. For example,

(*) $F(\emptyset) = \{1\}$, the one-element group.

(*) $F(\{x\}) \cong \mathbb{Z}$.

(*) $F(X)$ is nonabelian if $|X| \geq 2$.

Exercise 25. Let X be a set and G a group. Any function $f : X \to G$ extends uniquely to a homomorphism $f : F(X) \to G$.

Proposition 2.2.

$$F(X) \cong F(Y) \iff |X| = |Y|.$$

Proof. Clearly if $|X| = |Y|$, then $F(X) \cong F(Y)$. For the converse, if X is infinite, then $|X| = |F(X)|$, so the claim follows. Suppose both X and Y are finite, and $F(X) \cong F(Y)$. Let $\mathrm{Hom}(F, G)$ denote the group of homomorphisms from $F \to G$, with the group operation $\varphi_1\varphi_2(x) = \varphi_1(x)\varphi_2(x)$. Then $\mathrm{Hom}(F(X), \mathbb{Z}_2) \cong \mathrm{Hom}(F(Y), \mathbb{Z}_2)$, but any such homomorphism is uniquely determined by the image of the generators. So,

$$\Big|\mathrm{Hom}(F(X), \mathbb{Z}_2)\Big| = 2^{|X|} = \Big|\mathrm{Hom}(F(Y), \mathbb{Z}_2)\Big| = 2^{|Y|}.$$

$\square$

Let us return to our expression of D_n. We now realise that this defined D_n as a quotient group of F_2. That is, consider all words $r^{n_1}s^{n_2}\dots s^{n_{2k}}$ that are the identity in D_n. These define a normal subgroup $N \lhd F_2$, so that $D_n \cong F_2/N$, where N is the normal subgroup generated by $\langle r^n, s^2, rsrs^{-1}\rangle$.

In general,

Theorem 2.3. *Every group is the homomorphic image of a free group.*

The proof of this is exactly the analog of what we did for D_n. If X is a generating set for G, the set of words $\{w_i : w_i = 1 \in G\}$ is a normal subgroup of $F(X)$.

This characterises quotient groups of free groups. What about subgroups? Define the *rank* of a free group as the minimum size of a generating set.

Theorem 2.4 (Nielsen-Schreier)**.** *Every subgroup H of a free group $F(X)$ is free. If the rank of H is finite, it is equal to $|F : H|\big(|X| - 1\big) + 1$.*

Before we prove this, note that when $|X| = 1$, $F(X) = \mathbb{Z}$, and the theorem holds since any subgroup of $\mathbb{Z}$ is cyclic. When $|X| > 1$ is finite, $|F : H|\big(|X| - 1\big) + 1$ is typically larger than $|X|$, so a free group contains many free groups of larger rank.

Exercise 26. The free group of rank 2 contains a free group of infinite rank.

Let $F = F(X)$, where X is a *self-inverse* generating set (closed under inverses). Fix a subgroup $H \leq F$. Choose (right) coset representatives $T = \{t_i : i \in I\}$ for F/H, and call T a *transversal*. We have a map $F \to T$ defined by sending $x \to \bar{x}$, its coset representative.

Lemma 2.5. *If X is a self-inverse generating set of F, and $H \leq F$ with transversal T, then*

$$S = \left\{tx(\overline{tx})^{-1} : t \in T, x \in X\right\}$$

is a self-inverse generating set of H.

Proof. First note that

$$H\overline{tx} = Htx$$

so

$$tx(\overline{tx})^{-1} \in H.$$

So the subgroup generated by S is contained in H. For the reverse inclusion, we first need to check that S is closed under inverses. Since $H(\overline{tx})x^{-1} = Ht$, $t = \overline{(\overline{tx})x^{-1}}$. So,

$$\left(tx(\overline{tx})^{-1}\right)^{-1} = \overline{tx}x^{-1}t^{-1} = \overline{tx}x^{-1}\left(\overline{\overline{tx}x^{-1}}\right)^{-1} \in S.$$

Now to show that S generates H; let $h \in H$. Then $h = x_1 \dots x_n$ for some $x_i \in H$. Define

$$t_i = \overline{x_1 \dots x_i}, \quad t_0 = t_n = 1.$$

Then,

$$h = (t_0x_1t_1^{-1})(t_1x_2t_2^{-1})\dots(t_{n-1}x_nt_n^{-1}).$$

Since $t_k = \overline{t_{k-1}x_k}$,

$$t_{k-1}x_kt_k^{-1} = t_{k-1}x_k(\overline{t_{k-1}x_k})^{-1} \in S.$$

□

Of course, we may replace F in the above proof with an arbitrary group and the proof still holds. As a corollary, when T is finite,

Corollary 2.6. *Finite index subgroups of a finitely generated group are finitely generated.*

Proof of Nielsen-Schreier. We choose our transversal T in a specific way. Fix a well-ordering $\leq$ of X,[11] and choose the lexicographically shortest word in each coset of H.

Step (1)**.** T is closed under prefixes, i.e. if $w \in T$ and $w = ux$ for some $x \in X$, then $u \in T$.

Suppose $w = ux$ as above. If $u \notin T$, then for some $t \in T$, $t \neq u$, $\overline{u} = t$. Either t is shorter than u, or they have the same length, but t is lexicographically first.

$$Hw = Hux = Htx.$$

Since $w = ux \in T$, either ux has shorter length than tx, or ux is lexicographically first, a contradiction.

Step (2)**.** Every word $tx(\overline{tx})^{-1}$ is either reduced or the identity.

Suppose $tx(\overline{tx})^{-1}$ is not reduced. Then either t is of the form ux^{-1}, and $u \in T$ by step 1, so that

$$u = \overline{tx} \implies tx(\overline{tx})^{-1} = uu^{-1} = 1.$$

Or, $(\overline{tx})^{-1}$ begins with x^{-1}, i.e. $\overline{tx} = ux$, but u and t are both in T, so $u = t$, and

$$tx(\overline{tx})^{-1} = ux(ux)^{-1} = 1.$$

Step (3)**.** For any product $\left(t_1x_1(\overline{t_1x_1})^{-1}\right)\left(t_2x_2(\overline{t_2x_2})^{-1}\right)$, either (a) one of them is the identity, or (b) they are inverses of each other, or (c) x_1 and x_2 are not cancelled in the reduced form.

Suppose this product is not in reduced form. If $\overline{t_1x_1} = t_2$ and $x_1 = x_2^{-1}$, since the product lies in H, $t_1 = \overline{t_2x_2}$, and (b) they are inverses of each other. If x_2 is cancelled by $(\overline{t_1x_1})^{-1}t_2$, then t_2x_2 is a prefix of $\overline{t_1x_1}$, so $t_2x_2 = \overline{t_2x_2}$ by step 1, and (a) $t_2x_2(\overline{t_2x_2})^{-1} = 1$. If neither of these things happen, then (c) x_1 and x_2 are not cancelled in the reduced form.

Step (4)**.** The number of generators required to write every element of H in unique reduced form $|F(X) : H|\big(|X| - 1\big) + 1$.

[11] Axiom of choice.

Clearly we have a total of

$$|T| \cdot |X| = |F(X) : H| \cdot |X|$$

generators of H of the form $tx(\overline{tx})^{-1}$. How many of these generators do we need so that each word of H has a unique reduced form? Equivalently, so that the identity has a unique reduced form? By step 3, if $1 = \left(t_1x_1(\overline{t_1x_1})^{-1}\right)\left(t_2x_2(\overline{t_2x_2})^{-1}\right)$, where neither is equal to 1 or the inverse of the other, then x_1 and x_2 are not cancelled. So we count the number of distinct words $tx(\overline{tx})^{-1}$ that reduce to 1. Our argument from step 2 tells us this happens either if $tx \in T$, so t ends with x^{-1}, or $\overline{tx}$ ends with x. Disregarding inverses, for any nonidentity $t \in T$, there is exactly one x for which this happens, so this gives us $|T| - 1 = |F(X) : H| - 1$ such expressions. So the total number of generators needed is

$$|T| \cdot |H| - (|T| - 1) = |F(X) : H|\left(|X| - 1\right) + 1.$$

□

Let us look at one final property of free groups.

Definition 2.7. A group G is *residually finite* if

$$\bigcap_{N \lhd G, |G:N| < \infty} N = \{1\}.$$

Equivalently, for every nonidentity $g \in G$, there is a finite group H and a homomorphism $\varphi : G \to H$ such that $\varphi(g) \neq 1$.

Proposition 2.8. *Free groups are residually finite.*

Proof. Let X be a minimal generating set of $F(X)$. Let $w \in F(X)$ be a nonidentity word with reduced form $w = x_n^{\epsilon_n} \dots x_1^{\epsilon_1}$, where $x_i \in X$ and $\epsilon_i \in \{\pm 1\}$. Define a map $\phi : X \to S_{n+1}$ as follows. For each x_i, we want ϕ_{x_i} to be a permutation that maps $i \to i+1$ if $\epsilon_i = 1$, and $i+1 \to i$ if $\epsilon_i = -1$. Of course, some x_i may be equal; for example if $x_1 = x_3$, then ϕ_{x_1} must map $1 \to 2$ and $3 \to 4$. However, by assuming that w is in reduced form (so that $x_i = x_{i+1}$ implies $\epsilon_i = \epsilon_{i+1}$), we can choose a well-defined ϕ_x for each $x \in X$. By induction, $\phi_w(1) = n + 1$. □

2.2 Permutation groups

The *orbit-stabilizer lemma* (like Markov's inequality in probability theory) has powerful applications for a fairly simple statement.

Lemma 2.9 (Burnside's lemma)**.** *Let G be finite and $G \leq S_\Omega$. Let* $\mathrm{fix}(g)$ *denote the number of points of Ω fixed by g, and n the number of orbits of G on Ω. Then,*

$$n = \frac{1}{|G|} \sum_{g \in G} \mathrm{fix}(g).$$

The number of orbits is the average number of fixed points.

Proof. Clearly,

$$\sum_{g \in G} \mathrm{fix}(g) = \Big|\{(g, \omega) : \omega \cdot g = \omega\}\Big| = \sum_{\omega \in \Omega} |G_\omega|.$$

By the orbit-stabilizer lemma,

$$\sum_{\omega \in \Omega} |G_\omega| = |G| \sum_{\omega \in \Omega} \frac{1}{|\omega \cdot G|}.$$

Each of the n orbits, represented by $\omega_1, \dots, \omega_n$, is counted with multiplicity its size. So,

$$\sum_{g \in G} \mathrm{fix}(g) = |G| \sum_{i=1}^{n} \sum_{\omega \in \omega_i \cdot G} \frac{1}{|\omega_i \cdot G|} = n|G|.$$

□

For $x \in G$, let x^G denote the conjugacy class of x in G. As the action of G on itself by conjugation induces a partition into orbits,

Theorem 2.10 (Class equation)**.**
$$|G| = |Z(G)| + \sum_{x \notin Z(G)} |x^G|$$
where the latter sum runs over all the conjugacy classes of G not contained in the center.

In a p-group, each conjugacy class has size divisible by p, so

Corollary 2.11. *If G is a p-group, then G has nontrivial center.*

Exercise 27. The probability that two elements in a finite group commute is at most $5/8$.

Lemma 2.12. *The centralizer of a transitive permutation group is semi-regular.*

Proof. Denote the centralizer of $G \le S_\Omega$ by
$$C = \{h \in S_\Omega : gh = hg, \forall g \in G\}.$$
Let C_ω denote the stabilizer of ω in C. For $h \in C_\omega$, and any $\alpha \in \Omega$, there is some $g \in G$ such that $\omega g = \alpha$. Then,
$$\alpha h = \omega g h = \omega h g = \omega g = \alpha.$$
That is, $h \in C_\alpha$ for all $\alpha \in \Omega$. The action is faithful, so $h = 1$ and C_ω is trivial. □

Exercise 28. The centralizer of a semi-regular permutation group is transitive.

Theorem 2.13 (Bercov-Moser)**.** *If $G \le S_n$ is abelian, then $|G| \le 3^{n/3}$.*

Proof. We proceed by induction on n, the base case $n \le 2$ being trivial. First, suppose G is transitive. By the lemma, its centralizer $C \le S_n$ is semi-regular, and $G \le C$ as it is abelian, so G is regular and $|G| = n \le 3^{n/3}$. If G is not transitive, partition $[n]$ into orbits $\Omega_1, \dots, \Omega_k$ under the action of G. The restriction of G to each orbit yields a transitive action. These correspond to homomorphisms $\varphi_i : G \to S_{\Omega_i}$, such that $\bigcap_i \ker(\varphi_i) = 1$. So, by the induction hypothesis
$$|G| \le \prod_{i=1}^{k} \left| G/\ker(\varphi_i) \right| \le \prod_{i=1}^{k} 3^{n_i/3} = 3^{n/3}.$$
□

Exercise 29. For which abelian permutation groups $A \le S_n$ does $|A| = 3^{n/3}$ hold?

Exercise 30. Determine the order of the centralizer of an arbitrary permutation.

Theorem 2.14. *For $n \neq 6$, every automorphism of S_n is inner.*

Proof. Since two permutations are conjugate if and only if they have the same cycle type, and the transpositions generate S_n, it suffices to show that any automorphism σ maps transpositions to transpositions. We know that σ is order-preserving, so for any transposition $g \in G$, $\sigma(g)$ is the product of k commuting transpositions for some k. Suppose $k \ge 2$. Further, σ is an automorphism from $C_G(g) \to C_G(\sigma(g))$, so we compare the orders of the centralizers.
$$|C_G(\sigma(g))| = 2^k k!(n-2k)! = 2(n-2)! = |C_G(g)|$$
$$2^{k-1}k! = (n-2k+1)\dots(n-3)(n-2)$$
If $n > 2k$, each side of the equation has $2k-2$ factors, and each factor on the left is smaller than a corresponding factor on the right, so equality is not possible. If $n = 2k$, the equation becomes
$$2^{k-1}k! = (2k-2)!$$
It is easy to check this does not hold for $k = 1, 2$, does hold for $k = 3$, and for $k > 3$,
$$2^{k-1}k! = 4 \cdot 2^{k-3}k! < (2k-2)!$$
This shows that for $n \neq 6$, σ maps transpositions to transpositions, so it preserves cycle type and must be an inner automorphism. □

Exercise 31. What is an automorphism of S_6 that is not inner?

2.3 Groups of linear transformations

The alternating groups form an infinite family of finite simple groups. In this section we will construct another, the *projective special linear groups*.

Let V be a vector space, $GL(V)$ the group of invertible linear maps, $SL(V)$ the subgroup of maps with determinant 1. When V is d-dimensional, we write $GL(V) = GL(d, F)$ and $SL(V) = SL(d, F)$, the matrix groups. Note that $\det : GL(d, F) \to F^*$ is a homomorphism, so $\ker(\det) = SL(d, F) \lhd GL(d, F)$.

Consider the action of $GL(d, F)$ on the 1-dimensional subspaces of V (equivalently, on the projective space of dimension $d-1$, but it is not necessary to know what this means.) The kernel of this action is $Z(GL(d, F))$.

Exercise 32. The center of $GL(d, F)$ is the group of scalar matrices, i.e. $\{\lambda \cdot I : \lambda \in F^\times\}$, where I denotes the identity matrix.

Definition 2.15. The *projective general linear group* is

$$PGL(V) = {}^{GL(V)}\!/\!_{Z(GL(V))}.$$

Restricting the action to $SL(V)$, the *projective special linear group* is

$$PSL(V) = {}^{SL(V)}\!/\!_{Z(SL(V))}.$$

We are only interested in the case when V is finite-dimensional and F is some finite field $\mathbb{F}_q$.

$$\begin{aligned}
|GL(d,q)| &= (q^d - 1)(q^d - q)\dots(q^d - q^{d-1}) \\
|SL(d,q)| &= \frac{|GL(d,q)|}{q-1} \\
|PGL(d,q)| &= \frac{|GL(d,q)|}{q-1} \\
|PSL(d,q)| &= \frac{|SL(d,q)|}{\gcd(d,q-1)}
\end{aligned}$$

The last equality follows from the fact that $Z(SL(d,q))$ consists of the matrices $\lambda \cdot I$ such that $\lambda^d = 1$.

As promised,

Theorem 2.16. *$PSL(d, F)$ is simple, except when $d = 2$ and $|F| = 2$ or 3.*

Exercise 33. $PSL(2, 2) \cong S_3$ and $PSL(2, 3) \cong A_4$.

To prove the theorem, we will show that any proper normal subgroup of $SL(V)$ is contained in the center, so that the quotient $PSL(V)$ contains no nontrivial normal subgroups. We will need to construct a generating set for $SL(V)$.

Definition 2.17. If $\gamma : V \to V$ is a linear map such that $\operatorname{rank}(\gamma) = 1$ and $\operatorname{Im}(\gamma) \subset \ker(\gamma)$, then $I+\gamma \in SL(V)$ is a *transvection*.

The transvections in $SL(V)$ play a similar role to the transpositions in S_n. We will need many lemmas, so let us state them all first.

Lemma 2.18. *If $d \geq 3$, all transvections are conjugate in $SL(d, F)$.*

Lemma 2.19. *If $d = 2$, the subgroups*

$$T_U = \{I + \gamma : \operatorname{Im}(\gamma) = \ker(\gamma) = U\} \cup \{I\}$$

for each one-dimensional subspace $U \leq V$ are conjugate in $SL(V)$.

Lemma 2.20. *The transvections generate $SL(V)$.*

Lemma 2.21. *The commutator subgroup $SL(V)' = SL(V)$, except when $d = 2$ and $|F| = 2$ or 3.*

Lemma 2.22. *$SL(V)$ acts 2-transitively on the one-dimensional subspaces of V.*[12]

Lemma 2.23. *If G acts 2-transitively on Ω, any normal subgroup acts either trivially or transitively. Further, any stabilizer is a maximal subgroup.*

Lemma 2.24. *The stabilizer $H \leq SL(V)$ of a one-dimensional subspace contains an abelian normal subgroup consisting of I and some transvections.*

Let us see how this implies that $PSL(V)$ is simple.

Proof of Theorem 2.16. We will show that any proper normal subgroup of $SL(V)$ is contained in $Z(SL(V))$. Suppose $N \lhd SL(V)$. By Lemma 2.23, N acts either trivially or transitively on the one-dimensional subspaces of V. If N acts trivially, then every vector of V is an eigenvector for N, so $N \leq Z(SL((V))$. Suppose N acts transitively on the one-dimensional subspaces. Let H be a stabilizer, so H is a maximal subgroup of $SL(V)$ by Lemma 2.23. Then $H \leq NH \leq SL(V)$. However, N acts transitively, so we must have $NH = SL(V)$.

Let $K \lhd H$ be the abelian normal subgroup given by Lemma 2.24. Then $NK \lhd NH = SL(V)$. Since NK contains some transvections, by Lemma 2.18 NK contains all transvections, and by Lemma 2.20 $NK = SL(V)$. So,

$$SL(V)/N \cong K/K \cap N$$

K is abelian, so $SL(V)' \leq N$. This is where we use that we cannot have $d = 2$ and $|F| = 2$ or 3: $SL(V)' = SL(V)$ by Lemma 2.21, and this implies that $N = SL(V)$.

After all this, we finally obtain that $PSL(V)$ contains no nontrivial normal subgroups. □

Time to prove our many lemmas.

Lemma 2.18. *If $d \geq 3$, all transvections are conjugate in $SL(d, F)$.*

Proof. For any transvection $I + \gamma$, choose a basis $u_1, \ldots, u_d$ of V so that $\mathrm{Im}(\gamma) = \langle u_1 \rangle$, $\ker(\gamma) = \langle u_1, \ldots, u_{d-1} \rangle$, and $\gamma(u_d) = u_1$. In particular, this shows that any two transvections have the same matrix by a change of basis, so they are conjugate in $GL(V)$. If $d \geq 3$, then u_2 is distinct from both u_1 and u_d, so multiplying it by a suitable scalar α does not affect the matrix of $I + \gamma$, but changes the determinant of the transition matrix to 1. So any two transvections are conjugate in $SL(V)$. □

Lemma 2.19. *If $d = 2$, the subgroups*

$$T_U = \{I + \gamma : \mathrm{Im}(\gamma) = \ker(\gamma) = U\} \cup \{I\}$$

for each one-dimensional subspace $U \leq V$ are conjugate in $SL(V)$.

Proof. We want to show that for distinct one-dimensional subspaces U and U', the subgroups T_U and $T_{U'}$ differ by a change of basis. By the same argument above, there is a basis of V so that

$$T_U = \left\{ \begin{bmatrix} 1 & x \\ 0 & 1 \end{bmatrix} : x \in F \right\}$$

Again, it follows that any two such subgroups are conjugate in $SL(2, F)$. □

Lemma 2.20. *The transvections generate $SL(V)$.*

[12] This will be defined in the proof.

Proof. We prove by induction for $0 \leq k \leq d$, that for any $\phi \in SL(V)$ and $u_1, \ldots, u_k \in V$ linearly independent, there is a product of transvections ψ_k such that $\psi_k(u_1) = \phi(u_i)$ for $i = 1, \ldots, k$. For $k = 0$, choose $\psi_0 = I$ and the statement clearly holds.

Suppose the statement holds for some k. Fix $\phi \in SL(V)$, linearly independent vectors $u_1, \ldots, u_k, u_{k+1}$, and ψ_k the corresponding product of transvections for $u_1, \ldots, u_k$. Define

$$\phi' = \psi_k^{-1}\phi.$$

Then,

$$\phi'(u_i) = u_i, i = 1, \ldots, k$$

Let $\phi'(u_{k+1}) = w$, i.e. $\phi(u_{k+1}) = \psi_k(w)$. If $w = u_{k+1}$, then we are done, so let us assume they are different.

Case (1)**.** $u_1, \ldots, u_{k+1}$, and w are linearly independent.

Choose a transvection $I + \mu$ as follows.[13]

$$\langle u_1, \ldots, u_k \rangle \leq \ker(\mu),$$
$$\mu(u_{k+1}) = \mu(w) = w - u_{k+1}.$$

Then $(I + \mu)(u_i) = u_i$ for $i = 1, \ldots, k$, and $(I + \mu)u_{k+1} = w$. So $\psi_k(I + \mu)$ is the required product of transvections.

Step (2)**.** $u_1, \ldots, u_{k+1}, w$ are linearly dependent and $k + 1 < d$.

Extend $u_1, \ldots, u_{k+1}$ to a basis $v, v_{k+3}, \ldots, v_d$. Define a transvection $\phi_1 = I + \gamma_1$ such that γ_1 is zero on all basis vectors except for $\gamma_1(u_{k+1}) = \gamma_1(v) = v - u_{k+1}$. Then, $\phi_1(u_{k+1}) = v$. Since ϕ' is invertible, $u_1, \ldots, u_k, w$ are linearly independent, so we define ϕ_2 analogously to ϕ_1, but with $\phi_2(w) = v$. ϕ_1 and ϕ_2 are transvections, and $\psi_k\phi_2^{-1}\phi_1$ is the desired product of transvections.

Step (3)**.** $u_1, \ldots, u_{k+1}, w$ are linearly dependent and $k + 1 = d$.

In this case, $\phi'(u_{k+1}) = u + \lambda u_{k+1}$, for some $u \in \langle u_1, \ldots, u_k \rangle$. The matrix of ϕ' in this basis is

$$\begin{bmatrix} 1 & 0 & \ldots & * \\ 0 & 1 & \ldots & * \\ & & \vdots & \\ 0 & 0 & \ldots & \lambda \end{bmatrix}$$

Since $\det(\phi') = 1$, $\lambda = 1$, so ϕ' is itself a transvection and $\phi = \phi'\psi_k$. □

Exercise 34. If $\dim V = d$, what is the maximum number of transvections needed to express an element of $SL(V)$?

Lemma 2.21. *The commutator subgroup $SL(V)' = SL(V)$, except when $d = 2$ and $|F| = 2$ or 3.*

Proof. The commutator subgroup is normal, so it suffices to show that some transvection is a commutator. If $d \geq 3$,

$$[I + E_{12}, I + E_{23}] = (I + E_{12})^{-1}(I + E_{23})^{-1}(I + E_{12})(I + E_{23}) = I + E_{13}.$$

If $d = 2$, and $|F| \neq 2$ or 3, it suffices to show that some T_U contains a commutator. For arbitrary $a, c \in F^{\times}$, take the commutator

$$\left[\begin{bmatrix} a & 0 \\ 0 & a^{-1} \end{bmatrix}, \begin{bmatrix} 1 & c \\ 0 & 1 \end{bmatrix}\right] = \begin{bmatrix} 1 & c(1 - a^{-2}) \\ 0 & 1 \end{bmatrix}$$

Since $|F| \neq 2$ or 3, we can find some nonzero a for which $a^{-2} \neq 1$, so the resulting matrix is a transvection. □

Lemma 2.22. *$SL(V)$ acts 2-transitively on the one-dimensional subspaces of V.*[14]

[13] We can do this by extending the $k + 2$ vectors to a basis of V.

[14] This will be defined in the proof.

Proof. In general, we say a group G acts *2-transitively* on Ω, if for any $\omega_1, \omega_2 \in \Omega$ distinct, and $\alpha_1, \alpha_2 \in \Omega$ distinct, there is some $g \in G$ such that $\omega_1 \cdot g = \alpha_1$ and $\omega_2 \cdot g = \alpha_2$. So let $\langle a_1 \rangle, \langle a_2 \rangle$ be distinct one-dimensional subspaces, and $\langle b_1 \rangle, \langle b_2 \rangle$ be distinct one-dimensional subspaces of V. For any numbers $\alpha_1, \alpha_2 \in F$, we can find a $\phi \in GL(V)$ such that $\phi(a_1) = \alpha_1 b_1$ and $\phi(a_2) = \alpha_2 b_2$. For an appropiate choice of α_1 and α_2, $\det(\phi) = 1$, so $\phi \in SL(V)$. □

Lemma 2.23. *If G acts 2-transitively on Ω, any normal subgroup acts either trivially or transitively. Further, any stabilizer is a maximal subgroup.*

Proof. Suppose $N \lhd G$ does not act trivially. Choose $\omega \in \Omega$ and $n \in N$ such that $\omega \cdot n \neq \omega$. Then, for any distinct $\alpha, \beta \in \Omega$, there exists g such that $(\omega \cdot n)g = \alpha$ and $\omega g = \beta$. Then,

$$\alpha \cdot g^{-1} n^{-1} g = (\omega n) \cdot n^{-1} g^{-1} = \beta$$

so N acts transitively. □

Lemma 2.24. *The stabilizer $H \leq SL(V)$ of a one-dimensional subspace contains an abelian normal subgroup consisting of I and some transvections.*

Proof. Let $\langle u_1 \rangle \leq V$ be stabilized by H. For a fixed basis of V, each matrix of H has the form

$$\begin{bmatrix} \lambda & * \\ 0 & A \end{bmatrix},$$

where λ is a scalar and A is a $(d-1) \times (d-1)$ matrix. The map $H \to SL(d, F)$ sending each matrix to the submatrix A is a homomorphism. Its kernel is a set of matrices of the form

$$\begin{bmatrix} 1 & * \\ 0 & I_{d-1} \end{bmatrix}.$$

These are transvections which commute with each other, giving the desired subgroup of H.

□

2.4 Group extensions

Given N and G/N, can we recover the structure of the group G? First, let us consider how to obtain a group G from two groups N and H so that $N \lhd G$ and $G/N \cong H$. We can take the direct sum/product, but a more complicated construction is the *semidirect product*.

Definition 2.25. We say H is an *operator group* on a group N if there is a homomorphism $\varphi : H \to Aut(N)$. We denote the action of $h \in H$ on $n \in N$ by n^h.

Define the *semidirect product* of N by H as $N \rtimes H = \{(n, h) : n \in N, h \in H\}$ with the operation

$$(n_1, h_1)(n_2, h_2) = (n_1 n_2^{h_1^{-1}}, h_1 h_2)$$

The task of verifying that this is a group is left to the reader. Of course, the more skeptical reader will (rightly) ask, "What is the point of this?". Let us look at where a semidirect product occurs in nature.

Let V be a vector space, and $GL(V)$ the group of invertible linear transformations of V. When $V = \mathbb{R}^n$, there are some natural maps $\mathbb{R}^n \to \mathbb{R}^n$ that we would like to call "invertible transformations", but they are not necessarily linear. For example, translation, or rotation about a point different from the origin. This motivates the definition of an *affine transformation*.

An *affine subspace* A is a set of the form $a + U$, where $a \in V$ and U is a subspace of V. The *dimension* of A is defined as the dimension of U. An affine transformation is then a map $V \to V$ that preserves the dimension of any affine subspace. Of course, every element of $GL(V)$ is an affine transformation, but so are the translations, and these are not linear maps. Let $AG(V)$ be the group of translations of V, so $AG(V) \cong V$.

