Math 55a: Studies in Algebra and Group Theory

Eric K. Zhang
ekzhang@college.harvard.edu

Fall 2019

Abstract

These are notes for Harvard's *Math 55a*, the first semester of the year-long mathematics course described as "probably the most difficult undergraduate math class in the country." This year, the class was taught by Joe Harris[1]. The main topics covered were group theory, abstract linear algebra, and the representation theory of finite groups.

Course description: A rigorous introduction to abstract algebra, including group theory and linear algebra. This course covers the equivalent of Math 25a and Math 122, and prepares students for Math 123 and other advanced courses in number theory and algebra.

Contents

[1] With teaching fellows: Kailas Amin, Benjy Firester, Serina Hu, and Raluca Vlad

1 September 4

Today is the first lecture! We start with an overview of the course before diving straight into group theory. There are so many students today that people are sitting on the floor to hear Joe Harris's lecture, but the class will narrow down quickly in the coming few weeks.

1.1 Course Content

There will be four primary segments, each covering a different topic.

1. Group theory (Artin, *Algebra*)
2. Fields + vector spaces (Axler, *Linear Algebra Done Right*)
3. More group theory
4. Representation theory

1.2 Groups

Let's get started like any introductory algebra course, by introducing groups.

Definition 1.1 (Group)**.** A *group* G consists of a set S with a *law of composition*

$$m : S \times S \to S,$$

$$(a, b) \to ab,$$

satisfying the following axioms:

- (Identity) A distinguished identity element e exists (and also must be unique because $e = ee' = e'$).

$$\exists e \in S : \forall a \in S,\ ea = ae = a.$$

- (Associativity) The group operation is associative.

$$\forall a, b, c \in S : (ab)c = a(bc).$$

- (Inverse) Each element a has an inverse element $b = a^{-1}$ (which is also two-sided and unique).

$$\forall a \in S,\ \exists b \in S : ab = e.$$

We can make variations on groups as an algebraic structure by adding or removing properties as desired.

Definition 1.2 (Abelian group)**.** A group G is called *abelian* if its binary operation is commutative, i.e.,

$$\forall a, b \in G : ab = ba.$$

Definition 1.3 (Monoid)**.** A structure $G = (S, m)$ is called a *monoid* if it satisfies the above closure and associativity properties, but inverses do not necessarily exist.

Example 1.1 (Numerical examples)**.** We present common examples of groups.

- Groups under addition include $\mathbb{Q}, \mathbb{R}, \mathbb{C}$, as well as $\mathbb{Z}$ and $\mathbb{Z}/n\mathbb{Z}$.
- The unit interval $\mathbb{R}/\mathbb{Z} = [0, 1) \subset \mathbb{R}$ is a group under addition modulo 1.
- The *natural numbers* $\mathbb{N} = \{0, 1, 2, \ldots\}$ are only a monoid.
- If you remove the zero element (additive identity) to get $\mathbb{Q}^*, \mathbb{R}^*, \mathbb{C}^*$, these are groups under multiplication.
- The complex numbers on the unit circle $S^1 = \{z \in \mathbb{C} \mid |z| = 1\}$ form a group under multiplication, which is isomorphic to $\mathbb{R}/\mathbb{Z}$.

Definition 1.4 (Cardinality)**.** The *cardinality* or size of a group G is just the cardinality of its underlying set, denoted as $|G|$.

Example 1.2 (Trivial group)**.** The group consisting of one element $G = \{e\}$ is called the *trivial group*.

Example 1.3 (Symmetric group)**.** If S is any set, then the permutations of S are defined as the set of bijections between S and S

$$\text{Perm}(S) = \{\text{1-to-1 mappings } S \mapsto S\}.$$

In particular, if $S = \{1, 2, \ldots, n\}$, then

$$\text{Perm}(S) = S_n,$$

which is called the *symmetric group* on n symbols and has cardinality $n!$.

Example 1.4 (Symmetry groups)**.** Given some geometric figure $X \subset \mathbb{R}^2$ or $\mathbb{R}^3$, we can look at *rotations* of $\mathbb{R}^2$ or $\mathbb{R}^3$ that carry X to itself. We can also consider *reflections*. These give rise to the following symmetry groups:

1. Equilateral triangle: $\mathbb{Z}/3\mathbb{Z}$ for rotations, or S_3 for rotations and reflections.
2. Square: $\mathbb{Z}/4\mathbb{Z}$ for rotations, or D_8 for rotations and reflections.
3. Circle: S^1 for rotations.

Example 1.5 (Linear transformations)**.** The *general linear* and *special linear* groups are sets of $n \times n$ matrices over a given ring R under matrix multiplication. These are denoted $\text{GL}_n R$ and $\text{SL}_n R$ respectively, either with nonzero determinant (general) or singular determinant (special).

Example 1.6 (Three kinds of cardinality)**.** Based on cardinality, we can classify groups into three broad categories.

1. Finite groups $\mathbb{Z}/n\mathbb{Z}$, S_n
2. Countable groups $\mathbb{Q}$, $\mathbb{Z}$, $\mathbb{Z}^n$
3. Continuous groups $\mathbb{R}$, $\mathbb{C}$, $\mathrm{GL}_n \mathbb{R}$, etc.

Now that we have examples of groups, we can also take operations on these groups. The most basic of these is the *product*.

Definition 1.5 (Direct product)**.** The *product* of two groups G and H is the group of pairs of elements between the two groups (Cartesian product), where group multiplication is taken independently:

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

Example 1.7 (Finite vector spaces)**.** Iterated products give us

$$\mathbb{Z}^n = \{(a_1, a_2, \ldots, a_n) : a_i \in \mathbb{Z}\},$$

$$(a_1, a_2, \ldots, a_n) + (b_1, b_2, \ldots, b_n) = (a_1 + b_1, a_2 + b_2, \ldots, a_n + b_n).$$

We can similar construct groups of n-tuples from other sets: $\mathbb{Q}^n, \mathbb{R}^n, \mathbb{C}^n$.

With generalized products between infinitely many groups, we can also construct interesting examples such as $\prod_{i=0}^{\infty} \mathbb{R}$, which is the group of *power series* over $\mathbb{R}$.

Also, define the *direct sum* similarly to the product, except finitely many of the terms must be nonzero. An example is $\bigoplus_{i=0}^{\infty} \mathbb{R} = \{(a_0, a_1, a_2, \ldots)\}$, which is the group of polynomials under addition.

2 September 6

Today we begin looking at relationships between groups.

2.1 Subgroups

Definition 2.1 (Subgroup)**.** If G is any group, then a *subgroup* $H \subset G$ is a subset closed under composition and inversion, i.e.,

$$\forall a, b \in H,\ ab \in H,$$
$$\forall a \in H,\ a^{-1} \in H.$$

Note. Any subgroup must contain the identity e.

Definition 2.2 (Proper subgroup)**.** A subgroup $H \subset G$ is called *proper* if it does not equal G itself. We denote this by $H \subsetneq G$.

Some examples of this include:

$$\mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C},$$
$$S^1 = \{z \in \mathbb{C} \mid |z| = 1\} \subset \mathbb{C}^*,$$
$$\mathrm{SL}_n \mathbb{R} \subset \mathrm{GL}_n \mathbb{R}.$$

With these definitions, we can then ask new questions like: what are all the subgroups of $\mathbb{Z}$?

Claim. All nontrivial subgroups of $\mathbb{Z}$ are of the form, for $a \in \mathbb{Z}_{>0}$,

$$\mathbb{Z}a = \{na \mid n \in \mathbb{Z}\}.$$

Proof. Any nontrivial subgroup contains at least one nonzero element, and thus a positive element. We can then take the minimum positive element a. If there were to exist another element b such that $a \nmid b$, we use the Euclidean algorithm to derive a contradiction. □

Lemma 2.1. *Given group G, let $H, H' \subset G$ be any two subgroups. Then, $H \cap H'$ is also a subgroup.*

Proof. Simply check the composition and inverse properties. □

Definition 2.3 (Subgroup generated by S)**.** Given a group G and *any* subset $S \subset G$, we can find the smallest subgroup containing S in two distinct ways, namely

$$\bigcap_{\substack{H \subset G \\ H \supset S}} H = \langle S \rangle = \{a_1 a_2 a_3 \cdots a_k \mid a_i \in S \cup S^{-1}\}.$$

The second equality here is based on the concept of a *word* in G, which is mapping from a sequence of elements of G to a composition

$$(a_1, a_2, \ldots, a_k) \quad \mapsto \quad a_1 a_2 \cdots a_k \in G.$$

2.2 Homomorphisms

We begin our study of structure-preserving maps between groups.

Definition 2.4 (Homomorphism)**.** If G and H are groups, then a *homomorphism* $f : G \to H$ is a map of sets that respects (commutes with) the group laws on G and H:

$$\begin{aligned} &\forall a, b \in G, \\ f(a)f(b) &= f(ab) \\ f(a)^{-1} &= f(a^{-1}) \\ (\implies f(e) &= e). \end{aligned}$$

This can be represented compactly with the following commutative diagram.

$$\begin{array}{ccc} G \times G & \xrightarrow{f \times f} & H \times H \\ \downarrow{\scriptstyle m_G} & & \downarrow{\scriptstyle m_H} \\ G & \xrightarrow{\quad f \quad} & H \end{array}$$

Example 2.1 (Homomorphisms)**.** We have the following simple examples:

- $\mathbb{Z}/m\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ for $n \mid m$.
- $\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$.
- $\mathbb{R} \to (\mathbb{R}_{>0}, \times)$. (Exponential map)
- $S_n \to \mathbb{Z}/2\mathbb{Z}$. (Sign of a permutation)
- $\mathrm{GL}_n \mathbb{R} \to \mathbb{R}^\times$. (Determinant)
- $\mathbb{Z} \to G$. (Taking $n \to a^n$)

Definition 2.5 (Order)**.** Consider a group G, and its subgroup generated by one element $\langle a \rangle$. The cardinality of this group is denoted by $\operatorname{ord} a$, and it is the smallest positive k such that $a^k = e$.

Definition 2.6 (Kernel and Image)**.** If G, H are any groups and $\varphi : G \to H$ is a homomorphism, then we define the *kernel* of φ to be

$$\ker \phi = \{a \in G \mid \varphi(a) = e\} \subset G.$$

Similarly, the *image* of φ is

$$\operatorname{im} \phi = \{b \in H \mid b = \phi(a) \text{ for some } a \in G\} \subset H.$$

These are respectively *subgroups* of G and H.

Definition 2.7 (Isomophism)**.** If a homomorphism $\varphi : G \to H$ satisfies both $\ker \varphi = \{e\}$ (injective), as well as $\operatorname{im} \varphi = H$ (surjective), then it is a bijective mapping between the two groups. This means that G, H are essentially equivalent up to a relabeling of elements, and φ is an *isomorphism*.

Proposition 2.2 (Cayley's theorem)**.** *Every finite group G is isomorphic to a subgroup of S_n for $n = |G|$.*

Proof. We take the map $\varphi : G \to \mathrm{Perm}(G)$, which sends g to the bijection $m_g : G \to G$ defined by left-multiplication, i.e.,

$$m_g(h) = gh.$$

To finish the proof, we need to show that φ is associative and injective. These follow because

$$(gh)k = g(hk) \implies m_{gh}(k) = (m_g \circ m_h)(k),$$

$$m_g(e) = g \neq g' = m_{g'}(e).$$

□

Exercise 2.1. How many groups of order 2 are there? How about groups of order 3, and order 4? (Answer: $\mathbb{Z}/2\mathbb{Z}, \mathbb{Z}/3\mathbb{Z}, \mathbb{Z}/4\mathbb{Z}, \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$).

2.3 Interlude on Set Theory

Assume we are given a map $f : S \to T$.

Definition 2.8 (Injection)**.** f is *injective* if $\forall a, b \in S$,

$$f(a) = f(b) \iff a = b.$$

Definition 2.9 (Surjection)**.** f is *surjective* if $\forall c \in T$,

$$\exists a \in S : f(a) = c.$$

Definition 2.10 (Bijection)**.** f is *bijective* if it is both injective and surjective.

Definition 2.11 (Cardinality)**.** We define cardinality as having the property that S and T have the *same cardinality* if there exists a bijection between them $|S| = |T|$. Also, if there exists an injection $f : S \to T$, then $|S| \leq |T|$.

Proposition 2.3. *If $|S| \leq |T|$ and $|T| \leq |S|$, then there exists a bijection between S and T, i.e., $|T| = |S|$.*

Proof. This is nontrivial and requires argument, see Halmos NST p. 88. □

Example 2.2 (Countable sets)**.**

$$|\mathbb{N}| = |\mathbb{Z}| = |\mathbb{Q}|.$$

To see that $|\mathbb{N}| = |\mathbb{Z}|$, take

$$f : \mathbb{Z} \xrightarrow{\sim} \mathbb{N}$$

$$: n \to \begin{cases} 2n, n \geq 0 \\ -(2n+1), n < 0. \end{cases}$$

Proposition 2.4 (Cantor's diagonal argument)**.** *There exist uncountable sets; in particular,* $|\mathbb{R}| \neq |\mathbb{Z}|$.

Proof. Assume there exists a surjection φ from $\mathbb{Z}$ to $\mathbb{R}$ and write down their binary digits in an infinite grid. Then, you can generate a new real number not in the image of φ by taking the digits along the diagonal and inverting them, hence φ is not a surjection. □

3 September 9

Today we finish our interlude on set theory, and learn more about groups, homomorphisms, and in particular: *normal* subgroups.

3.1 Interlude on Set Theory (cont.)

Note that $|\mathbb{R}| = |(0,1)|$ by the bijection $t \mapsto \frac{t-0.5}{t(1-t)}$. Lots of infinite sets actually have the same cardinality; for example, the set of all sequences of real numbers.

Proposition 3.1. $|\mathbb{R}^{\mathbb{N}}| = |\mathbb{R}|$

Proof. An explicit bijection is to take a decimal expansion $0.r_1r_2r_3r_4\ldots$ of a real number in $x \in (0,1)$, then generate an infinite sequence of reals as follows:

$$\begin{aligned} x_1 &= 0.r_1r_3r_5r_7\ldots, \\ x_2 &= 0.r_2r_6r_{10}r_{14}\ldots, \\ x_3 &= 0.r_4r_{12}r_{20}r_{28}\ldots, \\ x_4 &= 0.r_8r_{24}r_{40}r_{56}\ldots, \\ &\vdots \end{aligned}$$

In each new decimal, we take every other digit of the decimal expansion, so we are left with an infinite sequence of digits each time, allowing us to generate a surjective mapping from $\mathbb{R}$ to $\mathbb{R}^{\mathbb{N}}$.

Alternatively, we can prove this more elegantly using the fact that $|\mathbb{N}| = |\mathbb{N} \times \mathbb{N}|$, as well as $|\mathbb{R}| = |\mathcal{P}(\mathbb{N})|$. This means that

$$\mathbb{R} = \mathcal{P}(\mathbb{N}) = \mathcal{P}(\mathbb{N} \times \mathbb{N}) = \mathbb{N} \times \mathbb{N} \to \{0,1\} = \mathbb{N} \to \mathbb{N} \to \{0,1\} = \mathbb{N} \to \mathbb{R}.$$

□

Proposition 3.2 (Cantor's Theorem)**.** *If S is any set, then its power set*

$$\mathcal{P}(S) = \{\textit{all subsets of } S\} = \{0,1\}^S$$

has strictly larger cardinality.

Proof. Suppose for the sake of argument that there exists a bijection $\phi : S \to \mathcal{P}(S)$. Then, consider the subset $A \subset S$ defined as

$$A = \{s \in S : s \notin \phi(s)\}.$$

However, now we consider the question of whether A is in the image of itself, $\phi(A)$. Either if $A \in \phi(A)$ or $A \notin \phi(A)$, we end up with a contradiction due to the definition of A, and thus ϕ cannot exist. □

Corollary 3.2.1. $|\mathbb{R}^{\mathbb{R}}| \geq |\{0,1\}^{\mathbb{R}}| > |\mathbb{R}|$.

3.2 Equivalence Relations

Definition 3.1 (Equivalence relation)**.** Let S be any set. An *equivalence relation* $\sim$ on S is a relation that holds between certain pairs of elements of S, denoted $a \sim b$, which satisfies 3 axioms:

- (reflexivity) $a \sim a$.
- (symmetry) $a \sim b \iff b \sim a$.
- (transitivity) $\forall a, b, c \in S : a \sim b \wedge b \sim c \implies a \sim c$.

A more precise but equivalent definition is as follows:

Definition 3.2 (Equivalence relation, formal)**.** An *equivalence relation* on S is a subset Φ of $S \times S$ such that

- $\Phi \supset \Delta = \text{diagonal} = \{(s, s)\} \subset S \times S$.
- $\Phi \to \Phi$ under the involution swapping elements, $S \times S \to S \times S$.
- Consider the set of 3-tuples $S \times S \times S$. Let π_{ij} be the map that takes indices i and j from the tuple and drops the last element. Then

$$\pi_{13}(\pi_{12}^{-1}(\Phi) \cap \pi_{23}^{-1}(\Phi)) \subset \Phi.$$

Based on which elements are equivalent under this relation, we can split up S into several equivalence classes, which provide the same information.

Definition 3.3 (Equivalence class)**.** Given an equivalence relation $\sim$ on S, an *equivalence class* is the subset of all elements of S equivalent to a given element

$$a \in S \mapsto \{s \in S \mid s \sim a\}.$$

All equivalence classes are distinct, and their union is all of S.

Definition 3.4 (Partition)**.** A *partition* of S is an expression of S

$$S = \coprod S_\alpha$$

as a disjoint union of nonempty subsets.

In general, these three definitions are evidently equivalent, and we have

$$\{\text{equivalence relations on } S\} \leftrightarrow \{\text{partitions of } S\} \leftrightarrow \{\text{surjections } S \xrightarrow{f} T\}.$$

3.3 Groups

Recall that a homomorphism $G \xrightarrow{\phi} H$ between groups is a map that preserves the structure of group multiplication. We can define the kernel and image of ϕ as before. Notice that if $K = \operatorname{im}\phi \subset H$, we can factor ϕ as

$$G \to K \to H.$$

Thus, we are primarily interested in *surjective homomorphisms* $\phi : G \to K$ with kernel $H \subset G$. We examine the partition associated with ϕ,

$$\phi^{-1}(k) = \{g \in G \mid \phi(g) = k\}.$$

Proposition 3.3. *Given surjective homomorphism $\phi : G \to K$ with kernel H, we have that*

$$\phi(g) = \phi(g') \iff g' = g\alpha, \alpha \in H.$$

Proof. For any $g_0 \in \phi^{-1}(k)$ and $h \in H$, we have that

$$\phi(g_0 h) = \phi(g_0)\phi(h) = k,$$

$$g_0 \in \phi^{-1}(k) \implies g_0 h \in \phi^{-1}(k).$$

Also, conversely we have that if $g, g' \in \phi^{-1}(k)$, then $\phi(g^{-1}g') = e$ and

$$\phi(g^{-1}g') = \phi(g^{-1})\phi(g') = e \implies \phi(g') = k.$$

□

With this proposition, we switch gears and now turn to describing groups in general by talking about their partitions into cosets.

Definition 3.5 (Cosets)**.** If $H \subset G$ is any subgroup, a *left coset* of H is a subset of the form gH for $g \in G$.

Proposition 3.4. *Any two cosets are equal or disjoint. In particular, if G is finite, then*

$$G = \coprod_{\alpha \in G/H} \alpha H.$$

Proof. Straightforward computation. If $gH \cap g'H \neq \emptyset$, then $\exists \alpha = gh = g'h'$, so

$$g = g'h'h^{-1}.$$

However, $h'h^{-1} \in H$ by closure, so g and g' are in the same left coset. □

Corollary 3.4.1 (Lagrange's Theorem)**.** *The order of any subgroup H of a finite group G divides order of G. In particular,*

$$|G| = |H| \cdot |G/H|.$$

We call $|G/H|$ the index of H in G.

After seeing these two similar concepts of cosets and surjective homomorphisms, we ask the natural question: when is a subgroup the kernel of some surjective homomorphism? If it were the kernel of some homomorphism, we could "factor" the group into kernel and image. This motivates the following definition:

Definition 3.6 (Normal subgroup)**.** If G is any group, and $H \subset G$ is any subgroup, then H is *normal* if the left cosets of H in G are equal to the right cosets of H in G. Equivalently, for all $g \in G$,

$$gH = Hg \iff gHg^{-1} = H.$$

Proposition 3.5. *The normal subgroup condition is necessary and sufficient for the existence of a surjective homomorphism with kernel H.*

4 September 11

Today we cover a variety of topics, including order and quotient groups. We also do a case study in properties of the symmetric group.

4.1 Order

We can consider sequences of elements $a, a^2, a^3, a^4, \ldots$ in a finite group. An infinite sequence of elements will necessarily have duplicates $a^i = a^j$, which means that $a^{j-i} = e$.

Definition 4.1 (Order)**.** For a finite group G and some element $a \in G$, define $\operatorname{ord} a$ to be the smallest integer n such that $a^n = e$.

Proposition 4.1. *For $a \in G$ finite,* $\operatorname{ord} a \mid |G|$.

Proof. Use Lagrange's theorem on the cyclic subgroup generated by a. □

Corollary 4.1.1. *Any group with prime order is cyclic.*

4.2 Quotient Groups

We start by reviewing cosets (from the last lecture). Cosets can be defined as equivalence classes under the relation

$$a \sim b \iff aH = bH.$$

Example 4.1. Consider $G = \mathbb{R}^2$, and $H \cong \mathbb{R}$ is some line passing through the origin. Then, the cosets of H in G are the set of lines parallel to H. If we treat the set of cosets as a group itself, we can then "factor" G into the product of H and G/H.

If we have a surjective homomorphism $G \xrightarrow{\phi} K$ with kernel H, then the fibers $\phi^{-1}(a) : a \in K$ are left and right cosets of H. Then, in what cases for $H \subset G$ can we give G/H the structure of a group, such that the map

$$\begin{aligned} G &\to G/H \\ a &\mapsto aH \end{aligned}$$

is a homomorphism?

Proposition 4.2. *The answer to our question is yes, i.e., we can give G/H a group structure and homomorphism $G \to G/H$, if and only if H is normal.*

Proof. For the necessary direction, suppose we have some homomorphism $\phi : G \to K$ with kernel H. Then, notice that

$$\phi(aha^{-1}) = \phi(a) \cdot \phi(h) \cdot \phi(a^{-1}) = \phi(a) \cdot \phi(a^{-1}) = e.$$

Thus, $aHa^{-1} = H$ is fixed under conjugation by elements of G, so H is a normal subgroup by definition.

To prove the other direction, given some normal subgroup H, we can define the group law on G/H by

$$aH \cdot bH = abH.$$

For this to be a valid homomorphism, we have to check

$$aH = a'H \implies abH = a'bH.$$

This is not true for general H, but assuming H is normal, we have

$$a'bH = a'b(b^{-1}Hb) = a'Hb = aHb = abH.$$

□

Definition 4.2 (Quotient group)**.** If G is any group and $H \subset G$ is a normal subgroup, then the quotient group, denoted G/H, is the set of all cosets aH with law of composition

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

There exists a surjective homomorphism $G \to G/H$ given by $a \mapsto aH$.

Corollary 4.2.1. *There exists a bijection between subgroups of G/H, and subgroups of G that contain H.*

Finally, we have a name for groups that cannot be factored in this way.

Definition 4.3 (Simple group)**.** A group G is called *simple* if it has no normal subgroups (other than G and $\{e\}$), and thus it cannot be factored into the product of H and G/H.

Proposition 4.3. *S_n is not simple for $n > 2$.*

4.3 Exact Sequences

Definition 4.4 (Exact)**.** Suppose we have a sequence of groups with homomorphisms between them:

$$\cdots \to G_i \xrightarrow{\phi_i} G_{i+1} \xrightarrow{\phi_{i+1}} G_{i+2} \to \cdots$$

We call this sequence of homomorphisms *exact* if $\forall i$,

$$\mathrm{im}(\phi_{i-1}) = \ker(\phi_i).$$

Definition 4.5 (Short exact)**.** The simplest and most common case is that of a *short exact* sequence,

$$\{e\} \to A \xrightarrow{\phi} B \xrightarrow{\psi} C \to \{e\}.$$

The exactness property in the case of a short exact sequence means that $A \to B$ is an inclusion, and $B \to C$ is surjective. We then have

$$A = \operatorname{im} \phi = \ker \psi \implies C = B/A.$$

Examples include:

$$\{e\} \to \mathbb{Z}/2\mathbb{Z} \to \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \to \mathbb{Z}/2\mathbb{Z} \to \{e\},$$

$$\{e\} \to \mathbb{Z}/2\mathbb{Z} \to \mathbb{Z}/4\mathbb{Z} \to \mathbb{Z}/2\mathbb{Z} \to \{e\},$$
$$\{e\} \to \mathbb{Z}/2\mathbb{Z} \to \mathbb{Z}/6\mathbb{Z} \to \mathbb{Z}/3\mathbb{Z} \to \{e\},$$
$$\{e\} \to \mathbb{Z}/3\mathbb{Z} \to \mathbb{Z}/6\mathbb{Z} \to \mathbb{Z}/2\mathbb{Z} \to \{e\},$$
$$\{e\} \to \mathbb{Z}/3\mathbb{Z} \to S_3 \to \mathbb{Z}/2\mathbb{Z} \to \{e\}.$$

However, there does **not** exist an exact sequence

$$\{e\} \to \mathbb{Z}/2\mathbb{Z} \to S_3 \to \mathbb{Z}/3\mathbb{Z} \to \{e\}.$$

4.4 Cycle Notation for Permutations

We would like to think more about the symmetric group S_n, so we need some notation to talk about it. Define a cycle $\in S_n$ to be a sequence of k elements such that

$$(a_1, a_2, \ldots, a_{k-1}, a_k) \mapsto (a_2, a_3, \ldots, a_k, a_1).$$

Any permutation can be expressed as a composition of disjoint cycles. For example, the permutation $12345 \mapsto 43251$ can be written as $(32)(451)$. Since this is not unique, we arbitrarily prefer to write the first lexicographical arrangement, e.g., $(145)(23)$.

