Math 122 Notes

Roman Berens

Lecture 1
September 4

Groups:

Definition: A symmetry is a map from an object to itself preserving all relevant structure.

Consider a smiley face in a plane. It has two symmetries: the identity map id and the "flip" map f that rotates it 180 degrees around the vertical axis. We can consider the four possible compositions of the maps:

$$id \circ id = id \qquad f \circ id = f \qquad id \circ f = f \qquad f \circ f = id.$$

What is a group? First we consider the following:

Definition: A semigroup is a set G and an operation $\cdot$ (or mult_G) : $G \times G \to G$ such that this operation is associative, i.e. $(a \cdot b) \cdot c = a \cdot (b \cdot c)\ \forall\ a, b \in G$.
Remark: Composition of functions is always associative.

Definition: A monoid is a s semigroup $(G, \cdot)$ such that there exists an element (1) which is a unit.

Definition: A unit in a semigroup is an element such that $\forall\ x \in G,\ 1 \cdot x = x \cdot 1 = x$.

Lemma: A monoid has at most one unit.
Proof: Assume for the sake of contradiction that 1 and $1'$ are both units. Then $1 = 1 \cdot 1'$ because $1'$ is a unit and $1' = 1' \cdot 1$ because 1 is a unit. Thus $1 = 1'$.

Definition: A group is a monoid such that every element has an inverse.

Definition: An inverse of an element $a \in G$ is an element $b \in G$ such that $a \cdot b = b \cdot a = 1$.

Lemma: An element a in a monoid G has at most one inverse.
Proof: Assume for the sake of contradiction $b, c \in G$ are both inverses of $a \in G$. Then:

$$b \cdot a \cdot c = (b \cdot a) \cdot c = 1 \cdot c = c$$

$$b \cdot a \cdot c = b \cdot (a \cdot c) = b \cdot 1 = b.$$

Thus $b = c$. We usually represent the inverse of a as a^{-1} when the operation is multiplication (or analogous to it) and as $-a$ when the operation is addition.

Summary:

A group is a set G with an operation $\cdot : G \times G \to G$ such that:
1. The operation is associative.
2. There exists a unit.
3. Every element has an inverse.

Comments on Associativity:

Given $x_1, \dots x_n \in G$ (group), define $x_1 \cdot x_n$ inductively as $(x_1 \cdot x_{n-1}) \cdot x_n$, i.e. as $(\cdots((x_1 \cdot x_2) \cdot x_3) \dots x_{n-1}) \cdot x_n$

Lemma:

$$\prod_{i=1}^{k} x_i \cdot \prod_{j=k+1}^{n} x_j = \prod_{i=1}^{n} x_i$$

Proof: By induction.

Examples of Groups:

The Mattress Group is the set of actions one one can perform on a mattress, also known as the Klein Four Group. It consists of the identity 1, a horizontal flip H, a vertical flip V and a spin S. The multiplication table follows. Note that the operation of the column is applied first.

	1	H	V	S
1	1	H	V	S
H	H	1	S	V
V	V	S	1	H
S	S	V	H	1

$(\mathbb{Z}, +)$ is an abelian (commutative) group (i.e. $\forall\ a, b \in G, a \cdot b = b \cdot a$). Its unit is 0.

$(\mathbb{Z}, \cdot)$ is not a group, but it is a monoid with 1 as its unit. The same is true for $(\mathbb{R}, \cdot)$.

$(\mathbb{R} - \{0\}, \cdot)$ is an abelian group with 1 as its unit.

$(\text{Mat}_n(\mathbb{R}), \cdot)$, i.e. the set of $n \times n$ matrices with real elements, is not a group, but it is a monoid with I (as a matrix) as its unit.

because no inverse for all zeros, and other matrices.

$GL_n(\mathbb{R}) = \{A \in \text{Mat}_n(\mathbb{R}) \mid A \text{ is invertible}\}$ is a group known as the general linear group with I (as a linear map) as its unit.

Check: If $A, B \in GL_n(\mathbb{R})$, $(AB) \in GL_n(\mathbb{R})$.

Proof: A and B are both invertible, and $(AB)^{-1} = B^{-1}A^{-1} \in GL_n(\mathbb{R})$

Definition: A subgroup $H < G$ is a subset $H \subset G$ such that:
1. If $a, b \in H$, then $ab \in H$. (Closure under the operation).
2. $1 \in H$
3. If $a \in H$, then $a^{-1} \in H$. (Closure under inversion).

Lecture 2
September 6

Examples of Subgroups:

$(\mathbb{Z},+) < (\mathbb{R},+) \qquad (2\mathbb{Z},+) < (\mathbb{Z},+) \qquad (\{1,-1\},\cdot) < (\{1,-1,i,-i\},\cdot) < (\mathbb{C}^*,\cdot)$ Note: $\mathbb{C}^* = \mathbb{C} - \{0\}$.

Aside (Application to Number Theory): What are the subgroups of $(\mathbb{Z},+)$?

Lemma: Let $H < \mathbb{Z}$. Then either $H = \{0\}$ or $H = a\mathbb{Z}, a \in \mathbb{Z}_{\geq 0}$. In fact, a will be the smallest positive integer in H.
Proof: Either $H = \{0\}$ or $\exists$ $b \in H, b \neq 0$. Then either $b > 0$ or $-b > 0$, so $\exists$ some positive integer in H. Then we shall use the well-ordering principle, a property of $\mathbb{Z}^+$ that states that every non-empty set of positive integers contains a least element. So $\exists$ $a \in H$ that is the smallest positive integer in H. We know that $0 \in H$ and $-a \in H$ because it is a subgroup. We know that $ka = \underbrace{a + \cdots + a}_{k \text{ times}} \in H$ by repeated application of the property of the subgroup of closure under addition. We treat $k(-a)$ similarly.

So $a\mathbb{Z} = \{a\ell \mid \ell \in \mathbb{Z}\} \subset H$. Now suppose $\exists$ $n \in H$ with $n \neq ka$ for some $k \in \mathbb{Z}$. Then $n = qa + r$ with $q \in \mathbb{Z},\ r \in \{1, \ldots, a-1\}$. So $qa \in H$ and $-qa \in H$. Thus $-qa + n = r \in H$. But $r \in \{1, \ldots a-1\}$, so r is a number in H that is smaller than a the smallest number in H. This is a contradiction. Thus $\nexists$ $n \in H$ with $n \neq ka$ for some $k \in \mathbb{Z}$, i.e. $H \subset a\mathbb{Z}$. Thus $H = a\mathbb{Z}$.

Idea: Given two integers a, b, we can form $\langle a, b\rangle = \{ka + \ell b \mid k, \ell \in \mathbb{Z}\} < \mathbb{Z}$. We call this the "subgroup generated by a and b."
Proposition: Let $\langle a, b\rangle = d\mathbb{Z}, d > 0$. Then:
1. $d = ra + sb$ with $r, s > 0$.
2. $d = \gcd(a, b)$
Proof:
1. $d\mathbb{Z} = \{ka + \ell b \mid k, \ell \in \mathbb{Z}\}$, so $d = ra + sb$.
2. $a \in d\mathbb{Z}$, so $a = kd$ and $d \mid a$. Similarly for b. If $e \mid a$ and $e \mid b$, then $e \mid ra + sb$, so $e \mid d$. Thus $e \leq d$, so d is the greatest common divisor of a and b.

Definition: p is prime if its only divisors are 1 and p.

Lemma: If p is prime and $p \mid ab$, then $p \mid a$ or $p \mid b$.
Proof: Either $p \mid a$ or $p \mid b$. If $p \nmid a$, $\gcd(p, a) = 1$. So $1 = ra + sp$. Thus $b = rab + spb$. $p \mid rab$ and $p \mid spb$, so $p \mid rab + spb$, which implies that $p \mid b$.

Corollary (Unique Factorization Theorem):
Given $n \in \mathbb{Z}_{>0}$, there exists a unique function $f : \{p \in \mathbb{Z} \mid p \text{ is prime}\} \to \mathbb{Z}_{\geq 0}$ such that

$$n = \prod_{p \text{ prime}} p^{f(p)}.$$

(We omit the terms with $f(p) = 0$).
Proof (from PSet 1):
Assume for the sake of contradiction that the set of integers with no prime factorizations is nonempty. The well-ordering principle tells us that this set has a smallest element a. This

means that if $n < a$, n has a prime factorization. We know $a \neq 1$, because 1 has a trivial prime factorization. Also, a cannot be prime, because all primes have a prime factorization as well. Thus a must have at least one divisor not equal to 1 or itself, which we will call b. a/b is an integer, and it is less than a, so it must have a prime factorization. $b < a$, so b has a prime factorization as well. Let

$$a/b = p_1^{e_1} \cdots p_n^{e_n} \text{ and } b = q_1^{f_1} \cdots q_n^{f_n}$$

be the prime factorization of a/b and b, respectively. Here the p_i and q_i are all prime and the exponents e_i and f_i are at least 1. If we multiply the prime factorization of a/b by b, we find

$$a = p_1^{e_1} \cdots p_n^{e_n} q_1^{f_1} \cdots q_n^{f_n},$$

which is another prime factorization. Obviously for any $p_i = q_j$, we would combine the terms and add the exponents. This contradicts our assumption that a was the smallest integer that does not have a prime factorization. Thus there can be no smallest element of the set described above, which means the set is empty.

Now we shall prove that every integer n has a unique prime factorization. Assume for the sake of contradiction that the set of integers with multiple prime factorizations is nonempty. Again, the well-ordering principle tells us that this set has a smallest element a. Thus if $n < a$, n has a unique prime factorization. Let the two prime factorizations of a be $p_1^{e_1} \cdots p_n^{e_n}$ and $q_1^{f_1} \cdots q_n^{f_n}$, where the p_i and q_i are all prime and the exponents e_i and f_i are at least 1. There are now two separate cases to consider: either the prime factorizations share at least one prime or they have no primes in common. In the first case, assume that there exists some i and j, with $1 \leq i \leq m$ and $1 \leq j \leq n$ such that $p_i = q_j$. We can divide each factorization by p_i or q_j, which yields

$$a/p_i = p_1^{e_1} \cdots p_i^{e_i - 1} \cdots p_n^{e_n} = q_1^{f_1} \cdots q_j^{f_j - 1} \cdots q_n^{f_n}.$$

If the prime factorizations are the same after dividing by the same number, the original prime factorizations must have been the same. But $a/p_i < a$, so this contradicts our assumption that a was the smallest prime with multiple factorizations. In the second case, the two prime factorizations do not have any prime in common. Take p_1, the first prime in the first factorization. p_1 divides a, so p divides the second factorization. By Euclid's Lemma (proved in class), p_1 must divide some q_j. But p_1 cannot divide any number except itself, so $p_1 = q_j$. This contradicts our assumption that the two factorization do not have any prime in common.

What exactly is this?

Examples of Groups:

Like what are these objects in the group?

Permutations: $\text{Perm}(S) = (\{f : S \to S \mid f \text{ is a bijection}\}, \circ)$
If $S = \{1, 2, \ldots, n\}$, we call $\text{Perm}(S)$ S_n, the symmetric group on n figures. We shall examine a few of these groups.

Okay, wow, so this is the set of possible ways a bijection could exist between S and S. So the id will always be in this set for all n.

$S_2 = \{id, T\}$. T is a transposition, i.e. $T(1) = 2$ and $T(2) = 1$.

To represent an element of S_6, consider how it acts on the elements of S. For example, consider

$$1 \mapsto 3 \qquad 2 \mapsto 6 \qquad 3 \mapsto 5 \qquad 4 \mapsto 4 \qquad 5 \mapsto 1 \qquad 6 \mapsto 2.$$

We examine the cycles:

$$1 \mapsto 3 \mapsto 5 \mapsto 1 \qquad 2 \mapsto 6 \mapsto 2 \qquad 4 \mapsto 4.$$

We represent these maps as cycles, we can do so because

Using cycle notation, we can represent this element as $(1\ 3\ 5)(2\ 6)(4)$. Note that each number occurs once, although we usually omit the cycles of 1 element. A caveat: this map is the same as $(5\ 1\ 3)(6\ 2)(4)$.

Thus the elements of S_3 are 1 (the identity), $(1\ 2), (1\ 3), (2\ 3), (1\ 2\ 3), (1\ 3\ 2)$.

don't get ugh

The product of any of these cycles is equivalent to composition of functions. Note that the second cycle is applied first. Consider $(1\ 2\ 3)(1\ 2)$. Since the cycles have overlapping elements, we can represent this as one cycle. To do so, we follow the elements:

$$1 \mapsto 2 \mapsto 3 \qquad 2 \mapsto 1 \mapsto 2 \qquad 3 \mapsto 3 \mapsto 1.$$

By examining the cycles again, we see that $(1\ 2\ 3)(1\ 2) = (1\ 3)$.

Group Homomorphisms:

Where H is an arbitrary subgroup?

No, I think it could be any group

Definition: $\phi : G \to H$ is a group homomorphism if and only if $\forall\ a, b \in G, \phi(a \cdot b) = \phi(a) \cdot \phi(b)$.
Note that the $\cdot$ on the left represents the group operation of G, and the $\cdot$ on the right represents the group operation of H. Another way to see this is that a group homomorphism is a map between groups that preserves the structure. A fancy way to write this is

$$\begin{tikzcd}
G \times G \arrow[r, "\phi \times \phi"] \arrow[d, "\text{mult}_G"'] & H \times H \arrow[d, "\text{mult}_H"] \\
G \arrow[r, "\phi"'] & H
\end{tikzcd}.$$

ϕ is a group homomorphism if this diagram commutes.

it just means that if you have a subgroup you can create an injective map that goes from the subgroup to the group.

Lecture 3
September 9

Properties of Group Homomorphisms:

it's the obvious map, which just sends an element in the subgroup to the same element in the group

Lemma: If ϕ is a homomorphism from G to H, then:
1. $\phi(1_G) = 1_H$.
2. $\phi(a^{-1}) = \phi(a)^{-1}$.

