Algebra | Math Notes • Study Guide

Group Theory

Table of Contents

1 Groups

1-1 Binary Operations

A **binary operation** on a set S is a rule for combining pairs a, b of S to get another element of S (S is **closed** under the operation), i.e. it defines a map $S \times S \to S$. Using multiplicative notation, the operation is…

1. **associative** if $(ab)c = a(bc)$.
   a. If the operation is associative then the product of any n elements (ordered) is well-defined without parentheses.
2. **commutative** if $ab = ba$.
3. Has an **identity** 1 if $1a = a, a1 = a$ for all a.
   a. An element a is invertible if there exists a^{-1} so that $aa^{-1} = 1 = a^{-1}a$.
   b. If a has a left and right inverse, they must be equal.
   c. An inverse is unique.
   d. Inverses multiply in opposite order: $(ab)^{-1} = b^{-1}a^{-1}$

Using additive notation, the identity is denoted by 0 and the inverse of a is denoted by $-a$. Exponents a^n become multiples na. All results will still be true whichever notation is used.
Ex. Composition of functions is associative.

1-2 Groups

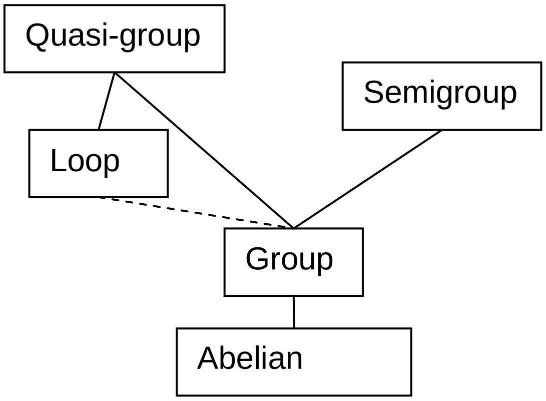
A **group** is a set G with an associative binary operation with identity such that every element is invertible. In an **abelian** group, the operation is commutative.

in other words…
Groups satisfy 1, 2, 3. Abelian groups also satisfy 4. A **semi-group** only needs to satisfy 1.

1. For every $a, b, c \in G, (ab)c = a(bc)$.
2. There exists an identity 1 so that $1a = a1 = a$ for all a.
3. Every element a has an inverse a^{-1} so that $aa^{-1} = a^{-1}a = 1$.
4. For every $a, b \in G$, $ab = ba$.

Note that the existence of right inverses and right identity element imply the existence of the left inverses and left identities (which must be the same).

In a **quasi-group**, if $ab = c$, then any two of a, b, c determine the third uniquely. A **loop** is a quasi-group with identity.



Cancellation Law: In a group, $ab = ac$ or $ba = ca$ implies $b = c$.

A **subgroup** of a group G is a group H in G, with the same binary operation. In other words,

1. Closure: $a, b \in H \Rightarrow ab \in H$
2. Identity: $1 \in H$
3. Inverse: $a \in H \Rightarrow a^{-1} \in H$.

A proper subgroup is not G or {1} (the trivial subgroup).
The subgroup $\langle S \rangle$ generated by a set $S \subseteq G$ is the minimal subgroup in G containing S, i.e. the subgroup of all combinations of the elements in S and their inverses.
The intersection of 2 subgroups is a subgroup; the **join** $H \vee K = \langle H, K \rangle$ of subgroups H, K is the minimal subgroup containing both of them.
Ex. All subgroups of the additive group of integers $\mathbb{Z}^+$ are in the form

$$a\mathbb{Z} = \{an | n \in \mathbb{Z}\}$$

for some integer a.[1]

The **order** of a group G, denoted by $|G|$ is the number of elements in G.

1-3 Examples of Groups

Groups	Description	Binary operation
$\mathbb{Z}^+, \mathbb{Q}^+, \mathbb{R}^+, \mathbb{C}^+$	Integers, rational numbers, real numbers, and complex numbers[2]	Addition
$\mathbb{R}^\times, \mathbb{C}^\times$	Nonzero real and complex numbers	Multiplication
$\mathbf{T}, \mathbb{R}/\mathbb{Z}$	The circle group: complex numbers of absolute value 1 Real numbers modulo 1	Multiplication Addition
$C_n, \mathbb{Z}_n, \mathbb{Z}/(n)$ $\mathbb{Z}/n\mathbb{Z}$	**Cyclic group** of order n. It can be represented by the integers modulo n, the rotational symmetries of a n-gon, or the nth roots of unity.	Multiplication Addition Composition Multiplication
$\mathbb{Z}(p^\infty)$	**Quasicyclic group**, p prime. Represented by the rational numbers with a power of p in the denominator, modulo 1, or the complex numbers z with $z^{p^k} = 1$ for some $k \in \mathbb{N}$.	Addition Multiplication
D_n	**Dihedral group** of order $2n$. Symmetries of a n-gon.	Composition
S_n	**Permutation group** on n elements: all permutations of $\{1,2,\dots,n\}$. S_X or $\mathrm{Perm}(X)$ denotes the permutations of set X.	Composition
A_n	**Alternating group** of order n: Permutations with sign $+1$, or even permutations.	Composition
H	**Quaternion group**: $\{\pm I, \pm\mathbf{i}, \pm\mathbf{j}, \pm\mathbf{k}\}$, where $I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \mathbf{i} = \begin{bmatrix} i & 0 \\ 0 & -i \end{bmatrix}, \mathbf{j} = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}, \mathbf{k} = \begin{bmatrix} 0 & i \\ i & 0 \end{bmatrix}$ $i^2 = j^2 = k^2 = -I, ij = -ji = k$ $jk = -kj = i, ki = -ik = j$	Multiplication
$\mathrm{GL}_n(F)$	**General linear group**: $n \times n$ invertible matrices over the field F.	Matrix multiplication

[1] This is simple number theory. For a comprehensive development, see Abstract Algebra [section number].
[2] $\mathbb{Z}^+, \mathbb{Q}^+, \mathbb{R}^+$ may also stand for "the positive --- numbers." The additive groups may be written $\mathbb{Z}_+, \mathbb{Q}_+, \mathbb{R}_+$ to avoid confusion (through this is less common).

Permutations:
A permutation on a set X is a bijective map from a set to itself. A permutation π can be written as a composition of cycles, a cycle written as $(a_1 a_2 \dots a_k)$: $\pi(a_1) = a_2, \pi(a_2) = a_3, \dots, \pi(a_k) = a_1$.
A permutation has sign $+1$ (-1) and is even (odd) if any of the equivalent are true:

1. The associated matrix (with 1s at $(\pi(i), i)$ and 0s elsewhere) has determinant $+1$ (-1).
2. It can be written as the product of an even (odd) number of transpositions. A transposition is a permutation switching 1 pair of elements and leaving everything else fixed. Note that a cycle of k elements can be written as a product of $n-1$ transpositions.
3. It has an even number of inversions, pairs $i < j$ with $\pi(i) > \pi(j)$.

Ex. S_3 has order $3! = 6$ and is generated by $x = (123), y = (12)$ with the relations $x^3 = 1, y^2 = 1, yx = x^2 y$.

1-4 Cyclic Groups

The **order** of an element x is the least positive integer n such that $x^n = 1$. (If no such n exists, x has infinite order.) The (minimal) **exponent** of a group G is (the smallest) n such that $x^n = 1$ for all $x \in G$.

A **cyclic** group $\langle x \rangle$ is generated by one element x. Its order is the same as the order of the element.
Let S be the set of all integers k such that $x^k = 1$. If the powers of x are not all different, then x has finite order n, and

1. $S = n\mathbb{Z}$, the multiples of n.
2. $x^r = x^s$ iff $r - s$ is a multiple of n.
3. $1, x, \dots, x^{n-1}$ are the distinct elements in $\langle x \rangle$.

1-5 Homomorphisms and Normal Subgroups

A **homomorphism** from a group G to a group G' is a function φ such that for all $a, b \in G$, $\varphi(ab) = \varphi(a)\varphi(b)$. As a consequence, $\varphi(1_G) = 1_{G'}$ and $\varphi(a^{-1}) = \varphi(a)^{-1}$. A homomorphism is an **isomorphism** if it is bijective: then it has an inverse function that is also a homomorphism. An **endomorphism/ automorphism** is an homomorphism/ isomorphism from a group to itself. Two groups are isomorphic ($G \cong G'$) if there is an isomorphism between them.
Below, $\varphi: G \to G'$ is a homomorphism.

- The **image** of φ is the subset of G'
$$\operatorname{im} \varphi = \{x \in G' | x = \varphi(a) \text{ for some } a \text{ in } G\}.$$
- The **kernel** of φ is the set of elements in G mapped to the identity:
$$\ker \varphi = \{a \in G | \varphi(a) = 1\}$$

Ex. A_n is the kernel of the sign homomorphism $\sigma: S_n \to \{\pm 1\}$.

The **conjugate** of an element $h \in G$ by $g \in G$ is $h^g = ghg^{-1}$. The conjugate of a subgroup H by g is $H^g = gHg^{-1}$. Since conjugation is a (injective) homomorphism gHg^{-1} is a subgroup of G as well.

- If $gHg^{-1} \subseteq H$ for all $g \in G$, then H is **normal** in G, written $H \lhd G$. (By counting elements, equality holds when H is finite, but not necessarily when H is infinite.)

- If $\varphi(H) = H$ for all automorphisms of G, then H is **characteristic** in G, written $H \text{ char } G$.
- If $\varphi(H) = H$ for all endomorphisms of F, then H is a **fully invariant** subgroup of G.

Basic relations

- $H \text{ char } K, K \text{ char } G \Rightarrow H \text{ char } G$
- $H \text{ char } K, K \lhd G \Rightarrow H \lhd G$

The image is a subgroup of $G^{'}$ and the kernel is a *normal* subgroup of G.

1-6 Cosets and Quotient Groups

A left/ right **coset** of a subgroup H is a set of the form

$$aH = \{ah | h \in H\}$$
$$Ha = \{ha | h \in H\}$$

respectively, for some $a \in G$. The distinct cosets partition G.

- $aH = bH$ iff $ab^{-1} \in H$.
- There are as many left as right cosets.

The **index** of H in G, denoted by $[G: H]$, is the number of cosets of H in G.

Counting Formula: (Lagrange's Theorem) Let H be a subgroup of G.

- $|G| = [G: H]|H|$ since each coset has $|H|$ elements.
- $|H|$ divides $|G|$, and the order of any element divides $|G|$.
- $[G: K] = [G: H][H: K]$, for K a subgroup of H.

Ex. Any group of prime order is cyclic.

Ex. The elements in $\mathbb{Z}_n$ relatively prime to n form a group under multiplication. The order of an element divides the order of the group, $\varphi(n)$. For n a prime, the order divides $n - 1$. The existence of a primitive element shows the group is cyclic.

When H is normal, $aH = Ha$ for all a and the cosets form the **quotient group** $\bar{G} = G/H$ with multiplication defined by

$$(aH)(bH) = abH.$$

The canonical map $\pi: G \to \bar{G}$ sending $a \rightsquigarrow aH$ is a surjective homomorphism with kernel H.

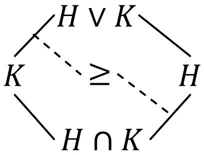
Let $\varphi: G \to G'$ be a homomorphism. φ determines an equivalence relation, with $a \equiv b$ iff $\varphi(a) = \varphi(b)$. This gives a partition of G into **fibers** of the map φ, where each fiber contains all the elements mapped to a single value. The fibers are the cosets of $\ker \varphi$ in G. The number of cosets is the number of elements in $\operatorname{im} \varphi$.

- $|G| = |\ker \varphi||\operatorname{im} \varphi|$
- $|\ker \varphi|$ divides $|G|$.
- $|\operatorname{im} \varphi|$ divides both $|G|$ and $|G^{'}|$.

Ex. A_n contains half of the elements of S_n for $n > 1$.

Index inequalities

- $[H: H \cap K] \le [H \vee K: K]$ with equality iff $HK = H \vee K$.
- $[H \vee K: H \cap K] \le [H \vee K: H][H \vee K: K]$ with equality iff $HK = H \vee K$.



For $A, B \subseteq G$, G is a union of disjoint double cosets of the form $AxB = \{axb | a \in A, b \in B\}$. The order of a double coset is $|AxB| = |A|[B: xAx^{-1} \cap B]$.

1-7

Isomorphism Theorems

Correspondence Theorem: Let $\varphi: G \to G'$ be a surjective homomorphism with kernel K.

- There is a bijective correspondence between subgroups of G' and subgroups of G that contain K. A subgroup of G containing K is associated with its image.

$$\begin{tikzcd}
G \arrow[r, "\varphi"'] \arrow[d, dash] & G^{'} \cong G/K \arrow[d, dash] \\
H \arrow[r] \arrow[d, dash] & H' \cong H/K \arrow[d, dash] \\
K \arrow[r] & 1
\end{tikzcd}$$

- If H, H' are corresponding subgroups, H is normal in G iff H' is normal in G'.
- $|H| = |H^{'}||K|$

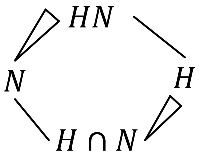
First Isomorphism Theorem: Let $\varphi: G \to G'$ be a homomorphism with kernel K.

- The quotient group $\bar{G} = G/K$ is isomorphic to the image G'.
- (Mapping property) Let $\pi: G \to \bar{G}$ be the canonical map. There is a unique homomorphism $\bar{\varphi}: \bar{G} \to G'$ such that $\varphi = \bar{\varphi} \circ \pi$.

$$\begin{tikzcd}
\bar{G} \arrow[dr, dashed, "\bar{\varphi}"] & \\
G \arrow[u, "\pi"] \arrow[r, "\varphi"] & G'
\end{tikzcd}$$

Second Isomorphism Theorem: (Diamond Theorem) Let G be a group. Let H be a subgroup, and N a normal subgroup. Then

- The product $HN = \{hn | h \in H, n \in N\}$ is a subgroup of G.
- $H \cap N$ is a normal subgroup of H.
- $HN/N \cong H/H \cap N$



Third Isomorphism Theorem: Let G be a group, and N and K be normal subgroups of G with $K \subseteq N \subseteq G$. Then

- $N/K \lhd G/K$
- $(G/K)/(N/K) \cong G/N$

1-8 Product Groups

The product group $G \times G'$ is the group consisting of the elements $(g, g^{'}), g \in G, g^{'} \in G'$, with coordinatewise multiplication $(a, a^{'})(b, b^{'}) = (ab, a^{'}b^{'})$. The inclusion homomorphisms $G, G' \rightarrow G \times G'$ are defined by $i(a) = (a, 1), i'(b) = (1, b)$ and the projection homomorphisms $G \times G' \rightarrow G, G'$ are defined by $p(a, a') = a, p^{'}(a, a^{'}) = a'$.
$V = C_2 \times C_2$ is called the Klein four group.

Let H, K be subgroups of subgroups of G, and let $f\colon H \times K \rightarrow G$ be the multiplication map $f(h, k) = hk$.

1. f is injective iff $H \cap K = \{1\}$.
2. f is a homomorphism iff elements of K commute with elements of H: $hk = kh$.
3. f is an isomorphism ($G \cong H \times K$) iff $H \cap K = \{1\}$, $HK = G$, and H, K are normal subgroups.

The **direct product** (a.k.a. unrestricted direct product) of groups $G_i, i \in I$ is the group where each element is an indexed set with 1 member from each group G_i, with coordinatewise multiplication. The **direct sum** (a.k.a. restricted direct product) is the subgroup of the direct product containing only those elements with a finite number of non-identity elements. The definitions coincide when there are finitely many factors.

2 Finite Groups

2-1 Permutations and G-sets

Cayley's Theorem: Every group is isomorphic to a subgroup of a permutation group.
Pf. Define $\varphi: G \to \mathrm{Perm}(G)$ (set of permutations of G) by associating $g \in G$ with the permutation of G induced by left multiplication by g.

A **group operation** of G on a set S is a map $G \times S \to S$ such that:

1. $1s = s$ for all $s \in S$.
2. $(gh)s = g(hs)$ for all $g, h \in G, s \in S$.

S is called a G-set. (G may act on the right instead.)

Multiplication by an element of G defines a permutation of the elements of S (they are permutations since $g^{-1}(gs) = s$). This gives a permutation representation of S, a map $G \to \mathrm{Perm}(S)$.

The **orbit** of $s \in S$ is the set of elements in S that s can be sent to by elements in G:

$$O_s = \{s' | s' = gs \text{ for some } g \in G\}$$

The orbits partition the set S. The operation is **transitive** if the orbit is the whole group (then any element can get sent to any other element).

The **stabilizer** of is the subgroup of elements of G that leave s fixed:

$$G_s = \{g \in G | gs = s\}$$

Note $|G| = |G_s||O_s|$ since for each $s' \in O_s$, there are $|G_s|$ elements g such that $s' = gs$.

Ex. 1: G acts transitively on the set of left cosets of a subgroup H (even when H is not normal) by defining $a(bH) = (ab)H$. The stabilizer of the coset H is the subgroup H.

Ex. 2: G acts on itself by conjugation: $g * x = gxg^{-1}$. The stabilizer of an element x under conjugation is the **centralizer**:

$$Z_G(x) = \{g \in G | gxg^{-1} = x\} = \{g \in G | gx = xg\}$$

The centralizer contains and the center Z. The orbit of x under conjugation is the conjugacy class of x:

$$C(x) = \{gxg^{-1} | g \in G\}$$

The conjugacy classes partition the group G.

Ex. 3: G acts on the set of subgroups of G by conjugation: $g * H = gHg^{-1}$. The stabilizer of a subgroup is the **normalizer**:

$$N_G(H) = \{g \in G | gHg^{-1} = H\}$$

The orbit of H is the set of subgroups conjugate to H. The elements of G leaving each element of H fixed is the centralizer:

$$C_G(H) = \{g \in G | ghg^{-1} = h \text{ for all } h \in H\}$$

2-2

Combinatorial Equations

Variations of the Same Concept

	Set of g so that g*h=h (g*H=H)	Set of g*h (g*H) possible	Equation
Left multiplication of G on subgroup H	H	Cosets	Counting formula (Lagrange's Theorem) $|G| = |H|[G:H]$
Homomorphism φ operating on gh with $g, h \in G$.	$(\varphi(gh) = \varphi(h))$ Kernel	(Set of $\varphi(gh)$) Image	$|G| = |\ker\varphi||\mathrm{im}\,\varphi|$
Group operation (G) on elements h	Stabilizer	Orbit	$|G| = |G_h||O_h|$ Orbit equation $|G| = \sum_{\text{orbit } O} |O|$
Conjugation of elements $h \in G$	Centralizer	Conjugacy class	$|G| = |Z(h)||C(h)|$ Class equation $|G| = \sum_{\text{conjugacy class } C} |C|$
Conjugation of subgroup $H \subseteq G$	Normalizer	Conjugates of H	$|G| = |N(H)|[G:N(H)]$

2-3

p-Sylow Subgroups

For p prime, a (finite) **p-group** is a group whose order is a power of p.

- The center of a nontrivial p-group is not trivial. (In the class equation, each term is a power of p. More than one term must be 1; these correspond to elements whose stabilizer is the whole group, i.e. in the center.)
- (Fixed Point Theorem) Let G operate on S. If the order of S is not divisible by p, there is a fixed point for the operation of G on S.

For G a finite group, if p is prime, $|G| = p^e m$, and H is a subgroup of order p^e, then H is a **p-Sylow subgroup** (p-SSG) of G.

Sylow Theorems:

1. G contains a p-SSG for all primes p.
    a. Let G act on the set S of *subsets* of order p^e by conjugation. There are $\binom{n}{p^e}$ such subsets. Writing the orbit equation for S, since $p \nmid \binom{n}{p^e}$, one orbit O has order not divisible by p. The stabilizer of a set U in O has order dividing $|U| = p^e$ (since U is partitioned into cosets of $\mathrm{Stab}(U)$) so must be a p-SSG.
2. Any two p-SSG are conjugate in G, and any subgroup of G which is a p-group is contained in some p-SSG.
    a. Given: p-subgroup K, p-SSG H. Let K operate by left multiplication on the set of cosets of H. There is a fixed point gH for this operation. The stabilizer is gHg^{-1}, which contains K.
3. If n_p is the number of p-SSGs then $n_p \equiv 1 \pmod{p}$ and divides the order of G.
    a. Let H operate on the set S of p-SSGs by conjugation. Each orbit has size a power of p, and is divisible by p unless it is a fixed point. If $H' \neq H$ is a fixed

point, they are both in N(H'), and conjugate in N(H') by (2), contradicting $H' \lhd N(H')$.