This notation also has the added benefit that a k-cycle can be written as a product of $k-1$ swaps, or 2-cycles. In particular,

$$(a_1 a_2 \ldots a_k) = (a_1 a_2)(a_2 a_3)(a_3 a_4) \ldots (a_{k-1} a_k).$$

Proposition 4.4. *If $\mu = \sigma_1 \sigma_2 \ldots \sigma_k = \tau_1 \tau_2 \ldots \tau_\ell$ where these are products of transpositions (2-cycles), then $k \equiv \ell \pmod 2$.*

Proof. Count the parity of the number of inversions $i < j$ such that $\mu_i > \mu_j$. Equivalently, consider the functions

$$f(x) = \prod_{1 \le i < j \le n} (x_j - x_i),$$

$$f_\sigma(x) = \prod_{1 \le i < j \le n} (x_{\sigma j} - x_{\sigma i}).$$

Then, we define the sign of a permutation such that

$$f_\sigma(x) = (\operatorname{sgn} \sigma) f(x).$$

□

5 September 13

We wrap up our discussion of groups today, in anticipation for moving on to rings, fields, modules, and vector spaces next week!

Definition 5.1 (Alternating group)**.** Consider the homomorphism $S_n \to \mathbb{Z}/2\mathbb{Z}$, given by $\sigma \mapsto \operatorname{sgn}\sigma$. The kernel of this homomorphism is the normal subgroup of even permutations in S_n, denoted by A_n.

$$\{e\} \to A_n \to S_n \to \mathbb{Z}/2\mathbb{Z} \to \{e\}.$$

Note. In S_3, the unique subgroup of order 3 is A_3. Since any automorphism sends subgroups to other subgroups of equal size, A_3 must be sent to itself by any automorphism. Conjugation is just one special class of automorphism, so A_3 is invariant under conjugation and hence normal.

Definition 5.2 (Inner and outer automorphisms)**.** There exists a homomorphism $G \to Aut(G)$ given by sending an element a to $c_a(g) = aga^{-1}$. The image of this map is called the *inner automorphisms* of G. All other automorphisms are called *outer automorphisms*.

Definition 5.3 (Dihedral group)**.** The *dihedral group of order* $2n$, denoted by D_n, is the group of symmetries of a regular n-gon.

How can we describe the structure of a dihedral group? Note that $D_5 \subset S_5$. The 10 elements of D_5 are the five rotations (including identity) and five reflections about some axis. Additionally, there are six nontrivial subgroups: one of order 5 consisting of the rotations, and five of order 2 each having a single reflection.

5.1 Three Constructions

Definition 5.4 (Center of a group)**.** If G is any group, then its *center*, denoted $Z(G)$ is the set of elements that commute with all elements in G. Equivalently,

$$Z(G) = \{a \in G \mid \forall g \in G : ag = ga\}.$$

Proposition 5.1. *The center $Z(G)$ of any group is a normal, abelian subgroup of G, and also, it is the kernel of the map $G \to Aut(G)$ given by conjugation.*

Example 5.1. The center of D_k for even k is $\{e, r\}$, where r is an 180° rotation. Also, the quotient $D_k/Z(D_k)$ is isomorphic to $D_{k/2}$.

Definition 5.5 (Commutator)**.** The *commutator* of a and b is

$$[a, b] := aba^{-1}b^{-1}.$$

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

Definition 5.6 (Free group)**.** We define the *free group* on 2 generators to be the set of all words on a, b. In other words, it is the set of all finite strings of symbols of the form a^k, b^ℓ with $k, \ell \in \mathbb{Z} \setminus \{0\}$ with no two a^k or b^ℓ adjacent. If our group operation is concatenation, then this is denoted F_2.

Definition 5.7 (Free product)**.** The *free product* of two groups G and H, denoted by $G * H$, is the set of finite strings of the form $g_1 h_1 g_2 h_2 \dots$ or $h_1 g_1 h_2 g_2 \dots$ consisting of alternating elements from G and H. This is similar to the Cartesian product, except we do not assume elements of G and H commute.

Example 5.2. Although $\mathbb{Z} \times \mathbb{Z} = \mathbb{Z}^2$, the free product $\mathbb{Z} * \mathbb{Z} = F_2$.

Example 5.3. There exists an obvious inclusion $F_2 \to F_3$, but weirdly, there also exists an inclusion $F_3 \to F_2$. However, these two groups are **not isomorphic**; the Schröder-Bernstein theorem fails spectacularly for groups.

6 September 16

Today we begin our discussion of linear algebra with fields and vector spaces, plus rings and modules.

6.1 Fields and Rings

Definition 6.1 (Field)**.** A *field* is a set S with two laws of composition, denoted $+$ and $\times$, satisfying the following properties:

- $(S, +)$ is an abelian group with identity $0 \in S$.
- $(S \setminus \{0\}, \times)$ is also an abelian group with identity $1 \in S$.
- Multiplication is distributive over addition, i.e., $a \times (b + c) = a \times b + a \times c$.
- $0 \neq 1$ (the field has more than 1 element).

Definition 6.2 (Ring)**.** If we take the same definition but only require that $(S \setminus \{0\}, \times)$ be a monoid (no inverses), this is called a *commutative ring*.

Proposition 6.1. *The following results follow from the field axioms:*

- $0 \times a = 0$.
- *If* $a \neq 0$, $ab = ac \implies b = c$.

Definition 6.3 (Ring homomorphism)**.** A *homomorphism of rings* $A \to B$ is a map that respects the two laws of composition

$$\varphi(a + b) = \varphi(a) + \varphi(b),$$

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

We also need the map to preserve multiplicative identity:

$$\varphi(1) = 1.$$

Example 6.1. The standard example of a ring is $\mathbb{Z}$, and standard examples of fields are $\mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$.

Example 6.2. The set of integers modulo n, $\mathbb{Z}/n\mathbb{Z}$, is a ring for $n \geq 2$. Furthermore, when p is prime, then $\mathbb{Z}/p\mathbb{Z}$ is a *finite field* $\mathbb{F}_p$ due to the existence of multiplicative inverses modulo p.

Definition 6.4 (Polynomial ring)**.** Given a field k, we can form the ring $k[x]$ of *polynomials* over k by taking linear combinations of powers of x:

$$k[x] = \{a_0 + a_1 x + \ldots + a_n x^n : n \in \mathbb{N}, a_i \in k\}.$$

We can also form polynomial ring over multiple variables, $k[x_1, x_2, \ldots, x_\ell]$ by taking linear combinations of products of powers of variables.

Definition 6.5 (Field of rational functions)**.** Given a field k, we can form a *field of rational functions* over k, denoted $k(x)$, by taking all quotients of polynomials in x modulo the obvious equivalence relation of fraction equality:

$$k(x) = \{p(x)/q(x) : p, q \in k[x], q \neq 0\},$$

$$p/q \sim p'/q' \iff qp' = q'p.$$

Definition 6.6 (Power series)**.** Given a field k, we can form the ring of *power series* over k by taking infinite expressions

$$k[[x]] = \{a_0 + a_1x + a_2x + \cdots : a_i \in k\}.$$

We can take formal products of power series by distributing from lower exponents up, i.e.,

$$(a_0 + a_1x + a_2x^2 + \cdots)(b_0 + b_1x + b_2x^2 + \cdots)$$

$$= a_0b_0 + (a_0b_1 + a_1b_0)x + (a_2b_0 + a_1b_1 + a_0b_2)x^2 + \cdots .$$

Observe that if $a_0 \neq 0$, then $(a_0 + a_1x + \cdots)$ has a multiplicative inverse.

Definition 6.7 (Laurent series)**.** The ring of power series has a corresponding field of *Laurent series* over k, which are formal power series that start at some smallest negative exponent:

$$k((x)) = \{a_{-n}x^{-n} + a_{-n+1}x^{-n+1} + \cdots\}.$$

Definition 6.8 (Extension field)**.** A generated field $k(x_1, x_2, \ldots, x_n)$ is the field created by adjoining the elements $\{x_i\}$ as generators to k, with certain algebraic properties. Some examples are

$$\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} : a, b, \in \mathbb{Q}\},$$

$$\mathbb{R}(i) = \{a + bi : a, b \in \mathbb{R}\} = \mathbb{C}.$$

6.2 Vector Spaces

Definition 6.9 (Module)**.** Given a ring R, an *R-module* is a set V with two laws of composition

- (vector addition) $+ : V \times V \to V$, such that $(V, +)$ is a group.
- (scalar multiplication) $\cdot : R \times V \to V$, that distributes over vector addition, and is also *compatible* (associative) with multiplication in R:
  - $\lambda(a + b) = \lambda a + \lambda b$.
  - $(\lambda + \mu)a = \lambda a + \mu a$.
  - $a(bv) = (ab)v$.
  - $1v = v$.

Definition 6.10 (Vector space)**.** A *vector space* over k is a k-module, where k is a field, and thus has scalar inverses.

For the rest of this discussion, fix a field k.

Definition 6.11 (Subspace)**.** A *subspace* $W \subset V$ is a subset closed under vector addition and scalar multiplication.

Example 6.3 (Tuples)**.** The vector space k^n is given by all n-tuples of elements in k:

$$k^n = \{(\alpha_1, \ldots, \alpha_n) : \alpha_i \in k\}.$$

Example 6.4 (Polynomials)**.** The polynomial ring $k[x]$ is a vector space over k, and it is a subspace of the power series $k[[x]]$.

Example 6.5 (Functions)**.** We can generalize the idea of tuples to functions from a set S to k, denoted k^S, which is a vector space over k. These vector spaces can be very large (*Hilbert spaces*); some examples include

$$C^\infty_{\mathbb{R}} \subset C_{\mathbb{R}} \subset \mathbb{R}^{\mathbb{R}}.$$

Definition 6.12 (Linear combination)**.** A linear combination of $v_1, \ldots, v_n \in V$ is, for any $\lambda_1, \ldots, \lambda_n \in k$, an expression of the form

$$v = \lambda_1 v_1 + \cdots + \lambda_n v_n.$$

Definition 6.13 (Spanning set)**.** We say that $\{v_1, v_2 \ldots\} \subset V$ is a *spanning set* of V if every vector $v \in V$ can be expressed as a finite linear combination of the vectors.

Definition 6.14 (Independence)**.** We say that $\{v_1, v_2, \ldots\} \subset V$ is *linearly independent* if no nontrivial finite linear combination of the vectors is zero.

Definition 6.15 (Basis)**.** A *basis* of V is a set of vectors $\{v_1, v_2, \ldots\} \subset V$ that is both spanning and independent. Equivalently, every vector $v \in V$ can be expressed uniquely as a finite linear combination

$$v = c_1 v_1 + c_2 v_2 + \cdots + c_n v_n.$$

Note. Given any $v_1, \ldots, v_n \in V$, we can define a map

$$\varphi_v : k^n \to V,$$

$$(\lambda_1, \lambda_2, \ldots, \lambda_n) \mapsto \sum_{i=1}^{n} \lambda_i v_i.$$

This set is spanning when φ_v is surjective, and independent when φ_v is injective. Thus, $\{v_i\}$ form a basis if and only if φ_v is isomorphism.

7 September 18

Today we will prove key facts about vector spaces, including the definition of *dimension*. We'll also show a couple examples of bases in finite and infinite dimensions.

7.1 More on Fields

Definition 7.1 (Characteristic)**.** Given a ring R, we can define a homomorphism of rings $\varphi : \mathbb{Z} \to R$ by

$$0 \mapsto 0, 1 \mapsto 1, 2 \mapsto 1+1, n \mapsto 1+1+\cdots+1.$$

The kernel of this homomorphism is either 0 or $n\mathbb{Z}$ for some n. If φ is surjective, then we say R has *characteristic* zero, and otherwise, it has characteristic n, the smallest positive integer such that $\varphi(n) = 0$. When R is an integral domain, its characteristic must be either zero or a prime p.

Definition 7.2 (Linear transformation)**.** A *vector space homomorphism*, or *linear transformation* $\varphi : V \to W$, is a map of sets that respects the vector space structure on V and W.

$$\varphi(a+b) = \varphi(a) + \varphi(b),$$

$$\varphi(\lambda a) = \lambda\varphi(a).$$

Note. The set of all homomorphisms $\mathrm{Hom}(V, W)$ itself can be given the structure of a k-vector space by adding functions $\varphi + \psi = v \mapsto \varphi(v) + \psi(v)$.

Definition 7.3 (Linear subspace)**.** A *subspace* $W \subset V$ is a subset closed under vector addition and scalar multiplication.

Definition 7.4 (Kernel and image)**.** If $\varphi : V \to W$ is any linear map, then the *kernel* $\ker\varphi = \{v \in V : \varphi(v) = 0\}$ is a subspace, and so is the *image* $\mathrm{im}\,\varphi$.

Note. If k is a field and $k' \subset k$ is a subfield, then k is a vector space over k'.

7.2 Basis and Dimension

Recall the definition of a basis from before.

Example 7.1. The field $k^n = \{(a_1, \ldots, a_n) : a_i \in k\}$ has basis

$$\{e_i = (0, \ldots, 0, 1, 0, \ldots, 0) : i = 1, \ldots, n\}.$$

Other bases exist, for example, in k^2 where k has characteristic not equal to 2, $\{(1,1), (1,-1)\}$ is a basis.

Example 7.2 (Infinite dimensions)**.** Define the set k_0^S to be all the functions $f : S \to k$ such that $f(s) = 0$ for all but finitely many $s \in S$. Then, given $\varphi_v = k_0^S \to V$ by

$$\varphi_v(f) = \sum_{\alpha \in S} f(\alpha) v_\alpha,$$

- $\{v_\alpha\}_{\alpha \in S}$ is a spanning set if φ_v is surjective.
- $\{v_\alpha\}_{\alpha \in S}$ is independent if φ_v is injective.
- $\{v_\alpha\}_{\alpha \in S}$ is a basis if φ_v is an isomorphism.

Proposition 7.1. *If $v_1, \dots, v_n$ span V, then some subset of $\{v_1, \dots, v_n\}$ is a basis.*

Proof. Assume that the set is not linearly independent. Then, we can throw away one element of the set by writing it as a linear combination of the other elements, so we have a smaller spanning set, and we proceed by induction. □

Lemma 7.2. *If S is a basis for V, then any proper subset of S is independent but does not span, and any proper superset spans but is not independent.*

Proof. Simply add or remove a vector. This result holds even when S has an infinite basis. □

Proposition 7.3. *If $\{v_1, \dots, v_m\}$ and $\{w_1, \dots, w_n\}$ are two bases for V, then $n = m$.*

Proof. Note that $\langle v_2, \dots, v_m \rangle$ fails to span V. Then there exists j such that $w_j \notin \langle v_2, v_3, \dots, v_m \rangle$. We claim that $\{w_j, v_2, \dots, v_m\}$ is again a basis.

Once we show this claim, then we can repeatedly swap out elements of the form v_i for w_j, completing the proof. □

Definition 7.5 (Dimension)**.** The *dimension* of a vector space V is the cardinality of any basis of V.

8 September 20

Today, we introduce the venerable linear transformation (a homomorphism of vector spaces), which is the key object of study in linear algebra.

8.1 Linear Transformations

Let V be a finite-dimensional vector space with basis $v_1, \dots, v_n \in V$. Then, there exists an isomorphism $k^n \to V$, given by

$$(c_1, \dots, c_n) \mapsto \sum_{i=1}^{n} c_i v_i.$$

Now, consider two vector spaces V and W, and assume that $\varphi : V \to W$ is a linear map. Then, considering a basis $v_1, \dots, v_m$ of V and $w_1, \dots, w_n$ of W, we have for some $a_{ij} \in k$,

$$\begin{aligned}
\varphi(v_1) &= a_{11}w_1 + a_{21}w_2 + \cdots + a_{n1}w_n, \\
\varphi(v_2) &= a_{12}w_1 + a_{22}w_2 + \cdots + a_{n2}w_n, \\
\varphi(v_3) &= a_{13}w_1 + a_{23}w_2 + \cdots + a_{n3}w_n, \\
&\vdots \\
\varphi(v_m) &= a_{1m}w_1 + a_{2m}w_2 + \cdots + a_{nm}w_n.
\end{aligned}$$

The coefficients a_{ij} totally specify the linear map φ, and furthermore, there exists a φ for each such set of coefficients. This motivates the following definition.

Definition 8.1 (Matrix)**.** An $n \times m$ *matrix* over k is a set of nm coefficients a_{ij} for $1 \le i \le n$ and $1 \le j \le m$. We denote it by

$$A = \begin{bmatrix}
a_{11} & a_{12} & a_{13} & \cdots & a_{1m} \\
a_{21} & a_{22} & a_{23} & \cdots & a_{1m} \\
a_{31} & a_{32} & a_{33} & \cdots & a_{1m} \\
\vdots & \vdots & \vdots & \ddots & \vdots \\
a_{n1} & a_{n2} & a_{n3} & \cdots & a_{nm}
\end{bmatrix}.$$

Proposition 8.1. *Given two vector spaces V, W of dimension m and n, there exists an vector space isomorphism between* $\mathrm{Hom}(V, W)$ *and the set of $n \times m$ matrices, for each selection of bases in V and W.*

We call $A = (a_{ij})$ the *matrix representative* of φ in terms of the bases $v_1, \dots, v_m$ and $w_1, \dots, w_n$, to make it clear that A depends on the specific choice of basis.

Definition 8.2 (Change of basis)**.** Suppose we have an old basis $v_1, \dots, v_m$ for V, and a new basis $v_1', \dots, v_m'$. We can express each vector in the new basis as a linear combination of vectors in the new basis, with some coefficients

$$v_i' = v_{1i}v_1 + \cdots + v_{mi}v_m.$$

Then, we call $B = (b_{ij})$ the *change-of-basis matrix*. Multiplying a vector in the new basis by B gives the equivalent vector in the old basis.

Proposition 8.2. *If we have a linear map $V \to W$ with matrix representative A, and we select two new bases for V and W with change-of-basis matrices B and C, then the new matrix representative is*

$$A' = C^{-1}AB.$$

8.2 Constructions on Vector Spaces

We consider how to combine and decompose abstract vector spaces.

Definition 8.3 (Direct sum)**.** The *direct sum*, or *Cartesian product* of two vector spaces V and W is given by ordered pairs of vectors where operations act on each independently, i.e.,

$$V \oplus W = V \times W = \{(v, w) \mid v \in V, w \in W\},$$
$$(v, w) + (v', w') = (v + v', w + w'),$$
$$\lambda(v, w) = (\lambda v, \lambda w).$$

Given vector spaces of dimensions n and m, the direct sum has dimension $n+m$. These same definitions apply for a collection of vector spaces $V_1, \ldots, V_n$.

Note. For an infinite sequence of vector spaces $V_1, V_2, V_3, \ldots$, the Cartesian product is defined as the set of tuples $(v_1, v_2, \ldots)$, but the direct sum requires $v_i = 0$ for all but finitely many i.

Definition 8.4 (Span and independence of subspaces)**.** Let W be any vector space, and let $W_1, W_2, \ldots, W_n \subset W$ be linear subspaces. We say that $W_1, \ldots, W_n$ *span* if every vector $w \in W$ is expressible as a sum

$$w = w_1 + w_2 + \cdots + w_n : w_i \in W_i.$$

Similarly, we say that $W_1, W_2, \ldots, W_n$ are independent if $w_1 + w_2 + \cdots + w_n = 0$ implies that $w_1 = w_2 = \cdots = w_n = 0$.

Definition 8.5 (Direct sum decomposition)**.** For some collection of subspaces $W_1, \ldots, W_n \subset W$, if these are both spanning and independent, then we say $\{W_i\}$ gives a *direct sum decomposition* of W. Equivalently, the disjoint union of the bases for each W_i is a basis for W, and $\dim W = \sum_{i=1}^{n} \dim W_i$.

8.3 Facts about Linear Maps

We prove an analogue of the First Isomorphism Theorem for vector spaces.

Proposition 8.3 (Rank-nullity theorem)**.** *Given a linear map $\varphi : V \to W$ between finite dimensional vector spaces, we define the kernel and image subspaces as in Definition 7.4. Then, we have*

$$\dim \ker(\varphi) + \dim \operatorname{im}(\varphi) = \dim V.$$

Proof. We start by picking a basis $u_1, \dots, u_m$ for $\ker(\varphi)$, and we complete this to form a basis for V: $u_1, \dots, u_m, v_1, \dots, v_{n-m}$. Then, we wish to prove that $\varphi(v_1), \varphi(v_2), \dots, \varphi(v_{n-m})$ is a basis for $\operatorname{im}(\varphi)$. This is clear because if we express an arbitrary vector $v \in V$ in terms of the basis, we have

$$v = \sum_{i=1}^{m} a_i u_i + \sum_{i=1}^{n-m} b_i v_i.$$

Then,

$$\varphi(v) = \cancel{\varphi\left(\sum_{i=1}^{m} a_i u_i\right)} + \varphi\left(\sum_{i=1}^{n-m} b_i v_i\right) = b_1\varphi(v_1) + \cdots + b_{n-m}\varphi(v_{n-m}).$$

Thus, $\{\varphi(v_i)\}$ is spanning, and similar argument shows also that it is independent (as otherwise it would belong in the kernel), so it is a basis. □

Note. Let $r = \dim \operatorname{im}(\varphi)$ be the rank of the map. If we complete the basis of W and write the matrix representative of φ, this is in block form:

$$\begin{bmatrix} I_r & 0_{r,n-r} \\ 0_{w-r,r} & 0_{w-r,n-r} \end{bmatrix}.$$

There really aren't that many different linear maps between vector spaces!

Consider linear *operators*, which are maps from a vector space to itself. What are the different operators under change of basis? Equivalently, what are the conjugacy classes of matrices where $A \sim B^{-1}AB$?

9 September 23

Today we talk about more constructions in the land of abstract linear algebra. This will hopefully be the last definition-heavy lecture.

9.1 Linear Constructions

Definition 9.1 (Quotient space)**.** Let V be a vector space over k, and let $U \subset V$ be a subspace. Since V and U are abelian groups, we can define the *quotient space* by the set of all cosets

$$V/U = \{v + U \mid v \in V\}.$$

We also give the quotient space scalar multiplication defined by

$$\lambda \cdot (v + U) = \lambda v + U.$$

Example 9.1 (Short exact sequence)**.** Any quotient space gives us have a natural map $V \to V/U = W$ that is surjective with kernel U. Furthermore, this gives us a short exact sequence

$$0 \to U \to V \to W \to 0.$$

Note that while V is isomorphic to $U \oplus W$ since they have the same finite dimension, there is no natural isomorphism between them.

Example 9.2 (Correspondence theorem)**.** If we have an arbitrary linear map $\varphi : V \to Y$, where Y is any vector space, then we can factor the map into

$$V \to V/\ker(V) \xrightarrow{\overline{\varphi}} Y.$$

In particular, there exists a bijection between subspaces of V/U and subspaces of V that contain U.

Definition 9.2 (Dual space)**.** Given any vector space V over k, define the *dual vector space* $V^* = \operatorname{Hom}(V, k)$. In other words, this is the vector space of all *linear functionals* over V.

Example 9.3 (Dual space given a basis)**.** Given $V = k^n$, there exists a basis $e_1, \dots, e_n$ for k^n. Then, any linear map $\ell : k^n \to k$ is determined by its values $\ell(e_i)$ on each basis vector, so it is effectively represented by a row vector. We then have an isomorphism $V^* \cong k^n$ given by

$$\ell \mapsto (\ell(e_1), \dots, \ell(e_n)).$$

Definition 9.3 (Dual basis)**.** If we have a basis for V given by $v_1, \dots, v_n$, then we can define the *dual basis* as a corresponding basis for V^* given by $v_1^*, \dots, v_n^*$, defined as

$$\begin{aligned} v_i^* : \quad & v_i \mapsto 1, \\ & v_j \mapsto 0 \quad (j \neq i). \end{aligned}$$

Note. There are many possible bases for the dual space and no single canonical one, so there does not exist a *natural isomorphism* from V to V^*.

Example 9.4 (Dual of the dual)**.** There exists a natural isomorphism from a finite-dimensional vector space V to the dual of its dual, $(V^*)^*$, given by

$$v \mapsto \ell \mapsto \ell(v).$$

Example 9.5 (Infinite dimensions break things)**.** If V is infinite-dimensional, there does not always exist an isomorphism from V to V^*. In particular, if we take $V = k[x]$, then $V^* \cong k[[x]]$.