Proof:
1. $\phi(1_G) \cdot \phi(1_G) = \phi(1_G)$. H is a group, so there exists an inverse of $\phi(1_G)$. Call it $\phi(1_G)^{-1}$. Then $\phi(1_G)^{-1} \cdot \phi(1_G) \cdot \phi(1_G) = \phi(1_G)^{-1} \cdot \phi(1_G) = \phi(1_G)$. Thus $\phi(1_G) = 1_H$.
2. $\phi(a) \cdot \phi(a)^{-1} = \phi(a \cdot a^{-1}) = \phi(1_G) = 1_H$. Similarly, $\phi(a)^{-1} \cdot \phi(a) = 1_H$. Thus $\phi(a^{-1}) = \phi(a)^{-1}$.

Inclusion of a subgroup, e.g. $i : \mathbb{Z} \hookrightarrow \mathbb{R}$ (as additive groups), is a group homomorphism.

Consider $C_6 = \{1, x, x^2, x^3, x^4, x^5\}$, with the group law defined as $x^i \cdot x^j = x^{i+j}$ mod 6. Note that $x^3 \cdot x^5 = x^2$ and $x^{-1} = x^5$. We call C_n with $n \in \mathbb{Z}_{>0}$ the cyclic group on n elements.

Consider $\phi : C_3 \to C_6$, i.e. $\{1, y, y^2\} \to \{1, x, x^2, x^3, x^4, x^5\}$. We must have $1 = \phi(1) = y^3 = \phi(y)^3$ for ϕ to be a group homomorphism. One option is

$$1 \mapsto 1 \qquad y \mapsto x^2 \qquad y^2 \mapsto x^4.$$

Another is

$$1 \mapsto 1 \qquad y \mapsto x^4 \qquad y^2 \mapsto x^2.$$

Of course, another option is for $\phi(a) = 1 \ \forall \ a \in C_3$.

Now consider $\psi : C_6 \to C_3$. There are similar restrictions that yield three options. They are

$$1 \mapsto 1 \qquad x \mapsto y \qquad x^2 \mapsto y^2 \qquad x^3 \mapsto 1 \qquad x^4 \mapsto y \qquad x^5 \mapsto y^2$$

or

$$1 \mapsto 1 \qquad x \mapsto y^2 \qquad x^2 \mapsto y \qquad x^3 \mapsto 1 \qquad x^4 \mapsto y^2 \qquad x^5 \mapsto y$$

or the constant map. Note that, ignoring the constant map, ψ is surjective. Note also that $\phi \circ \psi$ is neither injective nor surjective, though it is of course a group homomorphism.

Another example of a group homomorphism is the determinant det : $GL_n(\mathbb{R}) \to \mathbb{R}^*$. (We know $\det(AB) = \det(A)\det(B)$).

Group Representations:

Should I really unpack this stuff if I understand the result?

Recall the symmetric group S_n, the set of bijections $\sigma : \{1, \ldots, n\} \to \{1, \ldots, n\}$. Given a group homomorphism $\rho : S_n \to GL_n(\mathbb{R})$, we define $\rho(\sigma)$ to be the linear map such that $\rho(\sigma)(e_k) = e_{\sigma(k)}$, where e_k is the $n \times 1$ column vector consisting of a one in the kth spot and zeroes elsewhere. As a matrix, the ij entry of $\rho(\sigma)$ is one if $\sigma(j) = i$ and zero otherwise.

As examples in S_3, consider

$$M(\rho((1\ 2\ 3))) = \begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix} \qquad M)(\rho((1\ 2))) = \begin{bmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

so these are just adjacency matrices for a given bijection (that's provided in cycle notation)

(M is just the map from a linear map to its associated matrix).

Lemma: ρ is a group homomorphism.
Proof: We need to show that $\rho(\sigma) \circ \rho(\tau) = \rho(\sigma \circ \tau)$. It suffices to check this on the e_k, as they form a basis:

$$\rho(\sigma) \circ \rho(\tau)(e_k) = \rho(\sigma)(e_{\tau(k)}) = e_{\sigma(\tau(k))} = e_{(\sigma\circ\tau)(k)} = \rho(\sigma \circ \tau)e_k.$$

What is a linear group?

Definition: A representation of a group is a homomorphism to a linear group (e.g. $GL_n(\mathbb{R})$).

Example:
$\det\circ\rho : S_n \to \mathbb{R}^*$ is the representation of S_n. It is usually written as $\text{sign} : S_n \to \{-1, 1\}$. For example $\text{sign}((1\ 2\ 3)) = 1$ and $\text{sign}((1\ 2)) = -1$.

Image and Kernel:

If $\phi : G \to H$ is a group homomorphism, there are two important subgroups to consider. They are the image and kernel of ϕ and are defined as

$$\text{im}(\phi) = \{y \in H \mid \exists\ x \in G \text{ such that } \phi(x) = y\} < H$$

$$\ker(\phi) = \{x \in G \mid \phi(x) = 1\} < G.$$

Any subgroup of H is the image of some map ϕ from some group G. If $M < H$, let the inclusion mapping $i : M \hookrightarrow H$ be our map. This is not true for the kernel. For example, consider S_3 with subgroup $G = \{1, (1\ 2)\}$. Are there a group H and a map $\phi : S_3 \to H$ such that $\ker\phi = G$?

So here we conclude that the kernal of S3 could only be {1}, which is where phi maps 1->1 but nothing else there. Or it could be all of S3 where phi maps everything to 1. But it can't be in between.

Lemma: No.
Proof: We saw that $(1\ 2\ 3)(1\ 2) = (1\ 3)$ but $(1\ 2)(1\ 2\ 3) = (2\ 3) = (1\ 3\ 2)(1\ 2)$. Let $(1\ 2) = a$ and $(1\ 2\ 3) = b$. Then $ab = b^2a$. By assumption $\phi(a) = 1_H$ because $a \in \ker(\phi)$, so $\phi(b) = \phi(b)\phi(b)$. This is only true if $\phi(b) = 1_H$. Also, $\phi((1\ 3)) = \phi(ba) = 1_H$ and $\phi(2\ 3) = \phi(ab) = 1_H$. So ϕ must be the constant map to 1_H. Thus is $(1\ 2) \in \ker(\phi)$, then $\ker(\phi) = S_3$.

Given a group homomorphism $\phi : G \to H$, we consider the sequence

$$\ker(\phi) \hookrightarrow G \twoheadrightarrow \text{im}(\phi).$$

This "breaks up" G into smaller parts which interact in some way. More on this later.

What the fuck is the point of this?

Definition: $N < G$ is a normal subgroup if $g \cdot x \cdot g^{-1} \in N\ \forall\ x \in N$ and $\forall\ g \in G$. Then $g \cdot x \cdot g^{-1}$ is known as the conjugate of x by g.

Lemma: Given a homomorphism $\phi : G \to H$, $\ker(\phi)$ is a normal subgroup of G.
Proof: Suppose $x \in \ker(\phi)$ and $g \in G$. Then $\phi(gxg^{-1}) = \phi(g)\phi(x)\phi(g^{-1}) = \phi(g)\phi(g)^{-1} = 1$.

Definition: Conjugation by g is the map $C_g : G \to G$ that sends x to gxg^{-1}.
Note that this is a group homomorphism.

Aside: What does $C_g(x) = x$ mean? $gxg^{-1} = x$, so $gx = xg$ and $gxg^{-1}x^{-1} = 1$. (The term $gxg^{-1}x^{-1}$ is known as the commutator of g and x).

Lecture 4
September 11

Isomorphisms and Automorphisms:

So is an isomorphism a map that goes from G->H such that every element in G has an image in H and no two elements in G share their image in H, and moreover if you apply this map to two elements in G, the resulting image is the same regardless of whether you apply the map before or after you apply the group operation to the two elements?

Definition: An isomorphism is a bijective group homomorphism.

Theorem: Given a group homomorphism $\phi : G \to H$, the following are equivalent and show ϕ is an isomorphism:
1. ϕ is a bijection
2. $\exists\ \psi : H \to G$ that is a group homomorphism and such that $\psi \circ \phi = id_G$ and $\phi \circ \psi = id_H$.
Proof:
$2 \implies 1$: An inverse group homomorphism is also an inverse of a mpa of sets, so this shows that ϕ is a bijection of sets.
$1 \implies 2$: If ϕ is a bijection, then it has an inverse map of sets $\phi^{-1} : H \to G$. We can show that ϕ^{-1} is a group homomorphism.
Given $a, b \in H$, there exists $x, y \in G$ such that $\phi(x) = a$ and $\phi(y) = b$. Then $\phi(xy) = ab$, so $\phi^{-1}(ab) = xy$ and $\phi^{-1}(a)\phi^{-1}(b) = xy$.

If $\phi : G \to H$ is an isomorphism, we write $G \overset{\cong}{\to} H$. Also, if some isomorphism $\phi : G \to H$ exists, we write $G \cong H$ and say G is isomorphic to H.

Definition: An automorphism is an isomorphism from a group to itself.

Aut(G), the set of all automorphisms on G, is a group and is often called the "group of symmetries of G."

Examples:

Consider $C_3 = \{1, x, x^2\}$ with $x^3 = 1$. Then Aut$(C_3) = \{id, \text{swap}\} \cong C_2$. (The swap map is defined with $1 \mapsto 1$, $x \mapsto x^2$, and $x^2 \mapsto x$).

Recall conjugation by $g \in G$, the map $C_g : G \to G$ that take x to gxg^{-1}. This is an automorphism, which can be easily proved by proving it is a homomorphism and proving it has an inverse.

Now consider $C : G \to \text{Aut}(G)$ that sends g to C_g.
Proposition: This is a group homomorphism.
Proof: $C_{gh}(x) = (gh)x(gh)^{-1} = ghxh^{-1}g^{-1} = g(hxh^{-1})g^{-1} = C_g(hxh^{-1}) = (C_g \circ C_g)(x)$.

Warning/Note: If we were to use $\widetilde{C}_g(x) = g^{-1}xg = C_{g^{-1}}(x)$, then $\widetilde{C} : G \to \text{Aut}(G)$ is not generally a homomorphism.

Also, $\ker(C) = \{g \mid C_g : G \to G \text{ is } id\} = \{g \mid gxg^{-1} = x\ \forall\ g \in G\} = \{g \mid gx = xg\ \forall\ x \in G\} = \{g \mid g \text{ commutes will all elements of } G\} = \text{Center}(G)$.

Examples of the Center:
1. Center$(C_3) = C_3$. (This is true for all abelian groups).
2. Center$(S_3) = \{1\}$.
3. Center $(GL_2(\mathbb{R})) = \{\lambda I \mid \lambda \in \mathbb{R}^*\} < GL_2(\mathbb{R})$.

An element is in the center if it commutes with every element in the group (eg. the identity is always in the center)

If H is abelian, then would there be no distinction between right and left cosets?

Cosets:

So you're picking a specific g, not all g in G.

Definition: Given $H < G$, a left coset of H is a set of the form $gH = \{gh \mid h \in H\}$ with $g \in G$. A right coset is defined similarly.

Proposition: the left cosets of $H < G$ partition G, i.e.
1. Given two left cosets g_1H and g_2H, either $g_1H = g_2H$ or $g_1H \cap g_2H = \emptyset$.
2. The union of all left cosets is all of G

Proof:
1. Given g_1H and g_2H, either $g_1H \cap g_2H = \emptyset$ or $\exists\ x \in g_1H \cap g_2H$. Assume the latter is true. Let $x = g_1h = g_2k$ for some $h, k \in H$.
We first show $g_1H \subset g_2H$. Given $g_1\ell \in g_1H$ with $\ell \in H$, we can use $g_1h = g_2k$, which implies $g_1 = g_2kh^{-1}$, to write $g_1\ell = g_2kh^{-1}\ell$. $kh^{-1}\ell \in H$, as H is a subgroup. Thus $g_1\ell \in g_2H$, which implies $g_1H \subset g_2H$. Using a similar argument for $g_2a \in g_2H$, we can show $g_2H \subset g_1H$, so $g_1H = g_2H$ if their intersection is non-empty.
2. $g = g \cdot 1 \in gH$, so any $g \in G$ is in some gH.

When is the set of left cosets a group?
Proposition: Given $H < G$, the following are equivalent:
1. H is a normal subgroup of G.
2. $gH = Hg\ \forall\ g \in G$.
3. Every left coset is a right coset.

Proof:
$1 \implies 2$: Assume $H \triangleleft G$. We need to show that $gH \subset Hg$. Given gh, we need to write it as ag for some $a \in H$. We can do this thus using an inverse: $gh = ghg^{-1}g = (ghg^{-1})g \in Hg$.
$2 \implies 1$: If $gH = Hg$, then $gh = kg$ for some $k \in H$, so $ghg^{-1} = k \in H$.
$2 \implies 3$: Left cosets are sets of the form $gH = Hg$.
$3 \implies 2$: The left and right cosets containing g are gH and Hg, respectively. So $Hg = gH$.

Lecture 5
September 13

Quotients:

Given $H \lhd G$, we want to form G/H, i.e. "setting H equal to 1," such that G/H is a group. As a set, G/H is the set of all cosets of H. How should multiplication on G/H be defined, i.e. what should $aH \cdot bH$ be?

Proposition: The set $aH \cdot bH = \{xy \mid x \in aH, y \in bH\}$ is a coset of H. In fact, it is abH. Then $aH \cdot bH = abH$.
Proof: We first show that $abH \subset aH \cdot bH$. Given $h \in H$, $abh \in abH$. $abh = (a \cdot 1)(b \cdot h) \in aHbH$.
Now we show $aH \cdot bH \subset abH$. Given $h, k \in H$, we must show that $ah \cdot bk \in abH$. We shall use an inverse: $ahbk = abb^{-1}hbk = ab(b^{-1}hb)k$. We recall that $b^{-1}hb$ is conjugation of h by $b^{-}1$. Since H is normal, $b^{-1}hb \in H$. Thus $ahbk = abx$ for some $x \in H$, so $ahbk \in abH$.
Alternate Proof: $bH = Hb$, as H is normal. $aH \cdot bH = aH \cdot Hb = a(H \cdot H)b = aHb = a(Hb) = abH$.