The Sylow Theorems are useful in determining all groups of a certain order. (3) can be used to show a group of a certain order is not simple: if there is only 1 p-SSG then it must be normal.

Let P be a p-SSG in G, and let H be a subgroup so that $N_G(P) \subseteq H \subseteq G$. Then H is its own normalizer.

<u>Frattini Argument:</u> Let K be a normal subgroup of a finite group G. If P is a p-SSG, then $G = KN_G(P)$.

If each p-SSG in G is normal in G, then G is the direct product of its p-groups.

Exercises

1. Show that every group of order p^2 is abelian, and hence is C_p or C_{p^2}.
2. Let $n \geq 5$. Given that the only proper normal subgroup of S_n is A_n, show that the only proper subgroup of index less than n in S_n is A_n.
3. Let G be a group generated by k elements. There are at most $n!^k$ normal subgroups with index at most n.
4. Let G be a finite group and let p be the smallest prime which divides |G|. If H is a subgroup of G such that [G:H]=p, prove that H is normal in G.
5. Suppose that a finite group has exactly n elements of order p, where p is a prime. Prove that either n=0 or p divides n+1.
    a. Remark: The following theorem is due to Frobenius: Suppose $|G| = g$ and let C be a class of h conjugate elements. The number of solutions to $x^n = c, c \in C$ is a multiple of $\gcd(hn, g)$.
6. Let G be a group of order 4n+2. Prove that G is not a simple group.

3 Automorphisms

3-1 Inner and Outer Automorphisms

The automorphism group Aut(G) is the group of automorphisms of G under composition. An automorphism is **inner** if it is conjugation by some element of G; else it is **outer**. The group of inner automorphisms is Inn(G); Aut(G)/Inn(G) is the outer automorphism group.

Basic Theorems:
<u>N/C Lemma:</u> If $H \subseteq G$ then $C_G(H) \lhd N_G(H)$ and $N_G(H)/C_G(H)$ can be embedded in Aut(H).
$\mathrm{Inn}(G) \lhd \mathrm{Aut}(G)$ and $G/Z(G) \cong \mathrm{Inn}(G)$.
<u>Pf.</u> $C_G(H)$ is the kernel of the group of the restrictions of inner automorphisms (conjugation by an element in $N_G(H)$) to H.

Ex. If G is an elementary abelian group of order p^n then $\mathrm{Aut}(G) \cong GL_n(\mathbb{F}_p)$.
$\mathrm{Aut}(\mathbb{Z}) \cong C_2$.
$\mathrm{Aut}(G) = 1$ iff $|G| \leq 2$.
$\mathrm{Aut}(C_n) \cong U(\mathbb{Z}_n)$ where U(R) is the group of invertible elements (units) of the ring R. The group has $\varphi(n)$ elements.

- $\mathrm{Aut}(\mathbb{Z}_2) = \{1\}, \mathrm{Aut}(\mathbb{Z}_4) \cong \mathbb{Z}_2, \mathrm{Aut}(\mathbb{Z}_{2^m}) \cong \mathbb{Z}_2 \times \mathbb{Z}_{2^{m-2}}$. (5 has order 2^{n-2})
- For an odd prime p, $\mathrm{Aut}(\mathbb{Z}_{p^m}) \cong \mathbb{Z}_{(p-1)p^{m-1}}$ by primitive roots.
- If $n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$, then $\mathrm{Aut}(\mathbb{Z}_n) \cong \prod_{i=1}^{k} \mathrm{Aut}(\mathbb{Z}_{p_i^{\alpha_i}})$.

3-2 Complete Groups

A group is **complete** if it is centerless and every automorphism is inner. Then $G \cong \mathrm{Aut}(G)$.

S_n is complete iff $n \neq 2,6$.
<u>Pf.</u> An automorphism φ preserves transpositions iff φ is inner. Let T_k be the conjugacy class of k disjoint transpositions. φ sends T_1 to some T_k. When $n \neq 2,6$, then by counting, $|T_1| \neq |T_k|, k \neq 1$, so it sends T_1 to itself.
For n=6: S_5 operates by conjugation on its 6 5-SSGs (5-cycles). The image of the permutation representation (which is an isomorphism, because the kernel is a normal subgroup and hence {1}) is a transitive subgroup K of 120 elements in S_6. Now let S_6 operate on the cosets of K. The permutation representation is a bijection (and can be viewed as an automorphism). It can't preserve the cycle structure of (1 2).
<u>Cor.</u> Every outer automorphism of S_6 switches T_1, T_3 so $\mathrm{Aut}(S_6)/\mathrm{Inn}(S_6) \cong C_2$ and $|\mathrm{Aut}(S_6)| = 1440$.
<u>Cor.</u> Every finite group imbeds in a complete group. (Actually true for all groups)

Describing outer automorphisms of S_6:
A **syntheme** is a product of 3 disjoint transpositions; a **pentad** is a family of 5 synthemes, no two having a common transposition. Two synthemes have a common transposition iff they commute. S_6 has 6 pentads. An outer automorphism sends each transposition into a syntheme. There are 6 choices of pentads; then 5! choices for how to send {(1 2),…,(1 6)} to the synthemes in a pentad; this accounts for all 720 of them.

If G is a nonabelian simple group, then Aut(G) is complete.

	Pf. Let γ_g be conjugation by g in G and Γ_α be conjugation by α in Aut(G). Since G is simple and nonabelian, $G \cong \mathrm{Inn}(G) = I$. A=Aut(G) is centerless- only {1} commutes with every inner automorphism. For any $\sigma \in A$, the subgroup generated by commutators $[I, \sigma(I)] \in I \cap \sigma(I)$ and must be I (since I is simple). Then $\sigma(I) = I$ so $\sigma(\gamma_g) = \gamma_{\alpha(g)}$ for some automorphism α. Then $\tau = \sigma\Gamma_\alpha^{-1}$ is the identity map (check that $\tau(\beta)\beta^{-1} \in C_A(I) = \{1\}$) so $\sigma = \Gamma_\alpha$.
3-3	Holomorph Suppose G is mapped to $L(G) \subseteq S(G)$ under the left multiplication permutation representation and $R(G)$ under the right multiplication permutation. The **holomorph** $\mathrm{Hol}(G)$ is defined by $$\mathrm{Hol}(G) = \langle L(G), \mathrm{Aut}(G)\rangle$$ Equivalently, Hol(G) is the normalizer of the subgroup $L(G) \subseteq S(G)$. ***All automorphisms of G are induced by inner automorphisms of Hol(G).*** Properties: 1. $L(K) \lhd \mathrm{Hol}(K), L(K)\,\mathrm{Aut}(K) = \mathrm{Hol}(K), L(K) \cap \mathrm{Aut}(K) = \{1\}$ 2. $\mathrm{Hol}(K)/L(K) \cong \mathrm{Aut}(K)$ The subgroup of $\mathrm{Hol}(K)$ fixing 1 is $\mathrm{Aut}(K)$. 3. $Z_{\mathrm{Hol}(K)}(L(K)) = R(K)$ 4. Everything works if K^l and K^r are switched; left and right multiplication are switched. If $K \lhd G$ and K is complete, then K is a direct factor of G: there exists a normal subgroup Q of G so that $G = K \times Q$. Conversely, if K is a direct factor whenever it is (isomorphic to) a normal subgroup of a group, then K is complete. *Pf.* Take $Q = C_G(K)$. For the converse, identify K with K^l; $\mathrm{Hol}(K) = K^l \times B$ for some B. If $\varphi \in Aut(K)$ then $\varphi = \gamma_a$ for some a. Show $K^r \cap K^l = Z(K), K \cong B \times Z(K)$. If φ is an automorphism of Z(K) then we get an outer automorphism of K. So $\lvert Z(K)\rvert \leq 2$. If it's 2, embed $B \times N \subset B \times \mathbb{Z}_4$, contradiction. So $Z(K) = \{1\}$.

4 Symmetry

4-1 Symmetry

An **isometry** is a rigid motion in $\mathbb{R}^n$, i.e. a distance-preserving map. Every isometry can be uniquely written as the composition of a translation by some vector a and an orthogonal linear operator φ:

$$f = t_a\varphi$$

The set of isometries forms a group M_n.

Change of coordinates: If η changes coordinates, and the formula for the old and new coordinates are m and m', then

$$m^{'} = \eta^{-1}m\eta$$

A **symmetry** of a figure, pattern, or set of points F is an isometry that carries F to itself. The symmetries of F form a group. A symmetry f=$t_a\varphi$ preserves **orientation** if the $\det(\varphi) = 1$.

<u>Fixed Point Theorem:</u> Let G be a finite group of isometries. Then there is a point in the plane fixed by every element of G.
<u>Pf.</u> The centroid of the orbits of any point is sent to itself.

4-2 2-D Symmetry Groups

Isometries of the plane:

Type	Action	Orientation-preserving?
Translation	$t_v: p \to p + v$	Yes
Rotation	Rotate θ about some point ρ_θ = reflection around origin	Yes
Reflection	Reflect across some line l. r = reflection across x-axis	No
Glide symmetry	Reflection across line l, then translation by nonzero vector parallel to l.	No

Rules:

1. $t_v t_w = t_{v+w}$, $\rho_\theta\rho_\phi = \rho_{\theta+\phi}$, $rr = 1$
2. $\rho_\theta t_v = t_{v'}\rho_\theta, v^{'} = \rho_\theta(v)$
3. $rt_v = t_{v'}r, v^{'} = r(v)$
4. $r\rho_\theta = \rho_{-\theta}r$

A **discrete** group does not contain arbitrarily small nonzero rotations and translations, i.e. there exist $\epsilon > 0$ so

1. If translation by $a \neq 0$ is in G, then $|a| > \epsilon$.
2. If rotation by $\theta \neq 0$ around some point is in G, then $|\theta| > 0$.

In a discrete subgroup of $\mathbb{R}^2$, all nonzero vectors have length $|v| > \epsilon$. There is a vector of minimum length.

Tools for analyzing discrete symmetry groups G:

1. The **translation group** L is the set of vectors v such that $t_v \in G$. (Note that the elements are not linear operators.) Every discrete group in $\mathbb{R}^2$ is in the form:
    a. $\{0\}$
    b. $\mathbb{Z}a, a \neq 0$, or
    c. $\mathbb{Z}a + \mathbb{Z}b$, $\{a, b\}$ linearly independent. (A **lattice**.)
2. Define the homomorphism $\pi: M_n \to O_n$ by dropping the translation part of an isometry: $\pi(t_a\varphi) = \varphi$. The **point group** is $\text{im}(\pi|_G)$.
    a. A discrete point group can be…
        i. C_n, the **cyclic group** of order n generated by ρ_θ, $\theta = \frac{2\pi}{n}$.
        ii. D_n, the **dihedral group** of order $2n$ generated by ρ_θ and r.
    b. <u>Crystallographic Restriction</u>: The point group of the symmetries of a discrete subgroup in $\mathbb{R}^2$ is C_n or D_n for $n = 1,2,3,4,$ or 6. (Proof uses that there is a vector of minimal length.)
3. If $a \in L, \bar{g} \in \bar{G}$, then $\bar{g}(a) \in L$.

Discrete symmetry groups ($\mathbb{R}^2$):
1. $L = \{0\}$: C_n or D_n.
2. $L = \mathbb{Z}a$: **frieze pattern** (7 groups)
3. $L = \mathbb{Z}a + \mathbb{Z}b$: **two-dimensional crystallographic group** (17 groups)

4-3

3-D Symmetry Groups

Finite subgroups of the rotation group SO_3:

Group	Name and Description	Isomorphic to…	Class equation	Order
C_n	Cyclic group		$n = 1 + \cdots + 1$	n
D_n	Dihedral group		$2n = 1 + \cdots + 1 + n$	2n
T	Tetrahedral group: Rotational symmetries of a tetrahedron	A_4	$12 = 1 + 3 + 4 + 4$	12
O	Octahedral group: Rotational symmetries of a cube or octahedron			24
I	Icosahedral group: Rotational symmetries of dodecahedron or icosahedron.	A_5	$60 = 1 + 12 + 12 + 15 + 20$	60

Analyze using orbits of **poles**, unit vectors that are the axis of rotation for some element in the group. (From linear algebra, all orthogonal operators in $\mathbb{R}^3$ are rotations.)
230 three-dimensional crystallographic groups, classified into 7 crystal systems, 32 crystallographic point groups.

5 Permutation Groups

5-1 Symmetric Group

Two permutations in S_n are conjugate iff the cycles in their cycle decompositions have the same lengths. $\pi\sigma\pi^{-1}$ has the same cycle decomposition as σ, but with each i replaced by $\pi(i)$.

A_n is simple for $n \geq 5$.
Pf. The class equation of A_5 is 60=1+12+12 (2 classes with 5-cycles) +15 (Disjoint 2-cycles) +20 (3-cycles). A normal subgroup must be a union of conjugacy classes and have order dividing 60. Induct for $n > 5$ using the simplicity criteria in 5-3.

5-2 Transitive Groups

A G-set X with action φ is **faithful** if $\varphi: G \to S_X$ is injective. If G has faithful action, G can be called a permutation group. $|X|$ is the **degree** of the G-set.

The pointwise stabilizer is $G_{(x_1,\dots,x_n)} = \{g \in G | gx_i = x_i \forall i\}$ (order matters) and the setwise stabilizer is $G_Y = \{g \in G | g(Y) = Y\}$ where $Y = \{x_1, \dots, x_k\}$.

X is **transitive** if for every $x, y \in X$ there exists $g \in G$ so that $y = gx$. Every G-set can be partitioned into transitive G-sets. X is **k-transitive** if for every pair $(x_1, \dots, x_k), (y_1, \dots, y_k)$ of k-tuples having distinct entries in X, there exists $g \in G$ so that $gx_i = y_i$ for each i. For $k \geq 2$, X is k-transitive iff for every $x \in X$, $X - \{x\}$ is (k-1)-transitive. X is **sharply k-transitive** if only the identity fixes k distinct elements of X.[3] A sharply 1-transitive G-set is **regular**. G is a regular G-set, for any group G.

If X is transitive, then $H = \{g \in G | g \text{ fixes } s\}$ is a subgroup of G, and the elements of X can be put into 1-to-1 correspondence with the left cosets of H so that G acts the same way on X as on the left cosets.
The $g \in G$ that fix every element forms the largest normal subgroup of G in H.

If $tx = y, t \in G$ then $G_y = G_{tx} = tG_xt^{-1}$, and X has the same number of G_x-orbits as G_y-orbits. The **rank** of X is the number of G_x orbits in X, also equal to the number of G_xgG_x double cosets in G.
Every doubly transitive G-set has rank 2.

If X is k-transitive of degree n, then for every k distinct elements $(x_1, \dots, x_k)$,

$$|G| = n^{\underline{k}}|G_{(x_1,\dots,x_k)}|$$

If X is faithful, $|G_{(x_1,\dots,x_k)}|$ divides $(n-k)!$ If X is a sharply k-transitive, $|G| = n^{\underline{k}}$.

The **Frobenius kernel** N of G is the subset

$$N = \{1\} \cup \{g \in G | g \text{ has no fixed points}\}$$

If X is a faithful transitive G-set with each $g \in G - \{1\}$ having at most one fixed point and $\{1\} \subset N$, then G is a **Frobenius group**. A group G is a Frobenius group iff it has a Frobenius complement, a proper subgroup such that $H \cap gHg^{-1} = \{1\}$ for all $g \in H$. If there

[3] These adjectives also apply to groups. We say a group G is [adjective] if there exists a [adjective] G-set.

exists a faithful sharply 2-transitive G-set, then G is a Frobenius group.

Frobenius's Theorem: The Frobenius kernel of a Frobenius group is a normal nilpotent subgroup. (Part of proof in 12-4)

Example. Suppose X is a faithful sharply 2-transitive G-set of degree n.

1. $|N| = n$
2. If n is odd, then n is a prime power, N is an elementary abelian normal subgroup, and $G = N \rtimes G_x$.

Simplicity Criteria: Let X be a faithful k-transitive G-set, and suppose G_x is simple for some $x \in X$.

1. If $k \geq 4$, then G is simple.
2. If $k \geq 3$ and $|X|$ is a power of 2, then $G \cong S_3$ or G is simple.
3. If $k \geq 2$ and $|X|$ is not a prime power, then G is simple.

Application: Constructing larger simple groups (G) from smaller ones (G_x). A **transitive extension** of a permutation group on G is a transitive permutation group $\tilde{G}$ on $\tilde{X} = X \cup \{\infty\}$, where ∞ is an element not in G, so that $\tilde{G}_\infty = G$.

5-3 Primitive Groups

A **block** is a subset B of X such that for every $g \in G$, either $gB = B$ or $gB \cap B = \phi$. $\phi, X, \{x\}$ are trivial blocks. A transitive G-set is **primitive** if it contains no nontrivial blocks.

The $\frac{|G|}{|B|}$ distinct sets among $gB, g \in G$ form a partition of G. $Y = \{gB\}$ is a transitive G-set, the imprimitive system generated by B.

A transitive G-set is primitive iff for each $x \in X$, G_x is a maximal subgroup.
Pf. If $G_x \subset H \subset G$ then Hx is a nontrivial block.

(In other words, there are no nontrivial G-invariant equivalence relation, i.e. relations with $x \equiv y \Rightarrow gx \equiv gy$. Every doubly transitive G-set X is primitive.)

Jordan's Theorem: If G is a primitive subgroup of S_n and H is a nontrivial subgroup fixing m points and primitive in its action on the remaining $n - m$ points, then G is $(m + 1)$-fold transitive. In particular, if G contains a 3-cycle, then $G = S_n$ or A_n; if G contains a transposition, $G = S_n$. If H is not primitive, we can still conclude G is doubly transitive.
Pf. (1st part) Take a conjugate subgroup H' of H (distinct from H) that has the most non-fixed points in common with H; if it doesn't share all but 1 point, then conjugating H by a certain element in H' gives a subgroup with more non-fixed elements in common. $H \cup H'$ is doubly transitive. Repeat the construction with $H \cup H'$, adding 1 more element each time until you get to G.

A **perfect** group satisfies $G^{'} = G$. If G is a perfect group and X is a faithful primitive G-set, then there is $x \in X$ and an abelian normal subgroup $K \lhd G_x$ whose conjugates generate G, then G is simple.
Application: Proof of simplicity of PSL's.

5-4 Steiner Systems; Affine and Projective Spaces

Affine Geometry

The **affine group** $\mathrm{Aff}(V)$ of a vector space is the group of functions $a: V \to V$ for which there is a $y \in V, g \in \mathrm{GL}(V)$ such that $a(x) = gx + y$. It is a generalization of the group of isometries. If S is a m-dimensional subspace, $S + v$ is an **affine m-subspace**.

An **affine space** is a vector space V that's "forgotten its origin"- think of it as a list of the affine m-subspaces. Considering V as an affine space, Aut(V) is the group of automorphisms preserving affine m-subspaces (i.e. automorphisms such that S is an affine m-subspace iff θ(S) is). The vector space V is a doubly transitive $\mathrm{Aff}(V)$-space.

A **semilinear transformation** is a function $f: V \to W$ satisfying

1. $f(x+y) = f(x) + f(y)$
2. $f(\lambda x) = \sigma(\lambda) f(x)$ for some $\sigma \in \mathrm{Aut}(K)$. (V and W are over the field K.)

The bijective semilinear transformations on V form a group $\Gamma L(V)$ under composition. If $\dim V \geq 2$, every affine automorphism is in the form $f(x) = g(x) + u$, where $g \in \Gamma L(V)$.

1. $\Gamma L(V) \cong GL(V) \rtimes \mathrm{Aut}(K)$
2. $\mathrm{Aut}(V) \cong \mathrm{Tr}(V) \rtimes \Gamma L(V)$, where $\mathrm{Tr}(V)$ is the translation group.

Projective Geometry

For a vector space V over K of dimension n+1, let $V^{\#} = V - \{0\}$, $[x] = \{cx | c \in V^{\#}\}$. The **projective space** of V is $P_n(K) = P(V) = \{[x] | x \in V^{\#}\}$; it has projective dimension n. In homogeneous coordinates, $[x_0, \dots, x_n] = [cx_0, \dots, cx_n], c \in V^{\#}$. If W is a (m+1) dimensional subspace of V, $[W] = \{[x] | x \in W^{\#}\} \subset P(V)$ is a projective subspace of dimension m.