Definition 9.4 (Transpose map)**.** If we have an arbitrary linear map $\varphi : V \to W$, then we can define the *transpose* map ${}^t\varphi : W^* \to V^*$ given by

$${}^t\varphi : \ell \mapsto \ell \circ \varphi.$$

Example 9.6. For finite-dimensional V, W, we have that ${}^t({}^t\varphi) = \phi : V \to W$.

Example 9.7. If φ is injective then ${}^t\varphi$ is surjective. The converse is also true.

Definition 9.5 (Annihilator)**.** If V is a vector space and $U \subset V$ is any subspace, then the *annihilator* of U is a subspace of V^* given by

$$\mathrm{Ann}(U) = \{\ell : V \to k \mid \ell(U) \equiv 0\} = (V/U)^*.$$

9.2 Linear Operators

Last week we saw that linear maps from V to W aren't very interesting, since they are all effectively identity under an appropriate choice of basis. Now we discuss linear maps from $V \to V$, which gives us less freedom.

Definition 9.6 (Linear operator)**.** Given a vector space V, an *operator* on V is any linear map $\varphi : V \to V$.

Definition 9.7 (Endomorphism)**.** The space of all linear maps $\varphi : V \to V$ can be denoted $\mathrm{Hom}(V, V)$ or $\mathrm{End}(V)$, the space of *endomorphisms* on V. While in general $\mathrm{Hom}(V, W)$ has the structure of a group, $\mathrm{End}(V)$ is also a non-commutative ring, with multiplication given by composition of maps.

A natural question to ask is about whether there exist subspaces that remain the same under a linear map.

Definition 9.8 (Invariant subspace)**.** Given a subspace $U \subset V$, we say that U is *invariant* under a linear operator φ when $\varphi(U) = U$.

Definition 9.9 (Eigenvector)**.** When we have a one-dimensional invariant subspace U given by $k \cdot v$, there is not much freedom to choose a map. We must have that $\varphi v = \lambda v$ for some $\lambda \in k$. In this case, v is called an *eigenvector* for φ, and λ is called the corresponding *eigenvalue*.

Example 9.8 (Basis of eigenvectors)**.** If we have a map $\varphi : \mathbb{R}^2 \to \mathbb{R}^2$ with two eigenvectors v_1 and v_2 with eigenvalues λ and μ, then we can choose a basis for $\mathbb{R}^2$ given by v_1 and v_2, after which φ simply becomes the diagonal map

$$\begin{bmatrix} \lambda & 0 \\ 0 & \mu \end{bmatrix}.$$

However, we cannot always find a basis of eigenvectors, for example in the case

$$\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix},$$

which is a shear transformation.

Proposition 9.1 (Structural decomposition)**.** *Eigenvectors with distinct eigenvalues are linearly independent.*

Proof. Suppose that $v_1, \dots, v_\ell$ are eigenvectors for $\varphi : V \to V$ with distinct eigenvalues $\lambda_1, \dots, \lambda_\ell$. Furthermore, assume for the sake of contradiction that $v_1, \dots, v_\ell$ are linearly dependent, as well as a minimal such set. This means that we can write for some nonzero a_i,

$$a_1 v_1 + a_2 v_2 + \cdots + a_\ell v_\ell = 0.$$

Applying φ to both sides of this equation yields

$$a_1 \lambda_1 v_1 + a_2 \lambda_2 v_2 + \cdots + a_\ell \lambda_\ell v_\ell = 0.$$

We now have two linear equations in the $\{v_i\}$. If we multiply the first equation by λ_ℓ and subtract, this yields

$$(\lambda_1 - \lambda_\ell) a_1 v_1 + (\lambda_2 - \lambda_\ell) a_2 v_2 + \cdots + (\lambda_{\ell-1} - \lambda_\ell) a_{\ell-1} v_{\ell-1} = 0.$$

However, this is a smaller linear combination of $v_1, v_2, \dots, v_{\ell-1}$ that also vanishes, which contradicts the assumption that the $\{v_i\}$ are minimal. □

10 September 25

Today we continue our discussion on linear operators.

10.1 Linear Operators (cont.)

Recall that a linear operator $\varphi : V \to V$ is an endomorphism on a vector space, and these form a ring under composition and addition.

Definition 10.1 (Invertible)**.** We say that $\varphi \in \operatorname{End}(V)$ is *invertible* or *nonsingular* if any one of the following equivalent conditions hold:

- φ is injective.
- φ is surjective.
- φ is an isomorphism.
- $\operatorname{rank} \varphi = \dim V$.

Our goal is to express an operator in terms of simpler component operators on subspaces. We wish to find $V = A \oplus B$ such that A and B are both invariant subspaces under φ: $\varphi(A) \subset A$ and $\varphi(B) \subset B$. This is equivalent to finding a basis $v_1, \dots, v_n$ for V such that the matrix representative of φ is block diagonal.

Example 10.1 (Diagonalizable matrix)**.** If we have $n = \dim V$ one-dimensional invariant subspaces $A_1, \dots, A_n \subset V$, then there exists a basis $v_1, \dots, v_n$ for V such that the matrix representative for φ is diagonal. We call φ *diagonalizable*.

Example 10.2 (Block upper-triangular)**.** If we have an invariant subspace $A \subset V$ under φ, then we can choose a basis $v_1, \dots, v_k$ for A and complete to a basis for V: $v_1, \dots, v_n$. Then, the matrix representative of φ with respect to this basis is the *block upper-triangular* matrix

$$\begin{bmatrix} \overline{\varphi} & * \\ \mathbf{0} & * \end{bmatrix}.$$

10.2 Interlude on Polynomials

Suppose we have polynomials over a field k of the form

$$k[x] = \{a_n x^n + \cdots + a_0 \mid a_i \in k, n \in \mathbb{N}\}.$$

Proposition 10.1 (Lagrange's theorem)**.** *Given some polynomial f over a ring R that satisfies $f(a) = 0$ for some $a \in R$, then $(x - a) \mid f$. In other words, $f(x) = (x-a)g(x)$. As a corollary, if R is an integral domain and f has degree n, then there are at most n roots a_i such that $f(a_i) = 0$.*

Proof. Use polynomial long division. We have $f(x) = (x-a)g(x) + r$, and since a is a root, this means that $r = 0$. □

Definition 10.2 (Algebraically closed)**.** A field k is called *algebraically closed* if every non-constant polynomial has a root. Equivalently, combining this with the last proposition, every non-constant polynomial factors into a product

$$f(x) = c(x - \lambda_1)(x - \lambda_2) \cdots (x - \lambda_k).$$

Proposition 10.2 (Fundamental Thm. of Algebra)**.** *The field of complex numbers $\mathbb{C}$ is algebraically closed.*

Proof. Requires topology or complex analysis, left for Math 55b. □

Definition 10.3 (Algebraic closure)**.** Given a field k, we can construct $\overline{k} \supset k$ such that $\overline{k}$ is algebraically closed.

10.3 Eigenvectors

We use algebraic closure to prove some important results.

Proposition 10.3 (Existence of eigenvectors)**.** *Given a finite-dimensional vector space V over an algebraically-closed field $\mathbb{C}$ and some linear operator $\varphi : V \to V$, then φ has a an eigenvector.*

Proof. Say $\dim V = n$. Then, choose any nonzero $v \in V$, and consider the $n+1$ vectors

$$v, \varphi v, \varphi^2 v, \ldots, \varphi^n v \in V.$$

Since we have $n + 1$ vectors, they are linearly dependent, so there exists some coefficients $a_0, \ldots, a_n \in \mathbb{C}$, not all zero, such that

$$a_0 v + a_1 \varphi v + \ldots + a_n \varphi^n v = 0,$$

This means that we can construct a linear operator

$$T = a_0 + a_1 \varphi + \cdots + a_n \varphi^n,$$

which has nonzero kernel. By the fundamental theorem of algebra, we can factor this polynomial into an expression of the form

$$T = c(\varphi - \lambda_1)(\varphi - \lambda_2) \cdots (\varphi - \lambda_n).$$

Since $\ker T \neq 0$, we must have that at least one of the operators $\varphi - \lambda_i$ is singular, so there exists v such that $(\varphi - \lambda_i)(v) = 0$ for some i. In other words,

$$\varphi(v) = \lambda_i v.$$

□

Example 10.3. Consider the rotation map $(x, y) \mapsto (-y, x)$. This has no eigenvectors in $\mathbb{R}^2$, as visibly demonstrated by the rotation. However, in $\mathbb{C}^2$, this map has two eigenvectors

$$v_1 = e_1 + ie_2 \mapsto e_2 - ie_1 = -iv_1,$$

$$v_2 = e_1 - ie_2 \mapsto e_2 + ie_1 = iv_2.$$

Therefore, the 90° rotation map is really a diagonal operator over $\mathbb{C}^2$.

Proposition 10.4 (Weak normal form)**.** *Given a finite-dimensional vector space V over an algebraically-closed field $\mathbb{C}$, as well as a linear operator $\varphi : V \to V$, there exists a basis $v_1, \dots, v_n \in V$ for V such that the matrix representative of φ is upper triangular.*

Proof. We claim that there exists a *flag* of subspaces

$$0 \subset V_1 \subsetneqq V_2 \subsetneqq \cdots \subsetneqq V_n = V,$$

such that $\varphi(V_i) \subset V_i$ for all i. First, choose $v_1 \neq 0$ to be any eigenvector for φ, and let $V_1 = \langle v_1 \rangle$. Consider the induced map $\overline{\varphi} : V/V_1 \to V/V_1$ given by

$$\overline{\varphi}(v + V_1) = \varphi(v) + V_1.$$

Now, $\overline{\varphi}$ has an eigenvector $w \in V/V_1$, so we choose any $v_2 \in w + V_1$, which gives

$$\varphi(v_2) \in \langle v_1, v_2 \rangle.$$

Thus, define $V_2 = \langle v_1, v_2 \rangle$, and continue analogously for $V_3, \dots, V_n$. □

Proposition 10.5 (Singularity of upper triangular matrices)**.** *Suppose we have some basis $v_1, \dots, v_n$ for V and linear operator $\varphi : V \to V$. If the matrix representative A for φ with respect to $\{v_i\}$ is upper triangular, then φ is nonsingular if and only if all diagonal entries in A are nonzero.*

Proof. Suppose that we have some $a_{ii} = 0$. Then, we have

$$\varphi : \langle v_1, \dots, v_i \rangle \to \langle v_1, \dots, v_{-1} \rangle.$$

This cannot be injective as the image has smaller dimension than the domain, so φ has nonzero kernel.

Conversely, if we have singular φ, then we can take some vector $v \in \ker \varphi$ such that $\varphi(v) = 0$. This means that there exists some i such that the vectors $\{v_1, \dots, v_{i-1}, v\}$ are independent, but $\{v_1, \dots, v_i, v\}$ are dependent. Then,

$$v_i \in \langle v_1, \dots, v_{i-1}, v \rangle,$$

$$\varphi(v_i) \in \langle v_1, \dots, v_{i-1} \rangle + \langle \varphi(v) \rangle = \langle v_1, \dots, v_{i-1} \rangle.$$

This implies that $a_{ii} = 0$. □

11 September 27

Today we talk more about linear operators, and we also briefly discuss categories and functors. We are currently in Chapter 8 of Axler (skipped Chapter 6, 7).

11.1 More on Eigenvectors

Recall that we can choose a basis for any linear operator φ such that the matrix representative is upper triangular. From Proposition 10.5, we note that $\varphi - \lambda$ is singular if and only if $\lambda = a_{ii}$ for some i.

Corollary 11.0.1. *The eigenvalues of φ are exactly the diagonal entries in its upper triangular matrix representative. In particular,*

$$\lambda \text{ is an eigenvalue} \iff \varphi - \lambda \text{ singular} \iff \lambda = a_{ii}.$$

This means that the number of distinct eigenvalues is at most n.

Although this corollary is nice, it doesn't tell us anything about the *multiplicity* of repeated eigenvalues. We would like to have more information about this, but our upper triangular representation is not strong enough (and also not unique). This motivates the following definitions.

Definition 11.1 (Generalized kernel)**.** If $\varphi : V \to V$ is a linear operator, then the *kernel* of φ is the set of vectors v for which $\varphi(v) = 0$. The *generalized kernel* is defined as

$$\operatorname{gker}(\varphi) = \{v \in V \mid \exists m > 0 : \varphi^m v = 0\}.$$

Equivalently, we can also write $\operatorname{gker} \varphi = \ker \varphi^n$, where $n = \dim V$.

Definition 11.2 (Nilpotent)**.** If $\varphi^m = 0$ for some m, or equivalently $\operatorname{gker}(\varphi) = V$, then we say that φ is *nilpotent*.

Example 11.1 (Nilpotent map)**.** Consider the map $\varphi : k^2 \to k^2$ given by

$$e_1 \to 0,$$
$$e_2 \to e_1.$$

Then, $\varphi^2 = 0$, so φ is nilpotent.

Definition 11.3 (Generalized eigenvector)**.** We call $v \in V$ a *generalized eigenvector* with eigenvalue λ if it is in the generalized kernel, $v \in \operatorname{gker}(\varphi - \lambda)$. Equivalently, there exists some $m > 0$ such that

$$(\varphi - \lambda)^m v = 0.$$

Definition 11.4 (Algebraic multiplicity)**.** The *multiplicity* of an eigenvalue λ is the dimension of its *generalized eigenspace*

$$V_\lambda = \operatorname{gker}(\varphi - \lambda).$$

We now make a series of key claims that will complete our canonicalization of linear operators and describe their eigenvectors.

Proposition 11.1 (Generalized eigenspaces are invariant)**.** *For any eigenvalue λ, we have $\varphi(V_\lambda) \subset V_\lambda$.*

Proof. Assume that v is a member of V_λ. Then, we have that

$$(\varphi - \lambda)^n v = 0 \implies \varphi(\varphi - \lambda)^n v = 0.$$

However, we also know that φ commutes with itself and the identity, so

$$\varphi(\varphi - \lambda)^n v = (\varphi - \lambda)^n \varphi v = 0.$$

Thus, by definition we have $\varphi(v) \in V_\lambda$. □

Proposition 11.2 (Generalized eigenspaces are independent)**.** *When considered as subspaces of V, the generalized eigenspaces V_λ are independent for all λ. In particular, if $v_i \in V_{\lambda_i}$ for $i = 1, \ldots, \ell$, then*

$$v_1 + \cdots + v_\ell = 0 \iff \forall i : v_i = 0.$$

Proof. Assume for the sake of argument that $v_1 \neq 0$. By symmetry, this argument will work for any v_i. First, note that $(\varphi - \lambda_1)^n v_1 = 0$, so let k be the largest integer such that

$$w = (\varphi - \lambda_1)^k v_1 \neq 0.$$

Now, we have that $w \neq 0$, but applying the map $\varphi - \lambda_1$ one more time causes w to vanish, so $\varphi w = \lambda_1 w$. This means that w is an eigenvector!

Now, to our linear combination of vectors in each generalized eigenspace, we apply the operator

$$(\varphi - \lambda_1)^k (\varphi - \lambda_2)^n \cdots (\varphi - \lambda_\ell)^n.$$

This causes all of the v_i to vanish except for the first term v_1, which yields

$$\begin{aligned} 0 &= (\varphi - \lambda_1)^k (\varphi - \lambda_2)^n \cdots (\varphi - \lambda_\ell)^n v_1 \\ &= (\varphi - \lambda_2)^n \cdots (\varphi - \lambda_\ell)^n (\varphi - \lambda_1)^k v_1 \\ &= (\varphi - \lambda_2)^n \cdots (\varphi - \lambda_\ell)^n w. \end{aligned}$$

However, since w is an eigenvector, we have $(\varphi - \lambda)w = (\lambda_1 - \lambda)w$. Thus, this expression is equivalent to

$$(\lambda_1 - \lambda_2)^n \cdots (\lambda_1 - \lambda_\ell)^n w = 0.$$

Assuming that the λ_i are distinct, we have that $w = 0$, which is a contradiction. □

Proposition 11.3 (Generalized eigenspaces are spanning)**.** *The generalized eigenspace V_λ has dimension equal to the number of times λ appears on the diagonal of an upper triangular matrix representative.*

Proof. Left as an exercise, see Proposition 12.1. □

In conclusion, using these past three propositions, we can have the following decomposition for any linear operator φ.

Proposition 11.4. *For any linear operator $\varphi : V \to V$, we can decompose V into the direct sum of generalized eigenspaces*

$$V = \bigoplus_\lambda V_\lambda,$$

where λ ranges over the eigenvalues of φ. This direct sum also has the property that V_λ is invariant under φ.

Equivalently, in matrix terms, there exists a basis for V such that the matrix representative of φ is block diagonal, and each block $V_{\lambda_i} \to V_{\lambda_i}$ is an upper triangular matrix with diagonal entries all λ_i. We write this as

$$\varphi = \begin{bmatrix} \begin{pmatrix} \lambda_1 & \cdots & * \\ \vdots & \ddots & \vdots \\ 0 & \cdots & \lambda_1 \end{pmatrix} & \cdots & \mathbf{0} \\ \vdots & \ddots & \vdots \\ \mathbf{0} & \cdots & \begin{pmatrix} \lambda_\ell & \cdots & * \\ \vdots & \ddots & \vdots \\ 0 & \cdots & \lambda_\ell \end{pmatrix} \end{bmatrix}.$$

11.2 Interlude on Category Theory

Definition 11.5 (Category)**.** A *category* $\mathcal{C}$ consists of 3 things:

- a collection $\mathrm{Ob}(\mathcal{C})$ of *objects*,
- for each pair $A, B \in \mathrm{Ob}(\mathcal{C})$, a collection $\mathrm{Mor}(\mathrm{A}, \mathrm{B})$ of *morphisms*,
- and a law of composition $\circ$, with signature $\forall A, B, C \in \mathrm{Ob}(\mathcal{C})$,

$$\mathrm{Mor}(\mathrm{A}, \mathrm{B}) \times \mathrm{Mor}(\mathrm{B}, \mathrm{C}) \to \mathrm{Mor}(\mathrm{A}, \mathrm{C}).$$

The law of composition must further satisfy the following two axioms:

- (Associativity) $\forall A, B, C, D \in \mathrm{Ob}(\mathcal{C})$ and morphisms $\alpha \in \mathrm{Mor}(\mathrm{A}, \mathrm{B})$, $\beta \in \mathrm{Mor}(\mathrm{B}, \mathrm{C})$, $\gamma \in \mathrm{Mor}(\mathrm{C}, \mathrm{D})$,

$$(\gamma \circ \beta) \circ \alpha = \gamma \circ (\beta \circ \alpha).$$

- (Identity) $\forall A \in \mathrm{Ob}(\mathcal{C})$, $\exists\, \mathrm{id}_A \in \mathrm{Mor}(\mathrm{A}, \mathrm{A})$ such that

$$\forall \varphi \in \mathrm{Mor}(\mathrm{A}, \mathrm{B}) : \varphi \circ \mathrm{id}_{\mathrm{A}} = \mathrm{id}_{\mathrm{B}} \circ \varphi = \varphi.$$

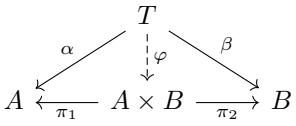
Example 11.2 (Category of sets)**.** The category **Set** of sets is the category with sets as objects, as functions as morphisms. In particular, $\mathrm{Mor}(\mathrm{A}, \mathrm{B})$ is the collection of all functions $f : A \to B$.

Example 11.3 (Category of groups)**.** The category **Grp** of groups is the category with all groups as objects, and homomorphisms of groups as morphisms.

Definition 11.6 (Product)**.** Given two objects $A, B \in \mathrm{Ob}(\mathcal{C})$, the *product* $A \times B$ is an object in $\mathrm{Ob}(\mathcal{C})$ with morphisms

$$\pi_1 : A \times B \to A,$$
$$\pi_2 : A \times B \to B,$$

such that for all $T \in \mathrm{Ob}(\mathcal{C})$ with morphisms $T \xrightarrow{\alpha} A$ and $T \xrightarrow{\beta} B$, there exists a unique morphism $\varphi : T \to A \times B$ such that the following diagram commutes.



12 September 30

Today we finish our discussions of linear operators. During the next lecture, we will catch up on categories and functors and introduce bilinear forms.

12.1 More on Eigenvectors (cont.)

Recall that given an operator φ over a finite-dimensional vector space V over an algebraically closed field k, we can find a basis for V such that φ is a block-diagonal matrix composed of upper-triangular maps on generalized eigenspaces.

Definition 12.1 (Similar)**.** Given two linear operators, $\varphi, \psi \in \mathrm{End}(V)$, we say that they are *similar* or *conjugate* if there exists a change-of-basis operator $A \in GL(V)$ such that

$$\varphi = A\psi A^{-1}.$$

The nicest possible case is if all diagonal entries are distinct, in which there must be a basis for V consisting of eigenvectors.

Definition 12.2 (Diagonalizable)**.** We call a linear operator φ *diagonalizable* or *semisimple* if there exists a basis for V consisting of eigenvectors of φ, or equivalently, if φ has a diagonal matrix representative under some basis (it is similar to a diagonal matrix).

In the case of repeated eigenvalues along the diagonal, we might not necessarily have a complete basis of eigenvectors. However, what we do have is a generalized eigenspace of the same dimension, as in the following proposition.

Proposition 12.1 (Repeated eigenvalues induce generalized eigenspaces)**.** *If an upper triangular matrix representative of a linear operator φ has an eigenvalue λ of multiplicity m_λ on its diagonal, then*

$$\dim \mathrm{gker}(\phi - \lambda) = \dim \ker(\phi - \lambda I)^n = m_\lambda.$$

Proof. Induct on m_λ. The idea is that either $\varphi - \lambda$ has a kernel of dimension m_λ, or if it doesn't, it maps onto its image, after which we can continue applying $\varphi - \lambda$ sufficiently many more times to get the rest of the generalized eigenvectors. See Axler p. 252 for details. □

Now, consider a single generalized eigenspace V_λ, and consider the matrix block of φ in this subspace, which we denote M_λ. Note that $\varphi|_{V_\lambda} - \lambda$ is nilpotent because M_λ has diagonal entries all λ. To finish our analysis, we wish to classify the nilpotent operators within each block.

Proposition 12.2 (Nilpotent Jordan)**.** *Given any nilpotent operator, we can write it as the direct sum of nilpotent Jordan blocks, each of the "descending*

ladder" form

$$J_{0,q} = \begin{bmatrix} 0 & 1 & 0 & 0 & \cdots & 0 \\ 0 & 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \ddots & \vdots \\ 0 & 0 & 0 & 0 & \ddots & 1 \\ 0 & 0 & 0 & 0 & \cdots & 0. \end{bmatrix}.$$

Proof. A nilpotent operator $\varphi : V \to V$ satisfies $\varphi^n = 0$, where $n = \dim V$. Let q be the smallest positive integer such that $\varphi^q = 0$, and take some $v \in V$ such that $\varphi^{q-1} v \neq 0$. Then, we can write a basis for an invariant subspace given by the descending ladder

$$A = \langle v, \varphi v, \varphi^2 v, \ldots, \varphi^{q-1} v \rangle.$$

Finally, we claim that we can decompose V into the direct sum

$$V = A \oplus B,$$

where B is also invariant under φ. Since $\varphi|_B$ is also a nilpotent map, we finish by induction on the dimension of the subspace. □

Corollary 12.2.1 (Number of nilpotent maps)**.** *The number of nilpotent operators on an n-dimensional vector space, up to conjugation, is equal to the number of integer partitions of n.*

Finally, we are ready to state the final conclusion, our "big result" about matrix classification.

Proposition 12.3 (Jordan canonical form)**.** *Suppose we have any linear operator $\varphi : V \to V$, where V is a finite-dimensional vector space over an algebraically closed field. There exists a basis for V such that the matrix representative J of φ is block diagonal,*

$$J = \begin{bmatrix} J_{\lambda_1, q_1} & 0 & \cdots & 0 \\ 0 & J_{\lambda_2, q_2} & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & J_{\lambda_\ell, q_\ell} \end{bmatrix},$$

and each block $J_{\lambda,q}$ is a q-dimensional Jordan block with eigenvalue λ:

$$J_{\lambda,q} = \begin{bmatrix} \lambda & 1 & 0 & \cdots & 0 & 0 \\ 0 & \lambda & 1 & \cdots & 0 & 0 \\ 0 & 0 & \lambda & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & \lambda & 1 \\ 0 & 0 & 0 & \cdots & 0 & \lambda. \end{bmatrix}.$$

13 October 2

Today we begin talking about bilinear forms and inner product spaces. Our long-term plan is to cover multilinear algebra and tensor algebra, then our second unit on group theory, and finally, representation theory.

13.1 Bilinear Forms

Definition 13.1 (Dot product)**.** Given a vector space $\mathbb{R}^n$, we can define the *dot product* to be the familiar map $\cdot : \mathbb{R}^n \times \mathbb{R}^n \to \mathbb{R}^n$ given by

$$u \cdot v = \sum_{i=1}^{n} u_i v_i.$$

A useful question is: how can we generalize the dot product to abstract vector spaces? It turns out that the most important property is *bilinearity.*

Definition 13.2 (Bilinear form)**.** Given a vector space V over field k, a *bilinear form* on V is a function

$$b : V \times V \to k,$$

which satisfies linearity properties in each factor:

- $b(\lambda x, y) = \lambda \cdot b(x, y)$.
- $b(u + x, y) = b(u, y) + b(x, y)$.
- $b(x, \lambda y) = \lambda \cdot b(x, y)$.
- $b(x, u + y) = b(x, u) + b(x, y)$.

