Math 55a Notes

Elvin Lo

Fall 2023

2024.5.19

Preface

These notes follow Math 55a, Studies in Algebra and Group Theory, at Harvard College. We divide the course into four chapters:

1. **Introduction to Group Theory**
2. **Linear Algebra Speedrun**
3. **Revisiting Group Theory**
4. **Representation Theory**

Contents

1 Introducion to Group Theory

In Lectures 1–6, we introduce group theory and roughly cover Artin chapter 2. These notes divide the discussion into four parts:

- **Groups and homomorphisms**, where we introduce the most fundamental language of groups and homomorphisms.
- **Cosets**, where we introduce equivalence relations, cosets, and Lagrange's Theorem.
- **Conjugation, normal subgroups, and some useful constructions**, including the center and the commutator subgroup.
- **Product and quotient groups**, including discussion of the product map and the First Isomorphism Theorem.

1.1 Groups and homomorphisms

Definition 1.1. Groups and subgroups
We begin with some fundamental definitions of groups:

- A *group* is a set G with a law of composition having the following properties: associativity, closure, existence of an identity element 1, and existence of inverses. We denote by $|G|$ the order of G, i.e., the cardinality of the set G.
- An *abelian group* is a group with a commutative law.
- A *subgroup* $H \subset G$ is a subset containing the identity that is closed under composition and inversion.

Proposition 1.2. Properties of inverses
Now some remarks on inverses:

- If a is invertible, its inverse is unique.
- If $a \in G$ has both a left inverse l and a right inverse r, then $l = r$ and a is invertible. Note that a non-invertible element a may still have a left inverse or a right inverse.
- If a and b are invertible, so is the product ab, and $(ab)^{-1} = b^{-1}a^{-1}$.

The existence of inverses gives us the cancellation law:

$$ab = ab' \implies b = b'.$$

Definition 1.3. Subgroup generated by a subset, generating set
Given a subset U, the subgroup of G *generated* by U is the smallest subgroup containing U, i.e., the subgroup of elements expressible as a product of finitely many elements of U and their inverses. Similarly, a subset U of G is a *generating set* of G if every element of G is such a product.

Definition 1.4. Order of an element, cyclic subgroups
The *order* $\mathrm{ord}(g)$ of $g \in G$ is the smallest positive integer such that $g^{\mathrm{ord}(g)} = 1$. The *cyclic subgroup* $\langle g \rangle$ of order $\mathrm{ord}(g)$ is given by

$$\langle g \rangle = \{1, g, \ldots, g^{\mathrm{ord}(g)=1}\}.$$

Definition 1.5. Homomorphism
Given groups G and G', a *homomorphism* is a map $\phi : G \to G'$ such that for all a, b in G,

$$\phi(ab) = \phi(a)\phi(b).$$

A homomorphism necessarily maps the identity in G to the identity in G', and inverses to inverses:

$$\phi(a^{-1}) = \big(\phi(a)\big)^{-1}.$$

An *isomorphism* is a bijective group homomorphism, and an *automorphism* is an isomorphism from a group to itself.

Definition 1.6. Image and kernel
Given $\phi : G \to G'$, the *image* $\operatorname{im}\phi$ or $\phi(G)$ is a subgroup of G', while the *kernel* $\ker\phi$ is a normal subgroup of G.

Proposition 1.7. Condition for injectivity
A homomorphism is injective iff the kernel is the trivial subgroup $\{1\}$.

1.2 Cosets

Definition 1.8. Equivalence relation
An *equivalence relation* $\sim$ on a set S is a relation holding between certain pairs of elements of S and satisfying three axioms: reflexivity, symmetry, and transitivity.

- Equivalence classes may be denoted by a representative element, e.g., $\{x\}$ denotes the equivalence class of the element x.
- An equivalence relation on a set S determines a partition of S by its equivalence classes, and conversely.

Definition 1.9. Coset
Given subgroup $H \subset G$ and element $a \in G$, we define the *left coset*

$$aH = \{g \in G : g = ah \text{ for some } h \in H\}.$$

Right cosets are defined analogously.

- Cosets partition a group, and each coset has equal order, for multiplication by a is a bijective map (whose inverse is multiplication by a^{-1}).
- The number of left cosets of $H \subset G$ is called the *index* $[G : H]$ of H in G.

Theorem 1.10. Lagrange's Theorem and the Counting Formula
Our remarks on cosets give us the Counting Formula,

$$|G| = |H||G : H|.$$

In particular,

- Lagrange's Theorem says that given any subgroup $H \subset G$, we have $|H| \mid |G|$.
- In particular, the order of any element divides the order of the group, for we may consider the cyclic subgroup generated by that element.
- Given a homomorphism $\phi : G \to G'$ of finite groups, there is a bijection between cosets of $\ker \phi$ and $\operatorname{im} \phi$. Thus the Counting Formula gives us

$$G = |\ker \phi| \cdot |\operatorname{im} \phi|.$$

1.3 Conjugation, normal subgroups, and some useful constructions

First we discuss conjugation and normal subgroups.

Definition 1.11. Conjugation
Conjugation by g is the map $\varphi_g : G \to G$ given by

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

We may verify conjugation maps φ_g are automorphisms with inverses $\varphi_{g^{-1}}$.

Definition 1.12. Normal subgroup
A *normal subgroup* is a subgroup closed under conjugation, i.e., $H \subset G$ is normal if for all $h \in H$ and all $g \in G$, the conjugate ghg^{-1} of h by g is in H.

Proposition 1.13. Subgroups of index 2 are normal
If $|G|/|H| = 2$, then $|H|$ is normal.

Proposition 1.14. Conjugate subgroups (Artin 2.8.18)
Some properties of conjugate subgroups:

- If H is a subgroup of a group G and g is an element of G, the set gHg^{-1} is also a subgroup.
- If a group G has just one subgroup H of order r, then that subgroup is normal.

Now we discuss some useful constructions: the center and the commutator subgroup. These are opposite constructions, for the bigger the center is, the smaller the commutator subgroup.

Definition 1.15. Center $Z(G)$
For any group G, the *center* $Z(G)$ is the set of elements that commute with all elements in G,

$$Z(G) = \{a \in G : gag^{-1} = a \forall g \in G\}.$$

Definition 1.16. Commutator subgroup
The *commutator* of elements a and b is

$$[a, b] \coloneqq aba^{-1}b^{-1}.$$

The *commutator subgroup* $C(G)$ is the normal subgroup generated by commutators, and the quotient $G/C(G)$ is called the abelianization of G.

1.4 Product and quotient groups

Definition 1.17. Product of two groups
The *product* $G \times H$ of groups G and H is the Cartesian product, i.e.,

$$G \times H = \{(a, b) \mid a \in G, b \in H\},$$

with a term-wise law of composition,

$$(a, b) \cdot \left(a', b'\right) \coloneqq \left(aa', bb'\right).$$

Definition 1.18. Quotient groups
Given a normal subgroup $H \subset G$, the set of cosets may be given the structure of a group and is called the *quotient group*

$$G/H = \{aH \mid a \in G\},$$

with operation $(aH)(bH) = abH$. For a non-normal subgroup, the set of cosets does not have this group operation, hence the importance of normality.

Now let us introduce some properties of group products and quotient groups.

Definition 1.19. Product set
Given subsets $A \subset G$ and $B \subset G$, define the product set

$$AB = \{ab \in G : a \in A \text{ and } b \in B\}.$$

Proposition 1.20. Product map for Cartesian products (Artin 2.11.4)
Let H and K be subgroups of a group G, and let $f : H \times K \to G$ be the multiplication map, defined by $f(h, k) = hk$. Its image is the set $HK = \{hk \mid h \in H, k \in K\}$.

(a) f is injective if and only if $H \cap K = \{1\}$.

(b) f is a homomorphism from the product group $H \times K$ to G if and only if elements of K commute with elements of $H : hk = kh$.

(c) If H is a normal subgroup of G, then HK is a subgroup of G.

(d) f is an isomorphism from the product group $H \times K$ to G iff $H \cap K = \{1\}$, $HK = G$, and also H and K are normal subgroups of G.

Note that the multiplication map may be bijective though not a group homomorphism, e.g., when $G = S_3$, and with the usual notation, $H = \langle x \rangle$ and $K = \langle y \rangle$.

Proof. Let us prove each statement.

(a) If $H \cap K$ contains an element $x \neq 1$, then x^{-1} is in H, and $f\left(x^{-1}, x\right) = 1 = f(1, 1)$, so f is not injective. Suppose that $H \cap K = \{1\}$. Let (h_1, k_1) and (h_2, k_2) be elements of $H \times K$ such that $h_1 k_1 = h_2 k_2$. We multiply both sides of this equation on the left by h_1^{-1} and on the right by k_2^{-1}, obtaining $k_1 k_2^{-1} = h_1^{-1} h_2$. The left side is an element of K and the right side is an element of H.

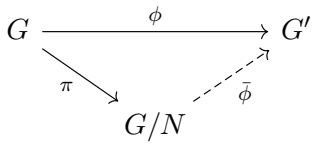
Since $H \cap K = \{1\}, k_1 k_2^{-1} = h_1^{-1} h_2 = 1$. Then $k_1 = k_2, h_1 = h_2$, and $(h_1, k_1) = (h_2, k_2)$.

(b) Let (h_1, k_1) and (h_2, k_2) be elements of the product group $H \times K$. The product of these elements in the product group $H \times K$ is $(h_1 h_2, k_1 k_2)$, and $f(h_1 h_2, k_1 k_2) = h_1 h_2 k_1 k_2$, while $f(h_1, k_1) f(h_2, k_2) = h_1 k_1 h_2 k_2$. These elements are equal if and only if $h_2 k_1 = k_1 h_2$.

(c) Suppose that H is a normal subgroup. We note that KH is a union of the left cosets kH with k in K, and that HK is a union of the right cosets Hk. Since H is normal, $kH = Hk$, and therefore $HK = KH$. Closure of HK under multiplication follows, because $HKHK = HHKK = HK$. Also, $(hk)^{-1} = k^{-1} h^{-1}$ is in $KH = HK$. This proves closure of HK under inverses.