- Every pair of distinct points lies on a unique projective line.
- If H is a projective hyperplane (of dimension n-1) and L is a projective line not in H, then $H \cap L$ is a projective point.

A **collineation** (projective isomorphism) is a bijection $\theta: P(V) \to P(V')$ such that S is a projective m-subspace iff $\theta(S)$ is a projective m-subspace. The **projectivity** $P(g): P(V) \to P(V')$ corresponding to the nonsingular semilinear transformation g is $g([x]) = [g(x)]$.

- Every projective line has $q - 1$ points.
- $P(\mathbb{F}_q^n) = \sum_{k=0}^{n} q^k$
- There are $q^2 + q + 1$ points and $q^2 + q + 1$ lines in $P(\mathbb{F}_q^2)$.

<u>Fundamental Theorem of Projective Geometry:</u> If $P(V), P(V^{'})$ have dimension $n \geq 2$ (V, V' have dimension ≥ 3), then every collineation $\theta: P(V) \to P(V^{'})$ is a projectivity.

- For $n \geq 2$ the group C of collineations of P(V) with itself is isomorphic to $P\Gamma L(V) = \Gamma L(V)/Z(V)$, where Z(V) is the center of $\mathrm{GL}(V)$ (nonzero scalar transformations).
- PSL(V) acts double transitively on P(V).

A **Steiner system** of type $S(t, k, v), t < k < v$ is an order pair (X, B) where X is a set with v elements (a.k.a. points), and B is a family of blocks (subsets, a.k.a. lines), each with k elements, so that every t elements of X lie in a unique block.

Ex. An affine plane over $\mathbb{F}_q$, with the lines being the blocks, has type $S(2, q, q^2)$.

The projective plane $P_2(\mathbb{F}_q)$ has type $S(2, q, q^2 + q + 1)$.

5-5 Mathieu Groups

For a field K, let $\widehat{K} = K \cup \{\infty\}$. If $\sigma \in \mathrm{Aut}(K)$ and $ad - bc \neq 0$, then the function

$$f(\lambda) = \begin{cases} \dfrac{a\sigma(\lambda) + b}{c\sigma(\lambda) + d}, & c\sigma(\lambda) + d \neq 0 \\ \infty, & c\sigma(\lambda) + d = 0 \\ \infty, & \lambda = \infty, c = 0 \\ a/c\,, & \lambda = \infty, c \neq 0 \end{cases}$$

is a **semilinear fractional transformation**, and a linear fractional transformation if σ is the identity. $\Gamma LF(K), LF(K)$ are the groups of semilinear, linear fractional transformations, respectively. Note $\Gamma LF(K) \cong P\Gamma L_2(K), LF(K) \cong \mathrm{PGL}_2(K)$, by associating f with the matrix $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$.

For $q = p^{2n}$, p an odd prime, and σ the (unique) automorphism of order 2, define the subgroup of $\Gamma LF(K)$:

$$M(q) = \left\{\lambda \rightsquigarrow \frac{a\lambda + b}{c\lambda + d} \middle| ad - bc \text{ square}\right\} \cup \left\{\lambda \rightsquigarrow \frac{a\sigma(\lambda) + b}{c\sigma(\lambda) + d} \middle| ad - bc \text{ not square}\right\}$$

Letting $K = \mathbb{F}_{p^{2n}}$, $\widehat{K}$ is a faithful sharply 3-transitive M(q)-set.

The **Mathieu groups** are 5 sporadic simple groups. Below, M_{10} is not considered a Mathieu group, TE=transitive extension, pm=primitive element.

Mathieu group (degree)	Order	Transitivity	Construction[4]	Automorphism of Steiner system (system is unique)	Reason for simplicity
M_{10}	$720 = 2^4 3^2 5$	Sharply 3-transitive	M(9) Acts on $\mathbb{F}_9 \cup \{\infty\}$.		Not simple
M_{11}	$7920 = 2^4 3^2 5 \cdot 11$	Sharply 4-transitive	Add ω to G-set. $\langle M_{10}, h\rangle$, where $h = (\omega\infty)\sigma$, $\sigma(\lambda) = \pi^2\lambda + \pi\lambda^3$, π pm of $\mathbb{F}_9$.	S(4,5,11)	If $H \lhd G$ nontrivial, • Transitive, 11 divides. • 11-SSG of H, $P \neq N_H(P)$ • $N_H(P) = N_{M_{11}}(P)$ • Frattini argument $M_{11} = H$
M_{12}	$95040 = 2^6 3^3 5 \cdot 11$	Sharply 5-transitive	Add Ω to G-set. $\langle M_{11}, k\rangle$ where $k = (\omega\Omega)\sigma$, $\sigma(\lambda) = \lambda^3$.	S(5,6,12)	TE of M_{11}
M_{22}	$443520 = 2^7 3^2 5 \cdot 7 \cdot 11$	3-transitive	Acts on $P_2(\mathbb{F}_4) \cup \{\infty\}$. $\langle PSL_3(\mathbb{F}_4), h_1\rangle$, where $h_1 = (\infty\ [1,0,0])f_1$, $f_1[x,y,z] = [x^2 + yz, y^2, z^2]$.	Subgroup of index 2 in Aut(S(3,6,22))	TE of $PSL_3(\mathbb{F}_4)$
M_{23}	$10200960 = 2^7 3^2 5 \cdot 7 \cdot 11 \cdot 23$	4-transitive	Add ω to G-set. $\langle M_{22}, h_2\rangle$, where $h_2 = (\omega\infty)f_2$, $f_2[x,y,z] = [x^2, y^2, \alpha z^2]$, α a pm of $\mathbb{F}_4$.	S(4,7,23)	TE of M_{22}

[4] σ, f_1, f_2, f_3 act on $\mathbb{F}_9, P_2(\mathbb{F}_4), P_2(\mathbb{F}_4), P_2(\mathbb{F}_4)$, respectively, and is the identity on everything else.

M_{24}	$244823040 = 2^{10}3^3 5 \cdot 7 \cdot 11 \cdot 23$	5-transitive	Add Ω. $\langle M_{23}, h_3\rangle$, where $h_3 = (\Omega\omega)f_3$, $f_3[x,y,z] = [x^2,y^2,z^2]$	S(5,8,24)[5]	TE of M_{23}

Neither M_{12} nor M_{24} have transitive extensions.
Sharply transitive groups of degree:

1. All finite groups.
2. Except for a finite number, can be imbedded in $\mathrm{Aut}(\mathbb{F}_q)$.
3. $\mathrm{PGL}_2(\mathbb{F}_q), M(p^{2n})$
4. S_4, S_5, A_6, M_{11}
5. A_5, S_6, A_7, M_{12}

≥ 6: S_k, S_{k+1}, A_{k+2}

5-6

Pólya Enumeration

Frobenius-Burnside Lemma: Let

1. $|G| \cdot (\text{number of orbits}) = \sum_{g\in G} |\operatorname{Fix}(g)|$, $\operatorname{Fix}(g) = \{s \in S | gs = s\}$.
   a. Both count the number of pairs $(g \in G, s \in S)$ such that $gs = s$.
2. $(\text{number of orbits}) = \frac{1}{|G|}\sum_{g\in G} |\operatorname{Fix}(g)|$

The **cycle index** of a permutation group *G* is the average of the cycle index monomials over all permutations *g* of the group:

$$Z_G(a_1, a_2, \dots) = \frac{1}{|G|}\sum_{g\in G}\prod_{i\geq 1} a_i^{j_i(g)}$$

where $j_i(g)$ is the number of cycles of length *i* in the disjoint cycle decomposition of *g*.

Pólya Enumeration Theorem: Let *A* be a group acting on a set *X* (the "slots") and and let G operate on Y^X, the set of all filled slot configurations- each slot in X is filled with an object in *Y* (the objects, such as beads of different colors, are weighted (1,0,…), (0,1,0,…), …, (0,…,1); the total weight gives the number of each color). Let $F_G(r, \dots, r_n)$ be the generating function of the number of orbits of configurations by weight, i.e.

$$F_G(r_1, \dots, r_n) = \sum_{r_1,\dots,r_n} f_G(t_1, \dots, t_n) r_1^{t_1} \cdots r_n^{t_n}$$

where $f_G(t_1, \dots, t_n)$ is the number of orbits with weight $(t_1, \dots, t_n)$. Then

$$F_G(a_1, \dots, a_n) = Z_G(a_1 + \cdots + a_n, a_1^2 + \cdots + a_n^2, a_1^3 + \cdots + a_n^3, \dots)$$

Pf. The only way to color a cycle of length k is to make them all the same color. Use Burnside's lemma.
Generalization: Let *G* be a group acting on a set *X* (the "slots") and hence X^Y, and consider the set Y^X of all functions from a set *X* to a weighted set *Y* (the objects) with weight function ω (the "filled slot configurations"), where the weight of a function *f* is the sum of the weights of its range.
The the generating function of the number of orbits of *G* on Y^X by weight (the equivalence classes of configurations induced by *X*) is given by

[5] Application: Golay codes and Leech lattices.

$$F_G(r_1, \dots, r_n) = Z_G\left(\sum_{y \in Y} \omega(y), \sum_{y \in Y} \omega(y)^2, , \dots, \sum_{y \in Y} \omega(y)^n\right)$$

Each ω(y) is a monomial in the variables r_1, r_2, r_3 ...

$$\sum_{y \in Y} \omega(y) = f(r_1, r_2, r_3, \dots)$$

where $f(r_1, r_2, r_3, \dots)$ is the generating function of the set Y by weight, so

$$F_G(a_1, \dots, a_n) = Z_G(f(a_1, \dots, a_n), f(a_1^2, \dots, a_n^2), f(a_1^3, \dots, a_n^3), \dots)$$

Ex. Counting the number of necklaces with n strings of beads on it.

Exercises

1. How many circular necklaces can be made with n beads, if there are c different colors and
    a. Rotations of necklaces are considered the same.
    b. Both rotations and reflections of necklaces are considered the same.
    c. Express the sum in closed form when n is a power of 2.

6 Normal Series

6-1 Composition Series

A chain of subgroups of G

$$G = A_0 \supseteq A_1 \supseteq \cdots \supseteq A_n = \{1\}$$

is a…

subnormal (subinvariant) **series** if each A_i is a normal subgroup of A_{i-1}.	**normal** (invariant) **series** if each A_i is a normal subgroup of G
composition series if each A_i is a maximal normal subgroup in A_{i-1}.	**principal** (chief) **series** if each A_i is maximal normal subgroup of G contained in A_{i-1}.

In general, a composition series will have fewer terms than a principal series, because there are more requirements.

Two subnormal series are **equivalent** if the factor groups are the same up to isomorphism and rearrangement. **Refining** of a subnormal series means to insert more groups between groups in the series.

Schreier Refinement Theorem: Two subnormal series

$$1 = H_0 \triangleleft \cdots \triangleleft H_r = G, 1 = K_0 \triangleleft \cdots \triangleleft K_s = G$$

for the same group G have equivalent refinements.

Pf. Use Zessenhaus Lemma: If $A \trianglelefteq B, C \trianglelefteq D$ then

$$\frac{A(B \cap D)}{A(B \cap C)} \cong \frac{C(D \cap B)}{C(D \cap A)}$$

Insert $H_{ij} = H_i\left(H_{i+1} \cap K_j\right), K_{ij} = K_j\left(K_{j+1} \cap H_i\right)$. Then $\frac{H_{i,j+1}}{H_{ij}} \cong \frac{K_{i+1,j}}{K_{ij}}$.

Jordan-Hölder Theorem: If G has a composition series S then any subnormal series R can be refined to a composition series, and any two composition series are equivalent.

Pf. R and S have equivalent refinements. Removing repeats, these refinements must be equivalent to R.

Ex. Taking G to be cyclic of order n, we get that n factors into primes uniquely.

Let H be a normal subgroup of G such that there is a composition series from G to H (in particular, this is true when G is a finite group). Then there is a principal series from G to H where every factor group is the direct product of isomorphic simple groups. Conversely, if such a principal series exists, then there is a composition series.

6-2 Commutators and Derived Groups

A **commutator** of a group G is in the form $(x, y) = xyx^{-1}y^{-1}$. The commutators generate the **derived subgroup** G' of G. The higher order commutators are defined recursively by $(x_1, \dots, x_n) = \left((x_1, \dots, x_{n-1}), x_n\right)$. For subgroups H_1, H_2, $(H_1, H_2) = \langle (x_1, x_2) | x_i \in H_i \rangle$, with higher order commutators defined similarly.

Properties of Commutators:

1. $(y, x) = (x, y)^{-1}$
2. $(xy, z) = (x, z)^y (y, z) = (x, z)(x, z, y)(y, z)$
3. $(x, yz) = (x, z)(x, y)^z = (x, z)(x, z, y)(y, z)$

4. $(x,y^{-1},z)(y,z^{-1},x)^{z}(z,x^{-1},y)^{x} = 1$ (Jacobi identity)
5. $(x,y,z)(y,z,x)(z,x,y) = (y,x)(z,x)(z,y)^{x}(x,y)(x,z)^{y}(y,z)^{x}(x,z)(z,x)^{y}$
6. $(Y,Z,X),(Z,X,Y) \subseteq G \Rightarrow (X,Y,Z) \subseteq G$

G/G' is abelian, and if K is a normal subgroup such that G/K is abelian, then $G^{'} \subseteq K$.

(Schur) If $Z(G)$ has finite index in G, then G' is finite. (See 7-8)

6-3 Solvable Groups

G is **solvable** if the sequence $G \supseteq G^{'} \supseteq G^{''} \supseteq \cdots$ terminates at the identity in a fixed number of steps. Equivalently, G has a solvable series, a subnormal series where all factor groups are abelian (actually, they can be made prime cyclic by refinement). Each of the higher commutator subgroups $G^{(i)}$ is characteristic in G.

- A finite group is solvable iff the factor groups in a composition series from G to 1 are of prime order.
- A finite group is solvable iff the factor groups in a principal series from G to 1 are elementary abelian groups.

Every subgroup and factor group of a solvable group is solvable. Conversely, if a finite group G has a normal subgroup H so that H and G/H are both solvable, then G is solvable. In particular, every abelian group is solvable.
Pf. If $\{1\} = G_n \subseteq \cdots \subseteq G_0 = G$, then take

- $\{1\} = H \cap G_n \subseteq \cdots \subseteq H \cap G_0 = H$
- $\{1\} = HG_n/H \subseteq \cdots \subseteq HG_0/H = G/H$.
- $1 = K_n \subseteq \cdots \subseteq K_0 = G/H$ gives $H = K_nH \subseteq \cdots \subseteq K_0H = G$. ($K_iH$ is the preimage of K_i under the natural map $G \to G/H$.)

A group that is both solvable and simple must be cyclic of prime order.

Application to Galois Theory: A polynomial equation over a field of characteristic 0 is solvable by radicals iff its Galois group is a solvable group. "Solvable by radicals" means we can get to the roots by repeatedly adjoining (prime) roots of elements in the field to the field; this corresponds to "enlarging" the Galois group by a prime factor each time.

6-4 Hall Subgroups

A **Hall subgroup** H of G is a subgroup whose order and index are relatively prime:

$$\gcd(|H|,[G:H]) = 1$$

Let p be a prime. If $G = p^n a, p \nmid a$, a **p-complement** of G is a subgroup with order a.

Extended Sylow Theorems: [Hall] Let G be a solvable group of order ab, where a, b are relatively prime. Then

1. G has a subgroup of order a.
2. Any two subgroups of order a are conjugate, and any subgroup of order dividing a is in a subgroup of order a.
3. The number of subgroups of order a is a product of factors, each of which
    a. Is congruent to 1 modulo some prime factor of a

b. Is a power of a prime and divides one of the chief factors of G.

Pf. Induct on $|G|$.
Case 1: G has a normal subgroup of order $a^{'}b^{'}, a^{'}|a, b^{'}|b, b^{'} < b$.
Existence: G/H has subgroup A/H of order $a/a^{'}$; A is the desired subgroup.
Conjugacy: Suppose A, A' have order a. Then $AH/H, A'H/H \subset G/H$ have order a/a' and are conjugate.
Case 2: Else, take H a minimal normal subgroup. $b = p^m$; use the Schur-Zassenhaus lemma.

Converse: If a group contains a p-complement for every prime dividing its order, then G is solvable.
Pf. If G is not simple, use the induction hypothesis for G/N (N normal). If G is simple, let $|G| = \prod_{i=1}^{n} p_i^{a_i}$, and let H_i be a p_i-complement. Let $D = \bigcap_{i=3}^{n} H_i$; then $|D| = p_1^{a_1}p_2^{a_2}$ is solvable by Burnside's theorem. Let N be a minimal normal subgroup of D. $G = H_2(D \cap H_1)$ by comparing orders; $N^G \subseteq H_2 \subset G$, contradiction. ($N^G$ is the minimal normal subgroup of G generated by N.)

6-5

Supersolvable and Nilpotent Groups

The following conditions are stronger than solvability:

- A group G is **supersolvable** if it has a finite normal series $G = A_0 \supseteq A_1 \supseteq \cdots \supseteq A_r = \{1\}$, with each factor group A_{i-1}/A_i cyclic. Any supersolvable group is finitely generated.
- G is **nilpotent** if it has a central series, i.e. a finite normal series $G = A_0 \supseteq A_1 \supseteq \cdots \supseteq A_r = \{1\}$, with A_{i-1}/A_i in the center of G/A_i.

1. Define $\Gamma_1(G) = G, \Gamma_k(G) = \langle (x_1, \dots, x_k) | x_i \in G \rangle$. Note that $\Gamma_{k+1}(G) = (\Gamma_k(G), G)$. The **lower central series** of G is $G = \Gamma_1(G) \supseteq \Gamma_2(G) \supseteq \cdots$. Each $\Gamma_k(G)/\Gamma_{k+1}(G)$ is in the center of $G/\Gamma_{k+1}(G)$.
2. The **upper central series** of G is $\{1\} = Z_0(G) \subseteq Z_1(G) \subseteq \cdots$ where $Z_{i+1}(G)/Z_i(G)$ is the center of $G/Z_i(G)$. Note each Z_i is a characteristic subgroup.

When G is nilpotent, upper and lower central series end at {1} and G, respectively, and have the same length. Then for any central series $G = A_0 \supseteq A_1 \supseteq \cdots \supseteq A_r = \{1\}$,

$$\Gamma_i(G) \subseteq A_i \subseteq Z_{r+1-i}(G)$$

The lower central series is "as fast down as you can go" in a central series, and the upper central series is "as fast up as you can go".

A group has **nil-c** if $\{(x_1, \dots, x_{c+1}) | x_i \in G\} = \{1\}$.

- If G has nil-c, then every subgroup and quotient group has nil-c.
- If H, K are normal subgroups of G, then HK has nil-(c+d).
- $\left(\Gamma_i(G), \Gamma_j(G)\right) \subseteq \Gamma_{i+j}(G)$

Subgroups and quotient groups of supersolvable groups are supersolvable.

Properties of Nilpotent Groups

- Every proper subgroup is strictly contained in its normalizer. (Normalizer condition)
- Every maximal subgroup is normal, of prime index, and contains the derived group.
- Any abelian group is nilpotent.
- Finite p-groups are nilpotent. (Pf. The center of a p-group is not the identity.)

- A finite group is nilpotent iff it is the direct product of its Sylow subgroups, which is true iff each p-SSG is normal. (Pf. Take a p-SSG P. $N_G(P)$ is its own normalizer so by the 1st bullet, is G.)
- A finite group is nilpotent iff its maximal subgroups are all normal. (A maximal subgroup is a proper subgroup contained in no other subgroup except G.)

6-5

Frattini Subgroup

The **Frattini subgroup** $\Phi(G)$ of G is the intersection of the maximal subgroups of G. It is the set of nongenerators, x such that $\langle T, x\rangle = G \Rightarrow \langle T\rangle = G$.
Pf. If $x \notin \Phi$, then $x \notin M$ for some maximal subgroup M. Then $M \subset \langle M, x\rangle = G$. If $x \in \Phi$, and $G = \langle T, x\rangle \supset \langle T\rangle$, then take the maximal K containing $\langle T\rangle$ but not x. If a maximal subgroup contains K, then it contains x (since $x \in \Phi$) and must actually be G, contradiction.