Definition 13.3 (Vector space of bilinear forms)**.** Given any vector space V over k, the set

$$B(V) = \{b : V \times V \to k\}$$

of all bilinear forms on V is itself a vector space, as it is closed under addition and scalar multiplication.

Exercise 13.1. What is $\dim B(V)$?

Definition 13.4 (Symmetric and skew-symmetric)**.** Given a bilinear form b on V, we call b:

- *symmetric* if $b(u, v) = b(v, u)$, $\forall u, v \in V$.
- *skew-symmetric* if $b(u, v) = -b(v, u)$, $\forall u, v \in V$.

Proposition 13.1. *Every bilinear form over a vector space V over k (with field characteristic not equal to 2) is uniquely expressible as a sum of a symmetric and skew-symmetric bilinear form. In particular,*

$$B(V) = B_{symm}(V) \oplus B_{skew}(V).$$

Proof. Simply observe that

$$b_1(u,v) = \frac{b(u,v) + b(v,u)}{2},$$
$$b_2(u,v) = \frac{b(u,v) - b(v,u)}{2}.$$

□

Proposition 13.2 (Bilinear forms are dual space homomorphisms)**.** *Given a bilinear form $b : V \times V \to k$, we can generate a map $\varphi_b : V \to V^*$ given by*

$$\varphi_b(v) = b(v, \bullet).$$

The map taking $b \mapsto \varphi_b$, from $B(V) \to \mathrm{Hom}(V, V^*)$, is an isomorphism.

Proof. Injectivity in the forward direction is clear. To exhibit the inverse, suppose that we have an arbitrary linear map $\varphi : V \to V^*$. Define the bilinear form b_φ by

$$b_\varphi(v,w) = \varphi(v)w.$$

Thus, we have an injective inverse map $\varphi \mapsto b_\varphi$, so $B(V) \cong \mathrm{Hom}(V, V^*)$. □

Definition 13.5 (Rank of bilinear forms)**.** We call a bilinear form b *non-degenerate* if its corresponding linear map, $\varphi_b : V \to V^*$, is an isomorphism. More generally, define the *rank* of a bilinear form b to be the rank of φ_b, where $\mathrm{rank}(b) \leq \dim V$.

Note. Equivalently, for a finite-dimensional vector space V, a bilinear form is *degenerate* if there exists a nonzero $v \in V$ such that for all $w \in W$, $b(v,w) = 0$.

Proposition 13.3 (Bilinear forms are matrices)**.** *Given a basis $e_1, \ldots, e_n$ for V and a bilinear form $b : V \times V \to k$, then b is determined by the values*

$$a_{ij} = b(e_i, e_j).$$

In particular, this forms a matrix $A = [a_{ij}]$ such that $b(v,w) = v^T A w$.

Proof. Let $v = \sum_i v_i e_i$ and $w = \sum_i w_i e_i$. Then, by bilinearity, we have that

$$\begin{aligned} b(v,w) &= \sum_i \sum_j b(v_i e_i, w_j e_j) \\ &= \sum_i v_i \left(\sum_j w_j b(e_i, e_j) \right) \\ &= \sum_i v_i \left(\sum_j a_{ij} w_j \right) \\ &= \sum_i \sum_j v_i (Aw)_{ij} \\ &= v^T A w. \end{aligned}$$

□

Definition 13.6 (Orthogonal complement)**.** Given a vector space V with non-degenerate bilinear form $b : V \times V \to k$, let $U \subset V$ be any subspace. Then, the *orthogonal complement* of U with respect to b is the set

$$U^\perp = \{v \in V \mid b(v, u) = 0, \forall u \in U\} = \operatorname{Ann}(\phi_b(U)).$$

Note. In general, we have $\dim U + \dim U^\perp = \dim V$, but $V \neq U \oplus U^\perp$.

Definition 13.7 (Inner product)**.** A bilinear form b is called an *inner product* when it has the additional properties that:

- (Symmetry) $b(u, v) = b(v, u)$.
- (Positive-definiteness) $b(u, u) \geq 0$, with equality when $u = 0$.

Note. Any inner product is also non-degenerate.

13.2 Inner Product Spaces

A vector space V augmented with an inner product $\langle \bullet, \bullet \rangle$ is called an *inner product space*, which provides us with an entirely new object of study.

Definition 13.8 (Length)**.** Given any vector $v \in V$, the *length* of v, denoted by $|v|$, is defined as

$$|v| = \sqrt{b(v, v)} = \sqrt{\langle v, v \rangle}.$$

Proposition 13.4 (Pythagorean Theorem)**.** *Given two vectors $u, v \in V$ such that $\langle u, v \rangle = 0$, we have that*

$$|u + v|^2 = |u|^2 + |v|^2.$$

Proof. Note that

$$\begin{aligned} |u + v|^2 &= \langle u + v, u + v \rangle \\ &= \langle u, u \rangle + 2\langle u, v \rangle + \langle v, v \rangle \\ &= |u|^2 + |v|^2 + 2\langle u, v \rangle. \end{aligned}$$

The result follows immediately. □

Proposition 13.5 (Cauchy–Schwarz)**.** *Given any two vectors $u, v \in V$,*

$$|\langle u, v \rangle| \leq |u| \cdot |v|.$$

Proof. We can assume without loss of generality that $|u| = 1$. Then, we let $S = \langle u \rangle$ (the one-dimensional vector space spanned by u), and also let $S^\perp$ be its orthogonal complement.

Now, we define a projection map $P : V \to S$ given by

$$v \mapsto \langle u, v \rangle \cdot u.$$

This map has $\ker P = S^\perp$ and $\operatorname{im} P = S$. In particular, we have that for any $v \in V$, there exists $w \in S^\perp$ such that

$$v = P(v) + w.$$

Finally, we have that

$$|v|^2 = |P(v)|^2 + |w|^2 \geq |P(v)|^2 = \langle u, v\rangle^2.$$

□

Definition 13.9 (Angle between vectors)**.** As a consequence of Prop. 13.5, we define the *angle* α between two nonzero vectors $u, v \in V$ by

$$\cos\alpha = \frac{\langle u, v\rangle}{|u| \cdot |v|}.$$

Definition 13.10 (Orthonormal basis)**.** A basis $v_1, \ldots, v_n$ for an inner product space V is called *orthonormal* if $\langle v_i, v_j\rangle = \delta_{ij}$ for all i and j. In other words, all pairs of basis vectors are orthogonal, and each basis vector has length 1.

Equivalently, the map $V \xrightarrow{\sim} \mathbb{R}^n$ given by the basis $\{v_1, \ldots, v_n\}$ respects the inner product (length-preserving).

Proposition 13.6 (Gram-Schmidt)**.** *A finite-dimensional inner product space V has an orthonormal basis.*

Proof. We proceed by induction on $n = \dim V$. Start with any nonzero $u \in V$, and replace u by

$$u_1 = \frac{u}{|u|}.$$

Then, let $V' = \langle u_1\rangle^\perp$, and apply the inductive hypothesis to generate a basis $u_2, \ldots, u_n$ for V'. Finally, $u_1, u_2, \ldots, u_n$ is a basis for V. □

14 October 7

Today we review bilinear forms and inner product spaces, and we discuss operators on inner product spaces.

14.1 More on Bilinear Forms

Proposition 14.1. *Suppose that b is a non-degenerate bilinear form over a finite-dimensional vector space V. Then, the following statements are true (and equivalent to non-degeneracy):*

1. *(φ_b injective) Given $v \in V$, if $\forall w \in V : b(v, w) = 0$, then $v = 0$.*
2. *(φ_b surjective) For all $\ell \in V^*$, there exists $w \in V$ such that $\ell(v) = b(w, v)$.*

Last week we talked about the orthogonal complement of a subspace with a bilinear form, and we noted that $V \neq U \oplus U^\perp$ in general. The counterexamples are precisely when $U \cap U^\perp$ is nontrivial, as in the following definition.

Definition 14.1 (Isotropic)**.** A symmetric bilinear form b is called *isotropic* when there exists a nonzero vector u such that $b(u, u) = 0$. Equivalently, if we let $U = \langle u \rangle$, then $u \in U^\perp$.

Note in particular that inner products are anisotropic because they are positive-definite, so for any inner product space V and subspace $U \subset V$, we have the decomposition $V = U \oplus U^\perp$.

14.2 Operators on Inner Product Spaces

Definition 14.2 (Orthogonal transformation)**.** Consider a finite-dimensional inner product space V. An operator $T : V \to V$ is called *orthogonal* if it preserves the length of vectors, i.e., for all $v, w \in V$, $\langle Tv, Tw \rangle = \langle v, w \rangle$.

Definition 14.3 (Orthogonal group)**.** The set of orthogonal transformations over V is closed under composition and thus forms a subgroup $O(V, b) \subset \mathrm{GL}(V)$. Since we are only working over reals, we can define the *orthogonal group* of dimension n, denoted $O(n)$, to be the length-preserving transformations of $\mathbb{R}^n$.

Definition 14.4 (Adjoint map)**.** Suppose that $T : V \to V$ is an operator on an inner product space V. Then, recall that the transpose ${}^tT$ is a natural map $V^* \to V^*$. If we take the natural isomorphism $V = V^*$ given by the inner product then, this gives us a map from $T^* : V \to V$ as follows.

$$\begin{array}{ccc} V^* & \xrightarrow{{}^tT} & V^* \\ \updownarrow & & \updownarrow \\ V & \xrightarrow{T^*} & V \end{array}$$

Then, T^* is called the *adjoint* of T, and it is defined by the condition

$$\langle v, Tw \rangle = \langle T^* v, w \rangle.$$

Definition 14.5 (Self-adjoint)**.** We call a linear operator $T : V \to V$ *self-adjoint* if $T = T^*$. In other words,

$$\langle v, Tw \rangle = \langle Tv, w \rangle.$$

Equivalently, T is self-adjoint when the matrix representative of T with respect to an orthonormal basis is symmetric. Note that self-adjoint operators are closed under addition, but not composition, so they form a subspace of $\mathrm{End}(V)$.

Note. In contrast, observe that for any orthogonal map T, we have

$$\langle Tv, w \rangle = \langle v, T^{-1}w \rangle = \langle v, T^*w \rangle,$$

so an orthogonal map is one that satisfies $T^{-1} = T^*$. As a consequence, the matrix representative of an orthogonal map with respect to an orthonormal basis has columns that also form an orthonormal basis in $\mathbb{R}^n$.

With these definitions noted, we will now make some observations that lead up to the spectral theorem.

Proposition 14.2. *Given a self-adjoint operator $T : V \to V$, suppose that $W \subset V$ is an invariant subspace, such that $T(W) \subset W$. Then, the orthogonal complement $W^\perp$ is also invariant, i.e., $T(W^\perp) \subset W^\perp$.*

Proof. If $v \in W^\perp$, then for all $w \in W$,

$$\langle v, w \rangle = 0 \implies \langle v, Tw \rangle = \langle Tv, w \rangle = 0.$$

Thus, $Tv \in W^\perp$. □

Corollary 14.2.1. *If T is self-adjoint, then T^2 is a positive operator, meaning that for all $v \in V$, we have $\langle T^2 v, v \rangle \geq 0$.*

Proof. Note that $\langle T^2 v, v \rangle = \langle Tv, Tv \rangle = |Tv|^2 \geq 0$. Equivalently, the matrix representative of T^2 is positive semidefinite. □

Corollary 14.2.2. *If $a > 0$ and T is self-adjoint, then $T^2 + a$ is invertible.*

15 October 9

Today we continue discussing operators on inner product spaces. On Friday, we will continue with Hermitian inner products, as well as rings and modules.

15.1 The Spectral Theorem

Continuing from the corollaries at the end of the last lecture, we prove another useful fact before moving to the spectral theorem.

Corollary 15.0.1. *If $p(x) = x^2 + ax + b$ is a real polynomial such that $p(x) > 0$ for all $x \in \mathbb{R}$ (i.e., $b > a^2/4$), then $p(T)$ is invertible.*

Proof. Note that for any $v \neq 0$,

$$\begin{aligned}\langle (T^2 + aT + b)(v), v\rangle &= \langle T^2 v, v\rangle + a\langle Tv, v\rangle + b\langle v, v\rangle \\ &\geq |Tv|^2 - a|Tv| \cdot |v| + b|v|^2 \qquad \text{(Cauchy-Schwarz)} \\ &= |v|^2 \left[\left(\frac{|Tv|}{|v|} \right)^2 - a\frac{|Tv|}{|v|} + b \right] > 0.\end{aligned}$$

□

Proposition 15.1 (Spectral theorem)**.** *Any self-adjoint operator has an orthonormal basis of eigenvectors, with all real eigenvalues.*

Proof. Choose any nonzero $v \in V$, a vector space with dimension $n = \dim V$, and consider the vectors

$$v, Tv, T^2 v, \ldots, T^n v.$$

Then, there exists some nonzero linear relation

$$a_0 v + a_1 Tv + a_2 T^2 v + \cdots + a_n T^n v = 0.$$

Consider the real polynomial $p(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_0$. We note that $p(T)$ has a kernel, as $(p(T))v = 0$. Note that a fact from elementary algebra is that given any real polynomial $p(x)$, we can factor it into a product of linear and quadratic factors as

$$p(x) = \pm \prod_{i=1}^{b} (x - \lambda_i) \cdot \prod_i q_i(x),$$

where each irreducible quadratic factor $q_i(x)$ is never zero on the reals. By Corollary 15.0.1, we know that $q_i(T)$ is invertible for all i. However, since $p(T)$ has nonzero kernel, there must exist some factor $x - \lambda_i$ with nonzero kernel, so λ_i is a real eigenvalue of T.

Once that we have a single real eigenvalue λ, let v be an eigenvector with eigenvalue λ. Then, note that $\langle v\rangle$ is an invariant subspace under T, so its orthogonal complement $\langle v\rangle^\perp$ is also invariant by Prop. 14.2. We can then continue this process inductively on $\langle v\rangle^\perp$, which allows us to find an orthonormal basis of eigenvectors. □

Corollary 15.1.1 (Principal axis theorem)**.** *If T is self-adjoint, then there exists an orthogonal matrix Q of eigenvectors and diagonal matrix Λ of real eigenvalues such that*

$$T = Q\Lambda Q^*.$$

Corollary 15.1.2 (Orthogonality of eigenspaces)**.** *If T is self-adjoint, then its eigenspaces are mutually orthogonal. In particular, if $Tv = \alpha v$ and $Tw = \beta w$ such that $\alpha \neq \beta$, then $\langle v, w\rangle = 0$.*

15.2 Orthogonal Operators

Note that $O(1)$, the length-preserving transformations on the real line, is just $\mathbb{Z}/2 = \{+1, -1\}$. The next simplest case is $O(2)$, which is precisely the symmetry group of a circle – all rotations and reflections in $\mathbb{R}^2$.

There exists a subgroup of rotations within $O(2)$ of just rotations, sometimes denoted $SO(2)$, which is isomorphic to $S^1 = \mathbb{R}/\mathbb{Z}$. In particular, this is a normal subgroup, and we have the short exact sequence

$$\{e\} \to S^1 \to O_2 \to \mathbb{Z}_2 \to \{e\}.$$

The structure of $O(2)$ is indeed very similar to that of the dihedral group, and indeed, we can embed any dihedral group $D_n \subset O(2)$.

Exercise 15.1. How can we characterize $O(3)$?

Proposition 15.2 (Spectral theorem for orthogonal operators)**.** *Given a finite-dimensional inner product space V and orthogonal operator $T : V \to V$, we can obtain a direct sum decomposition $V = \oplus_i V_i$ into one or two-dimensional invariant subspaces V_i, such that $T|_{V_i}$ has the property that:*

- *If $\dim V_i = 1$, then it is ± 1.*
- *If $\dim V_i = 2$, then it is either a reflection or a rotation.*

Furthermore, if we extend $\mathbb{R}$ to $\mathbb{C}$, then we can diagonalize an orthogonal operator to an orthonormal basis of eigenvectors, such that each complex eigenvalue has modulus 1. More on complex vector spaces tomorrow!

16 October 11

Today we introduce Hermitian forms and operators, and we also briefly discuss rings and modules.

16.1 Hermitian Forms

Exercise 16.1. Show that it is impossible to construct a positive definite bilinear form on a vector space over $\mathbb{C}$.

Proof. Assume this exists, and $b : V \times V \to \mathbb{C}$ is bilinear. Then for any $v \in V$, $b(v, v) > 0$, but $b(iv, iv) = i^2 b(v, v) < 0$, so we have a contradiction. □

Exercise 16.2. In fact, if V is a vector space of dimension at least 2 over $\mathbb{C}$ and b is a bilinear form, then there exists some v such that $b(v, v) = 0$.

Proof. We can proceed in a way analogous to the discriminant-based proof of Cauchy-Schwarz. Choose $v_1, v_2 \in V$ that are independent. Let

$$b(v_1, v_1) = a, b(v_1, v_2) = b, b(v_2, v_2) = c.$$

Then,

$$b(xv_1 + v_2, xv_1 + v_2) = ax^2 + 2bx + c^2.$$

Since $\mathbb{C}$ is algebraically closed, this quadratic polynomial in x has a root, so $v = xv_1 + v_2$ is satisfies $b(v, v) = 0$. □

Clearly, standard bilinear forms fail to be positive-definite in vector spaces over $\mathbb{C}$. What can we do instead, then?

Definition 16.1 (Hermitian form)**.** Let V be a vector space over $\mathbb{C}$. A *Hermitian form* on V is a map

$$h : V \times V \to \mathbb{C}$$

that has the following properties:

- Linear in the first factor: $h(\lambda v + u, w) = \lambda h(v, w) + h(u, w)$.
- Conjugate symmetric: $h(w, v) = \overline{h(v, w)}$.

This sometimes called a *sesquilinear form*, as it is linear in the first factor but only conjugate linear ("half-linear") in the second factor.

Definition 16.2 (Hermitian inner product)**.** If we additionally require $h(v, v) > 0$ for all nonzero $v \in V$, then h is a *positive-definite Hermitian inner product.*

Example 16.1 (Examples of Hermitian forms)**.** Consider $V = \mathbb{C}^n$. Then, one example of a Hermitian inner product is

$$h((z_1, \ldots, z_n), (w_1, \ldots, w_n)) = z_1\overline{w_1} + \cdots + z_n\overline{w_n}.$$

Also, if $V = L^2$ is the vector space of square-integrable functions $S^1 \to \mathbb{C}$, then

$$h(f, g) = \int_{S^1} f(z) \cdot \overline{g(z)}\, dz$$

is a Hermitian inner product.

Example 16.2 (Dual space)**.** If $h : V \times V \to \mathbb{C}$ is Hermitian, then we can define a map $V \to V^*$ given by $v \mapsto h(\bullet, v)$. However, this map is *not linear*.

Definition 16.3 (Conjugate transpose)**.** The adjoint of an operator $T : V \to V$ on a Hermitian inner product space is also called the *conjugate transpose*.

Definition 16.4 (Hermitian matrix)**.** A self-adjoint operator $T : V \to V$ on a finite-dimensional Hermitian inner product space is called *Hermitian*, i.e., if

$$\forall v, w : \langle T^* v, w \rangle = \langle v, Tw \rangle.$$

Definition 16.5 (Unitary matrix)**.** In analogy to real orthogonal operators, an operator $U : V \to V$ on a finite-dimensional Hermitian inner product space is called *unitary* if

$$\forall v, w : \langle Tv, Tw \rangle = \langle v, w \rangle.$$

Proposition 16.1 (Spectral theorem, Hermitian)**.** *Given a finite-dimensional Hermitian inner product space, consider a linear operator T. Then:*

- *If T is self-adjoint, then there exists an orthonormal basis of eigenvectors with all real eigenvalues.*
- *If T is unitary, then there exists an orthonormal basis of eigenvectors where all eigenvalues have modulus* 1*.*

16.2 Rings and Modules

Recall that an R-module (Def. 6.9) is an algebraic structure with addition and scalar multiplication, where scalars come from the commutative ring R.

Example 16.3 (Examples of rings)**.** Notable examples of rings include:

- (Integers) $\mathbb{Z}$,
- (Polynomials) $k[x]$,
- (Multivariate polynomials) $k[x_1, \ldots, x_n]$,
- (Indefinite multivariate polynomials) $k[x_1, x_2, \ldots]$,
- (Fractions over p) $\mathbb{Z}[1/p] = \left\{ \frac{a}{p^n} : a \in \mathbb{Z}, n \in \mathbb{N} \right\}$,
- (Fractions over not p) $\mathbb{Z}_{(p)} = \left\{ \frac{a}{b} : a, b \in \mathbb{Z}, p \nmid b \right\}$.

Definition 16.6 (Free module)**.** Given any ring R, we can define

$$R^n = \{(x_1, \ldots, x_n) : x_i \in R\}$$

to be the *free module* of rank n. In general, we call a module *free* if it has a basis (a spanning independent set).

Example 16.4 (Examples of modules)**.** Examples of non-free modules include

- Any abelian group is a module over $\mathbb{Z}$.
- $\mathbb{Z}/n\mathbb{Z}$, $(\mathbb{Z}/n\mathbb{Z})^k$, etc. are all modules over $\mathbb{Z}$.
- Any ring is a module over itself.
- The ideals of a ring R are the submodules of R.
- The quotient ring R/I is an R-module for any ideal I.

Definition 16.7 (Span and independence)**.** Observe that if M is any module, and we have a subset $\{m_1, \ldots, m_n\} \subset M$, then we can define the map

$$R^n \xrightarrow{\varphi} M,$$

$$(x_1, \ldots, x_n) \mapsto x_1 m_1 + \cdots + x_n m_n.$$

If φ is surjective, then we say that $\{m_1, \ldots, m_n\}$ *spans* or *generates* M. If φ is injective, then we say that $\{m_1, \ldots, m_n\}$ are *independent*.

Note. Not every independent set is contained within a basis, and not every spanning set contains a basis.

17 October 16

Today we continue our lecture on rings and modules, and we wrap up on bilinear forms.

17.1 Rings and Modules (cont.)

We know a lot about the linear algebra of vector spaces over fields, so can we use this to learn about modules over rings? It turns out that very little about vector spaces ports over to modules. We continue from where we left off from last week.

Definition 17.1 (Basis)**.** A subset $S \subset M$ is a *basis* if it is both spanning and independent. In other words, consder the map $\varphi : R^n \to M$ given by

$$(a_1, \ldots, a_n) \mapsto \sum_{i=1}^{n} a_i s_i.$$

If φ is an isomorphism, then S is a basis. However, unlike in vector spaces, bases do not always exist in modules. If a basis of size n exists, then M is isomorphic to R^n, and we call M a *free module of rank* n.

Proposition 17.1. *Given a finitely generated module M and a submodule $M' \subset M$, it is possible that M' is not finitely generated.*

Proof. Take $R = k[x_1, x_2, \ldots]$ as a module over itself, and consider the submodule $\mu' \in R$ consisting of polynomials with zero constant term, i.e., $\mu' = \{f \in R \mid f(0, 0, \ldots) = 0\}$. This requires one generator for each x_i, of which there are a countably infinite number, so it is not finitely generated. □

Definition 17.2 (Noetherian ring)**.** A ring R is called *Noetherian* if any submodule of a finitely generated R-module is also finitely generated.

Definition 17.3 (Module homomorphism)**.** A *homomorphism* between two modules M and N over R is a map $\varphi : M \to N$ that is a homomorphism of the underlying abelian groups, while respecting scalar multiplication. For any $\lambda \in R$,

$$\varphi(\lambda v) = \lambda \cdot \varphi(v).$$

Proposition 17.2. *As in the case of vector spaces, given any two R-modules, the set of homomorphisms* $\mathrm{Hom}(M, N)$ *has the structure of an R-module.*

Note. Unlike vector spaces, we can have $M, N \neq 0$ and $\mathrm{Hom}(M, N) = 0$, i.e., the only homomorphism between them is the zero map. For example, consider the two $\mathbb{Z}$-modules $M = \mathbb{Z}/2\mathbb{Z}$ and $N = \mathbb{Z}/3\mathbb{Z}$.

Definition 17.4 (Dual module)**.** Given any module M over a ring R, we can associate M to the dual module $M^* = \mathrm{Hom}(M, R)$.

Example 17.1 (Dual of the dual module)**.** Like in the case of vector spaces, there is a natural homomorphism $M \to (M^*)^*$ given by the evaluation map $v \mapsto \mathrm{ev}_v$, where $\mathrm{ev}_v(f) = f(v)$. However, unlike vector spaces, this map is not always an isomorphism.

17.2 Wrapping up Bilinear Forms

We consider how to structurally characterize bilinear forms.