(d) Suppose that H and K satisfy the conditions given. Then f is both injective and surjective, so it is bijective. According to (b), it is an isomorphism if and only if $hk = kh$ for all h in H and k in K. Consider the commutator $\left(hkh^{-1}\right) k^{-1} = h\left(kh^{-1}k^{-1}\right)$. Since K is normal, the left side is in K, and since H is normal, the right side is in H. Since $H \cap K = \{1\}, hkh^{-1}k^{-1} = 1$, and $hk = kh$. Conversely, if f is an isomorphism, one may verify the conditions listed in the isomorphic group $H \times K$ instead of in G. □

Theorem 1.21. First Isomorphism Theorem (Artin 2.12.10)
Let $\phi : G \to G'$ be a surjective homomorphism. Then we have the isomorphism $G/\ker\phi \cong G'$. Specifically, letting $\pi : G \to G/N$ be the canonical map, there is a unique isomorphism $\bar{\phi} : G/N \to G'$ such that $\phi = \bar{\phi} \circ \pi$.



In particular, given any homomorphism ϕ mapping from G to another group, we have $G/\ker\phi \cong \operatorname{im}\phi$.

2 Linear Algebra Speedrun

In Lectures 7–18, we run through linear algebra, roughly covering Axler. These notes divide the lectures into batches.

- **Lectures 7–9: The linear algebra fundamentals**, roughly covering Axler chapters 1–4.
  - Lecture 7 discusses fundamental definitions.
  - Lecture 8 discusses dimension.
  - Lecture 9 discusses linear maps, including COB matrices, normal form for homomorphisms from V to W, quotient spaces, dual spaces, and constructions like the annihilator and transpose arising from the dual space.
- **Lectures 10–12: Eigen-stuffs and operators**, roughly corresponding to Axler chapters 5 and 8.
  - Lecture 10 establishes some goals in our study of operators.
  - Lecture 11 discusses upper triangular operators.
  - Lecture 12 introduces generalized kernels and images, and then uses them to derive Jordan canonical form.
- **Lectures 13–16: Bilinear forms and inner product spaces, category theory,** roughly corresponds to Axler chapters 6–7 but generalizes to the more general language of bilinear forms and Hermitian inner product spaces. The present edition of these notes provides only a brief overview of these lectures.
- **Lectures 17–18: Multilinear algebra, tensor products,** is not covered in the third edition of Axler, though it is discussed in the fourth edition. The present edition of these notes provides only a brief overview of these lectures.

Also worth noting are some general proof tips in linear algebra:

- use induction,
- consider basis choices,
- given a linear operator, consider $T^i, \ker T, \operatorname{im} T$.

2.1 Lectures 7–9: The linear algebra fundamentals

We begin by introducing the language of vector spaces.

Definition 2.1. Fields, rings, and characteristics
A *field* k is a set with two laws of composition $+$ and $\times$ satisfying the following axioms:

- $(k, +)$ is an abelian group with identity $0 \in k$.
- $(k\backslash\{0\}, \times)$ is an abelian group with identity $1 \in k$.
- Multiplication is distributive over addition.
- $0 \neq 1$ (the field has more than 1 element).

A *commutative ring* has all the same axioms except that multiplicative inverses need not exist. Observe that the field axioms imply that for any field k,

- $0a = 0$ for any $a \in k$,
- for $a \neq 0$, $ab = ac \implies b = c$.

The *characteristic* $\text{char}(k)$ of a field k is the order of 1 in the abelian group $(k, +)$ if it is finite, and 0 otherwise. Note that if $\text{char}(k)$ is positive, then it must be a prime, for

$$\text{char}(k) = ab \implies ab \cdot 1 = (a \cdot 1)(b \cdot 1) = 0 \implies a \cdot 1 = 0 \text{ or } b \cdot 1 = 0.$$

Definition 2.2. Vector spaces and subspaces
A *vector space* over the field k is a set V with an addition on V (assigning an element $u+v \in V$ for every pair $u, v \in V$) and a scalar multiplication on V (assigning an element $\lambda v \in V$ to each $\lambda \in k$ and each $v \in V$) such that the following properties hold:

- Commutativity of addition
- Associativity of addition and scalar multiplication
- Additive identity: There exists an element $0 \in V$ s.t. $v + 0 = v$ for all $v \in V$
- Additive inverse: For every $v \in V$, there exists $w \in V$ s.t. $v + w = 0$
- Multiplicative identity: $1v = v$ for all $v \in V$
- Distributive properties

A subspace U of V is a subset that is also a vector space using the same addition and scalar multiplication as on V, i.e., a subset (necessarily containing the additive identity) that is closed under addition and scalar multiplication.

Definition 2.3. Linear independence, span, and basis
Define the following:

- A list of vectors is *linearly independent* if no nontrivial finite linear combination of the vectors equals zero, i.e., if

$$a_1 v_1 + \cdots + a_n v_n = 0 \implies a_1 = \cdots = a_n = 0.$$

- The *span* of a list of vectors is the set of all their linear combinations, i.e., the smallest subspace containing all the vectors in the list.
- The *dimension* of a vector space V is the number of elements in a basis of V, and of course any two bases are the same size.

Observe that any list of linearly independent vectors in V may be extended to a basis of V, while any spanning set of V contains a basis of V.

Definition 2.4. Direct sum
Given some vector space V, we say that V is the (internal) *direct sum* of subspaces U and W, i.e., we have the direct sum decomposition $V = U \oplus W$, if every vector $v \in V$ is uniquely expressible as a sum $v = u + w$ for $u \in U$ and $w \in W$. Equivalently, we have $V = U \oplus W$ if any two of the following hold:

- $U \cap W = \{0\}$;
- $\dim U + \dim W = \dim V$;
- $U \cup W$ spans V.

Isomorphically, the external direct sum of two vector spaces V and W is simply their Cartesian product, i.e,. the set of ordered pairs of vectors (v, w) where operations act on each independently. (The distinction between internal and external direct sums is made only on whether we (1) first define the summands and then define the direct sum in terms of the summands, or (2) first define some algebraic structure and then express it as a direct sum of substructures.)

Now we introduce linear maps.

Definition 2.5. Linear maps
A map is linear if it preserves the linear structure.

- A linear map is completely determined by where it sends a basis of V.
- $\mathrm{Hom}(V, W)$ is the vector space of linear maps $V \to W$, and, from its identification as the set of $m \times n$ matrices, it has dimension mn.

Definition 2.6. Kernel, image, and rank-nullity
The *kernel* and *image* of a linear map $T : V \to W$ are subspaces of V and W, respectively. Analogous to the Counting Formula or Lagrange in group theory, we have the rank-nullity theorem:

$$\dim V = \dim \operatorname{im} T + \dim \ker T.$$

Definition 2.7. Dual space
Given any vector space V over k, the dual vector space $V^* = \operatorname{Hom}(V, k)$ is the vector space of all linear functionals over V.

- Given any basis $\{v_i\}$ of V, we may form a corresponding *dual basis* $\{\varphi_i\}$ of V^*, where the linear functional φ_i sends v_j to the Kronecker delta δ_{ij}. In other words,

  $$\varphi_i(v_j) = \begin{cases} 1 & \text{if } i = j, \\ 0 & \text{if } i \neq j. \end{cases}$$

  The construction of the dual basis gives a non-canonical isomorphism $V \cong V^*$ (non-canonical due to the necessary choice of a basis of V).

- We have a natural (canonical) isomorphism $V \cong (V^*)^*$ mapping v to the evaluation map $\phi_v \in \operatorname{Hom}(V^*, k)$ evaluating a given linear functional at v.

- The *annihilator* of a subapce $U \subset V$ is the subspace of V^* given by

  $$\operatorname{Ann}(U) = \{\ell \in V^* : \ell(U) = 0\}$$

  with dimension $\dim \operatorname{Ann}(U) = \dim V - \dim U$.

- Dual spaces also give rise to the transpose: given $\phi : V \to W$, we have the transpose $\phi^* : W^* \to V^*$ mapping between the duals and going the other way. We may verify that the matrix of ϕ with respect to any bases $\{v_i\}$ and $\{w_i\}$ is precisely the matrix transpose of the matrix of ϕ^* with respect to the corresponding dual bases.

2.2 Lectures 10–12: Eigen-stuffs and operators

An *operator* on V is a linear map $T : V \to V$. We have the question: When is T diagonalizable? This motivates our discussion of eigenvectors and eigenvalues.

Definition 2.8. Eigenvectors and eigenvalues
If $T : V \to V$ is any operator, an *eigenvector* for T is a nonzero vector v such that $T(v) = \lambda v$ for some scalar $\lambda \in k$, where the scalar λ is called the *eigenvalue* of v. If we can find a basis for V consisting of eigenvectors of T, we say that T is *diagonalizable*.

- If a list of eigenvectors for T has distinct eigenvalues, then the list is linearly independent.

Theorem 2.9. Existence of eigenvalues
Over $\mathbb{C}$, every linear map has an eigenvalue.

Proof. Suppose we are working over $\mathbb{C}$, which is an algebraically closed field (implying that every polynomial has a root). Then for any T, the list $1, T, T^2, \dots$ is eventually linearly dependent, giving us a polynomial $P(T)$ which must have a root λ. Then $T - \lambda$ has a nontrivial kernel, and so λ is an eigenvalue. □

Definition 2.10. Generalized kernel and generalized image
Let V finite-dimensional and consider operator $T : V \to V$. To define the generalized kernel, consider the nested sequence

$$\ker(T) \subset \ker\left(T^2\right) \subset \ker\left(T^3\right) \subset \cdots \subset V.$$

Since V is finite-dimensional, these subspaces must stabilize: for some m we must have

$$\ker\left(T^m\right) = \ker\left(T^{m+1}\right) = \ker\left(T^{m+2}\right) = \dots.$$

Define the generalized kernel of T to be this limit,

$$\operatorname{gker}(T) \coloneqq \bigcup_m \ker\left(T^m\right) = \left\{v \in V \mid T^m v = 0 \text{ for some } m\right\}.$$

In fact, if for any n we have $\ker\left(T^n\right) = \ker\left(T^{n+1}\right)$, then we have $\ker\left(T^n\right) = \ker\left(T^m\right)$ for all $m \geq n$. Thus $\operatorname{gker}(T) = \ker(T^n)$.