We now have a set G/H and a well-defined operation on this set.
Proposition: this is a group.
Proof: Associativity follows from associativity of G. $(aH \cdot bH)(cH) = (ab)cH = a(bc)H = (aH)(bH \cdot cH)$. The identity is $H = 1H = hH$ for any $h \in H$. The inverse of an a element aH is $a^{-1}H$.

Examples of Quotients:

$n\mathbb{Z} \lhd \mathbb{Z}$: $\mathbb{Z}$ is abelian, so any subgroup is normal. $\mathbb{Z}/n\mathbb{Z}$ is the group of cosets of $n\mathbb{Z}$. The cosets are $0 + n\mathbb{Z}, 1 + n\mathbb{Z}, \ldots, (n-1) + \mathbb{Z}$. We call this group the integers modulo n with addition modulo n.

$G = \{f : \mathbb{R} \to \mathbb{R} \mid f(x) = ax + b,\ a \in \mathbb{R}^*,\ b \in \mathbb{R}\}$ with composition. Two interesting subgroups of this are the translations $T = \{f : \mathbb{R} \to \mathbb{R} \mid f(x) = x + b, b \in \mathbb{R}\}$ and the dilations $D = \{f : \mathbb{R} \to \mathbb{R} \mid f(x) = ax,\ a \in \mathbb{R}^*\}$. Note that T and D are abelian. We shall also define the maps $\tau : \mathbb{R} \overset{\cong}{\to} T$ that takes b to the map $f(x) = x + b$ and $m : \mathbb{R} \overset{\cong}{\to} D$ that takes a to the map $f(x) = ax$.
Also, we see that G is not abelian: with $f_1(x) = x + 1$, and $f_2(x) = 2x$, $f_1 \circ f_2(x) = 2x + 1$ but $f_2 \circ f_1(x) = 2x + 2$.
Now we consider if either of these subgroups is normal. If T is normal, then $m_{1/a} \circ t_b \circ m_a \in T$, and if D is normal, then $\tau_{-b} \circ m_a \circ \tau_b \in D$. Examining the first case, we see $m_{1/a} \circ t_b \circ m_a(x) = (1/a)((ax) + b) = x + b/a \in T$, so T is normal. In the second case, we see $\tau_{-b} \circ m_a \circ \tau_b(x) = a(x + b) - b = ax + b(a - 1) \notin D$, so D is not normal.

Claim: $G/T \cong \mathbb{R}^*$.
Proof: The cosets are $m_aT = \{f : \mathbb{R} \mapsto \mathbb{R} \mid f(x) = ax + b,\ b \in \mathbb{R}\}$ with $a \in G$ (as exercise). Also, $(m_{a_1}T)(m_{a_2}T) = m_{a_1}m_{a_2}T = m_{a_1a_2}T$. So $G/T \cong \mathbb{R}^*$ via $\phi : \mathbb{R}^* \to G/T$ that maps a to m_aT.

We now consider: $\mathbb{R} \overset{\tau}{\hookrightarrow} G \overset{S}{\twoheadrightarrow} \mathbb{R}^*$, with $\tau(b) = \tau_b$ and $S(\{x \mapsto ax + b\}) = a$. τ is injective, S is surjective, $\mathrm{im}(\tau) = \ker(S)$, and S gives the isomorphism between G/T and $\mathbb{R}^*$.

Definition: A short exact sequence is defined as $H \overset{\alpha}{\hookrightarrow} G \overset{\beta}{\twoheadrightarrow} G'$ with $\mathrm{im}(\alpha) = \ker(\beta)$.

Lecture 6
September 16

Quotients and Extensions:

First Isomorphism Theorem:
Suppose $\phi : G \to G'$ is a surjective group homomorphism. Then $G' \cong G/\ker(\phi)$
Proof: Delayed.

Note that if we have a short exact sequence: $H \overset{i}{\hookrightarrow} G \overset{\pi}{\twoheadrightarrow} K$ with $\mathrm{im}(i) = \ker(\pi)$, then $K \cong G/\mathrm{im}(i)$ by this theorem.

Theorem (Universal Property of the Quotient):
Given $H \triangleleft G$, suppose there is a homomorphism $\phi : G \to G'$ such that $H < \ker\phi$. Then there exists a unique homomorphism $\overline{\phi} : G/H \to G'$ such that $\overline{\phi} \circ \pi = \phi$, i.e. that the following diagram commutes:

$$\begin{tikzcd}
G \arrow[r, "\phi"] \arrow[d, "\pi"'] & G' \\
G/H \arrow[ur, "\overline{\phi}"'] &
\end{tikzcd} .$$

Proof: What must $\overline{\phi}(gH)$ be? If must be $\phi(g)$, as $\overline{\phi} \circ \pi(g) = \phi(g)$. Since this must hold for arbitrary $g \in G$, we have proved the uniqueness of $\overline{\phi}$.
Now we must prove the existence of $\overline{\phi}$. First we check that $\overline{\phi}(gH)$ is well-defined. We know $hH = H$ if $h \in H$, so we pick two elements $h_1, h_2 \in H$ and ensure that $\overline{\phi}$ maps h_1H and h_2H to the same element in G'. This is equivalent to checking that $\phi(gh_1) = \phi(gh_2)$. $\phi(gh_1) = \phi(g)\phi(h_1) = \phi(g)$ because $h_1 \in H < \ker(\phi)$. Similarly $\phi(gh_2) = \phi(g)\phi(h_2) = \phi(g)$, so $\phi(gx)$ with $x \in H$ is well-defined.
Next we check that this is a group homomorphism: $\overline{\phi}(g_1g_2H) = \phi(g_1g_2) = \phi(g_1)\phi(g_2) = \overline{\phi}(g_1H)\overline{\phi}(g_2H)$

Aside:
Definition: An abstract quotient Q, π for G and H with $H \triangleleft G$ is a group Q and a map $\pi : G \to Q$ such that $H < \ker(\pi)$ such that the Universal Property of the Quotient is satisfied (with Q, π is place.)

Theorem: Any abstract quotient is isomorphic to G/H
Proof: Exercise.

Proof of First Isomorphism Theorem: Given $H \triangleleft G$ and $\phi : G \to G'$ such that $H = \ker(\phi)$. By the Universal Property of the Quotient, there exists a unique homomorphism $\overline{\phi} : G/\ker(\phi) \to G'$ such that $\overline{\phi} \circ \pi(g) = \overline{\phi}(g \cdot \ker(\phi)) = \phi(g)\ \forall\ g \in G$.
We claim that this map is bijective, which implies it is an isomorphism. We first show that $\overline{\phi}$ is surjective. We know that ϕ is surjective, so given $x \in G'$, $\exists\ g$ such that $\phi(g) = x$. Then $\overline{\phi}(gH) = x$ for any $x \in G'$, so $\overline{\phi}$ is surjective. Next we show that $\overline{\phi}$ is injective. We know that $\overline{\phi}(gH) = \phi(g) = 1 \Leftrightarrow g \in \ker(\phi) \Leftrightarrow g\ker(\phi) = \ker(\phi)$. So the only element of $G/\ker(\phi)$ which is mapped by $\overline{\phi}$ to 1 is the coset $\ker(\phi)$. Thus $\overline{\phi}$ is injective.

Definition: A group extension of the groups H and K is a group G and two maps i, π

such that $H \overset{i}{\hookrightarrow} G \overset{\pi}{\twoheadrightarrow} K$ is a short exact sequence (with $\mathrm{im}(i) = \ker(\pi)$), i.e. with $G/H \cong K$.

Examples of Extensions:

Definition: The direct product of the groups H and K is the set $H \times K = \{(h,k) \mid h \in H, k \in K\}$ with multiplication defined as $(h_1,k_1)(h_2,k_2) = (h_1h_2, k_1k_2)$. This a group with unit $(1_H 1_K)$. Note also that $H \times \{1_K\}$ and $\{1_H\} \times K$ commute, as $(h,1) \cdot (1,k) = (h,k) = (1,k) \cdot (h,1)$.

Proposition: Suppose $H, K < G$ with $HK = G$ and $hk = kh \;\forall\; h \in H,\; k \in K$. Then $G \cong H \times K$.
Proof: We can show that $\phi : H \times K \to G$ is an isomorphism. First we show that it is a homomorphism:

$$\begin{aligned}
\phi((h_1,k_1)(h_2,k_2)) &= \phi(h_1h_2, k_1k_2) && \text{(definition of multiplication in } H \times K) \\
&= h_1h_2k_1k_2 && \text{(definition of } \phi) \\
&= h_1k_2h_2k_2 && \text{(elements of } H \text{ and } K \text{ commute with each other)} \\
&= \phi(h_1,k_1)\phi(h_2,k_2). && \text{(definition of } \phi)
\end{aligned}$$

Next we show that ϕ is surjective. We know that $HK = G$, which means that any element $g \in G$ can be expressed as $g = hk$. This means that $\forall\; g \in G, \exists\; (h,k) \in H \times K$ such that $\phi(h,k) = hk$. Thus ϕ is surjective. To show that ϕ is injective, consider $\ker(\phi)$. The only element of $H \times K$ that will map to the identity in G is $(1_H, 1_K)$, which is the identity in $H \times K$. Thus ϕ has a trivial kernel and is injective. Thus ϕ is a bijective homomorphism, so it is an isomorphism, and $G \cong H \times K$.

Example: $C_2 \times C_3 \cong C_6$, or more generally, $C_m \times C_n \cong C_{mn}$ if m and n are relatively prime.
Proof: $\{1, x\} \times \{1, y, y^2\} \cong \{1, z, z^2, z^3, z^4, z^5\}$ via ϕ defined with $x \mapsto z^3$, $y \mapsto z^2$, $y^2 \mapsto z^4$, $xy \mapsto z^5 = z^{-1}$, and $xy^2 \mapsto z$.
In general, we can form $\phi : \mathbb{Z}/mn\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$. (Note that $C_k \cong (\mathbb{Z}/k\mathbb{Z}, +)$ with 0 as the unit). ϕ maps 1 to $(1,1)$. 4(Neither of these is the unit). Because m and n are relatively prime, the lowest k such that $(k \bmod m, k \bmod n) = (0,0)$ is $k = mn$. So the map ϕ has a trivial kernel, which means it is injective. Also, $|\mathbb{Z}/mn\mathbb{Z}| = mn$ and $|\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}| = mn$, so ϕ is surjective.
Remark: $C_4 \ncong C_2 \times C_2$

Order and Index:

Definition: Given a group G, the order of G ($|G|$) is the number of elements in the group.

Definition: Given an element x of a group G, the order of x ($|x|$) is the smallest $k \in \mathbb{Z}$ such that $x^k = 1$. If no k exists, then x has infinite order.

Definition: Given a group G and a subgroup H, the index of H in G ($[G : H]$) is the number of left cosets of H in G.

Lagrange's Theorem: If G is a finite group and $H < G$, then $|H| \mid |G|$.
Proof: The left cosets of H partition G, and all are of size $|H|$, so $|G| = |H| \cdot [G : H]$

Corollary: The order of an element divides the order of the group if the group is finite.
Proof: Let $x \in \{1, x, x^2, \ldots, x^{k-1}\} < G$. $|x| = k = |H|$, so $|x| \mid |G|$.

Application (Fermat's Little Theorem):

$a^p \equiv a \bmod p$ for $a \in \mathbb{Z},\ p$ prime.
Proof: The group $(\mathbb{Z}/p\mathbb{Z})^*$ with multiplication modulo p has order $p-1$. So if $a \not\equiv 0 \bmod p$, $a^{p-1} \equiv 1 \bmod p$ because $a^k = 1 \bmod p$ for some k such that $k \mid (p-1)$. So $(a^k)^m = a^{p-1} \equiv 1 \bmod p$. So if $a \equiv 0 \bmod p$, the $a^p = a \bmod p$ and if $a \not\equiv 0 \bmod p$, $a^{p-1} \equiv 1 \bmod p \implies a^p = a \bmod p$.

Lecture 7
September 18

More on Order and Index:

Lemma: (Even if $|G|, |H|$ are infinite), there are n left cosets in G if and only if there are n right cosets of H in G.
Proof: We know $x \in gH \Leftrightarrow g^{-1}x \in H \Leftrightarrow (g^{-1}x)^{-1} = x^{-1}g \in H \Leftrightarrow x^{-1} \in Hg^{-1}$. Suppose $g_1H, \dots g_nH$ is a list of all the different left cosets. These partition G. Thus $Hg_1^{-1}, \dots Hg_n^{-1}$ partition the set of inverses, which is G.

Theorem: $\mathbb{Z}/mn\mathbb{Z} \cong \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ if m and n are relatively prime.
Proof: We can form the isomorphism $\phi : \mathbb{Z}/mn\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ defined with $a \mapsto (a \text{ reduced mod } m,\ a \text{ reduced mod } n)$

Rule: Given a cyclic group $\mathbb{Z}/k\mathbb{Z}$, a group homomorphism from $\mathbb{Z}/k\mathbb{Z}$ to G is just a choice of an element $x \in G$ such that $x^k = 1$ (or $k \cdot x = 0$ if the group is additive). If we examine the previous map defined with $1 \mapsto (1, 1)$, we see that this is a homomorphism.
Claim: This is an isomorphism.
Proof: Suppose $(\ell, \ell) = (0, 0) \in \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$. Then $m \mid \ell$ and $n \mid \ell$. Since m and n are relatively prime, $\exists\ a, b \in \mathbb{Z}$ such that $am + bn = 1$. Let $\ell = cm$. Then $n \mid cm$, so $acm + bcn = c \implies a\ell + bcn = c$. So $n \mid acm + bn$, i.e. $n \mid c$. So $\ell = cm = dmn$ and $mn \mid \ell$. So the least multiple of $(1, 1)$ that maps to $(0, 0)$. is $(mn, mn) = (0, 0)$. Thus the kernel is trivial, so this is a bijection and thus an isomorphism.