Proposition 17.3 (Inner products are unique)**.** *Any positive-definite inner product on an n-dimensional real vector space V is isomorphic to the standard inner product on $\mathbb{R}^n$.*

Proof. Perform the Gram-Schmidt process (Prop. 13.6) to find an orthonormal basis for V. This immediately gives an isomorphism to $\mathbb{R}^n$ by projection onto this basis. If we let the basis be $\{e_1, \ldots, e_n\}$, then the inner product of two vectors is

$$\langle u_1 e_1 + \cdots + u_n e_n, v_1 e_1 + \cdots + v_n e_n \rangle = \sum_{1 \le i,j \le n} u_i v_j \langle e_i, e_j \rangle = u_1 v_1 + \cdots + u_n v_n.$$

This is just the standard inner product on $\mathbb{R}^n$. □

Proposition 17.4 (Sylvester's law of inertia)**.** *Given a finite-dimensional real vector space V with a non-degenerate symmetric bilinear form b, there exists an orthogonal basis $\{e_1, \ldots, e_n\}$ for V such that $b(e_i, e_j) = 0$ for all $i \neq j$ and $b(e_i, e_i) = \pm 1$.*

Proof. Repeat the proof of the last proposition, but instead of scaling vectors to 1, we can only scale to ± 1 since we do not assume that $b(e_i, e_i) > 0$. □

Definition 17.5 (Standard bilinear forms)**.** By the previous Proposition, any non-degenerate symmetric real bilinear form is is isomorphic to

$$b(x, y) = \sum_{i=1}^{k} x_i y_i - \sum_{i=k+1}^{k+\ell} x_i y_i.$$

Similarly, any non-degenerate Hermitian form on a complex vector space is isomorphic to

$$h(x, y) = \sum_{i=1}^{k} x_i \overline{y_i} - \sum_{i=k+1}^{k+\ell} x_i \overline{y_i}.$$

We call these the standard forms with *signature* (k, ℓ).

Definition 17.6 (Indefinite orthogonal group)**.** There are variants of the orthogonal/unitary groups preserving lengths under non-degenerate symmetric bilinear forms of a given signature, denoted $O(k, \ell)$ and $U(k, \ell)$.

Example 17.2 (Lorentz group)**.** In special relativity, Minkowski spacetime has a metric with signature $(1, 3)$, and the corresponding symmetry group is $O(1, 3)$, called the Lorentz group.

Proposition 17.5 (Structure of skew-symmetric bilinear forms)**.** *Given an n-dimensional vector space V over a field (with characteristic not equal to 2), and $q : V \times V \to k$ is a non-degenerate skew-symmetric bilinear form, then:*

- *n is even ($n = 2k$).*
- *V has a basis $e_1, \ldots, e_{2k}$ such that*

$$q(e_i, e_j) = \begin{cases} 1 & \text{if } j = i + k \\ -1 & \text{if } j = i - k \\ 0 & \text{otherwise} \end{cases}.$$

In other words, q has a representative expressed by the block matrix

$$\begin{bmatrix} 0 & I_k \\ -I_k & 0 \end{bmatrix}.$$

Definition 17.7 (Symplectic group)**.** The group of symmetries of V that preserve a skew-symmetric form is called the *symplectic group* $\mathrm{Sp}(n)$.

18 October 18

Today we begin discussing multilinear algebra, and we define the tensor product of vector spaces. We will continue this on Monday as well.

18.1 Three Definitions of the Tensor Product

We present three equivalent definitions of the *tensor product*. For the rest of this section, fix a field k, and let V and W be vector spaces over k. Some of the following definitions of the tensor product $V \otimes W$ will assume that V, W are finite-dimensional, but they can be extended to infinite-dimensional cases.

Definition 18.1 (Tensor product basis)**.** Let $\{e_1, \dots, e_m\}$ be a basis for V and $\{f_1, \dots, f_n\}$ be a basis for W. Then, $V \otimes W$ is the vector space with a basis of mn linearly independent elements, denoted by $\{e_i \otimes f_j\}$.

Note. While the direct sum (or Cartesian product) of two vector spaces has dimension $m + n$, the tensor product has dimension mn.

Example 18.1 (Bilinear map to the tensor product)**.** Give two vector spaces V and W, we have a bilinear map $V \times W \to V \otimes W$ given by, for any $v = \sum_i a_i e_i$ and $w = \sum_j b_j f_j$,

$$(v, w) \mapsto \sum_{i,j} a_i b_j (e_i \otimes f_j) = v \otimes w.$$

The last notation $v \otimes w$ in this example motivates our second definition.

Definition 18.2 (Tensor products without bases)**.** We define a very large vector space U with basis $\{v \otimes w \mid v \in V, w \in W\}$. We then take the subspace $U_0 \subset U$ generated by the relations

$$\begin{aligned} U_0 = \Big\langle & \lambda v \otimes w - \lambda(v \otimes w), \\ & v \otimes \lambda w - \lambda(v \otimes w), \\ & (u + v) \times w - u \otimes w - v \otimes w, \\ & u \otimes (w + x) - u \otimes w - u \otimes x \Big\rangle. \end{aligned}$$

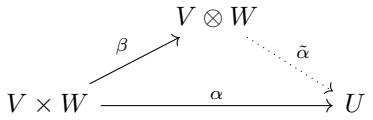
Then, the tensor product is defined by taking the quotient of U modulo these relations, or $V \otimes W = U/U_0$.

Exercise 18.1. Verify that Definitions 18.1 and 18.2 are equivalent.

Definition 18.3 (Tensor product, standard definition)**.** The *tensor product* $V \otimes W$ is a vector space with bilinear map $\beta : V \times W \to V \otimes W$, such that for all $\alpha : V \times W \to U$, there exists a linear map $\tilde{\alpha} : V \otimes W \to U$ such that

$$\alpha = \tilde{\alpha} \circ \beta.$$

In other words, we can factor any bilinear map $\alpha : V \times W \to U$ as follows.



Essentially, for any vector space U, the vector space of bilinear maps from $V \times W$ to U is isomorphic to $\mathrm{Hom}(V \otimes W, U)$.

Exercise 18.2. Verify that Definitions 18.2 and 18.3 are equivalent.

Exercise 18.3. If we extend Definitions 18.2 and 18.3 to modules over commutative rings, then the same rules apply. However, the properties of these tensor products differ. Verify that $\mathbb{Z}^m \otimes \mathbb{Z}^n = \mathbb{Z}^{mn}$, and that $\mathbb{Z}/2\mathbb{Z} \otimes \mathbb{Z}/3\mathbb{Z} = 0$.

18.2 Properties of Tensor Products

Definition 18.4 (Pure tensor)**.** An element of $V \otimes W$ is called *rank 1*, or *pure*, if it is of the form $v \otimes w$ for $v \in V$ and $w \in W$.

Example 18.2. Given a two-dimensional vector space $V = \langle e_1, e_2 \rangle$, a general element of $V \otimes V$ can be given by

$$xe_1 \otimes e_1 + ye_1 \otimes e_2 + ze_2 \otimes e_1 + we_2 \otimes e_2.$$

This is a pure tensor if and only if $xw = yz$.

Pure tensors form a subset of $V \otimes W$, but not a subspace, as they are not closed under linear combinations. In fact, any element of $V \otimes W$ is a linear combination of pure tensors. This allows for the following definition.

Definition 18.5 (Rank of a tensor)**.** In general, the *rank* of an element of $V \otimes W$ is the smallest η such that it can be expressed as a linear combination of η pure tensors.

Proposition 18.1 (Tensor product identities)**.** *Given vector spaces U, V, and W, the following identities involving tensor products hold:*

$$(U \oplus V) \otimes W = (U \otimes W) \oplus (V \otimes W),$$

$$(U \otimes V) \otimes W = U \otimes (V \otimes W),$$

$$(U \otimes V)^* = U^* \otimes V^*.$$

Proof. Left as an exercise. □

Proposition 18.2 (Linear maps are tensor products)**.** *Given any two vector spaces V and W,*

$$\mathrm{Hom}(V, W) = V^* \otimes W.$$

Proof. We can define a bilinear map $V^* \times W \to \mathrm{Hom}(V, W)$ given by

$$\begin{aligned}(\ell, w) \mapsto \varphi : V &\to W \\ v &\mapsto \ell(v) \cdot w.\end{aligned}$$

This is an isomorphism, so by factoring this by the bilinear map $V^* \times W \to V^* \otimes W$, there must exist an natural isomorphism $V^* \otimes W \to \mathrm{Hom}(V, W)$. □

Note. This gives us an alternative proof that

$$\mathrm{Hom}(V, W) = V^* \otimes W = V^* \otimes (W^*)^* = \mathrm{Hom}(W^*, V^*).$$

Proposition 18.3 (Bilinear forms are tensor products)**.** *For any vector space V, the bilinear forms $B(V) = \{V \times V \to k\}$ are naturally isomorphic to*

$$B(V) = V^* \otimes V^*.$$

Proof. Left as an exercise. □

Definition 18.6 (Tensor power)**.** Given a vector space V and nonnegative integer d, we define the *d-th tensor power* $V^{\otimes d}$ to be

$$V^{\otimes d} = \underbrace{V \otimes \cdots \otimes V}_{d \text{ times}}.$$

Definition 18.7 (Tensor algebra)**.** Observe that by associativity of the tensor product, for any $d, e \geq 0$ we have a natural map

$$V^{\otimes d} \otimes V^{\otimes e} \to V^{\otimes (d+e)}.$$

Then, we can form the algebraic structure

$$V = \bigoplus_{d=0}^{\infty} V^{\otimes d},$$

which is a non-commutative ring called the *tensor algebra* of V.

Definition 18.8 (Symmetric tensors)**.** Denote by $\mathrm{Sym}^d(V)$ the subspace of $V^{\otimes d}$ spanned by tensors that are invariant under actions by the symmetric group S_d, which permute factors.

19 October 21

Today we finish our discussion of tensors, before starting our second unit on group theory on Wednesday.

19.1 Symmetric and Exterior Algebras

Recall that we have a decomposition of bilinear forms into symmetric and skew-symmetric parts, denoted by

$$B(V) = V^* \otimes V^* = B_{symm}(V) \oplus B_{skew}(V).$$

In particular, we have that

$$\begin{aligned} B_{symm}(V) &= \{\text{tensors } \eta \in V^* \otimes V^* \text{ invariant under exchange of factors}\} \\ &= \operatorname{Sym}^2(V). \end{aligned}$$

Definition 19.1 (Averaging map)**.** We can define a linear map that makes a general tensor symmetric as follows:

$$p : V^{\otimes d} \to V^{\otimes d},$$

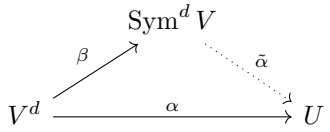
$$v_1 \otimes \cdots \otimes v_d \longmapsto \frac{1}{d!} \sum_{\sigma \in S_d} v_{\sigma(1)} \otimes \cdots \otimes v_{\sigma(d)}.$$

Definition 19.2 (Second definition of symmetric tensors)**.** Symmetric tensors are given by the quotient space

$$\operatorname{Sym}^d(V) = V^{\otimes d} \Big/ \langle t - \sigma(t) \mid t \in V^{\otimes d}, \sigma \in S_d \rangle.$$

In effect, we are "modding out" by differences of two tensors that are permutations of each others' factors.

Definition 19.3 (Third definition of symmetric tensors)**.** We also can define $\operatorname{Sym}^d V$ most nicely as a universal map, such that any symmetric d-linear form $\alpha : V^d \to U$ can be factored into a linear map $\tilde{\alpha} : \operatorname{Sym}^d V \to U$.



Proposition 19.1 (Basis for symmetric tensors)**.** *Given a basis $\{e_1, \ldots, e_n\}$ for V, we can find a basis for $\operatorname{Sym}^d V$ given by*

$$\begin{aligned} e^I &= e_1^{i_1} e_2^{i_2} \cdots e_n^{i_n} \\ &= p(\underbrace{(e_1 \otimes \cdots \otimes e_1)}_{i_1} \otimes \cdots \otimes \underbrace{(e_n \otimes \cdots \otimes e_n)}_{i_n}), \end{aligned}$$

where I ranges over all multi-indices

$$I = \left\{ i_1, \ldots, i_n \geq 0 \,:\, \sum_{\alpha=1}^{n} i_\alpha = d \right\}.$$

By a counting argument, this implies that $\dim(\operatorname{Sym}^d V) = \binom{n+d-1}{d}$.

Definition 19.4 (Symmetric algebra)**.** We can form the *symmetric algebra* of V by taking the direct sum of symmetric tensors of all dimensions, denoted by

$$\bigoplus_{d=0}^{\infty} \operatorname{Sym}^d(V),$$

which naturally has the structure of a commutative ring, with multiplication given by the tensor product

$$\operatorname{Sym}^d V \times \operatorname{Sym}^e V \to \operatorname{Sym}^{d+e} V.$$

This is isomorphic to the multivariate polynomial ring $k[e_1, \ldots, e_n]$.

Definition 19.5 (Skew-invariant tensors)**.** Define the *skew-invariant* tensors of dimension d to be the subspace of $V^{\otimes d}$ given by

$$\bigwedge^d(V) = \{\eta \in V^{\otimes d} \mid \forall \sigma \in S_d : \sigma(\eta) = \operatorname{sgn}(\sigma)\eta\}.$$

We also call this the wedge product.

Definition 19.6 (Skew-averaging map)**.** Similar to before, we can define a *skew-averaging map* on $V^{\otimes d}$ given by

$$q : V^{\otimes d} \to V^{\otimes d},$$

$$v_1 \otimes \cdots \otimes v_d \longmapsto \frac{1}{d!} \sum_{\sigma \in S_d} \operatorname{sgn}(\sigma) \cdot v_{\sigma(1)} \otimes \cdots \otimes v_{\sigma(d)}.$$

Proposition 19.2 (Basis for skew-symmetric tensors)**.** *Analogous to the symmetric case, consider a basis $\{e_1, \ldots, e_n\}$ for V. We can find a basis for $\bigwedge^d V$ given by*

$$\begin{aligned} e^I &= e_1^{i_1} e_2^{i_2} \cdots e_n^{i_n} \\ &= q(\underbrace{(e_1 \otimes \cdots \otimes e_1)}_{i_1} \otimes \cdots \otimes \underbrace{(e_n \otimes \cdots \otimes e_n)}_{i_n}), \end{aligned}$$

where I ranges over all multi-indices

$$I = \left\{ i_1, \ldots, i_n \in \{0, 1\} \,:\, \sum_{\alpha=1}^{n} i_\alpha = d \right\}.$$

Note as a corollary that $\dim \bigwedge^d V = \binom{n}{d}$.

Definition 19.7 (Exterior algebra)**.** We can form the *exterior algebra* on V by taking the direct sum of all wedge powers of V, denoted by

$$\bigoplus_{d=0}^{\infty} \bigwedge^d (V),$$

which naturally has the structure of a cummutative ring, with multiplication given by the wedge product

$$\bigwedge^d V \times \bigwedge^e V \to \bigwedge^{d+e} V.$$

19.2 Trace and Determinant

As an application of all the multilinear algebra we've talked about, we now conclude with natural definitions of the trace and determinant.

Definition 19.8 (Trace)**.** The *trace* of an $n \times n$ matrix $M = [a_{ij}]$ is given by

$$\operatorname{tr} M = \sum_{i=1}^{n} a_{ii}.$$

Our natural definition is to consider the *contraction map* $\kappa : V^* \otimes V \to k$ given by $\ell \otimes v \mapsto \ell(v)$. Then, the trace of a linear operator is simply the contraction of the corresponding element of $V^* \otimes V$ (see Prop. 18.2).

Definition 19.9 (Determinant)**.** The *determinant* of $M = [a_{ij}]$ is given by

$$\det M = \sum_{\sigma \in S_n} \left[\operatorname{sgn}(\sigma) \cdot \prod_{i=1}^{n} a_{i,\sigma(i)} \right].$$

Note that any linear operator $T : V \to V$ induces a natural map $V^{\otimes d} \to V^{\otimes d}$ given by taking each factor under T. In other words,

$$v_1 \otimes v_2 \otimes \cdots \otimes v_d \longmapsto T(v_1) \otimes T(v_2) \otimes \cdots \otimes T(v_d).$$

Recall that the dimension of $\bigwedge^n V$ is simply $\binom{n}{n} = 1$, so there is an induced map $\bigwedge^n V \to \bigwedge^n V$ between one-dimensional vector spaces, which must be a scalar multiplication. Then, the determinant of T is precisely this linear map.

Note. Observe that $V \otimes W = \operatorname{Hom}(V^*, W)$. In particular, for any such map $\varphi : V \to W$ there exist bases $e_1, \ldots, e_m$ for V and $f_1, \ldots, f_n$ for W, we can write φ with block matrix representative given by an identity matrix with dimension equal to its rank k. Then, we have that $\varphi = e_1 \otimes f_1 + \cdots + e_k \otimes f_k$, the sum of k pure tensors. We can also show that there is no way to express φ as the sum of $k-1$ or fewer pure tensors; hence, the rank of a tensor in $V \otimes W$ is equal to the rank of the corresponding linear map $V^* \to W$.

Note. In general, we know nothing about the rank of elements in the triple tensor product $U \otimes V \otimes W$. In the case that $\dim U = 2$, this classification was completed by Kronecker in the 19^{th} century.

20 October 23

Today we finally start Group Theory Part II, beginning with Artin §6.7.

20.1 Group Actions

The following construction proves useful in studying groups.

Definition 20.1 (Group action)**.** An *action* of a group G on a set S is a map $\varphi : G \times S \to S$ that associates with group multiplication and preserves identity:

- $\varphi(h, \varphi(g, s)) = \varphi(hg, s)$.
- $\varphi(e, s) = s$.

Equivalently, a group action is a homomorphism $G \to \text{Perm}(S)$. Oftentimes, the action that we are discussing is implied by context, so we typically write $g(s)$ as a shorthand for $\varphi(g, s)$.

Example 20.1. The following are standard examples of group actions:

- S_n acts on $\{1, \dots, n\}$.
- $\text{GL}_n(k)$ acts on k^n.
- D_8 acts on the vertices of a square.
- G acts on itself by left multiplication.
- G acts on itself by conjugation.

In the last two examples, there is an ambiguity when talking about "the action" of a group on itself, since left multiplication and conjugation are both studied. We have to be careful not to get these mixed up; Artin uses special notation for this.

20.2 Orbits and Stabilizers

This subsection introduces the key constructions on group actions.

Definition 20.2 (Orbit)**.** For all $x \in S$, the *orbit* of x is the set of all elements that x can be sent to under action by any element of G, i.e.,

$$G \cdot x = \{gx : g \in G\}.$$

We can alternatively define an equivalence relation on S such that $s \sim t$ if there exists $g \in G$ with $gs = t$. The orbits are then equivalence classes of S.

Note. Here, Joe uses the notation O_s for the orbit of s rather than $G \cdot s$, but I will use with the more conventional notation.

This last definition implies that S can be partitioned into the disjoint union of its orbits. In effect, an action on S can be broken down into separate actions on each orbit of S, so we have a name for actions with only one orbit.

Definition 20.3 (Transitive)**.** An action is *transitive* if $S = G \cdot s$ for any $s \in S$.

Observe that in our previous example, the action of G on itself by left multiplication is transitive, due to the existence of inverses. However, conjugation is not transitive, as the identity element is in an orbit by itself. We call the orbits of the conjugation action *conjugacy classes* of G.

Definition 20.4 (2-transitive)**.** An action is called 2-*transitive* if for all $s_1 \neq s_2$ and $t_1 \neq t_2$ in S, there exists a $g \in G$ such that $g(s_1) = t_1$ and $g(s_2) = t_2$.

Definition 20.5 (Stabilizer)**.** The *stabilizer subgroup* of x, for any $x \in S$, is the subgroup of G that sends x to itself. We write this as

$$G_x = \{g \in G : g(x) = x\}.$$

Note. Joe denotes this as $\text{stab}(x)$ instead of G_x, but I am not as violent.

For example, consider a group G and subgroup $H \subset G$. When we take the action of G on the left cosets G/H by left multiplication, note that the stabilizer of of any element is H, and each element of G/H is a coset of H. It turns out that this holds in general.

Proposition 20.1 (Stabilizers are conjugate subgroups)**.** *Let s and s' be members of the same orbit, given an action of G on S. Then, the stabilizers of s and s' are the same under conjugation.*

Proof. Let $s' = hs$. Then,

$$gs = s \iff (hgh^{-1})s' = s'.$$

□

Proposition 20.2 (Orbit-stabilizer theorem)**.** *For any transitive group action of G on S, let H be the stabilizer of any element. Then, there is a one-to-one identification between G/H and S. In general, this implies that for any group action (not necessarily transitive),*

$$|G|/|G_x| = |G \cdot x|.$$

Corollary 20.2.1 (Class equation)**.** *Given a finite group G, let $C_1, \ldots, C_k \subset G$ be the conjugacy classes. Then,*

$$|G| = |C_1| + \cdots + |C_k|.$$

In addition, by the orbit-stabilizer theorem, we have that $|C_i| \mid |G|$ for all i, and at least one of the conjugacy classes has size 1.

Corollary 20.2.2. *If $|G| = p^n$ where p is prime, then there exist at least p conjugacy classes of size 1.*

Proposition 20.3 (Groups of prime-square order are abelian)**.** *For any prime p, all groups G such that $|G| = p^2$ are abelian.*

Proof. We know that $\{e\} \subsetneq Z(G)$ because there are p conjugacy classes of size 1, each of which belongs in the center. By Lagrange's theorem, either $|Z(G)| = p^2$, in which case G is abelian, or $|Z(G)| = p$.

If $|Z(G)| = p$, then choose any $x \notin Z(G)$, and define the subgroup stabilizing x to be $Z(x) = \{h \in G : hx = xh\}$. We know that $Z(x) \supset Z(G)$, and also that $x \in Z(x)$. However, this implies that $Z(x)$ has at least $p + 1$ elements, so it must have order p^2, and $Z(x) = G$. This implies that x commutes with all elements of G, so $x \in Z(G)$, which is a contradiction. □

Finally, we prove a useful formula for counting orbits in a group.

Proposition 20.4 (Burnside's lemma)**.** *Given an action of G on S, let S/G be the set of orbits of S under the action. Also, let S^g be the subset of S that is fixed by g. Then,*

$$|S/G| = \frac{1}{|G|} \sum_{g \in G} |S^g|.$$

Proof. Consider the set

$$\Gamma = \{(g, s) : g \in G_s\} = \{(g, s) : gs = s\}.$$

We can then count the cardinality of Γ in two ways, either by elements of S or G. This gives us two equivalent formulas,

$$|\Gamma| = \sum_{g \in G} |S^g| = \sum_{s \in S} |G_s|.$$

However, note that for each orbit of the action, G_s has the same size for all elements of the orbit, as by Prop. 20.1. In particular, we can find this size using the orbit-stabilizer theorem, which yields

$$\sum_{g \in G} |S^g| = \sum_{O \subset S} \sum_{s \in O} |G_s| = \sum_{O \subset S} \sum_{s \in O} \frac{|G|}{|O|} = |G| \cdot |S/G|.$$

Dividing both sides by $|G|$ yields the desired result. □

21 October 25

I was absent from this lecture. Topics covered included actions of rotations in 3D space on a sphere.

22 October 28

Today we discuss symmetric groups and alternating groups.

22.1 Permutations

Recall that $\mathrm{Perm}(S)$ is the group of all permutations of S. When S is a finite set, $\mathrm{Perm}(S)$ depends only on the order of the set, so when $|S| = n$, we write

$$\mathrm{Perm}(S) \cong \mathrm{Perm}\{1, 2, \ldots, n\} = S_n.$$

Recall from Sec. 4.4 the cycle notation for permutations. Any permutation is uniquely expressible as a product of disjoint cycles, each of which commute. Note also that in the language of group actions, each cycle of σ is an orbit of the action of the subgroup $\langle\sigma\rangle$ generated by σ.

Proposition 22.1 (Conjugacy classes of S_n)**.** *Given any permutation τ and cycle $(a_1 \ldots a_k)$, the conjugate of the cycle with respect to τ is*

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

As a consequence, two permutations $\sigma, \sigma' \in S_n$ are conjugate if and only if they have the same cycle lengths.

Corollary 22.1.1. *The number of conjugacy classes of S_n is equal to $p(n)$, the number of integer partitions of n.*

One natural question we might ask is to determine how many elements belong to each conjugacy class. To derive a formula for this, we first write a partition of n in the form

$$n = b_1 \cdot 1 + b_2 \cdot 2 + b_3 \cdot 3 + \cdots,$$

where each b_j reflects the number of occurrences of j in the partition sum.

Proposition 22.2. *The number of elements in the conjugacy class of S_n given by the partition $\{b_1, b_2, \ldots, b_n\}$ is*

$$\frac{n!}{\prod_{i=1}^{n} i^{b_i} \cdot b_i!}.$$

Proof. The number of ways of breaking up a set of n elements into labeled subsets of size $c_1, \ldots, c_k$ is given by the multinomial coefficient

$$\binom{n}{c_1; \cdots; c_k} = \frac{n!}{c_1! \cdots c_k!}.$$

If we instead have unlabeled subsets, we also need to divide by the number of ways to arrange the subsets of each length, which yields the formula

$$\frac{n!}{((1!)^{b_1} \cdots (n!)^{b_n})(b_1! b_2! \cdots b_n!)}.$$

Now, within each selected cycle of length i, we have $(i-1)!$ ways to cyclically permute the elements of that cycle, so multiplying the formula above by the factor $((i-1)!)^{b_i}$ for each i gives us our final result. $\square$

Exercise 22.1. Count the number of permutations with no fixed points.