Definition 2.26. The *affine general linear group* of V, denoted $AGL(V)$ is given by $AG(V) \rtimes GL(V)$.

Each element $(v, M) \in AGL(V)$ acts on V by

$$(v, M) \circ x = v + Mx.$$

When $V = \mathbb{R}^n$, these are exactly the isometries.

But this is not the first example of a semidirect product we have seen in this note. Let us return once again to our dihedral group D_n. Define an action of $\mathbb{Z}_2$ on $\mathbb{Z}_n$, where the nonidentity element of $\mathbb{Z}_2$ maps each element of $\mathbb{Z}_n$ to its inverse. This is an automorphism because $\mathbb{Z}_n$ is abelian, and $D_n \cong \mathbb{Z}_n \rtimes \mathbb{Z}_2$.

Exercise 35. Give an example of a semidirect product $G \rtimes H$ such that $Z(G)$ and $Z(H)$ are nontrivial, but $Z(G \rtimes H)$ is trivial.[15]

A fundamental theorem in group theory is the following.

Theorem 2.27 (Schur-Zassenhaus)**.** *Let G be a finite group and $N \lhd G$. If $|N|$ and $|G : N|$ are coprime, then G is a semidirect product of N and G/N.*

Let us reformulate this as

Theorem (Schur-Zassenhaus)**.** *Let G be a finite group with $|G| = ab$, where $(a, b) = 1$. If G has a normal subgroup of order a, then it has a subgroup of order b.*

Proof that the two formulations are equivalent. Clearly the first statement of Schur-Zassenhaus implies the second. For the converse, let N be a normal subgroup of order a, and H a subgroup of order b. Then $N \cap H = \{1\}$ and $G = NH$, so $G = N \rtimes H$, where H acts on N by conjugation.[16] □

In order to prove the Schur-Zassenhaus theorem in its second formulation, we will reduce to the case when the normal subgroup N is abelian. We will need the following two results for the proof. Recall the following result.

Proposition 1.11. *If $M \operatorname{char} N$ and $N \lhd G$, then $M \lhd G$.*

This next result is a fundamental result in group theory, which we will use often.

Proposition 2.28. *(Frattini's argument) Let G be a finite group, $H \lhd G$, and P a Sylow p-subgroup of H. Then $G = HN_G(P)$, and $|G : H|$ divides $|N_G(P)|$.*

Proof. Since H is normal in G, $HN_G(P) = N_G(P)H$ is a well-defined subgroup of G. For any $g \in G$, $g^{-1}Pg \leq H$ is a Sylow p-subgroup in H. For some $x \in H$, $x^{-1}Px = g^{-1}Pg$, so $gx^{-1} \in N_G(P)$ and $g \in N_G(P)H$. □

Reduction to the case N abelian. We proceed by induction, the case $|G| \leq 5$ being clear as always. Let G be the least group for which the theorem fails; there is a normal subgroup N of order a, but no subgroup of order b.

Step (1)**.** N is a minimal normal subgroup of G.

If not, let $M \leq N$ be a proper nontrivial normal subgroup of G. Applying the induction hypothesis to $N/M \lhd G/M$, G/M has a subgroup K/M of order b, but this corresponds to a subgroup K in G of order b.

Step (2)**.** N is a vector space over $\mathbb{F}_p$, i.e. it is abelian and every element has order p.

Let P be a Sylow p-subgroup of N. By Frattini's argument, $G = NN_G(P)$, so

$$G/N \cong N_G(P)/(N \cap N_G(P)).$$

$N \cap N_G(P)$ is normal in $N_G(P)$, so if $N_G(P)$ is a proper subgroup of G, then $N_G(P)$ has a subgroup of order b, which is not possible. So $P \lhd G$, and by minimality of N, $N = P$. Of course, $Z(P)$ is a characteristic subgroup of P, hence normal in G, so $Z(P) = P$. Finally, we want to show that every element of N has order p; this amounts to showing that the subgroup $N^p = \{x^p : x \in N\}$ is trivial. N^p is characteristic in N, so it is normal in G, and therefore it is trivial.

[15] Hint: start with the smallest groups.

[16] It needs to be shown that under these hypotheses, $NH \cong N \rtimes H$, but this is definition-chasing.

Step (3)**.** A contradiction at last.

There exist more illuminating proofs, but for now let us see a self-contained (albeit tedious) proof. We follow the presentation of [7].

Let $Q = G/N$. Q has a natural action on N where $a^{Ng} = a^g = g^{-1}ag$. Choose a representative t_x for each coset xN. Our goal is to modify this to a set of coset representatives s_x such that $s_x s_y = s_{xy}$, thereby inducing an injective homomorphism $Q \to N$. For now though, all we can say is that since $t_x t_y N = t_{xy} N$, there is some $c(x, y) \in N$ such that

$$t_x t_y = t_{xy} c(x, y).$$

A little manipulation yields

$$c(xy, z) \cdot c(x, y)^z = c(x, yz) \cdot c(y, z).$$

Now define

$$d(y) = \prod_{x \in Q} c(x, y).$$

Since N is abelian

$$\begin{aligned} d(z) \cdot d(y)^z &= d(yz) \cdot c(y, z)^b, \text{ or equivalently} \\ d(yz) &= d(y)^z d(z) c(y, z)^{-b} \end{aligned}$$

Since $(a, b) = 1$, there is some $e(y) \in N$ such that $e(y)^b = d(y)^{-1}$, so we rewrite our last equation as

$$e(yz) = e(y)^z e(z) c(y, z).$$

We are almost done! We only need one more piece of notation: define

$$s_x = t_x e(x)$$

so that after some fun computations,

$$s_y s_z = t_y t_z e(y)^z e(z) = t_{yz} c(y, z) e(y)^z e(z) = t_{yz} e(yz) = s_{yz}$$

and this is the transversal we wanted. The map $s : Q \to G$ that sends $x \to s_x$ is a homomorphism. If $s_x = 1$, then $t_x \in N$ and $x = 1_Q$, so the homomorphism is injective, and this gives us a subgroup of order b in G. □

Remark. It is possible to prove more: that any two subgroups of order b are conjugate, but we do not need this.

2.5 p-groups

Recall that a p-group is a group G in which every element has order a power of p. If G is finite, an application of Cauchy's theorem – or Sylow's theorem, if you want to be fancy – shows that $|G| = p^k$ for some $k \in \mathbb{N}$.

Exercise 36. Groups of order p and p^2 are abelian. There is a nonabelian group of order p^3.

It is easy to check that

Proposition 2.29. *The property of being a p-group is preserved by subgroups, quotients, extensions, and direct sums.*

Note that an infinite direct product of p-groups may contain elements of infinite order. Infinite p-groups do exist:

1. The *quasicyclic group* $C_p^\infty = \bigcup_{k \geq 0} C_{p^k}$, or the group of all p-power roots of unity.
2. The group of *upper unipotent matrices* U_n – upper triangular matrices with 1's on the diagonal – over a field of characteristic p. Every element of this group can be written as $I + A$, where A is nilpotent, so $(I + A)^{p^k} = I^{p^k} + A^{p^k} = I$ for k large enough.

3. The *Tarski monster groups* are infinite p-groups such that every element has order p, and the only nontrivial subgroups are cyclic.

Recall that an easy application of the class equation told us that

Corollary 2.11. *If G is a p-group, then G has nontrivial center.*

The same counting argument tells us that

Corollary 2.30. *Any normal subgroup of a finite p-group intersects the center nontrivially.*

This is sajnos not true for infinite p-groups.

Theorem 2.31. *There is an infinite p-group with trivial center.*

Proof. We say a function $f : A \to B$ has *finite support* if the set $\{a \in A : f(a) \neq 1\}$ is finite. Define

$$\mathcal{F} = \left\{ f : C_p^\infty \to C_p^\infty : \quad f \text{ has finite support} \right\}.$$[17]

This is a group under pointwise multiplication. Let C_p^∞ act on $\mathcal{F}$ so that for $f \in \mathcal{F}$ and $a \in C_p^\infty$, $f^a(x) = f(xa^{-1})$. Our infinite p-group will be $G = \mathcal{F} \rtimes C_p^\infty$; we claim first that if $Z(G)$ is nontrivial, then $Z(G) \cap \mathcal{F}$ or $Z(G) \cap C_p^\infty$ is nontrivial. Suppose $(f, c) \in Z(G)$. If $c = 1$, then we are done. Otherwise, since $Z(G)$ is normal in G and f has finite support, conjugating by finitely many elements of the form $(g, 1)$ we obtain an element of $Z(G)$ that is in C_p^∞.[18]

Now, suppose $(f, 1) \in Z(G) \cap \mathcal{F}$. Then for all $c \in C_p^\infty$,

$$(1, c^{-1})(f, 1)(1, c) = (1, c^{-1})(f, c) = (f^c, 1) = (f, 1)$$

or,

$$f(xc) = f(x), \quad \forall x, c \in C_p^\infty.$$

However, if $f(x) \neq 1$ for some $x \in C_p^\infty$, then $f(xc) \neq 1$ for all $c \in C_p^\infty$, but f has finite support. So $Z(G) \cap \mathcal{F}$ is trivial.

Next, let $(1, c) \in Z(G) \cap C_p^\infty$. Then for all $f \in \mathcal{F}$,

$$(f^{-1}, 1)(1, c)(f, 1) = (f^{-1}, 1)(f^c, c) = (f^{-1} f^c, c) = (1, c).$$

In other words,

$$f^{-1} f(xc^{-1}) = x, \quad \forall f \in \mathcal{F}, \forall x \in C_p^\infty.$$

Clearly this is only possible if $c = 1$, so $Z(G) \cap C_p^\infty$ is also trivial and this concludes the proof. ∎

Another construction involves the *infinite* group U of upper unipotent matrices over $\mathbb{F}_p$ such that all but finitely many nondiagonal entries are 0; these are "infinite" upper triangular matrices whose diagonal entries are equal to 1. If I_∞ denotes the (countably) infinite identity matrix, and O the zero matrix, U consists of matrices of the form

$$\begin{bmatrix} M & O \\ O & I_\infty \end{bmatrix}$$

where M is an upper unipotent $n \times n$ matrix for some n. For any nonidentity element of U, i.e. any nonidentity $n \times n$ matrix M, consider the equations for $2n \times 2n$ matrices

$$\begin{bmatrix} M & O \\ O & I_n \end{bmatrix} \begin{bmatrix} I_n & I_n \\ O & I_n \end{bmatrix} = \begin{bmatrix} M & M \\ O & I_n \end{bmatrix},$$

but

$$\begin{bmatrix} I_n & I_n \\ O & I_n \end{bmatrix} \begin{bmatrix} M & O \\ O & I_n \end{bmatrix} = \begin{bmatrix} M & I_n \\ O & I_n \end{bmatrix}.$$

[17] We do not assume that f is a homomorphism!

[18] If $f(a) \neq 1$, choose g so that $g(ac) = f(a)^{-1}$ and $g(x) = 1$ otherwise. Then, $(g^{-1}, 1)(f, c)(g, 1) = (g^{-1} f g^{c^{-1}}, c)$, and the support of $g^{-1} f g^{c^{-1}}$ is a proper subset of that of f.

In other words, for any nonidentity matrix in U, we can find a matrix in U with which it does not commute, namely

$$\begin{bmatrix} M & O & O \\ O & I_n & O \\ O & O & I_\infty \end{bmatrix}\begin{bmatrix} I_n & I_n & O \\ O & I_n & O \\ O & O & I_\infty \end{bmatrix} \neq \begin{bmatrix} I_n & I_n & O \\ O & I_n & O \\ O & O & I_\infty \end{bmatrix}\begin{bmatrix} M & O & O \\ O & I_n & O \\ O & O & I_\infty \end{bmatrix}.$$

So U has trivial center.[19]

The Frattini subgroup

Let us return to finite p-groups. How far are they from being abelian?

Definition 2.32. A is an *elementary abelian p-group* if A is abelian and the order of every nonidentity element is p. Equivalently, A is a vector space over $\mathbb{F}_p$.

Proposition 2.33. *If G is a finite p-group, and $H \leq G$ a proper subgroup, then H is a proper subgroup of $N_G(H)$.*

Proof. We proceed by induction, the case $|G| = p$ being trivial. Suppose $|G| = p^n$, $n \geq 2$, and H is a proper subgroup of G.

Case (1)**.** $Z(G) \leq H$.

$Z(G)$ is nontrivial, so $H/Z(G)$ is a proper subgroup of $G/Z(G)$. By the induction hypothesis, there is some $K \leq G$ such that $H/Z(G) \lhd K/Z(G)$ and the containment is proper, so $H \lhd K$ and the containment is proper in G.

Case (2)**.** $Z(G)$ is not contained in H.

Since $Z(G) \leq N_G(H)$, H must be properly contained in $N_G(H)$. □

Corollary 2.34. *If M is a maximal subgroup in a finite p-group G, then $M \lhd G$ and $|G : M| = p$.*

Definition 2.35. For any group G, the *Frattini subgroup* is

$$\Phi(G) = \bigcap_{M \leq G \text{ maxl.}} M,$$

the intersection of all maximal proper subgroups of G.

Proposition 2.36. *For any group G,*

$$\Phi(G) = \{g \in G : \langle S, g\rangle = G \implies \langle S\rangle = G\},$$

i.e. the Frattini subgroup is the set of elements that can be removed from any generating set.

Proof. We will show that the complement of the statement holds, i.e.

$$G \setminus \Phi(G) = \{g \in G : \text{ for some } S, \langle S, g\rangle = G \text{ but } \langle S\rangle \neq G\}.$$

Suppose $x \in G \setminus \Phi(G)$, so that for some maximal subgroup M, $x \notin M$. Then $\langle M, x\rangle = G$, but $\langle M\rangle \neq G$, proving the containment $\subseteq$. Conversely, suppose for some S, $\langle S, x\rangle = G$ but $\langle S\rangle \neq G$. By Zorn's lemma, the set

$$\left\{H \leq G : \langle S\rangle \leq H, x \notin H\right\}$$

has a maximal element H, and this is a maximal proper subgroup of G not containing x; $x \in G \setminus \Phi(G)$. □

... and we return to p-groups.

Proposition 2.37. *If G is a finite p-group, $\Phi(G)$ is the smallest normal subgroup such that $G/\Phi(G)$ is an elementary abelian p-group.*

[19]There is a less constructive proof of this using projective limits: namely that U embeds in the projective limit of U_n, the upper $n \times n$ unipotent matrices. On one hand, the projection $U \to U_n$ by restricting to the upper $n \times n$ submatrix maps the center of U into the center of U_n. On the other hand, the projections $U_n \to U_{n-1}$ map the center of U_n trivially, so the center of U must be trivial as well.

Proof. If $M \leq G$ is a maximal subgroup, then G/M is cyclic of order p, so $[G,G] \leq M$. Then $[G,G] \leq \Phi(G)$, so $G/\Phi(G)$ is abelian. Further, for any $x \in G$, and any maximal subgroup M in G, $x^p \in M$, so $x^p \in \Phi(G)$ and $G/\Phi(G)$ is elementary abelian.

Conversely, suppose G/N is elementary abelian. For any $x \notin N$, there is a maximal subspace of G/N not containing xN. This corresponds to a maximal subgroup M/N in G/N such that $x \notin M$, and as a consequence, M is maximal in G. So $x \notin \Phi(G)$. This implies that $\Phi(G) \leq N$. □

Can we find a basis for $G/\Phi(G)$ as a vector space over $\mathbb{F}_p$?

Theorem 2.38 (Burnside's basis theorem)**.** *Let G be a finite p-group.* $\{g_1, \dots, g_d\}$ *is a minimal generating set for G if and only if* $\{\bar{g_1}, \dots, \bar{g_d}\}$ *is a minimal generating set for* $G/\Phi(G)$.

Proof.

$$\langle g_1, \dots, g_d \rangle = G \iff \langle g_1, \dots, g_d, \Phi(G) \rangle = G \iff \langle g_1\Phi(G), \dots, g_d\Phi(G) \rangle = G/\Phi(G).$$

Clearly one of the generating sets is minimal if and only if the other is. □

3 Nilpotent and solvable groups

3.1 Nilpotent groups

Recall that S_3 is the smallest nonabelian group, so any group that is a proper subgroup or quotient group of S_3 is abelian. More generally, we want to classify groups that can be built up as extensions of abelian groups. The most natural approach is to consider groups that can be built up from their centers.

Definition 3.1. The *upper central series* of G is

$$1 = Z^0(G) \leq Z^1(G) \leq \dots$$

where $Z^{n+1}(G)$ is defined by[20]

$$Z^{n+1}/Z^n = Z(G/Z^n).$$

Definition 3.2. G is *nilpotent* if its upper central series terminates in finitely many steps, i.e. $Z^n = G$ for some $n \in \mathbb{N}$. The least such n is called the *nilpotency class* of G.

Exercise 37. Z^n is characteristic in G $\forall n \in \mathbb{N}$.

It is easy to see that G has nilpotency class 1 if and only if G is abelian. However, there exist nonabelian nilpotent groups. For example, since any p-group has nontrivial center,

Proposition 3.3. *Any finite p-group is nilpotent.*

And we know that there exist nonabelian p-groups.

Lemma 3.4. *If* $G/Z(G)$ *is nilpotent, so is* G.

Proof. Let $H = G/Z(G)$.

$$Z^{n+1}(H)/Z^n(H) = Z(H/Z^n(H)).$$

But $H/Z^n(H) \cong G/Z^n(G)$, so by induction $Z^n(H) = Z^n(G)/Z(G)$ and the upper central series of G terminates. □

Of course, it is not always easy to compute the upper central series, so let us look at several equivalent characterisations:

Theorem 3.5. *Let G be a finite group. The following are equivalent.*

1. *G is nilpotent.*

[20] Sometimes it will be easier on the eyes to write Z^n instead of $Z^n(G)$, when G is clear from context.

2. *G has a central series,* $1 = H^0 \lhd H^1 \lhd \cdots \lhd H^n = G$*, such that* $H^{i+1}/H^i \leq Z\big(G/H^i\big)$ *for all* i*.*

3. *Every proper subgroup of G is a proper subgroup of its normalizer.*

4. *Every Sylow subgroup is normal in* G*.*

5. *G is isomorphic to the direct sum of its Sylow subgroups.*

6. *Every maximal subgroup of G is normal.*

I am sure there are several other equivalent conditions one can concoct, but these are the most useful.

Remark. The second condition says that it suffices to find a good sequence of normal subgroups, not necessarily the center. The last 4 conditions generalise nice properties of abelian groups, and show that the largest class of groups satisfying these is that of the nilpotent groups.

In order to prove the equivalence of the last property, we will need Frattini's argument.

Proposition 2.28. *(Frattini's argument) Let G be a finite group,* $H \lhd G$*, and P a Sylow p-subgroup of H. Then* $G = HN_G(P)$*, and* $|G : H|$ *divides* $|N_G(P)|$*.*

Proof of Theorem 3.5. $1 \implies 2$ is clear.

$2 \implies 3$: We proceed by induction on $|G|$, the case $|G| \leq 5$ being trivial. By 2, it follows that $Z(G) \neq 1$. If H does not contain $Z(G)$, then $Z(G) \leq N_G(H)$, so H is properly contained in $N_G(H)$. Suppose $Z(G) \leq H$. Applying the induction hypothesis to $G/Z(G)$, $H/Z(G)$ is properly contained in its normalizer $N/Z(G) \leq G/Z(G)$. However, $N = N_G(H)$, so H is properly contained in it in G.

$3 \implies 4$: If G is a p-group for some prime p this is clear. Otherwise, let P be a (proper) Sylow p-subgroup of G, and $N = N_G(P)$. P is normal in N, so it is the unique Sylow p-subgroup of N, so it is characteristic in N. This implies that $P \lhd N_G(N)$. If N is a proper subgroup of G, then $N_G(N)$ is strictly bigger than N, which is not possible. so $N = G$, i.e. $P \lhd G$.

$4 \implies 5$: We show by induction that if $P_1, \ldots, P_t$ are distinct (normal) Sylow p-subgroups of G, then $P_1 \ldots P_t \cong P_1 \times \cdots \times P_t$. The base case $t = 1$ is an exercise for the reader. For the general case,

$$P_t \cap (P_1 \ldots P_{t-1}) = 1 \implies P_1 \ldots P_{t-1}P_t \cong P_1 \times \cdots \times P_t.$$

$5 \implies 1$: Again, we proceed by induction, and take the base case $|G| \leq 5$ for granted. Since $G \cong P_1 \times \cdots \times P_r$, $Z(G) \cong Z(P_1) \times Z(P_r)$. By induction, $G/Z(G)$ is nilpotent, so G is nilpotent by the earlier lemma.

$3 \implies 6$: If M is a maximal proper subgroup of G, and M is properly contained in its normalizer, then M is normal in G.

$6 \implies 5$: Suppose P is a Sylow p-subgroup of G that is not normal, and M a maximal proper subgroup of G containing $N_G(P)$. $M \lhd G$, so by Frattini's argument, $G = MN_G(P)$, contradicting our choice of M.

□

Now that we have several definitions for nilpotent groups, let us study some properties.

Proposition 3.6. *The class of nilpotent groups is closed under subgroups, quotient groups, and finite direct products.*

The converse is not true: if N and G/N are nilpotent, G need not be nilpotent.

Exercise 38. S_3 is not nilpotent.

Corollary 3.7. *If A is a maximal normal abelian subgroup of a nilpotent group G, then* $A = C_G(A)$*.*

Proposition 3.8. *If G is nilpotent and* $1 \neq N \lhd G$*, then* $N \cap Z(G)$ *is nontrivial.*

Proof. There is some i for which $N \cap Z^i$ is trivial, and $N \cap Z^{i+1}$ is nontrivial. It is easy to check that for the upper central series,

$$[G, Z^{i+1}] \leq Z^i.$$

Since N is normal in G, we also have $[G, N] \leq N$. In other words,

$$[G, N \cap Z^{i+1}] \leq [G, N] \cap [G, Z^{i+1}] \leq N \cap Z^i = \{1\}.$$

This shows that $N \cap Z^{i+1}(G) \leq Z(G)$, and by hypothesis this is a nontrivial subgroup of N contained in $Z(G)$; $N \cap Z(G) \neq \{1\}$ and $i = 1$. □

Corollary 3.9. *A minimal normal subgroup of a nilpotent group is contained in the center.*

3.2 Solvable groups

Our greatest disappointment from the previous subsection is that the extension of a nilpotent group by a nilpotent group need not be nilpotent. So let us define a larger class of groups – solvable groups – that is closed under such extensions.

Definition 3.10. The *derived series* of G is

$$G = G^{(0)} \geq G^{(1)} \geq \dots$$

where

$$G^{(n+1)} = [G^{(n)}, G^{(n)}].$$

Just as we defined a nilpotent group,

Definition 3.11. G is *solvable* if its derived series terminates in finitely many steps, i.e. $G^{(n)} = \{1\}$ for some $n \in \mathbb{N}$.

As the commutator subgroup $[G, G]$ is often denoted by G', the term derived series makes sense. Again, we look at several equivalent characterisations of solvability.

Theorem 3.12. *Let G be a finite group. The following are equivalent.*

1. *G is solvable.*
2. *There is a sequence $G = G_0 \geq G_1 \geq \dots G_n = \{1\}$ such that $G_i \lhd G$ and G_{i-1}/G_i is abelian for all i.*
3. *There is a sequence $G = G_0 \geq G_1 \geq \dots G_n = \{1\}$ such that $G_i \lhd G_{i-1}$ and G_{i-1}/G_i has prime order for all i.*

Proof. $1 \implies 2$ is clear.

$2 \implies 3$: If G_{i-1}/G_i is abelian, by the fundamental theorem of abelian groups, we can find intermediate subgroups $G_i = H_1 \leq H_2 \cdots \leq H_k = G_{i-1}$ so that H_j/H_{j-1} has prime order. Note that the resulting H_j need not be normal in G, but it is normal in G_{i-1}.

$3 \implies 1$: We show by induction that $G^{(i)} \leq G_i$. The base case is clear, as G/G_1 is abelian implies that $[G, G] \leq G_1$. In general, since G_i/G_{i+1} is abelian,

$$G^{(i+1)} = [G^{(i)}G^{(i)}] \leq [G_iG_i] \leq G_{i+1}.$$

□

It is similarly easy to check:

Proposition 3.13. *The class of solvable groups is closed under subgroups, quotient groups, and finite direct products.*

Unlike for nilpotent groups,

Proposition 3.14 (Three-for-two)**.** *If N and G/N are solvable, so is G.*

The many characterisations of nilpotent and solvable groups make the following proposition easy.

Proposition 3.15. *Every nilpotent group is solvable.* [21]

However, the converse is not true.

Exercise 39. S_3 is solvable.

Why are solvable groups interesting? It is straightfoward to check that if H and K are normal solvable subgroups of G, then HK is solvable. In particular, every finite group G contains a maximal normal solvable subgroup S. The quotient ${}^{G}\!/_{S}$, if nontrivial, is not solvable, hence contains no abelian normal subgroups. That is, every group is the extension of a group with no abelian normal subgroups by a solvable group.

3.3 The Three-Subgroup Lemma

Let us study some further structure of nilpotent groups.

Definition 3.16. The *lower central series* of G is

$$G = Z_0(G) \geq Z_1(G) \geq \dots$$

where

$$Z_{n+1}(G) = [G, Z_n(G)].$$

Again, for convenience, we will simply write Z_n when G is clear from context.

As the lower central series is obtained by repeatedly taking commutators, let us list some properties of commutators. Some notation: just as x^G denotes the conjugacy class of x in G, let x^g denote the conjugate of x by g, $g^{-1}xg$. Denote by $[x_1, \dots, x_n] = [[x_1, \dots, x_{n-1}], x_n]$ (the order matters!)

Proposition 3.17. *Let $x, y, z \in G$.*

(i) $[x, y] = [y, x]^{-1}$.

(ii) $[xy, z] = [x, z]^y [y, z]$ *and* $[x, yz] = [x, z][x, y]^z$.

(iii) $[x, y^{-1}, z] = \left([x, y]^{y^{-1}}\right)^{-1}$.

(iv) (Witt identity)

$$[x, y^{-1}, z]^y [y, z^{-1}, x]^z [z, x^{-1}, y]^x = 1.$$

Proof. The first three claims are straightforward to prove. For the Witt identity, observe that setting

$$u = xzx^{-1}yx, \quad v = yxy^{-1}zy, \quad w = zyz^{-1}xz$$

yields

$$[x, y^{-1}, z]^y = u^{-1}v, \quad [y, z^{-1}, x]^z = v^{-1}w, \quad [z, x^{-1}, y]^x = w^{-1}u.$$

□

Given any sets $X, Y \subset G$, we can define their commutator subgroup to be

$$[X, Y] = \langle [x_1, x_2] : x_1 \in X_1, x_2 \in X_2 \rangle$$

and extend this to finitely many terms,

$$[X_1, \dots, X_n] = [[X_1, \dots, X_{n-1}], X_n].$$

Denote by $X_1^{X_2}$ the subgroup generated by all conjugates of elements of X_1 by elements of X_2,

$$X_1^{X_2} = \langle y^{-1}xy : x \in X_1, y \in X_2 \rangle.$$

[21]For example, by induction, it suffices to show that N and G/N are solvable for some nontrivial normal subgroup N.

Proposition 3.18. *Let $X \subset G$ and $K \leq G$.*

(1) $X^K = \langle X, [X, K]\rangle$.

(2) $[X, K]^K = [X, K]$.

(3) If $K = \langle Y\rangle$, *then* $[X, K] = [X, Y]^K$.

Proof. (1) follows from the identity $x^k = x[x, k]$ for each $x \in X$ and $k \in K$.

(2) The containment $[X, K] \subset [X, K]^K$ is clear. $[X, K]^K$ is generated by the elements $[x, k_1]^{k_2}$. Using identity (ii) from the previous proposition,
$$[x, k_1]^{k_2} = [x, k_2]^{-1}[x, k_1k_2] \in [X, K].$$

(3) Since $[X, Y]^K = [X, Y] \leq [X, K]$ by (2), it suffices to show that $[X, K] \leq [X, Y]^K$. For each $k \in K$, we have an expression
$$k = y_1^{\epsilon_1} \dots y_r^{\epsilon_r} : \quad y_i \in Y, \epsilon_i = \pm 1.$$
If $r = 1$, then
$$[x, y_1] \in [X, Y]^K, \text{ and } [x, y_1^{-1}] = \left([x, y_1]^{y_1^{-1}}\right)^{-1} \in [X, Y]^K$$
using identity (iii) from the previous proposition. By induction on r, if $r > 1$, let $k' = ky_r^{-\epsilon_r}$. Then, using identity (ii) from the previous proposition,
$$[x, k] = [x, y_r^{\epsilon_r}][x, k']^{y_r^{\epsilon_r}}.$$
This product belongs to $[X, Y]^K$ by the induction hypothesis, completing the proof. □

Now let us return to the relationship between the upper and lower central series. $1 = H^0 \leq H^1 \leq \cdots \leq H^n = G$ is called a *central series* if each quotient H^{i+1}/H^i is contained in the center of G/H^i.