Corollary: If $n_1, \dots n_k$ are relatively prime, then $\mathbb{Z}/n_1 \cdots n_k\mathbb{Z} \cong \mathbb{Z}/n_1\mathbb{Z} \times \cdots \times \mathbb{Z}/n_k\mathbb{Z}$ via $a \mapsto (a \bmod n_1, \dots, a \bmod n_k)$

Chinese Remainder Theorem: Suppose we want $x \in \mathbb{Z}$ such that $x \equiv a \bmod n_1, x \equiv a_k \bmod n_k$. Then $\exists\ x$ which is unique modulo $n_1 \cdots n_k$.
Proof: Exercise.

More on Group Extensions:
We shall discuss three types:
1. Direct Products: ($G = H \times K$ with $H \overset{i}{\hookrightarrow} G \overset{\pi}{\twoheadrightarrow} K$ a short exact sequence). We've discussed these already.
2. Split Extensions (Semidirect Products)
3. Non-Split Extensions (These are tricky).

Definition: Given $H \overset{i}{\hookrightarrow} G \overset{\pi}{\twoheadrightarrow} K$ (i.e. $K \cong G/H$), this is a split extension if there exists a group homomorphism (a "section") $\sigma : K \to G$ such that $\pi \circ \sigma = id_K$, i.e. there exists a copy of the quotient $G/H \cong K$ in G which is given as $\text{im}(\sigma)$. If there is no such σ, this is a non-split extension. (We informally say that an extension is non-split if "we can't see G/H in G." More on this later.)

Split Extensions:

Example: $G = \{f : \mathbb{R} \to \mathbb{R} \mid f(x) = ax + b, a \neq 0\}$. Consider the sequence $\mathbb{R} \overset{\tau}{\hookrightarrow} G \overset{\pi}{\twoheadrightarrow} \mathbb{R}^*$ with τ defined with $b \mapsto f(x) = x + b$ and π defined with $f(x) = ax + b \mapsto a$. The section $\sigma : \mathbb{R}^* \to G$ is defined with $a \mapsto f(x) = ax$. If we consider the translations T and the dilations D that we have previously discussed, we see that $T = \text{im}(\tau) \cong \mathbb{R}$ in G is normal and $D = \text{im}(\sigma) \cong \mathbb{R}^*$ in G is not normal.

Non-Split Extensions:

Example: Consider $\mathbb{Z}/2\mathbb{Z} \overset{i}{\hookrightarrow} \mathbb{Z}/4\mathbb{Z}$ with i defined with $1 \mapsto 2$. We choose the subgroup $\{0, 2\} < \{0, 1, 2, 3\} < \mathbb{Z}/4\mathbb{Z}$. Then the quotient is $(\mathbb{Z}/4\mathbb{Z})/\text{im}(i) = \{\{0, 2\}, \{1, 3\}\}$, These elements are the cosets $\text{im}(i)$ and $1+\text{im}(i)$. Here $\{0, 2\}$ is the identity and $\{1, 3\}+\{1, 3\} = \{0, 2\}$, so $(\mathbb{Z}/4\mathbb{Z})/\text{im}(i) \cong C_2$.

If we now consider the sequence $\mathbb{Z} \overset{i}{\hookrightarrow} \mathbb{Z}/4\mathbb{Z} \overset{\pi}{\twoheadrightarrow} (\mathbb{Z}/4\mathbb{Z})/\text{im}(i)$, does there exist a section σ such that $\pi \circ \sigma = id$? We know that σ must be a homomorphism, so $\sigma(\{0, 2\}) = 0$. Thus $\sigma(\{1, 3\})$ can be 1 or 3. $1 + 1 \equiv 2 \bmod 4$ and $3 + 3 \equiv 2 \bmod 4$, so for whatever element we choose, $\sigma(\{1, 3\}) + \sigma(\{1, 3\}) = 2$. But $\sigma(\{1, 3\}) + \sigma(\{1, 3\}) = \sigma(\{0, 2\}) = 0$ because σ is a group homomorphism. This is a contradiction, so no such σ exists. Thus this extension is non-split.

Quaternions:

Definition: The quaternions are a group defined as $Q = \{\pm 1, \pm \mathbf{i}, \pm \mathbf{j}, \pm \mathbf{k}\}$ and with multiplication defined with $\mathbf{i}^2 = \mathbf{j}^2 = \mathbf{k}^2 = \mathbf{ijk} = -1$, $\mathbf{ij} = \mathbf{k}$, $\mathbf{ji} = -\mathbf{k}$, $\mathbf{jk} = \mathbf{i}$, $\mathbf{kj} = -\mathbf{i}$, $\mathbf{ki} = \mathbf{j}$, and $\mathbf{ik} = -\mathbf{j}$. Note that 1 is the identity and -1 commutes with everything.

To see why this is a group, we represent $Q < GL_2(\mathbb{R})$ with

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

Lecture 8
September 20

More on the Quaternions:

The set of elements in Q that commute is $\text{Center}(Q) = \{1, -1\} \triangleleft Q$. The quotient of Q by this subgroup is $Q/\{1, -1\} = \{\{\pm 1\}, \{\pm \mathbf{i}\}, \{\pm \mathbf{j}\}, \{\pm \mathbf{k}\}\}$, which we can represent as $\{1, x, y, z\}$ with $x^2 = y^2 = z^2 = 1$ and $xy = yx = z$. Thus $Q/\{1, -1\}$ is isomorphic to K_4, the Klein Four Group (which is also isomorphic to $C_2 \times C_2$).

We now consider the sequence $\{1, -1\} \overset{i}{\hookrightarrow} Q \overset{\pi}{\twoheadrightarrow} Q/\{1, -1\}$. This is a short exact sequence, as $\text{im}(i) = \{1, -1\} = \ker(\pi)$. We wish to know if this forms a split extension, that is, if there is a homomorphism $\sigma : Q/\{1, -1\} \to Q$ such that $\pi \circ \sigma = id_K$.
We know that $\sigma(1) = 1$, as σ is a homomorphism. We have two choices for $\sigma(x)$, namely $\mathbf{i}$ or $-\mathbf{i}$, because $\pi(\{\pm \mathbf{i}\}) = x$. For either of these choices, we know that $\sigma(x)^2 = -1$, but we also know that $\sigma(x)^2 = \sigma(x^2) = \sigma(1) = 1$ because σ is a homomorphism. This is a contradiction, so there is no such σ.
Thus the extension, which can also be written as $\mathbb{Z}/2\mathbb{Z} \overset{i}{\hookrightarrow} Q \overset{\pi}{\twoheadrightarrow} \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, is non-split
Aside: This is called a central extension, i.e. an extension $A \overset{i}{\hookrightarrow} G \overset{\pi}{\twoheadrightarrow} K$ with $A \subset \text{Center}(G)$ (i.e. A is abelian).

Lemma: If a central extension G of A, K is split, then $G \cong A \times K$.
Proof: Exercise.

More on Split Extensions:

We consider the sequence $H \overset{i}{\hookrightarrow} G \overset{\pi}{\twoheadrightarrow} K$ with $\text{im}(i) = \ker(\pi)$, i.e. a short exact sequence. By the First Isomorphism Theorem, $G/H \cong K$. If it is split, there exists $\sigma : K \to G$ such that $\sigma \circ \pi = id_K$.

Claim: If $im(i)$ and $\text{im}(\sigma)$ are two subgroups of G, then $im(i) \triangleleft G$ and
1. $\text{im}(i) \cap \text{im}(\sigma) = \{1\}$
2. $\text{im}(i) \cdot \text{im}(\sigma) = G$.
Proof:
1. $\sigma \circ \pi \circ i(x) = \sigma(1) = 1 \in K$ because $\text{im}(i) = \ker(\pi)$ and σ is a group homomorphism. So if $x \in \text{im}(i) \cap \text{im}(\sigma)$, then $k = 1$.
2. Let $g \in G$. Then $\pi(g) \in K$, $\sigma \circ \pi(g) \in \text{im}(\sigma) < G$, and $\pi \circ \sigma \circ \pi(g) = \pi(g)$. We now consider $(\sigma \circ \pi(g)) \cdot g^{-1}$. We know $\pi \circ \sigma \circ \pi(g) \cdot \pi(g^{-1}) = \pi(g) \cdot \pi(g^{-1}) = \pi(1) = 1$. Thus $(\sigma \circ \pi(g)) \cdot g^{-1} \in \ker(\pi) = \text{im}(i)$. So $\sigma \circ \pi(g)) \cdot g^{-1} = h$ for some $h \in \text{im}(i)$. Then $h^{-1}(\sigma \circ \pi(g)) = g$. We know $h^{-1} \in \text{im}(i)$ and $\sigma \circ \pi(g) \in \text{im}(\sigma)$. So we have expressed an arbitrary element in G as a product of elements in $\text{im}(i)$ and $\text{im}(\sigma)$. Thus $\text{im}(i) \cdot \text{im}(\sigma) = G$.

Now we suppose (after some renaming), that $H, K < G$ with $H \triangleleft G$, $H \cap K = \{1\}$, and $HK = G$.
Corollary: G is in bijection with pairs (h, k) via $(h, k) \mapsto hk$.
Proof: Suppose $h_1 k_1 = h_2 k_2$. Then $h_2^{-1} h_1 = k_2 k_1^{-1}$. Both of these must equal 1, as they are in $H \cap K$. Thus the map defined above is an injective map between maps of the same size, so it is bijective.

(Note that the above conditions are close to those for a direct product, except we need the elements of H and K to commute with each other, which is not necessarily the case here).

What is the group law? Cleverly using some inverses, we can write $hkh'k' = h(kh'k^{-1})kk'$. Since H is normal, $h(kh'k^{-1}) \in H$ and we know $kk' \in K$. To record this, we define a map $\phi : K \to \mathrm{Aut}(H)$ with $k \mapsto \phi_k(x) = kxk^{-1}$. We have previously shown that ϕ is a group homomorphism. Using this, we can write $hkh'k' = h\phi_k(h')kk'$.

Definition: A semidirect product of H and K mediated by $\phi : K \to \mathrm{Aut}(H)$ is a group which is $H \times K$ (as a set) with group law $(h, k) \cdot (h', k') = (h\phi_k(h'), kk')$. We write this as $H \underset{\phi}{\rtimes} K$.

Theorem:
1. Given any $H, K, \phi : K \to \mathrm{Aut}(H)$, $H \underset{\phi}{\rtimes} K$ is a group and $H \triangleleft (H \underset{\phi}{\rtimes} K)$
2. Any split extension is a semidirect product.
3. Any sequence $H \overset{i_1}{\hookrightarrow} H \underset{\phi}{\rtimes} K \overset{\pi}{\twoheadrightarrow} K$ (with i_1 defined with $h \mapsto (h, 0)$) is a split short exact sequence with section $i_2 : K \to H \underset{\phi}{\rtimes} K$ defined with $k \mapsto (0, k)$.

Proof:
1. Exercise: Check that it is a group and the maps i_1, π, i_2 are homomorphisms.
2. Done.

Examples:
Consider $G = \{f : \mathbb{R} \to \mathbb{R} \mid f(x) = ax + b, a \in \mathbb{R}^*, b \in \mathbb{R}\}$. We shall denote $f(x) = ax + b$ as $f_{a,b}$. We then consider the split short exact sequence $\mathbb{R} \overset{\tau}{\hookrightarrow} G \overset{\pi}{\twoheadrightarrow} \mathbb{R}^*$ with $\tau(b) = f_{0,b}$ and $\pi(f_{a,b}) = a$ and with section $\sigma : \mathbb{R}^* \to G$ defined as $\sigma(a) = f_{a,0}$. Then $G \cong \mathbb{R}^* \underset{\phi}{\ltimes} \mathbb{R}$ for some $\phi : \mathbb{R}^* \to \mathrm{Aut}(\mathbb{R})$. To determine ϕ, we consider the conjugation $f_{a,0} \circ f_{0,b} \circ f_{1/a,0} = f_{0,\phi_a(b)}$. This yields $a((1/a)x + b) = x + ab$. Thus $\phi_a(a) = ab$, so ϕ takes an element to multiplication of that element and $G \cong \mathbb{R}^* \underset{\text{mult}}{\ltimes} \mathbb{R}$

Lecture 9
September 23

More on Semidirect Products:

We recall that we should think "$\phi_{k_1}(h_2) = k_1 h_2 k_1^{-1}$." Indeed: $(1, k_1)(h_2, 1)(1, k^{-1}) = (\phi_{k_1}(h_2), k_1)(1, k_1^{-1}) = (\phi_{k_1}(h_2)\phi_{k_1}(1), k_1 k_1^{-1}) = (\phi_{k_1}(h_2), 1)$. Note that if ϕ sends k to id_K $\forall\ k \in K$, then $H \underset{\phi}{\ltimes} K \cong H \times K$.

Check: $H \underset{\phi}{\ltimes} K$ is a group.
1. Identity: $(1, 1)$
2. Inverses: $(h, k)^{-1} = (x, k^{-1})$ where $\phi_k(x) = h^{-1}$. It turns out $x = (\phi_k)^{-1}(h^{-1}) = \phi_{k^{-1}}(h^{-1})$.
More intuitively, we can view (h, k) as "$h \cdot k''$, so it would be natural to try $(h, k)^{-1} = (1, k^{-1})(h^{-1}, 1)$. Indeed $(h, 1)(k, 1)(1, k^{-1})(h^{-1}, 1) = (1, 1)$. So $(h, k)^{-1} = (1, k^{-1})(h^{-1}, 1) = (\phi_{k^{-1}}(h^{-1}), k^{-1})$.
3, Associativity: $((h_1, k_1)(h_2, k_2))(h_3, k_3) = (h_1\phi_{k_1}(h_2), k_1k_2)(h_3, k_3) = (h_1\phi_{k_1}(h_2)\phi_{k_1k_2}(h_3), k_1k_2k_3) = (h_1\phi_{k_1}(h_2)\phi_{k_1}(\phi_{k_2}(h_3)), k_1k_2k_3) = (h_1\phi_{k_1}(h_2\phi_{k_2}(h_3)), k_1k_2k_3) = (h_1, k_1)(h_2\phi_{k_2}(h_3), k_2k_3) = (h_1, k_1)((h_2, k_2)(h_3, k_3))$.