22.2 The Alternating Group

Since the alternating group A_n is pretty much almost the symmetric group (it has index 2), we borrow the same cycle notation for permutations in A_n. However, we will see that A_n gives us some additional restrictions on the lengths of cycles, and also, conjugacy classes in A_n are no longer as simple as in S_n.

Recall that the sign of a permutation σ is given by the sign homomorphism, taking $S_n \to \mathbb{Z}/2\mathbb{Z} = \{\pm 1\}$, which maps

$$\sigma \longmapsto \frac{\prod_{i<j}(x_i - x_j)}{\prod_{i<j}(x_{\sigma(i)} - x_{\sigma(j)})} = \pm 1.$$

The kernel of this sign homomorphism is precisely A_n. Notice that any cycle is an even permutation if it has odd length, and conversely a cycle is an odd permutation if it has even length. Since every permutation can be broken up into cycles, we can describe the elements of A_n in cycle notation.

Proposition 22.3. *A permutation in S_n is in A_n if and only if it has an even number of cycles of even length.*

Since conjugacy classes of S_n are precisely given by permutations with the same partition into cycle lengths, we know that every conjugacy class $C \subset S_n$ is either disjoint from A_n or contained in it. However, some conjugacy classes may be broken up.

Example 22.1 (Additional conjugacy classes in A_n)**.** In S_4, we have that the two cycles (123) and (124) are conjugate, as

$$(124) = (34)(123)(34).$$

However, these two permutations are not conjugate in A_4, as (34) is not an element of A_4. In particular, by the orbit-stabilizer theorem, any conjuacy class must divide the group in order. While the order of the (123) conjugacy class in S_4 is 8, the order of A_4 is 12, so the conjugacy class must be broken up.

Proposition 22.4. *If G acts transitively on S and $H \subset G$ is a subgroup of index 2, then the action of H on S has either one or two orbits.*

Proof. Note that taking any $a \notin H$, we have that $G = H \cup aH$, the union of two cosets. This implies that

$$G(s) = Hs \cup aHs,$$

and the result follows immediately. If $Hs = aHs$, then the action of H on S is transitive, but otherwise it has two orbits. This occurs if and only if there exists an $a \notin H$ such that $as = s$. $\square$

This means that given any conjugacy class $C \subset S_n$ there are three possibilities for the form of C in A_n:

- $C \cap A_n = \emptyset$, if C consists of odd permutations.
- $C \subset A_n$ and is a conjugacy class in A_n.
- $C \subset A_n$ and is the union of *two* conjugacy classes in A_n.

Exercise 22.2. What are the conditions on C for distinguishing between the second and third of these possibilities?

23 October 30

Today we continue with more facts about symmetric and alternating groups, and we prove the Sylow theorems.

23.1 More on Symmetric and Alternating Groups

Recall the exercise from last lecture: to determine whether a conjugacy class C_b in S_n is still a conjugacy class in A_n, or if is broken up into two orbits.

Proposition 23.1. *A conjugacy class $C_b \subset S_n$ that lies within A_n is broken up into two conjugacy classes of A_n if and only if both:*

- *All cycles of the permutation have odd length ($b_{2k} = 0$).*
- *No two cycles have the same length ($b_{2k+1} \leq 1$).*

Otherwise, C_b is a conjugacy class of A_n.

Proof. If $b_{2k} \neq 0$ for some k, then a permutation $\sigma \in C_b$ looks like

$$\sigma = (\ )(\ )(a_1 \dots a_{2k})(\ )(\ ) \cdots (\ ).$$

This clearly commutes with the even cycle $(a_1 \dots a_{2k}) \in S_n \backslash A_n$, so it is invariant under conjugation by this cycle (the action), and therefore the action of A_n on C_b is transitive.

Also, if $b_{2k+1} > 1$, then $\sigma \in C_b$ looks like

$$\sigma = (\ )(\ )(a_1 \dots a_{2k+1})(b_1 \dots b_{2k+1})(\ )(\ ) \cdots (\ ).$$

Notice that this commutes with the permutation that swaps a_i with b_i for all i, which is an odd permutation because $2k+1$ is odd. Thus, σ is once again invariant under the action of a permutation in $S_n \setminus A_n$, so the action of A_n on C_b is transitive.

The reverse direction of this proof is left as an exercise. □

Example 23.1. The class equations for S_5 and A_5 are shown below.

C_b	S_5	A_5
e	1	1
(12)	10	—
(123)	20	20
(1234)	30	—
(12345)	24	**12 + 12**
(12)(34)	15	15
(12)(345)	20	—

This fact is quite nice, and it leads to the following important corollary.

Corollary 23.1.1 (A_5 is simple)**.** *The class equation for A_5 is*

$$|A_5| = 60 = 1 + 20 + 12 + 12 + 15.$$

However, no sub-sum (including 1) of classes divides 60. Thus, by Lagrange's theorem, there are no nontrivial normal subgroups of A_5, so it is simple.

We're only talking about A_5 here, which is important in broader mathematics because it is related to the fact that quintic polynomials are not solvable. However, it turns out that this is true more generally, as the following proposition shows.

Proposition 23.2. *For any $n \geq 5$, A_n is a simple group.*

Proof. First, observe the following basic facts:

- A_n is generated by 3-cycles, as $(ijk)(j\ell i) = (ik)(j\ell)$.
- In A_n for $n \geq 5$, the 3-cycles form a single conjugacy class.

It suffices to prove that any nontrivial normal subgroup $\{e\} \neq N \subset A_n$ contains a 3-cycle. If so, then we can conjugate that 3-cycle to generate all 3-cycles in A_n, which then generates the entire alternating group.

To complete the proof, choose any $\sigma \neq e$ in N, and replace σ by $\tau = \sigma^a$ for some a such that τ has prime order ℓ. We can then do casework on ℓ:

- $\ell \geq 5$. Conjugate each 5-cycle to its inverse, except one, $(abcde)$, which will map to $(ebcad)$. Then, $(abcde)(ebcad) = (abc)$.
- $\ell = 3$. Conjugate each 3-cycle to its inverse, except one, π. This leaves us with a single 3-cycle π^2.
- $\ell = 2$. Conjugate each 2-cycle to its inverse, except one, π. If there exists any fixed point of the permutation, then we are done. Otherwise n is even and at least 6, so there are at least three 2-cycles; conjugate all others to their inverses. Then, we can multiply $(ab)(cd)(ef)$ by $(ad)(be)(cf)$ to get $(ace)(bdf)$, which reduces to the last case.

□

23.2 The Sylow Theorems

Take an arbitrary group G. Recall that by Lagrange's theorem, we know that the order of any element $g \in G$ divides $|G|$. The converse of this statement is that for any $m \mid |G|$, there exists an element of order m. This is clearly not true, as the example of $(\mathbb{Z}/p\mathbb{Z})^k$ easily shows.

We might consider a slightly weaker question: if there exists a subgroup of order m for any m dividing $|G|$. It turns out that this is also false, as you can take $G = A_5$ and $m = 30$ as a counterexample. However, by weakening this a little further, we arrive at the first Sylow theorem.

Proposition 23.3 (First Sylow theorem)**.** *For every prime p of multiplicity n in the factorization of $|G|$, there exists a subgroup $H \subset G$ of order p^n. This is called a Sylow p-subgroup (or p-Sylow subgroup).*

Corollary 23.3.1. *For any group G and prime p such that $p \mid |G|$, there exists an element $g \in G$ of order p.*

Proof. Let H be a Sylow p-subgroup, and let $h \in H$ be a non-identity element. By Lagrange's theorem, h has order dividing $|H| = p^n$, so let the order of h be p^k for $k \geq 1$. Then, $h^{p^{k-1}}$ has order p in G. □

Proposition 23.4 (Second Sylow theorem)**.** *For any group G, all Sylow p-subgroups of G are conjugate to one another. In other words, if H and K are Sylow p-subgroups, then $gHg^{-1} = K$ for some $g \in G$.*

Proposition 23.5 (Third Sylow theorem)**.** *Let the number of Sylow p-subgroups be s, and write $|G| = p^n m$, where n is the multiplicity of p. Then, $s \mid m$ and $s \equiv 1 \pmod{p}$.*

We will prove all three theorems in the following lectures!

24 November 1

I was absent from this lecture. Topics covered included examples of applying the Sylow theorems to classify groups of orders 15 and 21, as well as proofs of the first and second Sylow theorems.

25 November 4

Today we finish a proof of the Sylow theorems and discuss one more application of them. On Wednesday, we will move on to group presentations, finite abelian groups, and representation theory.

25.1 Normalizers and the Third Sylow Theorem

We define a new notation related to conjugation of subgroups.

Definition 25.1 (Normalizer)**.** Given a group G and any subgroup $H \subset G$, the *normalizer* of H is given by

$$N(H) = \{g \in G \mid gHg^{-1} = H\}.$$

This is essentially the largest subgroup of G such that H is a normal subgroup of $N(H)$. Considering the action of G on its subgroups by conjugation, the normalizer $N(H)$ is just the stabilizer of the subset H, or $G_{[H]}$.

Considering the action of G under conjugation, this immediately tells us (by the orbit-stabilizer theorem) that

$$\#(\text{subgroups conjugate to } H) = \frac{|G|}{|N(H)|}.$$

We can use this fact to prove the third Sylow theorem.

Proposition 25.1 (Third Sylow theorem)**.** *If G is a finite group such that $|G| = p^e m$ and $p \nmid m$, then a Sylow p-subgroup of G is any group of cardinality p^2. If s_p is the number of such groups, then $s_p \mid m$ and $s_p \equiv 1 \pmod{p}$.*

Proof. From the second Sylow theorem, if H is any Sylow p-subgroup, then all other Sylow p-subgroups are conjugate to H. Then, by the last observation about normalizer subgroups,

$$s_p = \frac{|G|}{|N(H)|}.$$

However, note that $|H| \mid |N(H)|$ by Lagrange's theorem as H is a normal subgroup of $N(H)$, which implies that

$$s_p \mid \frac{|G|}{|H|} = m.$$

This gives us the first part of the theorem. To prove the second fact, let $T = \{\text{Sylow } p\text{-subgroups of } G\}$. Then, consider the action of H on T by conjugation, and observe that $[H]$ is a fixed point for this action (the set corresponding to H). We claim that $[H]$ is the only fixed point.

Assume that there exists some H' that is fixed under conjugation by H. Then, this implies that $H \subset N(H')$, and we also know that $H' \subset N(H')$ as a

normal subgroup. Since $N(H') \subset G$, the order of $N(H')$ must be of the form $p^e \cdot n$, so this means that H, H' are both Sylow p-subgroups of $N(H')$, and by the second Sylow theorem, they must be conjugate. However, recall that H' is already a normal subgroup of $N(H')$, so it is invariant under conjugation, and therefore $H = H'$ is the only fixed point.

Now, under action of H, T is a disjoint union of orbits. However, each orbit must have size p^k for some k by the orbit-stabilizer theorem, as the size must divide the order of H. Since $[H]$ is the only fixed point for the action of H on T, it is the only orbit of size 1, so therefore $|T| \equiv 1 \pmod{p}$. □

25.2 Applying the Sylow Theorems

We present an example of classifying finite groups of a given order.

Example 25.1. What are the groups of order 12?

Observe that the number of Sylow 3-subgroups, by the third Sylow theorem, is equal to 1 or 4. Similarly the number of Sylow 2-subgroups is equal to 1 or 3. Let K be a Sylow 3-subgroup and H be a Sylow 2-subgroup of G, and consider the following cases.

- $s_2 = s_3 = 1$. This means that H, K are each normal and $G = H \times K$, so G is either $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ or $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$.
- $s_3 = 4, s_2 = 3$. This would mean that ignoring the identity element, there are at least $2s_3 = 8$ elements with order 3 and $3s_2 = 9$ elements with order 2 or 4. However, $1 + 8 + 9 > 12$, so this case is impossible.
- $s_3 = 4, s_2 = 1$. Then, H is normal and K is not normal. Observe that G acts on the set T_3 of Sylow 3-subgroups of G under conjugation. Then, the stabilizer $G_{[K_i]}$ has order equal to $|G|/|T_3| = 3$, but observe that $K_i \subset G_{[K_i]}$, so thus each K_i is fixed by only elements of itself. This means that no non-identity element of G fixes all four elements of T_3, so there exists an inclusion $G \hookrightarrow S_4$. Hence, $G \cong A_4$.
- $s_3 = 1, s_2 = 3$. Let $K = \{1, y, y^2\}$. For all $x \in H$, note that $xyx^{-1} \in K$ because K is normal, so xyx^{-1} is either y or y^2. This breaks up into two cases based on the structure of H.
  - $H \cong \mathbb{Z}/4\mathbb{Z}$. Let x be a generator of H, and note that if $xyx^{-1} = y$ then x and y would commute and then $G = \mathbb{Z}/12\mathbb{Z}$, which contradicts our assumption that $s_2 = 3$. Then $xyx^{-1} = y^2$, and G is generated by x, y under the relations $x^4 = y^3 = e$ and $xyx^{-1} = y^2$. This is called the dicyclic group of order 12, denoted Q_{12}.
  - $H \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. Let $H = \langle x, z \rangle$. This implies that $xyx^{-1} = y^2$ and $zyz^{-1} = y$, so G is generated by x, y, z under the relations $x^2 = z^2 = (xz)^2 = e$, $xyx^{-1} = y^2$, and $zyz^{-1} = y$. It turns out that this is isomorphic to the dihedral group D_{12}.

Thus, there are two abelian and three non-abelian groups of order 12.

26 November 6

Today we discuss free groups, generators, and relations in the context of group presentations. We will also talk about finite abliean groups.

26.1 Free Groups and Presentations

Recall that the definition of the free group on 2 generators (Def. 5.6) to be the set of all words on a, b, a^{-1}, b^{-1}, with law of composition given by concatenation and reduction. We can generalize this to n generators with the following definition.

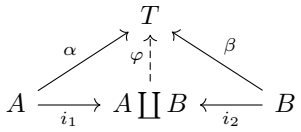
Definition 26.1 (Free group)**.** The free group F_n on n generators is given by all words on $c_1, c_1^{-1}, \ldots, c_n, c_n^{-1}$, with law of composition given by concatenation of words, and subject to the reduction relation $c_i c_i^{-1} = e$.

Note that we can additionally define F_S for any set S, but in practice this rarely comes up because we'll have at most countably many generators.

Recall that we can also generalize this definition to the *free product* of two groups $G * H$, which is a group consisting of reduced words with elements alternating between G and H (see Def. 5.7).

Proposition 26.1 (Free product in category theory)**.** *The free product is the coproduct (or sum) in the category of groups.*

Proof. Recall it suffices to show that there exists a unique φ such that the following diagram commutes for any T and homomorphisms α, β.



In other words, any two homomorphisms $A \to T$ and $B \to T$ factor to a unique homomorphism $A * B \to T$. This is easy to check because $A \cup B$ generates $A * B$ with no restrictions (hence a "free" product). □

Corollary 26.1.1. *In the category of abelian groups, the free product is the same as the ordinary product, and thus the coproduct and product coincide.*

Example 26.1 (Examples of free products)**.** Free products tend to show up often in standard examples. For example, $F_2 = \mathbb{Z} * \mathbb{Z}$ is the the free group on two generators. Also, $D_\infty = \mathbb{Z}/2 * \mathbb{Z}/2$ is the infinite dihedral group, and $\mathbb{Z}/2 * \mathbb{Z}/3 \cong SL_2\mathbb{Z}$ is the group of 2×2 matrices with determinant 1 on $\mathbb{Z}$.

With all these interesting properties of free groups, it is then instructive to consider how they might relate to groups in general. If G is a finitely generated group (with n generators), there exists a surjective homomorphism $F_n \to G$. Then, the kernel $K \subset F_n$ is the subgroup of relations on the free group.

Definition 26.2 (Group presentation)**.** If G is a finitely generated group, then call G *finitely presented* if the kernel K is also finitely generated. Then, we can write the *group presentation* of G as

$$G = \langle F_n \mid K \rangle = \langle \alpha_1 \dots \alpha_n \mid \beta_1 \dots \beta_m \rangle,$$

for some symbols $\{\alpha_j\}$ and relations $\{\beta_j\}$ each consisting of words of symbols.

Example 26.2. The non-abelian group with 21 elements has presentation

$$G_{21} = \langle x, y \mid x^7, y^3, yxy^{-1}x^{-2} \rangle.$$

Note that although presentations exist, they do not actually tell us much information about groups. In general, it turns out that the problem of determining the structure of a group based on its presentation is undecidable (this is called the *word problem*).

26.2 Finite Abelian Groups

We first write down the "big shot" structure theorem about finite abliean groups.

Proposition 26.2 (Fundamental theorem of finite abelian groups)**.** *Any finite abelian group G is the product of cyclic groups*

$$G \cong \bigoplus_{i=1}^{\ell} \mathbb{Z}/a_i.$$

Note that in general the a_i's are not uniquely determined by G, but they can be factored uniquely into a product of prime powers.

Proof. Let $|G| = n = \prod_{i=1}^{k} p_i^{e_i}$. By the Sylow theorems, there are unique Sylow p-subgroups $H_i \subset G$ for each i. Furthermore, each of these subgroups is unique by the second Sylow theorem (because they are normal), so G is the direct sum of the H_i. This provides us with half of the proof.

The remaining part of the proof is to show that if G is an abelian group of order p^e, then there exist some e_i summing to e such that such that

$$G \cong \bigoplus_{i=1}^{m} \mathbb{Z}/p^{e_i}.$$

The rest of the proof is deferred to Math 123, as it requires the structure theorem of finitely generated modules over a principal ideal domain. □

Corollary 26.2.1 (Number of finite abelian groups)**.** *Given an integer n with prime factorization $n = \prod_{i=1}^{\ell} p_i^{e_i}$, the number of distinct finite abelian groups with order n is given by*

$$\prod_{i=1}^{\ell} p(e_i),$$

where $p(k)$ is the partition function representing the number of distinct integer partitions of k.

26.3 Group Characters

While on the topic of abliean groups, we can see one application of this structure theorem to the new subject of characters.

Definition 26.3 (Character of an abelian group)**.** Given an abelian group G, a character χ of G is a homomorphism

$$G \longrightarrow S^1 = \mathbb{R}/\mathbb{Z} = \{z = \mathbb{C} : |z| = 1\}.$$

Observe that the set of all characters on G forms a group $\widehat{G} = \text{Hom}(G, S^1)$ with multiplication given by $(\chi\psi)(g) = \chi(g)\psi(g)$.

Lemma 26.3 (Characters of products)**.** *For any abelian groups G, H,*

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

Proof. Apply Prop. 26.1. □

Lemma 26.4 (Characters of cyclic groups)**.** *For any n, there is an isomorphism $\widehat{\mathbb{Z}/n} \cong \mathbb{Z}/n$, though this is not canonical.*

Proof. Observe that characters of $\mathbb{Z}/n$ are determined by the image of 1, which can be sent to an n-th root of unity $e^{2\pi ik/n}$, for some $k \in \{0, 1, \ldots, n-1\}$. We conclude that there we can construct the map $\chi \mapsto k$, which is an isomorphism from $\widehat{\mathbb{Z}/n}$ to $\mathbb{Z}/n$. □

Proposition 26.5 (Characters of finite abelian groups)**.** *If G is a finite abelian group, then $G \cong \widehat{G}$, though not canonically.*

Note that this theorem does not necessarily hold when G is infinite, as in the example $\widehat{Z} = S^1$. However, when G is finite, this gives the characters a structure analogous to that of a dual vector space. In particular, it turns out that there is a natural isomorphism between G and $\widehat{\widehat{G}}$ given by

$$g \mapsto (\chi \mapsto \chi(g)).$$

From here, we don't have enough time to start representation theory, but we'll do it next lecture. Our main reference will be Fulton-Harris chapters 1–3, and an alternative source is Serre's *Linear representation of finite groups*.

27 November 8

Today we start representation theory. For a little bit of a history lesson: in the 19^{th} century, a group was simply a subset of GL_n closed under matrix multiplication and inversion. However, in the 20^{th} century, people began seeing groups as sets with a law of composition satisfying certain axioms, which are abstract equivalence classes of "19^{th} century" groups under isomorphism.

Thus, the problem of "classifying all groups" in the 19^{th} century sense breaks up into two steps:

- Classifying all abstract groups.
- For a given G, describe all ways G can be mapped to GL_n.

27.1 Representations

We therefore study the second of the above tasks, which forms the basis of representation theory.

Definition 27.1 (Representation)**.** Given a finite group G, a representation is a vector space V on which G acts, such that for all $g \in G$, the action $g : V \to V$ is linear. Equivalently, a representation of G is a homomorphism $\rho : G \to \mathrm{GL}(V)$.

Note that this definition does not necessarily guarantee that each group element reflects a distinct linear transformation. We have another term for this.

Definition 27.2 (Faithful representation)**.** A representation $\rho : G \to \mathrm{GL}(V)$ is called *faithful* if it is injective. In other words, there is no non-identity element $g \in G$ that acts on all vectors in V as the identity.

At the other end of the spectrum, we can always represent a group by trivially mapping all elements to the identity morphism.

Example 27.1 (Trivial representation)**.** If $\rho = e$, meaning that the action of every group element is the identity, then this is a representation called the *trivial representation* of G on V.

Note. We will abuse notation by calling a particular representation of G on a vector space V simply by the name V, implying the representation structure.

27.2 Constructions on Representations

For the rest of this course (except the last lecture), we assume that V will always be a vector space over $\mathbb{C}$. Our end goal will be to classify all representations of a finite group. However, first we need to get through a few definitions.

Definition 27.3 (Homomorphism of representations)**.** Let V, W be representations of a group G. A *homomorphism* is a linear map $\varphi : V \to W$ that respects the action of G on V, W, meaning that

$$\varphi(gv) = g(\varphi(v)).$$

This makes the following diagram commute.

$$\begin{array}{ccc} V & \xrightarrow{\varphi} & W \\ \downarrow{\scriptstyle g} & & \downarrow{\scriptstyle g} \\ V & \xrightarrow{\varphi} & W \end{array}$$

We call the set of all homomorphisms from a representation V to another representation W by the name $\mathrm{Hom}_G(V, W)$.

Definition 27.4 (Subrepresentation)**.** In the special case of a faithful representation V of G, then a *subrepresentation* U is a subspace $U \subset W$ such that $g(U) = U$ for all $g \in G$.

Definition 27.5 (Trivial subrepresentation)**.** If V is any representation of the group G, then the *trivial subrepresentation* is the maximal subrepresentation of V that is trivial. It is defined by

$$V^G = \{v \in V \mid \forall g \in G : gv = v\}.$$

Note. Given a representation V and a subrepresentation of G on U, then we can also define the induced action of G on the quotient space V/U, which is called the *quotient representation*.

Definition 27.6 (Irreducible representation)**.** We call a representation V of G *irreducible* if there does not exist a nontrivial proper subspace $W \subsetneq V$ such that $g(W) = W$.

Definition 27.7 (Linear algebra on representations)**.** Given representations V, W of G, the *direct sum* $V \oplus W$ has the structure of a representation of G, with action

$$g(v, w) = (gv, gw).$$

The *tensor product* $V \otimes W$ also has the structure of a representation, with action

$$g(v \otimes w) = g(v) \otimes g(w).$$

The *dual space* V^* has the structure of a representation, with action

$$g \mapsto {}^t g^{-1}.$$

We can similarly define $V^{\otimes n}$, $\mathrm{Sym}^n V$, and $\bigwedge^n V$, such that the corresponding identities apply. In particular, we have that $\mathrm{Hom}(V, W) = V^* \otimes W$, so we can define the action of G on $\mathrm{Hom}(V, W)$ to be

$$g : \varphi \longmapsto g_W \circ \varphi \circ g_V^{-1}.$$

Exercise 27.1. Given representations V, W, of G, show that

$$\mathrm{Hom}(V, W)^G = \mathrm{Hom}_G(V, W).$$

28 November 11

Today we talk about complete reducibility, an important property of representations of finite groups, as well as Schur's lemma. We'll also give some concrete examples of representations.

28.1 Complete Reducibility

We move on to an important theorem, which will first require a lemma.

Lemma 28.1. *Given a representation V of G, there exists a Hermitian inner product $H : V \times V \to \mathbb{C}$ that is invariant under G, i.e,*

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

Proof. We start with any Hermitian inner product $H_0 : V \times V \to \mathbb{C}$, and define a new Hermitian inner product H by applying the "averaging" map

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

Since this is a sum of Hermitian inner products, it is itself a Hermitian inner product, which is clearly invariant under G. Note that this is not canonical because of the choice of H_0, though we will see later on that it is unique when V is irreducible. □

Proposition 28.2 (Complete reducibility)**.** *Every representation of a finite group G is a direct sum of irreducible representations. In other words, given a representation V of G and subrepresentation (invariant subspace) $U \subset V$, there exists another invariant $W \subset V$ such that $V = W \oplus U$.*

Proof. Using the previous lemma, we know that for any invariant U, $gU = U$ for all $g \in G$, and g is also a unitary operator under the Hermitian inner product H. This implies that $U^\perp$ is also invariant under g, so we are done.