Similarly, we may consider

$$V \supset \operatorname{im}(T) \supset \operatorname{im}\left(T^2\right) \supset \operatorname{im}\left(T^3\right) \supset \dots$$

and because this again has to stabilize, we define the generalized image of T as

$$\operatorname{gim}(T) \coloneqq \bigcap_m \operatorname{im}\left(T^m\right) = \left\{v \in V \mid v \in \operatorname{im}\left(T^m\right) \text{ for all } m\right\} = \operatorname{im}(T^n).$$

The generalized kernel and generalized image have the following two properties:

Lemma 2.11. Nested sequence of kernel stabilizes
As stated above, we have

$$\ker T^k = \ker T^{k+1} \implies \ker T^{k+1} = \ker T^{k+2} \implies \operatorname{gker} T = \ker T^n.$$

See the proof in Homework 5 Problem 1.

Theorem 2.12. V is direct sum of generalized kernel and generalized image
If $T : V \to V$ is any operator on finite-dimensional V, then

$$V = \operatorname{gker}(T) \oplus \operatorname{gim}(T).$$

Proof. First, since $\operatorname{gker}(T) = \ker(T^n)$ and $\operatorname{gim}(T) = \operatorname{im}(T^n)$ for $n = \dim V$, we see that

$$\dim \operatorname{gker}(T) + \dim \operatorname{gim}(T) = n.$$

Thus, to prove that $V = \operatorname{gker}(T) \oplus \operatorname{gim}(T)$ we just have to show that $\operatorname{gker}(T) \cap \operatorname{gim}(T) = 0$. But now observe that since $T(\operatorname{gim}(T)) = \operatorname{gim}(T)$ by definition, any power of T maps $\operatorname{gim}(T)$ to itself isomorphically; thus $\operatorname{gim}(T)$ cannot contain any nonzero element of $\operatorname{gker}(T)$. □

Lemma 2.13. Direct sum decomposition from a nilpotent operator
An operator $T : V \to V$ is called nilpotent if $T^m = 0$ for some m; equivalently, if $\operatorname{gker}(T) = V$ or $\operatorname{gim}(T) = (0)$. If $T : V \to V$ be any nilpotent operator, then we have

$$V = \bigoplus U_\alpha \quad \text{with} \quad T(U_\alpha) \subset U_\alpha$$

and such that U_α has a basis $v_1, v_2, \ldots, v_{m_\alpha}$ with

$$T(v_1) = 0 \quad \text{and} \quad T(v_i) = v_{i-1} \text{ for } i = 2, 3, \ldots, m_\alpha.$$

As a corollary, if $T : V \to V$ is any nilpotent operator, we can find a basis $v_1, v_2, \ldots, v_n$ such that for each i, either $T(v_i) = v_{i-1}$ or $T(v_i) = 0$.

Proposition 2.14. Exists a basis of generalized eigenvectors
The notion of generalized kernels is exactly what allows us to get past the problem of repeated eigenvalues. Consider operator $T : V \to V$. Just as an eigenvector with eigenvalue λ is an element of $\ker(T - \lambda)$, a generalized eigenvector for T is an element of $\operatorname{gker}(T - \lambda)$, i.e., a vector killed by some power of $T - \lambda$.

If T is any operator on the vector space V, we have

$$V = \bigoplus_{\lambda \in k} \operatorname{gker}(T - \lambda);$$

in other words, V always has a basis of generalized eigenvectors for a given operator T.

Proof. We simply induct on the dimension of V. We do know that T has at least one eigenvector; that is, for some λ we have $\operatorname{gker}(T-\lambda) \neq 0$. Now we invoke Proposition 1.1.2 to write

$$V = \operatorname{gker}(T-\lambda) \oplus \operatorname{gim}(T-\lambda)$$

and apply the inductive hypothesis to $\operatorname{gim}(T-\lambda)$. □

Theorem 2.15. Jordan Canonical Form
We may write any operator $T : V \to V$ as a diagonal matrix (with all the eigenvalues) plus an operator with 0s and 1s in the upper diagonal.

2.3 Lectures 13–16: Bilinear forms and inner product spaces, category theory

An overview of these lectures is as follows:

- Lecture 13 lays some groundwork by introducing characteristic and minimal polynomials, and then giving an interlude on category theory. Then it introduces bilinear forms.
- Lecture 14 introduces inner product spaces, a specific example of bilinear forms on vector spaces over $\mathbb{R}$. Then it discusses orthogonality, including orthogonal subspaces and orthonormal bases.
- Lecture 15 discusses operators on inner product spaces, including orthogonal and self-adjoint operators. Discussed properties include the spectral theorem.
- Lecture 16 introduces Hermitian inner products. It first generalizes fields and vector spaces to rings and modules. Then it defines Hermitian inner products and discusses self-adjoint and unitary operators.

2.4 Lectures 17–18: Multilinear algebra, tensor products

We begin by defining the tensor product and giving its three most standard constructions, beginning with the intuitive basis pairs construction and ending with the universality property. One important result is that $V^* \otimes W \cong \mathrm{Hom}(V, W)$. The language of tensor products also gives rise to a natural definition of the trace.

3 Revisiting Group Theory

In Lectures 19–26, we revisit group theory, roughly covering Artin chapters 6 and 7.

- **Lecture 19: Group actions**, roughly corresponds to Artin 6.7–6.11, 7.1, and 7.6.
- **Lecture 20: The class equation and applications to p-groups**, roughly corresponds to Artin 7.2–7.3.
- **Lecture 21: Finite rotation groups, $SO(3)$,** corresponds to Artin 6.12. (Notes on this lecture are omitted.)
- **Lecture 22: Conjugation in the symmetric and alternating groups**, roughly corresponds to Artin 7.5.
- **Lectures 23–24: Sylow theorems**, roughly corresponds to Artin 7.7–7.8.
- **Lectures 25–26: Free groups, semidirect products, abelian groups,** wrap up some odds and ends in group theory. Lecture 25, roughly corresponding to Artin 7.9–7.10, defines free groups and discusses generators and relations. Lecture 26 discusses semidirect products (those cursed things) and abelian groups (including Structure Theorem and characters).

3.1 Lecture 19: Group actions

We begin with lecture 19, which roughly corresponds to Artin 6.7–6.11, 7.1, and 7.6. First we establish some definitions.

Definition 3.1. Action of a group on a set
Let G be a group and S a set. By an action of G on S we will mean a map

$$\phi : G \times S \to S,$$

where we write gs for $\phi(g, s)$, satisfying the two axioms

$$\begin{aligned} g(hs) = (gh)s \quad & \forall g, h \in G \text{ and } s \in S \\ es = s \quad & \forall s \in S. \end{aligned}$$

Alternatively, we may define a group action by a homomorphism

$$\rho : G \to \mathrm{Perm}(S).$$

To see this, consider a group action ϕ. Then for each $g \in G$ we get an automorphism $m_g : S \to S$, which is a homomorphism by the axioms of group actions and bijective with inverse $m_{g^{-1}}$. Hence each g determines a permutation of S.

Definition 3.2. Transitivity
An action $\phi : G \times S \to S$ is transitive if for all $s, t \in G$, there exists an element $g \in G$ with $gs = t$; equivalently, if for any $s \in S$, the map $G \to S$ sending g to gs is surjective. Note that this is true for some $s \in S$ iff it's true for all $s \in S$.

Similarly, an action is twice transitive if any pair of distinct elements of S can be carried into any other such pair by an element of G; that is, for all $s, t, u, v \in S$ with $s \neq u$ and $t \neq v$, there exists a $g \in G$ with $gs = t$ and $gu = v$.

Definition 3.3. Faithful
An operation $\phi : G \times S \to S$ is faithful if e is the only element in G fixing every $s \in S$. Alternatively, considering the permutation representation $\rho : G \to \mathrm{Perm}(S)$, the action is faithful if ρ is injective, i.e., if e is the only element in G such that $\rho(e)$ is the identity permutation.

An example of a faithful operation is the action of G on itself by left multiplication. We thus have Cayley's Theorem: this faithful operation gives us an injective map $\rho : G \to S_n$, and G being isomorphic to its image implies that any finite group is some subgroup of S_n.

Now we have three important constructions.

Definition 3.4. Orbits
Consider the action $\phi : G \times S \to S$ and some $s \in S$. We define the orbit O_s of $s \in S$ as the subset

$$O_s \coloneqq \{t \in S : t = gs \text{ for some } g \in G\}.$$

Alternatively, these are the equivalence classes of the equivalence relation on S given by

$$s \sim t \quad \iff \quad gs = t \text{ for some } g \in G.$$

Observe that S is the disjoint union of orbits, and note that to transitivity is tantamount to saying S is one big equivalence class.

Definition 3.5. Stabilizers
Consider action $\phi : G \times S \to S$ and suppose $s \in S$. Define the stabilizer of s to be the subgroup of elements of G that carry s to itself; that is

$$H_s = \text{stab}(s) \coloneqq \{g \in G \mid gs = s\}.$$

One important observation: if $s' \in S$ is any element of the orbit O_s of s, i.e., $s' = as$ for some $a \in G$, then the stabilizer $H_{s'}$ of s' is conjugate to the stabilizer H_s of s; specifically,

$$H_{s'} = a \cdot H_s \cdot a^{-1}.$$

In the case of G acting on itself by conjugation, the stabilizer of an element g is called the centralizer or normalizer of g.

Proposition 3.6. Orbit-stabilizer, bijection between orbits and the quotient by the stabilizer
Consider action $\phi : G \times S \to S$ and suppose $s \in S$. Then we have an intuitive bijection between the orbit O_s of s and the set G/H of cosets of the stabilizer $H = \text{stab}(s)$ in G.

Consequently, we have for any $s \in S$ the orbit-stabilizer theorem,

$$|O_s| \cdot |H_s| = |G|.$$

Definition 3.7. Fixed point sets
Consider action $\phi : G \times S \to S$ and suppose $g \in G$. Define the fixed point set S^g to be the set of elements of s fixed by g; that is,

$$S^g \coloneqq \{s \in S : gs = s\}.$$

Now let's dive into some applications of group actions.