Example:
The symmetries of the n-gon in the plane is also known as D_n, the dihedral group of order $2n$. This group can be generated from a rotation counterclockwise by $2\pi/n$, ρ and a reflection about a line f.
If we consider the triangle: $D_3 = \{1, \rho, \rho^2, f, \rho f, \rho^2 f\}$. The defining characteristic of the group law is that $f\rho = \rho^2 f = \rho^{-1} f$. The two subgroups are the rotations $\{1, \rho, \rho^2\}$ and the reflections $\{1, f\}$. The rotations form a normal subgroup, as $f\rho f^{-1} = \rho^{-1}$ (Exercise). Note that $D_3 = \{1, \rho, \rho^2\} \cdot \{1, f\}$.
We can also write $D_n \cong (\mathbb{Z}/n\mathbb{Z}) \underset{\phi}{\rtimes} \{-1, 1\}$ with $\phi : \{-1, 1\} \to \text{Aut}(\mathbb{Z}/n\mathbb{Z})$ defined as $1 \mapsto id$ and $-1 \mapsto \phi_{-1}$ such that $f\rho^a f^{-1} = \rho^{\phi_{-1}(a)}$. Since $f\rho^a f^{-1} = \underbrace{f\rho f^{-1} \cdot f\rho f^{-1} \cdots f\rho f^{-1}}_{(a \text{ times})} = \rho^{-a}$, $-1 \mapsto f(a) = -a$.

We now consider the Bij$(\mathbb{R}^2, \mathbb{R}^2)$, the set of all bijections from $\mathbb{R}^2$ to itself. We examine subgroups of translations and rotations (defined as $T = \{t_{a,b} \mid a, b \in \mathbb{R}\} \cong \mathbb{R} \times \mathbb{R}$ with $t_{a,b}(x, y) = (x + a, y + b)$ and $R = \{\rho_\theta \mid \theta \in [0, 2\pi]\} \cong \mathbb{R}/2\pi\mathbb{Z}$ with $\rho_\theta = (x\cos\theta - y\sin\theta, x\sin\theta + y\cos\theta)$. Note that this form for ρ_θ comes from converting from the form in polar coordinates $(\rho_\theta(r, \psi) = (r, \psi + \theta))$ into Cartesian coordinates : $\rho_\theta(x, y) = (r\cos(\psi + \theta), r\sin(\psi + \theta)) = (r\cos\psi\cos\theta - r\sin\psi\sin\theta, r\cos\psi\sin\theta + r\sin\psi\cos\theta) = (x\cos\theta - y\sin\theta, x\sin\theta + y\cos\theta)$.

Claim: TR is a subgroup of Bij$(\mathbb{R}^2, \mathbb{R}^2)$.
Proof: It suffices to show that $RT \subset TR$, as then $TRTR \subset TTRR \subset TR$, so TR is closed under multiplication. We consider an element $\rho_\theta t_{a,b}$. Then $\rho_\theta t_{a,b}(x, y) = ((x + a)\cos\theta - (y + b)\sin\theta,\ (x + a)\sin\theta + (y + b)\cos\theta) = (x\cos\theta - y\sin\theta + a\cos\theta - b\sin\theta,\ x\sin\theta + y\cos\theta + a\sin\theta + b\cos\theta) = t_{\rho_\theta(a,b)}(x\cos\theta - y\sin\theta,\ x\sin\theta + y\cos\theta) = t_{\rho_\theta(a,b)}\rho_\theta \in TR$.

We conclude that TR is a group and is isomorphic to $(\mathbb{R} \times \mathbb{R}) \underset{\phi}{\rtimes} (\mathbb{R}/2\pi\mathbb{Z})$ with $\phi : (\mathbb{R}/2\pi\mathbb{Z}) \to \text{Aut}(\mathbb{R} \times \mathbb{R})$ defined by $\theta \mapsto \phi(\theta)(a, b) = (a\cos\theta - b\sin\theta, a\sin\theta + b\cos\theta)$.

Claim (for later): TR is $\mathrm{Isom}^+(\mathbb{R}^2)$, the orientation-preserving isometries of $\mathbb{R}^2$.

Now we consider $F = \{id, \text{ reflect about } x \text{ axis}\} \cong \{1, -1\}$.
Claim: TRF is a subgroup of $\mathrm{Bij}(\mathbb{R}^2, \mathbb{R}^2)$.
Proof: It suffices to show that $FTR = TRF$, as then $TRFTRF \subset TT(RF)(RF) \subset TRF$, so TRF is closed under multiplication. We can show that $F(TR) = (TR)F$ by showing $f \circ t_{a,b} \circ \rho_\theta = t_{a,-b} \circ \rho_{-\theta} \circ f$. (Exercise.)

We conclude that $TRF \cong ((\mathbb{R} \times \mathbb{R}) \underset{\phi}{\rtimes} (\mathbb{R}/2\pi\mathbb{Z})) \underset{\psi}{\rtimes} \mathbb{Z}/2\mathbb{Z}$ with ϕ defined in the same way as before and $\psi : \mathbb{Z}/2\mathbb{Z} \to \mathrm{Aut}((\mathbb{R} \times \mathbb{R}) \underset{\phi}{\rtimes} (\mathbb{R}/2\pi\mathbb{Z}))$ defined with $1 \mapsto id$ and $-1 \mapsto \psi_1((a,b),\theta) = ((a,-b),-\theta)$.

Lecture 10
September 25

Rings:

Definition: A commutative ring is a set R with two operations $+, \cdot$ and two distinguished elements $0, 1$ $(0 \neq 1)$ such that
1. $(R, +)$ is a commutative group with identity 0.
2. $(R, \cdot)$ is a commutative monoid with identity 1.
3. $\forall\ a \in R, m_a : R \to R$ defined with $a \mapsto ax$ is a group homomorphism of $(R, +)$.

These properties of a ring can also be written in the following way:
Identity under $+ : 0 + a = a + 0 = a$
Associativity under $+ : (a + b) + c = a + (b + c)$
Commutativity under $+ : a + b = b + a$
Invertibility under $+ : \forall\ a, \exists(-a)$ such that $a + (-a) = (-a) + a = 0$
Identity under $\cdot : 1 \cdot a = a \cdot 1 = a$
Associativity under $\cdot : (a \cdot b) \cdot c = a \cdot (b \cdot c)$
Commutativity under $\cdot : a \cdot b = b \cdot a$
Distributivity of $\cdot$ over $+ : a \cdot (b + c) = a \cdot b + a \cdot c$.

Examples of Rings:
$\mathbb{Z}$, $\mathbb{Z}/n\mathbb{Z}$ with $+, \cdot$ mod n, $\mathbb{Z}[x]$: polynomials in x with integer coefficients, $\mathbb{R}[x]$, $\mathbb{Z}[x, y]$.

Fields:

Definition: A field is a set with distinguished elements $0, 1$ and operations $+, \cdot$ such that
1. $(F, +)$ is a commutative group with identity 0.
2. $(F - \{0\}, \cdot)$ is a commutative group with identity 1.
3. $\forall\ a \in F, m_a : F \to F$ defined with $a \mapsto ax$ is a group homomorphism of $(F, +)$.

Fields have the same properties of rings listed above, but also obey the following:
Invertibility under $\cdot$: $\forall\ a \in F, a \neq 0, \exists\ a^{-1}$ such that $a^{-1} \cdot a = a \cdot a^{-1} = 1$.

Examples of Fields:
$\mathbb{Q}$: the rational numbers, $\mathbb{R}$: the real numbers, $\mathbb{C}$: the complex numbers, $\mathbb{R}(x)$: the rational functions of the form polynomial / polynomial, $\mathbb{Q}[\sqrt{2}] = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\} \subset \mathbb{R} \subset \mathbb{C}$.

We shall check this last example:
Closure under $\cdot$: $(a + b\sqrt{2})(c + d\sqrt{2}) = (ac + 2bd) + (ad + bc)\sqrt{2}$
Closure under Inversion: $(a+b\sqrt{2})^{-1} = (a-b\sqrt{2})/(a^2-2b^2) = (a/(a^2-2b^2))-(b/(a^2-2b^2))\sqrt{2}$

We shall also check the complex numbers, which can also be expressed as $\mathbb{C} = \mathbb{R}[i] = \{a + bi \mid a, b \in \mathbb{R}\}$:
Closure under $\cdot$: $(a + bi)(c + di) = (ab - cd) + i(ad + bc)$
Closure under Inversion: $(a + bi)^{-1} = (a - bi)/(a^2 + b^2) = (a/(a^2 + b^2)) - (b/(a^2 - 2b^2))i$

In addition, $\mathbb{Z}/p\mathbb{Z}$ is a field with p prime because:
1. $\mathbb{Z}/p\mathbb{Z}$ is a group under $+$.
2. $(\mathbb{Z}/p\mathbb{Z})^*$ is a group under $\cdot$.

3. $m_a : \mathbb{Z}/p\mathbb{Z} \to \mathbb{Z}/p\mathbb{Z}$ is a homomorphism, as we saw earlier that $\text{Aut}(\mathbb{Z}/p\mathbb{Z}, +) \cong (\mathbb{Z}/p\mathbb{Z})^*$

Examples and Non-Examples:
$\mathbb{Z}/2\mathbb{Z} = \{0, 1\}$ is a field with multiplication and addition modulo 2.
$\mathbb{Z}/4\mathbb{Z}$ is not a field because 2 has no multiplicative inverse. Even worse, $2 \cdot 2 \equiv 0 \bmod 4$, so 2 is a zero divisor.

For a four-element field, consider $F_4 = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ as an additive group. Its elements are $\{0, 0\}, \{1, 0\}, \{0, 1\}, \{1, 1\}$. $\{0, 0\}$ is the additive identity and $\{1, 1\}$ is the multiplicative identity. $F_4 - \{0\} = \{1, 0\}, \{0, 1\}, \{1, 1\} = \{1, x, x^2\}$ must be the cyclic group C_3. We also check the distributive law. We see that $\text{Aut}(F_4) \cong S_3$, so the three maps m_1, m_x, m_{x^2} each fix $(0, 0)$ and permute the other elements.

Vector Spaces over F:

Definition: A vector space over F is an abelian group V with operation $+$ and identity 1 and a map (scalar multiplication) : $F \times V \to V$, defined with $(a, v) \mapsto m_a(v)$, such that
1. $m_a(v + w) = m_a(v) + m_a(w)$
2. $m_{ab}(v) = m_a \circ m_b(v)$.
Equivalently, we can define it as a group and a homomorphism : $F \to \text{Aut}(V)$ defined with $a \mapsto m_a$.

Definition: Given $W \subset V$, W is a subspace if it is a subgroup such that $m_a|_W : W \to W \ \forall \ a \in F$.

Definition: If V, W are two vector spaces over F, A is a linear map if $A : V \to W$ is a homomorphism of $(V, +)$ to $(W, +)$, i.e., $A(v + w) = A(v) + A(w)$ and such that $m_a \circ A = A \circ m_a$ and $aA(v) = A(av)$. Another way to fulfill the last two conditions is that this diagram commutes:

$$\begin{tikzcd}
V \arrow[r, "A"] \arrow[d, "m_a"'] & W \arrow[d, "m_a"] \\
V \arrow[r, "A"'] & W
\end{tikzcd}.$$

An isomorphic map of vector spaces is a linear map with an inverse linear map.

Quotients:

Let V and W be vector spaces over F with $W \subset V$. Then V/W is a vector space over F. We wish to show that its quotient V/W is a group. We choose $\pi : V \to V/W$ as a quotient map (also a group homomorphism). We know that $W \subset \ker(\pi \circ m_a)$. Thus by the Universal Property of the Quotient, $\exists! \ m_a^W : V/W \to V/W$ such that $m_a^W \circ \pi = \pi \circ m_a$. In other words, the following diagram commutes:

$$\begin{tikzcd}
V \arrow[r, "m_a"] \arrow[d, "\pi"'] & V \arrow[d, "\pi"] \\
V/W \arrow[r, "\exists! \ m_a^W"'] & V/W
\end{tikzcd}.$$

We also need to check that $m_{ab}^W = m_a^W \circ m_b^W$ works as well.

Proof: The diagram commutes:

$$\begin{tikzcd}
V \arrow[r, "m_a"] \arrow[d, "\pi"'] & V \arrow[r, "m_b"] \arrow[d, "\pi"] & V \arrow[d, "\pi"] \\
V/W \arrow[r, "\exists!\ m_a^W"'] & V/W \arrow[r, "\exists!\ m_b^W"'] & V/W
\end{tikzcd}.$$

Example of a Vector Space:

$F^n = \underset{n\text{ times}}{F \times \cdots \times F}$. This is a direct product of additive groups. Scalar multiplication is defined with $a(x_1, x_2, \ldots) = (ax_1, ax_2, \ldots)$

Three Definitions:
A spanning set is a surjection $\phi : F^n \to V$.
A linearly independent set is an injection $\phi : F^n \to V$.
A basis is an isomorphism $\phi : F^n \to V$.