The Frattini subgroup of a finite group is nilpotent.
Pf. Take a p-SSG P of G. Since every conjugate of P in Φ is conjugate to P in Φ, $[G{:}N_G(P)] = [\Phi{:}N_\Phi(P)] \Rightarrow [G{:}\Phi] = [N_G(P){:}N_\Phi(P)] = [N_G(P){:}N_G(P) \cap \Phi]$. But $[N_G(P) \vee \Phi{:}\Phi] \ge [N_G(P) \cap \Phi]$, so $G = N_G(P) \vee \Phi = \langle N_G(P), \Phi\rangle$. Since Φ consists of nongenerators, $G = N_G(P)$.

Burnside Basis Theorem: Let Φ be the Frattini subgroup of the p-group P.

1. The factor group $A = P/\Phi$ is an elementary abelian group.
2. If $|A| = p^r$, every set of elements which generate P contains a subset of r elements that generate P. (In other words, any minimal generating set has $\dim G/\Phi(G)$ elements.)
3. In the canonical map $P \to A$ they are mapped onto a basis for A.
4. Conversely, any set of r elements which is mapped to a set of generators for A will generate P.
5. A has $\theta(p^r) = \prod_{i=0}^{r-1} p^r - p^i$ bases and hence $\theta(p^r)$ automorphisms. $|Aut(P)|$ divides $p^{r(n-r)}\theta(p^r)$.

7 Extensions and Cohomology

7-1 The Extension Problem

The **extension** of a group K by a group Q is a group G with normal subgroup $K_1 \cong K$ and factor group $G/K_1 \cong Q$. In category theory terms, there is an exact sequence

$$\{1\} \to N \to G \to Q \to \{1\}$$

(each arrow represents a homomorphism; the image of each is the kernel of the next).
Why care? Every finite group has a composition series; by knowing the simple groups and the answer to the extension problem we can "recreate" any finite group from the factor groups in the series.
Ex. $K \times Q$ is an extension of K by Q, but it is by no means the only one because the elements of Q can permute the elements of K under conjugation.

7-2 Direct Products

A group G is **decomposable** if it is $\{1\}$ or it can be written as $G = H \times K$, with $H, K \neq \{1\}$.
A group has the…

- **Ascending chain condition** (ACC) if there is no infinite strictly increasing chain of normal subgroups
$$K_1 \subset K_2 \subset \cdots$$
- **Descending chain condition** (DCC) if there is no infinite strictly decreasing chain of normal subgroups
$$H_1 \supset H_2 \supset \cdots$$

Ex. $\mathbb{Z}$ has ACC but not DCC; $\mathbb{Z}(p^\infty)$ has DCC not ACC.

If G satisfies both chain conditions, then G is a direct product of a finite number of indecomposable groups.

- If $H \lhd G$, and $H, G/H$ have both chain conditions, so does G.
- If $H \times K$ has both chain conditions, so do H, K.
- If G has both chain conditions, a normal endomorphism is an injection iff it is a surjection.

An endomorphism is normal if $\varphi(axa^{-1}) = a\varphi(x)a^{-1}$ for all $a, x \in G$. φ is **nilpotent** if there exists $k \in \mathbb{N}$ so that $\varphi^k = 0$ (the transformation sending every element to 1).

Fitting's Lemma: Let G have both chain conditions and φ be a normal endomorphism. Then $G = K \times H$ for some φ-invariant subgroups H, K, with $\varphi|_K$ nilpotent and $\varphi|_H$ surjective.
Pf. $K_n = \ker \varphi^n, H_n = \operatorname{im} \varphi^n$ form an increasing/ decreasing chain stopping at the desired K, H.

Krull-Schmidt Theorem: Let G be a group satisfying both chain conditions. If

$$G = H_1 \times \cdots \times H_s = K_1 \times \cdots \times K_t$$

are two decompositions into indecomposable factors, then $s = t$ and there is a reindexing so that $H_i \cong K_i$ for all i. Moreover, given any r $(1 \le r \le s)$, the reindexing may be chosen so that $G = H_1 \times \cdots \times H_r \times K_{r+1} \times \cdots \times K_s$.
Pf. Induct on r. For $r = 1$,

1. Let $\pi_i: G \to H_i, \lambda_i: H_i \hookrightarrow G, \sigma_j: G \to K_j, \mu_j: K_j \hookrightarrow G$ be the projection and inclusion maps.
2. Every partial sum of $\pi_1\left(\sum \mu_j \sigma_j\right)\lambda_1$ is a normal endomorphism of G.

3. If φ, ψ are nilpotent endomorphisms, and $\varphi + \psi$ (defined by $(\varphi + \psi)(x) = \varphi(x)\psi(x)$) is an endomorphism, then it is nilpotent by the binomial theorem. This generalizes to more summands.
4. In an indecomposable group, every normal endomorphism if nilpotent or an automorphism. From the contrapositive of (3), and (4), some summand, say $\pi_1\mu_1\sigma_1\lambda_1$, in (2) is a (normal) automorphism of H_1. Then $\sigma_1\lambda_1$ is an isomorphism.

7-3 Operator Groups

A set of **operators** Ω is just a set of endomorphisms of G. (Note, however, that the elements of Ω are allowed to act on different groups, called Ω-groups.) A **Ω-map** is a homomorphism between Ω-groups invariant under all endomorphisms in Ω: $\varphi(\omega g) = \omega\varphi(g)$ for all $\omega \in \Omega, g \in G$. An **admissible** subgroup H is invariant under Ω: $\omega h \in H$ for all $\omega \in \Omega, h \in H$.

Ex. If Ω is the set of inner automorphisms, then the admissible subgroups are the normal subgroups, and a Ω-isomorphism is called a **central isomorphism**.

The definitions and results about normal subgroups, composition series, and direct products generalize to operator groups:

- A group is **Ω-simple** if it has no proper admissible subgroups.
- A **Ω-series** is a normal series with each term admissible; a **Ω-composition series** has each factor group Ω-simple.
- A group is **Ω-decomposable** if it is the direct product of nontrivial admissible subgroups.

Jordan-Hölder Theorem: Every two *Ω*-composition series of a *Ω*-group are equivalent.

Fitting's Lemma: Let G have both chain conditions *on admissible subgroups* and be a *Ω*-endomorphism. Then $G = H \times K$ for some *admissible* subgroups H, K, with $\varphi|_K$ nilpotent and $\varphi|_H$ surjective.

Krull-Schmidt Theorem: Let G be a Ω-group satisfying both chain conditions *on admissible subgroups*. If

$$G = H_1 \times \cdots \times H_s = K_1 \times \cdots \times K_t$$

are two decompositions into *Ω*-indecomposable factors, then $s = t$ and there is a reindexing so that $H_i \cong K_i$ for all i. Moreover, given any r $(1 \le r \le s)$, the reindexing may be chosen so that $G = H_1 \times \cdots \times H_r \times K_{r+1} \times \cdots \times K_s$.

Ex. The strengthened Jordan-Hölder theorem shows that if a vector space has a finite basis, then the size of a basis is always the same. Fitting's Lemma shows that if $T: V \to V$ is a linear transformation for V a finite-dimensional vector space, then $V = U \oplus W$, for subspaces U, W with $T|_U$ nilpotent and $T|_W$ nonsingular.

7-4 Semidirect Product

A subgroup $Q \subseteq G$ is a **complement** of subgroup $K \subseteq G$ if $K \cap Q = 1$ and $G = KQ$. If they exist, complements are unique up to isomorphism. (Warning: Not every normal subgroup has a complement, for example, $\langle a^2 \rangle \subseteq \langle a \rangle = C_4$. No primary cyclic group is a semidirect product of non-{1} subgroups.)

G is the **semidirect product** of K by Q

$$G = K \rtimes Q$$

if $K \lhd G$ and Q is (isomorphic to) a complement of K. G is said to split over K. Each element of Q induces an automorphism of K so this is equivalent to the following formulation:
Let θ be a homomorphism of Q into Aut(K); θ_x is the image of $x \in Q$. The semidirect product S of K by Q is the set of pairs $(x,u), x \in K, u \in H$ with the following rule

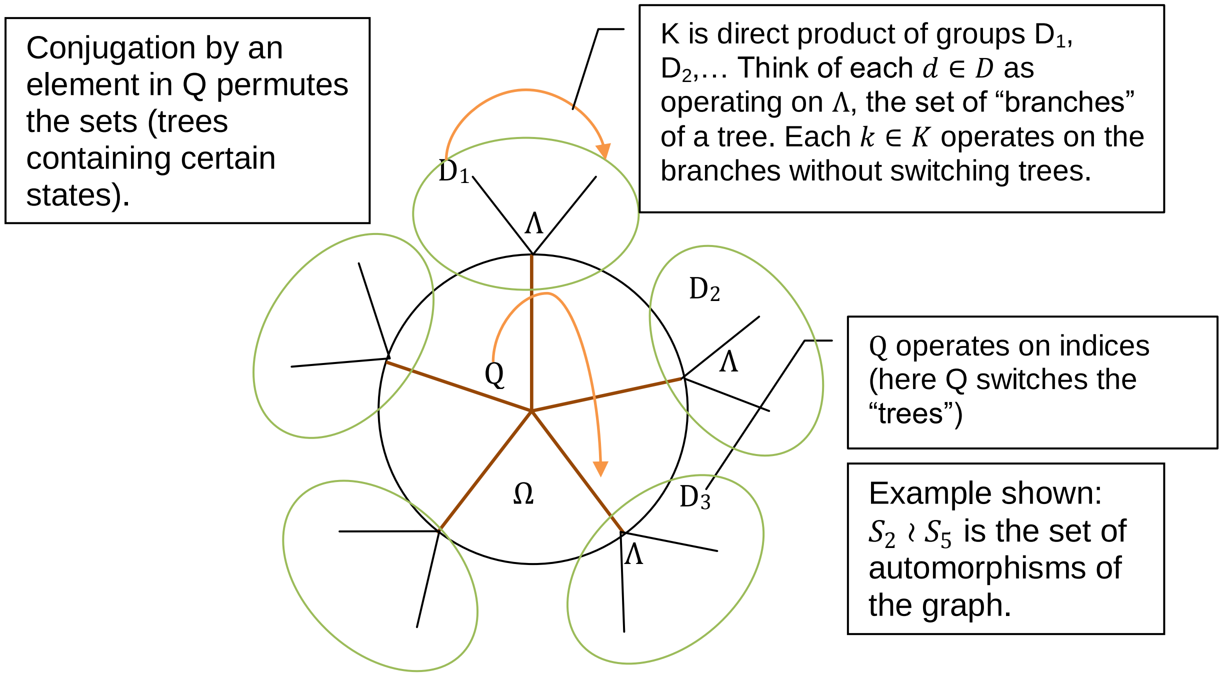
$$(x,u)(x^{'},u^{'}) = (xx^{'}, \theta_{x^{'}}(u)u^{'})$$

Connecting the two, θ_x is conjugation by $x \in Q$. We say that G realizes θ; $G = K \rtimes_\theta Q$. With the above construction, any homomorphism θ can be realized. (Note a group may have distinct factorizations into a semidirect product.)

Ex. $S_n = A_n \rtimes C_2$
$D_{2n} = C_n \rtimes C_2$
$\mathrm{Hol}(K) = K^l \rtimes \mathrm{Aut}(K)$

Wreath Product

Let D and Q be groups, $\{D_\omega | \omega \in \Omega\}$ a family of groups isomorphic to D, let Q operate on Ω, and let $K = \prod_{\omega\in\Omega} D_\omega$. The **wreath product** of D by Q, $G = D \wr Q$, is the semidirect product of K by Q, where Q acts on K by $q \cdot (d_\omega) = \left(d_{q\omega}\right), q \in Q$. The normal subgroup K is the base of the wreath product G.



Conjugation by an element in Q permutes the sets (trees containing certain states).

K is direct product of groups D₁, D₂,… Think of each $d \in D$ as operating on Λ, the set of "branches" of a tree. Each $k \in K$ operates on the branches without switching trees.

Q operates on indices (here Q switches the "trees")

Example shown: $S_2 \wr S_5$ is the set of automorphisms of the graph.

The permutation version:
If Λ is a D-set, then $\Lambda \times \Omega$ can be made into a $(D \wr Q)$-set.
Let $d_\omega^*(\lambda,\omega') = \begin{cases} (d\lambda,\omega^{'})\ if\ \omega^{'} = \omega \\ (\lambda,\omega^{'})\ if\ \omega^{'} \neq \omega \end{cases}$, i.e. d_ω^* operates on one tree, the one indexed by ω.
Let $q^*(\lambda,\omega^{'}) = (\lambda, q\omega^{'})$, i.e. q* permutes the trees.
Then $D \wr Q \cong \langle Q^*, D_\omega^* \rangle \subseteq S_{\Lambda\times\Omega}$.
If Λ=Q is a Q-set acting on itself, then $W = D \wr_r Q$ is the regular wreath product.

If Ω is an infinite set, then the wreath product can be complete or restricted depending on whether the direct product is complete or restricted. (A restricted direct product only include the elements with a finite number of non-1 coordinates.)
If Ω and Λ are finite then $T \wr (D \wr Q) = (T \wr D) \wr Q$.

Ex. If p is a prime, then a p-SSG of S_{p^n} is an iterated wreath product $W_n = C_p \wr_r \cdots \wr_r C_p$ (n times).
Pf. Induct on n. Take $\Lambda = S_{p^n}$, $Q = C_p$. Then the resulting wreath product is in $S_{\Lambda\times\Omega} \cong S_{p^{n+1}}$ and has the right order.
Use to calculate a p-SSG of S_m for any m: partition based on base p representation, take p-SSG of each.

7-5 Cohomology: Background

[To be added.]

7-6 Factor Sets: The Second Cohomology Group

From here on, use additive notation in K and G, multiplicative notation in Q, and let xa denote x operating on a.
For $K \subseteq G$, a right (left) transversal T of K in G is a complete set of right (left) coset representatives- a set containing one element from each right (left) coset. This is less restrictive than a complement.

If $\pi: G \to Q$ is surjective, a **lifting** of $x \in Q$ is an element $l(x) \in G$ with $\pi\big(l(x)\big) = x$. $\{l(x) | x \in Q\}$ is a transversal of ker(π)- each coset is a fiber corresponding to an element in the image.

Let G be an extension of K by Q, and $l: Q \to G$ a transversal. If K is abelian, there is a homomorphism $\theta: Q \to \mathrm{Aut}(K)$ with $\theta_x(a) = l(x) + a - l(x)$ for every $a \in K$. θ_x (conjugation by x) is the same for any transversal l.
Pf. Let $\mu = \gamma_g \in \mathrm{Aut}(K)$ (with the range restricted to K). Since K is abelian, we can define $\mu': G/K \to \mathrm{Aut}(K)$ by $K + g \to \mu(g)$. Let $\lambda: Q \to G/K$ be the canonical map defined by $\lambda(x) = K + l(x)$. $\theta_x = \mu'\lambda(x) = \mu\big(l(x)\big) \in \mathrm{Aut}(K)$ is independent of l. In other words, l(x) can differ by something in K, which commutes with K.

Call an ordered triple (Q,K,θ) **data** if K is an abelian group (for our purposes), Q is a group, and $\theta: Q \to \mathrm{Aut}(K)$ is a homomorphism. G realizes this data if G is an extension of K by Q and for every transversal $l: Q \to G$, $xa = \theta_x(a) = l(x) + a - l(x)$ for all $x \in Q, a \in K$. (Before, we could state an analogue of this directing by assuming Q is a complement of K; now we introduce transversals to circumvent this!)

Since cosets of K partition G, every element $g \in G$ has a unique expression in the form

$$g = a + l(x), a \in K, x \in Q$$

Then

$$l(x) + l(y) = f(x, y) + l(xy)$$
$$[a + l(x)] + [b + l(y)] = a + xb + f(x, y) + l(xy)$$

for some $f(x, y) \in K$ because $l(x) + l(y), l(xy)$ represent the same coset.

If $\pi: G \to Q$ is a surjective homomorphism with kernel K, and $l: Q \to G$ is a given transversal with $l(1) = 0$, then the function $f: Q \times Q \to K$ defined above is a **factor set** or cocycle.
Basic properties: For all $x, y, z \in Q$,

1. $f(1, y) = 0 = f(x, 1)$
2. Cocycle identity (derived from associativity)
$$f(x,y) + f(xy,z) = xf(y,z) + f(x,yz)$$
3. Converse: Given data (Q,K,θ), $f: Q \times Q \to K$ is a factor set iff it satisfies the cocycle identity. Construct G_f by letting
$$(a,x) + (b,y) = (a + xb + f(x,y), xy)$$
4. If G realizes (Q, K, θ), and l, l' are transversals with $l(1) = 0 = l'(1)$ that give rise to factor sets f, f', then there is a function $h: Q \to K$ such that $h(1) = 0$ and
$$f'(x,y) - f(x,y) = xh(y) - h(xy) + h(x) \ \forall\, x, y \in Q$$

Function	Domain and Range
f	$Q \times Q \to K$
l	$Q \to G$
h	$Q \to K$

The factor set measures the deviation of G from being a semidirect product- the obstruction of the transversal l to being a homomorphism. For example, it is identically 0 when G is a semidirect product of K and Q.

A **coboundary** is a function $g: Q \times Q \to K$ for which there exists $h: Q \to K$ so that $h(1) = 0$ and
$$g(x,y) = xh(y) - h(xy) + h(x)$$
$Z^2(Q, K, \theta)$ is the (abelian) group of all factor sets under addition. $B^2(Q, K, \theta)$ is the subgroup of all coboundaries. $H^2(Q, K, \theta) = Z^2(Q, K, \theta)/B^2(Q, K, \theta)$ is the **second cohomology group** of the data. From (4) above, two extensions G, G' realizing (Q, K, θ) are equivalent if they are in the same coset of $B^2(Q, K, \theta)$, i.e. if they determine the same element of $H^2(Q, K, \theta)$. Two equivalent extensions are isomorphic, but not necessarily vice versa.
Each element in $H^2(Q, K, \theta)$ represents an equivalence class of extensions realizing (Q,K,θ). The identity corresponds to the class of the semidirect product.

G, G' are equivalent iff there is an isomorphism γ (dotted line) making the following diagram commute:

$$\begin{tikzcd}
 & & G \arrow[dr] \arrow[dd, dashed] & & \\
\{0\} \arrow[r] & K \arrow[ur] \arrow[dr] & & Q \arrow[r] & \{1\} \\
 & & G' \arrow[ur] & &
\end{tikzcd}$$

Pf. The isomorphism is $\gamma\big(a + l(x)\big) = a + h(x) + l'(x)$ $(a \in K)$.
We say γ stabilizes the extension; the set of such γ is the stabilizer of the extension.

$Ext(K, Q)$ is the set of equivalence classes of abelian extensions G of K by Q, where θ is the trivial map.

The complete regular wreath product $K \wr_r Q$ contains an isomorphic copy of every extension of K by Q. (K not necessarily abelian)

7-7 Theorems

Schur-Zassenhaus Lemma: A normal Hall subgroup K of a finite group has a complement, so $G = K \rtimes G/K$. Any two complements of K in G are conjugate.

Pf.

1. An abelian normal Hall subgroup has a complement. (Pf. Sum the cocycle identity $xf(y,z) - f(xy,z) + f(x,yz) = f(x,y)$ over $z \in Q = G/K$. Use Bezout's Theorem to get $s|K| + t|Q| = 1$; multiply the sum by t and substitute to get that f is a coboundary with $h(x) = t\sum_{y \in Q} f(x,y)$.)
2. (cont.) Any 2 complements are conjugate. (Pf. We can choose the factor sets to be zero. Sum $0 = f_1(x,y) - f_2(x,y) = xh(y) - h(xy) + h(x)$ and use Bezout to get $h(x) = xb_0 - b_0$; then $-b_0 + Q_1 + b_0 = Q_2$.)
3. For the nonabelian case: If K contains a proper subgroup normal in G, use the induction hypothesis. Else K is a minimal subgroup of G. Using the Frattini argument and the 2nd isomorphism theorem, if P is a p-SSG of K (not {1}), $G/K = N_G(P)/N_K(P)$. If $N_G(P) \subset G$, then by the hypothesis, $N_G(P)$ has a subgroup of order n. Else, $P \lhd G, K = P, Z(P) = P$ and P is abelian; use (1).
4. If either K or G/K is solvable, then any two complements of K in G are conjugate. (Pf. Induction. Suppose Q_1, Q_2 are complements. If K is solvable, and not abelian, then $Q_1K^{'}/K'$ is conjugate to $Q_2K^{'}/K'$ by induction. If G/K is solvable, let M/K be the minimal normal subgroup of G/K. M=G gives Q_1, Q_2 p-SSGs; else by induction, $M \cap Q_i$ are conjugate. We can assume $J = M \cap Q_1 = M \cap Q_2$. Then $Q_1/J, Q_2/J$ are complements in $J(N_G(J) \cap K)/J$ in $N_G(J)/J$, and use induction.
5. One of K, G/K is odd and hence solvable by the Feit-Thompson Theorem.