Proposition 3.19. *Let $1 = H^0 \leq H^1 \leq \cdots \leq H^n = G$ be a central series of G.*

(1) $Z_i \leq H^{n-i+1}$, *so* $Z_{n+1} = 1$.

(2) $H^i \leq Z^i$, *so* $Z^n = G$.

(3) G is nilpotent if and only if its lower central series terminates, in which case its nilpotency class is the length of the lower central series, which is the length of the upper central series.

Proof. We prove (1) by induction on i, and the proof of (2) will be analogous. Clearly if $i = 1$, then $Z_1 \leq H^n$. For $i > 1$, since H^{n-i+1}/H^{n-i} is in the center of G/H^{n-i}, $[H^{n-i+1}, G] \leq H^{n-i}$. By the induction hypothesis,
$$Z_{i+1} = [Z_i, G] \leq [H^{n-i+1}, G] \leq H^{n-i}.$$
To prove (3), note that (1) and (2) imply that the upper and lower central series are the shortest central series of G. □

To establish further relationships, we will need the following "lemma".

Theorem 3.20 (Three subgroup lemma)**.** *Let $H, K, L \leq G$, and $N \lhd G$. If two of $[H, K, L]$, $[K, L, H]$, and $[L, H, K]$ are contained in N, so is the third.*

Proof. The Witt identity shows that if two of $[h, k^{-1}, l]$, $[k, l^{-1}, h]$, $[l, h^{-1}, k]$ belong to a normal subgroup of G, so does the third, and this implies the result. □

From this,

Corollary 3.21. *Let G be a group and $i, j > 0$. Then,*

(i) $[Z_i, Z_j] \leq Z_{i+j}$,

(ii) $Z_i(Z_j(G)) \leq Z_{ij}(G)$,

(iii) $[Z_i, Z^j] \leq Z^{j-1}$ *if* $j \geq i$, *and*

(iv) $Z^i(G/Z^j) = Z^{i+j}/Z^j$.

Each can be proved by a standard induction argument, and we have seen many of those already, so the proof is left as an exercise.

3.4 Hall's theorems

Now let us study solvable groups.

Let Π be a set of primes. We say a number is Π' if it is coprime to every prime in Π. Sylow's theorem says that for any finite group G and any prime p dividing $|G|$, if $\Pi = \{p\}$, then there is a subgroup $H \leq G$ so that $|G : H|$ is Π', and any two such subgroups are conjugate. What if we generalised this to an arbitrary set of primes?

Definition 3.22. If Π is a set of primes, a Π-*subgroup* is a subgroup H of G if each of the primes dividing $|H|$ is in Π. H is a *Hall* Π-subgroup if it is a Π-subgroup and $|G : H|$ is Π'.

That is, if $|G| = p_1^{\alpha_1} \dots p_r^{\alpha_r}$ is its prime factorisation, and $\Pi = \{p_1, \dots, p_l\}$, then H is a Hall Π-subgroup of G if and only if $|H| = p_1^{\alpha_1} \dots p_l^{\alpha_l}$. Of course, Hall Π-subgroups need not exist; A_5 has no Hall $\{3, 5\}$-subgroup. In this section we will prove Hall's theorem(s).

Theorem 3.23. *(Hall's first theorem) Let G be a finite solvable group, and* Π *a set of primes dividing* $|G|$. *Then,*

1. *G contains a Hall* Π-*subgroup, and*
2. *any* Π-*subgroup is contained in the conjugate of a given Hall* Π-*subgroup.*

Note that the second condition implies that any two Hall Π-subgroups are conjugate. It is perhaps surprising that the converse of this theorem also holds.

Theorem 3.24. *(Hall's second theorem) Let G be a finite group. If G contains a Hall* Π-*subgroup for every set of primes* Π *dividing* $|G|$, *then G is solvable.*

We will need some preliminary results.

Lemma 3.25. *Let G be a finite solvable group. If* $M \lhd G$ *is a minimal normal subgroup, M is an elementary abelian* p-*group.*

Proof. M is solvable, so if M is simple, then $M \cong \mathbb{Z}_p$ for some prime p. If not, then $M' = [M, M]$ is characteristic in M, so it is normal in G. Since M is solvable but not simple, it has a proper normal subgroup N of prime index, so $M' \leq N$. By the minimality of M, $M' = \{1\}$ so M is abelian. If p divides $|M|$, then $\{x \in M : x^p = 1\}$ is characteristic in M, hence normal in G, so M is an elementary abelian p-group. □

And recall

Proposition 2.28. *(Frattini's argument) Let G be a finite group,* $H \lhd G$, *and P a Sylow p-subgroup of H. Then* $G = HN_G(P)$, *and* $|G : H|$ *divides* $|N_G(P)|$.

Proof of Hall's first theorem. We proceed by induction on G, the case $|G| \leq 5$ a triviality. Now for the general case, if G is simple then it has prime order, so there is again nothing to prove.

Let M be a minimal normal subgroup of G, and L any Π-subgroup of G. We distinguish three cases:

Case (1)**.** G/M is not a Π-group, i.e. there is a prime $q \notin \Pi$ that divides $|G : M|$.

By induction, G/M contains a nontrivial Hall Π-subgroup K/M, and $|G : K|$ is Π'. As K is a proper subgroup of G, we again use the induction hypothesis to find a Hall Π-subgroup H of K, and this is a Hall Π-subgroup of G.

Now, LM/M is a Π-subgroup in K/M, so it is contained in some conjugate of K/M. So a conjugate of LM is contained in K, and applying the induction hypothesis to K, LM is contained in a conjugate of H.

Case (2)**.** M is an elementary abelian p-group for $p \in \Pi$.

Let H/M be a Hall Π-subgroup in G/M, so H is a Hall Π-subgroup in G. By induction, LM/M is contained in a conjugate of HM/M, so LM is contained in a conjugate of HM. By the maximality of H, $HM = H$, so L is contained in a conjugate of H.

Case (3)**.** M is an elementary abelian p-group for $p \notin \Pi$, and G/M is a Π-group.

In this case, $|G| = ap^m$, where $|M| = p^m$ and Π is the set of primes dividing a. Let N/M be a minimal normal subgroup of G/M, so N/M is an elementary abelian q-group for some $q \in \Pi$. Let $Q \leq N$ be a Sylow q-subgroup. If Q is normal in G, we may proceed as in case (2), so we assume that $N_G(Q)$ is a proper subgroup of G. By Frattini's argument, $NN_G(Q) = G$. Since $Q \leq N_G(Q)$, and $QM = N$, we can write $MN_G(Q) = G$. Then $M \cap N_G(Q)$ is normal in $MN_G(Q) = G$. M cannot be contained in $N_G(Q)$ as $N_G(Q) \neq G$, so $M \cap N_G(Q) = 1$. Then $|N_G(Q)| = a$, i.e. it is a Hall Π-subgroup of G.

Now, $LM \cap N_G(Q)$ is a Π-subgroup of LM; we claim that it is in fact a Hall Π-subgroup of LM. Note that

$$LM = LM \cap G = LM \cap N_G(Q)M = (LM \cap N_G(Q))M$$

so,

$$|LM : LM \cap N_G(Q)| = |(LM \cap N_G(Q))M : LM \cap N_G(Q)| = |M|$$

where the last equality follows from the second isomorphism theorem and the fact that $M \cap N_G(Q) = 1$. If $LM \neq G$, by induction L is contained in a conjugate of $LM \cap N_G(Q)$. If $LM = G$, then $LN = G$, and $L \cap N$ is a Sylow q-subgroup Q_1 in N. Q_1 is conjugate to Q, so $N_G(Q_1)$ is conjugate to to $N_G(Q)$. Further, $Q_1 = L \cap N \lhd L$, so $L \leq N_G(Q_1)$ is contained in a conjugate of $N_G(Q)$. □

To prove the second theorem, we will need a theorem that will be proved later using representation theory.

Theorem 3.26. *[Burnside's theorem] Groups of order $p^a q^b$ are solvable.*

Proof of Hall's second theorem. We proceed by induction on the number of prime divisors of $|G|$. If G is a p-group, or if G has order $p^a q^b$, then G is automatically solvable, so the theorem holds. Suppose $|G| = p_1^{e_1} \dots p_k^{e_k}$ contains a Hall Π-subgroup for every set of primes Π dividing $|G|$, but G is not solvable. If N is a nontrivial normal subgroup of G, and H a Hall Π-subgroup of G, then $H \cap N$ and HN/N are Hall Π-subgroups of N and G/N respectively. By the induction hypothesis, N and G/N are solvable, but this contradicts our assumption that G is not solvable. So G must be simple.

By Burnside's theorem, we know that $k > 2$. For each prime p_i, let $\Pi_i = \{p_1, \dots, p_k\} \setminus \{p_i\}$, and H_i be a Hall Π_i-subgroup of G. Let $H = H_3 \cap \dots \cap H_k$. A quick computation tells us that $|G : H| = p_3^{e_3} \dots p_k^{e_k}$, so $|H| = p_1^{e_1} p_2^{e_2}$; H is solvable. Let M be a minimal normal subgroup of H, and suppose M is an elementary abelian p_1-group. $|H \cap H_2| = p_1^{e_1}$ is a Sylow p_1 subgroup of H, and M is normal, so $M \leq H \cap H_2 \leq H_2$. By order considerations, $G = (H \cap H_1)H_2$. It follows that

$$M^G = M^{H_2} \leq H_2 \leq G$$

is a proper nontrivial normal subgroup of G, contradicting that G is simple. Finally, we circle back to our original (false) assumption and deduce that G is solvable. □

3.5 Supersolvable groups

Recall the equivalent definitions of a solvable group:

Theorem 3.12. *Let G be a finite group. The following are equivalent.*

1. *G is solvable.*
2. *There is a sequence $G = G_0 \geq G_1 \geq \dots G_n = \{1\}$ such that $G_i \lhd G$ and G_{i-1}/G_i is abelian for all i.*
3. *There is a sequence $G = G_0 \geq G_1 \geq \dots G_n = \{1\}$ such that $G_i \lhd G_{i-1}$ and G_{i-1}/G_i has prime order for all i.*

A *supersolvable* group is obtained by merging definitions 2. and 3.

Definition 3.27. G is a *supersolvable group* if there is a sequence $G = G_0 \geq G_1 \geq \cdots \geq G_n = \{1\}$ such that $G_i \lhd G$ and G_{i-1}/G_i has prime order for all i.

Vigyázz. Clearly a supersolvable group is solvable, but the converse is not true! For example, the commutator of the alternating group A_4 is isomorphic to the Klein-four group V_4 which is abelian, so A_4 is solvable. However, A_4 has no cyclic normal subgroup, so it cannot be supersolvable.

Our goal is to characterise supersolvable groups by their *subgroup lattices*.

Definition 3.28. The *subgroup lattice* of a group G is the partially ordered set $\{H : H \text{ is a subgroup of } G\}$ ordered by inclusion. The *meet* of two subgroups $H, K \leq G$ is the smallest subgroup containing them, i.e. $\langle H, K\rangle$, and their *join* is the largest subgroup contained in them, i.e. $H \cap K$.

In general, given a poset $\mathcal{P}$, one may define its *Hasse diagram*. This is the directed graph on the vertex set $\mathcal{P}$ with an edge (u, v) if and only if $u \leq v$ and there is no other $w \in \mathcal{P}$ such that $u \leq w \leq v$. It is the Hasse diagram which is typically referred to as the lattice of a group. Of course, given a finite group G, this is a finite graph, so we may speak about things like "longest paths". The "source" vertex of the subgroup lattice of G is the identity subgroup, while the "sink" vertex is G itself, and every other subgroup of G lies on a directed path from $\{1\}$ to G. A natural question to ask is: do all directed paths from $\{1\}$ to G have the same length? We say G satisfies the *(Jordan-Dedekind) chain condition* if this holds.

Theorem 3.29 (Iwasawa)**.** *G satisfies the chain condition if and only if G is supersolvable.*

Let us first look at some structure of supersolvable groups.

Lemma 3.30. *If G is supersolvable, there is a unique chain $1 = N_0 \leq N_1 \leq \cdots \leq N_k \leq G$ such that $N_i \lhd G$, N_i/N_{i-1} has order p_i for some prime p_i, and $p_1 \geq \cdots \geq p_k$.*

Proof. We know that G has a normal series $1 = G_0 \leq \cdots \leq G_k \leq G$ such that the successive quotients are prime. Suppose G_{i+1}/G_i has order p_{i+1}, G_i/G_{i-1} order p_i, and $p_{i+1} > p_i$. Then, G_{i+1}/G_{i-1} has a unique Sylow p_{i+1}-subgroup N[22] which is characteristic in G_{i+1}, therefore normal in G. Replacing G_i with N, $p_i = |G_{i+1}/N| < |N/G_{i-1}| = p_{i+1}$. Repeating this process finitely many times, we obtain the desired series. □

Corollary 3.31. *If q is the largest prime divisor of $|G|$, G has a normal subgroup of order q.*

Corollary 3.32. *If q is the largest prime divisor of $|G|$, G has a unique Sylow q-subgroup.*

We state the following lemma without proof, as the argument is routine.

Lemma 3.33. *Abelian groups and nilpotent groups are supersolvable. Subgroups and quotients of supersolvable groups are supersovable.*

Vigyázz. A three-for-two result does not hold! For example, $V_4 \leq A_4$ and A_4/V_4 are supersolvable, but A_4 is not.

Lemma 3.34. *The index of a maximal subgroup in a supersolvable group is prime.*

Proof. Let $H \leq G$ be a maximal subgroup, and M a minimal normal subgroup of prime order. If $M \nleq H$, then $H \cap M = \{1\}$, $HM = G$, so $|G : H| = M$. Otherwise, H/M is maximal in G/M and the result follows by induction on $|G|$. □

Proof of Theorem 3.29. Suppose G is supersolvable, and $1 = H_0 \leq H_1 \leq \cdots \leq H_k = G$ is a directed path in the subgroup lattice. H_{i-1} is a maximal subgroup in H_i, which is supersolvable, so H_i/H_{i-1} has prime order. Then, k is the number of prime factors (including multiplicity) of $|G|$, so all such paths have the same length.

For the converse, we prove the statement for solvable groups. Then, we have a series $1 = G_0 \leq G_1 \leq \cdots \leq G_k = G$ such that $G_{i-1} \lhd G_i$ and G_i/G_{i-1} has prime order. This is clearly a maximal directed path, so the length of every maximal directed path is the number of prime factors (including multiplicity) of $|G|$. As a result, every maximal subgroup of G has prime index. Our goal is to find a normal subgroup $N \lhd G$ of prime order. The subgroup lattice of G/N is the union of the directed paths from N to G, and since N is a minimal subgroup of G, the subgroup lattice of G/N satisfies the chain condition, and we may apply induction to say that G/N is supersolvable. By the minimality of N, a normal series of G/N such that successive quotients have prime order extends to a normal series of G with the same property.

Let A be a minimal normal subgroup of G, hence an elementary abelian p-group for some prime p.

[22] Recall Corollary 1.24.

Case (1)**.** A is a Sylow p-subgroup of G.

By the Schur-Zassenhaus theorem, there exists $H \leq G$ such that $G = AH$, $A \cap H = 1$. If H is properly contained in some subgroup $K \leq G$, then $K \cap A \neq \{1\}$, so $K = G$ by the minimality of A. This implies that H is a maximal subgroup of G, so $A \lhd G$ has prime order.

Case (2)**.** A is not a Sylow p-subgroup of G, and p is not the largest prime divisor of $|G|$.

Let q be the largest prime divisor of G. Since G/A is solvable, it has a normal subgroup B/A of order q. $|B| = p^k q$ and is supersolvable by the induction hypothesis, so it has a unique Sylow q-subgroup Q. $Q \operatorname{char} B$ and $B \lhd G$, so $Q \lhd G$ has prime order.

Case (3)**.** A is not a Sylow p-subgroup of G, and p is the largest prime divisor of $|G|$.

Let P be a Sylow p-subgroup of G containing A, so P/A is Sylow p-subgroup of G/A. Since A is abelian and supersolvable, G/A satisfies the chain condition. Since p is the largest prime divisor of $|G/A|$, $P/A \lhd G/A$, so $P \lhd G$. Further, $A \lhd P$, so $A \cap Z(P)$ is nontrivial. However, $Z(P) \operatorname{char} P$, so $A \cap Z(P) \lhd G$, hence $A \leq Z(P)$. By the Schur-Zassenhaus theorem, there is some $H \leq G$ such that $PH = G$ and $P \cap H = \{1\}$. Let K be a maximal subgroup of G containing H, so $|G : K| = p$. Since $K \cap A$ is normal in both K and P, $K \cap A = \{1\}$ or A. In the first case, A has order p and we are done. In the second case, $A \leq K$. By the induction hypothesis, K satisfies the chain condition so K is supersolvable and contains a minimal normal subgroup $A_1 \leq A$ of order p. Then, $N_G(A_1) \leq K$, and $A_1 \leq A \leq Z(P)$, so $A_1 \lhd G$ has prime order.

□

4 Permutation groups

How do we generalise the idea of a transitive permutation group? We can define k-transitivity, where we would like 1-transitivity to just be transitivity. Let $\Omega^{(k)}$ denote the set of ordered k-tuples of Ω whose elements are *pairwise distinct*. If G acts on Ω, then it induces an action on $\Omega^{(k)}$ by

$$(\omega_1, \dots, \omega_k) \to (\omega_1 g, \dots, \omega_k g).$$

Definition 4.1. G acts *k-transitively* on Ω if its induced action on $\Omega^{(k)}$ is transitive.

We would like k-transitivity to imply $(k-1)$-transitivity, which is not immediate from this definition, and we would also like it to mean that after "removing one level" of transitivity, we obtain a $(k-1)$-transitive action. For these reasons, the following characterisation is often more useful.

Proposition 4.2. *Let $k > 1$ and $\omega \in \Omega$. G acts k-transitively on Ω if and only if G_ω acts $(k-1)$-transitively on $\Omega \setminus \{\omega\}$.*

Proof. This is a standard definition-chasing type argument. Suppose G_ω acts $(k-1)$-transitively on $\Omega \setminus \{\omega\}$ for every $\omega \in \Omega$. Let $(\alpha_1, \dots, \alpha_k)$ and $(\beta_1, \dots, \beta_k)$ be in $\Omega^{(k)}$. Then there is some $g \in G_{\alpha_1}$ and $h \in G_{\beta_k}$ such that

$$(\alpha_1, \dots, \alpha_k) \xrightarrow{g} (\alpha_1, \beta_2, \dots, \beta_k) \xrightarrow{h} (\beta_1, \beta_2, \dots, \beta_k).$$

So gh is the desired element of G. The reverse implication is even easier to prove. □

Corollary 4.3. *If G acts k-transitively on Ω, and $|\Omega| = n$, then $n(n-1)\dots(n-k+1)$ divides $|G|$.*

If G acts faithfully on a set of cardinality n, we will say G is a permutation group of *degree n*.

Exercise 40. S_n is n-transitive and A_n is $(n-2)$-transitive.

Corollary 4.4. *If G is a finite $(n-2)$-transitive group of degree n, then G is A_n or S_n.*

Sajnos, there are not "many" k-transitive groups. In fact, for $k \geq 6$ and arbitrary n, the only k-transitive groups of degree n are A_n and S_n. This motivates the definition of a *primitive* permutation group, which has weaker requirements than 2-transitivity.

4.1 Primitive permutation groups

Let G be a finite group acting *transitively* on Ω. $\Delta \subset \Omega$ is a *block* for G if for every $g \in G$, $\Delta \cap \Delta g = \Delta$ or $\Delta \cap \Delta g = \emptyset$. Further, the sets $\{\Delta g : g \in G\}$ partition Ω. Of course, we may take the *trivial blocks*: $\Delta = \Omega$ or $\Delta = \{\omega\}$ for some $\omega \in \Omega$, and these will be blocks for any group G.

A system of blocks corresponds to a *G-invariant equivalence relation* $\sim$ on Ω, where $\omega \sim \omega'$ implies $\omega \cdot g \sim \omega' \cdot g$ for all $g \in G$.

Definition 4.5. G is a *primitive permutation group* on Ω if G is transitive and G has no nontrivial blocks.

Equivalently,

Proposition 4.6. *A transitive group G acts primitively on Ω if and only if each stabilizer G_ω is a maximal subgroup of G.*

Proof. Here is another definition-chasing argument. Suppose G acts primitively on Ω, and let H be a subgroup of G properly containing some G_ω. Define

$$\Delta = \{\omega \cdot h : h \in H\}.$$

Since H properly contains G_ω, $|\Delta| \geq 2$. Further, suppose $\Delta \cdot g \cap \Delta \neq \emptyset$ for some $g \in G$. Then, for some $h \in H$,

$$\omega g = \omega h \implies h^{-1} g \in G_\omega \implies g \in H.$$

So Δ is a block for G. If H is a proper subgroup of G, then $|H : G_\omega| < |G : G_\omega| = |\Omega|$, so Δ is a nontrivial block for G, which is not possible, so G_ω is maximal.

Conversely, suppose G is not primitive; let Δ be a nontrivial block and $\sim$ the corresponding equivalence relation. Again, let H be the *setwise stabilizer* of Δ,

$$H = \{g \in G : \Delta \cdot g \subset \Delta\}$$

H is a proper subgroup of G since G is transitive, and clearly H properly contains any stabilizer G_ω for $\omega \in \Delta$. □

Exercise 41. If $A \leq S_\Omega$ and $B \leq S_\Gamma$ then the "natural" action of $A \times B$ on $\Omega \times \Gamma$ is not primitive.

Clearly, if a subgroup is maximal, so are all of its conjugates. So the problem of determining maximal subgroups is in some sense equivalent to the problem of determining primitive actions of a group. We will see this more explicitly when we apply the *O' Nan-Scott theorem* (the classification of all finite primitive permutation groups) to determine all maximal subgroups of S_n.

This is a good point to stop and remark on the difference between the *pointwise stabilizer* and the *setwise stabilizer* of $\Delta \subset \Omega$. The *setwise stabilizer* is

$$G_{\{\Delta\}} = \left\{g \in G : \Delta \cdot g = \Delta\right\},$$

while the *pointwise stabilizer* is

$$G_\Delta = \left\{g \in G : \delta g = \delta, \forall \delta \in \Delta\right\} = \bigcap_{\delta \in \Delta} G_\delta.$$ [23]

Exercise 42. If G is 2-transitive, then G is primitive.

Is there a converse to this exercise?

Theorem 4.7 (Jordan)**.** *Let $G \leq \mathrm{Sym}\Omega$ be a finite primitive permutation group. Let $\Delta \subset \Omega$, $1 \leq |\Delta| \leq |\Omega| - 2$.*

(a) If G_Δ is transitive on Γ, then G is 2-transitive on Ω.

(b) If G_Δ is primitive on Γ, then G is $(|\Delta| + 1)$-transitive on Ω.

Proof. For convenience, let $|\Omega| = n$.

[23]Not to be confused with the G_δ sets of topology.

(a) We proceed by induction on Δ; if $|\Delta| = 1$, this is clear. Suppose $|\Delta| > 1$, and also that $|\Delta| \leq n/2$. Since Δ is not a block for G, there is some $g \in G$ for which
$$1 \leq |\Delta \cdot g \cap \Delta| < |\Delta|$$
By order considerations, $\Gamma \cap \Gamma \cdot g \neq \emptyset$. Since $\langle G_\Delta, G_{\Delta \cdot g}\rangle \leq G_{\Delta \cap \Delta \cdot g}$, the latter subgroup is transitive on $\Gamma \cup \Gamma \cdot g$, so we apply the induction hypothesis. If $|\Delta| > n/2$, then $|\Gamma| \leq n/2$, so we use the induction hypothesis and the same argument as earlier.

(b) To make our lives easier, let us say G is *k-primitive* if it is k-transitive and the pointwise stabilizer of any k-element set is primitive. Equivalently, G is k-primitive if it is transitive and every point stabiliser is $(k-1)$-primitive. Our goal is to show that if G_Δ is primitive on Γ, then G is $(|\Delta|+1)$-primitive on Ω. Again, we use induction, the base case $|\Delta| = 1$ being clear. If $|\Delta| \geq 2$, we consider $G_{\Delta \cdot g \cap \Delta}$ as in (a) which is also primitive, and apply induction to obtain that G is 2-primitive. So for any $\delta \in \Delta$, G_δ is primitive, and we apply induction again to obtain that G_δ is $|\Delta|$-primitive. □

Exercise 43. If $G \leq S_p$ is transitive where p is a prime, then G is primitive.

Corollary 4.8. *If $G \leq S_n$ is primitive and contains a p-cycle where p is prime, then G is $(n-p+1)$-transitive.*

Proof. Let Γ be the support of the p-cycle $g \in G$, and $\Delta = \Omega \setminus \Gamma$. Since g is transitive on Γ, so is G_Δ, but any transitive group on a p-element set is primitive. □

Corollary 4.9. *If $G \leq S_n$ is primitive and contains a 2-cycle, then $G = S_n$. If G contains a 3-cycle, then $G \geq A_n$.*

Theorem 4.10 (Bechert's bound)**.** *If $G \leq S_n$ is primitive, either $G = A_n$, $G = S_n$, or $|S_n : G| \geq \lfloor (n+1)/2 \rfloor!$.*

Proof. Let Δ be a (cardinality) minimal set such that $G_\Delta = 1$, i.e. if g and h agree on Δ, then $g = h$. Call Δ the *base* of G. If $|\Delta| \leq n/2$, since each element of G is uniquely determined by its action on Δ,
$$|G| \leq n(n-1)\ldots(n-|\Delta|+1) = \frac{n!}{(n-|\Delta|)!}$$
or,
$$|S_n : G| \geq (n-|\Delta|)! \geq \lfloor (n+1)/2 \rfloor!$$
If $|\Delta| > n/2$, we want to show that G contains a 3-cycle so we can apply the previous corollary. Since $\Gamma = \Omega \setminus \Delta$ has smaller cardinality than Δ, $G_\Gamma \neq 1$. Choose a nonidentity element $g \in G_\Gamma$. There is some $\delta \in \Delta$ such that $\delta \cdot g \neq \delta$. Since $\Delta \setminus \{\delta\}$, is also not a base for G, there is some $h \in G_{\Delta \setminus \{\delta\}}$ such that $\delta \cdot h \in \Gamma$. It is then routine to check that $hgh^{-1}g^{-1}$ is the 3-cycle $(\omega, \omega \cdot h, \omega \cdot g)$. □

4.2 Minimal normal subgroups

We will classify primitive permutation groups by properties of their minimal normal subgroups. For the rest of this section, we only consider finite groups.

Lemma 4.11. *If $M \lhd G$ is a minimal normal subgroup, then M is a direct product of pairwise isomorphic finite simple groups.*

It will be useful to define the following notion.

Definition 4.12. A group M is *characteristically simple* if it has no nontrivial characteristic subgroups.

For example, a simple group is characteristically simple because every characteristic subgroup is normal. What does this have to do with the lemma? If M is a minimal normal subgroup, then it must be characteristically simple, and further

Lemma 4.13. *Any characteristically simple group M is the direct product of pairwise isomorphic simple groups.*

Proof. Suppose M is not simple, and let T be a minimal normal subgroup of M. Since T is not characteristic in M, we consider all the subgroups of the form $\phi(T) : \phi \in Aut(M)$. Each of these is isomorphic to T, thus a minimal normal subgroup in M. First, suppose $\phi_1(T) \neq \phi_2(T)$. Then $\phi_1(T) \cap \phi_2(T)$ must be trivial by minimality. That is, for some $k \in \mathbb{N}$,

$$\{\phi(T) : \phi \in Aut(M)\} = \{\phi_1(T), \dots, \phi_k(T)\}$$

where the $\phi_i(T)$'s are pairwise disjoint. So,

$$\phi_1(T) \times \dots \phi_k(T) \hookrightarrow M$$

However, the above direct product is characteristic in M by construction, so it must be all of M.

If T contains a nontrivial normal subgroup N, then $\phi_1(N) \times \dots \phi_k(N)$ is characteristic in M, a contradiction. So M is the direct product of pairwise isomorphic simple groups. □

Lemma 4.14. *Any normal subgroup of a direct product of finite simple groups is equal to the direct product of some of them.*

Proof. We may assume the groups are all nonabelian. Let

$$N \lhd S_1 \times \cdots \times S_k = G$$

For each S_i, $[N, S_i]$ is normal in G, so $[N, S_i] = 1$ or S_i. If N and S_i commute, then $N \cap S_i = 1$, otherwise $S_i \leq N$. □

Given a group $G = G_1 \times \cdots \times G_k$, let $\pi_i : G \longrightarrow G_i$ denote the canonical projection for $i = 1, \dots, k$.