Lecture 11
September 27

More on Vector Spaces (Bases, Subspaces Dimensions):

Remarks on Vector Spaces:
Claim: Given G, H two abelian groups, $\text{Hom}(G, H) = \{\phi : G \to H \mid \phi \text{ is a group homomorphism}\}$ is an abelian group under part-wise additions.
Proof: Let $\phi, \psi : G \to H$. Then $(\phi + \psi)(g) = \phi(g) + \psi(g) \in H$ and $(\phi + \psi)(g_1 + g_2) = \phi(g_1) + \psi(g_1) + \phi(g_2) + \psi(g_2) = (\phi + \psi)(g_1) + (\phi + \psi)(g_2)$. Thus $\phi + \psi$ is a homomorphism.

Furthermore: $\text{Hom}(G, G)$ with G abelian is a non-commutative ring with addition as above and multiplication being composition of homomorphisms (which is non-commutative).
A map from F to $\text{Hom}(V)$ is a ring homomorphism, i.e. with m_a being a group homomorphism, $m_{a+b} = m_a + m_b$ and $m_{a+b} = m_a + m_b$.

A list of elements $\underline{v} = (v_1, \ldots, v_n)$ corresponds to a map $\phi_{\underline{v}} : F^n \to V$ defined with $e_i \mapsto v_i$. (Here e_i corresponds to a n-element list of zeroes with a one in the ith spot. It is often represented by a column vector.)

Thus:
$\underline{\text{v}}$ is a linearly independent set if $\phi_{\underline{v}}$ is an injection, i.e. $\sum a_i v_i$ with $a_i \in F$ has no repeats in $\underline{v}$.
$\underline{\text{v}}$ is a spanning set if $\phi_{\underline{v}}$ is a surjection, i.e. $\sum a_i v_i$ with $a_i \in F$ contains every element of $\underline{v}$.
$\underline{\text{v}}$ is a basis if $\phi_{\underline{v}}$ is an isomorphism, i.e. $\sum a_i v_i$ with $a_i \in F$ contains every element of $\underline{v}$ exactly once.

Proposition: The following are equivalent:
1. $(v_1, \ldots, v_n)$ forms a basis.
2. $(v_1, \ldots, v_n)$ spans V and no proper subcollection spans.
3. $(v_1, \ldots, v_n)$ is a linearly independent set and $\forall\ v \in V$, $(v, v_1, \ldots, v_n)$ is not a linearly independent set.
Proof:
$1 \implies 2$ and $1 \implies 3$ by definition.
$2 \implies 1$: Suppose $(v_1, \ldots, v_n)$ is not linearly independent, i.e. $\sum a_i v_i = 0$ with not all $a_i = 0$. Without loss of generality, let $a_1 \neq 0$. Then $v_1 = (\sum_{i=2}^n a_i v_i)/a_1$. Then $(v_2, \ldots v_n)$ spans V, which is a contradiction of our assumption that no proper subcollection spans V. Thus $(v_1, \ldots, v_n)$ must be linearly independent and thus forms a basis.
$3 \implies 1$: We can show that $(v_1, \ldots, v_n)$ spans, i.e. given any $v \in V$, we can express v as a linear combination of the v_i. $(v, v_1, \ldots, v_n)$ is not linearly independent, so $av + \sum a_i v_i = 0$ with not all $a_i = 0$. If $a = 0$, then $(v_1, \ldots, v_n)$ is not linearly independent, which is a contradiction. Thus $a \neq 0$ and $v = (-\sum a_i v_i)/a$. Thus $(v_1, \ldots, v_n)$ spans V and is thus a basis.

Corollary: If V is finitely generated as a vector space (i.e. the same finite collection spans), then it has a basis.
Proof: We take a spanning set and find the minimal spanning subset by induction. By 2, this is a basis.

Corollary: Any finitely generated vector space is isomorphic to F^n.
Proof: Exercise.

Dimension:

Theorem: Given a spanning set $(v_1, \ldots, v_n)$ and a linearly independent set $(w_1, \ldots, w_m)$ in V, then $n \geq m$

Proof: By induction on m. The base case of $m = 0$ is trivial. In the inductive step, we assume that this holds for smaller m. We write w_1 as a sum of $a_i v_i$. At least one of the a_i is not 0. Without loss of generality, let $a_1 \neq 0$. Then we can write v_1 in terms of the the remaining v_i, i.e. $v_1 = (w_1 - \sum_{i=2}^n a_i v_i)/a)$. So $(w, v_2, \ldots, v_n)$ is a spanning set.

We now consider $V/\langle w_1 \rangle$ and the surjective map $\pi : V \twoheadrightarrow V/\langle w_1 \rangle$. We call $\langle w_1 \rangle = \{aw \mid a \in F\} \subset V$ "the subspace generated by w_1."

Claim:
1. $(\overline{v}_2, \ldots, \overline{v}_n)$ spans $V/\langle w \rangle$.
2. $(\overline{w}_2, \ldots, \overline{w}_m)$ is linearly independent.
Here $\overline{v} = \pi(v)$.

Proof:
1. Given $\pi(v) \in V/\langle w_1 \rangle$ (π is surjective, so this a general element), we want to express $\pi(v)$ as a linear combination of the $\overline{v}_i$. We know from constructing our previous spanning set that $v = a_1 w_1 + \sum_{i=2}^n a_i v_i$. Thus $\pi(v) = \sum_{i=2}^n a_i v_i$ and $(\overline{v}_2, \ldots, \overline{v}_n)$ spans $V/\langle w \rangle$.
2. Suppose not. Then $\sum_{i=2}^m a_i \pi(w_i) = 0 \implies \pi(\sum_{i=2}^m a_i w_i) = 0 \implies \sum_{i=2}^m a_i w_i \in \langle w_1 \rangle \implies \sum_{i=2}^m a_i w_i = a w_1$. Thus we have expressed w_1 in terms of the other w_i, which contradicts our earlier definition of $(w_1, \ldots, w_m)$ as a linearly independent set. Thus $(\overline{w}_2, \ldots, \overline{w}_m)$ is linearly independent.

Corollary: All bases of a finitely generated vector space V have the same size. (This is known as the dimension of V).

Proof: Each basis spans and is linearly independent, so $m \leq n$ and $n \leq m$, so $m = n$.

Corollary: If $W \subset V$, then $\dim(W) \leq \dim(V)$, with equality if and only if $W = V$ (assuming V is finite dimensional).

Proof: We can extend a basis of W, which is a linearly independent set in V to a basis of V by adding elements that are not spanned.

Corollary: $F^n \cong F^m \Leftrightarrow m = n$

Theorem: If $W \subset V$, then $\dim(W) + \dim(V/W) = \dim(V)$.

Sketch of Proof:

Claim: Given $(w_1, \ldots, w_m)$ as a basis for W and $(u_1, \ldots, u_n)$ such that $(\pi(u_1), \ldots, \pi(u_n))$ is a basis for V/W. Then $(w_1, \ldots, w_m, u_1, \ldots, u_n)$ is a basis for V.

Suppose $T : V \to W$ is a linear map transformation. The kernel and the image of this transformation are subspaces of V and W, respectively.

Corollary (Rank-Nullity Theorem): $\dim(\ker(T)) + \dim(\operatorname{im}(T)) = \dim(V)$.

Proof: We can express T as a surjective map from V to $\operatorname{im}(T)$. The First Isomorphism Theorem then tells us that $V/\ker(T) \cong \operatorname{im}(T)$. Let $\overline{T} : V/\ker(T) \to \operatorname{im}(T)$ be the isomorphism. Then $\dim(\ker(T)) + \dim(\operatorname{im}(T)) = \dim(V)$ by the previous theorem. The following diagram will also commute:

$$\begin{tikzcd}
V \arrow[r, "T"] \arrow[d, "\pi"'] & \operatorname{im}(T) \\
V/\ker(T) \arrow[ur, "\overline{T}"'] &
\end{tikzcd}.$$

Remark: In fact, $\overline{T}$ is linear and is an isomorphism of vector spaces. We know that $\overline{T}(\pi(v)) = T(v)$ by definition. Then $\overline{T}(a\pi(v)) = \overline{T}(\pi(av)) = T(av) = aT(v) = a\overline{T}(\pi(v))$. $\overline{T}$ is bijective because it is an isomorphism of abelian groups. We can see that T^{-1} is also linear: $\overline{T}^{-1}(w) = v \implies \overline{T}(av) = aw \implies \overline{T}^{-1}(aw) = av = a\overline{T}^{-1}(v)$.

Lecture 12
September 30

Matrix of a Linear Transformation:

We consider the map $T : V \to W$, which we say is F-linear, where V, W are finite-dimensional vector spaces over F with dimensions n and m. We can choose bases for V and W by using the following isomorphisms: $\phi : F^n \xrightarrow{\cong} V$ with $e_i \mapsto \phi(e_i) = v_i$ for $1 \leq i \leq n$ and $\psi : F^m \to W$ with $e_i \mapsto \psi(e_i) = w_i$ for $1 \leq i \leq m$. Note that $\{v_i \mid 1 \leq i \leq n\}$ and $\{w_i \mid 1 \leq i \leq m\}$ are bases of V and W, respectively. We can also express this with a diagram:

$$\begin{tikzcd}
F^n \arrow[r, "A"] \arrow[d, "\phi"', "\cong"] & F^m \arrow[d, "\psi", "\cong"'] \\
V \arrow[r, "T"] & W
\end{tikzcd}.$$

We define the map $A : F^n \to F^m$ as $A = \psi^{-1} \circ T \circ \phi$ because the diagram must commute. Equivalently, given A, we can define $T : V \to W$ as $T = \psi \circ A \circ \phi^{-1}$

Thus if we are given a linear map $A : F^n \to F^m$, it is completely determined by its values on the basis, i.e. $\{A(e_k) \mid 1 \leq k \leq n\}$. This makes sense, because any $v \in V$ can be expressed as $v = \sum_k c_k e_k$ and $A(v) = \sum_k c_k A(e_k)$, because A is linear.
We can also express each the value A takes on each basis vector in the basis of F^m, i.e. $A(e_k) = \sum_j A_{jk} e_j$, where $\{e_j \mid 1 \leq j \leq m\}$ is the basis for F^m. In matrix form this looks like:

$$\underbrace{\begin{bmatrix} & A_{1k} & \\ & \vdots & \\ & A_{mk} & \end{bmatrix}}_{m\times n} \cdot \underbrace{\begin{bmatrix} 0 \\ \vdots \\ 1 \\ \vdots \\ 0 \end{bmatrix}}_{n\times 1} = \underbrace{\begin{bmatrix} A_{1k} \\ \vdots \\ A_{mk} \end{bmatrix}}_{m\times 1}.$$

Note that the 1 in the second matrix is in the kth spot, as the matrix represents the basis vector $e_k \in V$.

Now we consider the composition of two linear transformations. We choose $B : F^m \to F^\ell$, so $B \circ A : F^n \to F^\ell$. If we let $\{e_k \mid 1 \leq j \leq m\}$, $\{e_j \mid 1 \leq j \leq m\}$,and $\{e_i \mid 1 \leq j \leq m\}$ be bases of F^n, F^m, and F^ℓ, respectively, we can see how this composition acts on a basis vector of V : $BA(e_k) = B(\sum_j A_{jk} e_j) = \sum_i \sum_j B_{ij} A_{ij} e_i$. If we examine this in matrix form:

$$\underbrace{\begin{bmatrix} & & \\ B_{i1} & \cdots & B_{im} \\ & & \end{bmatrix}}_{\ell\times m} \cdot \underbrace{\begin{bmatrix} & A_{1k} & \\ & \vdots & \\ & A_{mk} & \end{bmatrix}}_{m\times n} \cdot \underbrace{\begin{bmatrix} 0 \\ \vdots \\ 1 \\ \vdots \\ 0 \end{bmatrix}}_{n\times 1} = \underbrace{\begin{bmatrix} (BA)_{1k} \\ \vdots \\ (BA)_{\ell k} \end{bmatrix}}_{\ell\times 1},$$

we find that $(BA)_{ik} = \sum_j B_{ij} A_{jk}$. Thus, once we have fixed a basis, we can view composition of linear functions as analogous to matrix multiplication.

Change of Basis:

Consider the diagram:

$$\begin{tikzcd}
F^n \arrow[rrr, "A = \psi_1^{-1} \circ T \circ \phi_1"] \arrow[dr, "\phi_1", "\cong"'] \arrow[dd, "C = \phi_2^{-1} \circ \phi_1"'] & & & F^m \arrow[dl, "\psi_1"', "\cong"] \arrow[dd, "D = \psi_2^{-1} \circ \psi_1"] \\
& V \arrow[r, "T"] & W & \\
F^n \arrow[rrr, "B = \psi_2^{-1} \circ T \circ \phi_2"] \arrow[ur, "\phi_2", "\cong"'] & & & F^m \arrow[ul, "\psi_2"', "\cong"]
\end{tikzcd}.$$

The linear maps $C : F^n \to F^n$ and $D : F^m \to F^m$ are called the change of basis maps. Their definitions in terms of the isomorphisms come from the requiring that the above diagram commutes. This requirement also gives us another expression for B, namely $B = D \circ A \circ C^{-1}$.

Now we examine the case where $V = W$. The diagram becomes

$$\begin{tikzcd}
F^n \arrow[rrr, "A = \phi_1^{-1} \circ T \circ \phi_1"] \arrow[dr, "\phi_1", "\cong"'] \arrow[dd, "C = \phi_2^{-1} \circ \phi_1"'] & & & F^n \arrow[dl, "\phi_1"', "\cong"] \arrow[dd, "C = \phi_2^{-1} \circ \phi_1"] \\
& V \arrow[r, "T"] & V & \\
F^n \arrow[rrr, "B = \phi_2^{-1} \circ T \circ \phi_2"] \arrow[ur, "\phi_2", "\cong"'] & & & F^n \arrow[ul, "\phi_2"', "\cong"]
\end{tikzcd}.$$

Requiring that this diagrams commutes yields $B = C \circ A \circ C^{-1}$. Thus we see that changing the basis conjugates the matrix representation of the linear map by the change of basis matrix.