Gaschütz's Theorem: Let K be a normal abelian p-subgroup of a finite group G, and let P be a p-SSG of G. K has a complement in G iff K has a complement in P.

Pf. If Q is a complement of K in G, take $Q \cap P$. If Q is a complement of K in P, choose a transversal U of P in G; then Q+U and -U+Q are transversals. Let f be the factor set of –U+Q. When $z = K + q, q \in Q$, we have $f(x,z) = 0$ and the cocycle identity becomes $f(x, y + z) = f(x,y)$. Letting $\{t_i\} = T = -U$, fixing g and defining $K + g + t_i = K + t_{\pi(i)} + q_i$, π is a permutation. Sum the cocycle identity over z in $\{K + t | t \in T\}$ and proceed as in (1) above to show f is a coboundary.

7-8 Transfer

If $Q \subseteq G$ is a subgroup of finite index n, then the **transfer** ("Verlagerung") is the *homomorphism* $V: G \to Q/Q'$ ($V_{G \to Q}$) defined by:

$$V(g) = \prod_{i=1}^{n} x_i Q'$$

where $\{l_1, \ldots, l_n\}$ is any left transversal of Q in G and $gl_i = l_j x_i$. (V is independent of the transversal chosen.)

If K is a complement, $K \subseteq \ker V$ since all terms in the product would be 1. The transfer is used to find a normal complement K to a normal (p-SSG) subgroup Q. (See Burnside Theorem)

Useful facts:

- If $Q \subseteq G$ is a subgroup of finite index n, and $\{l_i\}, \{h_i\}$ are left transversals, for a fixed $g \in G$ and each i, there is a unique $\sigma(i)$ with $x_i \in Q, gh_i = l_{\sigma(i)}x_i$. σ is a permutation.
- For each $g \in G$, there exist $h_i \in \{l_j\}, n_i \in \mathbb{N}, 1 \le i \le m$, so that
  - $h_i^{-1} g^{n_i} h_i \in Q$,
  - $\sum n_i = n = [G:Q]$,
  - $V(g) = \prod (h_i^{-1} g^{n_i} h_i) Q'$ (Pf. Cycle decomposition of σ)
- If Q has finite index n with $Q \subseteq Z(G)$, then $V(g) = g^n$ for all g.

If a p-SSG if a finite group G has a normal p-complement, G is p-nilpotent.

Burnside Normal Complement Theorem: Let G be a finite group and let Q be an abelian Sylow subgroup contained in the center of its normalizer: $Q \subseteq Z(N_G(Q))$. Then Q has a characteristic complement K.
Pf. Take the kernel of the transfer.

Applications:

1. If p is the smallest prime divisor of $|G|$, and G has a cyclic p-SSG, then G is p-nilpotent. (Use that $N(C)/C(Q)$ can be imbedded in $\mathrm{Aut}(Q)$.)
2. A nonabelian finite simple group cannot have a cyclic 2-SSG.
3. If every p-SSG of a finite group G is cyclic, then G is solvable. A group of squarefree order is solvable.
4. If G is nonabelian simple, and p is the smallest prime divisor of $|G|$, then $p^3 || G|$ or $12 || G|$. Using the Feit-Thompson Theorem, every finite simple nonabelian group has order divisible by 8 or 12.
5. (Schur) If $Z(G)$ has finite index in G, then G' is finite. ($G', G' \cap Z(G)$ are finitely generated; $G' \cap Z(G)$ has finite exponent so is finite.)

7-9

Derivations: The First Cohomology Group

Given data (Q, K, θ), a **derivation** is a function $d: Q \to K$ such that

$$d(xy) = xd(y) + d(x)$$

A **principal derivation** is in the form

$$d(x) = a - xa$$

for some $a \in K$.
The kernel of a derivation is the subgroup $\ker d = \{x \in Q | d(x) = 0\}$.
The set of derivations $\mathrm{Der}(Q, K, \theta)$ forms an abelian group under addition; the set of principal derivations $\mathrm{PDer}(Q, K, \theta)$ forms a subgroup.
The **first cohomology group** is $H^1(Q, K, \theta) = \mathrm{Der}(Q, K, \theta) / \mathrm{PDer}(Q, K, \theta)$. Note that the derivation formula comes from the coboundary formula set to 0 (as with semidirect products, when the transversal is a homomorphism).
Basic properties:

1. $d(1) = 0$
2. $d(x^{-1}) = -x^{-1} d(x)$
3. $d(x) = d(y) \Leftrightarrow x^{-1} y \in \ker d$

The stabilizer of an extension G realizing (Q, K, θ) (i.e. the group of automorphisms fixing each element of K and fixing each coset of K) is isomorphic to $\mathrm{Der}(Q, K, \theta)$. Regarding the elements of G as ordered pairs $(a,x), a \in K, x \in Q$, each stabilizing automorphism is in the form $\gamma\colon (a,x) \to (a + d(x), x)$, where d is a derivation.

Let $G = K \rtimes_\theta Q$, and let $\gamma\colon (a,x) \to (a + d(x), x)$ be a stabilizing automorphism.

- γ is an inner automorphism iff d is a principal derivation.
- $H^1(Q,K,\theta) \subseteq \mathrm{Aut}(G)/\mathrm{Inn}(G)$.
- If C, C' are complements of K in G, and $H^1(Q,K,\theta) = 0$, then C, C' are conjugate.

Application: Another proof of 1&2 in Schur-Zassenhaus. For an abelian normal subgroup of finite index n in a group G, let $\{l_i\}$ be a left transversal of K in G. For $g \in G$, let $el_i = l_{\sigma(i)}\kappa_i(e), a_i(e) = l_{\sigma(i)}\kappa_i(e)l_{\sigma(i)}^{-1}, d(e) = \prod_{i=1}^{n} a_i(e)$. Gruenberg's derivation satisfies similar properties as the transfer; in fact $d|_K$ is the transfer.

7-10

Projective Representations and the Schur Multiplier

A **central extension** of K by Q is an extension G of K by Q with $K \subseteq Z(G)$.
The **Schur multiplier** of Q is the abelian group $M(Q) = H^2(Q,\mathbb{C}^\times) = H^2(Q,\mathbb{C}^\times,I)$.
The **minimal exponent** $\exp(G)$ of a group is the least $e \in \mathbb{N}$ with $x^e = 1$ for all $x \in G$.
A **projective representation** of Q is a homomorphism $\tau\colon Q \to \mathrm{PGL}(n,\mathbb{C}) = \mathrm{GL}(n,\mathbb{C})\,/Z(n,\mathbb{C})$.
If K is abelian, the **character group** of K is $K^* = \mathrm{Hom}(K,\mathbb{C}^\times)$.[*]
If U is a central extension of K by Q, the **transgression** of the factor set $e\colon Q \times Q \to K$ is the homomorphism $\delta^U\colon K^* \to M(Q)$ defined by $\delta(\varphi) = [\varphi \circ e]$.
Let $\nu\colon U \to Q$ be a surjective homomorphism with kernel K, with U a central extension of K by Q. If $\tau\colon Q \to \mathrm{PGL}(n,\mathbb{C})$ is a projective representation, then τ can be lifted to U if there exists a homomorphism make the diagram commute:

$$\begin{tikzcd}
U \arrow[r, "\nu"] \arrow[d, dashed, "\tilde{\tau}"'] & Q \arrow[d, "\tau"] \\
G \arrow[r, "\pi"] & PG
\end{tikzcd}$$

U has the **projective lifting property** if every projective representation of Q can be lifted to U.
A **cover** of Q is a central extension U of an abelian group K by Q with the projective lifting property and with $K \subseteq U'$.

- If Q is finite, $M(Q)$ is finite and $\exp\big(M(Q)\big)\,||Q|$.
- The transgression δ is surjective iff U has the projective lifting property.
- δ is injective iff $K \subseteq U'$.
- If Q is finite, $B^2(Q,\mathbb{C}^\times)$ has a finite complement $M \cong M(Q)$ in $Z^2(Q,\mathbb{C}^\times)$.

<u>Cover Theorem:</u> [Schur] Every finite group Q has a cover U which is a central extension of $M(Q)$ by Q.

If Q is finite, $\exp\big(M(Q)\big)\exp(Q)\,||Q|$. Hence, if every p-SSG of Q is cyclic, then $M(Q) = 1$.

Exercises

1. Classify all groups of order pq, p and q prime. In particular, when is there more than one possibility?
2. Find all natural numbers n such that any group of order n is
   a. cyclic
   b. abelian

8 Abelian Groups

We use additive notation and assume the Axiom of Choice.

8-1 Finite Abelian Groups

(Cohn) If A and B are isomorphic abelian groups such that $A = G \times \langle b \rangle$ and $B = H \times \langle c \rangle$, where $\langle b \rangle \cong \langle c \rangle$, then $G \cong H$.

An abelian group corresponds to a ℤ-module with integer multiplication defined by $nv = \underbrace{v + v + \cdots + v}_{n \text{ times}}$***, so abelian groups and ℤ-modules are equivalent concepts.*** The following is proved using modules (See Abstract Algebra Notes 5-3):

<u>Structure Theorem for Finitely Generated Abelian Groups:</u>
a.k.a Unicity Theorem for Abelian Group Decomposition, Basis Theorem
A finitely generated abelian group V is the direct sum of cyclic subgroups and a free abelian group: $V = C_{d_1} \oplus \cdots \oplus C_{d_k} \oplus L$. The orders can be chosen uniquely to satisfy either of the following two conditions:

1. $1 < d_1 | d_2 \cdots | d_k$
2. All the d_i are prime power orders. (Uniqueness follows from counting orders in p-groups.)

An **elementary abelian** p-group is a direct sum of cyclic groups of order p. If G is an elementary abelian p-group of order p^n, then $\mathrm{Aut}(G) \cong \mathrm{GL}_n(\mathbb{F}_p)$, since G has the structure of a vector space and homomorphisms correspond to linear transformations.

8-2 Infinite Abelian Groups

A group is **p-primary** if every element has order a power of p. It generalizes a p-group for abelian groups, to include infinite groups such as $\mathbb{Z}(p^\infty)$.

The **torsion subgroup** of an abelian group G is the set of elements with finite order:

$$tG = \{x \in G | nx = 0 \text{ for some } n \in \mathbb{N}\}$$

A group is

- **Torsion (periodic)** if all elements have finite order ($tG = G$).
- **Torsion-free (aperiodic)** if all nonzero elements have infinite order ($tG = \{0\}$).

Facts:

- G/tG is torsion-free; i.e. G is an extension of a torsion group by a torsion-free group.
- Every torsion group is a direct sum of primary groups.
- Let $G_p = \{x \in G | p^n x = 0 \text{ for some } n \in \mathbb{N}_0\}$. Let G and H be torsion groups. $G \cong H$ iff $G_p \cong H_p$ for each prime p.

Every finitely generated torsion-free abelian group is free abelian.

<u>Fundamental Theorem:</u>
Every finitely generated abelian group G is the direct sum of primary and infinite cyclic groups, and the number of summands depends only on G.

Simultaneous Bases:

Let H be a subgroup of finite index in a free abelian group of finite rank n. Then there exist bases $\{y_1, \ldots, y_n\} \in F$ and $\{h_1, \ldots, h_n\} \in H$ so that $h_i \in \langle y_i \rangle$.

8-3

Divisible Groups

An abelian group G is **divisible** (complete) if for any $a \in G$ and any natural number n, the equation

$$nx = a$$

has a solution. A group G is **reduced** if it contains no complete subgroup.

Injective property: Let D be a divisible group and A a subgroup of B. If $f: A \to B$ is a homomorphism, then f can be extended to a homomorphism $\varphi: B \to D$.

$$\begin{tikzcd}
A \arrow[r, hook, "i"'] \arrow[d, "f"'] & B \arrow[ld, dashed, "\varphi"] \\
D &
\end{tikzcd}$$

Note that the injective property is dual to the projective property in category theory, and a divisible group is like the dual of a free group.

- Every factor group of a divisible group is divisible.
- The direct sum of divisible groups is divisible.
- Any divisible subgroup of a divisible group G is a direct summand of G.

Every abelian group can be decomposed into the direct sum of a complete group and a reduced group

$$G = D \oplus R.$$

$\bar{A}$ is the sum of all divisible subgroups of G, the unique maximal divisible subgroup. (For comparison, G is an extension of by a torsion-free group, but may not be a direct summand.)

The **quasicyclic p-group** is the p-primary group $\mathbb{Z}(p^\infty) = \{\frac{a}{p^k} | a, k \in \mathbb{N}\}$ with addition modulo 1. Though it is not cyclic, each of its subgroups is.

Classification of Divisible Abelian Groups: Every divisible group is isomorphic to the direct sum of some number of additive groups of rational numbers and quasicyclic p-groups.

$$D \cong (\mathbb{Q}^+ + \cdots) + (p_1^\infty + \cdots) = H + F$$

where F is periodic and H is torsion-free and complete.

Pf. Write $D = tD \oplus V$, V torsion-free. A torsion-free divisible group can be viewed as a vector space over $\mathbb{Q}$, (in a torsion-free group, $ny = x$ has at most one solution for x, so division by natural numbers is well-defined) so is a direct sum of $\delta_\infty(D) = \dim_{\mathbb{Q}} D/tD$ copies of $\mathbb{Q}$. tD is a sum of p-primary groups: Letting $D[p] = \{x \in G | nx = 0\}$, the p-primary component G of is the sum of $\delta_p(D) = \dim_{\mathbb{Z}_p} D[p]$ copies of $\mathbb{Z}(p^\infty)$.

Two divisible groups are isomorphic iff they have the same values δ_p, δ_∞ (for each p).

Every abelian group can be embedded in a divisible abelian group. G is a direct summand of every abelian group that contains it as a subgroup iff it is divisible.

8-4 Pure Subgroups

A subgroup H of an abelian group G is a **pure** (isolated, serving) subgroup if for every $h \in H$ and every natural number n, the equation

$$nx = h$$

can be solved in H if it can be solved in G. (i.e.)
Ex. A direct summand is pure.

A subgroup B of a torsion group G is **basic** if

1. B is a direct sum of cyclic groups.
2. B is a pure subgroup of G.
3. G/B is divisible.

Every torsion group G has a basic subgroup, and so is the extension of a direct sum of cyclic groups by a divisible group.
Pf. Consider when G is p-primary. G has a pure nonzero cyclic subgroup $\langle y \rangle$- find an element $x = p^k y$ divisible by p^k but not p^{k+1} for some k. Take a maximal independent set X with $\langle X \rangle$ pure using Zorn's lemma. Then $G/\langle X \rangle$ is divisible.

H is a pure subgroup of a torsion-free abelian group G iff G/H is torsion-free.

8-5 Direct Sum Decompositions

Let G be a p-primary group.

- The elements of the same order form a **layer** of G. For a p-primary group, the elements of order p form the lowest layer.
- An element a has **height** h if the equation $p^k x = a$ has a solution when $k \leq h$. If it has a solution for all $k \geq 0$, a has infinite height.
- If every element of the lowest layer of a primary group G has infinite height, then G is divisible.

Kulikov's Criterion: A primary abelian group G is a direct sum of cyclic groups iff it is the union of an ascending sequence of subgroups

$$A_1 \subseteq A_2 \subseteq \cdots$$

such that the elements of each subgroup are of bounded height in G.
Pf. Build a well-ordered set of elements of order p until the group it generates contains the lowest layer of G. If it won't contain the lowest layer, take the one of smallest order not contained; get a contradiction.

Prüfer's First Theorem: (Prüfer-Baer) Every group with elements of bounded order is a direct sum of cyclic groups.
Pf. The only divisible group of bounded order is $\{0\}$. So G is basic.

If G is a p-primary group and , then G has

$$U(n, G) = \dim_{\mathbb{Z}_p} (p^n G \cap G[p])/(p^{n+1} G \cap G[p])$$

cyclic summands of order p^{n+1}. If G and H are direct sums of p-primary groups, $G \cong H$ iff they have the same **Ulm invariants**: $U(n, G) = U(n, H)$ for all n.

- Any 2 basic subgroups of a p-primary group are isomorphic.
- If tG has bounded order, then tG is a direct summand.
- A non-divisible torsion group has a p-primary cyclic direct summand, for some p.
- An indecomposable group is either torsion or torsion-free.

<u>Prüfer's Second Theorem:</u> Every countable primary group without elements of infinite height is a direct sum of cyclic groups.

- If an abelian group G is a direct sum of cyclic groups, then every subgroup H of G is also a direct sum of cyclic groups.
- If an abelian group is a direct sum of cyclic groups, it can be written so uniquely.
- Every abelian group is the union of a countable ascending sequence of direct sums of cyclic groups.

A **completely decomposable** (reducible) group can be written as a direct sum of groups of rank 1. It can be written this way uniquely.
The unrestricted direct sum of an infinite set of infinite cyclic groups is not completely decomposable.

8-6 Subgroups of $\mathbb{Q}$

The **rank** $\rho(G)$ of a torsion-free group G is the number of elements in a maximal independent subset. (Any two maximal independent subsets have the same number of elements.) The rank of an arbitrary abelian group is $\rho(G/tG)$.

Every torsion-free group G of rank n can be embedded in a divisible abelian torsion free group $\mathbb{Q}^n$. In particular, every torsion-free group of rank 1 is isomorphic to a subgroup of $\mathbb{Q}$.

A **characteristic** is an infinite sequence of whole numbers or ∞. Two characteristics a, b are equivalent (of the same **type**) if $a_n = b_n$ for all n except a finite number for which they are both finite.

Each abelian torsion-free group of rank 1 corresponds to a type: let a be any nonzero element, write the primes $p_1 < p_2 < \cdots$ in order, and let a_n be the maximum whole number for which $p_n^{a_n} x = a$ can be solved. They type determines G up to isomorphism.
Ex. The subgroup of generated by all the $\frac{1}{p_i^{a_i}}$ (when a_i finite) or $\left\{\frac{1}{p_i^k}\middle| k \in \mathbb{N}\right\}$ (when a_i infinite) has type $(a_1, a_2, \ldots)$.

9 Free Groups

9-1 Free Groups

Take 1:
A **free group** F has a **basis** X of generators that satisfy no relations other than implied by the group axioms. A word is a finite string of symbols from X or their inverses. The binary operation is juxtaposition. If xx^{-1} or $x^{-1}x$ appears in a word, it can be cancelled (into an equivalent word); a word is reduced if no cancellation can be made.
This defines a group because… (3 proofs)

1. There is only one reduced form of a word. (Induct on length. If w has xx^{-1}, then one of the x's is cancelled at some stage; cancelling it first has the same effect as cancelling xx^{-1}.) Products of equivalent words are equivalent, and the associative law holds.
2. Van der Waerden trick: For each $x \in X$, associate x, x^{-1} it with the functions $|x^a|, a = 1, -1$ defined by (all exponents below are ± 1).
$$|x^a|\left(x_1^{a_1}\cdots x_n^{a_n}\right)=\begin{cases}x^a x_1^{a_1}\cdots x_n^{a_n}, \text{if } x^a \neq x_1^{-a_1}\\ x_2^{a_2}\cdots x_n^{a_n}, \text{if } x^a = x_1^{a_1}\end{cases}$$
Let $\mathcal{F}$ be the subgroup of S_F generated by $\{|x|: x \in F\}$. Then $F \cong \mathcal{F}$ so F is a group.