Alternatively, we can also prove this without using Hermitian forms. Let $W_0 \subset V$ be any complementary subspace such that $V = U \oplus W_0$. Then, let $\pi_0 : V \to U$ be the projection map with kernel W_0, and define $\pi : V \to U$ to be the "averaged" map

$$\pi(v) = \sum_{g \in G} g^{-1} \pi_0(gv).$$

Observe that π applied to any element of U is simply a constant multiple of the identity, so $\pi|_U = |G| \cdot \mathrm{id}_U$. This means that π is surjective. Furthermore, observe that the kernel $W = \ker(\pi)$ is invariant under g, so $V = U \oplus W$. □

Note. Both of these proofs assume that we are working on vector spaces over a field of characteristic zero. This statement is false in groups with positive characteristic.

Example 28.1 (Irreducibility of an infinite group)**.** Consider the representation of $\mathbb{R}$ in $\mathbb{R}^2$ given by the action

$$t \longmapsto \begin{bmatrix} 1 & t \\ 0 & 1 \end{bmatrix}.$$

Then, the x-axis $\langle (1,0) \rangle$ is an invariant subspace, but there does not exist a complementary invariant subspace under this action.

Note. Complete reducibility still holds for special classes of infinite groups: in particular, representations that consist of continuous maps on S^1. In this case, we can represent this Lie group by replacing the sum in the second proof above by an integral on the unit circle.

28.2 Schur's Lemma

We move to a foundational lemma in the study of irreducible representations.

Proposition 28.3 (Schur)**.** *Assume that V, W are irreducible representations of a finite group G over $\mathbb{C}$, and let $\varphi : V \to W$ be a homomorphism of representations. Then,*

i) φ is either an isomorphism or zero.

ii) In the case that $V = W$, $\phi = \lambda \cdot \mathrm{id}$ for some $\lambda \in \mathbb{C}$.

Proof. Note that $\ker \varphi \in V$ and $\operatorname{im} \varphi \in W$ are invariant subspaces, so by the complete reducibility of representations, either $\ker \varphi = 0$ and $\operatorname{im} \varphi = W$, or $\ker \varphi = V$ and $\operatorname{im} \varphi = 0$. This gives us the first part.

For the second part, observe that if we have a homomorphism $\varphi : V \to V$, then this must have an eigenvalue λ by the algebraic closure of $\mathbb{C}$. Then, $\varphi - \lambda I$ has a kernel, so hence it is zero. □

Note. Observe that if

$$\begin{aligned} V &= V_1^{\oplus a_1} \oplus \cdots \oplus V_k^{\oplus a_k} \\ &= W_1^{\oplus b_1} \oplus \cdots \oplus W_\ell^{\oplus b_\ell}, \end{aligned}$$

then let φ be an isomorphism between these two direct sums. Take any W_i, and consider $\varphi|_{W_i}$ applied to each V_j. By Schur's lemma, this is either zero or an isomorphism. Thus, we must have a copy of each V_j in the $\{W_i\}$.

Proposition 28.4 (Representations of abelian groups)**.** *If G is abelian, then any irreducible representation of G is one-dimensional.*

Proof. In general, if V is a representation of G, then for all $g \in G$ there is a map $g : V \to V$. Considering g as a linear map, in general we do not have that g is a homomorphism of representations from V to V, as $g(hv) \neq h(gv)$. However, this is true for the special case of abelian groups!

Then, by Schur's lemma we know that each element of g is a constant times the identity, so V as an irreducible representation must be one-dimensional. □

Corollary 28.4.1 (Simultaneously diagonalizable representations)**.** *Given any representation of a finite abelian group G in $\mathrm{GL}(V)$, there exists a basis for V such that all actions $g \in G$ are diagonal.*

28.3 Examples of Representations

Given our last statement about representations of abelian groups, the first interesting example should be $G = S_3$. This has a couple of irreducible representations.

Example 28.2 (Trivial representation)**.** There is the *trivial representation* $U \cong \mathbb{C}$ with actions given by the identity.

Example 28.3 (Alternating representation)**.** The *alternating representation* of S^3 on $U' \cong \mathbb{C}$ is given by $\sigma(v) = \operatorname{sgn}(\sigma) \cdot v$, for all $\sigma \in S_3$ and $v \in V$.

Example 28.4 (Standard representation)**.** The *standard representation* of S^3 on $V \cong \mathbb{C}^2$ is the representation that permutes basis elements, on the subset of $(a_1, a_2, a_3) \in \mathbb{C}^3$ such that $a_1 + a_2 + a_3 = 0$.

Note that we might consider the permuation representation of S^3 on $\mathbb{C}^3$ directly, but this has an invariant subspace given by triples (a_1, a_2, a_3) such that $a_1 = a_2 = a_3$. Thus, this representation is not irreducible; it is a direct sum of the standard representation and the trivial representation of S_3.

Proposition 28.5. *U, U', V are the only irreducible representations of S_3.*

Proof. Suppose that W is any representation of S_3, and let $\tau \in A_3 \subset S_3$ be a 3-cycle. Then, we can find a basis $v_1, \dots, v_n$ for W consisting of eigenvectors of τ, meaning that

$$W = \langle v_1, \dots, v_n \rangle : \tau(v_i) = \omega^{a_i} v_i,$$

where $\omega = e^{2\pi i/3}$ is a principal third root of unity.

Now, say that $\sigma \in S_3$ is a transposition, so that σ and τ generate S_3 with the relation $\sigma\tau\sigma^{-1} = \tau^2$. We would like to know that σ does to v_i. Observe that if $\tau(v_i) = \omega v_i$,

$$\tau(\sigma(v_i)) = \sigma(\tau^2(v_i)) = \sigma(\omega^2 v_i) = \omega^2 \cdot \sigma(v_i).$$

In conclusion, $\sigma(v_i)$ is again an eigenvector for τ, but with eigenvalue ω^2. We can similarly that σ sends the ω^2-eigenspace to the ω-eigenspace, and the 1-eigenspace to itself.

We now proceed by casework. Let v be any eigenvector for τ with eigenvalue ω, and consider $\langle v, \sigma v \rangle \subset W$. If this is an invariant subspace, then it is congruent to the standard representation V. Otherwise, if $\sigma v = \pm v$, then $(\sigma\tau)^2 v = \omega^2 v$, which is a contradiction.

Finally, if $\tau v = v$, then we have two cases. If σv is a multiple of v, then $\langle v \rangle$ is invariant and either U or U'. Otherwise, σv is linearly independent from v, so $\langle v + \sigma v \rangle$ is invariant and congruent to U. □

Now, suppose that W is any representation of S_3. Then, we know that

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

for some a, b, c. We might ask how to determine a, b, and c. To do this, we consider the dimensions of various eigenspaces of group elements τ and σ. These are determined by the number of eigenvalues of each in U, U', and V, so the dimensions satisfy:

- dimension of the 1-eigenspace of τ: $a + b$.
- dimension of the ω-eigenspace τ: c.
- dimension of the 1-eigenspace of σ: $a + c$.
- dimension of the -1-eigenspace of σ: $b + c$.

Note. In this case, it is enough to consider the eigenvalues of only τ and σ not because they generate S_3, but because they give us one representative for each conjugacy class (which maps to similar matrices).

For an example of applying this, we might ask which irreducible representations of S_3 appear in $V \otimes V$. Consider the basis for V consisting of eigenvectors e_1, e_2 for τ, with eigenvalues ω and ω^2. Then, the eigenvectors for $\tau : V \otimes V \to V \otimes V$ are precisely $e_i \otimes e_j$ for all $i, j \in \{1, 2\}$, so the eigenvalues are ω^2, 1, 1, ω. Similarly, σ acts on $V \otimes V$ with eigenvalues 1, 1, -1, -1. Thus, we can verify that $V \otimes V \cong U \oplus U' \oplus V$.

Exercise 28.1. Write $\operatorname{Sym}^2 V$ and $\operatorname{Sym}^4 V$ as a direct sum of irreducible representations.

29 November 13

Today we recap the representations of S_3, and we introduce character theory.

29.1 Theory of Characters

We begin with some motivation for characters. Suppose a group G acts on a complex vector space V. For each $g \in G$, there is a collection of eigenvalues of the corresponding linear operator, which is an unordered set of n values. Furthermore, there is a bijection between unordered n-tuples of $z_i \in \mathbb{C}$, and monic polynomials of degree n in $\mathbb{C}[x]$, given by the polynomial with those roots $\prod(z - z_i)$. Finally, there is a correspondence between monic polynomials and their coefficient sequence, which is an ordered n-tuple of $a_i \in \mathbb{C}$ given by

$$\begin{aligned} a_1 &= -(z_1 + z_2 + \cdots + z_n), \\ a_2 &= \sum_{i<j} z_i z_j, \\ &\vdots \\ a_n &= (-1)^n \prod_{i=1}^{n} z_i. \end{aligned}$$

To put this in context, take the multivariate polynomial ring $\mathbb{C}[z_1, \ldots, z_n]$, which S_n acts on by permuting the variables.

Definition 29.1 (Symmetric polynomials)**.** The subring $\mathbb{C}[z_1, \ldots, z_n]^{S_n}$ fixed by permuation of variables is called the *symmetric polynomials* of degree n, and it is generated by the *elementary symmetric polynomials* $a_1, a_2, \ldots, a_n$.

It turns out, however, that elementary symmetric polynomials are not the only set that generate the symmetric polynomials.

Proposition 29.1 (Newton's identities)**.** *Let the power sums of degree n be*

$$\begin{aligned} b_1 &= z_1 + \cdots + z_n, \\ b_2 &= z_1^2 + \cdots + z_n^2, \\ &\vdots \end{aligned}$$

Then, the set $\{b_1, b_2, \ldots, b_n\}$ also span $\mathbb{C}[z_1, \ldots, z_n]^{S_n}$.

Proof. We can verify the identities

$$\begin{aligned} e_1 &= p_1, \\ 2e_2 &= e_1 p_1 - p_2, \\ 3e_3 &= e_2 p_1 - e_1 p_2 + p_3. \end{aligned}$$

This pattern continuous, so the first n power sums generate the elementary symmetric polynomials. □

Our goal with characters is to communicate information about the eigenvalues of $g : V \to V$. A naive way to do this is by transmitting the elementary symmetric polynomials in those eigenvectors, but this is inefficient. Instead, we choose to communicate the *sum* of the eigenvalues for each g, which motivates the following definition.

Definition 29.2 (Character of a representation)**.** The *character* of a representation V of a group G is a function $\chi_V : G \to \mathbb{C}$ given by

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

For a given g, this function determines all the power sums of eigenvalues of g given by $\chi_V(g), \chi_V(g^2), \chi_V(g^3)$, etc., and hence all the eigenvalues of g.

To get a feeling for characters of representations, they satisfy (or don't satisfy) the following properties.

- χ_V is not necessarily a homomorphism.
- It is a class function: constant on conjugacy classes, as the trace of similar matrices are equal.
- $\chi_V : G \to \mathbb{C}$ determines the eigenvalues of each $g : V \to V$.
- To be shown later: χ_V determines V, which will allow us to prove that there are a finite number of irreducible representations of a finite group, as well as classify these representations.

Let's look at some specific examples of characters.

Example 29.1 (Characters of constructions)**.** For any representations V, W:

- $\chi_V(e) = \operatorname{tr} I = \dim V$.
- $\chi_{V \oplus W} = \chi_V + \chi_W$.
- $\chi_{V \otimes W} = \chi_V \chi_W$.
- $\chi_{V^*} = \overline{\chi_V}$.
- $\chi_{\operatorname{Hom}(V,W)} = \overline{\chi_V} \chi_W$.

The third of these formulas arises from the fact that the eigenvectors of $g_{V \otimes W}$ are of the form $v_i \otimes w_j$, for eigenvectors v_i of g_V and w_j of g_W. The fourth formula comes from the fact that $g_{V^*} = {}^t g^{-1}$, so the eigenvalues z_i of g_V become their multiplicative inverses z_i^{-1}. However, since all elements $g \in G$ have finite order, their eigenvalues must have modulus 1 (roots of unity), so $z_i^{-1} = \overline{z_i}$, which is additive.

30 November 15

Today we introduce a couple of basic definitions, then continue our discussion of characters.

30.1 Permutation Representations

If G acts on a set S, then we can form a vector space V with one basis element for each element of the set. This provides a link between group actions and representations.

Definition 30.1 (Permutation representation)**.** Given a group G acting on a set S, construct a vector space V with basis $\{e_s\}_{s \in S}$. Then, the *permutation representation* of G acts on V by permuting the corresponding basis vectors.

An important action of any group is left multiplication over itself as a set.

Definition 30.2 (Regular representation)**.** Given any group G, the action of G on itself has a corresponding permutation representation called the *regular representation* of G. Because group elements are invertible, this is also a faithful representation.

30.2 More on Character Theory

We talked last week about how to find characters of various constructions on representations, which all had nice formulas. Here we present a slightly more interesting example.

Example 30.1 (Character of the exterior square)**.** Suppose we have a representation V of a group G, and consider $\bigwedge^2 V$. If V has a basis $v_1, \dots, v_n$ of eigenvectors for g with eigenvalues $\alpha_1, \dots, \alpha_n$, then a basis of eigenvectors for $\bigwedge^2 V$ is given by $\{v_i \wedge v_j\}$ for $1 \le i < j \le n$. Then, the character of the exterior square is

$$\chi_{\bigwedge^2 V}(g) = \sum_{1 \le i < j \le n} \alpha_i \alpha_j = \frac{\left(\sum_i \alpha_i\right)^2 - \sum_i \alpha_i^2}{2} = \frac{\chi_V(g)^2 - \chi_V(g^2)}{2}.$$

We can also do similar calculations for the characters of the symmetric powers. Now, suppose that G acts on the set S, and take the permutation representation V of G. Since the trace of a matrix is the sum of the diagonal entries, this is the number of fixed points of a permutation, so

$$\chi_V(g) = \#(\text{elements fixed by } g) = |S^g|.$$

Example 30.2 (Character table for S_3)**.** We have the following character table (with one representative for each conjugacy class) for S_3:

	e	(12)	(123)
χ_U	1	1	1
$\chi_{U'}$	1	-1	1
χ_V	2	0	-1
χ_W	3	1	0

Here, W is the permutation representation of S_3 acting on a 3-element set, and observe that since $W = U \oplus V$, the two rows for χ_U and χ_V add up to χ_W.

The interesting observation here is that the rows of this character table are independent. If Z is any representation of S_3 given by $U^{\oplus a} \oplus U'^{\oplus b} \oplus V^{\oplus c}$, then

$$\chi_Z = a(1,1,1) + b(1,-1,1) + c(2,0,-1).$$

Thus, by being able to compute the characters (or in general, the eigenvalues of each conjugacy class), we can decompose any representation of a group into its irreducible parts.

Now, we can start analyzing certain projections.

Proposition 30.1 (Projection formula)**.** *Consider any finite group G with irreducible representations $V_1, \dots, V_k$. If V is any representation of G, then*

$$V = V_1^{\oplus a_1} \oplus \cdots \oplus V_k^{\oplus a_k}.$$

Without loss of generality, let V_1 be the trivial one-dimensional representation. This satisfies

$$V_1^{\oplus a_1} = V^G = \{v \in V \mid \forall g \in G : gv = v\}.$$

Furthermore, if we define the idempotent averaging map $\phi : V \to V^G$ given by

$$\phi(v) = \frac{1}{|G|} \sum_{g \in G} gv,$$

then we can express the dimension of the trivial representation by the formula

$$a_1 = \dim V^G = \operatorname{tr}(\phi) = \frac{1}{|G|} \sum_{g \in G} \chi_V(g).$$

Proof. Observe that ϕ is a homomorphism of representations because

$$\phi(hv) = \frac{1}{|G|} \sum_{g \in G} ghv = \frac{1}{|G|} \sum_{g \in G} gv = \phi(v),$$

$$h\phi(v) = \frac{1}{|G|} \sum_{g \in G} hgv = \frac{1}{|G|} \sum_{g \in G} gv = \phi(v).$$

This also means that the image of ϕ is invariant under actions by all elements in G, so it is a subset of V^G. The idempotency $\phi^2 = \phi$ also follows, showing that ϕ is a projection map. As a consequence, this gives us the direct sum decomposition $V = V^G \oplus \ker(\phi)$, and the result follows. □

Corollary 30.1.1. *Given representations V and W of a group G, the number of linearly independent homomorphisms of representations from V to W is*

$$\dim \mathrm{Hom}_G(V,W) = \dim \mathrm{Hom}(V,W)^G = \frac{1}{|G|}\sum_{g\in G}\overline{\chi_V(g)}\chi_W(g).$$

In other words, if $\mathcal{C}$ is the set of conjugacy classes in G, then define the Hermitian inner product H on $\mathbb{C}^{\mathcal{C}}$, which is the set of class functions on G, by

$$H(\alpha,\beta) = \frac{1}{|G|}\sum_{g\in G}\overline{\alpha(g)}\beta(g).$$

(Note that this is the opposite sign convention of our definition of a sesquilinear form from before, but let's not worry about that.) Then,

$$\dim \mathrm{Hom}_G(V,W) = H(\chi_V,\chi_W).$$

This corollary allows us to perform the following magic trick.

Proposition 30.2 (Irreducible characters are orthonormal)**.** *If $V_1,\dots,V_k$ are irreducible representations of G, then*

$$H(\chi_{V_i},\chi_{V_j}) = \begin{cases} 0 & i\neq j \\ 1 & i=j \end{cases}.$$

Proof. This follows directly from Schur's lemma. This means that if $V\neq W$, then $\mathrm{Hom}_G(V,W)=0$, and otherwise, $\mathrm{Hom}_G(V,V)=\mathbb{C}\cdot\mathrm{id}$. □

Corollary 30.2.1. *The characters χ_{V_i} are linearly independent in $C^{\mathcal{C}}$, so there number of irreducible representations is at most the number of conjugacy classes in G (we will see later that this is an equality).*

Corollary 30.2.2. *Any representation V of G is completely determined by χ_V. In particular, note that there is some irreducible decomposition $V=\bigoplus_i V_i^{\oplus a_i}$. Then, by the properties of characters,*

$$\chi_V = \sum_i a_i\chi_{V_i}.$$

Applying Prop. 30.2 to this equation, we have

$$H(\chi_{V_i},\chi_V) = a_i.$$

Corollary 30.2.3. *A representation V of G is irreducible if and only if*

$$H(\chi_V,\chi_V) = 1.$$

In general, we have that

$$H(\chi_V,\chi_V) = \sum_i a_i^2.$$

Example 30.3 (Character table of S_4)**.** We can analyze the characters of S_4. This has 5 conjugacy classes, with representatives e, (12), (123), (1234), and (12)(34). The irreducible representations are U (trivial), U' (alternating), V (standard), $V' = V \otimes U'$, and one more. Also, let Z be the permutation representation. The character table is as follows:

	e	(12)	(123)	(1234)	(12)(34)
χ_U	1	1	1	1	1
$\chi_{U'}$	1	-1	1	-1	1
χ_V	3	1	0	-1	-1
$\chi_{V\otimes U'}$	3	-1	0	1	-1
χ_W	2	0	-1	0	2
χ_Z	4	2	1	0	0

31 November 18

Today we continue discussing character theory.

31.1 More on Character Theory (cont.)

We first look at an application of the theory we developed last Friday. For any group G, recall that it has a regular representation R given by taking the action of left multiplication on a set of basis vectors, one for each element. This is not an irreducible representation, so it's interesting to consider how it might be decomposed.

Proposition 31.1 (Regular representation decomposition)**.** *If R is the regular representation of a group G and $V_1, \dots, V_k$ are the irreducible representations, then suppose that*

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

Then, $a_i = \dim V_i$. In plain English, each irreducible representation appears in the regular representation a number of times equal to its dimension.

Proof. We apply Corollary 30.2.2, which yields

$$\begin{aligned} a_i &= H(\chi_R, \chi_{V_i}) \\ &= \frac{1}{|G|} \sum_{g \in G} \chi_R(g) \cdot \chi_{V_i}(g) \\ &= \chi_{V_i}(e) \\ &= \dim V_i. \end{aligned}$$

□

Corollary 31.1.1. *For any finite group G, if all the irreducible representations of G are $V_1, \dots, V_k$, then*

$$|G| = \sum_{i=1}^{k} (\dim V_i)^2.$$

This gives us a way to determine when we have found all irreducible representations of a given group. This could be useful, for example, in finding the character table of S_4.

31.2 Applications of Characters

Example 31.1 (Plethysm)**.** In the representation theory of S_4, we might ask what is $V \otimes V$ as a sum of irreducible representations. Note that

$$\chi_{V \otimes V} = \chi_V^2 = (9, 1, 0, 1, 1).$$

Then, the inner product of this character with itself is

$$H(\chi_{V\otimes V}, \chi_{V\otimes V}) = \frac{1}{24}(81 + 6 + 0 + 6 + 3) = 4.$$

Each of the resulting irreducible representations then must be repeated 1 or 2 times. However, if an irreducible representation were repeated twice, this is impossible because $\chi_{V\otimes V}$ is not double of any row in the character table. Using the table, we find that

$$V \otimes V \cong U \oplus V' \oplus V \oplus W.$$

Example 31.2 (Symmetries of a Cube)**.** Consider the action of S_4 on the six faces of a cube, and let the permutation representation of this be Z. We wish to find χ_Z.

To do this, we compute the value of the character χ_Z at a representative of each conjugacy class, by counting the number of faces fixed by each permutation. First, $\chi_Z(e) = 6$. Also,

$$\begin{aligned}\chi_Z((12)) &= 0,\\ \chi_Z((123)) &= 0,\\ \chi_Z((1234)) &= 2,\\ \chi_Z((12)(34)) &= 2.\end{aligned}$$

Then, $H(\chi_Z, \chi_Z) = \frac{1}{24}(36 + 4 \cdot 6 + 4 \cdot 3) = 3$, so Z is the direct sum of three irreducible representations. In particular,

$$Z \cong U \oplus V' \oplus W.$$

For intuition about this: U is the sum of all faces, while V' is the subspace of Z spanned by differences of opposite faces. W is everything else.

32 November 20

Today we finish character theory, discussing A_4, S_5, and A_5. At the end of the semester, we will move from representations in complex vector spaces to those in real vector spaces.

32.1 Representations of the Alternating Group

First, we examine the conjugacy classes of A_4. Each of the three even conjugacy classes in S_4 maps to A_4; however, the class represented by (123) in S_4 splits into (123) and (124) in A_4. Then, the conjugacy classes of A_4 are e, (123), (124), and (12)(34).

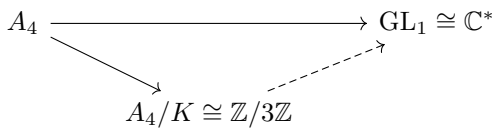
	e	(123)	(124)	(12)(34)
χ_U	1	1	1	1

We can then start drawing a character table for A_4, as above. Clearly, the trivial representation U is an irreducible representation of A_4, so we add it as the first row. In addition, any of the representations of S_4 is also a representation of A_4 by restricting it to the elements of A_4, although not necessarily irreducible. We can then expand our table as below.

	e	(123)	(124)	(12)(34)
χ_U	1	1	1	1
χ_V	3	0	0	-1
χ_{W_1}	1			
χ_{W_2}	1			
χ_W	2	-1	-1	2

Observe that $H(\chi_V, \chi_V) = \frac{1}{12}(9 \cdot 1 + 1 \cdot 3) = 1$, so it is irreducible. Similarly, we can check that $H(\chi_W, \chi_W) = \frac{1}{12}(4 \cdot 1 + 1 \cdot 4 + 1 \cdot 4 + 4 \cdot 3) = 2$. Then, W is the sum of two distinct irreducible representations $W_1 \oplus W_2$, and if we check that $H(\chi_W, \chi_U) = H(\chi_W, \chi_V) = 0$, this means that W_1 and W_2 are the remaining two irreducible representations.

Now, we find W_1 and W_2. Since both are one-dimensional, the group elements are members of $\mathrm{GL}_1 \cong \mathbb{C}^*$, which is an abelian group. This implies that all elements in the commutator subgroup $K = \{e, (12)(34), (13)(24), (14)(23)\}$ of A_4 must map to the identity in $\mathbb{C}^*$. In particular, we can pull back the representation homomorphism



The only maps from A_4/K to $\mathbb{C}^*$ are those mapping the elements to third roots of unity. These are therefore the last two irreducible characters of A_4.

Example 32.1 (Character Table of A_4)**.** The alternating group A_4 on four elements has four irreducible representations, with the following character table.

	e	(123)	(124)	$(12)(34)$
χ_U	1	1	1	1
χ_V	3	0	0	-1
χ_{W_1}	1	ω	ω^2	1
χ_{W_2}	1	ω^2	ω	1
χ_W	2	-1	-1	2

Note. We have seen in our analysis of the representation theory of symmetric groups that all characters of S_n have had integer values. In general, this is a special property of symmetric groups and not the case for general finite groups. The character table of A_4 shows that in general, characters can be arbitrary complex numbers.

Note. We showed earlier that $\chi_{V^*} = \overline{\chi_V}$. As a corollary, a representation V is isomorphic to its dual space if and only if its character is real. Also, in the representation theory of A_4, $W_1^* \cong W_2$.