Definition: An endomorphism is a homomorphism from an object to itself. If this object is a vector space, then an endomorphism is a linear map.
Note that if an endomorphism is invertible, then it is an automorphism as well. Then set of endomorphisms is denoted $\text{End}(V) = \text{Hom}_F(V, V)$. The general linear group on V is $GL(V) = \{T \in \text{End}(V) \mid T \text{ is invertible}\}$ aka the automorphisms. This could also be written as $GL(F^n)$ or $GL_n(F)$, although this notation technically refers to the matrices associated with these maps.

A big topic is understanding linear transformations up to a change of basis, i.e. up to conjugations by invertible linear transformations. We would like to have a broader understanding of linear transformations independent of a basis. This is equivalent to understanding the conjugacy classes of $GL(V)$ (or even $\text{End}(V)$ under conjugation by elements of $GL(V)$). More on this later.

Claim: Sets of the form $\{x \in G \mid, x = hgh^{-1} \text{ for some } h \in G\}$ partition G.
Proof: Delayed.

Definition: An equivalence relation is a relation $\sim$, (i.e. a subset of $S \times S$, which we

think of as being the set of (a, b) such that $a \sim b$ is true) such that it obeys the following:
1. Reflexivity: $\forall\ a \in S$, $a \sim a$.
2. Symmetry: $\forall\ a, b \in S$, $a \sim b \implies b \sim a$.
3. Transitivity: $\forall\ a, b, c \in S$, $a \sim b, b \sim c \implies a \sim c$.

Proposition: Sets of the form $S_a = \{x \in S \mid a \sim x\}$ partition S.
Proof: Exercise, or see section 2.7.

We now define a conjugation equivalence relation $\sim_{\text{conj}}$ on $G : x \sim_{\text{conj}} y \Leftrightarrow \exists\, h \in G$ such that $x = hyh^{-1}$. If $x \sim_{\text{conj}} y$ we say x and y are conjugate.

Proof from before: Thus the sets of the form $\{x \in G \mid, x = hgh^{-1}$ for some $h \in G\}$ are the partitioning sets for the above equivalence relation. These must partition G by the above proposition. These sets consist of all conjugate elements and are called the conjugacy classes of G.

Examples of Conjugacy Classes:

1. If G is abelian, each conjugacy class is one element.

Remark: $1 \in G$ is always alone, i.e. $\{1\}$ is a conjugacy class. (This actually holds for anything in Center(G)).

2. $S_3 = \{1, (1\ 2), (1\ 3), (2\ 3), (1\ 2\ 3), (1\ 3\ 2)$
The conjugacy classes are $\{1\}, \{(1\ 2), (1\ 3), (2\ 3)\}, \{(1\ 2\ 3), (1\ 3\ 2)\}$. We can quickly see that the third is true by considering the following diagram:

$$\begin{tikzcd}
\{1,2,3\} \arrow[r, "(1\ 2\ 3)"] & \{1,2,3\} \\
\{1,2,3\} \arrow[u, "\substack{1 \mapsto 1 \\ 2 \mapsto 3 \\ 3 \mapsto 2}"] \arrow[r, "(1\ 3\ 2)"] & \{1,2,3\} \arrow[u, "\substack{1 \mapsto 1 \\ 3 \mapsto 2 \\ 2 \mapsto 3}"']
\end{tikzcd},$$

which tells us that $(1\ 2\ 3) = (2\ 3)^{-1}(1\ 3\ 2)(2\ 3) = (2\ 3)(1\ 3\ 2)(2\ 3)$.

Proposition: The conjugacy classes of S_n correspond to ways to partition n into $n = n_1 + n_2 + \cdots + n_k$ without order of the n_i.
Proof: Exercise.

We recall that we wish to find properties of linear transformations in End(V) that have no reference to basis.

One of these is the concept invariant subspaces.
Definition: $W \subset V$ is T-invariant if $\forall\ w \in W, Tx \in W$.

Examples:
Proposition: $\ker(T)$, $\operatorname{im}(T)$, $\ker(T^k)$ and $\operatorname{im}(T^k)$ for any $k \in \mathbb{Z}_{\geq 0}$ are invariant.
Proof:
$\ker(T^k)$: By definition, $v \in \ker(T^k)$ if $T^k(v) = 0$. Then $Tv \in \ker(T^k)$ because $T^k(Tv) =$

$TT^k(v) = T(0) = 0$.

$\mathrm{im}(T^k)$: By definition, $v \in \mathrm{im}(T^k)$ if $\exists$ w such that $T^k(w) = v$. Then $Tw \in \mathrm{im}(T^k)$ because $T^k(T(w)) = T^{k+1}(w) = T(T^k(w)) = T(v)$.

Suppose $Tv = \lambda v$ for some $\lambda \in F$. i.e. v is an eigenvector of T with an eigenvalue of λ. Then $\langle v \rangle = \{av \mid a \in F\}$ is T-invariant.

Lecture 13
October 4

Midterm Problems

3a. Find a nonabelian group of order 21.
We know that there must be an element of order 3 and an element of order 7, i.e. an element in $\mathbb{Z}/3\mathbb{Z}$ and an element in $\mathbb{Z}/7\mathbb{Z}$. However these groups are abelian. One way to negate this is to use a semidirect product $\mathbb{Z}/7\mathbb{Z} \underset{\phi}{\rtimes} \mathbb{Z}/3\mathbb{Z}$. We define $\phi : \mathbb{Z}/3\mathbb{Z} \to \mathrm{Aut}(\mathbb{Z}/7\mathbb{Z})$ with $1 \mapsto m_2$. Another solution is to consider the groups $\{1, x, x^2\}$ and $\{1, y, \ldots y^6\}$, and to choose $\{x^a y^b \mid a \in \mathbb{Z}/3\mathbb{Z},\ b \in \mathbb{Z}/7\mathbb{Z}\}$, but there is a lot to check here to be consistent.

3b. Identify $\mathrm{Aut}(\mathbb{Z}/8\mathbb{Z})$ with a familiar group
We can think of the automorphisms of permutations of the elements, i.e. there is a map $\mathbb{Z}/8\mathbb{Z} \hookrightarrow S_8$.
There is a generator $1 \in \mathbb{Z}/8\mathbb{Z}$. Thus if $\phi : \mathbb{Z}/8\mathbb{Z} \to \mathbb{Z}/8\mathbb{Z}$ is a homomorphism, $\phi(1)$ completely determines ϕ. Thus we have 8 homomorphisms $\phi : \mathbb{Z}/8\mathbb{Z} \to \mathbb{Z}/8\mathbb{Z}$ defined with $1 \mapsto 0, 1, 2, 3, 4, 5, 6, 7$. We call these homomorphisms $m_0, m_1, \ldots m_7$, (multiplication by 0, multiplication by 1, etc.). Which of these are bijections? We examine the kernels. m_0 has the entire set as its kernel. m_2 has a kernel of $\{0, 4\}$, etc. We see that multiplication by an even number with have a nontrivial kernel. Thus only m_1, m_3, m_5, and m_7 are bijective. Now we examine the composition. $m_3 \circ m_3 = m_9 = m_1$, $m_3 \circ m_5 = m_{15} = m_7$, etc. Thus we see that each element has order 2, as m_1 is the identity, and the composition of two distinct non-identity elements yields the third non-identity element. Thus this is the Klein Four Group.

Back to Linear Algebra: Eigenvalues and Eigenvectors

Let V be a finite dimensional vector space over a field F and let $T : V \to V$ be an F-linear map, i.e. $F \in \mathrm{End}(V)$. Note that T is not necessarily invertible.

Definition: $v \neq 0$ is an eigenvector of T with eigenvalue λ if $Tv = \lambda v$.

Remark: If λ is an eigenvalue of T, then is is an eigenvalue of ATA^{-1}, i.e. an eigenvalue is independent of a basis.

Claim: If $v_1, \ldots, v_k$ are eigenvectors with distinct eigenvalues $\lambda_1, \ldots, \lambda_k$. Then $v_1, \ldots, v_k$ are linearly independent.
Proof: We shall induct on k. The base case is trivial, as a single vector is linearly independent. In our inductive step, we suppose that our claim is true for $n < k$, but false for $n = k$. Then $\sum_i^k a_i v_i = 0$ with some $a_i \neq 0$. Without loss of generality, we assume that $a_1 \neq 0$. Then $T(\sum_i^k a_i v_i) = \sum_i^k \lambda_i a_i v_i = 0$. Then we multiply the first equation by λ_1 and subtract it from out second one. This yields $\sum_i^k \lambda_i a_i v_i - \sum_i^k \lambda_1 a_i v_i = \sum_{i=2}^k (\lambda_i - \lambda_1) a_i v_i = 0$. Note that $\lambda_i - \lambda_1 \neq 0$. We now consider that actually at least two elements of $\{a_i \mid 1 \leq i \leq k\}$ must be nonzero, or else this reduces to the base case. Thus at least one element of $\{a_i \mid 2 \leq i \leq k\}$ must be nonzero. Thus the coefficients $(\lambda_i - \lambda_1)a_i$ cannot all be zero. This implies that $v_2, \ldots, v_k$ is not linearly independent, even though the vectors have distinct eigenvalues. This contradicts the inductive step, because we have assumed that this holds for $n < k$. Thus it must hold for $n = k$, i.e. $v_1, \ldots, v_k$ is linearly independent.

Definition: The spectrum of T is Spec(T)= $\{\lambda \in F \mid \lambda$ is an eigenvalue of $T\}$.

Corollary: $|\text{Spec}(T)| \leq |\dim(V)|$.

Remark: Spec(T) can be empty, e.g. $V = \mathbb{R}^2,\ F = \mathbb{R},\ T = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}$. Here T is is a rotation by $\pi/2$, which has no eigenvectors and thus no eigenvalues.

Definition: A field F is algebraically closed if, given any polynomial over F, i.e. $p(x) = a_0 + a_1 x + \cdots + a_k x^k$ with $k \geq 1,\ a_k \neq 0$, then there exists $c \in F$ such that $p(c) = 0$.

Examples:

$\mathbb{R}$ is not algebraically closed, let $p(x) = x^2 + 1$. $\mathbb{C}$ is by the Fundamental Theorem of Algebra, which we will not prove here.

What about $F_p = \mathbb{Z}/p\mathbb{Z}$? It is not.
Proof: Consider the map $\Phi : (\mathbb{Z}/p\mathbb{Z})^* \to (\mathbb{Z}/p\mathbb{Z})^*$ given by $a \mapsto a^2$. This a homomorphism, as $(ab)^2 = a^2 b^2$.

Subclaim: The only $a \in \mathbb{Z}/p\mathbb{Z}$ such that $a^2 = 1$ are ± 1.
Proof: Suppose $p \mid a^2 - 1$. Then $p \mid (a+1)(a-1)$, so $p \mid a+1$ or $p \mid a-1$. This corresponds to $a = \pm 1$. (Note that if $p = 2,\ 1 \equiv -1$).
Since $|\ker(\Phi)| \cdot |\text{im}(\Phi)| = p-1$ and $|\ker(\Phi)| = 2$ this means that the image of Φ only contains half the elements of $(\mathbb{Z}/p\mathbb{Z})^*$.

Corollary: There exist $(p-1)/2$ values of $c \in \mathbb{Z}/p\mathbb{Z}$ such that $x^2 - c = 0$ has no solutions mod p.

Proposition: If $p(x) = a_0 + a_1 x + \cdots + a_k x^k\ k \geq 1,\ a_k \neq 0$ is a polynomial of degree of at least 1 over an algebraically closed field, then there exists $r_1, \ldots, r_k$ (possibly with repeats) such that $p(x) = d \prod_{i=i}^{k} (x - r_i)$.
Proof: First we need to know how to divide with remainder: Given $p(x),\ f(x)$, there exist polynomials $q(x),\ r(x)$ with $\deg(r(x)) \leq \deg(f(x))$ such that $p(x) = q(x) \cdot f(x) + r(x)$ (Proof as Exercise).
Now suppose r_1 is a root. Then divide by $x - r_1 : p(x) = q(x)(x - r_1) + c$. Note $c = p(r_1) = 0$. We then induct on the degree of p.

Lecture 14
October 7

More on Eigenvalues

Proposition: Any endomorphism $T \in \mathrm{End}(V)$ with V a finite-dimensional vector space over F, where F is algebraically closed (e.g. $\mathbb{C}$), has an eigenvalue.
Proof: Let $\dim(V) = n$. So if we take some $v \in V$, $v \neq 0$, then $v, Tv, T^2, \dots T^n v$ can't be linearly independent, as it is a list of $n+1$ vectors. Then there exists a set $\{a_0, a_1, \dots, a_n\}$ with not all $a_i = 0$ such that $a_0 v + a_1 Tv + \cdots + a_n T^n v = 0$. Note that a_0 can't be the only nonzero coefficient either, because $v \neq 0$. Now let k be the largest index such that $a_k \neq 0$. We then have $a_0 v + a_1 Tv + \cdots + a_k T^k v = 0$ with $a_k \neq 0$ $k \geq 1$. Consider $p(x) = a_0 + a_1 x + \cdots + a_k x^k = 0$, a polynomial over F. F is algebraically closed, so $\exists$ $\{\lambda_1, \dots \lambda_k\}$ (not necessarily distinct) and $\exists$ $c \in F, c \neq 0$ such that $p(x) = c(x - \lambda_1)(x - \lambda_2) \cdots (x - \lambda_k)$. Note that $c = a_k$. Now let $P(T) = a_0 I + a_1 T + \cdots + a_k T^k \in \mathrm{End}(V)$, a linear map from V to V. We have $P(T)v = 0, v \neq 0$. We also have $P(T) = c(T - \lambda_1 I)(T - \lambda_2 I) \cdots (T - \lambda_k I)$, so $c(T - \lambda_1 I)(T - \lambda_2 I) \cdots (T - \lambda_k I)v = 0$. Thus $\exists$ $j \in [1, k]$ such that $T - \lambda_j I$ has a nontrivial kernel. We take $w \in \ker(T - \lambda_j I)$. Then $Tw - \lambda_j w = 0$, so $Tw = \lambda_j w$.