Let F be the free group generated by X, and R a set of words of F. The group generated by X with the relations $r = 1, r \in R$ is defined as the quotient group F/R where R is the smallest *normal* subgroup of F containing R. (We impose extra conditions on the elements; and only conditions derived from those need to be satisfied.) The **presentation** of F/R is
$$\langle x_1, \ldots, x_n | r_1, \ldots, r_k\rangle$$
where x_i are the basis elements in X and r_i are the relations in R.

A free abelian group is the free group with the relations $xyx^{-1}y^{-1} = 1$ for all letters $x, y \in X$. Developing it from scratch, it is defined as above but the order of the letters is not important.

Take 2: (Category Theory viewpoint)
Mapping (Injective) property of the free group:
F is a free group with basis X iff for every group G and every function $f: X \to G$, there exists a unique homomorphism $\varphi: F \to G$ extending f:

$$\begin{tikzcd} F \arrow[rd, dashed, "\varphi"] & \\ X \arrow[u, hook, "\text{inclusion}"] \arrow[r, "f"] & G \end{tikzcd}$$

φ sends a word in X to the product of the images of the letters in the word.
Thus every group G is a quotient of a free group. (Pf. Associate each element in G with an element in X.)

Projective Property:
Let $\alpha: F \to C$ be a homomorphism and $\beta: B \to C$ be a surjective homomorphism. Then there exists a homomorphism $\gamma: F \to B$ such that $\beta\gamma = \alpha$:

$$\begin{tikzcd}
& F \arrow[d, "\alpha"] \arrow[dl, dashed, "\gamma"'] \\
B \arrow[r, two heads, "\beta"] & C
\end{tikzcd}$$

All the above properties hold if “free group” is replaced by “free abelian group” and “group” is replaced by “abelian group.”

Two free groups with bases X, Y are isomorphic iff $|X| = |Y|$. The **rank** of a free group is the number of elements in a basis. If H is a subgroup of the free abelian group F, $\text{rank}(H) \le \text{rank}(F)$.

__Pf.__ By considering X/X', Y/Y' we may assume that X, Y are abelian. $|Y| = \dim Y/pY = \dim X/pX = |X|$. For the last part, let $F = \langle x_k | k \in K\rangle$ (K well-ordered), $H_k' = H \cap \langle x_j | j < k\rangle, H_k = H \cap \langle x_j | j \le k\rangle$. Then $H_k = H_k'$ or $H_k = H_k' \oplus \langle h_k\rangle$. The h_k form a basis for H.

Free semigroups Σ are defined similarly, except there are no inverses and no cancellation. A congruence on a semigroup is an equivalence relation such that $a \equiv b, a' \equiv b' \Rightarrow aa' \equiv bb'$. The quotient semigroup $\Sigma/\equiv$ is defined by $[a][b] = [ab]$ ($[a]$ is the equivalence class of a.) The congruence generated by a subset $E \subseteq \Sigma \times \Sigma$ is the intersection of all congruences containing E. The quotient subgroup $\Sigma/\equiv$ has the presentation $(X | w_i = u_i \text{ for all } i \in I)$. If $(w, u) \in E$ then the group has to satisfy $w = u$; it satisfies only those relations implied by these. We cannot write them as $wu^{-1} = 1$ because inverses may not exist!

9-2 Todd-Coxeter Algorithm

The Todd-Coxeter Algorithm determines the operation of a finite group on the cosets of a subgroup.

Rules for operating on the right cosets of H:

1. The operation of each generator is a permutation.
2. The relations are the identity operator.
3. The generators of H fix H.
4. The operation is transitive.

To compute its group given its presentation $\langle x_1, \dots, x_n | r_1, \dots, r_k\rangle$:

1. Choose a subgroup H. For convenience, use the cyclic subgroup generated by one of the basis elements x. (It is possible to use {1} but this often takes too long.)
2. Let 1 represent the coset H.
3. Make tables, one for each relation. Across the top write the letters of the relation in order, and down the columns write the numbers representing cosets. Each letter sends the columns of numbers to the left of it to the column of numbers to the right. For example, here y sends 1 to 2, 2 to 3.

	letters	y	z …
Numbers representing cosets	1	2	…
	2	3	…

4. Start filling in the table with 1. Fill in spaces adjacent to numbers currently in the table. First, see if you can deduce what a letter sends a number to, using the tips below:
   a. x sends 1 to itself (rule 3), so write

	x	…

1 1

b. The entry in the last column of a table matches the first entry by rule (2).

c. If you know y sends $a \to b$ from somewhere else in the table, then you can fill in

$$\dfrac{\quad y \quad \dots}{a \quad ?} \quad \rightarrow \quad \dfrac{\quad y \quad \dots}{a \quad b}, \quad \dfrac{\quad y \quad \dots}{? \quad b} \quad \rightarrow \quad \dfrac{\quad y \quad \dots}{a \quad b}$$

The second implication follows from rule (1).

5. If you can't deduce what a letter sends a number to, then introduce a new number in the next column (for example, we set $y: 1 \to 2$ above). For each new number (coset), introduce a new row starting with that number.
6. Collapsing: If at any time $y: a \to b$ and $y: a \to c$, then set $b = c$ (erase all c's and replace them with b's.) Similarly if $y: a \to b$ and $y: c \to b$ then set $a = c$.
7. When all numbers in the table have been accounted for, and no more collapsing can take place, you're done. (Rule 4 says not to introduce any more cosets.) Find $|H|$ (somehow) and use $|G| = |H|[G:H]$ to find the order of G.
8. This procedure may not terminate.

9-3

Fundamental Group and Nielsen-Schreier Theorem

Algebraic Topology Background: The Fundamental Group

A **complex** is a family of nonempty subsets, **simplexes** (points, edges, triangles, tetrahedrons…), of a set of vertices so that each vertex is a simplex and each nonempty subset of a simplex is a simplex. A simplex with q+1 vertices is a q-simplex; a complex where each simplex has at most n vertices is a n-complex.

A 1-complex is simply a graph; terminology carries over from graph theory. Two paths are **homotopic**[6] (equivalent) if one can be obtained by the other by elementary moves- replacing (u,v)(v,w) by (u,w) where {u,v,w} is a simplex. $[a]$ denotes the equivalence class of path a.

The **fundamental group** of a complex K with basepoint v is

$$\pi(K, v) = \{[a] | a \text{ is a closed path at } v\}$$

Multiplication is defined by joining the paths together: $[a][b] = [ab]$. If K is connected, then the fundamental groups of the different vertices are isomorphic.

A **simply connected** complex is connected if it is connected and $\pi(K, v)$ only has the trivial path. A simply connected 1-complex is a tree.

Tietze's Theorem: If K is a connected complex and T is a maximal tree in K, then $\pi(K, w) \cong \mathcal{T}(K, T)$ where $\mathcal{T}(K, T)$ has the presentation:

Generators: Edges $(u, v) \in K$

Relations:

(a) $(u, v) = 1$ for $(u, v) \in T$

(b) $(u, v)(v, x) = (u, x)$ if $\{u, v, w\}$ is a simplex in K

Thus, if K is a connected 1-complex (graph), then it is a free group with rank equal to the number of edges not in T.

[6] I.e. One can be continuously deformed into the other (across the 2-simplex, or face).

K' is a **covering complex** of K if there exists a map $p: K' \to K$ sending simplexes to simplexes, and such that for each simplex s in K, $p^{-1}(s)$ is a *disjoint* union of simplexes.

Nielsen-Schreier Theorem: Every subgroup of a free group is free.
Pf. 1 (Sketch) The fundamental group of a graph K with n cycles meeting at a common point is the free group F with n generators. A subgroup H of F corresponds to a subgroup π of $\pi(K, w)$, create a covering complex K' with fundamental group H as follows:

1. The vertices of K' are equivalence classes of paths in K starting at w, where two paths are equivalent if joining their ends gives a path in π: $a \equiv b$ iff they have the same end point and $[ab^{-1}] \in \pi$ (b^{-1} is the path b in the opposite direction).
2. Two vertices are connected iff there are paths corresponding to the vertices that differ by a path wholly contained in one simplex (i.e. $b = aa^{'}$, $a^{'}$ a path in one simplex).
3. The only "meaningful" closed paths in K' are created by elements that project to π, the paths corresponding to elements of H.

Since K' is a graph, its fundamental group is free.
Pf. 2 (Sketch) The **Cayley graph** of a group G with respect to the generators X is the directed graph with vertices the elements of G, with an edge from g to h if there exists $x, h = gx$ for some $x \in X$. An automorphism of a graph is a bijective map on the vertices (and edges) sending adjacent vertices to adjacent vertices. Define a metric on the graph: $d(x, y)$ is the minimal number of edges in a path from x to y; this extends to subsets.
A group G acts freely on a graph (as automorphisms) if the only element of G fixing a vertex or reversing an edge is trivial. Any group acting freely on a locally finite tree (i.e. each vertex has finite degree) is a free group:

1. Take vertex ω, order others in increasing distance. Put ω in Γ_ω and at stage k, put vertex ω_k in if it is adjacent to $\omega_j, j < k$ with $\omega_j \in \Gamma_\omega$, and ω_k is not in the G-orbit of an element of Γ_ω. Γ_ω is a subtree with one vertex in each G-orbit.
2. $\Gamma_a \cap \Gamma_b = \phi$ when they are distinct.
3. $T = \{t \in G | d(\Gamma, t\Gamma) = 1\} = T^{-1}$ can be written as a disjoint union $R \cup R^{-1}$. R is a set of generators for G; if a relation that's not supposed to be 1 in the free group is 1, then there is a cycle, contradiction.

For G free, G acts freely on its Cayley graph, so a subgroup does also, and is free.

If F is a free group of rank n, and H is a subgroup of finite index j, then $\text{rank}(H) = jn - j + 1$.
Let H be a subgroup of F. A **Schreier transversal** of H in F is a right transversal S such that whenever the reduced word $x_1^{\varepsilon_1} x_2^{\varepsilon_2} \cdots x_n^{\varepsilon_n}$ ($x_i \in X, \varepsilon_i = \pm 1$) lies in S, then so does every initial segment $x_1^{\varepsilon_1} x_2^{\varepsilon_2} \cdots x_k^{\varepsilon_k}$. There exists a Schreier transversal of H in F, and given any Schreier transversal $S = \{l(Ha) | a \in F\}$, then the set of $h_{a,x} = l(Ha)xl(Hax)^{-1}, x \in X$ not equal to 1 form a basis of H.

9-4 Free Products and Amalgams

The **free product** of groups $*_{i \in I} A_i$ is the group generated by the groups A_i when the elements in the different groups are considered to be distinct and which satisfies no relations than those relations in each A_i. In other words, it is the set of all words with letters that are the elements of the A_i, with juxtaposition as multiplication, and where 2 adjacent

letters can be combined only if they are in the same group A_i.
In category theory terms, the free product is the (unique) coproduct of the groups A_i, i.e. it satisfies the *Universal Mapping Property*: The free product is a group P with homomorphisms $i_j: A_j \to P$ (imbeddings) so that for every group G and every family of homomorphisms $f_j: A_j \to G$ there exists a unique homomorphism f such that $f i_j = f_j$ for all j.

$$\begin{tikzcd}
& P \arrow[d, dashed, "f"] \\
A_j \arrow[ur, "i_j"] \arrow[r, "f_j"] & G
\end{tikzcd}$$

Each $g \in *_{i\in I} A_i$ has a unique factorization called the normal form:

$$g = a_1 \cdots a_n$$

where adjacent factors lie in distinct $A_i - \{1\}$.

Each graph is the fundamental group of some 2-complex.
<u>Pf.</u> Take a presentation $\langle X|\Delta\rangle$, take a graph of $|X|$ cycles with a common point, each relation is a closed path. Drape a triangulated 2-D cell over each such path. Proof uses Seifert-van Kampen's Theorem from algebraic topology.

<u>Kurosh Theorem:</u> Let $G = *_{i\in I} A_i$. If $H \subseteq G$ is a subgroup, then $H = F * (*_{j\in J} H_j)$ for some index set J, where F is a free group and each H_j is a conjugate of some A_i.

- If each A_i is torsion, and H is torsion-free, then H is a free group.
- If H is finite, it is conjugate to a subgroup of some A_i. Every element of finite order is conjugate to an element of finite order in some A_i.

Let A_1, A_2 be groups having isomorphic subgroups B_1, B_2, respectively, and let $\theta: B_1 \to B_2$ be an isomorphism. The **amalgam** is $A_1 *_\theta A_2 = A_1 * A_2/N$, where N is the normal subgroup generated by $\{b\theta(b^{-1}): b \in B_1\}$. The amalgam is the (unique) pushout of the diagram

$$\begin{tikzcd}
B_1 \arrow[r, "i_1"'] \arrow[d, "i_2\theta"'] & A_a \\
A_2
\end{tikzcd}$$

The i_1, i_2 are the inclusion maps of $B_1 \to A_1, B_2 \to A_2$. The pushout is the category theory generalization of union.

Choose a left transversal l of B_i in A_i, with $l(1) = 1$. Each element $wN \in A_1 *_\theta A_2$ has a unique **normal form** $F(w)N = wN$, where

$$F(w) = l(a_1)l(a_2)\cdots l(a_n)b, b \in B_1$$

and $l(a_j)$ lie in transversals of B_{i_j} in A_{i_j}, and adjacent $l(a_j)$ lie in different A_i.

<u>Torsion Theorem:</u> An element in $A_1 *_\theta A_2$ has finite order iff it is conjugate to an element of finite order in A_1 or A_2.

9-5

HNN Extensions

HNN Extensions

1. Let G be a group and let $\varphi: A \to B$ be an isomorphism between subgroups A and B

of G. Then the **HNN extension** $G\ \Omega_{\varphi}\ A$ with base G and stable letter p is the group with the presentation $\langle G; p | p^{-1}ap = \varphi(a) \text{ for all } a \in A\rangle$. This group contains G.

2. Let $\varphi: A_i \to B_i$ be isomorphisms, with $\varphi(a_{ij}) = b_{ij}$ (for some index sets I, J). The group
$$E^{\Omega} = \langle E; p_i, i \in I | p_i^{-1} a_{ij} p_i = b_{ij} \text{ for all } i, j\rangle$$
is an HNN extension with base E and stable letters p_i.

Visualize the HNN extension of a fundamental group as the fundamental group after topologically “adding a handle” to connect two subcomplexes.

We say that two words are congruent if they have exactly the same spelling before simplifying. If ω is a word on $X = \{x_i | 1 \leq i \leq n\}$ then β is a subword if there are words α, γ so $\omega \equiv \alpha\beta\gamma$. A **pinch** in a HNN extension is a word of the form $w \equiv p_i^e g p_i^{-e}$, where either $e = -1, w \in A_i \subseteq A$ or $e = 1, w \in B_i \subseteq B$.

Britton’s Lemma: If ω is a word with $\omega = 1$ in E^{Ω} containing at least one stable letter, then ω has a pinch as a subword.

A p-reduced word contains no pinch in the form $p^e g p^{-e}$ as a subword.
Let E^{Ω} be a HNN extension with base E and stable letter p. Then each word on $\{X, p\}$ has a unique normal form: a reduced word in the form $\omega_0 p^{e_1} \omega_1 \cdots p^{e_n} \omega_n$.

9-6

The Word Problem, Decidability of Group Theory Problems

Does there exist an algorithm that can always decide (in finite time) whether two words in a finitely presented group are the same element? NO. (Novikov-Boone-Britton)

Essentially every algorithm can be run on a Turing machine. The word problem for semigroups Γ (Markov-Post) yields a negative answer because the words can be viewed as configurations on the tape in a Turing machine, and (with special choice of semigroup) the operation of the Turing machine corresponds to “simplifying” the word. By a “diagonalization” argument there exists a recursively enumerable (re) subset S of $\mathbb{N}$ (there’s a Turing machine T* that will stop whenever it’s fed an element of S) that is not recursive ($\mathbb{N} - S$ is not recursively enumerable, i.e. no algorithm is guaranteed to say if an element is in S). Adapting this gives a non-recursive set $\{\omega | \omega = \omega_0 \text{ in } \Gamma\}$. An semi-explicit counterexample for groups depending on T* can be given. It is built from multiple HNN extensions to take advantage of Britton’s lemma (pinches). Boone’s lemma says $A(\Sigma) = B(\Sigma) \Leftrightarrow \Sigma^* = q$ for certain words depending on a word Σ; the connection between these two diagrams can be visualized by supplying relator polygons using the theorem below. Σ^* is a positive word, so apply the word problem for semigroups to see that there is no decision process for $A(\Sigma)B(\Sigma)^{-1}$.

Each relation in a presentation of a group can be depicted by a relator polygon, where the edges are labeled with the generators appearing in the relation in order going counterclockwise and arrows point with/ against the flow depending on whether its exponent is 1 or -1.

Fundamental Theorem of Combinatorial Group Theory: Let G have a finite presentation $\langle X | \Delta\rangle$ where

1. Each relation is cyclically reduced (no cyclic permutation has a subword in the form $xx^{-1}, x^{-1}x, x \in X$).
2. If $\delta \in \Delta$, then $\delta^{-1} \in \Delta$ and every cyclic permutation of δ is in Δ.

If ω is a cyclically reduced word, then $\omega = 1$ iff there is a diagram having a boundary word ω and whose regions are relator polygons of relations in Δ. Two elements ω, ω' are conjugate in G iff the annulus with outside/ inside polygon corresponding to ω/ω' can be subdivided into relator polygons.

R is **recursively presented** if it has a presentation

$$R = \langle u_1, \dots, u_m | \omega = 1, \omega \in E \rangle$$

where E is recursively enumerable.

Higman Imbedding Theorem: Every recursively presented group can be imbedded in a finitely presented group.

Every countable group can be imbedded in a group H having two generators.

There exists a universal finitely presented group, a finitely presented group containing a copy of every finitely presented group as a subgroup.

A property M of finitely presented groups is a **Markov property** if

1. Every group isomorphic to a group with property M has property M.
2. There exists a finitely presented group with property M.
3. There exists a finitely presented group that cannot be imbedded in a finitely presented group with property M.

If M is Markov, there does not exist a decision process which will determine for an arbitrary finite presentation, whether the group has property M. This includes:

1. Order 1
2. Finite
3. Finite exponent
4. P-group
5. Abelian
6. Solvable
7. Nilpotent
8. Simple
9. Torsion
10. Torsion-free
11. Free
12. Having a solvable word problem
13. Having a solvable conjugacy problem

9-7

The Burnside Problem

General: If *G* is a periodic group, and *G* is finitely generated, then is *G* necessarily a finite group? NO.

If *G* is a finitely generated group with exponent *n*, is *G* necessarily finite? NO.

Note: It suffices to check whether the **free Burnside group** $B(m,n) = \langle x_1, \dots, x_m | x_1^n = \cdots = x_m^n = 1 \rangle$ is finite. It is finite for $n = 1,2,3,4,6$.

Ex. $|B(m,3)| = 3^{\binom{r}{3}+\binom{r}{2}+r}$. Every commutator of weight 4 is the identity.

10 Linear Groups

10-1 Classical Groups

Name	Group	Definition
General linear group	$GL_n(F)$	Set of invertible matrices
Special linear group	$SL_n(F)$	$\{P \in GL_n(F) \| \det P = 1\}$
Projective group	$PSL_n(F)$	$SL_n(F)/\{\pm I\}$
Orthogonal group	O_n	$\{P \in GL_n(\mathbb{R}) \| P^T P = I\}$
Special orthogonal group	SO_n	$\{P \in O_n \| \det P = 1\}$
Unitary group	U_n	$\{P \in GL_n(\mathbb{C}) \| P^* P = I\}$
Special unitary group	SU_n	$\{P \in U_n \| \det P = 1\}$
Symplectic group	SP_{2n}	Preserve the skew symmetric form $S = \begin{bmatrix} 0 & I \\ -I & 0 \end{bmatrix}$; $\{P \in GL_{2n}(\mathbb{R}) \| P^T SP = S\}$
Lorentz group for (p,m)=(3,1)	$O_{p,m}$	Preserves the bilinear form with signature (p,m)

A **homeomorphism** $\varphi: X \to Y$ is a continuous bijective map whose inverse function is also continuous. A **manifold** of dimension d is a set where every point has a neighborhood homeomorphic to an open set of $\mathbb{R}^d$.