Theorem 3.8. Burnside's formula
Let G be a finite group acting on a finite set S, and let m be the number of orbits of the action. Then

$$\sum_{g \in G} |S^g| = m|G|.$$

Proof. The proof involves introducing an auxiliary set: we define

$$\Gamma \coloneqq \{(g, s) \in G \times S \mid gs = s\}$$

and let $\pi_1 : \Gamma \to G$ and $\pi_2 : \Gamma \to S$ be the two projections. Now, for every $g \in G$, the fiber $\pi_1^{-1}(g)$ is just the fixed point set S^g of g. Thus

$$|\Gamma| = \sum_{g \in G} |S_g|$$

On the other hand, we can also calculate the cardinality of Γ via the second projection: since the fiber $\pi_2^{-1}(s)$ of Γ over $s \in S$ is just the stabilizer H_s of s, we have

$$|\Gamma| = \sum_{s \in S} |H_s|$$

But we can simplify the latter expression for $|\Gamma|$: if s and $t \in S$ are in the same orbit O, their stabilizers are conjugate subgroups of G, and so have the same cardinality; moreover, that cardinality is equal to $|G|/|O|$, the order of G divided by the cardinality of the orbit. Thus, if we denote the set of orbits by C, we have

$$|\Gamma| = \sum_{O \in C} \sum_{s \in O} \frac{|G|}{|O|} = \sum_{O \in C} |G| = m|G|,$$

establishing Burnside's formula. □

As an example of Burnside's, consider homework problem 7.6. How many different bracelets can you make with 4 white beads and 4 black beads? Effectively, we consider the action of D_8 on the set of all bead arrangements, and then the number of bracelets is the number of orbits. To help this calculation, it is worth noting that elements of a group which are conjugate have the same number of fixed points, i.e., we need only consider the conjugacy classes (and only up to isomorphism).

3.2 Lecture 20: The class equation and applications to p-groups

We now enter lecture 20, which roughly corresponds to Artin 7.2–7.3. In this lecture and in lecture 22, we will often see the action of a group G on itself by conjugation.

Example 3.9. G acts on itself by conjugation
An important group action is the action of G on itself by conjugation. Then

- the conjugacy classes C are the orbits, each with order dividing $|G|$ by orbit-stabilizer; and
- at least one of the conjugacy classes has size 1, for we have the class of the identity $e \in G$.

Definition 3.10. Class equation
A group G is the disjoint union of its conjugacy classes, giving us the class equation

$$|G| = \sum_{C \in \mathcal{C}} |C|.$$

This gives strong restrictions on the sizes of conjugacy classes.

Definition 3.11. p-groups
Let p be a prime. A finite group is called a p-group if its order $|G| = p^n$ is a power of p.

The class equation gives especially strong restrictions on the sizes of conjugacy classes for p-groups. For example, we can easily derive that the center $Z(G)$ is nontrivial, i.e., that the identity cannot be the only conjugacy class of size 1, because every class has order p^k for some k and the sum of the orders is a multiple of p.

3.3 Lecture 21: Finite rotation groups, $SO(3)$

This lecture corresponds to Artin 6.12.

3.4 Lecture 22: Conjugation in the symmetric and alternating groups

In lecture 22, we discuss conjugation in the symmetric and alternating groups. This roughly corresponds to Artin 7.5.

Proposition 3.12. Conjugation in the symmetric group
Suppose we have a simple k-cycle $\sigma \in S_n$ and any permutation $\tau \in S_n$. Then the conjugate $\tau\sigma\tau^{-1}$ is again a k-cycle given by

$$\tau\sigma\tau^{-1} = \big(\tau\,(a_1)\,\tau\,(a_2)\ldots\tau\,(a_k)\,\big).$$

The analogous holds for a product of disjoint cycles. Thus two permutations are conjugate in S_n iff they have the same cycle lengths, so in general, the number of conjugacy classes in S_n is the partition function $p(n)$ defined as the number of integer sequences $\beta = (\beta_1, \beta_2, \ldots)$ with

$$\sum i\beta_i = n,$$

where β_k denotes the number of k-cycles. This sizes of each conjugacy class are easy to calculate combinatorially.

Proposition 3.13. Parity of a permutation
Suppose we write a permutation σ as a product of transpositions. Then the number of transpositions is the same for all such representations.

Of course a p-cycle is the product of $p-1$ transpositions. So supposing σ is the product of k disjoint cycles of lengths $l_1, \ldots, l_k$, then the parity of σ is given by

$$\sum_{i=1}^{k}(l_i - 1).$$

We also define the signature

$$\operatorname{sgn}(\sigma) = \begin{cases} +1 & \text{if } \sigma \text{ is even,} \\ -1 & \text{if } \sigma \text{ is odd.} \end{cases}$$

Definition 3.14. Alternating group
Define $A_n \subset S_n$ as the subgroup of S_n containing only even permutations. Observe that the A_n is precisely the kernel of the sgn homomorphism defined above.

Definition 3.15. Simple group
A simple group is a group whose only normal subgroups are the two trivial subgroups.

Proposition 3.16. Conjugacy classes in A_n
Suppose we have a conjugacy class $C_\beta \subset S_n$. Then either

$$C_\beta \cap A_n = \emptyset \quad \text{if } \sum \beta_i \text{ odd},$$
$$C_\beta \subset A_n \quad \text{if } \sum \beta_i \text{ even.} s$$

Considering the latter case, we have that C_β is either still one conjugacy class in A_n, or it is split into two conjugacy classes of equal size (see homework 8 problem 1).

Proposition 3.17. A_n is simple for $n \geq 5$
To show A_n is simple for particular n, we need only realize that any normal subgroup is a union of conjugacy classes that, in particular, must contain the trivial subgroup of order 1. Then we may calculate the sizes of the conjugacy classes and see that no union of them (containing that trivial subgroup) will have size dividing the order of A_n, which would necessarily occur in any subgroup.

To show A_n is simple in the general for $n \geq 5$, the proof will consist of three statements:

- A_n is generated by 3-cycles;
- 3-cycles form a single conjugacy class in A_n for $n \geq 5$; and
- If $H \subset A_n$ is a nontrivial normal subgroup and $n \geq 5$ then H contains a 3-cycle.

The second statement is obvious; the first two are proved in lecture notes 23.

3.5 Lectures 23–24: Sylow theorems

In lectures 23–24, we discuss the Sylow theorems and use them to classify groups of various orders. This section roughly corresponds to Artin 7.7–7.8.

3.5.1 Statement of the Sylow theorems

Consider a group G of order n, and let p be a prime integer that dividing n. Let p^e be the largest power of p dividing n, so that

$$n = p^e m, \ p \nmid n.$$

Subgroups $H \subset G$ of order p^e are called Sylow p-subgroups of G, i.e., a Sylow p-subgroup is a p-group whose index in the group isn't divisible by p.

Theorem 3.18. First Sylow Theorem
A finite group whose order is divisible by a prime p contains a Sylow p-subgroup.

Corollary 3.19.
A finite group whose order is divisible by a prime p contains an element of order p.

Specifically, suppose G is such a group and H a Sylow p-subgroup of G. Suppose $x \in H$ such that x is not the identity. We have $\text{ord}(x) \mid |H|$, so $\text{ord}(x) = p^k$ for some k. Then $x^{p^{k-1}}$ has order p.

Theorem 3.20. Second Sylow Theorem
Let G be a finite group whose order is divisible by a prime p.

(a) The Sylow p-subgroups of G are conjugate subgroups.

(b) Every subgroup of G that is a p-group is contained in a Sylow p-subgroup.

A conjugate subgroup of a Sylow p-subgroup will be a Sylow p-subgroup too. This also implies that G has exactly one Sylow p-subgroup iff that subgroup is normal.

Theorem 3.21. Third Sylow Theorem
If s_p is the number of p-Sylow subgroups of G, then

$$s_p \mid m$$
$$s_p \equiv 1 \pmod{p}.$$

3.5.2 Classifying groups with Sylow

First let us recall the following:

Proposition 3.22. Every group of prime order is cyclic
For a prime number p, every group of order p is cyclic: each element in the group besides the identity has order p by Lagrange's theorem, so the group has a generator. In fact each nonidentity element of the group is a generator.

Now let us use the Sylow theorems to classify some groups.

Example 3.23. Classifying groups of order 15
(a) Every group of order 15 is cyclic.

Proof. Let G be a group of order 15 and s_3, s_5 its number of Sylow 3- and 5-subgroups, respectively. By the Third Sylow Theorem, s_3 divides 5 and is congruent 1 modulo 3, i.e., there is one Sylow 3-subgroup, say H, and it is normal. Similarly, there is just one Sylow 5-subgroup, say K, and it is normal. The subgroup H is cyclic of order 3, and K is cyclic of order 5. The intersection $H \cap K$ is the trivial group, implying by Artin 2.11.4(d) that $G \cong H \times K \cong C_{15}$, as desired. □

Example 3.24. Classifying groups of order 6
There are two isomorphism classes of groups of order 6, the class of the cyclic group C_6 and the class of the symmetric group S_3.

Proof. Let G be a group of order 6. The First Sylow Theorem tells us that G contains a Sylow 3-subgroup $H \cong C_3$ and a Sylow 2-subgroup $K \cong C_2$. The Third Sylow Theorem tells us that s_3 divides 2 and is congruent 1 modulo 3, i.e., there is one Sylow 3-subgroup H, and it is normal. Similarly, theorem also tells us that s_2 divides 3 and is congruent 1 modulo 2, i.e., $s_2 = 1$ or $s_2 = 3$.

Case 1: If $s_2 = 1$, then as in the previous example, $G \cong H \times K \cong C_6$.

Case 2: Now suppose G contains 3 Sylow 2-subgroups, say K_1, K_2, K_3. Consider the action of G on the set $S = \{[K_1], [K_2], [K_3]\}$ by conjugation, i.e., the homomorphism $\varphi : G \to S_3$. The Second Sylow Theorem tells us that the operation on S is transitive, so $\mathrm{stab}([K_i]) \subset G$ has order 2 and is thus equal to K_i. Since $K_1 \cap K_2 = \{1\}$, the identity is the only element of G that fixes all elements of S. The operation is faithful, i.e., the permutation representation φ is injective. Since G and S_3 have the same order, φ is an isomorphism, so $G \cong S_3$, as desired. □

Example 3.25. Classifying groups of order 21
There are two isomorphism classes of groups of order 21: the class of the cyclic group C_{21}, and the class of a group G generated by two elements x and y that satisfy the relations $x^7 = 1, y^3 = 1, yx = x^2y$.