Definition 4.15. A subgroup $H \leq G = G_1 \times \cdots \times G_k$ is called a *subdirect product* if $\pi_i(H) = G_i$ for $i = 1, \dots, k$.

For example, if $M = T^k$, then the full diagonal subgroup $D = \{(t, \dots, t) : t \in T\}$ is a subdirect product of M.

Exercise 44. If $M = T^k$ is the direct product of pairwise isomorphic nonabelian simple groups, then the full diagonal subgroup D is self-normalizing in M.

Lemma 4.16. *Suppose $M = T_1 \times \cdots \times T_k$ is the direct product of pairwise isomorphic nonabelian simple groups, and H is a subdirect product of M. There exists a partition of $[k]$ into nonempty sets $I_1, \dots, I_l$ such that $H = \prod_{j=1}^{l} D_j$, where D_j is the full diagonal subgroup of $\prod_{i \in I_j} T_i$.*

If $l = 1$, then H is the full diagonal subgroup, and if $l = k$, then $H = M$.

Proof. We proceed by induction on k, the case $k = 1$ being clear. Let $S \subset [k]$ be minimal such that $D = H \cap \prod_{i \in S} T_i \neq \{1\}$. Since H is nontrivial, $|S| \geq 1$. Further, $D \lhd H$, so $\pi_i(D) \lhd \pi_i(H)$ for $i \in S$. By the minimality of S, $\pi_i(D) = \pi_i(H)$ for $i \in S$. For the same reason, $\ker(\pi_i|_D)$ is trivial for each $i \in S$, so D is the full diagonal subgroup of $\prod_{i \in S} T_i$. If $S = [k]$, then we are done.

Suppose $S \subsetneq [k]$, and let π_S denote the projection onto $\prod_{i \in S} T_i$. $D \lhd \pi_S(H)$, and D is self-normalizing in $\prod_{i \in S} T_i$, so $D = \pi_S(H)$. Let $H' = H \cap \prod_{i \notin S} T_i$. Clearly $D \cap H' = \{1\}$, D and H' commuute, and $H = DH'$, so $H = D \times H'$. We only need to show that for each $i \in [k] \setminus S$, $\pi_i(H')$ is nontrivial. Then $\pi_i(H') \lhd \pi_i(H)$ implies that $\pi_i(H') = T_i$, and we can apply the induction hypothesis to H'.

Fix $i \in [k] \setminus S$ and $t \in T_i$, so there exists $h \in H$ such that $\pi_i(h) = t$. Define h' so that $\pi_j(h') = \pi_j(h)$ if $j \in [k] \setminus S$, and $\pi_j(h') = 1$ otherwise, i.e. h' and h agree on $[k] \setminus S$. Since $h'h^{-1} \in D$, $h' \in H$ and $\pi_i(h') = t$ as desired. □

Minimal normal subgroups of primitive permutation groups

The following lemma will be used several times, so it is worth remembering.

Lemma 4.17. *A nontrivial normal subgroup N of a primitive group G is transitive.*

Proof. Let N partition the ground set Ω into orbits; since N is nontrivial, each orbit has size > 1. Then, for any $g \in G$, if α and β are in the same N-orbit,

$$\alpha \cdot n = \beta \implies \alpha \cdot g(g^{-1}ng) = \beta \cdot g,$$

then $\alpha \cdot g$ and $\beta \cdot g$ are in the same N-orbit. In other words, the N-orbits form a system of blocks for G, so N must be transitive. □

Finally,

Proposition 4.18. *If G is primitive, then G has either*

1. *a unique minimal normal subgroup, or*
2. *exactly two minimal normal subgroups which are regular, centralize each other, and are isomorphic.*

Proof. Suppose G contains two distinct minimal normal subgroups, M_1 and M_2. Then,

$$[M_1, M_2] \leq M_1 \cap M_2 = 1$$

so they centralize each other. The centralizer of a transitive group is semi-regular, so M_1 and M_2 are regular. Further, since M_1 and M_2 are also transitive subgroups of $S = S_\Omega$, their centralizers $C_S(M_1)$ and $C_S(M_2)$ are also regular; by order considerations, $M_2 = C_S(M_1)$ and $M_1 = C_S(M_2)$. We know that any regular group is permutation isomorphic to its right regular representation, and it is not hard to show that its centralizer corresponds to its left regular representation; this shows that M_1 and M_2 are permutation isomorphic. □

Definition 4.19. The *socle* of a group G is the group generated by the minimal normal subgroups of G.

Corollary 4.20. *If M is the socle of G, then $M \lhd G$. In fact, $M \operatorname{char} G$.*

Corollary 4.21. *The socle of a primitive permutation group is the product of pairwise isomorphic simple groups.*

Theorem 4.22 (Burnside again)**.** *Let G be a finite 2-transitive group. Then G has a unique minimal normal subgroup M such that either*

1. *M is an elementary abelian p-group, and regular, or*
2. *M is nonabelian, simple, and primitive.*

Proof. Let M be a minimal normal subgroup of M, so M is characteristically simple.

First suppose M is elementary abelian. Then $M \leq C_G(M)$, so M is regular. Proposition 4.18 tells us that M is the unique minimal normal subgroup of G

Now suppose M is not elementary abelian. If M is regular, then G embeds in $M \rtimes Aut(M)$. $Aut(M)$ is the stabilizer of the identity, so it acts transitively on $M \setminus \{1\}$. Then all nonidentity elements of M have the same order, which must be prime, a contradiction, So M is not regular and again unique by Proposition 4.18. To show that M is primitive, we will use a fact about *Frobenius groups* that will be proved later using representation theory.

We say a permutation group H is a *Frobenius group* if it is transitive, not regular, and every nonidentity element has at most one fixed point. The *Frobenius kernel* K of a Frobenius group is

$$K = \{g \in H : g \text{ has no fixed points }\} \cup \{1\}.$$

We will later show that the Frobenius kernel is a normal subgroup of H in subsection 6.2, and take it for granted for now. We want to show that if M is not primitive, then M is a Frobenius group, and that $K \lhd G$, contradicting the minimality of M.

Let Δ be a (cardinality) minimal nontrivial block for M. Then $\Delta \cdot g$ is a block for M for every $g \in G$. By the minimality of Δ, $|\Delta \cap \Delta \cdot g| \leq 1$. Since G is 2-transitive, any two elements of Ω are contained in some $\Delta \cdot g$, and by the above observation g is uniquely determined. Let $\ell_{\alpha,\beta}$ be the unique block $\Delta \cdot g$ containing $\alpha, \beta \in \Omega$.

Suppose $g \in M$ fixes both $\alpha, \beta \in \Omega$: $g \in M_{\alpha,\beta}$. Then g fixes the block $\ell_{\alpha,\beta}$, and for any $\gamma \notin \ell_{\alpha,\beta}$, g fixes the blocks $\ell_{\alpha,\gamma}$ and $\ell_{\beta,\gamma}$ setwise, so it fixes γ. This yields $M_{\alpha,\beta} \leq M_{\alpha,\gamma}$. By interchanging the roles of β and γ, we obtain that every element of $M_{\alpha,\gamma}$ fixes every point outside $\ell_{\alpha,\gamma}$, in particular the points of $\ell_{\alpha,\beta}$. So g fixes all points of Ω, i.e. $g = 1$ and M is a Frobenius group. If K is the Frobenius kernel in M, then

$$\alpha(gkg^{-1}) = \alpha \implies (\alpha g)k = (\alpha)g.$$

that is gkg^{-1} has the same number of fixed points as k, so $K \lhd G$, which is the contradiction we wanted.

Finally, now that we know that M is primitive, assume that M is not simple. By Proposition 4.18 it either has a unique minimal normal subgroup – but this is not possible because a unique minimal normal subgroup is characteristic – or it has two isomorphic minimal normal subgroups S_1 and S_2. Again, $S_1 \times S_2$ is characteristic in M, so $M = S_1 \times S_2$. M acts faithfully on S_1 by conjugation, so let N be the normalizer of M in $\mathrm{Sym}(S_1)$, and H the normalizer of S_1, i.e. the stabilizer of S_1 under conjugation by N. S_1 is either mapped to itself, or to S_2, so $|N : H| = 2$. Further, $G \leq H$ so $H \cong S_1 \rtimes Aut(S_1)$ is 2-transitive, and $Aut(S_1)$ is transitive on $S_1 \setminus \{1\}$, again a contradiction. □

4.3 Wreath products

Recall the definition of a semidirect product in subsection 2.4. Let us make this more complicated. We will partially follow the notation of [2]. Suppose K is a group and H is an operator group[24] on K. We know we can define the semidirect product $K \rtimes H$. What if we have additional structure?

If H acts on a set Γ, let $B = K^\Gamma = \{b : \Gamma \to K\}$ be the set of functions $\Gamma \to K$. This has a natural group structure under pointwise multiplication: $bb'(\gamma) = b(\gamma)b'(\gamma)$. We can define H to be an operator group on B as follows. Write the action of $h \in H$ on $b \in B$ as b^h, and define

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

In other words, $b^h(\gamma h) = b(\gamma)$.

Definition 4.23. The *wreath product* of K by H, denoted $K \wr H$, is the group $B \rtimes H$.

Each function $b : \Gamma \to K$ is determined by a string $(a_\gamma)_{\gamma\in\Gamma} \in K^\Gamma$. H acts on $K^{|\Gamma|}$ by permuting the coordinates: h sends a_γ to the (γh)-th coordinate.

If K acts on a set Δ, then $K \wr H$ acts on the set $\Delta \times \Gamma$. Namely,

$$(\delta', \gamma') \cdot \big((a_\gamma)_{\gamma\in\Gamma}, h\big) = \big(\delta' a_{\gamma' h}, \gamma' h\big).$$

It might be useful to break this down into the actions of $B \rtimes \{1\}$ and $\{1\} \rtimes H$.

$$\begin{aligned} (\delta', \gamma') \cdot \big((a_\gamma)_{\gamma\in\Gamma}, 1\big) &= \big(\delta' a_{\gamma'}, \gamma'\big), \\ (\delta', \gamma') \cdot \big((1)_{\gamma\in\Gamma}, h\big) &= \big(\delta', \gamma' h\big). \end{aligned}$$

We call this the *canonical action* of the wreath product. Where do wreath products occur in nature?

Proposition 4.24. *Let T be a nonabelian simple group. Considering $Aut(T)$ as a permutation group on T, and S_k as a permutation group on $[1, \ldots, k]$,*

$$Aut(T^k) \cong Aut(T) \wr S_k = Aut(T)^k \rtimes S_k.$$

Proof. The intuition is that any automorphism of T^k can act as an automorphism on each copy of T, and permute the k copies of T, and that these are the only possible automorphisms. We will establish the map $\psi : Aut(T) \wr S_k \to Aut(T^k)$, and leave it to the reader to check the details. For $(a_1, \ldots, a_k; \pi) \in Aut(T) \wr S_k$, define

$$\psi_{(a_1,\ldots,a_k;\pi)}(t_1, \ldots, t_k) = (t_{1\pi^{-1}} a_{1\pi^{-1}}, \ldots, t_{k\pi^{-1}} a_{k\pi^{-1}}).$$

□

Of course, any group is a permutation group with respect to its right regular action, so we may forget about the sets Δ and Γ. Define the *standard wreath product* $K \wr H$ as the wreath product with respect to the right regular actions, i.e.,

$$K \wr H = K^H \rtimes H.$$

The underlying sets Δ and Γ and the corresponding actions of K and H will typically be clear from context, so we will use the same wreath product notation for them all.

[24] Recall Definition 2.25.

Proposition 4.25. *If K and H are transitive on Δ and Γ respectively, then the canonical action of $W = K \wr H$ on $\Delta \times \Gamma$ is transitive as well.*

Here is where the name "wreath product" comes in. Think of $\Delta \times \Gamma$ as a wreath consisting of Γ copies of Δ. $B \rtimes \{1\}$ permutes each copy of Δ within itself, while $1 \rtimes H$ permutes the Γ copies amongst each other. In other words, W is like a symmetry group for the wreath: it can rotate the wreath itself, or rotate each object on the wreath.

Exercise 45. Let K and H act transitively on Δ and Γ respectively. If $|\Delta| > 1$ and $|\Gamma| > 1$, show that the canonical action of $K \wr H$ is imprimitive.

Product action of a wreath product

So let's define a primitive action of $K \wr H$. Just as we considered K^Γ to define the wreath product, we consider Δ^Γ, the set of functions $f : \Gamma \to \Delta$. We can define an action of $K \wr H$ on this set as follows:

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

Again, it will be helpful to break this action down to understand what is happening. For $(b, 1) \in W$, $f(\gamma) = f^{(b,1)}(\gamma) \cdot b(1)$. And for $(1, h) \in W$, $f(\gamma) = f^{(1,h)}(\gamma h^{-1})$.

It is routine to check that this does define a *right* group action. When is it primitive?

Theorem 4.26. *The product action of $K \wr H$ is primitive if and only if K is primitive but not regular, and H is transitive.*

Proof. We begin with the implication $\implies$.

Suppose K is not primitive, and let $\sim$ be a K-invariant equivalence relation on Δ. Define an equivalence relation $\simeq$ on Δ^Γ by $f \simeq g$ if $f(\gamma) \sim g(\gamma)$ for each $\gamma \in \Gamma$. This is a nontrivial equivalence relation for the product action of $K \wr H$.

Next, suppose K is primitive and regular, so $K = \mathbb{F}_p$ for some prime p. Then, $\Delta^\Gamma = \mathbb{F}_p^\Gamma$ is a vector space over $\mathbb{F}_p$. Define an equivalence relation by $f \simeq g$ if $\sum_\gamma f(\gamma) = \sum_\gamma g(\gamma)$.

Finally, suppose H is not transitive. Fix an H-orbit $S \subset \Gamma$ and define an equivalence relation $\simeq$ on Δ^Γ by $f \simeq g$ if $f(\gamma) = g(\gamma)$ for all $\gamma \in S$.

Now for the converse implication $\impliedby$. Let B be the base group of the wreath product and identify H with $\{1\} \rtimes H$. Clearly B, and hence $W = B \rtimes H$ is transitive. If $\phi_\delta : \Gamma \to \Delta$ is the constant δ function for some $\delta \in \Delta$, then its stabilizer in W is

$$L = \Big\{(b, h) : b(\gamma) \in K_\delta \text{ for all } \gamma \in \Gamma\Big\}.$$

Let M be a subgroup of W properly containing L. It suffices to show that $M = W$. Since $W = BL$, $M = (M \cap B)L$, so $M \cap B$ properly contains $L \cap B$. Since $1 \rtimes \{H\} \leq M$, we will show that $M \cap B = B$, i.e. $B \leq M$.

For some γ_0, there exists $(b, 1) \in M \cap B$ with $b(\gamma_0) \notin K_\delta$. Since K is primitive and not regular, $K_\delta = N_K(K_\delta)$, hence for some $u \in K_\delta$

$$b(\gamma_0)^{-1} u b(\gamma_0) \notin K_\delta.$$

Define $b' : \Gamma \to K$ by

$$b'(\gamma) = \begin{cases} [b(\gamma_0), u], & \gamma = \gamma_0 \\ 1, & \text{otherwise.} \end{cases}$$

Since $b'(\gamma) \notin K_\delta$, $\langle K_\delta, b'(\gamma_0)\rangle = K$ by primitivity of K. Further, $(b', 1) \in M$ by construction, so M contains the subgroup

$$B(\gamma_0) = \Big\{(b', 1) \in B : b'(\gamma) = 1 \text{ for all } \gamma \neq \gamma_0\Big\}.$$

Since $H \leq M$ and H is transitive on Γ, $\prod_\gamma B(\gamma) = B \leq M$, as desired. □

Finally, let us look at one more type of wreath product - the *twisted wreath product*. This is a wreath product with some additional structure imposed. Let K and H be groups, with a subgroup $F \leq H$ that is an operator group on K, $\varphi : F \to Aut(K)$ a homomorphism. Let H act on itself with *right* multiplication; this is a right action. We want to define a wreath product that is compatible with the action of F on K. For example, for $f \in F$, we would like

$$(k_h)_{h \in H} \cdot f = (k_{hf})_{h \in H} = (\varphi_{f^{-1}} \cdot k_h)_{h \in H}.$$

Define

$$B_F = \Big\{(k_h)_{h\in H} : k_{hf} = \varphi_{f^{-1}} \cdot k_h, \forall h \in H\Big\}.$$

It is routine to check that B_F is a group, and that H is an operator group on it. The *twisted wreath product* $K \wr_F H$ is defined as

$$B_F \rtimes H.$$

4.4 Classification of primitive permutation groups

We devote the entirety of this section to proving the following theorem. The proof follows the presentation of [6], with some assistance from [2] and [4].

Theorem 4.27 (O' Nan-Scott)**.** *Let G be a finite primitive permutation group on Ω with socle M. Then G is of one of the following types.*
Affine type:

(HA) M is an elementary abelian p-group, hence the unique minimal normal subgroup of G. M is regular, so Ω can be identified with a d-dimensional vector space over $\mathbb{F}_p$. Then $G \le AGL(d,p)$, $AG(d,p) \le G$, and the stabilizer of the zero vector $G_0 \le GL(d,p)$ has no invariant subspaces.

Almost simple type:

(AS) M is a nonabelian simple group T. Then M is the unique minimal normal subgroup of G and does not act regularly. $Inn(T) \le G \le Aut(T)$. The proof of this classification requires the Schreier conjecture, that $Out(T) \cong Aut(T)/Inn(T)$ is solvable, the only proof of which relies on CFSG.

Diagonal type:

(HS) G has two minimal normal subgroups, each of which is a nonabelian simple group T, and $M \cong T \times T$. The action of M is primitive, and $M \cong T.Inn(T) \le G \le T.Aut(T)$.

(SD) $M \cong T^k$ for $k \ge 2$ and this is the unique nonabelian minimal normal subgroup of G. Let $H = \{(t,\dots,t) : T \in T\} \le M$ be the diagonal subgroup. M acts on the cosets of H in M by right multiplication; we can identify Ω with T^{k-1}. In this case, $M \lhd G \le M \cdot \big(Out(T) \times S_k\big)$ and G induces a primitive subgroup of S_k on the k factors of M.

Product type:

(HC) G has two minimal normal subgroups, each of which is T^k, $k \ge 2$, for T a nonabelian simple group, so $M \cong T^k \times T^k$. As in the HS case, M acts transitively, and $M \cong T^k.Inn(T^k) \le G \le T^k.Aut(T^k)$. Further, G induces a subgroup of $Aut(T^k)$ that acts transitively on the k factors of T^k.

(CD) This is similar to the case SD; $\Omega = \Delta^k$, and $G \le H \wr S_k$, where H is of type SD on Δ. If the minimal normal subgroup of H is T^l, then T^{kl} is the minimal normal subgroup of G, and G induces a transitive subgroup of S_k.

(PA) G has a unique nonabelian minimal normal subgroup T^k, $k \ge 2$, that does not act regularly. $\Omega = \Delta^k$ and $G \le H \wr S_k$, where H is an AS group. Further, G induces a transitive subgroup of S_k in its action on the k factors of M.

Twisted wreath type:

(TW) G has a unique nonabelian minimal normal subgroup T^k, $k \ge 2$, that acts regularly. G is isomorphic to a twisted wreath product $T \wr_F G_\alpha$.

Let us begin by studying the socle M.

Case (1: HA)**.** M is abelian.

By Proposition 4.18, if G has an abelian minimal normal subgroup M, then it is unique. By Lemma 4.11, M is an elementary abelian p-group. M is a transitive subgroup of S_Ω contained in its centralizer, so M is regular. In other words, $M \cong V$, a d-dimensional vector space over $\mathbb{F}_p$, and for any stabilizer G_α, $G = M \rtimes G_\alpha$. We want to show that $G \le AGL(d, p)$. For each $a \in G_\alpha$, define an automorphism $\phi_a : M \to M$ by $\phi_a(m) = a^{-1}ma$. Fix a $\mathbb{Z}$-isomorphism $\theta : M \to V$ (so that we can write the vector space operation additively). Then, $\theta^{-1}\phi_a\theta \in GL(d, p)$ for all $a \in G_\alpha$. Since each element of G can be written uniquely as ma for $m \in M$ and $a \in G_\alpha$, we have an injective homomorphism $\psi : G \to V^* \rtimes GL(d, p)$,

$$\psi(ma) = (m\theta)^*(\theta^{-1}\phi_a\theta).$$

This yields $G \le AGL(d, p)$. Further, the image of M under ψ is V^*, so $V^* \cong AG(d, p) \le \psi(G)$. Finally,

Exercise 46. If $AG(d, p) \le G \le AGL(d, p)$, then G is primitive if and only if G_0, the stabilizer of the zero vector, has no nontrivial invariant subspaces.

In this case, G is called the *holomorph of an abelian* group (**HA**). □

Case (2: AS)**.** M is a nonabelian simple group T.

Each $g \in G$ induces an automorphism of T by conjugation, so we have a homomorphism $\varphi : G \to Aut(T)$. Then, $\ker(\varphi) = C_G(T)$. However, $C_G(T) \lhd G$ and $C_G(T) \cap T = \{1\}$, so by the uniqueness of T, $C_G(T) = \{1\}$. So φ is injective, and $T \cong \varphi(T) = Inn(M)$. It only remains to show that T is not regular, and this is the part which relies on the Schreier conjecture, so we will omit the proof.

In this case, G is called an *almost simple* group (**AS**).

For the remaining cases, $M = T^k$ where T is a nonabelian simple group and $k \ge 2$. Write $M = T_1 \times \cdots \times T_k$, where $T_i \cong T$. Let $\pi_1, \ldots, \pi_k$ be the projections from $M \to T_i$.

Case (3)**.** The stabilizer M_α, $\pi_i(M_\alpha) = T_i$ for some i.

Since G_α is maximal in G and G acts transitively on the set $\{T_1, \ldots, T_k\}$, M_α is a maximal proper G_α-invariant subgroup of M. So, $\pi_j(M_\alpha) = T_j$ for all $j = 1, \ldots, k$, i.e. M_α is a subdirect product of M. So there exists a partition of $[k]$ into nonempty sets $I_1, \ldots, I_l$ such that $M_\alpha = D_1 \times \cdots \times D_l$, where D_j is the diagonal subgroup of $\prod_{i \in I_j} T_i$. Suppose $|I_1| = m$. G_α acts transitively on $\{D_1, \ldots, D_l\}$, so $|I_j| = m$ for all $j = 1, \ldots, l$. As a consequence, $m \ge 2$ since M_α is a proper subgroup of M. Let $P \le S_k$ be the group induced by the action of G on $\mathcal{T} = \{T_1, \ldots, T_k\}$.

Case (3.1: HS and SD)**.** $l = 1$, i.e. M_α is the full diagonal subgroup.

Suppose $\Delta \subset \mathcal{T}$ is a nontrivial block for P. The diagonal subgroup Y of M corresponding to this system of blocks is a G_α-invariant subgroup of M with $M_\alpha \le Y \le M$. This contradicts the maximality of M_α, so either $P = \{1\}$, $k = 2$ and G has two minimal normal subgroups, or P is primitive.

In the first case, T_1 and T_2 are regular minimal normal subgroups of G, acting on Ω by left and right multiplication respectively. M acts primitively on Ω. G embeds in the normalizer of T_1 in S_Ω, which is isomorphic to $T \rtimes Aut(T)$. G is of type *holomorph of a simple* group (**HS**).

In the second case, if P is primitive, then M must be the unique minimal normal subgroup of G. The action of M on Ω is equivalent to the action of M on the right cosets of M_α, the diagonal subgroup, so we can identify Ω with T^{k-1}. G embeds in the normalizer of of M in S_Ω, which is isomorphic to $M \cdot \left(Out(T) \times S_k\right)$.[25] G is of type *simple diagonal* (**SD**).

Case (3.2: HC and CD)**.** $l > 1$, i.e. M_α is not the diagonal subgroup.

Set $K = T_1 \times \cdots \times T_m$ so that D_1 is the full diagonal subgroup of K, and set $N = N_G(K)$. D_1 is a maximal N_α-invariant subgroup of K. We want to find a group H of type HS or CD such that G is permutation equivalent to a subgroup of $H \wr S_l$ with a product action.

[25] Take this fact for granted

For any subgroup $L \le N$, define L^* to be the subgroup of $Aut(K)$ induced by the conjugation action of L, i.e. $L^* = LC_G(K)/C_G(K)$. Note that $C_G(K) \cap M = T_{m+1} \times \cdots \times T_k$, so M is "almost" contained in $C_G(K)$. Since $M \le N$, N is transitive on Ω so $N = MN_\alpha$. Then,

$$N^* = MN_\alpha C_G(K)/C_G(K) = KN_\alpha C_G(K)/C_G(K) = K^* N_\alpha^*.$$

We want to show that $N_\alpha C_G(K)$ is a maximal subgroup of N, so let Y be a maximal subgroup of N containing it. Then, $Y \cap K$ is an N_α-invariant subgroup of K containing D_1, so $D_1 = Y \cap K$, hence $Y \cap M = D_1 \times T_{m+1} \times \cdots \times T_k$. Further, $Y = (Y \cap M)N_\alpha$, so $Y^* = D_1^* N_\alpha^* = N_\alpha^*$ (since D_1 stabilizes α), so $Y = N_\alpha C_G(K)$.

Finally, set $H = N^*$, and let Γ be the coset space of N_α^* in H. Each point stabilizer of this action is isomorphic to N_α^*, which is a maximal subgroup of N^*, so H acts primitively on Γ. The socle of H is $K^* \cong K$, so H is of type HS or SD. Further, an easy calculation shows that $|\Omega| = |\Gamma|^l$.

It remains to show that G is a subgroup of $H \wr S_l$ with the product action on Γ^l. We give the embedding and leave it to the reader to check the details. Choose a right transversal $\{g_1, \ldots, g_l\}$ for N_α in G_α (and thus for N in G) so that $D_1^{g_i} = D_i$ for $1 \le i \le l$. Write $K_i = K^{g_i}$ so that G permutes the set $\{K_1, \ldots, K_l\}$. For $g \in G$, write $G = n_g \bar{g}$, for $\bar{g} \in \{g_1, \ldots, g_l\}$ and $n_g \in N$. Finally, embed G in $H \wr S_l$ by

$$g \to (a_1^*, \ldots, a_l^*; \pi),$$

where $\pi \in S_l$ is the permutation induced by g on $\{K_1, \ldots, K_l\}$, and $a_i = (g_i g)(\overline{g_i g})^{-1} \in N$. If H is of type HS or SD, G is of type *holomorph of a compound* group (**HC**) or *complex diagonal* (**CD**) respectively.

Case (4: PA and TW)**.** $R_i = \pi_i(M_\alpha)$ is a proper subgroup of T_i for each i.

Each R_i is an $N_G(T_i)$-invariant subgroup of T_i, so G_α is transitive on the set $\{T_1, \ldots, T_k\}$. So each R_i is equal to the image of R_1 under an isomorphism $T_1 \to T_i$. Since $R_1 \times \cdots \times R_k$ is G_α-invariant, it is equal to M_α, and R_1 is a maximal $N_{G_\alpha}(T_1)$-invariant subgroup of T_1. Set $N = N_G(T_1)$, and for $L \le N$, denote $L^* = LC_G(T_1)/C_G(T_1)$. By a similar argument as earlier, $N = MN_\alpha$ and $N^* = T_1^* N_\alpha^*$.

Suppose $T_1^* \not\le N_\alpha^*$. Again, we can show that $N_\alpha C_G(T_1)$ is a maximal subgroup of N, so that setting $H = N^*$, H acts primitively on the coset space $\Gamma = H/N_\alpha^*$. H has a unique minimal normal subgroup $T_1^* \cong T_1$ so H is of type AS. A similar argument to case 3.2 shows that $G \le H \wr S_k$ with the product action on Γ^k. G is said to be of type *product action* (**PA**).

Now suppose $T_1^* \le N_\alpha^*$, so $N^* = N_\alpha^*$. If $R_1 \ne 1$, then

$$T_1 = \langle R_1^{T_1} \rangle \le \langle R_1^{C_G(T_1)N_\alpha} \rangle = \langle R_1^{N_\alpha} \rangle \le G_\alpha,$$

which is nonsense. So, $R_1 = 1$, and $M \cong T_1 \times \cdots \times T_k$ is regular, hence the unique minimal normal subgroup of G. Define $\varphi : N \to Aut(T_1)$ to be the natural homomorphism so that $\ker\varphi = C_G(T_1) \cap G_\alpha$, and $\mathrm{Im}\varphi = N_\alpha^*$ contains $Inn(T_1) = T_1^*$. By an application of the Schreier conjecture (the details of which can be found in [6]), we can show that M is equal to the kernel of the action of G on $\{T_1, \ldots, T_k\}$ by conjugation. Thus, the stabilizer G_α acts faithfully and transitively on $\{T_1, \ldots, T_k\}$. Let $F \le G_\alpha$ be the stabilizer of T_1, so that $\varphi : F \to Aut(T_1)$ is defined. We claim that G is isomorphic to the twisted wreath product $T_1 \wr_F G_\alpha$ with its product action on $|T_1|^k$.