10-2 General Linear Group

If G is an elementary abelian p-group of order p^n, then $\operatorname{Aut} G \cong \mathrm{GL}_n(\mathbb{F}_p)$, since G has the structure of a vector space and homomorphisms correspond to linear transformations.

$$\left|\mathrm{GL}_n(\mathbb{F}_q)\right| = \prod_{k=0}^{n-1} q^n - q^k = q^{\frac{n(n-1)}{2}}(q^n - 1)\cdots(q - 1)$$

$$\left|\mathrm{SL}_n(\mathbb{F}_q)\right| = \prod_{k=1}^{n-1} q^n - q^k = q^{\frac{n(n-1)}{2}}(q^n - 1)\cdots(q^2 - 1)$$

- The **standard Borel subgroup** is the subgroup B of all (invertible) upper triangular matrices in the general linear group G.
- A matrix is **upper unitriangular** if it is upper triangular and all entries on the diagonal are 1. They form a group U.
- A matrix is **unipotent** if its characteristic polynomial is $(\lambda - 1)^n$.[7]
- T is the group of all diagonal matrices.
- The **Weyl subgroup** W is the set of all permutation matrices. $W \cong S_n$
- A **transvection** (elementary matrix of the first type) $X_{ij}(a)$ is a matrix with 1's along the diagonal and entry (i,j) equal to a. (Multiplication by a transvection adds a multiple of a row/ column to another.) A **root subgroup** is $\{X_{ij}(a)\}$ for some fixed i,j.

<u>Bruhat Decomposition:</u> $G = BWB$, and G is the disjoint union of the $n!$ double cosets

[7] Or $(1 - \lambda)^n$, depending on how you define characteristic polynomial.

$BwB, w \in W$.

The general linear group is generated by the set of invertible diagonal matrices and all transvections; the special linear group is generated by transvections.

Parabolic subgroups
A **flag** on F^n is an increasing chain of subspaces $0 \subset W_1 \subset \cdots \subset W_r = F^n$. A complete flag has n subspaces- one for each dimension 1 to n. The standard flag has $W_i = \mathrm{span}(e_1, \dots, e_i), 1 \le i \le n$. A subflag is a flag containing some of the W_i. G acts on the (complete) flags by $g(W_1, \dots, W_r) = (gW_1, \dots, gW_r)$. For the complete flags, the action is transitive and the stabilizer of the standard flag is the Borel subgroup.

$B = U \rtimes T$ (triangular = upper unitriangular $\rtimes$ diagonal)
Kolchin's Theorem: Any unipotent subgroup of G is conjugate with a subgroup of U.

A **parabolic subgroup** P is the stabilizer of some flag on F^n. Choose subspaces so $W_i = W_{i-1} \oplus Y_i$. The unipotent radical of P is the subgroup U_P of matrices that induce the identity transformation on each W_i/W_{i-1}. A Levi complement L_P of U_P is the common stabilizer of the Y_i; it is isomorphic to $\mathrm{GL}_{y_1}(F) \times \cdots \times \mathrm{GL}_{y_r}(F)$, where $y_i = \dim W_i - \dim W_{i-1}$.

$$P = U_P \rtimes L_P, P = N_G(U_P)$$

A **staircase group** is a parabolic subgroup of G stabilizing some subflag of the standard flag.
Ex. The staircase group of $0 \subset W_2 \subset W_3 \subset W_6$ consists of matrices of the form $\begin{bmatrix} * & * & * & * & * & * \\ * & * & * & * & * & * \\ 0 & 0 & * & * & * & * \\ 0 & 0 & 0 & * & * & * \\ 0 & 0 & 0 & * & * & * \\ 0 & 0 & 0 & * & * & * \end{bmatrix}$, the unipotent radical $\begin{bmatrix} 1 & 0 & * & * & * & * \\ 0 & 1 & * & * & * & * \\ 0 & 0 & 1 & * & * & * \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}$, and a Levi complement $\begin{bmatrix} * & * & 0 & 0 & 0 & 0 \\ * & * & 0 & 0 & 0 & 0 \\ 0 & 0 & * & 0 & 0 & 0 \\ 0 & 0 & 0 & * & * & * \\ 0 & 0 & 0 & * & * & * \\ 0 & 0 & 0 & * & * & * \end{bmatrix}$.
The only subgroups of G containing B are the staircase groups.

The center Z of GL is the multiples of the identity matrix, and the center of SL is $Z \cap SL$.

10-3

SU_2 and SO_3

SU_2 contains exactly the matrices in the form

$$P = \begin{bmatrix} a & b \\ -\bar{b} & \bar{a} \end{bmatrix}, \bar{a}a + \bar{b}b = 1$$

or

$$P = \begin{bmatrix} x_0 + x_1 i & x_2 + x_3 i \\ -x_1 + x_2 i & x_0 - x_1 i \end{bmatrix}, x_0^2 + x_1^2 + x_2^2 + x_3^3 = 1$$

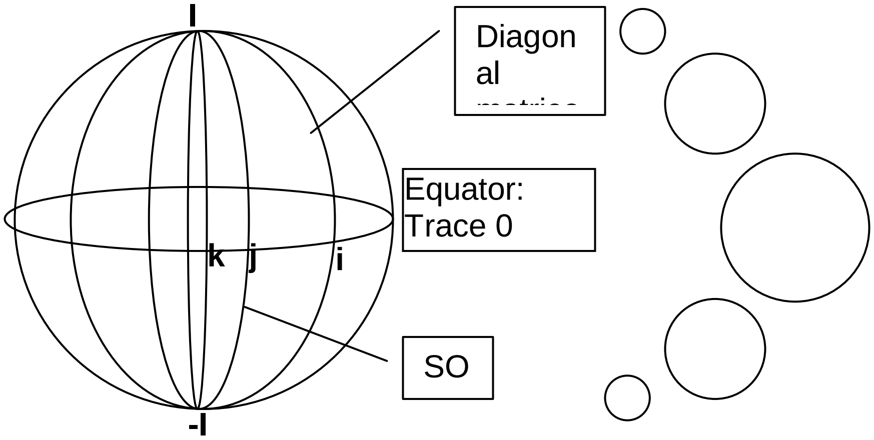
With the correpondence

$$I=\begin{bmatrix}1&0\\0&1\end{bmatrix}, \mathbf{i}=\begin{bmatrix}i&0\\0&-i\end{bmatrix}, \mathbf{j}=\begin{bmatrix}0&1\\-1&0\end{bmatrix}, \mathbf{k}=\begin{bmatrix}0&i\\i&0\end{bmatrix}$$

this becomes the quaternion algebra.

The matrices in SU$_2$ correspond to points on the unit 3-sphere $\mathbb{S}^3$ in $\mathbb{R}^4$.

1. The **latitudes** of $\mathbb{S}^3$ are given by
$$x_0 = c, x_1^2 + x_2^2 + x_3^3 = 1 - c^2$$
Each latitude is a 2-dimensional sphere.
A latitude corresponds to the conjugacy class of matrices with trace 2c.
    a. The **equator** $\mathbb{E}$ is the latitude with $x_0 = 0$; it contains matrices with trace 0. Each matrix on the equator is associated with the unit vector $(x_1, x_2, x_3)^T \in \mathbb{R}^3$.
2. The **longitudes** of $\mathbb{S}^3$ are
$$W \cap \mathbb{S}^3, W \text{ a } 2-\text{dimensional subspace of } \mathbb{R}^4 \text{ containing I}$$
They have the parameterization $l(\theta) = \cos\theta\, I + \sin\theta\, A, A \in \mathbb{E}$.
The longitudes are conjugate subgroups of SU$_2$.



Conjugation by an element of SU$_2$ rotates the equator (a 2-D sphere).

For an element P in SU$_2$, let γ(P) be the (matrix corresponding to) this rotation (with respect to the basis i, j, k). Then the **spin homomorphism** $\gamma: SU_2 \to SO_3$ is surjective with kernel $\{\pm I\}$.

If $P = \cos\theta\, I + \sin\theta\, A, A \in \mathbb{E}$, then γ_P has spin (A,2θ).

γ is a 2-to-1 mapping (antipodal, or opposite points have the same image) so SU$_2$ is a double covering of SO$_3$:

$$\mathrm{SO}_3 \cong \mathrm{SU}_2/\mathrm{Z} = \mathrm{SU}_2/\{\pm \mathrm{I}\}$$
$$\mathrm{SO}_3 \cong \mathbb{P}^3 \text{ (projective } 3-\text{space)}$$

Pf. Define a bilinear form for elements of the equator as follows: let $\langle \mathrm{U}, \mathrm{V}\rangle = \mathrm{u}_1\mathrm{v}_1 + \mathrm{u}_2\mathrm{v}_2 + \mathrm{u}_3\mathrm{v}_3$, where $\mathrm{U} = \mathrm{u}_1\mathrm{i} + \mathrm{u}_2\mathrm{j} + \mathrm{u}_3\mathrm{k}, \mathrm{V} = \mathrm{v}_1\mathrm{i} + \mathrm{v}_2\mathrm{j} + \mathrm{v}_3\mathrm{k}$, i.e use the standard dot product with the coordinates. Then $\langle \mathrm{U}, \mathrm{V}\rangle = -\frac{1}{2}\mathrm{trace}(\mathrm{UV})$. $\gamma(\mathrm{P})$ is orthogonal because $\langle \gamma_\mathrm{P}\mathrm{U}, \gamma_\mathrm{P}\mathrm{V}\rangle = \langle \mathrm{U}, \mathrm{V}\rangle$. The determinant of γ_P is always 1 by continuity. So the image is in SO_3. Just verify $\gamma_\mathrm{P}\mathrm{j} = \cos 2\theta\, \mathrm{j} + \sin 2\theta\, \mathrm{k}$ for $\mathrm{P} = \cos\theta\, \mathrm{I} + \sin\theta\, \mathrm{i}$; (2) holds by conjugation.

10-4 One-Parameter Groups

Recall (see Linear Algebra, 9.1)

$$e^{At} = \sum_{i=0}^{\infty} \frac{(At)^n}{n!}$$

1. The series converges for any A.
2. If A and B commute, $e^{A+B} = e^A e^B$. In particular, $e^{t_1 A} e^{t_2 A} = e^{(t_1+t_2)A}$.
3. $\frac{d}{dt} e^{tA} = Ae^{tA}$

A **one-parameter group** is a differentiable homomorphism

$$\varphi: \mathbb{R}^+ \to GL_n$$

These homomorphisms are $\varphi(t) = e^{At}$, for some $A \in GL_n(\mathbb{C})$, and the images of one-parameter groups are exactly those in the form $\{e^{At} | t \in \mathbb{R}\}$.

__Pf.__ Let $A = \left.\frac{d\varphi}{dt}\right|_{t=0}$. Then $\frac{d\varphi}{dt} = A\varphi$.

Finding one-parameter groups in a subgroup G of GL$_n$:

1. Require that $e^{At} \in G$ for all t. Differentiate to get possibilities for

$$A = \left.\left(\frac{d}{dt} e^{At}\right)\right|_{t=0}$$

2. Check to see whether all these matrices A work.

Examples:

Group G	Property Used	One-parameter groups in G are e^{At} with A:
O_n	If A is real skew-symmetric, then e^A is orthogonal.	Real skew-symmetric
U_n	If A is skew-Hermitian, then e^A is unitary.	Skew-Hermitian
SL_n	$e^{\text{trace }(A)} = \det e^A$	Trace zero matrix

10-5 Lie Algebras

A **Lie algebra** is a real vector space with a bracket operation $V \times V \to V$ denoted by $[v, w]$ such that

1.	$[cv_1 + v_2, w] = c[v_1, w] + [v_2, w]$ $[v, cw_1 + w_2] = c[v, w_1] + [v, w_2]$	Bilinearity (one implies the other)
2.	$[v, w] = -[w, v]$	Skew symmetry
3.	$[u, [v, w]] + [v, [w, u]] + [w, [u, v]] = 0$	Jacobi Identity

A vector v is tangent to a subset S of $\mathbb{R}^k$, or a set of matrices, at a point (matrix) x if there is a differentiable path φ in S such that $\left.\frac{d\varphi}{dt}\right|_{t=t_0} = v$ and $\varphi(t_0) = x$ for some t_0. The **Lie algebra** of a subgroup $G \subset GL_n(\mathbb{C})$ is the set of tangent vectors to G at I, with the bracket defined by

$$[A, B] = AB - BA$$

A is in the Lie algebra of G iff e^{At} is a one-parameter subgroup in G.

10-6 Simple Linear Groups

Left multiplication (translation) m_P by an element P of a matrix group G is a homeomorphism. Homogeneity is the property that the group “looks the same” everywhere.

A subgroup of $GL_n(\mathbb{R})$ which is a closed subset of $GL_n(\mathbb{R})$ is a manifold.
Ex. The orthogonal group O_n is a manifold of dimension $\frac{n(n-1)}{2}$, using the fact that the exponential e^A maps a small neighborhood U of 0 in $\mathbb{R}^{n\times n}$ homeomorphically to a neighborhood of I in $GL_n(\mathbb{R})$.

If $H \subseteq G$ is a subgroup of the path-connected matrix group G that contains a nonempty open subset U, then $H = G$.
Pf.

1. The union of cosets of U in H is H. Since the union of an arbitrary number of open sets is open, H is open.
2. A path connected set is not the disjoint union of nonempty open sets: If $S = U_0 \cup U_1$ and p is a path connecting U_0 and U_1, $\sup\{x|p(x) \in U_0\}$ can’t be in either set.
3. G is the union of cosets of H, so $G = H$.

$SO_3 \cong SU_2/\{\pm 1\}$ is a simple group.
Pf. Let N be a normal subgroup of SO_3

1. For $P_0 \in N$, the conjugacy class (latitude) C of P_0 is in N.
2. Take a nontrivial path $P(t)$ from P_0 to P_1 in C. Let $Q(t) = P(t)P_0^{-1}$. Then Q is in G and goes from I to some other matrix. Q goes through all conjugacy classes sufficiently close to I, so N contains a neighborhood of I and $N = SO_3$.

If q is a power of a prime,

1. $|SL_2(\mathbb{F}_q)| = q^3 - q$
2. $|PSL_2(\mathbb{F}_q)| = q^3 - q$ if q is a power of 2
3. $|PSL_2(\mathbb{F}_q)| = \frac{1}{2}(q^3 - q)$ else

Some relationships: $PSL_2(\mathbb{F}_2) \cong S_3, PSL_2(\mathbb{F}_3) \cong A_4, PSL_2(\mathbb{F}_4) \cong PSL_2(\mathbb{F}_5) \cong A_5, PSL_2(\mathbb{F}_9) \cong A_6, PSL_2(\mathbb{F}_7) \cong GL_3(\mathbb{F}_2)$[8]

If F is a field of order at least 4,

1. The only normal subgroup of $SL_2(F)$ is the center $Z = \{\pm 1\}$.
2. $PSL_2(F)$ is simple.

Pf. Let N be a normal subgroup.

1. Choose s so that $s^2 \neq \pm 1,0$
2. For any $A \in N$, there is a matrix $P \in SL_2(F)$ so that the commutators $APA^{-1}P^{-1} \in N$ has eigenvalues $s, \frac{1}{s}$.
3. The matrices having eigenvalues $s, \frac{1}{s}$ are in a single conjugacy class in SL_2 contained in N.
4. $\begin{bmatrix}1 & x\\ 0 & 1\end{bmatrix}, \begin{bmatrix}1 & 0\\ x & 1\end{bmatrix} \in N$
5. These matrices generate SL_2.

[8] See AMM 116/8 (10/2009), pg. 727

A **complex algebraic group** is a subgroup of $GL_n(\mathbb{C})$ that is the locus of complex solutions to a finite system of complex polynomial equations in the matrix entries.

<u>Cartan's Theorem:</u>

1. The centers of $SL_n(\mathbb{C}), SO_n(\mathbb{C}), SP_{2n}(\mathbb{C})$ are finite cyclic groups.
2. $SL_n(\mathbb{C})/Z, SO_n(\mathbb{C})/Z, SP_{2n}(\mathbb{C})/Z$ are path-connected complex algebraic groups. They are simple except for $SO_2(\mathbb{C}), SO_4(\mathbb{C})$.
3. The other simple, path connected complex algebraic groups, the exceptional groups, are in one of five isomorphism classes.

Pf. Based on a classification of Lie algebras.

Exercises

1. Let G be an elementary abelian p-group of order $n \leq p$. Show that G has no automorphism of order p^2.

11 Representation Theory

11-1 The Basics

Groups are assumed to be finite unless otherwise specified. $M_n(F)$ denotes the algebra of $n \times n$ matrices over F.

View 1: Representations and Characters

- A **representation** of a group G is a homomorphism from G to the general linear group $\mathrm{GL}_n(F)$ or $\mathrm{GL}(V)$ (the first sends G to matrices with entries in the field F; the second sends G to linear transformations from the vector space V to itself; they are equivalent since linear transformations correspond to matrices). Two representations $\rho: G \to \mathrm{GL}(V)$ and $\rho^{'}: G \to \mathrm{GL}(V^{'})$ are **isomorphic** if there exists a G-invariant linear transformation $T: V \to V^{'}$:
$$T(\rho_g v) = \rho_g^{'} T(v) \text{ for all } g \in G, v \in V$$
- The **character** of the representation is the function
$$\chi(g) = \mathrm{trace}(\rho_g).$$
- A vector is **G-invariant** if $\rho_g v = v$ for all $g \in G, v \in V$, and a subspace W is G-invariant if $\rho_g W \subseteq W$ for all $g \in G$ (equality actually holds by invertibility).
- A representation $\rho: G \to \mathrm{GL}(V)$ is the **direct sum** $\alpha \oplus \beta$ of two representations α, β if there are G-invariant subspaces W_1, W_2 such that $V = W_1 \oplus W_2$ and α, β are the projections of ρ onto W_1, W_2. With suitable (change of) basis, all the matrices in the image of ρ will be in the form $\begin{bmatrix} A_g & \mathcal{O} \\ \mathcal{O} & B_g \end{bmatrix}$, where $A_g = \alpha(g), B_g = \beta(g)$.
- A **reducible** representation has a proper G-invariant subspace. (This is equivalent to having nontrivial direct sum decomposition.) If G *is* a linear group, we simply say G is reducible (the representation being the identity). A character is reducible if its corresponding representation is.

View 2A: Linear Actions and the Group Ring

- A **linear action** of G on a vector space V over F is a group operation satisfying:
  - $g(v + w) = gv + gw$ for all $g \in G$ and $v, w \in V$.
  - $g(cv) = c(gv)$ for all $g \in G, c \in F, v \in V$.
- $g \in G$ operates *directly* on the vector space, while above, the representation ρ_g operates on the vector space. Less wordy!
- The **group ring** RG (R a ring) is the set of all linear combinations of elements of G with coefficients in the field R. The elements of G form a basis for the ring. Multiplication is defined like polynomial multiplication:
$$\left(\sum_{g \in G} a_g g\right)\left(\sum_{g \in G} b_g g\right) = \left(\sum_{g,h \in G} a_g b_h gh\right)$$
If R is a field F, then FG is a group algebra.
- The group ring acts on V by extending the linear action of G. Thus we say that V is a RG-**module**. The group ring acts like matrices/ linear transformations acting on the vector space V. The distinct modules correspond to the different representations.
- The **character** of a FG-module U is the function χ_U with $\chi_U(g)$ defined as the trace of the linear transformation of left multiplication by g. A character is reducible if its corresponding module is simple.

Some Algebra Background

- A module is…
  - **Simple** if it has no proper submodules.
  - **Semisimple** if it is the direct sum of simple modules.
- An algebra is…
  - **Simple** if it has no proper two-sided ideals. (A two sided ideal of A is a subset M so that $aMb \subseteq A$ for any $a, b \in A$.) Note that A may be simple as an algebra, but not as an A-module.
  - **Semisimple** if all nonzero A-modules are semisimple. Equivalently, A is semisimple as an A-module.
- A **R-module homomorphism** is a homomorphism $\varphi: M \to N$ such that $\varphi(rm) = r\varphi(m)$ for any $r \in R, m \in M$. $\mathrm{Hom}_R(M, N)$ is the set of R-module homomorphisms and $\mathrm{End}_R(M)$ is the set of R-module endomorphisms ($\varphi: M \to M$). $\mathrm{End}_R(M)$ forms a division algebra for composition replacing multiplication.
- The **direct sum** of modules $M_1 \oplus M_2$ is the Cartesian product with componentwise addition and scalar multiplication.
- The **direct sum** of algebras $A_1 \oplus A_2$ is the Cartesian product with componentwise addition, scalar multiplication, *and multiplication*. Note that $a_1 \in A_1, a_2 \in A_2$ implies $a_1 a_2 = 0$. When they are matrix algebras, imagine $A_1 \oplus A_2$ as $\left\{\begin{bmatrix} B_1 & \mathcal{O} \\ \mathcal{O} & B_2 \end{bmatrix} \middle| B_1 \in A_1, B_2 \in A_2\right\}$.