Proof. Let G be a group of order 21. The Third Sylow Theorem shows that the Sylow 7-subgroup K must be normal, and that the number of Sylow 3-subgroups is 1 or 7. Let x be a generator for K, and let y be a generator for one of the Sylow 3-subgroups H. Then $x^7 = 1$ and $y^3 = 1$, so $H \cap K = \{1\}$, and therefore the product map $H \times K \to G$ is injective by Artin 2.11.4(a). Since G has order 21, the product map is bijective. The elements of G are the products $x^i y^j$ with $0 \le i < 7$ and $0 \le j < 3$.

Since K is normal, $yxy^{-1} \in K$ is some power of x, say, x^i with i in the range $1 \le i < 7$. So we have

$$x^7 = 1, y^3 = 1, yx = x^i y.$$

These relations are sufficient to determine the multiplication table for the group, for knowing i, we may apply the relation $yx = x^i y$ repeatedly to reduce any expression of the form $x^\alpha y^\beta x^\gamma y^\delta$ to one of the form $x^\mu y^\nu$.

However, the relation $y^3 = 1$ restricts the possible i, because it implies that $y^3 x y^{-3} = x$:

$$x = y^3 x y^{-3} = y^2 x^i y^{-2} = y x^{i^2} y^{-1} = x^{i^3}.$$

Therefore $i^3 \equiv 1$ modulo 7. This tells us that i must be 1, 2, or 4.

Case 1: $yxy^{-1} = x$, i.e., x commutes with y. Then both H and K are normal subgroups, so as before, $G \cong H \times K \cong C_7 \times C_3 \cong C_{21}$.

Case 2: $yxy^{-1} = x^2$. As noted above, the multiplication table is determined. But we still have to show that this group actually exists. This comes down to showing that the relations don't cause the group to collapse, as happens when $i = 3$. A systematic method for doing this is the Todd-Coxeter Algorithm, in Artin Section 7.11. Another way is to exhibit the group explicitly, for example as a group of matrices, but some experimentation is required to do this.

Since we require an element of order 7, we may try to find suitable matrices with entries modulo 7. At least we can write down a 2×2 matrix with entries in $\mathbb{F}_7$ of order 7, namely the matrix x below. Then y can be found by trial and error. The matrices

$$x = \begin{bmatrix} 1 & 1 \\ & 1 \end{bmatrix}, \quad \text{and} \quad y = \begin{bmatrix} 2 & \\ & 1 \end{bmatrix}$$

with entries in $\mathbb{F}_7$ satisfy the relations $x^7 = 1, y^3 = 1, yx = x^2 y$, and they generate a group of order 21.

Case 3: $yxy^{-1} = x^4$. Then $y^2 x y^{-2} = x^2$. We note that y^2 is also an element of order 3. So we may replace y by y^2, which is another generator for H. The result is that the exponent 4 is replaced by 2, which puts us back in the previous case.

Thus there are two isomorphism classes of groups of order 21, as desired. □

In lecture 25, we also tackle a harder example: classifying all groups of order 12. The derivation may be found in lecture 25 notes, Artin 7.8, or Dummit and Foote (chapter 5, page 182). Another harder example of group classification is homework 9 problem 10, classifying all groups of order 18, which also uses semidirect products.

3.6 Lectures 25–26: Free groups, semidirect products, abelian groups

In our final lectures on group theory, we wrap up some odds and ends. We begin with lecture 25, where we precisely define free groups and discuss generators and relations. This corresponds to Artin 7.9–7.10.

3.6.1 Free groups and generators and relations

Definition 3.26. Free groups
The free group F_n on n generators $x_1, \ldots, x_n$ is defined to be the set of all words

$$x_{i_1}^{\alpha_1} x_{i_2}^{\alpha_2} \cdots x_{i_k}^{\alpha_k}$$

for some $k = 0, 1, 2 \ldots$, with the conditions

$$\alpha_l \in \mathbb{Z} \backslash \{0\} \quad \text{and} \quad i_l \neq i_{l+1} \text{ for all } l.$$

The group law is defined by concatenation and simplification: we just place one word after the other, and then simplify the resulting string to satisfy the conditions above.

Definition 3.27. Specifying groups with generators and relations
The free group has a universal property: if G is any group, and $g_1, \ldots, g_n \in G$ any n elements of G, we get a unique map

$$\phi_g : F_n \to G \quad \text{sending} \quad x_i \mapsto g_i.$$

To say that the elements $g_1, \ldots, g_n \in G$ generate G simply means that ϕ_g is surjective.

Suppose now that G is any group, and $g_1, \ldots, g_n$ generate G. Let $R \coloneqq \ker(\phi_g)$, so that we have an exact sequence

$$\{e\} \to R \to F_n \to G \to \{e\}.$$

R is called the group of relations on the generators g_i, and specifying R as a subgroup of F_n in turn determines G. Thus we have a way of specifying the group G.
In particular, let $r_1, \ldots, r_n \in F_n$ be any elements of the free group F_n, and let $R \subset F_n$ be the smallest normal subgroup of F_n containing $\{r_1, \ldots, r_k\}$. The group $G \coloneqq F_n/R$ is called the group with generators x_i and relations r_j, denoted

$$G = \langle x_1, \ldots, x_n \mid r_1, \ldots, r_k \rangle .$$

Remark 3.28. On using generators and relations
Note that it's not always clear how large a subgroup $R \subset F_n$ of relations will be. As a particular example, there is a problem called the *word problem*: given $r_1, \ldots, r_k \in F_n$, when is the smallest normal subgroup $R \subset F_n$ containing $\{r_1, \ldots, r_k\}$ equal to F_n ? In other words, when is the group with generators x_i and relations r_j the trivial group?

Also note that it is not generally feasible to verify without, say, a multiplication table, that a group specified by generators and relations does not collapse.

Now in lecture 26, we discuss semidirect products and abelian groups.

3.6.2 Semidirect products

Definition 3.29. Semidirect product
Given that G contains trivially intersecting subgroups N and H such that N is normal and $G = NH$, the semidirect product enables us to classify G. Let

$$\{e\} \longrightarrow N \xrightarrow{i} G \xrightarrow{\pi} H \longrightarrow \{e\}$$

be an exact sequence of groups. If there exists a homomorphism

$$\alpha : H \to G \quad \text{ such that } \pi \circ \alpha = \mathrm{id}_H,$$

then we say G is the semidirect product of N and H, and write $G = N \rtimes H$.

If we think of the quotient H as the set of cosets of N in G, then the map α is simply picking one element $\alpha(h)$ in each coset h, in such a way that the image $\alpha(H) \subset G$ is a subgroup. In this case, we often suppress the α and simply think of H as a subgroup of G. In these terms, and assuming G is finite, the situation can be described by saying that the group G has subgroups $N, H \subset G$ such that

$$N \cap H = \{e\}; \quad |N| \cdot |H| = |G|, \quad \text{ and } \quad N \subset G \text{ is normal.}$$

Proposition 3.30. Classifying semidirect products
Something to do with the classes of automorphisms. See lecture notes.

3.6.3 Abelian groups and characters

First, abelian groups are completely classified with the structure theorem.

Theorem 3.31. Structure theorem
Every finite abelian group is a direct sum of cyclic groups of prime power orders, i.e., for any abelian G, we may write

$$G = \mathbb{Z}/n_1 \times \mathbb{Z}/n_2 \times \cdots \times \mathbb{Z}/n_k$$

for some $n_1, \ldots, n_k$. Of course different choice of the n_i may yield the same group, for we have $\mathbb{Z}/n_1 \times \mathbb{Z}/n_2 \cong Z/n_1 n_2$ if $\gcd(n_1, n_2) = 1$.

So instead of classifying abelian groups, here we will introduce the characters of abelian groups.

Definition 3.32. Characters of abelian groups, dual group
Let G be a finite abelian group. By a character of G we will mean simply a homomorphism

$$\chi : G \to \mathbb{C}^*$$

from G to the multiplicative group $\mathbb{C}^*$ of nonzero complex numbers. Because every element $g \in G$ has finite order, any such homomorphism $\chi : G \to \mathbb{C}^*$ necessarily factors through the inclusion

$$S^1 \coloneqq \{z \in \mathbb{C} : |z| = 1\} \subset \mathbb{C}^*.$$

Definition 3.33. Dual group
The set of characters of G forms the (multiplicative) dual group $\widehat{G}$. Given $\alpha, \beta \in \widehat{G}$, we define

$$(\alpha\beta)(g) \coloneqq \alpha(g) \cdot \beta(g).$$

We may also verify that given two finite abelian groups G, H, we have

$$\widehat{G \times H} \cong \widehat{G} \times \widehat{H}.$$

Given any cyclic group $\mathbb{Z}/n$, any character on $\mathbb{Z}/n$ takes on values that are n^{th} roots of unity, i.e., values in the subgroup

$$\Gamma_n \coloneqq \{z \in \mathbb{C}^* : z^n = 1\} = \left\{e^{2\pi i k/n} : 0 \leq k \leq n-1\right\} \subset \mathbb{C}^*$$

and is determined by its value $\chi(x)$ on any generator $x \in \mathbb{Z}/n$. Thus we have (non-canonically) $\widehat{\mathbb{Z}/n} \cong \Gamma_n \cong \mathbb{Z}/n$, and since any finite abelian group is a product of cyclic groups $\mathbb{Z}/n$, it follows that for any finite abelian group G we have

$$G \cong \widehat{G}.$$

4 Representation Theory

One of the major motivations of representation theory is the following: Given abstract group G, how can we describe all the ways that G can be embedded in (or more generally mapped to) a linear group GL_n? Lectures 27–34 discuss the representation theory of finite groups, roughly covering Fulton and Harris chapters 1–3. We introduce the fundamental language of representation theory and Schur's in Lecture 27, and the main goals of our discussion are to know for a given group G the following:

- How to find all irreducible representations of G;
- For a given representation V of G, say how V decomposes as a direct sum of irreducible representations; and
- For given representations V, W of G, describe other representations built up from these by multilinear-algebraic constructions (like $V \otimes W$, $\mathrm{Hom}(V, W), \mathrm{Sym}^n V, \wedge^n V$, etc.) as direct sums of irreducibles. (Note that by relations like $V \otimes (U \oplus W) = (V \otimes U) \oplus (V \otimes W)$ it is enough to do this for V, W irreducible representations.)