Another way to see the symmetry between W_1 and W_2 in the above table is to notice that there is an *outer automorphism* in A_4 that takes (123) to (124), which is determined by restricting conjugation by (34), which is an inner automorphism in S_4, to the elements of A_4.

32.2 More on Projection Formulas

Previously, we observed that given a representation V of a finite group G, the action of an element $g \in G$ does not in general induce a homomorphism of representations. However,

$$\phi = \frac{1}{|G|} \sum_{g \in G} g \quad \in \quad \mathrm{Hom}(V, V)$$

is a homomorphism of representations. It is an interesting question to ask what other linear combinations of $g \in G$ are homomorphisms of representations.

Proposition 32.1. *Let $\alpha : G \to \mathbb{C}$ be any function on G, and let V be a representation of G. Then, define a linear map $\phi_{\alpha,V} : V \to V$ by*

$$\phi_{\alpha,V} = \sum_{g \in G} \alpha(g) \cdot g.$$

Then, $\phi_{\alpha,V}$ is a (G-linear) homomorphism of representations for all V, if and only if α is a class function.

Proof. We prove the "if" direction of this proposition. Suppose that α is a class function, and fix some representation V. Then, we wish to show that ϕ_α is G-linear, i.e., for any $h \in G$ and $v \in V$,

$$h\phi_\alpha(v) = \phi_\alpha(hv).$$

This can be shown with some algebra as follows:

$$\begin{aligned}
\phi_\alpha(hv) &= \sum_{g\in G} \alpha(g)\cdot g(hv) \\
&= \sum_{g\in G} \alpha(hgh^{-1})\cdot (hgh^{-1})(hv) \\
&= \sum_{g\in G} \alpha(g)\cdot hgv \\
&= h\left(\sum_{g\in G} \alpha(g)\cdot gv\right) \\
&= h(\phi_\alpha(v)).
\end{aligned}$$

□

Finally, we are ready to prove our big result about the number of irreducible representations.

Proposition 32.2. *If $V_1, \dots, V_k$ are the irreducible representations of G, then the characters $\{\chi_{V_i}\}$ span the space $\mathbb{C}^{\mathcal{C}}$ of class functions, i.e., k is equal to the number of conjugacy classes.*

Proof. Assume for the sake of contradiction that we have some class function α not in the span of our k characters. We want to show that if α is a class function and $H(\alpha, \chi_{V_i}) = 0$ for all i, then $\alpha = 0$.

Let $V = V_i$ be any irreducible representation, and look at $\phi_\alpha : V \to V$. By Schur's lemma, any endomorphism of an irreducible representation is simply scalar multiplication by a constant, so

$$\phi_{\alpha,V} = \sum_{g\in G} \alpha(g)\cdot g = \lambda \cdot \mathrm{Id}_V\,.$$

In particular, note that

$$\begin{aligned}
\lambda &= \frac{1}{n}\cdot \mathrm{tr}(\phi_\alpha, v) \\
&= \frac{1}{n}\sum_{g\in G} \alpha(g)\cdot \chi_V(g) \\
&= \frac{1}{n}\sum_{g\in G} \alpha(g)\cdot \overline{\chi_{V^*}(g)} \\
&= \frac{|G|}{n}\cdot H(\chi_{V^*}, \alpha).
\end{aligned}$$

However, if V is an irreducible representation then its dual V^* is also irreducible, so $H(\chi_{V^*}, \alpha) = 0$, and thus $\lambda = 0$.

Now, consider an arbitrary representation $V = \bigoplus_i V_i^{\oplus a_i}$. Since V is the direct sum of irreducible representations, the previous fact implies that $\phi_{\alpha,V} = 0$ for all representations V. In particular, if R is the regular representation then $\phi_{\alpha,R} = 0$, and the result follows. □

32.3 Representations of S_5

In this section, we use the results we just proved to analyze the representations of S_5 and A_5. We start off with the character table for S_5, and we partially fill it in below.

	1	10	20	30	24	15	20
	e	(12)	(123)	(1234)	(12345)	(12)(34)	(12)(345)
χ_U	1	1	1	1	1	1	1
$\chi_{U'}$	1	−1	1	−1	1	1	−1
χ_V	4	2	1	0	−1	0	1
$\chi_{V\otimes U'} = \chi_{V'}$	4	2	1	0	−1	0	1

Here, U is the trivial representation, U' is the alternating representation, and V is the standard representation. To find more irreducible representations of S_5, we examine $V \otimes V$, which is broken down as

$$V \otimes V = \operatorname{Sym}^2 V \oplus \bigwedge^2 V.$$

In particular, we can compute the character of $\bigwedge^2 V$ using the formula

$$\chi_{\bigwedge^2 V}(g) = \frac{\chi_V(g)^2 - \chi_V(g^2)}{2}.$$

This tells us that $\chi_{\bigwedge^2 V} = (6, 0, 0, 0, 1, 2, 0)$, which is irreducible. Next, we look at $\operatorname{Sym}^2 V$, whose character is related by the formula

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

This tells us that $\chi_{\operatorname{Sym}^2 V} = (10, 4, 1, 0, 0, 2, 1)$. We can check that the inner product of this character with itself is 3, so it is reducible and the sum of three irreducible representations. Also, observe that

$$H(\chi_{\operatorname{Sym}^2 V}, \chi_U) = 1 \implies U \subset \operatorname{Sym}^2 V,$$
$$H(\chi_{\operatorname{Sym}^2 V}, \chi_V) = 1 \implies V \subset \operatorname{Sym}^2 V.$$

Thus, $\operatorname{Sym}^2 V = U \oplus V \oplus W$, for some remaining representation W. Adding in W and W' finally allows us to complete our character table.

Example 32.2 (Character Table of S_5)**.** The symmetric group S_5 on five elements has seven irreducible representations, with the following character table.

	1	10	20	30	24	15	20
	e	(12)	(123)	(1234)	(12345)	(12)(34)	(12)(345)
χ_U	1	1	1	1	1	1	1
$\chi_{U'}$	1	−1	1	−1	1	1	−1
χ_V	4	2	1	0	−1	0	1
$\chi_{V\otimes U'} = \chi_{V'}$	4	2	1	0	−1	0	1
$\chi_{\bigwedge^2 V}$	6	0	0	0	1	2	0
χ_W	5	1	−1	−1	0	1	1
$\chi_{W\otimes U'} = \chi_{W'}$	5	−1	−1	1	0	1	−1

Note. The general approach used here, of analyzing characters of representations in the tensor algebra of V, will always work in general. This is a consequence of Problem 2.37 in Fulton-Harris, which shows that if V is any faithful representation, then all irreducible representations appear in some tensor power $V^{\otimes n}$ of V. It is not clear, however, how many tensor powers you will need to take before all the irreducible representations show up.

Exercise 32.1. Use this character table to show that S_5 is not the symmetry group of any three-dimensional object in $\mathbb{R}^3$.

33 November 22

Today we review the character tables of S_5 and A_5, then talk about induced representations and the representation ring.

33.1 Representations of A_5

The conjugacy classes of A_5 are e, (123), (12)(34), (12345), and (12354). We start by carrying over the irreducible representations of S_5 into A_5, giving us the following table.

	1	20	15	12	12
	e	(123)	(12)(34)	(12345)	(12354)
χ_U	1	1	1	1	1
χ_V	4	1	0	-1	-1
χ_W	5	-1	1	0	0
$\chi_{\bigwedge^2 V}$	6	0	-2	1	1

However, representations that are irreducible in S_5 may not be irreducible when we restrict them to A_5. This tells us that

$$H(\chi_V, \chi_V) = \frac{1}{60}(16 + 20 + 12 + 12) = 1,$$
$$H(\chi_W, \chi_W) = \frac{1}{60}(25 + 20 + 15) = 1,$$
$$H(\chi_{\bigwedge^2 V}, \chi_{\bigwedge^2 V}) = \frac{1}{60}(36 + 60 + 12 + 12) = 2.$$

Thus, V and W are irreducible representations, and $\bigwedge^2 V$ is the sum of the last two irreducible representations. Note that there is an outer automorphism of A_5 that swaps the conjugacy classes (12345) and (12354), so the remaining two irreducible representations must be of the form $\bigwedge^2 V = Z \oplus Z'$, conjugate under this automorphism, with characters shown below.

	1	20	15	12	12
	e	(123)	(12)(34)	(12345)	(12354)
χ_U	1	1	1	1	1
χ_V	4	1	0	-1	-1
χ_W	5	-1	1	0	0
χ_Z	3	0	-1	α	β
$\chi_{Z'}$	3	0	-1	β	α
$\chi_{\bigwedge^2 V}$	6	0	-2	1	1

We can use orthogonality to solve for the remaining values α and β, from which we see that they are equal to $(1 \pm \sqrt{5})/2$. This completes the table.

Example 33.1 (Character Table of A_5)**.** The alternating group A_5 on five elements has five irreducible representations, with the following character table.

	1	20	15	12	12
	e	(123)	$(12)(34)$	(12345)	(12354)
χ_U	1	1	1	1	1
χ_V	4	1	0	-1	-1
χ_W	5	-1	1	0	0
χ_Z	3	0	-1	$(1+\sqrt{5})/2$	$(1-\sqrt{5})/2$
$\chi_{Z'}$	3	0	-1	$(1-\sqrt{5})/2$	$(1+\sqrt{5})/2$

33.2 Induced Representations

Our motivation for this section is to describe representations of an arbitrary group by looking at representations of its subgroups. Suppose we have a group G and subgroup $H \subset G$. Then, we have a map from representations of G to representations of H, by taking the restriction

$$\rho : G \to \mathrm{GL}(V) \quad \longmapsto \quad \rho|_H : H \to \mathrm{GL}(V).$$

This is what we used to find the representations of the alternating group using the symmetric group. However, we'd like to go the other way, to find a natural map from representations of H to representations of G (smaller to larger).

Suppose that V is a representation of G, and suppose that $W \subset V$ is a subspace invariant under H (and thus an H-subrepresentation). Then, $\sigma W = gW$ depends only on the coset $\sigma = gH$ of H.

Definition 33.1 (Induced representation)**.** If V is a representation of a finite group G, H is a subgroup of G, and $W \subset V$ is a subspace invariant under H, then V is *induced from* W if

$$V = \bigoplus_{\sigma \in G/H} \sigma W.$$

Example 33.2 (Induced permutation representation)**.** Let W be the trivial representation of H and V be the permutation representation of G corresponding to the action of G on G/H. That is,

$$V = \bigoplus_{\sigma \in G/H} \langle e_\sigma \rangle.$$

Then, V is induced from W.

Proposition 33.1 (Induced representations exist and are unique)**.** *Consider any finite group G and subgroup $H \subset G$. If W is a representation of H, then there exists a unique representation V of G such that V is induced from W.*

Proof. We will prove uniqueness, from which a construction will arise. Choose one element g_σ from each coset. if V is induced from W, then

$$V = \bigoplus_{\sigma \in G/H} g_\sigma W.$$

Given any $g \in G$, we need to determine how g acts on V. Then, let $v \in V$ be any vector. We can write

$$v = \sum_{\sigma \in G/H} g_\sigma w_\sigma.$$

This means by linearity that

$$g(v) = \sum_{\sigma \in G/H} g(g_\sigma w_\sigma) = (g g_\sigma)(w_\sigma).$$

However, observe that $g g_\sigma$ will simply be mapped to a different, unique coset $\tau \in G/H$, so we can write $g g_\sigma = g_\tau h_\tau$ for some $h_\tau \in H$. It follows that

$$g(v) = \sum_{\sigma \in G/H} g_\tau (h_\tau w_\sigma).$$

This is uniquely determined by h_τ which is already defined, as well as g_τ which we know, so we have extended this to a unique action over all $g \in G$. $\square$

34 November 25

This is the second-to-last lecture. Today we discuss the representation ring and induced representations.

34.1 More on Projection Formulas (cont.)

Recall from Prop. 32.1 that for any class function $\alpha \in \mathbb{C}^{\mathcal{C}}$ and representation V, there exists an endomorphism of representations on V defined by

$$\phi_{\alpha,V} = \frac{1}{|G|} \sum_{g \in G} \alpha(g) \cdot g.$$

In this case, we are allowed to use any class function, so consider some irreducible representation V_i, and let $\alpha = \chi_{V_i^*}$. Also, suppose that $V = V_j$ is an irreducible representation, and consider the map

$$\phi_{\chi_{V_i^*},V_j} : V_j \to V_j.$$

Furthermore, by Schur's lemma, we know that this homomorphism of representations must be a scalar multiplication, $\lambda \cdot \mathrm{Id}_{V_j}$. To find λ, we compute the trace of the operator, which is given by

$$\begin{aligned}
\lambda &= \frac{1}{\dim V_j} \operatorname{tr}(\phi_{\chi_{V_i^*},V_j}) \\
&= \frac{1}{\dim V_j} \cdot \frac{1}{|G|} \sum_{g \in G} \overline{\chi_{V_i}(g)} \chi_{V_j}(g) \\
&= \frac{1}{\dim V_j} \cdot \frac{1}{|G|} H(\chi_{V_i}, \chi_{V_j}).
\end{aligned}$$

Thus, this map is a nonzero scalar multiplication precisely when $i = j$, and otherwise, it is the zero map. Then, it follows that for any irreducible representation V_i and representation V, the map $\phi_{\chi_{V_i^*},V}$ is a projection homomorphism from V to the component $V_i^{\oplus a_i}$ in its direct sum decomposition.

Philosophically, this tells us that given any explicit representation of a finite group, we can find a projection onto any of its irreducible representations by taking this sum of group elements weighted by the character of $\chi_{V_i^*}$.

34.2 Representation Rings

Observe that the set S of representations of a finite group G (up to isomorphism) almost has the structure of a ring under the direct sum and tensor product operations. This satisfies all the ring axioms except the existence of additive inverses, as we cannot take "negative sums" of irreducible representations. In other words, with respect to $\oplus$, this is an commutative monoid, rather than a group. We introduce a construction that allows us to form an abelian group from any commutative monoid.

Definition 34.1 (Grothendieck group)**.** Given an commutative monoid S, we can form a group with the following construction, in two steps.

1. Let G_0 be the free abelian group generated by S. In other words,
$$G_0 = \left\{ \sum_{i=1}^{n} a_i S_i \mid s_i \in S, a_i \in Z \right\}.$$
2. Let $H \subset G_0$ be a subgroup generated by elements of the form
$$\{\alpha + \beta - \gamma \mid \gamma = \alpha + \beta\},$$
where $\alpha, \beta, \gamma \in S$. Then, we take the quotient group $G = G_0/H$, and we call G the *Grothendieck group* of S.

An intuition for this construction is that we are simply "adding in" the inverse elements of each element $g \in S$, then providing a suitable relation for which the group operation is defined.

Example 34.1. The Grothendieck group of $\mathbb{N}$ is $\mathbb{Z}$.

Example 34.2. The Grothendieck group of $\mathbb{N}^k$ is $\mathbb{Z}^k$.

Definition 34.2 (Representation ring)**.** Given a finite group G, the *representation ring* $R(G)$ is defined to be the the Grothendieck group of the set of representations of G. Because the representations of G are given by
$$V \cong \bigoplus_{i=1}^{k} V_i^{\oplus a_i}, \qquad a_i \in \mathbb{N},$$
the representation ring is isomorphic to $\mathbb{Z}^k$ and given by
$$R(G) = \left\{ \bigoplus_{i=1}^{k} V_i^{\oplus a_i} \right\}, \qquad a_i \in \mathbb{Z}.$$
Elements of the representation ring are called *virtual representations* of V.

Proposition 34.1. *The tensor product $\otimes$ gives $R(G)$, originally an abelian group, the additional structure of a commutative ring.*

Proof. Recall from tensor product identities that
$$V \otimes (U \oplus W) = (V \otimes U) \oplus (V \otimes W).$$
This means that tensor products distribute over direct sums. We can then define the product $R(G) \times R(G) \to R(G)$ given by
$$\left(\sum_{i=1}^{k} a_i V_i \right) \left(\sum_{j=1}^{k} b_j V_j \right) = \sum_{1 \le i,j \le k} a_i b_j (V_i \otimes V_j).$$
This construction satisfies all the axioms of a commutative ring. □

In these terms, the character function gives an inclusion map from $R(G)$ to class functions on G. This is shown in the diagram below.

$$\begin{array}{ccc} R(G) & \hookrightarrow & \mathbb{C}^{\mathcal{C}} \\ \updownarrow & & \updownarrow \\ \mathbb{Z}^k & & \mathbb{C}^k \end{array}$$

In particular, the virtual representations $R(G)$ form a *lattice* in the complex space of all class functions on G. Within this lattice, the set of actual representations of G forms a *linear cone*. The focus of representation theory is to describe the lattice $R(G)$, as well as characterize the cone of representations.

34.3 Induced Representations (cont.)

Recall that our basic setup is a finite group G with subgroup $H \subset G$, with two operations. First, given a representation of the larger group G, we can easily restrict this to a representation of H, which extends by linearity to a ring homomorphism $R(G) \to R(H)$.

Also, given a representation W of H, there exists a unique representation V of G with subspace $W \subset V$ invariant under H such that $V = \bigoplus_{\sigma \in G/H} \sigma W$, called the induced representation. Hence, our two maps are:

- $\text{Res}_H^G : R(G) \to R(H)$, ring homomorphism.
- $\text{Ind}_H^G : R(H) \to R(G)$, *not* a ring homomorphism.

The induced representation map is not a ring homomorphism, which can be shown by a dimension-counting argument. Because $\dim V = |G/H| \cdot \dim W$, it is not true that

$$\text{Ind}_H^G(W \otimes U) = \text{Ind}_H^G(W) \otimes \text{Ind}_H^G(U).$$

However, we can show that induced representations satisfy a basic rule.

Proposition 34.2 (Homomorphisms of rings induce modules)**.** *Given two rings A and B, suppose we have a ring homomorphism $\varphi : A \to B$. Then, φ gives B the structure of an A module.*

Proof. We can check the ring axioms, with the operation of A on B defined by

$$A \times B \to B,$$
$$(a, b) \mapsto \varphi(a) \cdot b.$$

□

The basic rule for induced representations is as follows. Observe that Res_H^G gives $R(H)$ the structure of a $R(G)$-module. Then, $\text{Ind}_H^G : R(H) \to R(G)$ is a module homomorphism between $R(H)$ and $R(G)$, both viewed as modules over $R(G)$ under the restriction map. In other words, if U is a representation of G and W is a representation of H, then

$$U \otimes \text{Ind}_H^G(W) = \text{Ind}_H^G(\text{Res}_H^G(U) \otimes W).$$

35 December 2

This is the last lecture. We wrap up induced representations, briefly discuss real representations, then talk about future math courses after 55a!

35.1 More on Induced Representations

Suppose that U is a representation of G and W is a representation of H, where $H \subset G$ is a subgroup. Then,

$$\mathrm{Hom}_H(W, \mathrm{Res}\, U) = \mathrm{Hom}_G(\mathrm{Ind}\, W, U).$$

In other words, this is saying that any H-linear map $\varphi : W \to U$ extends uniquely to a G-linear map $\mathrm{Ind}(W) \to U$. This is because

$$\mathrm{Ind}(W) = \bigoplus_{\sigma \in G/H} g\sigma W,$$

which means that we can extend φ to

$$g\sigma W \xrightarrow{(g\sigma)^{-1}} W \xrightarrow{\varphi} U \xrightarrow{g\sigma} U.$$

Note. The induced and restricted representations are not inverses of each other, which can be seen by a dimension counting argument. In fact, it can be seen that in general, $\mathrm{Ind}(\mathrm{Res}\, U) = U^{\oplus [G:H]}$.

We can apply this statement as well to irreducible representations, which by Schur's lemma tells us that the number of times W occurs in $\mathrm{Res}(U)$ is equal to the number of times $\mathrm{Ind}(W)$ occurs in U. This has the following implication.

Proposition 35.1 (Frobenius reciprocity)**.** *The following two Hermitian inner products on characters in G and H are equal:*

$$H_G(\chi_{\mathrm{Ind}_H^G W}, \chi_U) = H_H(\chi_W, \chi_{\mathrm{Res}_H^G U}).$$

35.2 Real Representations

By the algebraic closure of $\mathbb{C}$, the representation theory of finite groups over $\mathbb{C}$ is very nice, as we have both complete reducibility and Schur's lemma. When we look at representations of finite groups over $\mathbb{R}$, however, Schur's lemma does not hold.

Example 35.1 (Schur's lemma fails)**.** Consider the action of $\mathbb{Z}/n\mathbb{Z}$ on $\mathbb{R}^2$ by rotation about the origin by an angle of $2\pi\alpha/n$. This is an irreducible representation of $\mathbb{Z}/n\mathbb{Z}$ on $\mathbb{R}^2$. However,

$$\mathrm{Hom}_{\mathbb{Z}/n}(\mathbb{R}^2, \mathbb{R}^2) \neq \mathbb{R}.$$

Instead, we would like to use our knowledge of complex representations to analyze real representations. Let V be a real vector space. Then, we can turn the scalars from real numbers to complex numbers by treating $\mathbb{C}$ as a two-dimensional vector space over $\mathbb{R}$, so the *complexification* $V^{\mathbb{C}} = V \otimes_{\mathbb{R}} \mathbb{C}$ is a representation of G over $\mathbb{C}$. In particular, we have the following diagram.

$$G \to \mathrm{Aut}(V) \cong \mathrm{GL}_n(\mathbb{R}) \hookrightarrow \mathrm{GL}_n(\mathbb{C}) \cong \mathrm{Aut}(V^{\mathbb{C}}).$$

This gives us a map from representations of G on real vector spaces, to representations of G on complex vector spaces.

Definition 35.1 (Real representation)**.** We call a representation of G on a complex vector space V *real* if it arises in this fashion, as the complexification of some real representation.

Our question is then: given a complex representation V of G, when is it real? Immediately, we can see that a necessary condition is that χ_V is real, as all eigenvalues of operators in $\mathrm{GL}_n(\mathbb{R})$ are real numbers. We explore this.

It turns out that the converse is not true; having χ_V be real is not a sufficient condition. Suppose that V is any complex representation of G with χ_V real. Then, $\chi_V = \overline{\chi_V} = \chi_{V^*}$, meaning that $V \cong V^*$ as representations of G.

In the special case that V is irreducible, there exists a unique G-linear map $\varphi : V \to V^*$, meaning that there is a bilinear form $B \in V^* \otimes V^*$ invariant under the action of G. In equation form,

$$(V^* \otimes V^*)^G \longleftrightarrow \mathrm{Hom}_G(V, V^*).$$

Now, notice that $V^* \otimes V^* \cong \mathrm{Sym}^2 V^* \oplus \bigwedge^2 V^*$. Since both $\mathrm{Sym}^2 V^*$ and $\bigwedge^2 V^*$ are natural constructions from V^*, they must each be invariant under the action of G (automorphisms). This means that we can factor B into symmetric and skew-symmetric parts, each of which is invariant under G. However, recall by Schur's lemma that B is unique up to scalar multiplication. This means that B is either wholly symmetric or skew-symmetric.

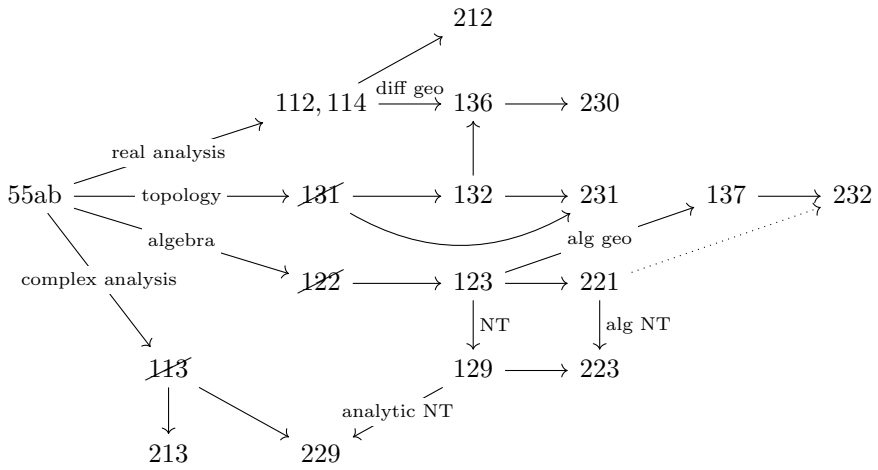
To summarize, given an irreducible representation of G on a complex vector space V, there are 3 possibilities:

- V is complex, χ_V is not real, and $V \ncong V^*$.
- V is real, χ_V is real, and there exists a symmetric bilinear form B invariant under G. Also, V is the complexification $V_0 \otimes_{\mathbb{R}} \mathbb{C}$ of some real vector space V_0 with a G-action.
- V is *quaternionic*, χ_V is real, and there exists a skew-symmetric bilinear form B that is invariant under G.

This demonstrates a common technique for dealing with real vector spaces, by taking their complexification (which may have nicer properties) and attempting to deduce facts about the original real objects.

35.3 What's Next?

That concludes the content of Math 55a! Joe draws for us the following map of math courses at Harvard.



In general, any topic covered by Math 55 completely subsumes any introductory undergraduate course on that topic. The crossed-out items in the diagram above represent courses that will be covered by 55.