11-2

The Bulk of It

Modules, Linear Actions	Representations and Characters
G acts linearly on V.	The representations of G act on V.
Group ring (ex. $\mathbb{C}G$) acts on V.	The matrices (or linear transformations) in $\mathrm{span}\{\rho_g \mid g \in G\}$ act on V.
R-module homomorphism invariant under R	Isomorphism of representations invariant under G.
Simple module has no proper submodule.	Irreducible representation has no proper G-invariant subspace.
A module is the direct sum of simple submodules.	V is the direct sum of minimal G-invariant subspaces. This corresponds to a representation being the direct sum of irreducible representations.
Schur's Lemma: If φ is a homomorphism between simple R-modules, then $\varphi = 0$ or φ is an isomorphism. *Pf.* $\ker\varphi = 0 \text{ or } M$.	Schur's Lemma: If ρ, ρ' are irreducible representations on V, V', and $T: V \to V'$ is a G-invariant linear transformation, then $T = 0$ or T is an isomorphism.
Special case: If S is a simple A-module, $\mathrm{End}_R(S) = \{\varphi(s) = cs \text{ for some } c\}$.	If ρ is an irreducible representation on V, then any G-invariant linear operator $T: V \to V$ is in the form $T = cI$.
Maschke's Theorem: Suppose F has characteristic 0 or coprime to $\lvert G\rvert$. If U is a FG-module, and V is a FG-submodule, then V is a direct summand of U. Thus, every FG-module is semisimple (a direct	Maschke's Theorem: Suppose F has characteristic 0 or coprime to $\lvert G\rvert$, and ρ is a representation on V. Then V is a direct sum of G-invariant subspaces and ρ is a direct

sum of simple modules) *Pf.* Take an "average": Write $U = V \oplus W$, and let $\pi: U \to V$ be the projection along W. Define $\pi^{'}(u) = \frac{1}{\lvert G\rvert}\sum_{g\in G} g\pi(g^{-1}u)$; then $U = V \oplus \ker \pi'$ as modules.	sum of irreducible representations corresponding to these subspaces. *Pf.* Take the "average" to get a G-invariant inner product. Take an arbitrary inner product {-,-} and let $\langle v, w\rangle = \frac{1}{\lvert G\rvert}\sum_{g\in G}\{gv, gw\}$. Then $V = W \oplus W^{\perp}$ using the new inner product, with $W^{\perp}$ G-invariant.
F is a trivial FG-module by defining $gc = c$ for every $g \in G, c \in F$.	The trivial representation is $\rho_1(g) = [1]$ for all $g \in G$, and the trivial character has $\chi_1(g) = 1$ for all $g \in G$.
If G operates on X, then FX (the set of linear combinations of elements of X) is a FG-module, called a permutation module.	The permutation representation corresponding to a G-set X sends each $g \in G$ to the permutation matrix corresponding to left-multiplication by g.
FG is a FG-module.	Let $G = \{g_i \mid 1 \le i \le \lvert G\rvert\}$. If $gg_i = g_{\pi(i)}$, then the **regular representation** ρ^{reg} sends g to the permutation matrix corresponding to π.
Let A be a semisimple algebra, and suppose that *as A-modules* $A \cong \oplus S_i$, where each S_i is simple. Then any simple A-module S is isomorphic with some S_i. *Pf.* Take $0 \neq s \in S$; define $\varphi: A \to S$ by $\varphi(a) = as$. The restrictions of φ to S_i are 0 or isomorphisms by Schur's. One of them is an isomorphism.	Suppose $\rho^{\text{reg}} = \oplus \rho_i$, where each ρ_i is an irreducible representation. Then any irreducible representation is isomorphic with some ρ_i.
Suppose A is a semisimple algebra. Let M be an A-module, and write $M \cong \oplus_{i=1}^{r} n_i S_i$, where S_i are all the distinct simple modules. Then the n_i are uniquely determined. *Pf.* Jordan-Hölder for modules.	Every representation can be written as a direct sum uniquely: $\rho = \oplus_{i=1}^{r} n_i \rho_i$
Let D be a division algebra. Then $M_n(D)$ is a simple algebra and any simple $M_n(D)$-module is isomorphic with D^n. As modules, $M_n(D) \cong nD^n$.	$M_n(\mathbb{C})$ has no two-sided ideals. $\mathbb{C}^n$ has no $M_n(\mathbb{C})$-invariant subsets. Informally, $M_n(\mathbb{C})$ can only operate nontrivially on $\mathbb{C}^n$.
The **opposite algebra** B^{opp} has multiplication defined by $a \cdot b = ba$.	Transposing matrices, multiplication goes the other way 'round.
Wedderburn's Structure Theorem: An algebra A is semisimple iff it is isomorphic with the direct sum of matrix algebras over division algebras. If F is algebraically closed, any semisimple algebra is isomorphic to a direct sum of matrix algebras over F. *Pf.* 1. If S_i are distinct simple A-modules, and $U = \oplus_{i=1}^{r} n_i S_i$, then $\text{End}_A(U) \cong \oplus_{i=1}^{r} \text{End}_A(n_i S_i)$.	If F is algebraically closed (such as $\mathbb{C}$), then as algebras, $FG \cong \oplus_{i=1}^{n} M_{n_i}(F)$ for some n_i.

2. $\text{End}_A(n_i S_i) \cong M_n(\text{End}_A(S))$ 3. Taking $U = A$, and taking opposite twice, $A \cong \bigoplus_{i=1}^{r} M_{n_i}(\text{End}_A(S_i)^{\text{op}})$.	
If A is simple, then A is isomorphic with a matrix algebra over a division algebra.	Suppose G is an irreducible linear group in $\text{GL}_n(F)$. Then $\text{span}(G) = M_n(F)$.[9]

11-3 The Character Table and Orthogonality Relations

Basic properties:

1. $\chi(1) = \dim \chi$, the number of rows/ columns in the matrix representation.
2. χ is a class function, i.e. a function $G \to F$ that is constant on every conjugacy class.
3. If g has order k, $\chi(g)$ is a sum of $\dim \chi$ k$^{\text{th}}$ roots of unity.
4. $\chi(g^{-1}) = \overline{\chi(g)}$
5. If χ, χ' correspond to ρ, ρ', then $\chi + \chi'$ corresponds to $\rho \oplus \rho'$. In terms of modules, $\chi_{U\oplus V} = \chi_U + \chi_V$.
6. $\chi_{U\otimes V} = \chi_U \chi_V$
7. $\chi_{U^*} = \overline{\chi_U}$, where $U^* = \text{Hom}_F(U, V)$ (The eigenvalues are inverse.)
8. $\chi_{\text{Hom}(U,V)} = \overline{\chi_U}\chi_V$ $(\text{Hom}(U,V) \cong U^* \otimes V)$

On irreducible characters:

1. The number of irreducible characters equals the number of conjugacy classes.
   a. Suppose $\mathbb{C}G \cong \bigoplus_{i=1}^{r} M_{n_i}(\mathbb{C})$ is the decomposition into simple algebras. The center Z of $\mathbb{C}G$ are all elements with g, h having the same coefficients when they are in the same conjugacy class, so has dimension equal to the number of conjugacy classes. Also $\dim_{\mathbb{C}} Z = r$ from the decomposition; the center of $M_{n_i}(\mathbb{C})$ are scalar matrices.
2. The irreducible characters are linearly independent.
   a. Let e_i be the identity element of $M_{n_i}(\mathbb{C})$. If $\sum_{j=1}^{r} \lambda_j \chi_j = 0$ then $0 = \sum_{j=1}^{r} \lambda_j \chi_j(e_j) = \lambda_i \dim_{\mathbb{C}} S_i$ so all $\lambda_i = 0$.
3. Hence, representations (or $\mathbb{C}G$-modules) are isomorphic iff they have the same character.

An inner product is defined for characters (and, in general, class functions) as follows:

$$\langle \chi_U, \chi_V \rangle = \frac{1}{|G|}\sum_{g\in G} \overline{\chi(g)}\chi'(g) = \frac{1}{|G|}\sum_{\text{conjugacy class } C} |C| \cdot \overline{\chi(C)}\chi'(C)$$

For any $\mathbb{C}G$-modules U and V,

$$\langle \chi_U, \chi_V \rangle = \dim_{\mathbb{C}} \text{Hom}_{\mathbb{C}G}(U, V)$$

Pf.

1. Let $a = \frac{1}{|G|}\sum_{g\in G} \chi_U(g)$: Then $a^2 = a$ so the linear transformation of left multiplication by a satisfies $T^2 - T = 0$ and is diagonalizable with eigenvalues 0 and 1. The eigenspace of 1 is U^G; its dimension equals the trace of T. So $\dim_{\mathbb{C}G} U^G = \frac{1}{|G|}\sum_{g\in G} \chi_U(g)$.
2. $\text{Hom}_{\mathbb{C}G}(U, V) = \text{Hom}(U, V)^G$; use (1) and property (8).

Let χ_i be the irreducible characters of G. The character table has the characters written

[9] The LHS says $\text{span}(G) \cong M_m(F)$ for some m. Since $\mathbb{C}^m$ is a simple $\text{span}(G)$-module, m=n.

down the left, and conjugacy classes across the top, with the entries the values the characters take on the conjugacy classes:

$$\begin{array}{ccc} & C_1 = \{1\} \quad \cdots & C_r \\ \chi_1 & d_1 & \\ \vdots & \vdots & \\ \chi_r & d_r & \end{array}$$

By convention, χ_1 is the trivial character.

<u>Row Orthogonality:</u> $\langle \chi_i, \chi_j \rangle = \delta_{ij} = \begin{cases} 0, i \neq j \\ 1, i = j \end{cases}$

<u>Pf.</u> By Schur's lemma, $\mathrm{Hom}_{\mathbb{C}G}(S_i, S_j) = 0$ and $\mathrm{Hom}_{\mathbb{C}G}(S_i, S_i) \cong \mathbb{C}$.

<u>Cor.</u> $\langle \sum_{i=1}^r a_i \chi_i, \sum_{i=1}^r b_i \chi_i \rangle = \sum_{i=1}^r a_i b_i$. If χ is a virtual character, $\chi = \sum_{i=1}^r \langle \chi, \chi_i \rangle \chi_i$.

Thus, the characters form an orthonormal basis for the vector space of class functions. The columns are also orthonormal with respect to the same Hermitian form:

<u>Column Orthogonality:</u> $\sum_{t=1}^r \overline{\chi_t(g_i)} \chi_t(g_j) = \begin{cases} 0, & i \neq j \\ \frac{|G|}{|C_i|} = |C_G(g_i)|, & i = j \end{cases}$

Determining the irreducible characters:

1. Find the conjugacy classes of G, to determine the number of irreducible characters.
2. If N is a normal subgroup of G, $\pi: G \to G/N$ is the canonical homomorphism, and χ is a (irreducible) character of N, then $\chi\pi$ is a (irreducible) character for G.
3. Every irreducible character of a finite abelian group is 1-dimensional. (So any matrix representation is simultaneously diagonalizable.)
4. $d_i||G|$ for each i. (Pf. in 12-5)
5. $\sum_{i=1}^r d_i^2 = |G|$.
    a. By modules: $|G| = \dim_{\mathbb{C}} \mathbb{C}G = \sum_{i=1}^r \dim_{\mathbb{C}} M_{d_i}(\mathbb{C})$.
    b. By representations: $\langle x^{\mathrm{reg}}, \chi_i \rangle = \dim \chi_i$; $|G| = \dim \chi^{\mathrm{reg}} = \sum_{i=1}^r d_i \dim \chi_i$
6. Try to find the eigenvalues of representations. For example, if x, x^a are conjugate, then $\rho_x = \rho_{x^a}$; if λ is an eigenvalue then so is λ^a.

Normal Subgroups

1. Let $K_\chi = \{g \in G | \chi(g) = \chi(1)\}$. Then K_χ is a normal subgroup. (The corresponding representation maps $g \in K_\chi$ to I.) The normal subgroups of G are exactly the sets in the form $\bigcap_{i \in I} K_{\chi_i}$ for some $I \subseteq \{1, \ldots, r\}$.
2. Let $Z_\chi = \{g \in G || \chi(g)| = \chi(1)\}$. If χ is irreducible, $Z_\chi / K_\chi = Z(G/K_\chi)$. $Z(G) = \bigcap_{i=1}^r Z_{\chi_i}$. If G is nonabelian and simple, $Z_{\chi_i} = 1$ for all $i > 1$.

11-4 Frobenius Reciprocity

Let $H \subseteq G$.

- If V is a FH-module, the FG-module $\mathrm{Ind}_H^G V = FG \otimes_{FH} V$ is the **induced** FG-module of V.
    - If ϕ is the character for V, the induced character of $\mathrm{Ind}_H^G V$ is denoted by ϕ^G.
- If U is a FG-module, the FH-module $\mathrm{Res}_H^G V$ is the **restriction** of U to H.
    - If χ is the character for U, the character of $\mathrm{Res}_H^G V$ is denoted by $\chi|_H$.

Note that $\dim_F \mathrm{Ind}_H^G V = [G:H] \dim_F V$, and as F-vector spaces $\mathrm{Ind}_H^G V = \oplus_{t \in T} t \oplus V$ for T a transversal for H in G.

Frobenius Reciprocity: As F-vector spaces, $\mathrm{Hom}_{FH}(V, \mathrm{Res}_H^G\, U) \cong \mathrm{Hom}_{FG}(\mathrm{Ind}_H^G\, V\,, U)$. In terms of characters, $\langle \phi, \chi|_H \rangle = \langle \varphi^G, \chi \rangle$. (The left inner product is in H; the right one is in G.)

The Induction-Restriction Table

Let $\phi_i(1 \le i \le r), \chi_j(1 \le j \le s)$ be the irreducible characters for H and G. The induction-restriction table of (G,H) is the $r \times s$ matrix with (i,j)-entry equal to $\langle \phi_i, \chi_j|_H \rangle = \langle \phi_i^G, \chi_j \rangle$. The ith row gives the multiplicities with which the χ_j appear in the decomposition of ϕ_i^G; the jth row gives the multiplicities with which the ϕ_i appear in the decomposition of $\chi_j|_H$.

Finding induced characters in G given characters in H:

Let χ be a character of $H \subseteq G$. If no element of H is conjugate to $g \in G$, then $\chi^G(g) = 0$. Else, let s be the number of conjugacy classes of H whose members are conjugate in G to g. Choose representatives of the conjugacy classes h_i. Then

$$\chi^G(g) = \sum_{i=1}^{s} \frac{Z_G(g)}{Z_H(h_i)}\chi(h_i) = \sum_{i=1}^{s} [G\colon H]\frac{C_H(h_i)}{C_G(g)}\chi(h_i)$$

where $C_A(x)$ denotes the conjugacy class of x in A and $Z_A(x)$ denotes the centralizer of x in A.

11-5

Applications of Representation Theory

Frobenius's Theorem: Let G be a transitive permutation group on a finite set X, with each non-identity element fixing at most one element of X. Then the Frobenius kernel $\mathcal{N}=\{1\} \cup \{g \in G | g \text{ has no fixed points}\}$ of G is a normal subgroup.

Pf. Let $H = G_x$ with irreducible characters φ_i. Every element of $G - N$ is conjugate with an element of H; take conjugacy class representatives and use formula in 12-4. Take $\chi_i = \varphi_i^G - \varphi_i(1)\varphi_1^G + \varphi_i(1)\chi_1$ for $1 < i \le s$, and $\chi = \sum_{i=1}^{s} \varphi_i(1)\chi_i$. Then the Frobenius kernel is K_χ.

Using Algebraic Integers

1. The algebraic integers form a subring of $\mathbb{C}$; that is, the sum and product of algebraic integers is an algebraic integer. A real rational algebraic integer is an integer.
2. For any character χ and $g \in G$, $\chi(g)$ is an algebraic integer. (Sum of roots of unity)
3. For any irreducible character χ and $g \in G$, $[G\colon Z_G(g)]\frac{\chi(g)}{\chi(1)}$ is an algebraic integer.
    a. Let S be the corresponding simple module. For C(g) the conjugacy class of g, the map $S \to S$ defined by $\varphi(s) = as, a = \sum_{x \in C(g)} x$ must be multiplication by a scalar λ (Schur's lemma). $\lambda\chi(1) = a = [G\colon Z_G(g)]\chi(g)$ so $\lambda = [G\colon Z_G(g)]\frac{\chi(g)}{\chi(1)}$.
    b. φ is a linear transformation $\mathbb{C}G \to \mathbb{C}G$. Each entry in the matrix is 0 or 1 so the characteristic equation has integer coefficients.
4. $d_i||G|$ for each i.
    a. $\frac{|G|}{\chi(1)} = \frac{|G|}{\chi(1)}\langle \chi, \chi \rangle = \sum_{\text{conjugacy class } C} |C| \frac{\overline{\chi(C)}}{\chi(1)}\chi'(C)$; each term in the sum is an algebraic integer so $\frac{|G|}{\chi(1)}$ is a rational algebraic integer and hence an integer.
5. If $\gamma = \frac{\chi(g)}{\chi(1)}$ is a nonzero-algebraic integer, then $\gamma = 1$.

    a. $\chi(g)$ is a sum of roots of unity so $\gamma = \sum_{k=1}^{d} e^{\frac{2\pi i m_k}{n_k}} / \chi(1)$ for some m_k, n_k. $\chi(g)$ has conjugates among $\sum_{k=1}^{d} e^{\frac{2\pi i l_k}{n_k}} / \chi(1), 1 \leq l_k \leq n_k$, the product of the conjugates must be an integer. But each factor has absolute value less than 1 and not 0, unless $\gamma = 1$.

6. If G has a conjugacy class of non-trivial prime power, G is not simple.
    a. Suppose G has a conjugacy class of order p^n containing $g \neq 1$. From column orthogonality,
$$0 = \frac{1}{p} + \sum_{i=2}^{r} \frac{\chi_i(g)\chi_i(1)}{p}$$
    b. $\frac{\chi_i(g)\chi_i(1)}{p}$ is not an algebraic integer for some $i | 2 \leq i \leq r$. Then $p \nmid \chi_i(1)$; by Bezout, $a[C: Z_G(g)] + b\chi_i(1) = 1$ for integers a, b. Then multiplying by $\chi_i(g)/\chi_i(1)$,
$$\frac{\chi_i(g)}{\chi_i(1)} = a[G: Z_G(g)]\frac{\chi_i(g)}{\chi_i(1)} + b\chi_i(g)$$
is an algebraic integer by 2 and 3 so $|\chi_i(g)| = \chi_i(1), g \in Z_{\chi_i}$. Z_{χ_i} is nontrivial so G is not simple. (See 12-3)

Burnside's p-q Theorem: Every group of order $p^a q^b | a, b \in \mathbb{N}_0$, where p, q are distinct primes, is solvable.
Pf. Induct on $a + b$. P-groups are solvable. Take Q a q-SSG. For $Q \neq 1$, $Z(Q) \neq 1$; take $g \in Z(Q)$. Then $[G: Z_G(g)] = p^n$ for some n. If n=0 then $Z(G)$ is nontrivial. Else apply 6 to see G is not simple.

Exercises
1. Find the irreducible characters of $G \times H$ from the irreducible characters of G, H.
2. [PiGT] Let G be a linear group of degree n.
    a. If G is irreducible and $\mathrm{tr}(g), g \in G$ takes on at most m values, show that $|G| \leq m^{n^2}$.
    b. If $g^m = 1$ for all $g \in G$, show that $|G| \leq m^{n^3}$.

References

Groups and Representations by J. Alperin and Rowen Bell (GTM 162)
Algebra by Michael Artin
Abstract Algebra: The Basic Graduate Year, by Robert Ash http://www.math.uiuc.edu/~r-ash/
Elements of Abstract Algebra by Richard Dean
Problems in Group Theory by John Dixon
Permutation Groups by Dixon and Mortimer (GTM 163)
The Theory of Groups by Marshall Hall, Jr.
An Introduction to the Theory of Groups by Joseph Rotman (GTM 148)