As a rough roadmap/breakdown of our representation theory exploration (this is taken from the semester-end review session):

- Understand group actions.
- Define a representation.
- Every group has the trivial and regular representations.
- Define what it means for a representation to be faithful; V is faithful if ρ is injective, or equivalently, if $\chi_V(g) = \dim V \iff g = e$.
- Define irreducible representation; V irreducible if it has no nontrivial invariant subspaces.
- Define G-linear homomorphisms; then introduce Schur's lemma.
- Define the character of a representation; then the Hermitian inner product.
- Theorem: The characters of the irreducible representations form an orthonormal basis.
- There are some nice properties of characters, e.g., each eigenvalue is a root of unity.
- It is also good to understand the motivation for why we care about characters.
- We can determine representations by factoring through quotient map. If $H \subset G$ normal, then we may construct a map $\pi : G \to G/H$ and then a map $\alpha : G/H \to \mathbb{C}^*$, and then set $\rho = \pi \circ \alpha$.

The specific breakdown of lectures is as follows:

- **Lecture 27: Representation theory fundamentals**, roughly corresponding to Fulton and Harris 1.1–1.2.
- **Lecture 28: Abelian groups and S_3**, roughly corresponding to Fulton and Harris 1.3.
- **Lecture 29: Characters**, roughly corresponding to Fulton and Harris 2.1.
- **Lectures 30–32: Projection formulas**, roughly corresponding to Fulton and Harris 2.1–2.4.
- **Lectures 33–34: Induced representations**, roughly corresponding to Fulton and Harris 3.3. (This lecture is skipped in these notes.)

4.1 Lecture 27: Representation theory fundamentals

We begin lecture 27 with the fundamental definitions of representation theory. Then we discuss the important theorem of complete reducibility, which motivates much of our exploration of representation theory. Finally, we prove a very powerful result: Schur's lemma.

We begin by defining a representation of a group. Note the parallels between a group action and a representation of a group.

Definition 4.1. Representation of a group
Let G be a finite group. By a representation V of G, we will mean a complex vector space V with a homomorphism

$$\rho : G \to GL(V).$$

We will generally denote the representation as just V, rather than (V, ρ). If ρ is injective, then we say the representation is faithful.

Equivalently, a representation of G is a complex v.s. V with an action of G, i.e., a map

$$G \times V \to V,$$

where as always gv denotes the image of (g, v). This must satisfy the usual group action axioms:

$$(gh)v = g(hv) \quad \text{and} \quad ev = v \quad \forall\ g, h \in G,\ v \in V.$$

Additionally, we require that for each $g \in G$, the map $\rho_g : V \to V$ sending $v \in V$ to gv is linear, i.e.,

$$g(\lambda v) = \lambda g v \quad \text{and} \quad g(v + w) = gv + gw$$

for all $v, w \in V$ and $\lambda \in \mathbb{C}$.

Remark 4.2. Reasons to choose $\mathbb{C}$
Choosing to define V over the field $\mathbb{C}$ is convenient because $\mathbb{C}$ has characteristic 0 and is algebraically closed. Notably, complete reducibility, introduced below, fails in characteristic p.

Definition 4.3. Homomorphism of representations
If V and W are representations of G, then a homomorphism of representations $\phi : V \to W$ is a linear map $\phi : V \to W$ that respects the action of G, i.e., for any $g \in G$ and $v \in V$ we have

$$\phi(gv) = g(\phi(v)),$$

or equivalently, we have the commutative diagram

$$\begin{array}{ccc} V & \xrightarrow{\phi} & W \\ {\scriptstyle g}\downarrow & & \downarrow{\scriptstyle g} \\ V & \xrightarrow[\phi]{} & W \end{array}$$

Remark 4.4. Notation
We will generally denote representations by just V, the complex vector space over which the group acts, rather than (V, ρ).

We will refer to $\mathrm{Hom}(V, W)$ as the space of all linear maps $V \to W$, and $\mathrm{Hom}_G(V, W)$ as the linear subspace of all homomorphisms of representations. If a linear map $\phi : V \to W$ is a homomorphism of representations, we'll say that it is G-linear.

Definition 4.5. Subrepresentation
If V is any representation of G, then a subrepresentation $W \subset V$ is a vector subspace W such that $g(W) = W$ for all $g \in G$; equivalently, W is a representation of G and the inclusion $W \hookrightarrow V$ is a homomorphism of representations. Another word for such a W is an invariant subspace of V.

Definition 4.6. Irreducible
A representation V of G is irreducible if it has no invariant subspaces/subrepresentations except the trivial ones $W = 0$ and $W = V$.

Lemma 4.7. Existence of an invariant Hermitian inner product
If V is any representation of the finite group G, there exists a Hermitian inner product H on V invariant under G; that is, such that

$$H(gv, gw) = H(v, w) \quad \forall\ v, w \in V,\ g \in G.$$

To construct such H, start with any Hermitian inner product H_0 on V, and define

$$H(v, w) \coloneqq \sum_{g \in G} H_0(gv, gw).$$

This is clearly invariant under G, and it's positive definite: for any $v \neq 0 \in V$, we have $H(v, v) = \sum H_0(gv, gv) > 0$. (Note that we couldn't have used a symmetric bilinear form B_0 for this purpose; when we sum, we might get 0.)

Theorem 4.8. Complete reducibility
Let V be any representation of G. If $W \subset V$ an invariant subspace, then there exists a complementary invariant subspace; that is, a subspace $U \subset V$ such that

$$gU = U\ \forall g \in G \quad \text{and} \quad V = W \oplus U.$$

As such, any representation of G is the direct sum of irreducible representations.

Proof. This follows immediately from the previous lemma. Simply take $U = W^{\perp}$ the orthogonal complement of $W \subset V$.

□

Thus, our mission is clear: given a finite group G, our goal will be to find all irreducible representations of G.

Definition 4.9. Dual representation
If V is a representation of G with map $\rho : G \to GL(V)$, we define the dual representation $\rho^* : G \to GL(V^*)$ to be given by

$$\rho^*(g) \coloneqq {}^t\rho\left(g^{-1}\right).$$

Definition 4.10. Other related representations
Suppose V and W are representations of G. Then we may give the following related vector spaces the structure of a representation as follows:

- Direct sum: The action of g on $V \oplus W$ is

$$g(v, w) \coloneqq (gv, gw).$$

- Tensor product: For $V \otimes W$,

$$g(v \otimes w) \coloneqq (gv \otimes gw)$$

  Of course, $V^{\otimes n}, \operatorname{Sym}^n V$, and $\wedge^n V$ are also naturally representations of G.

- Vector space of homomorphisms: For $\varphi \in \operatorname{Hom}(V, W)$, we define

$$g(\varphi) = g \circ \varphi \circ g^{-1},$$

  where on the LHS g acts $\operatorname{Hom}(V, W)$, and on the RHS g acts on W while g^{-1} acts on V.

4.1.1 Schur's lemma

The main tool we have for analyzing representations of a given group G is Schur's lemma. It sounds simple, but as you'll see it's quite a powerful tool.

Lemma 4.11. Schur's lemma
Let G be a finite group and V and W irreducible representations of G; let $\phi : V \to W$ be any homomorphism of representations.

1. Either ϕ is an isomorphism or $\phi = 0$; and
2. If $V = W$, then $\phi = \lambda \cdot I$ with $\lambda \in \mathbb{C}$ and I the identity map.

In other words, $\dim \mathrm{Hom}_G(V, W)$ is either 0 or 1,

$$\dim \mathrm{Hom}_G(V, W) = \begin{cases} 1, & \text{if } V \cong W; \\ 0 & \text{if not.} \end{cases}$$

Thus, if

$$V = \bigoplus V_\alpha^{\oplus n_\alpha} \quad \text{and} \quad W = \bigoplus V_\alpha^{\oplus m_\alpha}$$

are any two representations, then any homomorphism of representations $\phi : V \to W$ must carry the summand $V_\alpha^{\oplus n_\alpha}$ of V to the summand $V_\alpha^{\oplus m_\alpha}$ of W. Note also that

$$\dim \mathrm{Hom}_G(V, W) = \sum n_\alpha m_\alpha.$$

Proof. The first statement is immediate, since $\ker(\phi)$ is an invariant subspace of V and $\mathrm{im}(\phi)$ is an invariant subspace of W. As for the second, if $W = V$ then since $\mathbb{C}$ is algebraically closed the map ϕ must have an eigenvalue λ; in other words, $\phi - \lambda \cdot I$ has a kernel, and from the first part it follows that $\phi - \lambda \cdot I = 0$. □

4.2 Lecture 28: Abelian groups and S_3

In lecture 28, we begin by introducing a special case of representations: permutation representations. Then we discuss characterize representations of (1) abelian groups, and (2) the symmetric group S_3.

4.2.1 Permutation representations

Definition 4.12. Permutation representations
Suppose a finite group G acts on a set S with $|S| = n$. We can then form a vector space V from basis vectors corresponding to the elements of S, i.e.,

$$V \coloneqq \left\{ \sum_{s \in S} c_s \cdot e_s \right\}.$$

We may define on this V a permutation representation: if G acts on S, then it acts linearly on V by sending the basis vector e_s to the basis vector e_{gs}.

There is one special case of this that is useful. Any group G acts on itself by left multiplication, so letting $S = G$, then the corresponding permutation representation of G is called the regular representation of G. This is always faithful, which in particular says that every finite group can be realized as a subgroup of GL_n for some n.

More significantly, we will see next week that every irreducible representation of G is a sub-representation of the regular representation, which will give us in theory a way of constructing all irreducible representations of G.