For $1 \le i \le k$, choose $c_i \in G_\alpha$ so that $T_i^{c_i} = T_1$. Then, for $m = (m_1, \ldots, m_k) \in T_1 \times \ldots T_k$, $m_i^{c_i} \in T_1$. Clearly $G = MG_\alpha$, so define the map $\nu : G \to T_1 \wr_F G_\alpha$ by

$$\nu : mu \to \nu_m u,$$

where ν_m is the function $G_\alpha \to T_1$ given by $\nu_m(c_i q) = m_i^{c_i q}$. Some manipulation shows us that ν is the desired isomorphism, and G is said to be of *twisted wreath* type (**TW**).

4.5 Subgroups of S_n

Let us look at some applications of primitive permutation groups to subgroups of the symmetric group.

Theorem 4.28. *The alternating groups A_n are simple for $n \ge 5$.*

Proof. We proceed by induction. There are many ways to check the base case $n = 5$, the easiest of which is perhaps to show that no nontrivial union of conjugacy classes in A_5 divides 60.

Suppose $n > 5$. Let $N \lhd A_n$ be a nontrivial normal subgroup. Since A_n is at least 4-transitive for $n > 5$, A_n is primitive, so N is transitive. The stabilizer G_1 is isomorphic to A_{n-1}, and hence is simple. So $N \cap G_1 = 1$ or $N \cap G_1 = G_1$. The second case cannot hold as G_1 is a maximal subgroup and N is transitive. So we are in the first case, and again by the maximality of G_1, $G_1 N = A_n$. By the Schur-Zassenhaus theorem, there is a homomorphism $\varphi : G_1 \to Aut(N)$ so that A_n is the semidirect product $N \rtimes G_1$ with respect to this homomorphism. G_1 is not normal in A_n, so φ cannot be trivial. Since $\ker\varphi \lhd G_1$, φ must be injective. However, it is easy to check that $Aut(N)$ is not 3-transitive, while A_{n-1} is 3-transitive for $n > 5$. □

Next,

Proposition 4.29. *The Sylow p-subgroups of S_{p^k} are isomorphic to $\mathbb{Z}_p \wr \cdots \wr \mathbb{Z}_p$, the k-fold wreath product.*

Proof. This is a simple matter of checking that (1) $\mathbb{Z}_p \wr \cdots \wr \mathbb{Z}_p$ embeds in S_{p^k} (it does), and (2) $\left|\mathbb{Z}_p \wr \cdots \wr \mathbb{Z}_p\right| = p^{(p^k-1)/(p-1)}$ (it is). □

5 Representations of finite groups

Now we will switch tracks entirely. We wrung out many deep results just by considering each group as a permutation group. The idea of representation theory is a generalisation of this: by considering homomorphisms of a group G into the automorphism group of some structure, we would like to use properties of the structure to derive properties of the group. The structure we consider here is a vector space.

Definition 5.1. Let G be a group and V a vector space over a field $\mathbb{F}$. A *representation* of G is a group homomorphism $\varphi : G \to GL(V)$. The dimension of V is called the *degree* of the representation.

Just as with group actions, we say a representation is *faithful* if $\ker\varphi$ is trivial. For any group G and any vector space V, we have a *trivial representation*, the identically identity homomorphism. If G is a finite group of order n, and $\mathbb{F}$ a field, consider the n-dimensional vector space V over K with basis $\{e_g : g \in G\}$. The *left* regular action of G defines the *regular representation* φ,

$$\varphi_g(e_h) = e_{gh}.$$

In general, given a *left* action of G on a set X and a field $\mathbb{F}$, define a vector space V with basis $\{e_x : x \in X\}$, so the corresponding representation φ of G is

$$\varphi_g(e_x) = e_{gx}.$$

Vigyázz. We have returned to writing actions from the left, because we typically consider matrix multiplication from the left.

5.1 Irreducible representations and Maschke's theorem

As always, when we define a new structure, we want to ask (1) when do we call two objects equivalent?, and (2) what are the "irreducible" objects, upto equivalence?

Definition 5.2. Two representations $\varphi : G \to GL(V)$ and $\psi : G \to GL(W)$ are *equivalent* if there is an invertible linear map $\tau : V \to W$ so that

$$\tau\varphi_g = \psi_g\tau; \quad \forall g \in G.$$

That is, $\dim V = \dim W$, and φ and ψ differ by a change of basis. This answers the first question. To answer the second, let us instead ask, "Which representations are clearly not irreducible?"

Definition 5.3. If $\varphi_i : G \to GL(V_i)$ is a representation $\forall i \in I$, define the *direct sum* $\varphi = \bigoplus_{i\in I} \varphi_i$ as the representation $\varphi : G \to \bigoplus_{i\in I} GL(V_i)$ over the vector space $\bigoplus_{i\in I} V_i$.

When I is finite and each V_i is finite-dimensional, the matrices φ_g of the direct sum are block diagonal matrices. In general, the embedding of each $V_i \leq V$ is invariant under each φ_g.

Definition 5.4. Let $\varphi : G \to GL(V)$ be a representation, and $U \leq V$ a subspace. U is an *invariant subspace for* φ if $\varphi_g(U) \subseteq U$ for each $g \in G$.

Since each φ_g is invertible, this is equivalent to saying $\varphi_g(U) = U$.

Definition 5.5. A representation $\varphi : G \to GL(V)$ is *irreducible* if it has no nontrivial invariant subspaces.

Definition 5.6. A representation $\varphi : G \to GL(V)$ is *completely reducible* if every invariant subspace U has an invariant orthogonal complement $\tilde{U}$, that is $V = U \oplus \tilde{U}$ and $\tilde{U}$ is invariant under G.

Proposition 5.7. *A finite-dimensional representation is completely reducible if and only if it is the direct sum of irreducible representations.*

Proof. Suppose $\varphi : G \to GL(V)$ is completely reducible. Choose minimal invariant subspaces $U_1, \dots, U_k$ such that $U_1 \oplus \cdots \oplus U_k = U \leq V$ has maximal dimension. U is an invariant subspace, and by complete reducibility, $U = V$.

Conversely, let $V = U_1 \oplus \dots U_k$ be the direct sum of irreducible representations, and U an invariant subspace of V. Choose a maximal invariant subspace $\tilde{U}$ such that $U \cap \tilde{U} = \{0\}$. If some U_i is not contained in $U \oplus \tilde{U}$, since U_i is irreducible, $U_i \cap (U \oplus \tilde{U}) = \{0\}$. In particular, $U_i \oplus \tilde{U}$ is a larger invariant subspace contradicting the maximality of $\tilde{U}$, so $U \oplus \tilde{U} = V$. □

We would like every representation to be completely reducible, so that we can focus on studying irreducible representations.

Theorem 5.8 (Maschke)**.** *Let G be a finite group. If* $\mathrm{char}\mathbb{F}$ *does not divide* $|G|$, *then every representation of G over $\mathbb{F}$ is completely reducible.*

Proof. Suppose V has a nontrivial invariant subspace U. By extending to a basis of V, we can find a subspace W such that $V = W \oplus U$. Every element can be uniquely expressed as $u + w \in U + W$; let π be the projection to U along W, $\pi(u + w) = u$. Define $\hat{\pi} : V \to V$ by

$$\hat{\pi} = \frac{1}{|G|} \sum_g \varphi_g \pi \varphi_{g^{-1}}.$$

Claim (1)**.** $\hat{\pi}$ is a projection onto U along $\ker\hat{\pi}$.

Since U is invariant, $V = U \oplus \varphi_g(W)$ for each $g \in G$, and $\varphi_g \pi$ is the corresponding projection onto U. So,

$$\hat{\pi}(u + w) = \frac{1}{|G|} \sum_g \varphi_g \pi \varphi_{g^{-1}}(u + w) = \frac{1}{|G|} \sum_g \varphi_g \pi \varphi_{g^{-1}}(u) = u.$$

Claim (2)**.** $\ker\hat{\pi}$ is an invariant subspace.

We want to show that if $\hat{\pi}(v) = 0$, then for any $h \in G$, $\hat{\pi}\varphi_h(v) = 0$.

$$\begin{aligned} \hat{\pi}\varphi_h(v) &= \frac{1}{|G|} \sum_g \varphi_g \pi \varphi_{g^{-1}} \varphi_h(v) \\ &= \varphi_h \left(\frac{1}{|G|} \sum_g \varphi_{h^{-1}g} \pi \varphi_{g^{-1}h}(v) \right) \\ &= \varphi_h \hat{\pi}(v) = 0. \end{aligned}$$

Clearly $U \oplus \ker\hat{\pi} = V$, so this completes the proof. □

Maschke's theorem is an if and only if statement; the converse will be easier to prove once we have seen the group algebra.

5.2 The group algebra

There is another, sometimes more useful way to think of representations. A representation $\varphi : G \to GL(V)$ endows V with a G-action and an $\mathbb{F}$-action, both of which commute.

$$\lambda \cdot \varphi_g(v) = \varphi_g(\lambda v); \quad \forall g \in G, \forall \lambda \in \mathbb{F}.$$

Definition 5.9. If G is a group and $\mathbb{F}$ a field, the *group algebra* $\mathbb{F}G$ is the ring of *finite* formal sums $\sum_{g \in G} \alpha_g g$ where $\alpha_g \in \mathbb{F}$. The ring operations are

$$\sum_{g \in G} \alpha_g g + \sum_{h \in G} \beta_h h = \sum_{x \in G} (\alpha_x + \beta_x) x$$

$$\sum_{g \in G} \alpha_g g \sum_{h \in G} \beta_h h = \sum_{x \in G} \Big(\sum_{h \in G} \alpha_{xh^{-1}} \beta_h \Big) x$$

In other words, $\mathbb{F}G$ is the $\mathbb{F}$-algebra generated by the elements of G. Further, if V is an $\mathbb{F}G$-module, then V is an $\mathbb{F}$-vector space and the action of G on V is a representation of G on V. Conversely, given any representation of G on a vector space V over $\mathbb{F}$, there is a natural extension of this action to V as an $\mathbb{F}G$-module. Consequently, given a representation of G on V

(*) two representations are equivalent $\iff$ the corresponding $\mathbb{F}G$-modules are isomorphic,

(*) $U \leq V$ is an invariant subspace $\iff$ U is an $\mathbb{F}G$-submodule of V,

(*) the representation is irreducible $\iff$ V is a simple $\mathbb{F}G$-module (it has no nontrivial submodules), and

(*) the representation is completely reducible $\iff$ V is a semisimple $\mathbb{F}G$-module (it is the direct sum of simple submodules).

The equivalent formulation of Maschke's theorem is then,

Theorem (Maschke)**.** *If G is a finite group and* $\operatorname{char}\mathbb{F}$ *does not divide G, then $\mathbb{F}G$ is semisimple.*

It is also easy to see that the $\mathbb{F}G$-module corresponding to the regular representation of G is $\mathbb{F}G$ itself.

Remark. Let us take a brief detour into ring theory to make the rest of this section clear. A *simple* ring R is one which has no nontrivial (two-sided) ideals. We say a ring R is semisimple if it is the direct sum of simple rings. As we will see, the only simple rings are essentially the matrix rings.

Exercise 47. Let G be a finite group such that $\operatorname{char}\mathbb{F}$ divides $|G|$.

(a) Show that
$$I = \Big\{ \sum_{g \in G} \alpha_g g : \sum_{g \in G} \alpha_g = 0 \Big\}$$
is a submodule of $\mathbb{F}G$.

(b) Show that $\mathbb{F}G$ is not completely reducible.

We will need the following structure theorem for semisimple rings.

Theorem (Wedderburn-Artin)**.** *R is a semisimple ring if and only if there are division rings $D_1, \ldots, D_k$ and integers $n_1, \ldots, n_k$ so that*

$$R \cong M_{n_1}(D_1) \oplus \cdots \oplus M_{n_k}(D_k).$$

We will primarily consider the case when $\mathbb{F} = \mathbb{C}$, and $R = \mathbb{C}G$. In this case, each division ring D_i is a finite extension of $\mathbb{C}$, so must be equal to $\mathbb{C}$. In other words,

Theorem. *If G is a finite group, there exist integers $n_1, \ldots, n_k$ so that*

$$\mathbb{C}G \cong M_{n_1}(\mathbb{C}) \oplus \cdots \oplus M_{n_k}(\mathbb{C}).$$

Let the image of each $g \in G$ under this isomorphism be $(\varphi_g^{(1)}, \dots, \varphi_g^{(k)})$.

Corollary 5.10. *The map $g \to \varphi_g^{(i)}$ is an irreducible representation of G.*

We want to show that these are the only irreducible representations of G. If φ is an irreducible representation of G on a d-dimensional vector space, we say d is the *degree* or *dimension* of φ.

The key lemma in our proof is the following.

Theorem 5.11 (Schur's lemma)**.** *An R-module homomorphism between two simple modules U and V is either identically* 0 *or an isomorphism.*

Proof. If $\varphi : U \to V$ is a homomorphism, then $\ker(\varphi) \leq U$ and $\mathrm{Im}(\varphi) \leq V$, so this completes the proof. □

Assume $\mathbb{F}$ is a field and G a finite group such that char$\mathbb{F}$ does not divide $|G|$. For two $\mathbb{F}G$-modules U and V, let $\mathrm{Hom}_G(U, V)$ denote the space of all $\mathbb{F}G$-module homomorphisms $U \to V$. $\mathrm{Hom}_G(U, V)$ is an $\mathbb{F}$-vector space, so define $\langle U, V\rangle = \dim_{\mathbb{F}} \mathrm{Hom}_G(U, V)$.

Corollary 5.12. *If U and V are simple $\mathbb{F}G$-modules, then $\langle U, V\rangle = 1$ if $V \cong U$ and $\langle U, V\rangle = 0$ otherwise.*

Proposition 5.13. *Let V be an $\mathbb{F}G$-module with a decomposition $V = V_1 \oplus \cdots \oplus V_r$ into simple $\mathbb{F}G$-submodules, and let W be any simple $\mathbb{F}G$-module. If $n(W, V)$ denotes the number of V_i isomorphic to W, then*

$$\langle W, W\rangle \cdot n(W, V) = \langle W, V\rangle = \langle V, W\rangle.$$

Proof. Since

$$\mathrm{Hom}_G(W, V) \cong \prod_i \mathrm{Hom}_G(W, V_i),$$

we have

$$\langle W, V\rangle = \langle W, V_1\rangle + \cdots + \langle W, V_k\rangle = n(W, V)\langle W, W\rangle,$$

where the last equality follows from Schur's lemma. □

Lemma 5.14. *For any irreducible $\mathbb{F}G$-module U, the map $\mathrm{Hom}_G(\mathbb{F}G, U) \to U$ that sends $\varphi \to \varphi(1)$ is an isomorphism. In particular, $\langle \mathbb{F}G, U\rangle = \dim_{\mathbb{F}} U$.*

Proof. Clearly the map $\varphi \to \varphi(1)$ is a homomorphism. Since any such $\mathbb{F}G$-module homomorphism is uniquely determined by its value at 1, this map is an isomorphism. □

Theorem 5.15. *Each irreducible representation appears in the regular representation with multiplicity equal to its degree.*

Proof. Let U be an irreducible $\mathbb{F}G$-module. Then,

$$n(U, \mathbb{F}G) = \langle \mathbb{F}G, U\rangle = \dim_{\mathbb{F}}(U).$$

□

To summarise the results of this section: we know that the group algebra $\mathbb{C}G$ corresponds to the regular representation of G. By Wedderburn-Artin,

$$\mathbb{C}G \cong M_{n_1}(\mathbb{C}) \oplus \cdots \oplus M_{n_k}(\mathbb{C})$$

is its decomposition into simple submodules, or irreducible representations. Further, every irreducible representation, or simple module of G corresponds to some $M_{n_i}(\mathbb{C})$. This tells us that these k matrix rings in the decomposition of $\mathbb{C}G$ correspond to the irreducible representations of G (where each appears with multiplicity equal to its dimension).

As a corollary, if d_i is the dimension of the ith irreducible representation, then

$$|G| = \sum_{i=1}^{k} d_i^2.$$

We will in fact prove that d_i divides $|G|$ in subsection 6.1.

5.3 Characters and class functions

Now that we know that a finite group has only finitely many representations over $\mathbb{C}$, our next question is - how many?

Theorem 5.16. *k is the number of conjugacy classes of G.*

Proof. Given that

$$\mathbb{C}G \cong M_{n_1}(\mathbb{C}) \oplus \cdots \oplus M_{n_k}(\mathbb{C}),$$

we will show that the dimension of the center of both sides is equal to the number of conjugacy classes. For a ring R, its center is defined as one would expect,

$$Z(R) = \{a \in R : ar = ra, \forall r \in R\}.$$

On one hand,

$$Z(M_{n_1}(\mathbb{C}) \oplus \cdots \oplus M_{n_k}(\mathbb{C})) \cong Z(M_{n_1}(\mathbb{C})) \oplus \cdots \oplus Z(M_{n_k}(\mathbb{C})).$$

The center of a matrix algebra is the set of scalar matrices, which has dimension 1 over the base field, so the dimension of the above expression is k. Now let us consider $Z(\mathbb{C}G)$. Since $\mathbb{C}$ is commutative, $Z(\mathbb{C}G)$ consists exactly of those elements of $\mathbb{C}G$ which commute with G.

$$\begin{aligned} Z(\mathbb{C}G) &= \Big\{\sum_g \alpha_g g : h\sum_g \alpha_g g = \sum_g \alpha_g gh, \forall h \in G\Big\} \\ &= \Big\{\sum_g \alpha_g g : \sum_g \alpha_g g = \sum_g \alpha_g h^{-1}gh, \forall h \in G\Big\} \\ &= \Big\{\sum_g \alpha_g g : \alpha_g = \alpha_{hgh^{-1}}, \forall h \in H\Big\}, \end{aligned}$$

and it is clear that the dimension of this space is the number of conjugacy classes of G. □

Corollary 5.17. *G is abelian if and only if every irreducible representation is 1-dimensional.*

Proof. G is abelian if and only if the number of conjugacy classes is equal to $|G|$. So,

$$\dim_{\mathbb{F}} \mathbb{F}G = |G| = \sum_{i=1}^{|G|} n_i^2.$$

Each n_i must be equal to 1, so each irreducible representation is 1-dimensional. □

This relationship between conjugacy classes and irreducible representations is better studied using *characters*.

Definition 5.18. The *character* χ of a representation $\varphi : G \to GL(d, \mathbb{C})$ is defined as

$$\chi(g) = \mathrm{Tr}\varphi_g.$$

An *irreducible character* is one that corresponds to an irreducible representations. If two representations are equivalent, the corresponding characters are equal. Further, the characters are constant on each conjugacy class

$$\chi(x^{-1}gx) = \mathrm{Tr}(\varphi_{x^{-1}}\varphi_g\varphi_x) = \mathrm{Tr}\varphi_g = \chi(g).$$

We can also show a converse, that if two irreducible characters are equal, then the corresponding representations are equal. Recall that the distinct irreducible representations of G are given by $g \to \varphi_g^{(i)}$ in the notation of Corollary 5.10. Let χ_i denote the corresponding irreducible character and $e_i = (0, \dots, 1, \dots 0) \in \mathbb{C}G$ with the $(n_i \times n_i)$ identity matrix in the ith coordinate and 0 everywhere else. Then, for $i \neq j$, $\chi_i(e_i) = n_i$ but $\chi_j(e_i) = 0$, so $\chi_i \neq \chi_j$.

Let us study some properties of characters before we obtain some results as corollaries of Theorem 5.15. An easy observation is that $\chi(1)$, as the trace of the identity matrix, is equal to the dimension of the representation. This implies that $|G| = \sum_\chi \chi(1)^2$, where the sum runs over the irreducible characters of G.

Lemma 5.19. *Let φ be a representation of G with character χ, and let $g \in G$ with $|g| = n$.*

(a) φ_g *is similar to a diagonal matrix with entries* $(\epsilon_1, \ldots, \epsilon_r)$.

(b) $\epsilon_i^n = 1$ *for each* $i = 1, \ldots, r$.

(c) $\chi(g) = \sum_{i=1}^r \epsilon_1$, *and* $|\chi(g)| \leq \chi(1)$.

(d) $\chi(g^{-1}) = \overline{\chi(g)}$.

Proof. The restriction of φ to a subgroup is also a representation, so we may assume that $G = \langle g \rangle$. By Maschke's theorem, φ_g is similar to a block diagonal matrix corresponding to the decomposition into irreducible representations. Since $\langle g \rangle$ is abelian, each irreducible representation is 1-dimensional, so its matrix is diagonal, proving (a). (b) follows easily from the fact that $g^n = 1$, and (c) and (d) are similarly easy to show. □

Lemma 5.20. *If* $\varphi = \varphi_1 \oplus \ldots \varphi_m$ *are representations of G, and* $\chi_1, \ldots, \chi_m$ *are the characters corresponding to* $\varphi_1, \ldots, \varphi_m$*, then the character of* φ *is*

$$\chi(g) = \chi_1(g) + \cdots + \chi_m(g).$$

Let ρ denote the character corresponding to the regular representation ϕ.

Lemma 5.21. $\rho(1) = |G|$ *and* $\rho(g) = 0$ *if* $g \neq 1$.

Proof. Consider $G = \{g_1, \ldots, g_n\}$ as a basis for the vector space. Each matrix ϕ_g is a permutation matrix, and $\rho(g)$ counts the number of 1's on the diagonal. However, $(\phi_g)_{ii} = 1$ if and only if $gg_i = g_i$, and the lemma follows immediately from this. □

Since each irreducible representation appears in the regular representation with multiplicity $\chi(1)$ for its corresponding character χ,

Corollary 5.22. *If* $\chi_1, \ldots, \chi_k$ *are the irreducible characters of G,*

$$\rho(g) = \sum_{i=1}^{k} \chi_i(1)\chi_i(g).$$

Corollary 5.23. *If* $\chi_1, \ldots, \chi_k$ *are the irreducible characters of G,*

$$|G| = \sum_{i=1}^{k} \chi_i(1)^2.$$

We say a character χ is *linear* if it is an irreducible one-dimensional character, i.e. $\chi(1) = 1$.

Corollary 5.24. *Every irreducible character of an abelian group is linear. In general, a finite group G has exactly* $|G : [G,G]|$ *linear characters.*

5.4 Inner products of characters

A $\mathbb{C}$-valued function that is constant on the conjugacy classes of G is called a *class function*. The set of all class functions is a vector space over $\mathbb{C}$ with dimension the number of conjugacy classes of G. We want to show

Theorem 5.25. *The irreducible characters form a basis for all class functions.*

We can define an inner product on the space of class functions on a finite group G by[26]

$$\langle \mu, \nu \rangle = \frac{1}{|G|} \sum_{g \in G} \mu(g)\overline{\nu(g)}.$$

Restricted to characters, we obtain

$$\langle \chi_1, \chi_2 \rangle = \frac{1}{|G|} \sum_{g \in G} \chi_1(g)\chi_2(g^{-1}).$$

[26]Check that this is a well-defined Hermitian inner product.

Theorem 5.26 (First orthogonality relation)**.** *If χ_i and χ_j are irreducible characters of G, then $\langle \chi_i, \chi_j \rangle = 1$ if $\chi_i = \chi_j$, and* 0 *otherwise.*

Proof. Let

$$\mathbb{C}G \cong M_{n_1}(\mathbb{C}) \oplus \cdots \oplus M_{n_k}(\mathbb{C})$$

and let e_i denote the element $(0, \ldots, 0, 1, 0 \ldots, 0)$ with the $n_i \times n_i$ identity matrix in the ith position, and the 0 matrix everywhere else. Write $e_i = \sum_g \alpha_g g$; we want to compute the coefficients α_g. For $h \in G$,

$$he_i = (0, \ldots, \varphi_h^{(i)}, \ldots 0).$$

If ρ is the character of the regular representation,

$$\rho(he_i) = \sum_g \alpha_g \rho(hg) = \alpha_{h^{-1}} |G|.$$

On the other hand, using the decomposition of the regular representation and the identity for he_i,

$$\rho(he_i) = \sum_{j=1}^{k} \chi_j(1)\chi_j(he_i) = \chi_i(1)\chi_i(h).$$

That is,

$$\alpha_h = \frac{1}{|G|}\chi_i(1)\overline{\chi_i(h)},$$

so

$$e_i = \frac{1}{|G|}\sum_g \chi_i(1)\overline{\chi_i(g)}g.$$

Using the fact that $e_i e_j = \delta_{ij} e_i$,[27]

$$\begin{aligned} e_i e_j &= \frac{1}{|G|^2}\sum_g \chi_i(1)\overline{\chi_i(g)}g \sum_h \chi_j(1)\overline{\chi_j(h)}h \\ &= \frac{\chi_i(1)\chi_j(1)}{|G|^2}\sum_{g,h}\chi_i(g^{-1})\chi_j(h^{-1})gh \\ &= \frac{\chi_i(1)\chi_j(1)}{|G|^2}\sum_{g,x}\chi_i(g^{-1})\chi_j(x^{-1}g)x. \end{aligned}$$

Looking at the coefficient for $x = 1$,

$$\begin{aligned} i = j &\implies \frac{1}{|G|}\sum_g \chi_i(g)\chi_i(g^{-1}) = 1, \\ i \neq j &\implies \frac{1}{|G|}\sum_g \chi_i(g^{-1})\chi_j(g) = 0. \end{aligned}$$

□

This gives us a proof of the fact that the irreducible characters form a basis of the space of class functions – in fact, an orthonormal basis.

Corollary 5.27. *A class function χ is an irreducible character of G if and only if $\chi(1) > 0$ and $\langle \chi, \chi \rangle = 1$.*

Corollary 5.28. *Two irreducible representations of G are equivalent if and only if their characters are equal.*

Corollary 5.29. *Let ν be a class function of G, and $\nu = \sum_{i=1}^k c_i \chi_i$ its expression in terms of the irreducible characters. ν is a character of G if and only if each c_i is a nonnegative integer.*

[27] For those unfamiliar, $\delta_{ij} = 1$ if $i = j$ and 0 otherwise.

A natural question to ask is: what if the sum in the inner product is taken over the irreducible characters of G? Let $Irr(G)$ denote the set of irreducible characters.

Theorem 5.30 (Second orthogonality relation)**.** *Let $g, h \in G$. Then,*

$$\sum_{\chi \in Irr(G)} \chi(g)\overline{\chi(h)}$$

is equal to 0 *if g is not conjugate to h, and equal to $|C_G(g)|$ otherwise.*

Proof. Let $g_1, \dots, g_k$ be representatives of the conjugacy classes of G, $Cl(g_i)$ the corresponding conjugacy class, and $\chi_1, \dots, \chi_k$ the irreducible characters. Let X be the $k \times k$ matrix whose (ij)-entry is $\chi_i(g_j)$. The first orthogonality relation says,

$$|G|\delta_{ij} = \sum_{g \in G} \chi_i(g)\overline{\chi_j}(g) = \sum_{v=1}^{k} |Cl(g_v)| \cdot \chi_i(g_v)\overline{\chi_j(g_v)}.$$

Let D be the $k \times k$ diagonal matrix with diagonal entries $|Cl(g_i)|$. We can represent this system of equations as the $k \times k$ matrix equation

$$|G| \cdot I = XDX^*,$$

where $X^* = \overline{X}^T$. This says $|G|^{-1} \cdot X$ is a left inverse for DX^*, so they commute.

$$|G|I = DX^*X.$$

As a system of equations, this yields

$$|G|\delta_{ij} = \sum_{v} |Cl(g_i)| \cdot \overline{\chi_v(g_i)}\chi_v(g_j).$$

Since $|G|/|Cl(g_i)| = |C_G(g_i)|$,[28] we get

$$\sum_{\chi \in Irr(G)} \chi(g_j)\overline{\chi(g_i)} = |C_G(g_i)|\delta_{ij}.$$

□

Let us look at the *character table* of a group G to shed some light on these orthogonality relations. This is a $k \times k$ table whose rows are indexed by the irreducible characters of G, and columns by the conjugacy classes, i.e. we consider the matrix X that we defined as a table. If we consider the standard Hermitian inner product on $\mathbb{C}^k$, $\langle x, y \rangle_{\mathbb{C}} = \sum_{i=1}^{k} x_i \overline{y_i}$, then the first orthogonality relation says,

Corollary 5.31. *The rows of the character table are orthogonal.*

and the second orthogonality relation says,

Corollary 5.32. *The columns of the character table are orthogonal.*

Let us look at some example of character tables. If ω denotes a primitive 3rd root of unity, then the following is the character table on $\mathbb{Z}_3$.