4.2.2 Representations of Abelian groups

Example 4.13. Representations of abelian groups
If V is a representation of G, then suppressing ρ, we have for every $g \in G$ a linear map $g : V \to V$. But this linear map will not in general be G-linear, for to have $g : V \to V$ a homomorphism of representations would require that for any $h \in G$,

$$h(g(v)) = g(h(v)).$$

Of course, one circumstance that the maps $g : V \to V$ are G-linear is when G is abelian! In this case Schur's lemma has major implications: given abelian G and any representation V, Schur tells us that for all $g \in G$, the associated map $g : V \to V$ is just multiplication by a scalar λ. In particular, this means every subspace $W \subset V$ is invariant under G and hence any irreducible representation of an abelian group is one-dimensional.

Now, the automorphism group of a one-dimensional complex vector space is just $\mathbb{C}^*$, so an irreducible representation of an abelian group G is simply a homomorphism $G \to \mathbb{C}^*$, or what we've called a character of G. All in all, then, we see that the set of irreducible representations of G is simply the dual group $\widehat{G}$. (Note that under this bijection, the group law on $\widehat{G}$ corresponds to tensor product of representations.)

4.2.3 Representations of S_3

Part I: Characterizing representations of S_3

Let us characterize the representations of first non-abelian group, S_3. Consider S_3 and, by way of notation, denote $\sigma = (12)$ and $\tau = (123)$. Also note that these satisfy the basic relation

$$\sigma\tau\sigma = \tau^2.$$

Also take $\omega \in \mathbb{C}^*$ to be any cube root of 1. Now, say V is any representation of S_3. Since we understand representations of $A_3 \cong \mathbb{Z}/3$, we can restrict the action of S_3 on V to the subgroup A_3; this gives us a decomposition

$$V = V_0 \oplus V_1 \oplus V_2$$

where τ acts on V_1 by multiplication by ω, τ acts on V_2 by multiplication by ω^2, and τ acts trivially on V_0.

Now the question becomes, how does σ act on these subspaces? To answer this, suppose that $v \in V_1$ is any vector. To see where σ sends the vector v, we ask how τ acts on $\sigma(v)$; we invoke the relation above and see that

$$\tau(\sigma(v)) = \sigma\left(\tau^2(v)\right) = \sigma\left(\omega^2 v\right) = \omega^2\sigma(v)$$

In other words, if v is an eigenvector for τ with eigenvalue ω, then $\sigma(v)$ is an eigenvector for τ with eigenvalue ω^2; that is, $\sigma(v) \in V_2$. By the analogous calculation, we see that σ maps V_0 to itself, and exchanges V_1 and V_2.

Part II: The irreducible representations of S_3

Now that we have the general picture of a representation of S_3, let's consider the following three irreducible representations of S_3:

- The trivial representation U: First, there's always the trivial, 1-dimensional representation $U = \mathbb{C}$ with all of S_3 acting as the identity.
- The alternating representation U': This is again 1-dimensional, with τ acting as the identity and σ acting by multiplication by -1.
- The standard representation V: Since S_3 acts on a set with three elements, it is natural to consider its action on $\mathbb{C}^3$ by permuting the basis elements. This is not irreducible, for the subspace

  $$U \coloneqq \{(z_1, z_2, z_3) : z_1 = z_2 = z_3\}$$

  is an invariant subspace. But the theorem on complete reducibility tells us that there must be a complementary invariant subspace $V \subset \mathbb{C}^3$, and indeed it's not hard to spot: we can take

  $$V \coloneqq \{(z_1, z_2, z_3) : z_1 + z_2 + z_3 = 0\}$$

  and this is called the standard representation of S_3. To describe this representation, note that V is spanned by the vectors $v_1 = \left(\omega, \omega^2, 1\right)$ and $v_2 = \left(\omega^2, \omega, 1\right)$, which are eigenvectors for τ with eigenvalues ω and ω^2. Thus, in terms of the description above of representations of S_3 in general, V_1 and V_2 are one-dimensional eigenspaces for τ, with σ exchanging them. Note that from this description it follows that V is irreducible: if $W \subset V$ were any invariant subspace, it would have to contain some eigenvector for τ and hence (since σ switches V_1 and V_2) both V_1 and V_2.

These irreducible representations U, U', V are, in fact, all the irreducible representations of S_3. This is not hard to see: if W is any irreducible representation of S_3, then we can decompose W into eigenspaces for the action of τ, as before; we write

$$W = W_0 \oplus W_1 \oplus W_2.$$

Now, if $W_1 = 0$ then we have $W_2 = 0$ as well; thus τ acts as the identity on W, and the representation must be either U or U'. On the other hand, if $W_1 \neq 0$, just take any nonzero vector $v \in W$; the subspace $\langle v, \sigma(v) \rangle \subset W$ spanned by v and $\sigma(v)$ is then invariant under S_3 and hence equal to W, so W is the standard representation.

Part III: Decomposing arbitrary representations of S_3

Now having found the three irreducible representations of S_3, how can we decompose a given representation W of S_3 into a direct sum of copies of U, U' and V?

The key here is to look at the eigenvalues of σ and τ acting on W. To start, we'll make a table of their eigenvalues on U, U' and V:

	e-values of τ	e-values of σ
U	1	1
U'	1	-1
V	ω, ω^2	$1, -1$

Now suppose W is any representation of S_3. We know that we can write

$$W = U^{\oplus a} \oplus U^{\oplus b} \oplus V^{\oplus c}$$

for some integers a, b and c; we want to determine a, b and c. We can do this if we know the eigenvalues of σ and τ acting on W: we have

$$\begin{aligned} a + b &= \text{ multiplicity of 1 as eigenvalue of } \tau \\ c &= \text{ multiplicity of } \omega \text{ as eigenvalue of } \tau \\ a + c &= \text{ multiplicity of 1 as eigenvalue of } \sigma \\ b + c &= \text{ multiplicity of } -1 \text{ as eigenvalue of } \sigma \end{aligned}$$

and these are enough to determine a, b and c.

By way of an example, let's pose the question: if V is as above the standard representation of S_3, what is $V \otimes V$? By the above, the first step is to find the eigenvalues of σ and τ. This is straightforward: V has a basis v_1, v_2 of eigenvectors for τ with eigenvalues ω and ω^2 respectively; so $V \otimes V$ will have a basis

$$\{v_1 \otimes v_1, v_1 \otimes v_2, v_2 \otimes v_1, v_2 \otimes v_2\}$$

which are eigenvectors for the action of τ on $V \otimes V$ with eigenvalues $\omega^2, 1, 1$ and ω respectively. Similarly, V has a basis u_1, u_2 of eigenvectors for σ with eigenvalues 1 and -1 respectively; so $V \otimes V$ will have a basis

$$\{u_1 \otimes u_1, u_1 \otimes u_2, u_2 \otimes u_1, u_2 \otimes u_2\}$$

which are eigenvectors for σ with eigenvalues $1, -1, -1$ and 1 respectively. Thus, if we write

$$V \otimes V = U^{\oplus a} \oplus U'^{\oplus b} \oplus V^{\oplus c},$$

we have

$$a + b = 2; \quad c = 1; \quad a + c = 2 \quad \text{and} \quad b + c = 2$$

and we deduce that $a = b = c = 1$; that is,

$$V \otimes V = U \oplus U' \oplus V.$$

4.3 Lecture 29: Characters

In lecture 29, we introduce the character of a representation. Previously, in lecture 28, we saw that that the crucial information about a representation $\rho : G \to GL(V)$ is the eigenvalues of the action $\rho(g) : V \to V$ of each element $g \in G$.

4.3.1 Symmetric polynomials

We want some map, which we will define as the character, associating with g information about the eigenvalues of $\rho(g)$. To motivate our definition of the character, we will begin by discussing symmetric polynomials. (But this discussion is ultimately just motivation.)

Consider the polynomial ring $R = k[x_1, \ldots, x_n]$ in n variables and the subring R^{S_n} of polynomials invariant under permutations of the variables.

Remark 4.14.
In general, whenever we have a group G acting on a set X we denote by X^G the subset of elements of X that are fixed by all elements of G. Often, when X has additional structure and the action of G respects this structure, X^G will inherit this structure as well.

Theorem 4.15. Elementary symmetric polynomials generate the ring of symmetric polynomials
One way to generate invariant polynomials is to introduce an auxiliary variable t, and consider the polynomial

$$f(t) = \prod (t + x_i) = t^n + \sigma_1 (x_1, \ldots, x_n) t^{n-1} + \cdots + \sigma_n (x_1, \ldots, x_n) .$$

Then the coefficients $\sigma_\alpha (x_1, \ldots, x_n)$ are called the elementary symmetric polynomials, and we have

$$\sigma_\alpha (x_1, \ldots, x_n) = \sum_{1 \le i_1 < \cdots < i_\alpha \le n} x_{i_1} x_{i_2} \cdots x_{i_\alpha}.$$

The elementary symmetric polynomials generate the ring of symmetric polynomials; in fact, we have an isomorphism

$$k [x_1, \ldots, x_n]^{S_n} = k [\sigma_1, \ldots, \sigma_n]$$

In other words, every polynomial $f (x_1, \ldots, x_n)$ invariant under S_n is uniquely expressible as a polynomial in the elementary symmetric polynomials.

Theorem 4.16. Power sums generate the ring of symmetric polynomials
The power sums are defined simply by

$$\tau_k(x_1, \ldots, x_n) \coloneqq \sum_{i=1}^{n} x_i^k.$$

The first n powers sums $\tau_1(x_1, \ldots, x_n), \ldots, \tau_n(x_1, \ldots, x_n)$ also generate the ring of symmetric polynomials; in fact, we have an isomorphism

$$k[x_1, \ldots, x_n]^{S_n} = k[\tau_1, \ldots, \tau_n].$$

Note that the power sums require the hypothesis that k has characteristic zero, while the elementary symmetric polynomials still generate the ring of symmetric polynomials for k with characteristic $p > 0$.

Now revisiting characters, suppose we specify the sum of the eigenvalues of each element $g \in G$. The point is, if the eigenvalues of g are $\{\lambda_1, \ldots, \lambda_n\}$, then we know the eigenvalues of $g^k \in G$ are $\{\lambda_1^k, \ldots, \lambda_n^k\}$; if we know the sum of each of these, that tells us the value of the power sums $\tau_k(\lambda_1, \ldots, \lambda_n)$ for each k, and by the previous theorem this determines the set $\{\lambda_1, \ldots, \lambda_n\}$!