	0	1	2
$\mathbf{1}$	1	1	1
χ_1	1	ω	ω^2
χ_2	1	ω^2	ω

In general, if $\mathbb{Z}_n$ is the cyclic group with generator g, and ζ_n denotes a primitive nth root of unity, then the character table X is given by

$$X_{ij} = \chi_i(g^j) = \left(\zeta_n\right)^{ij}, i = 0, \dots, n-1.$$

[28] This is by the orbit-stabilizer lemma!

Let us try to determine the character table of the smallest nonabelian group, S_3. We immediately know of two characters: the trivial character and the sign character, which sends each permutation to its sign in $\{\pm 1\}$. Since $[S_3, S_3] = A_3 (\cong \mathbb{Z}_3)$, and $|S_3 : A_3| = 2$, these are the only linear characters of S_3. Further, S_3 has exactly 3 conjugacy classes, so the remaining irreducible character must be 2-dimensional.

	1	(12)	(123)
$\mathbf{1}$	1	1	1
χ_{sign}	1	-1	1
?	2	?	?

Since the columns of the character table are orthogonal, we can fill in the remaining values.

	1	(12)	(123)
$\mathbf{1}$	1	1	1
χ_{sign}	1	-1	1
χ_{standard}	2	0	-1

The last character corresponds to the *standard representation* of S_3. Let $\{e_1, e_2, e_3\}$ be the standard basis vectors of $\mathbb{C}^3$, and let $V \subset \mathbb{C}^3$ be the 2-dimensional subspace $V = \{\lambda_1 e_1 + \lambda_2 e_2 + \lambda_3 e_3 : \lambda_1 + \lambda_2 + \lambda_3 = 0\}$. The action of S_3 on V by permuting the standard basis vectors of $\mathbb{C}^3$ is the standard representation.

5.5 Induced representations

Given a representation φ of a group G, its restriction φ_H to a subgroup $H \leq G$ is a representation of H. Conversely, given a representation of a subgroup H of G, how can we extend it to the whole group? We study *induced representations* by studying their characters.

Definition 5.33. Given a class function ν on H, where $H \leq G$, the *induced class function* on G is

$$\nu^G(g) = \frac{1}{|H|} \sum_{x \in G} \nu^o(xgx^{-1})$$

where $\nu^o(xgx^{-1}) = \nu(xgx^{-1})$ if $xgx^{-1} \in H$, and 0 otherwise.

Vigyázz. If $H \lhd G$, ν is constant on the conjugacy classes of H, but not necessarily on the conjugacy classes of H in G, which is why we need this "averaging". That is, for $g \in G$ and $x \in H$, it is not necessary that x and gxg^{-1} are conjugate in H.

Equivalently, let T be a *transversal* (a set of representatives) for the cosets of H in G. Then,

$$\nu^G(g) = \sum_{t \in T} \nu^o(tgt^{-1}).$$

It is not immediately clear that the induction of a character of H is a character of G, and we will need the following statement to prove it.

Proposition 5.34 (Frobenius reciprocity)**.** *Let $H \leq G$, ν be a class function on H and μ a class function on G. Then,*

$$\langle \nu, \mu_H \rangle_H = \langle \nu^G, \mu \rangle_G.$$

Proof. We have

$$\begin{aligned}
\langle \nu^G, \mu \rangle &= \frac{1}{|G|} \sum_g \nu^G(g)\overline{\mu(g)} \\
&= \frac{1}{|G|}\frac{1}{|H|} \sum_g \sum_x \nu^o(xgx^{-1})\overline{\mu(g)} \\
&= \frac{1}{|G|}\frac{1}{|H|} \sum_g \sum_x \nu^o(xgx^{-1})\overline{\mu(xgx^{-1})} \\
&= \frac{1}{|G|}\frac{1}{|H|} \sum_x \sum_y \nu^o(y)\overline{\mu(y)} \\
&= \frac{1}{|H|} \sum_{y \in H} \nu(y)\overline{\mu(y)} \\
&= \langle \nu, \mu_H \rangle.
\end{aligned}$$

□

Corollary 5.35. *If $H \leq G$ and ν is a character of H, then ν^G is a character of G.*

Proof. We only need the fact that for any irreducible character $\chi \in Irr(G)$, $\langle \nu^G, \chi \rangle$ is a nonnegative integer, which follows from Frobenius reciprocity. □

Corollary 5.36. *If $H \leq G$ and $\nu \in Irr(H)$, then for some $\chi \in Irr(G)$, ν is a constituent of χ_H.*

Clifford's theorem

How do we induce characters from normal subgroups? Let $N \lhd G$ and $\nu \in Irr(N)$. G acts on $Irr(N)$ by conjugation,

$$\nu \to \nu^g; \quad \nu^g(x) = \nu(gxg^{-1}).$$

Each stabilizer is called an *inertia subgroup*,

$$I_G(\nu) = \{g \in G : \nu^g = \nu\}.$$

Theorem 5.37 (Clifford's theorem)**.** *Let $N \lhd G$ have finite index, and $\chi \in Irr(G)$. For any $\nu \in Irr(N)$ such that $\langle \chi_N, \nu \rangle \neq 0$, there exist positive integers e and t so that*

$$\chi_N = e \sum_{i=1}^{t} \nu_i,$$

where ν_i runs over the orbit of ν, and $t = |G : I_G(\nu)|$.

Proof. It is clear that the distinct conjugates of ν, say $\nu_1, \nu_2, \ldots, \nu_t$, correspond to the index of the inertia subgroup. For $n \in N$,

$$\nu^G(n) = \frac{1}{|N|} \sum_g \nu^0(g^{-1}ng) = \frac{1}{|N|} \sum_g \nu^g(n)$$

If $\phi \in Irr(N)$ is different from the ν_i, then

$$0 = \langle \sum_g \nu^g, \phi \rangle = \langle (\nu^G)_H, \phi \rangle = 0.$$

Since χ is a constituent of ν^G by Frobenius reciprocity, it follows that $\langle \chi_N, \phi \rangle = 0$. So all the irreducible constituents of χ_N are among the ν_i, and

$$\chi_N = \sum_{i=1}^{t} \langle \chi_N, \nu_i \rangle \nu_i.$$

Since $\chi_N^g = \chi_N$ for all $g \in G$,

$$\langle \chi_N, \nu_i \rangle = \langle \chi_N, \nu \rangle = e$$

is the desired integer. □

Theorem 5.38 (Still Clifford)**.** *Let $I = I_G(\nu)$. Define*

$$\mathcal{I} = \{\psi \in Irr(I) : \langle \psi_N, \nu \rangle \neq 0\},$$

and

$$\mathcal{G} = \{\chi \in Irr(G) : \langle \chi_N, \nu \rangle \neq 0\}.$$

The map $\psi \longrightarrow \psi^G$ is a bijection of $\mathcal{I}$ onto $\mathcal{G}$. Further, if $\psi^G = \chi$, then ψ is the unique irreducible constituent of χ_I in $\mathcal{I}$.

As a corollary of this, the irreducible character χ from Clifford's first theorem is in fact induced by an irreducible character of the inertia subgroup.

Proof. Let $\psi \in \mathcal{I}$ as in the statement, and $\chi \in Irr(G)$ be an irreducible constituent of ψ^G. By Frobenius reciprocity, ψ is an irreducible constituent of χ_I, and since ν is a constituent of ψ_N, $\langle \nu, \chi_N \rangle \neq 0$. Then,

$$\chi_N = e \sum_{i=1}^{t} \nu_i$$

and ν is I-invariant, so

$$\psi_N = f \cdot \nu$$

for some integer f. ψ is a constituent of χ_N, so $f \leq e$. So,

$$et \cdot \nu(1) = \chi(1) \leq \psi^G(1) = t \cdot \psi(1) = ft \cdot \nu(1) \leq et \cdot \nu(1).$$

Since we have equality everywhere, $\chi(1) = \psi^G(1)$, so $\chi = \psi^G$. Further,

$$\langle \psi_N, \nu \rangle = f = e = \langle \chi_N, nu \rangle.$$

This shows that the map $\psi \longrightarrow \psi^G$ is injective. Suppose $\psi_1, \psi_2 \in \mathcal{I}$, $\psi_1^G = \chi$, and ψ_2 is a constituent of χ_I.

$$\langle \chi_N, \nu \rangle \geq \langle (\psi_1 + \psi_2)_N, \nu \rangle = \langle (\psi_1)_N, \nu \rangle + \langle (\psi_2)_N, \nu \rangle > \langle (\psi_1)_N, \nu \rangle,$$

which contradicts Frobenius reciprocity. So, ψ_1 is the unique irreducible constituent of χ_N.

Finally, suppose $\chi \in Irr(G)$, and $\langle \chi_N, \nu \rangle \neq 0$. Then there is an irreducible constituent $\psi \in Irr(I)$ of χ_I with $\langle \psi_N, \nu \rangle \neq 0$. Clearly $\psi \in \mathcal{I}$ and χ is an irreducible constituent of ψ^G, i.e. $\chi = \psi^G$. □

6 Applications of representation theory

6.1 Burnside's theorem

Theorem 3.26. *[Burnside's theorem] Groups of order $p^a q^b$ are solvable.*

Lemma 6.1. *If χ is an irreducible character of G, then*

$$|G : C_G(g)| \frac{\chi(g)}{\chi(1)}$$

is an algebraic integer.

Proof. Let $g_1, \ldots, g_k$ represent the conjugacy classes of G, and say $g \sim g_i$ if they are conjugate. A basis for $Z(\mathbb{C}G)$ is then given by the elements $s_i = \sum_{g \sim g_i} g$. Since each product $s_i s_j \in Z(\mathbb{C}G)$, there are nonnegative integers a_{jm} such that

$$s_i s_j = \sum_{m=1}^{k} a_{jm} s_m.$$

Since each irreducible representation appears in the decomposition of $\mathbb{C}G$, we consider the representation φ associated to χ as a map $\varphi : \mathbb{C}G \to \mathbb{C}G$. Then, $\varphi(s_i)$ is equal to some $\lambda_i \in Z(\mathbb{C}G)$. Let $A = (a_{jm})_{j,m=1}^k$ and $\lambda = (\lambda_m)_{m=1,\ldots,k}$.

$$A \cdot \lambda = \lambda_i \cdot \lambda.$$

As an eigenvalue of an integer matrix, λ_i is an algebraic integer. So, on one hand since $\varphi(s_i)$ is a diagonal matrix,

$$\chi(s_i) = \operatorname{Tr}(\varphi(s_i)) = \lambda_i \chi(1)$$

and on the other,

$$\chi(s_i) = \sum_{g \sim g_i} \chi(g) = |G : C_G(g_i)|\chi(g_i).$$

□

Lemma 6.2. *The dimension of an irreducible representation divides the order of the group.*

Proof. It is clear that $|G|/\chi(1)$ is a rational number. We want to show that it is an algebraic integer, and then use the fact that the only rational numbers that are algebraic integers are the integers. Since $\langle \chi, \chi \rangle = 1$,

$$\frac{|G|}{\chi(1)} \langle \chi, \chi \rangle = \sum_g \frac{1}{\chi(1)} \chi(g)\chi(g^{-1}) = \sum_{i=1}^k \frac{|G : C_G(g_i)|}{\chi(1)} \chi(g_i)\chi(g_i^{-1}).$$

$\chi(g_i^{-1})$ is the sum of some roots of unity, so the expression on the right is an algebraic integer. □

Lemma 6.3. *If* $\gcd\big(|G : C_G(g)|, \chi(1)\big) = 1$, *then* $\chi(g) = 0$ *or* $|\chi(G)| = \chi(1)$.

Proof. Write $\chi(g) = \epsilon_1 + \cdots + \epsilon_d$ as a sum of rth roots of unity, where r is the order of g (by Lemma 5.19). Let K be a splitting field over $\mathbb{Q}$ for the nth roots of unity, where $n = |G|$. We can write

$$1 = u \cdot \chi(1) + v \cdot |G : C_G(g)|; \quad u, v \in \mathbb{Z}.$$

Then,

$$\frac{\chi(g)}{\chi(1)} = u \cdot \chi(g) + v \cdot |G : C_G(g)| \frac{\chi(g)}{\chi(1)}.$$

This is an algebraic integer, so

$$\operatorname{Nm}_{K/\mathbb{Q}}\Big(\chi(g)/\chi(1)\Big) = \prod_{\operatorname{Gal}(K/\mathbb{Q})} \sigma\Big(\chi(g)/\chi(1)\Big) \in \mathbb{Z}.$$

However, as $\chi(g)$ is a sum of d roots of unity, and $\chi(1) = d$, for all $\sigma \in \operatorname{Gal}(K/\mathbb{Q})$,

$$\Big|\sigma\Big(\chi(g)/\chi(1)\Big)\Big| \leq 1 \implies \operatorname{Nm}_{K/\mathbb{Q}}\Big(\chi(g)/\chi(1)\Big) \in \big\{-1, 0, 1\big\}.$$

If the norm is 0, then $\chi(g) = 0$, and if it is ± 1, then $|\chi(g)| = \chi(1)$. □

Lemma 6.4. *If the conjugacy class of some element* $g \neq 1$ *has size a prime power, then either* G *is not simple or* G *has prime order.*

Proof. Recall the notation $Cl(g)$ for its conjugacy class, and that $|Cl(g)| = |G : C_G(g)|$. If $|Cl(g)| = 1$ for all $g \in G$, then G is abelian and the lemma holds. Suppose G is nonabelian. If $|Cl(g)| = 1$ for some nonidentity $g \in G$, then $Z(G)$ is nontrivial, so G is not simple.

So we may assume that for all nonidentity $g \in G$, $|Cl(g)| = p^e$, for $e > 0$, where the prime p may depend on g. We want to show that there is an irreducible character χ such that $\gcd(\chi(1), p) = 1$ and $|\chi(g)| = \chi(1)$. Suppose for every such character, $\chi(g) = 0$ by the previous lemma. By the second orthogonality relation, since 1 and g are not conjugate,

$$0 = \sum_\chi \overline{\chi(1)}\chi(g) = 1 + \sum_{p \mid \chi(1)} \chi(1)\chi(g).$$

Rearranging,

$$-1/p = \sum_{p \mid \chi(1)} \chi(1)\chi(g)/p.$$

The above expression must be an algebraic integer, but $-1/p$ is not, a contradiction.

Choose χ such that $|\chi(g)| = \chi(1)$ and $\gcd(p, \chi(1)) = 1$. If the kernel of the corresponding representation φ is nontrivial, then G is not simple – so suppose it is faithful. Then $G \cong \varphi(G)$. Since $|\chi(g)| = \chi(1)$, and $\chi(g)$ is the sum of $\chi(1)$ roots of unity, there is a basis in which φ_g is a scalar matrix. In this case, $Z(G) \cong Z(\varphi(G))$ is nontrivial. □

Proposition 6.5. *There is no simple group of order $p^a q^b$.*

Proof. If G is simple, then $|Z(G)| = 1$, and no nonidentity conjugacy class has prime power order by the previous lemma. Each nonidentity class must have size divisible by pq, so $|G| = 1 + kpq$ by the class equation, but this is nonsense. □

Burnside's theorem now follows easily by induction on $|G|$. By Proposition 6.5, G has a nontrivial normal subgroup N, and N and G/N are solvable by induction.

6.2 The Frobenius kernel

Now we will prove that the Frobenius kernel of a Frobenius group is a normal subgroup, which is a fact we used in Theorem 4.22. We will formulate an entirely group-theoretic statement, and magically use representation theory to prove it. We say a permutation group $G \leq S_\Omega$ is a *Frobenius group* if it is transitive, not regular, and every nonidentity $g \in G$ has at most one fixed point.

Definition 6.6. The *Frobenius kernel K* of a Frobenius group G is

$$K = \{g \in G : g \text{ has no fixed points}\} \cup \{1\}$$

By Burnside's lemma,

$$1 = \frac{1}{|G|} \sum_{g \in G} \operatorname{fix}(g) = \frac{1}{|G|}\left(\sum_{g \notin K} 1 + |\Omega|\right) = \frac{|G| - |K| + |\Omega|}{|G|}.$$

In other words,

$$|K| = |\Omega|.$$

Of course, having named K a kernel, we would like it to be a normal subgroup of G. Clearly, $1 \in K$, and if $k \in K$ has no fixed points, neither does k^{-1}. Similarly, if $k \in K$ and $g \in G$, then $g^{-1}kg$ also has no fixed points. Surprisingly, the tricky part of the proof is to show that K is in fact a sub*group*: that it is closed under the group operation.

Lemma 6.7. *The following are equivalent.*

1. *G is a Frobenius group.*
2. *There is a nontrivial proper subgroup $H \leq G$ such that $\forall g \in G \setminus H$, $g^{-1}Hg \bigcap H = \{1\}$.*

Proof. The action of G on the cosets of a stabiliser by conjugation is equivalent to the action of G on Ω. So if G is a Frobenius group, set $H = G_\omega$. Conversely, if H is such a subgroup, G is a Frobenius group acting by conjugation on the cosets of H. □

Corollary 6.8. *If H is a subgroup as in part 2 of the lemma, then the Frobenius kernel of G is*

$$K = G \setminus \left(\bigcup_g g^{-1}Hg\right) \cup \{1\}.$$

Theorem 6.9. *The Frobenius kernel is a normal subgroup of G.*

Proof. We will construct K as the kernel of some homomorphism, by using the alternative characterisation of a Frobenius group. Let H be a nontrivial subgroup of G as in the lemma.

Step (1)**.** If $h_1, h_2 \in H$ are conjugate in G, then they are conjugate in H.

If $h_1 = g^{-1}h_2g$ for $g \in G$, then $g^{-1}Hg \cap H \neq \emptyset$, so $g \in H$.

Step (2)**.** If f is a class function on H, the extension $\tilde{f}$ to G defined by

$$\tilde{f}(x) = \begin{cases} f(h), & \text{if } x \text{ is conjugate to } h \\ f(1), & \text{otherwise} \end{cases}$$

is a class function on G.

Since conjugacy is an equivalence relation, we only need to check that this is well-defined, i.e if x is conjugate to both h_1 and h_2 in G, then h_1 is conjugate to h_2 in H, but this was proved in step 1.

Step (3)**.** $\tilde{f} : \mathbb{C}G \to \mathbb{C}$ is a ring homomorphism that preserves complex conjugation.

This is more of an observation than a statement requiring proof.

Step (4)**.** If f is a class function on H, and t a class function on G, then

$$\langle \tilde{f}, t\rangle_G = \langle f, t_H\rangle_H + f(1)\big(\langle 1_G, t\rangle_G - \langle 1_H, t_H\rangle_H\big).$$

This formula is linear in f, and every class function on H can be expressed as a linear combination of 1_H and some class function f such that $f(1) = 0$. So it suffices to check it for these two types of functions.

If $f = 1_H$, then $\tilde{f} = 1_G$, so

$$\langle 1_G, t\rangle_G = \frac{1}{|G|}\sum_{g\in G} t(g) = \frac{1}{|G|}\sum_{i=1}^{n}\sum_{x\in g_i^{-1}Hg_i} t(x) = \frac{1}{|H|}\sum_{x\in H} t(x) = \langle 1_H, t_H\rangle_H,$$

where $g_1, \dots, g_n$ form a system of coset representatives for G/H.

Now suppose $f(1) = 0$.

$$\langle \tilde{f}, t\rangle_G = \frac{1}{|G|}\sum_{g\in G} \tilde{f}(g)\overline{t(g)} = \frac{1}{|G|}\sum_{i=1}^{n}\sum_{x\in g_i^{-1}Hg_i} \tilde{f}(x)\overline{t(x)} = \frac{1}{|H|}\sum_{x\in H} \tilde{f}(x)\overline{t(x)} = \langle f, t_H\rangle_H.$$

Step (5)**.** The map $f \to \tilde{f}$ is an isometry, i.e.

$$\langle f_1, f_2\rangle_H = \langle \tilde{f}_1, \tilde{f}_2\rangle_G.$$

We use Frobenius reciprocity:

$$\langle \tilde{f}_1, \tilde{f}_2\rangle_G = \langle \tilde{f}_1\overline{\tilde{f}_2}, 1_G\rangle_G = \langle f_1\overline{f_2}, 1_H\rangle_H = \langle f_1, f_2\rangle_H.$$

Step (6)**.** If f is a character of H and t is a character of G, then $\langle \tilde{f}, t\rangle_G$ is an integer.

Now, t_H is a character of H, so from step 4,

$$\langle \tilde{f}, t\rangle_G = \langle f, t_H\rangle_H + f(1)\big(\langle 1_G, t\rangle_G - \langle 1_H, t_H\rangle_H\big) \in \mathbb{Z}.$$

Step (7)**.** If χ is an irreducible character of H, then $\tilde{\chi}$ is an irreducible character of G.

$\tilde{\chi}$ is an irreducible character of G if and only if $\tilde{\chi}(1) > 0$ and $\langle \tilde{\chi}, \tilde{\chi}\rangle_G = 1$. Suppose $\chi \neq 1_H$, so $\tilde{\chi} \neq 1_G$, then by step 5

$$\langle \tilde{\chi}, \tilde{\chi}\rangle_G = \langle \chi, \chi\rangle_H = 1.$$

Step (8)**.** The Frobenius kernel is the kernel of the regular representation of H extended to G.

Let ρ be the character of the regular representation of H; we claim that the kernel of the representation associated to $\tilde{\rho}$ is the Frobenius kernel. This follows because $\tilde{\rho}(x) = \rho(1)$ if x is not conjugate to any element of H, i.e. $x \in K$ and $\tilde{\rho}(x) = 0$ otherwise. $\square$

6.3 Induced characters

Let us look at extending irreducible characters from a normal subgroup to the entire group.

Theorem 6.10. *If G/N is cyclic and $\nu \in Irr(N)$ is G-invariant, i.e. $\nu^g = \nu$ for all $g \in G$, then $\exists \chi \in Irr(G)$ such that $\chi_N = \nu$.*

Proof. Let $|G : N| = k$, $a \in G$ be a generator of G/N, and $a^k = b \in N$. Suppose ν corresponds to a representation φ of N on V. We want to define $\varphi_a \in GL(V)$ so that

(i) $\varphi_{a^{-1}}\varphi_x\varphi_a = \varphi_{a^{-1}xa}$ for all $x \in N$, and

(ii) $\left(\varphi_a\right)^k = \varphi_b$.

□

Since condition (i) corresponds to finding a good conjugate representation, we can find some matrix A satisying it. Then, $A^{-k}\varphi_x A^k = \varphi_{b^{-1}}\varphi_x\varphi_b$, or $\varphi_x(A^k\varphi_{b^{-1}}) = (A^k\varphi_{b^{-1}})\varphi_x$. $A^k\varphi_{b^{-1}}$ commutes with every matrix φ_x, and these generate the full matrix algebra by Wedderburn-Artin, so $(A^k\varphi_{b^{-1}})$ is a scalar matrix $\lambda \cdot I$. Setting $\varphi_a = \lambda^{1/k} \cdot A$ yields the desired irreducible representation of G.

M-groups

Definition 6.11. $\chi \in Irr(G)$ is *monomial* if there is some $H \leq G$ and $\lambda \in Irr(H)$ so that $\chi = \lambda^G$ and $\lambda(1) = 1$.

We say an irreducible representation is monomial if the corresponding character is. An *M-group* is one for which every irreducible representation is monomial.

Theorem 6.12. *Every nilpotent group is an M-group.*

Proof. Let G be a nilpotent group and $\chi \in Irr(G)$. Let H be a minimal subgroup of G so that for some $\psi \in Irr(H)$, $\chi = \psi^G$. Then ψ is a faithful primitive character of $\bar{H} = H/\ker(\psi)$. (A primitive character is one that cannot be induced from a proper subgroup.) Since $\bar{H}$ is nilpotent, it has a normal self-centralizing subgroup A. By Clifford's theorem, $\psi_A = e\sum_{i=1}^{t}\nu_i$, where the ν_i are some irreducible characters of A. And $\psi = \nu^{\bar{H}}$ induced from the inertia subgroup. But ψ is primitive and faithful on $\bar{H}$, so $t = 1$, and $\psi_A = e\nu$ for some $\nu \in Irr(A)$: ν is *linear*. Thus $A \leq Z(\psi(\bar{H})) \leq Z(\bar{H})$, and $C_G(A) = \bar{H}$, so H itself must be abelian. So ψ is a linear character and this completes the proof. □

6.4 The order of a finite simple group

In this section we will take a baby step towards the **c**lassification of **f**inite **s**imple **g**roups. We say an *involution* in a group is an element of order 2. Our main goal will be to show that the order of a finite simple group can be bounded by the structure of its involutions. We will achieve this using characters. Let us begin by defining the *symmetric* and *alternating* parts of a character χ. Suppose χ corresponds to a representation of G on V. We can associate a representation on the space $V \otimes V$, which is defined as follows. Let $v_1, \ldots, v_d$ be a basis of V. A corresponding basis of $V \otimes V$ is given by the *elementary tensors*

$$v_i \otimes v_j : \quad i, j = 1, \ldots, d.$$

A "typical" element of $V \otimes V$ has the form

$$\sum_{i,j} a_i b_j (v_i \otimes v_j).$$

The representation of G is extended as

$$\varphi_g(v_i \otimes v_j) = \varphi_g v_i \otimes \varphi_g v_j.$$

This is then extended linearly as a representation of G on $V \otimes V$, so the corresponding action of $\mathbb{C}G$ on $V \otimes V$ as a $\mathbb{C}G$-module is given by

$$\Big(\sum_g \alpha_g g\Big)v = \sum_g \alpha_g \varphi_g(v).$$

Vigyázz. Of course, given representations of G on V and W, we can consider the $\mathbb{C}G$-module $V \otimes W$ defined analogously. It is not obvious, but it is easy to show, that $V \otimes W$ is unique (up to isomorphism) independent of the choice of bases for V and W. In the theory of rings and modules, it is not typically true that if V and W are R-modules, then $V \otimes W$ is an R-module with $r(v \otimes w) = rv \otimes rw$. For this reason, it is not necessary that for any $\alpha \in \mathbb{C}G$, $\alpha(v_i \otimes v_j) = \alpha v_i \otimes \alpha v_j$.

In the more general setting of $V \otimes W$, we have that

Theorem 6.13. *If V and W are $\mathbb{C}G$-modules with corresponding characters χ and ψ, then $V \otimes W$ has character $\chi\psi$, independent of the choice of basis.*

Proof. This follows from the fact that for any two matrices $A \in GL(V)$ and $B \in GL(W)$, $\mathrm{Tr}(A \otimes B) = \mathrm{Tr}(A)\mathrm{Tr}(B)$, but this can also be proven directly. [29] □

Now, we can decompose the space $W = V \otimes V$ into *symmetric* and *alternating* parts as follows. Define a linear map $* : W \longrightarrow W$ on the basis

$$(v_i \otimes v_j)^* = v_j \otimes v_i.$$

Define

$$W_S = \{w \in W : w^* = w\}, \quad W_A = \{w \in W : w^* = -w\}.$$

It is clear that these are subspaces of W, $W_S \cap W_A = 0$, and since for all $w \in W$, $w + w^* \in W_S$ and $w - w^* \in W_A$, the decomposition

$$w = \frac{w + w^*}{2} + \frac{w - w^*}{2}$$

tells us that $W = W_S \oplus W_A$. Their respective bases are given by

$$W_S = \Big\langle (v_i \otimes v_j) + (v_j \otimes v_i) : i \le j \Big\rangle, \quad W_A = \Big\langle (v_i \otimes v_j) - (v_j \otimes v_i) : i < j \Big\rangle.$$

Finally, we want to see that W_S and W_A are $\mathbb{C}G$-modules. We claim that $(\varphi_g w)^* = \varphi_g(w^*)$. It suffices to check this on the basis of elementary tensors:

$$(\varphi_g v_i \otimes \varphi_g v_j)^* = \varphi_g v_j \otimes \varphi_g v_i = \varphi_g\Big((v_i \otimes v_j)^*\Big).$$

As a result, any character χ induces a character χ^2 on W, which decomposes into symmetric and alternating parts

$$\chi^2 = \chi_S + \chi_A.$$

We are interested in the *class function*

$$\chi^{(2)}(g) = \chi(g^2).$$

Proposition 6.14.

$$\chi^{(2)} = \chi_S - \chi_A.$$

Proof. Let us compute χ_A. Suppose

$$\varphi_g v_i = \sum_k a_{ik} v_k.$$

Then,

$$\varphi_g(v_i \otimes v_j - v_j \otimes v_i) = \sum_{k,l} \big(a_{ik}a_{jl} - a_{jk}a_{il}\big) v_k \otimes v_l = \sum_{k<l} \big(a_{ik}a_{jl} - a_{jk}a_{il}\big)(v_k \otimes v_l - v_k \otimes v_l).$$

[29] The matrix Kronecker product of $A \in GL(m, \mathbb{C})$ and $B \in GL(n, \mathbb{C})$, $A \otimes B$, is obtained by taking the $(mn) \times (mn)$ block matrix

$$\begin{bmatrix} a_{11}B & \dots & a_{m1}B \\ & \vdots & \\ a_{m1}B & \dots & a_{mm}B \end{bmatrix}.$$

So,

$$\chi_A(g) = \sum_{i<j} a_{ii}a_{jj} - a_{ji}a_{ij}.$$

This tells us that

$$2\chi_A(g) = \sum_{i\neq j} a_{ii}a_{jj} - \sum_{i\neq j} a_{ji}a_{ij} = \Big(\sum_i a_{ii}\Big)\Big(\sum_j a_{jj}\Big) - \sum_{i,j} a_{ij}a_{ji} = \mathrm{Tr}(\varphi_g^2) - \mathrm{Tr}(\varphi_g)^2 = \chi(g)^2 - \chi(g^2).$$

Using the fact that $\chi^2 = \chi_S + \chi_A$, we obtain the desired identity. □

For the rest of this section, χ denotes an irreducible character unless stated otherwise.