4.3.2 Character of a representation

Definition 4.17. Character of a representation
We define the character χ_V of a representation V of G to be the function on G (not generally a homomorphism) associating to each $g \in G$ the sum of the eigenvalues of g, i.e., $\chi_V : G \to \mathbb{C}$ is given by

$$\chi_V(g) = \operatorname{trace}(g : V \to V).$$

By the previous theorem, this information is exactly what's needed to determine the eigenvalues of every element of g, and so, as we'll see shortly, exactly enough information to determine the representation. But knowing $\chi_V(g)$ for a single element $g \in G$ does not determine the eigenvalues of the action of g on V; we need to know $\chi_V(g)$ for all $g \in G$ to determine the eigenvalues of the action of every $g \in G$ on V.

Proposition 4.18. Basic facts about characters
Observe the following:

- χ_V is what's called a class function, meaning it takes the same value on conjugate elements of g, for conjugate elements have the same eigenvalues.
- $\chi_V(e) = \dim(V)$.
- For any representations V and W of G, we have

$$\chi_{V\oplus W} = \chi_V + \chi_W; \quad \text{and} \quad \chi_{V\otimes W} = \chi_V \cdot \chi_W$$

  (both of these follow from choosing bases $v_1, \ldots, v_m$ for V and $w_1, \ldots, w_n$ for W consisting of eigenvectors for the action of a given $g \in G$).
- Next, this one is a little trickier: if V^* is the dual representation of V, then

$$\chi_{V^*} = \overline{\chi}_V$$

  To see this, suppose that $\lambda_1, \ldots, \lambda_n$ are the eigenvalues of $\rho_V(g)$ acting on V. Then as we defined the dual representation, the eigenvalues of $\rho_{V^*}(g)$ acting on V^* are the reciprocals $\lambda_1^{-1}, \ldots, \lambda_n^{-1}$; but since the λ_i are complex numbers of modulus 1, we have $\lambda_i^{-1} = \overline{\lambda_i}$; that is, the reciprocal of λ_i is equal to its conjugate.
- Finally, for V and W any representations of G, combining the above we have

$$\chi_{\mathrm{Hom}(V,W)} = \chi_{V^*\otimes W} = \chi_W \cdot \bar{\chi}_V.$$

Proposition 4.19. Formulas of characters of associated representations
If V is any representation of the group G, then for any $g \in G$ we have

$$\chi_{\wedge^2 V}(g) = \frac{\chi_V(g)^2 - \chi_V\left(g^2\right)}{2}$$

and

$$\chi_{\mathrm{Sym}^2 V}(g) = \frac{\chi_V(g)^2 + \chi_V\left(g^2\right)}{2}.$$

Proof. Proof. Fix $g \in G$ and let $v_1, \ldots, v_n$ be a basis for V consisting of eigenvectors for g; let $\lambda_1, \ldots, \lambda_n$ be the corresponding eigenvalues. Then $\wedge^2 V$ has basis $\{v_i \wedge v_j\}_{1\le i<j\le n}$, and these are eigenvectors for g with eigenvalues $\lambda_i\lambda_j$. Thus

$$\begin{aligned}\chi_{\wedge^2 V}(g) &= \sum_{1\le i<j\le n} \lambda_i\lambda_j \\ &= \frac{\left(\sum \lambda_i\right)^2 - \sum \lambda_i^2}{2} \\ &= \frac{\chi_V(g)^2 - \chi_V\left(g^2\right)}{2}.\end{aligned}$$

The second formula may be proved similarly. □

4.3.3 Character tables

Proposition 4.20. Character of a representation determines the representation
The character table for G is a grid of character values, with columns labelled by conjugacy classes of G and rows by irreducible representations of G. For example, the character table for S_3 is

	e	(12)	(123)
U	1	1	1
U'	1	-1	1
V	2	0	-1

Note the rows of the character table for S_3 are linearly independent. Thus if

$$W = U^{\oplus a} \oplus U^{\oplus b} \oplus V^{\oplus c},$$

then we have

$$\chi_W = a\chi_U + b\chi_{U'} + c\chi_V,$$

and this determines a, b and c. In other words, any representation W of a group is determined by its character χ_W.

4.3.4 Characters of permutation representations

Proposition 4.21. Characters of permutation representations
Suppose now that we have an action of our group G on a set S and we let V be the corresponding permutation representation. The matrix representative of g is thus what's called a permutation matrix: all the entries are either 0 or 1, with exactly one 1 in each row and column.

In this case, rather than working out the eigenvectors and eigenvalues of the action of g, we can find the trace by adding the diagonal entries of the matrix. The 1's appearing in the diagonal correspond to elements $s \in S$ with $gs = s$, and so

$$\chi_V(g) = |S^g|,$$

i.e., the number of fixed points of g acting on S.

As a special case of this, consider the regular representation R of G, i.e., the permutation representation of G acting on itself by left multiplication. Here the identity fixes all the elements of G, and any other $g \in G$ has no fixed points. Thus

$$\chi_R(g) = \begin{cases} |G|, & \text{if } g = e \\ 0, & \text{otherwise.} \end{cases}$$

4.4 Lectures 30–32: Projection formulas

Lemma 4.22. Projection onto the trivial invariant subspaces
Let G be a finite group, and suppose that $\{V_\alpha\}$ are the irreducible representations of G, so that any representation V of G is a direct sum

$$V = \bigoplus_\alpha V_\alpha^{\oplus n_\alpha}$$

Let us call the trivial representation of dimension 1 V_0, and try to determine the subspace $V_0^{\oplus n_0}$. We are aided in this by the fact that we can characterize the subspace $V_0^{\oplus n_0} \subset V$ very simply: it is just the subspace V^G of V consisting of vectors $v \in V$ that are invariant under G; that is, such that $gv = v$ for all $g \in G$.
The basic idea we'll use to do this is one we've encountered before: it's the observation that if $\rho : G \to GL(V)$ is a representation of G, then the linear maps $\rho(g) : V \to V$ are in general not homomorphisms of representations. But we can make a homomorphism of representations out of them by averaging: we define the linear map $\phi : V \to V$ by

$$\phi(v) := \frac{1}{|G|} \sum_{g \in G} \rho(g)(v).$$

The key observation is that map $\phi : V \to V$ is a homomorphism of representations; and it is the projection onto the direct summand $V^G = V_0^{\oplus n_0}$ in the direct sum decomposition.

Proof. For the first part, we have to show that for any $h \in G, \phi(hv) = h\phi(v)$ for all $v \in V$. Just write it out: we have

$$\begin{aligned}\phi(hv) &= \frac{1}{|G|} \sum_{g \in G} g(hv) \\ &= \frac{1}{|G|} \sum_{g \in G} h(gv) \\ &= h(\phi(v))\end{aligned}$$

where the two sums are equal because as g ranges over G, gh and hg each range over G as well.

As for the second part, this is just the sum of two observations: that the restriction of ϕ to V^G is the identity; and the image of ϕ is equal to V^G. □

Corollary 4.23. $\dim V^G$
We have

$$\dim(V^G) = \text{trace}(\phi) = \frac{1}{|G|} \sum_{g \in G} \text{trace}(g) = \frac{1}{|G|} \sum_{g \in G} \chi_V(g).$$

Proof. See lecture notes. □

Proposition 4.24. Hermitian inner product of characters
Suppose $\mathbb{C}^{\mathcal{C}}$ is the vector space of class functions on G, i.e., the functions on G that are constant on the conjugacy classes of G. Then define a Hermitian inner product on $\mathbb{C}^{\mathcal{C}}$ by

$$\langle \alpha, \beta \rangle \coloneqq \frac{1}{|G|} \sum_{g \in G} \overline{\alpha}(g) \cdot \beta(g).$$

Then for any two representations V and W, we have

$$\dim \operatorname{Hom}_G(V, W) = \langle \chi_V, \chi_W \rangle.$$

For irreducible V, W, Schur's yields that

$$\dim \operatorname{Hom}_G(V, W) = \langle \chi_V, \chi_W \rangle = \begin{cases} 1, & \text{if } V = W \\ 0, & \text{otherwise.} \end{cases}$$

In other words, for the defined Hermitian inner product, the characters χ_V of the irreducible representations of G are orthonormal.

Proof. See lecture notes. □

Corollary 4.25. Properties of the Hermitian inner product on characters
Let us observe some corollaries using the Hermitian inner product of characters:

- V is irreducible iff
$$\langle \chi_V, \chi_V \rangle = 1.$$
- The number of irreducible representations of a finite group G is less than or equal to the number of conjugacy classes in G; in particular, it is finite.
- A representation V of G is determined by its character χ_V.

Proposition 4.26. Decomposing the regular representation
Let $V_1, \ldots, V_k$ be the irreducible representations of G, and R the regular representation of G. Writing

$$R = V_1^{\oplus a_1} \oplus \cdots \oplus V_k^{\oplus a_k},$$

we have that

$$a_i = \langle \chi_R, \chi_{V_i} \rangle = \frac{1}{|G|} \sum_{g \in G} \chi_R(g) \chi_{V_i}(g) = \chi_{V_i}(e) = \dim V_i,$$

following from the fact that the value of $\chi_R(g)$ is 0 for all $g \neq e \in G$.

In other words, every irreducible representation V_i of G appears $\dim V_i$ times in the regular representation R; and in particular every irreducible representation appears in the regular representation. By comparing dimensions, we have that

$$|G| = \sum \dim (V_i)^2 .$$

Theorem 4.27. Characters of irreducible representations form an orthonormal basis
The characters of the irreducible representations of G span the space of class functions $\mathbb{C}^{\mathcal{C}}$ on G.

Thus, the characters of the irreducible representations of G form an orthonormal basis for $\mathbb{C}^{\mathcal{C}}$; and in particular the number of irreducible representations of G is equal to the number of conjugacy classes in G.

Proof. See lecture notes. □

4.5 Lectures 33–34: Induced representations

This section roughly corresponds to Fulton and Harris 3.3.