Definition 6.15. The *Frobenius-Schur indicator* of an irreducible character χ is

$$\nu(G) = \frac{1}{|G|}\sum_g \chi(g^2).$$

We say χ is *real-valued* if $\chi(g) \in \mathbb{R}$ for all $g \in G$, and *complex-valued* otherwise.

Proposition 6.16. *If χ is real-valued, $\nu(\chi) = \pm 1$, and $\nu(\chi) = 0$ otherwise.*

Proof. Let 1_G denote the trivial character. From the previous proposition,

$$\nu(\chi) = \frac{1}{|G|}\sum_g \chi^{(2)}(g) = \langle \chi_S - \chi_A, 1_G\rangle = \langle \chi^2, 1_G\rangle - 2\langle \chi_A, 1_G\rangle = \langle \chi, \overline{\chi}\rangle - 2\langle \chi_A, 1_G\rangle.$$

If χ is not real-valued, then $\langle \chi^2, 1_G\rangle = 0$. Since χ_A is a constituent of χ^2, and the inner product of characters is always a nonnegative integer, $\langle \chi_A, 1_G\rangle = 0$ and $\nu(\chi) = 0$. If χ is real-valued, then $\langle \chi^2, 1_G\rangle = \langle \chi, \overline{\chi}\rangle = 1$. Then $\langle \chi_A, 1_G\rangle = 0$ or 1, so $\nu(\chi) = \pm 1$. □

Define

$$\gamma(g) = \Big|\{x \in G : x^2 = g\}\Big|.$$

It is easy to check that γ is a class function on G, so we must be able to write it as a linear combination of irreducible characters.

Lemma 6.17.

$$\gamma(g) = \sum_{\chi \in Irr(G)} \nu(\chi)\chi(g).$$

Proof. We need to show that writing γ as a sum of irreducible characters, each coefficient $\langle \gamma, \chi\rangle$ is equal to $\nu(\chi)$.

$$\langle \gamma, \chi\rangle = \frac{1}{|G|}\sum_{g\in G} \gamma(g)\overline{\chi(g)} = \frac{1}{|G|}\sum_g \sum_{x^2=g} \overline{\chi(x^2)} = \frac{1}{|G|}\sum_{x\in G} \chi(x^2) = \nu(\chi).$$

□

Let t denote the number of involutions of G (we do not count the identity). Clearly $\gamma(1) = 1 + t$.

Corollary 6.18.

$$t \leq \sum_{\chi \neq 1_G \in Irr(G)} \chi(1).$$

Lemma 6.19. *There is a non-identity conjugacy class with at most $\Big((|G| - 1)/t\Big)^2$ elements.*

Proof. Let m be the number of non-identity conjugacy classes, and let $d_1, \ldots, d_m$ be the degrees of the nontrivial irreducible characters of G. By the previous lemma,

$$t^2/m^2 \leq \Big(\sum_{i=1}^m d_i\Big)^2/m^2 \leq \sum_{i=1}^m d_i^2/m = \frac{|G|-1}{m}.$$

Multiplying both sides of the inequality by $|G|-1$ and rearranging,

$$\frac{|G|-1}{m} \leq \Big(\frac{|G|-1}{t}\Big)^2.$$

The left-hand side is the expected size of a non-identity conjugacy class, so there is a class with at most as many elements. □

Finally,

Theorem 6.20 (Brauer-Fowler)**.** *If G is a finite simple group with an involution i, then*

$$|G| \leq (|C_G(i)|^2)!$$

Proof. Every element of $C_G(i)$ is an involution so $|C_G(i)| \leq t$. Since G is simple, the action of G on the conjugacy class of size $\leq \Big((|G|-1)/t\Big)^2$ is faithful and G embeds in the corresponding symmetric group.

$$|G| \leq \Big(\frac{|G|-1}{t}\Big)^2!$$

□

6.5 Representations of S_n

Before we determine all irreducible representations of S_n, let us look at a "natural" example. S_n acts by permutation on the k-element sets of $[n]$; this corresponds to a representation ϕ_k of S_n over an $\binom{n}{k}$-dimensional space. Let π_k be the corresponding character, and set $\chi_k = \pi_k - \pi_{k-1}$, for $1 \leq k \leq n/2$. We would like to show that χ_k is an irreducible character.

$$\langle \pi_j, \pi_k \rangle = \frac{1}{n!} \sum_{g \in S_n} \pi_j(g)\pi_k(g).$$

Since $\phi_k(g)$ is a permutation matrix, there is a 1 on the diagonal exactly when the corresponding k-set is fixed by G. In particular, $\pi_j\pi_k$ is the character of the action of S_n on the pairs of sets $(X, Y) : |X| = j, |Y| = k$, and this counts the number of fixed points. So $\langle \pi_j, \pi_k \rangle$ counts the average number of fixed points, but this is the number of orbits of the action, which is $1 + \min(j, k)$.[30]

$$\langle \chi_k, \chi_k \rangle = \langle \pi_k, \pi_k \rangle - 2\langle \pi_k, \pi_{k-1} \rangle + \langle \pi_{k-1}, \pi_{k-1} \rangle = 1.$$

And

$$\chi_k(1) = \binom{n}{k} - \binom{n}{k-1} > 0,$$

so χ_k is an irreducible character.

To determine *all* irreducible representations of S_n, we turn to combinatorics. A *partition* of the integer n into k parts is a k-tuple $\lambda = (\lambda_1, \ldots, \lambda_k)$ such that each $\lambda_1 \geq \cdots \geq \lambda_k > 0$, and $\lambda_1 + \cdots + \lambda_k = n$. What does this have to do with representations of S_n? Two elements of S_n are conjugate if and only if they have the same *cycle type* – they can be (uniquely) written as a product of k disjoint cycles with sizes $\lambda_1 \geq \ldots \lambda_k \geq 1$, $\lambda_1 + \cdots + \lambda_k = n$. This immediately establishes that the number of partitions of n is equal to number of conjugacy classes of S_n, or the number of irreducible representations.

To make this correspondence explicit, we will consider the *Young diagram* of a partition λ. This is a table of boxes, where the ith row has λ_i boxes.

[30] The size of the intersection $X \cap Y$ is invariant in each orbit.

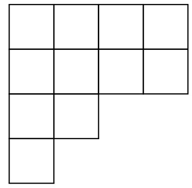


Figure 1: The Young diagram corresponding to the partition $(4, 4, 2, 1)$ of 11.

Given a Young diagram, we define the corresponding *Young tableau* by filling in the boxes with the integers $1, \ldots, n$ in some order. We say two tableaux are *(row-)equivalent* if their underlying Young diagrams are the same, and one can be obtained by permuting the elements within a row or column of the other.

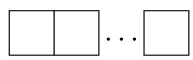
1	5	9	4
3	11	6	10
2	8		
7			

4	5	9	1
3	6	10	11
8	2		
7			

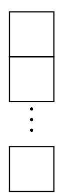
Figure 2: Two (row-)equivalent Young tableaux.

A *tabloid* is an equivalence class of tableaux. For a fixed Young diagram λ, let M^λ be the vector space whose basis is the set of λ-tabloids. The action of S_n on the tabloids yields a representation of S_n over M^λ.

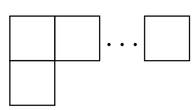
Example 6.21. The *trivial partition* $\lambda = (n)$ yields the trivial representation of S_n, as any two tableaux are row-equivalent.



Example 6.22. The partition $\lambda = (1, 1, \ldots, 1)$ yields the regular representation $\mathbb{C}S_n$, as no two tableaux are row-equivalent.



Example 6.23. Let $\lambda = (n-1, 1)$. Let t_i be the tabloid with i in the second row, for $1 \leq i \neq n$. Each permutation $g \in S_n$ sends t_i to $t_{g(i)}$, so M^λ is the permutation representation $\mathbb{C}S_n$.



Unfortunately, M^λ does not always give us an irreducible representation. We will look at the *Specht module* S^λ, generated by the set of *polytabloids*. Given a Young tableau T, let $R(T)$ denote the subgroup of permutations of S_n that only permute the elements within each row, and $C(T)$ the subgroup of permutations that only permute the elements within each column. That is, the tabloid corresponding to T is the equivalence class $[T] = \{r \cdot T : r \in R(T)\}$. The *polytabloid* corresponding to T is

$$e_T = \sum_{g \in C(T)} \sigma(g) \cdot g[T]$$

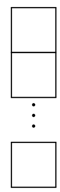
where $\sigma : S_n \longrightarrow \{\pm 1\}$ is the sign homomorphism. The submodule $S^\lambda \leq M^\lambda$ generated by the polytabloids of λ is called the *Specht module*. An easy lemma to check is that

Lemma 6.24.

$$g \cdot e_T = e_{g \cdot T}.$$

Let us look at the Specht module of the earlier examples. Clearly, $\lambda = (n)$ still yields the trivial representation.

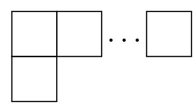
Example 6.25. $\lambda = (1, 1, \ldots, 1)$. For any tableaux T and U, clearly $C(T) = C(U)$, but $e_T = e_U$ if and only if U can be obtained from T by an even permutation. Since $g(e_T) = e_{(gT)} = \sigma(g)e_T$, S^λ is the one-dimensional sign representation of S_n.



Example 6.26. $\lambda = (n-1, 1)$. Again, if T is a tableau with i in the second row, its polytabloid is of the form $\{t_i\} - \{t_j\}$, for some $j \neq i$. So,

$$S^\lambda = \left\{c_1\{t_1\} + \cdots + c_n\{t_n\} : c_1 + \cdots + c_n = 0\right\}$$

This is the called the *standard representation* of S_n and it is $(n-1)$-dimensional.



Let us formalise all this. Given a Young diagram λ with a corresponding tableau T, define

$$r(T) = \sum_{a \in R(T)} a, \quad c(T) = \sum_{b \in C(T)} \sigma(b) \cdot b,$$

and

$$h(T) = r(T)c(T) = \sum_{a \in R(T), b \in C(T)} \sigma(b)ab.$$

We will show that the left ideal generated by $h(T)$ in $\mathbb{C}S_n$ is a simple $\mathbb{C}S_n$-module. Another easy lemma:

Lemma 6.27.

$$h(gT) = g^{-1}h(T)g.$$

Given two Young diagrams $\alpha = (\alpha_1, \ldots, \alpha_k)$ and $\beta = (\beta_1, \ldots, \beta_l)$, we say $\alpha \geq \beta$ if $(\alpha_1, \ldots, \alpha_k)$ is *lexicographically* bigger than $(\beta_1, \ldots, \beta_l)$[31].

Lemma 6.28. *Let α and β be Young diagrams with tableaux T and U respectively. Then, either (a) there exists a transposition $t \in R(T) \cap C(U)$, or (b) $\alpha = \beta$ and $U = ab(T)$ for some $a \in R(T)$ and $b \in C(T)$.*

Proof. Part (a) says that there are two elements i, j that are in the same row in T and the same column as U. Let $\alpha = (\alpha_1, \ldots, \alpha_k)$, and $\beta = (\beta_1, \ldots, \beta_l)$. If $\alpha_1 > \beta_1$, then there are two elements in the first row of T that are in the same column of U. Proceeding in this manner, if at some point $\alpha_i > \beta_i$, (a) holds. Otherwise, $\alpha = \beta$. If (a) still does not hold, then every pair of elements in the same column of U are in different rows of T. So there is some $d \in C(U)$ and $a \in R(T)$ such that $dU = aT$, or $U = d^{-1}a(T)$. Since $C(U) = d^{-1}aC(T)a^{-1}d$, for some $b \in C(T)$,

$$\begin{aligned} d &= d^{-1}aba^{-1}d, \\ ab^{-1} &= d^{-1}a, \\ U &= ab^{-1}T. \end{aligned}$$

□

[31] For the least i where $\alpha_i \neq \beta_i$, $\alpha_i > \beta_i$.

Corollary 6.29. *Suppose $\alpha \neq \beta$ and T and U are corresponding Young tableaux. Then,*

(a) $h(U)h(T) = 0$*, and*

(b) for all $a \in R(T), b \in C(T)$*,*
$$a \cdot h(T) \cdot \sigma(b)b = h(T).$$

(c) If $x \in \mathbb{C}S_n$ *satisfies that for all* $a \in R(T), b \in C(T)$*,*
$$a \cdot x \cdot \sigma(b)b = x,$$
then $x \in \mathbb{C}h(T)$*.*

Proof. (a) From our proof of the previous lemma, we see that if $\alpha \neq \beta$, assuming without loss of generality that $\alpha \succeq \beta$, there is a transposition $t \in R(T) \cap C(U)$.
$$h(U)h(T) = r(U)c(U)r(T)c(T) = r(U)c(U)t^2 r(T)c(T) = -r(U)c(U)r(T)c(T) = 0.$$
Here we use the observation that if $t \in C(U)$, then $c(U)t = \sigma(t)c(U)$.

(b) follows by a similar observation. If $a \in R(T)$, then $a \cdot r(T) = r(T)$, so
$$a \cdot h(T) \cdot \sigma(b)b = a \cdot r(T)c(T) \cdot \sigma(b)b = r(T)c(T) = h(T).$$

(c) Write $x = \sum_g c_g \cdot g$. We want to show that when $g = ab$ for some $a \in R(T), b \in C(T)$, then $c_g = c_x$ is some constant, and $c_g = 0$ otherwise. For $a \in R(T), b \in C(T)$,
$$a \cdot x \cdot \sigma(b)b = \sum_g \sigma(b)c_g agb = x$$
In other words, $c_{agb} = \sigma(b)c_g$. Or, $c_{ab} = \sigma(b)c_1$, where $c_1 = c_x$ will be our desired constant. If g is not of the form ab, let $U = gT$. By Lemma 6.28, there is a transpositon $t \in R(T) \cap C(U) = R(T) \cap gC(T)g^{-1}$. Let $a = t$, and $b = g^{-1}tg$, so $\sigma(b) = \sigma(t) = -1$, and
$$\sigma(t)c_g = c_{agb} = c_{tgg^{-1}tg} = c_g,$$
so $c_g = 0$. ☐

Corollary 6.30. $h(T)^2 = \mu_T h(T)$ *for some* $\mu_T \in \mathbb{Z}$*.*

Proof. It is easy to check that $h(T)^2$ satisfies condition (c) of the previous lemma. It is not so easy to check that μ_T is an integer, and we will not need it for our purposes, so we will simply state this useful fact. ☐

We are finally ready to prove that the left ideals $h(T)$ generated by the Young diagrams are pairwise nonisomorphic simple modules of $\mathbb{C}S_n$.

Theorem 6.31. *Let λ be a Young diagram, and T a corresponding Young tableau.*

(1) The left ideal $L(T) = \mathbb{C}S_n h(T)$ *is a simple* $\mathbb{C}S_n$*-module.*

(2) If μ is a Young diagram different from λ and U a corresponding Young tableau, then $L(T)$ and $L(U)$ are nonisomorphic.

Proof. (1) Suppose $L \leq L(T)$ is a $\mathbb{C}S_n$-submodule, i.e. a left ideal of $\mathbb{C}S_n$. For any $x \in \mathbb{C}S_n$, $h(T)xh(T)$ satisfies part (c) of Corollary 6.29, so $h(T)L(T) \leq \mathbb{C}h(T)$. Then,
$$h(T)L \leq h(T)L(T) \leq \mathbb{C}h(T).$$
$\mathbb{C}h(T)$ is a one-dimensional vector space over $\mathbb{C}$, so either $h(T)L = 0$ or $h(T)L = \mathbb{C}h(T)$. In the first case,
$$L^2 \leq L(T)L = \mathbb{C}S_n \cdot h(T)L = 0.$$

However, it is easy to check that this implies $L = 0$. In the second case,

$$L(T) = (\mathbb{C}S_n)\mathbb{C}h(T) = \mathbb{C}S_n h(T)L \leq L.$$

so $L = L(T)$.

(2) If $L(T)$ and $L(U)$ are isomorphic as $\mathbb{C}S_n$-modules, then their annihilators are equal. However, for $x = \sum_g c_g \cdot g \in \mathbb{C}S_n$,

$$h(U)xh(T) = \sum_g c_g\big(h(U)gh(T)\big) = \sum_g c_g g\big(h(g^{-1}U)h(T)\big) = 0.$$

By (a) of Lemma 6.28, $h(g^{-1}U)h(T) = 0$ for all $g \in S_n$. This shows that $h(U) \cdot L(T) = 0$, but $h(U) \cdot L(U) = \mathbb{C}h(U)$ is nonzero, so the modules are not isomorphic. □

6.6 $SU(2)$ and $SO(3)$

To warm up for the next section, we will study the (infinite) groups $SU(2)$ and $SO(3)$, and their representations.

Definition 6.32. The 3-dimensional *special orthogonal group* $SO(3)$ is the 3-dimensional rotation group, given by

$$SO(3) = \left\{X \in GL(3,\mathbb{R}) : XX^T = 1, \det(X) = 1\right\}.$$

Each matrix of $SO(3)$ is a rotation of $\mathbb{R}^3$ about a line through the origin. In particular, each matrix of $SO(3)$ is uniquely identified by the pair of antipodal points $\{P, -P\}$ where its axis intersects the unit sphere, and the angle of rotation it induces in each plane orthogonal to the axis.

We may define the 3-dimensional *orthogonal* group,

$$O(3) = \left\{X \in GL(3,\mathbb{R}) : XX^T = 1\right\}.$$

In particular, for $X \in O(3)$, $\det(X) = \pm 1$, so $SO(3)$ is a normal subgroup of index 2 in $O(3)$. As a subset of $\mathbb{R}^{3\times 3}$, $O(3)$ inherits the subspace topology, making it a compact set. It has two connected components – $SO(3)$ and $-SO(3)$. Before we get into representation theory, let us classify the finite subgroups of $SO(3)$.

Finite subgroups of $SO(3)$

Let $G \leq SO(3)$ be a nontrivial finite subgroup, so it contains rotations with only finitely many axes. Let $P_1, \ldots, P_n$ be the points where they intersect the sphere. G induces an action on the points of the sphere, and each stabilizer G_{P_i} is a finite cyclic group of some order n_i. Assume without loss of generality that G induces k orbits on O, and that $P_1, \ldots, P_k$ are the representatives of these k orbits. Of course, each point in the orbit of P_i has the same order of stabilizer, and the number of points in the orbit is $|G|/n_i$. Further, every nonidentity element of G fixes exactly 2 points, and $\sum_{g\in G} |\mathrm{fix}(g)| = \sum_{i=1}^k n_i$. Removing the identity of G from both sides of the equation,

$$\begin{aligned} 2(|G| - 1) &= \sum_{i=1}^k (n_i - 1) \\ &= \sum_{i=1}^k \left(|G| - \frac{|G|}{n_i}\right) \\ \implies 2 - \frac{2}{|G|} &= \sum_{i=1}^k \left(1 - \frac{1}{n_i}\right). \end{aligned}$$

Recall that $|G| > 1$ and $n_i > 1$ for each $i = 1, \ldots, k$. The left-hand side then takes values in the interval $[1, 2)$, while each term on the right is at least $1/2$, so $k \in \{2, 3\}$. If $k = 2$, then $n_1 = n_2 = |G|$, so G is a cyclic group generated by a rotation of order n. This is the rotational symmetry group of a regular n-gon. If $k = 3$, suppose $n_1 \leq n_2 \leq n_3$. For the right-hand side to lie in $[1, 2)$, we must have $n_1 = 2$, and $n_2 \in \{2, 3\}$. If $n_2 = 2$, then $n_3 = |G|/2$. In other words, G has an element of order 2 that maps a point P to $-P$ (corresponding to n_3), while n_1 and n_2 correspond to antipodal points P_1 and $-P_1$ so that G has a rotation of order $|G|/2$ about the corresponding axis. This is all a complicated way to say that G is a dihedral group D_{n_3}.

We will not go into too much detail for the remaining three cases. If $(n_1, n_2, n_3) = (2, 3, 3)$, then $|G| = 12$, and the three orbits have sizes 4, 4, and 6. One of the orbits of size 4 can be chosen as the vertices of a regular tetrahedron, so that $G \cong A_4$, its orientation-preserving symmetry group. If $(n_1, n_2, n_3) = (2, 3, 4)$, then $|G| = 24$, and the three orbits have sizes 6, 8, and 12. The orbit of size 8 can be chosen as the vertices of a cube, so that $G \cong S_4$, its orientation-preserving symmetry group. Finally, if $(n_1, n_2, n_3) = (2, 3, 5)$, then $|G| = 60$, and the three orbits have sizes 12, 20, and 30. The orbit of size 20 can be chosen as the vertices of a regular dodecahedron, so that $G \cong A_5$, its orientation-preserving symmetry group.

$SU(2)$ and its representations

It is now time to define $SU(2)$, the *special unitary group*. This is a *complex* matrix group:

$$SU(2) = \left\{A \in GL(2, \mathbb{C}) : AA^* = 1\right\}.$$

where A^* denotes the adjoint of A. It is easy to check that $A \in SU(2)$ if and only if it is of the form

$$A = \begin{bmatrix} \alpha & -\overline{\beta} \\ \beta & \overline{\alpha} \end{bmatrix} : |\alpha|^2 + |\beta|^2 = 1.$$

First, we will define a homomorphism of $SU(2)$ onto $SO(3)$ by defining an action of $SU(2)$ on a 3-dimensional real vector space. Define

$$V = \left\{ \begin{bmatrix} x & y + iz \\ y - iz & -x \end{bmatrix} : x, y, z \in \mathbb{R} \right\}.$$

Alternatively, V is characterised by

$$V = \left\{X \in GL(2, \mathbb{C}) : X^* = X, \mathrm{Tr}(X) = 0\right\}.$$

Let $SU(2)$ act on V by

$$A : X \longrightarrow A^* X A; \quad A \in SU(2), X \in V.$$

Clearly, $\mathrm{Tr}(A^*XA) = 0$, and $(A^*XA)^* = A^*XA$, so this is a well-defined action. Consider the image of $SU(2)$ in $GL(3, \mathbb{R})$ under this homomorphism. Since the action preserves the determinant of matrices in V, i.e. the length of vectors in $\mathbb{R}^3$, this image is contained in $O(3)$. The image is connected and contains the identity matrix, hence is $SO(3)$.

Now, any representation of $SU(2)$ induces a representation of $SO(3)$ under this homomorphism, so we will study the irreducible representations of $SU(2)$. Let $n \in \mathbb{N}$, and let V_n be the $\mathbb{C}$-vector space of homogenous polynomials of degree n, with basis $X^n, X^{n-1}Y, \ldots, XY^{n-1}, Y^n$. Define an action of $SU(2)$ on V_n by

$$Af\left(\begin{bmatrix} X \\ Y \end{bmatrix}\right) = f\left(A^* \begin{bmatrix} X \\ Y \end{bmatrix}\right): \quad A \in SU(2), f \in V_n.$$

It is not difficult, but tedious, to check that this is a well-defined representation of $SU(2)$. It remains to show that this is irreducible. Suppose $U \leq V_n$ is an invariant subspace for $SU(2)$; in particular, it is an invariant subspace for the diagonal matrices of $SU(2)$. Any diagonal matrix with entries $(e^{i\theta}, e^{-i\theta})$ is mapped to the diagonal matrix $(e^{-ni\theta}, \ldots, e^{ni\theta})$. These matrices have an orthonormal basis of eigenvectors in V_n, so U is a direct sum of these eigenvectors. However, any matrix in $SU(2)$ which is mapped to a matrix with only nonzero entries will not leave U invariant. Given the action of $SU(2)$ on V_n, it is not hard to believe that such a matrix exists.

7 Infinite groups

7.1 Burnside groups

The *Burnside problem* was originally posed by William Burnside in 1902: is a finitely generated group in which every element has finite order necessarily a finite group? It is easy to conceive of an infinite group in which every element has finite order – for example, the *quasicyclic* group C_p^∞, but this is not finitely generated. It is not so easy to conceive of a *finitely generated* such infinite group, so we will see a construction of one.[32]

An infinite 2-generated p-group

The idea is to define the p-measure of a group, show that every group of nonnegative p-measure has a proper subgroup of nonnegative p-measure, and then construct a group of positive p-measure. Since we inductively obtain an infinite chain of subgroups with nonnegative p-measure, this group is infinite.

Fix a group G and a prime p. Define the *p-height* of an element $g \in G$ by

$$ht_p(g) = \sup\{p^k : x^{p^k} = g \text{ for some } x \in G\}.$$

Definition 7.1. Let $G = \langle x_0, \ldots, x_n \mid w_i : i \in I\rangle$ be a presentation of G. Define the *p-measure* of the presentation

$$m_p(x_0, \ldots, x_n \mid w_i) = n - \sum_{i \in I} \frac{1}{ht_p(w_i)}.$$

For example,

$$D_4 = \langle x_0, x_1 \mid x_0^4, x_1^2, (x_0x_1)^2\rangle.$$

and

$$m_2\langle x_0, x_1\rangle = 1 - 1/4 - 1/2 - 1/2 = -1/4.$$

Lemma 7.2. *If the p-measure of a presentation of G is nonnegative, then G contains a normal subgroup of index p.*

Proof. Let $G = \langle x_0, \ldots, x_n \mid w_i : i \in I\rangle$ be a presentation of G with nonnegative p-measure. Let $F = \langle x_0, \ldots, x_n\rangle$ be a free group, and $N = \langle w_i : i \in I\rangle$ a normal subgroup, so that $G = F/N$. We want to find a *proper* subgroup H of F, $N \leq H \lhd F$, so that $|F : H| = p$. Choose $M \lhd F$ so that F/M is a maximal elementary abelian p-group, so $|F/M| = p^{n+1}$. For each $w_i \in N$, if $w_i \notin M$, then w_i has no pth root in F, i.e. $ht_p(w_i) = 1$. Since the p-measure of the presentation is nonnegative, this holds for at most n w_i's.

$$\implies |MN : M| \leq p^n \implies MN \neq F.$$

Let H be a maximal subgroup of F containing MN. Since F/M is abelian, $H \lhd F$, and since H is maximal, $|F : H| = p$. That is,

$$|{}^F\!/\!_N : {}^H\!/\!_N| = |F : H| = p.$$

$\square$

Next step: to find a suitable presentation for H/N that has nonnegative p-measure. In general, if A is a group and $g \in A$, let g^A denote the conjugates of g in A.

Lemma 7.3. *For each $w_i \in N$,*

(a) if $C_F(w_i) \not\leq H$, then $w_i^H = w_i^F$, and

(b) if $C_F(w_i) \leq H$, there is some $\alpha \in F$ such that

$$F = \bigcup_{j=0}^{p-1} \alpha^j H, \text{ and } w_i^F = \bigcup_{j=0}^{p-1} (\alpha^{-j} w_i \alpha^j)^H.$$

[32]The answer to the Burnside problem is no.

Proof. The inclusion $w_i^H \leq w_i^F$ is clear. In case (a), $C_F(w_i)H = F$ by the maximality of H, so every $f \in F$ can be expressed as $f = c \cdot h$ for $c \in C_F(w_i)$ and $h \in H$. Thus,

$$f^{-1}w_i f = h^{-1}(c^{-1}w_i c)h = h^{-1}w_i h \in w_i^H,$$

so $w_i^H = w_i^F$.

In case (b), choose α so that $F = \bigcup_{j=0}^{p-1} \alpha^j H$. For $0 \leq l, k \leq p-1$, if $\alpha^{-l}w_i\alpha^l$ and $\alpha^{-k}w_i\alpha^k$ are conjugate in F, then $\alpha^{k-l} \in C_F(w_i) \leq H$, so $k = l$. In other words, every element of F can be uniquely written as $\alpha^j h$ for $0 \leq j \leq p-1$, and $h \in H$, so the result follows. □

Lemma 7.4. *$ht_p(w_i; H) = ht_p(w_i; F)$ or $ht_p(w_i; F)/p$.*

Proof. The inequality $ht_p(w_i; H) \leq ht_p(w_i; F)$ is clear. Suppose w_i has a p^kth root u in F; then $u^p \in H$, so $ht_p(w_i; H) \geq ht_p(w_i; F)/p$. The height $ht_p(w_i; H)$ has to be an integer power of p, so it must be equal to one of these two. In particular, every root of w_i commutes with w_i, so if $C_F(w_i) \leq H$, then $ht_p(w_i; H) = ht_p(w_i; F)$. □

Corollary 7.5. *H/N has nonnegative p-measure.*

Proof. By Nielsen-Schreier, H/N has rank $(n + 1 - 1)|F : H| + 1 = np + 1$. We can define a presentation of H/N with the relations

$$\{w_i : C_F(w_i) \nleq H\} \bigcup \{\alpha^{-j}w_i\alpha^j : C_F(w_i) \leq H, 0 \leq j \leq p-1\}.$$

The p-measure of this presentation is given by

$$\begin{aligned}
m_p &= np - \sum_i \frac{1}{ht_p(w_i; H)} \\
&= np - p \sum_{C_F(w_i) \leq H} \frac{1}{ht_p(w_i; F)} - \sum_{C_F(w_i) \nleq H} \frac{1}{ht_p(w_i; F)} \\
&\geq np - p\left(\sum_{C_F(w_i) \leq H} \frac{1}{ht_p(w_i; F)} + \sum_{C_F(w_i) \nleq H} \frac{1}{ht_p(w_i; F)} \right) \\
&= p \cdot m_p(F/N).
\end{aligned}$$

□

As argued earlier, by constructing an infinite chain of nonempty proper subgroups with nonnegative p-measure, we it follows that

Theorem 7.6 (Schlage-Puchta)**.** *Any group with nonnegative p-measure is infinite.*

It only remains to actually construct such a group. Let F be the free group on 2 generators; $F = \langle x_0, x_1 \rangle = \{w_i : i \in \mathbb{N}\}$. Define

$$G = \langle x_0, x_1 \mid w_i^{p^i}, i \in \mathbb{N} \rangle.$$

Clearly, G is a 2-generated p-group, and the p-measure of the presentation is

$$1 - \sum_{i \geq 1} \frac{1}{ht_p(w_i)} \geq 1 - \sum_{i \geq 1} \frac{1}{p^i} = \frac{p-2}{p-1} > 0.$$

The bounded Burnside problem

Of course, this construction feels a little like cheating; this group has elements of arbitrarily large order. Define the *exponent* of a group G to be the least positive number n such that $g^n = 1$ for all $g \in G$ (this may be infinite). Now we pose the *bounded Burnside problem*: is a finitely generated group with finite exponent necessarily a finite group?

We may reduce this to a simpler problem. If F_r denotes the free group of rank r, then any r-generated group with exponent n is isomorphic to a subgroup of F_r/F_r^n. Define the Burnside group $B(r, n) = F_r/F_r^n$, so it suffices to ask whether $B(r, n)$ is finite. We can immediately make the following observations.

- $B(r,1) = \{1\}$.
- $B(1,n) = \mathbb{Z}_n$, the cyclic group of order n.
- $B(r,2) = \oplus_{i=1}^r \mathbb{Z}_2$. Since every element has order 2, every commutator $xyx^{-1}y^{-1} = (xy)^2 = 1$, so $B(r,2)$ is abelian and we apply the fundamental theorem of finitely generated abelian groups.

In general, $B(r,3), B(r,4)$, and $B(r,6)$ are known to be finite, while $B(2,5)$ remains unknown. The best known result for infinite Burnside groups is that $B(r,n)$ is infinite for all $r > 1$ and $n \geq 8000$. The finiteness of $B(r,3)$ and $B(r,4)$ can be proven by elementary but convoluted calculations, so let us see what they are.

Theorem 7.7. *$B(r,3)$ is finite.*

Proof. We proceed by induction, as $B(1,3) = \mathbb{Z}_3$. Let $H = B(r-1,3)$, $G = B(r,3)$, and choose $a \in G$ so that $G = \langle H, a\rangle$. By induction, H is finite, and every $g \in G$ can be written as some product

$$h_0 a^{\epsilon_1} h_1 a^{\epsilon_2} \dots a^{\epsilon_m} h_m : \epsilon_i \in \{\pm 1\}, h_i \in H.$$

Further,

$$(ah)^3 = 1 \implies aha = h^{-1}a^{-1}h^{-1}.$$

Whenever $\epsilon_i = \epsilon_{i+1}$, we may use this identity to reduce the number of a's in our expression. Further, writing $a^{-1} = a^2$, we may reduce this further to obtain an expression of the form

$$h_0 a h_1 a^{-1} h_2.$$

It is clear that there are only finitely many such expressions, so G is finite. We remark that $|B(r,3)| = 3^{r+\binom{r}{2}+\binom{r}{3}}$. □

The proof that $B(r,4)$ is finite involves a similar manipulation of identities, only we do so in a lemma.

Lemma 7.8. *If G has exponent 4, and $G = \langle H, a\rangle$ where H is finite and $a^2 \in H$, then G is finite.*

Note that this implies

Theorem 7.9. *$B(r,4)$ is finite.*

as we inductively apply the lemma to $\langle x_1\rangle \leq \langle x_1, x_2^2\rangle \leq \langle x_1, x_2\rangle \dots$.

Proof. Again, since $a^2 \in H$, every element of G can be written as

$$h_0 a h_1 a \dots a h_m : h_i \in H.$$

And,

$$(ah)^4 = 1 \implies aha = h^{-1}a(a^2h^{-1}a^2)ah^{-1}$$

so we may replace each term $ah_i a$ by this identity. In particular, we would like $h_{i-1}^{-1} = h_i$ so we may reduce the length of the expression. Consider the expressions obtained by repeated substitution of the identity:

$$\begin{aligned} h_0 a h_1 a h_2 a h_3 a \dots \\ h_0 a h_1 h_2^{-1} a(h_2') a h_2^{-1} h_3 \dots \\ h_0 a h_1 h_2^{-1} h_3^{-1} \dots \end{aligned}$$

If none of these reduce to the identity and $m > |H|$, then two of the beginning strings must be equal. As a result, $h_{i-1}^{-1} = h_i$ for some i. We can reduce this to an expression with $< |H|$ terms, so G is finite. □

7.2 Divisible groups

Definition 7.10. G is a *divisible* group if for every $g \in G$ and $n \in \mathbb{N}$, there exists $u \in G$ such that $u^n = g$.

For example, $\mathbb{Q}$ under addition is a divisible group. Using a construction involving direct limits and wreath products, we will show that

Theorem 7.11. *Every group can be embedded in a divisible group.*

Direct limits

What is a direct limit? First, we say $(I, \le)$ is a *directed set* if $\le$ is a partial order on I, and for any $i, j \in I$ there is some $k \in I$ such that $i \le k$ and $j \le k$. That is, any two elements of I have a common upper bound. A *directed system* of groups is a collection of groups $(A_i : i \in I)$ indexed by a directed set I with group homomorphisms $(f_{ij} : i \le j \in I)$ such that

(i) f_{ii} is the identity, and

(ii) $f_{ik} = f_{jk} \circ f_{ij}$ for all $i \le j \le k$.

Define an equivalence relation $\sim$ on the disjoint union $A = \bigsqcup_{i \in I} A_i$ by $x_i \sim x_j$ for $x_i \in A_i$ and $x_j \in A_j$ if for some $k \ge i, j$, $f_{ik}(x_i) = f_{jk}(x_j)$. Intuitively, two elements are equivalent if they are "equal" at some point. Define the *direct limit* $\varinjlim A_i$ as $A/{\sim}$. This induces maps $\phi_i : A_i \longrightarrow \varinjlim A_i$ by sending each element to its equivalence class, and the group operation is defined on $\varinjlim A_i$ so that the maps ϕ_i are homomorphisms.

For example, given equivalence classes $[x_i], [x_j] \in \varinjlim A_i$ for $x_i \in A_i$ and $x_j \in A_j$, choose $k \ge i, j$ and define $[x_i][x_j] = [f_{ik}(x_i) f_{jk}(x_j)]$; any two elements will eventually lie in the same group A_k. The simplest example of a direct limit of groups is when the A_i are an increasing chain of groups, i.e. I is totally ordered, $A_i \subset A_j$ for $i \le j$, and the direct limit is just the union $\bigcup_{i \in I} A_i$. A less simple example is the quasicyclic group C_p^∞. For $i \le j \in \mathbb{N}$, define the homomorphism $f_{ij} : \mathbb{Z}_{p^i} \longrightarrow \mathbb{Z}_{p^j}$ as multiplication by p^{j-i}. This yields a directed system $\{0\} \longrightarrow \mathbb{Z}_p \longrightarrow \mathbb{Z}_{p^2} \longrightarrow \dots$ whose direct limit is C_p^∞. A more intuitive approach is to think of these as the inclusion maps of the p^ith roots of unity in the p^jth roots of unity.

Proof of Theorem 7.11. For any group H, consider the wreath product $H \wr C_m = \prod_{i=1}^m H \rtimes C_m$. H embeds in this as the diagonal subgroup $\prod_{i=1}^m H \rtimes \{1\}$. Let t be a generator of C_m, and $(h, h, \dots, h; 1) \in \prod_{i=1}^m H \rtimes \{1\}$. Then, $(h, 1, \dots, 1; t)^m = (h, h, \dots, h; 1)$.

Now, let a_m be the product of the first m primes. Define $G_0 = H$, and recursively $G_m = G_{m-1} \wr C_{a_m}$. G_{m-1} has a canonical embedding in G_m, so these form a directed system of groups whose direct limit is a divisible group. □

Divisible abelian groups

We do not have to work so hard to embed every abelian group in a divisible group. A *free abelian group* with basis a set I is defined as $\bigoplus_I \mathbb{Z}$. Equivalently, this is the quotient $F(I)/F(I)'$ where $F(I)'$ is the commutator subgroup of the free group with base I.

Theorem 7.12. *Every abelian group can be embedded in a divisible group.*

Proof. We need two observations: (1) quotients and direct sums of divisible groups are divisible, and (2) every abelian group is the quotient of a free abelian group. Given an abelian group G, we have a set of relations R such that

$$G \cong {}^{\oplus_I \mathbb{Z}}\!/\!_R \le {}^{\oplus_I \mathbb{Q}}\!/\!_R$$

and the right-hand side is a divisible group. □

While $\mathbb{Q}$ is a torsion-free divisible abelian group, the groups C_p^∞ are torsion divisible abelian groups, and these are essentially the only examples.

Theorem 7.13. *Every divisible abelian group is a direct sum of some quasicyclic groups and $\mathbb{Q}$, i.e. if D is a divisible abelian group, then*

$$D \cong \bigoplus_{(I_p)_p} \mathbb{C}_p^\infty \bigoplus_I \mathbb{Q}.$$

The proof of the theorem is easy once we are able to reduce to the case when D contains no nontrivial direct summands.

Lemma 7.14. *If D is a divisible subgroup of an abelian group G, then there exists $E \leq G$ such that $G = D \oplus E$.*

Proof. We write G additively. First, apply Zorn's lemma to the poset

$$\Big\{E \leq G : E \cap D = \{0\}\Big\}$$

and obtain a maximal subgroup $E \leq G$ which is "disjoint" from D. We claim that $D \oplus E = G$. If not, choose a nonzero element $a + (D \oplus E) \in G/(D \oplus E)$. By the maximality of E, there exists a least positive integer n such that

$$n \cdot a + e = d; \quad e \in E, d \in D.$$

Letting $u \in D$ be an nth root for d, $n(a - u) = E$. Since $a \notin D \oplus E$, $a - u \notin E$, so $E + \langle a - u\rangle$ strictly contains E. However, if it intersects E nontrivially, since $n(a - u) \in E$, there exists a positive integer $m < n$ such that $m(a - u) \in D \oplus E$, so $ma \in D \oplus E$, contradicting the minimality of n. □

It is even easier to see that any direct summand of a divisible abelian group is divisible. All that remains is to show that any direct summand-free divisible abelian group is either (1) torsion, or (2) torsion-free, and then construct appropriate isomorphisms to C_p^∞ or $\mathbb{Q}$.

Exercise 48. Do that.

7.3 Infinite abelian groups

Thanks to the fundamental theorem of finitely generated abelian groups, we know almost all there is to know about their structure. Infinitely generated abelian groups tend not to be as well-behaved, but if we impose some finite structure *locally*, we can better understand them.

Locally cyclic groups

Definition 7.15. G is a *locally cyclic* group if every finitely generated subgroup is cyclic.

It is easy to check that every subgroup and quotient group of a locally cyclic group is locally cyclic. Some nontrivial examples of locally cyclic groups are the quasicyclic groups C_p^∞, and the additive group $\mathbb{Q}$.

Proposition 7.16. *Every locally cyclic group is abelian.*

More generally – and we will not prove this – every locally cyclic group is a *subquotient* of $\mathbb{Q}$, i.e. a quotient of a subgroup of $\mathbb{Q}$.

A useful tool for studying local properties of groups is the subgroup lattice, which we introduced in subsection 3.5. Locally cyclic groups can be classified by their subgroup lattices. Given a lattice, denote by $X \vee Y$ the *join* of X and Y, and by $X \wedge Y$ their *meet*.

Definition 7.17. A lattice is said to be distributive if one of the following (equivalent) conditions holds.

(1) For all X, Y, Z, $X \wedge (Y \vee Z) = (X \wedge Y) \vee (X \vee Z)$.

(2) For all X, Y, Z, $(X \wedge Y) \vee (Y \wedge Z) \vee (X \wedge Z) = (X \vee Y) \wedge (Y \vee Z) \wedge (X \vee Z)$.

Theorem 7.18 (Ore)**.** *G is locally cyclic if and only if its subgroup lattice is distributive.*

Proof. Suppose G is locally cyclic. We will show that G satisfies (1). Clearly, $X \wedge Y$ and $X \wedge Z$ are contained in $X \wedge (Y \vee Z)$, so $(X \wedge Y) \vee (X \vee Z) \leq X \wedge (Y \vee Z)$. For the reverse inclusion, let $x \in X \wedge (Y \vee Z)$. x is generated by *finite* subgroups $Y_1 \leq Y$ and $Z_1 \leq Z$, and these generate a cyclic group, so $x \in (X \wedge Y_1) \vee (X \wedge Z_1) \leq (X \wedge Y) \vee (X \wedge Z)$.

For the converse, we will first show that G is abelian. Let $X = \langle x\rangle$, $Y = \langle y\rangle$, and $Z = \langle xy\rangle$. Then, since G satisfies (2),

$$\begin{aligned} &\langle x, y\rangle \cap \langle x, xy\rangle \cap \langle y, xy\rangle = \langle x, y\rangle \\ \implies &\langle x \cap y, x \cap xy, y \cap xy\rangle = \langle x, y\rangle. \end{aligned}$$

The group on the left-hand side is a subgroup of $\langle xy\rangle$, so x and y must commute. If G is not locally cyclic, some definition-chasing tells us that there are subgroups $A \leq B \leq G$ such that $B/A \cong \mathbb{Z}_p \times \mathbb{Z}_p$ for some prime p, and this induces a sublattice of G which is not distributive. □

The minimum condition

Now we consider infinite abelian groups where ascending or descending chains of subgroups can only be finite.

Definition 7.19. A group G satisfies the *maximum condition* if every ascending chain of subgroups $A_1 \leq A_2 \leq \ldots$ eventually terminates. That is, there exists $N \in \mathbb{N}$ such that for all $n \geq N$, $A_n = A_N$.

It is easy to see that an infinitely generated group cannot satisfy the maximum condition, and conversely, since we know what the finitely generated abelian groups are,

Theorem 7.20. *An abelian group G satisfies the maximum condition if and only if it is finitely generated.*

A more interesting property to study for abelian groups is the *minimum condition*.

Definition 7.21. A group G satisfies the *minimum condition* if every descending chain of subgroups $A_1 \geq A_2 \geq \ldots$ eventually terminates.

Now, a characterisation is not so clear. For example, even $\mathbb{Z}$ does not satisfy the minimum condition. This leads to the easy observation

Lemma 7.22. *If G satisfies the minimum condition, every element of G has finite order.*

We will need one more lemma about the torsion-part of an abelian group. Let G be an abelian group, and $T \leq G$ the subgroup of all elements of G of finite order. For each prime p, let $T_p \leq T$ be the subgroup of all elements with order a power of p. We call T the *torsion-part* of G, and T_p the *p-torsion*.

Lemma 7.23.

$$T \cong \bigoplus_p T_p.$$

Vigyázz. When G is not abelian, this need not hold. In fact, T need not even be a subgroup of G.

Theorem 7.24. *An abelian group G satisfies the minimum condition if and only if it is a finite direct sum of quasicyclic groups and finite cyclic groups.*

Proof. If suffices to consider the case when G is an infinite p-group for some prime p. Let H be a minimal infinite subgroup of G by the minimum condition. Since H is a p-group, for every m coprime to p, $mH = H$. If $pH = H$, then H is divisible, so $H \cong C_p^\infty$. Otherwise, as a proper subgroup of H, pH is finite. Then H_p, the set of elements in H of order p, is infinite. But this is an infinite-dimensional vector space over $\mathbb{F}_p$, hence cannot satisfy the minimum condition.

Finally, it is clear that any group which satisfies the minimum condition cannot contain an infinite direct sum of subgroups. □

7.4 Free abelian groups

Recall the definition of a free abelian group with base I as $\bigoplus_I \mathbb{Z}$. We call $|I|$ the *rank* of the group.

Theorem 7.25. *Every subgroup of $\bigoplus_I \mathbb{Z}$ is free of rank at most $|I|$.*

Proof. Let $F = \bigoplus_I \mathbb{Z}$ and take a well-ordering $\leq$ of I. For $x \in F$, define its *leading term* $l(x)$ as follows. If $x = n_1 b_1 + \ldots n_k b_k$, for $b_1, \ldots, b_k \in I$ and $n_1, \ldots, n_k \in \mathbb{Z} \setminus \{0\}$, assume without loss of generality that $b_1 \leq \cdots \leq b_k$, and define $l(x) = n_k b_k$. Let X be a subgroup of F. For each $b \in I$, define

$$X_b = \left\{ n \in \mathbb{Z} \setminus \{0\} : \text{ for some } x \in X, l(x) = n \right\} \cup \left\{ 0 \right\}.$$

Each X_b is a subgroup of $\mathbb{Z}$, so $X_b = \langle n_b \rangle$ for some $n_b \in \mathbb{Z}$. Choose a representative $x_b \in X$ such that $l(x_b) = n_b$. We claim that $\left\{ x_b : b \in I \right\}$ is a free generating set for X.

Clearly, the terms x_b are independent over $\mathbb{Z}$; no nontrivial finite linear combination $n_1 x_{b_1} + \cdots + n_k x_{b_k}$ is equal to 0. Suppose the set

$$S = \left\{ x \in X : x \notin \bigoplus_{b \in I} \mathbb{Z} x_b \right\}$$

is nonempty. Choose $x \in S$ whose leading term is $\preceq$-minimal. Write x as $x = y + n \cdot b$, where $l(x) = n \cdot b$. Since $\langle n_b \rangle = X_b$, we have that n_b divides n. The element $x - \frac{n}{n_b} \cdot x_b$ then yields a smaller counterexample, a contradiction.

Finally, it is clear that $\left| \{x_b\} \right| \leq |I|$. □

The Baer-Specker group

What about infinite direct products? For example, given any set I, consider the direct product $\prod_I \mathbb{Z}_2$. This has a natural structure as a $\mathbb{Z}_2$-vector space, so there exists a basis $B \subset \prod_I \mathbb{Z}_2$ such that $\prod_I \mathbb{Z}_2 = \bigoplus_B \mathbb{Z}_2$. That is, every direct product of $\mathbb{Z}_2$ is isomorphic to a direct sum. Does the same hold for $\mathbb{Z}$?

Of course, every finite direct product is a finite direct sum. Since every subgroup of a free abelian group is free, it suffices to consider $\prod_I \mathbb{Z}$ when I is countable. Call $B = \prod_I \mathbb{Z}$ the *Baer-Specker* group.

Theorem 7.26. $\mathrm{Hom}(B, \mathbb{Z})$ *is a free abelian group generated by the projections.*

Proof. For each $i \in I$, we have the projection $\pi_i : B \to \mathbb{Z}$ that sends $(a_j)_{j \in I} \to a_i$. Let $e_i \in B$ be the sequence such that $e_i(i) = 1$ and $e_i(j) = 0$ for all $j \neq i$.

Step (1)**.** There is no $\phi \in \mathrm{Hom}(B, \mathbb{Z})$ such that $\phi(e_i) \neq 0$ for all $i \in I$.

Suppose such a ϕ exists. Choose a sequence $(a_n)_{n \in \mathbb{N}} \subset \mathbb{Z} \setminus \{0\}$ such that a_{n-1} divides a_n, and $a_n > 2 \sum_{i<n} a_i \phi(e_i)$. Then, for each $N \in \mathbb{N}$,

$$\phi\Big((a_n)\Big) = \sum_{n<N} a_n \phi(e_n) + a_N \cdot \phi\Big((b_n)_{n \geq N}\Big)$$

for some nonzero sequence (b_n). So, for each $N \in \mathbb{N}$

$$\left|\phi\Big((a_n)\Big)\right| > \left|a_N / 2\right|$$

but this is not possible.

Step (2)**.** There is no $\phi \in \mathrm{Hom}(B, \mathbb{Z})$ which is nonzero for infinitely many e_i.

Let $S = \{e_i : \phi(e_i) \neq 0\}$. If $|S| = |I|$, any bijection $f : I \to S$ induces a homomorphism $B \to B$. Then, $\phi \circ f \in \mathrm{Hom}(B, \mathbb{Z})$ is nonzero for all e_i, contradicting step 1.

Step (3)**.** If $\phi(e_i) = 0$ for all i, then $\phi = 0$.

Let $(a_n)_{n \in \mathbb{N}} \in B$ be arbitrary. For each n, there exist $x_n, y_n \in \mathbb{Z}$ such that $a_n = 2^n x_n + 3^n y_n$. Then,

$$\phi\Big((2^n x_n)\Big) = 2^N \phi\Big((x_n)_{n \geq N}\Big)$$

for any $N \in \mathbb{N}$, so $\phi\Big((2^n x_n)\Big) = 0$. Similarly, $\phi\Big((3^n y_n)\Big) = 0$, so $\phi\Big((a_n)\Big) = 0$

Putting this all together,

Step (4)**.** The projections form a basis for $\mathrm{Hom}(B, \mathbb{Z})$.

□

Corollary 7.27. *The Baer-Specker group is not free.*

Proof. Some set theory tells us that $|B|$ is uncountable. Suppose $B \cong \bigoplus_S \mathbb{Z}$ for some set S. If S is countable, then $\bigoplus_S \mathbb{Z}$ is countable, so this is not possible. If S is uncountable, then for each $s \in S$, we have a projection $\pi_s : \bigoplus_S \mathbb{Z} \to \mathbb{Z}$. So, $\mathrm{Hom}(\bigoplus_S \mathbb{Z}, \mathbb{Z})$ is uncountable, but $\mathrm{Hom}(B, \mathbb{Z})$ is countable, again a contradiction. □

References

[1] Conrad, “The Schur-Zassenhaus Theorem”, available at https://kconrad.math.uconn.edu/blurbs/grouptheory/schurzass.pdf.

[2] Dixon and Mortimer. *Permutation Groups*.

[3] Dummit and Foote, *Abstract Algebra*.

[4] Fawcett, *The O’Nan-Scott Theorem for finite primitive permutation groups, and finite representability*.

[5] Isaacs, *Character Theory of Finite Groups*.

[6] Liebeck, Praeger, Saxl. “On the O’Nan-Scott theorem for finite primitive permutation groups”.

[7] Robinson, *A Course in the Theory of Groups*.

Index

k-cycle, transposition, 3
k-primitive, 31
k-transitivity, 29
p-group, 5
p-height, 62
p-measure, 62
(Hall) Π-subgroup, 26

abelian group, 2
affine transformation, 16
antipodal points, 60
automorphism, inner automorphism, 6

base of a primitive group, 31
blocks, G-invariant equivalence relation, 30
bounded Burnside problem, see $B(r,n)$, 63
Burnside problem, 61

center of a group, 6
central series, 25
centralizer and normalizer, 6
character of a representation, 43
character table, 46
characteristic subgroup, 5
characteristically simple group, 31
class function, 44
commutator, commutator subgroup, 6
completely reducible representation, 40
conjugate, conjugacy classes, 4
cycle type of a permutation, 56
cyclic group, 2

degree/dimension of a representation, 42
derived series, 23
directed system, direct limit, 65
distributive lattice, 66
divisible group, 65

elementary abelian p-group, 20
equivalent representations, 39
Examples of groups
  A_n, 3
  C_p^∞, 5
  D_n, 3
  S_n, $\mathrm{Sym}(n)$, 3
  V_4, 3
  $\mathbb{Z}_n$, 2
  $\mathbb{Z}_n^\times$, 3
  $AG(V), AGL(V)$, 17
  $B(r,n)$, 63
  $GL(V), SL(V), GL(d,F), SL(d,F)$, 3
  $PGL(V), PSL(V)$, 13
  $SO(3), O(3)$, 60
  $SU(2)$, 61
  U_n, 18
  Baer-Specker group, 68
exponent of a group, 63

faithful action, 7
faithful representation, 39
Frattini subgroup, 20
free abelian group, 65
free group, 9
Frobenius group, 33, 51
Frobenius kernel, 33, 51
Frobenius-Schur indicator, 55

group action, 7
group algebra, 41
group homomorphism, isomorphism, 4

Important results
  $PSL(d,F)$ is almost always simple, 13
  Baer-Specker group is not free, 68
  Bechert's bound, 31
  Bercov-Moser, 12
  Brauer-Fowler, 56
  Burnside's $p^a q^b$ theorem, 27, 49
  class equation, 12
  Clifford's theorem, 48
  first isomorphism theorem, 4
  first orthogonality relation for characters, 45
  Frattini's argument, 17, 22, 26
  Frobenius reciprocity, 47
  Fundamental theorem of finitely generated abelian groups, 5
  Hall's theorem(s), 26
  Iwasawa, see supersolvable group, 28
  Jordan, see primitive permutation group, 30
  Maschke's theorem, 41
  Nielsen-Schreier theorem, 9
  O'Nan-Scott, 36
  Ore's theorem, 66
  Schlage-Puchta, 63
  Schreier conjecture, 36
  Schur's lemma, 42
  Schur-Zassenhaus, 17

second isomorphism theorem, 5
second orthogonality relation for characters, 46
Sylow's theorems, 8
The orbit-stabilizer lemma, 7
third isomorphism theorem, 5
three subgroup lemma, 25
Wedderburn-Artin, 41
induced class function, induced representation, 47
inertia subgroup, 48
invariant subspace, 40
involution, 53
irreducible character, 43
irreducible representation, 40

join, meet, 66

kernel, 4

locally cyclic group, 66
lower central series, 24

M-group, 53
Maschke's theorem, 40
maximum condition, 67
minimum condition, 67

nilpotent group, 21
normal subgroup, 4
Notation
$G : H$, 2
$H \leq G$, 2
$N \lhd G$, 4
$[g, h], [G, G]$, 6
$\bigoplus_{i \in I} G_i, \prod_{i \in I} G_i$, 4
$\mathbb{C}G$, 41
$\mathbb{F}G$, 41
$\langle S \rangle$, 2
$\text{fix}(g)$, 11
ν^G, 47
$Aut(G), Inn(G)$, 6
$C_G(S), N_G(S)$, 6
$G \cong H$, 4
$H \text{char} G$, 5
$Irr(G)$, 46
$K \wr H$, 34
$V \otimes V$, 53
x^G, 12
$Z(G)$, 6

operator group, 16
orbit of a group action, 7

partition of the integer n, 56
permutation group, 7
polytabloid, Specht module, 57
primitive character, 53
primitive permutation group, 30

quotient group, 4

regular action, 8
regular representation, 39
representation of a group, 39
residually finite group, 11

semi-regular action, 7
semidirect product, 16
semisimple module, 41
setwise stabilizer, 30
simple group, 5
simple ring, 41
solvable group, 23
stabilizer of a group action, 7
standard representation of S_n, 58
subdirect product, 32
subgroup lattice, 28
supersolvable group, 28
Sylow p-subgroup, 8
symmetric and alternating characters, 54

tabloid, 57
torsion, torsion-free, 2
torsion-part, p-torsion, 67
transitive action, 7
transvection, 13
transversal, 9
trivial representatin, 39
twisted wreath product, 36

upper central series, 21

wreath product, 34

Young diagram, Young tableau, 56