Toward Jordan Normal Form

We'll show (over an algebraically closed field F and a finite-dimensional vector space V over F) that any $T \in \mathrm{End}(V)$ has a decomposition $T = T^{\text{diag}} + T^{\text{nilp}}$ (diagonalizable and nilpotent).

Definition: A linear map T is diagonalizable if it has a basis of eigenvectors, i.e. there exists a basis such that in this basis the matrix for T is diagonal, with the eigenvalues along the diagonal.

Definition: A linear map T is nilpotent if $\exists$ $k \in \mathbb{Z}_{\geq 1}$ such that $T^k = 0$.

Example:

$$A \to \begin{bmatrix} 0 & 3 & 7 \\ 0 & 0 & 2 \\ 0 & 0 & 0 \end{bmatrix} \qquad A^2 \to \begin{bmatrix} 0 & 0 & 6 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix} \qquad A^3 \to \begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}$$

More on Invariant Subspaces

Recall that $W \subset V$ is T-invariant if $Tw \in W$ $\forall$ $w \in W$.

Examples:
-$\langle v \rangle$ (the subspace generated by v) with v being an eigenvector of T.
-$\ker(T)$, and in fact $\ker(T^k)$ for any $k \in \mathbb{Z}_{\geq 0}$
-$\mathrm{im}(T)$, and in fact $\mathrm{im}(T^k)$ for any $k \in \mathbb{Z}_{\geq 0}$

Note that $V \supset \mathrm{im}(T) \supset \mathrm{im}(T^2) \supset \cdots \supset \mathrm{im}(T^k) \supset \mathrm{im}(T^{k+1})$

Claim: If $n = \dim(V)$ and $k \in \mathbb{Z}_{\geq 0}$, then $\mathrm{im}(T^n) = \mathrm{im}(T^{n+k})$ and T is invertible on this $\mathrm{im}(T^n)$.

Proof: Look at the smallest ℓ such that $\operatorname{im}(T^\ell) = \operatorname{im}(T^{\ell+1})$. (Such an ℓ exists because $\operatorname{im}(T^\ell) \supsetneq \operatorname{im}(T^{\ell+1})$ can only happen for at most n values of ℓ). Then $T|_{\operatorname{im}(T^\ell)}$ is invertible, and we see that $\operatorname{im}(T^\ell) = \operatorname{im}(T^{\ell+k})$ for all $k \geq 0$. So $\operatorname{im}(T^{\dim(V)}) = \operatorname{im}(T^{\dim(V)+k}),\ k \geq 0$. Also, consider $0 \in \ker(T) \subset \ker(T^2) \subset \cdots$. This must stabilize (i.e., become a sequence of equality and not subsumption) at $\ker(T^{\dim(V)})$ or sooner because $\dim(\ker(T^{\dim(V)})) + \dim(\operatorname{im}(T^{\dim(V)})) = \dim(V)$ by Rank-Nullity.

Example:

$$T \to \begin{bmatrix} 2 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{bmatrix} \qquad T^2 \to \begin{bmatrix} 4 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix} \qquad T^3 \to \begin{bmatrix} 8 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}$$

We can derive the following.
$\ker(T) = \{(0, b, 0, 0)\}$ and $\operatorname{im}(T) = \{(a, b, c, 0)\}$
$\ker(T^2) = \{(0, b, c, 0)\}$ and $\operatorname{im}(T^2) = \{(a, b, 0, 0)\}$
$\ker(T^3) = \{(0, b, c, d)\}$ and $\operatorname{im}(T^3) = \{(a, 0, 0, 0)\}$.

Lecture 15
October 9

Direct Sums

Definition: Given V, W, two vector spaces over F, the direct sum $V \oplus W = \{v + w \mid v \in V,\ w \in W\}$ is another vector space over F with addition and scalar multiplication.

We can also define $\bigoplus_{i=1}^{n} V_i$ similarly. We also consider an "internal" sum. Given $W_1, W_2 \subset V$, we can form $W_1 + W_2 = \{v \in V \mid v = w_1 + w_2,\ w_1 \in W_1,\ w_2 \in W_2\}$.

Proposition: If $W_1 \cap W_2 = \{0\}$, then $W_1 + W_2 \cong W_1 \oplus W_2$.
Proof: We form a linear map $T : W_1 \oplus W_2 \to W_1 + W_2 \subset W$ with $w_1 + w_2 \mapsto w_1 + w_2$. This is trivially surjective. To show that it is injective, consider $w_1 + w_2 = w_1' + w_2'$. Then $w_1 - w_1' = w_2 - w_2'$. Then left hand side is in W_1, and the right hand side is in W_2. Then $w_1 - w_1' = w_2 - w_2' = 0 \implies w_1 = w_1'$ and $w_2 = w_2'$.

We also discussed $\ker(T^{\dim(V)})$ and $\operatorname{im}(T^{\dim(V)})$, two T-invariant subspaces. We saw that $0 \subset \ker(T) \subset \ker(T^2) \subset \cdots \subset \ker(T^{\dim(V)})$ and $V \supset \operatorname{im}(T) \supset \operatorname{im}(T^2) \supset \cdots \supset \operatorname{im}(T^{\dim(V)})$. As an example, consider

$$T \to \begin{bmatrix} 2 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{bmatrix} \qquad T^2 \to \begin{bmatrix} 4 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix} \qquad T^4 \to \begin{bmatrix} 16 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}$$

$\ker(T^2) = \operatorname{span}(e_2, e_3)$ and $\ker(T^4) = \operatorname{span}(e_2, e_3, e_4)$.
$\operatorname{im}(T^2) = \operatorname{span}(e_1, e_2)$ and $\operatorname{im}(T^4) = \operatorname{span}(e_1)$.

Claim:
1. $\ker(T^{\dim(V)}) \cap \operatorname{im}(T^{\dim(V)}) = \{0\}$.
2. $V \cong \ker(T^{\dim(V)}) \oplus \operatorname{im}(T^{\dim(V)})$.

Proof:
1. T is nilpotent on $\ker(T^{\dim(V)})$, i.e. $(T\mid_{\ker(T^{\dim(V)})})^k = 0$ for some k. (In fact, $k = \dim(V)$ works). Note that $T\mid_{\ker(T^{\dim(V)})}: \ker(T^{\dim(V)}) \to \ker(T^{\dim(V)})$.
Now consider $T\mid_{\operatorname{im}(T^{\dim(V)})}: \operatorname{im}(T^{\dim(V)}) \to \operatorname{im}(T^{\dim(V)})$. We know that $\operatorname{im}(T^{\dim(V)}) \subset \operatorname{im}(T)$, so $\operatorname{im}(T\mid_{\ker(T^{\dim(V)})}) = \operatorname{im}(T^{\dim(V)})$. Thus by Rank-Nullity, $\ker(T\mid_{\operatorname{im}(T^{\dim(V)})}) = \{0\}$ So here T is invertible on $\operatorname{im}(T^{\dim(V)})$. Thus $\ker(T^{\dim(V)}) \cup \operatorname{im}(T^{\dim(V)}) = \{0\}$ because we can't have a nonzero vector $v \in \operatorname{im}(T^{\dim(V)})$ such that $T^k v = 0$ with T invertible on this subspace because T^k is also invertible. Thus we cannot have a nontrivial intersection.
2. Thus $\ker(T^{\dim(V)}) + \operatorname{im}(T^{\dim(V)}) \cong \ker(T^{\dim(V)}) \oplus \operatorname{im}(T^{\dim(V)})$, and by Rank-Nullity, $\dim(\ker(T^{\dim(V)}) \oplus \operatorname{im}(T^{\dim(V)})) = \dim(V)$. Thus $V \cong \ker(T^{\dim(V)}) \oplus \operatorname{im}(T^{\dim(V)})$.

So far we have V split into two T-invariant subspaces, with T nilpotent on one and invertible on the other. This is equivalent to having the matrix in the following block form:

$$\begin{bmatrix} \text{Nilp} & 0 \\ 0 & \text{Inv} \end{bmatrix}.$$

Definition: The generalized eigenspace $V^{(\lambda)}$ of $T : V \to V$ with eigenvalue λ is defined as $V^{(\lambda)} = \ker((T - \lambda I)^{\dim(V)})$.

Remark: The eigenspace of T with eigenvalue λ is $V_\lambda = \ker(T - \lambda I)$. Note $V_\lambda \subset V^{(\lambda)}$.

Claim: $V^{(\lambda)} \cap V^{(\mu)} = \{0\}$ if $\lambda \neq \mu$.
Proof: We will show that $T - \lambda I$ is nilpotent on $V^{(\lambda)} = \ker((T - \lambda I)^{\dim(V)})$. We first claim that $T - \lambda I$ is invertible on $V^{(\mu)}$. We know that $V^{(\mu)}$ is $(T - \mu I)$-invariant and also invariant under cI for any c. So it is also $(T - \lambda I)$-invariant and T-invariant. We can use this to find the inverse of $T - \lambda I$. We know that $T - \mu I$ is nilpotent on $V^{(\mu)}$. $(T - \lambda I) = (T - \mu I) + (\mu - \lambda)I = c(I - N)$, with $c = \mu - \lambda$ and $N = (-1/(\mu - \lambda))(T - \mu I)$ (which is nilpotent).
Note $(1-x)(1+x+x^2+\cdots+x^{k-1}) = 1-x^k$. so $c(I-N)\frac{1}{c}(I+N+N^2+\cdots+N^{k-1}) = I-N^k = I$. (We chose k such that $N^k = 0$, e.g. $k = \dim(V)$). So $c(I - N) = T - \lambda I$ is invertible on $V^{(\mu)}$ (and its inverse is $\frac{1}{c}(I + N + N^2 + \cdots + N^{k-1})$). Thus $V^{(\lambda)} \cap V^{(\mu)} = \{0\}$ by the same argument as before.

Theorem: If F is algebraically closed, then $V \cong \bigoplus_{\lambda \in \mathrm{Spec}(T)} V^{(\lambda)}$. Here $T = \lambda I + (T - \lambda I)$ (We know that $T - \lambda I$ is nilpotent on $V^{(\lambda)}$). This theorem gives us a matrix in the following block form:

$$\begin{bmatrix} \lambda_1 I + N_1 & 0 & 0 \\ 0 & \lambda_2 I + N_2 & \vdots \\ \vdots & 0 & \ddots & 0 \\ 0 & 0 & \lambda_k I + N_k \end{bmatrix}.$$

Proof: We induct of the number of elements in Spec(T), i.e., the number of distinct eigenvalues. The base case is $\#(\mathrm{Spec}(T)) = 1$. (It can't be 0 if $\dim(V) \geq 1$ because F is algebraically closed). Then $V \cong V^{(\lambda)} \oplus \mathrm{im}((T - \lambda I)^{\dim(V)})$. Consider $T \mid_{\mathrm{im}((T-\lambda I)^{\dim(V)})}$. If $\dim(\mathrm{im}((T - \lambda I)^{\dim(V)}) \geq 1$, then T has an eigenvalue here. This eigenvalue can't be λ, which is a contradiction. The inductive step is $\#(\mathrm{Spec}(T) = k$. Let $\lambda_k \in \mathrm{Spec}(T)$. Then $V \cong V^{(\lambda_k)} \oplus \mathrm{im}(T - \lambda_k I)^{\dim(V)}$. T is invariant on both of these spaces.

Claim: $\mathrm{Spec}(T \mid_{\mathrm{im}((T-\lambda_k I)^{\dim(V)})}) = \{\lambda_1, \ldots, \lambda_{k-1}\}$
Proof: We claim that if v is an eigenvector with eigenvalue λ_j $(j \neq k)$, then $v \in \mathrm{im}((T - \lambda_k I)^{\dim(V)})$. We know that $v = v_1 + v_2$ with $v_1 \in V^{(\lambda_k)}$, and $v_2 \in \mathrm{im}((T - \lambda_k I)^{\dim(V)})$. We're claiming that $v_1 = 0$. Suppose $Tv = \lambda_j v$ then $(T - \lambda_k I)^{\dim(V)} v_1 = 0$ because $(T - \lambda_k I)^{\dim(V)}$ sends v_1 to something in $V^{(\lambda_k)}$ and v_2 to something in $\mathrm{im}(T - \lambda_k I)^{\dim(V)}$. Then $v_1 = 0$ because $v_1 \in V^{(\lambda_j)}$, and $V^{(\lambda)} \cap V^{(\lambda_k)} = \{0\}$. By induction, $\mathrm{im}(T - \lambda_k I)^{\dim(V)} = \bigoplus_{j=1}^{k-1} V^{\lambda_j}$.

Lecture 16
October 11

More on Eigenspace and Nilpotent Maps

Recall our generalized eigenspace $V^{(\lambda)} = \ker((T - \lambda I)^{\dim(V)})$ with $T : V \to V$ a linear map over a field F.

Suppose T is nilpotent. We have $0 \subsetneq \ker(T) \subsetneq \ker(T^2) \subsetneq \cdots \subsetneq \ker(T^n) = \ker(T^{n+1})$.
We also have $\ker(T^{n-1}) \subsetneq \ker(T^n)$, with n the smallest positiver integer such that $\ker(T^n) = \ker(T^{n+1})$. We would like to find a basis for the complement of $\ker(T^{n-1})$. This can be done by choosing $\{v_1, \dots v_\ell\}$ such that $\ker(T^n) \cong \ker(T^{n-1}) \oplus Fv_1 \oplus \cdots \oplus Fv_\ell$. To construct this set, we just take $\ker(T^n)/\ker(T^{n-1})$ and choose a basis $\{u_1, \dots u_\ell\}$. Then we choose $\{v_1, \dots v_\ell\}$ such that $\pi(v_j) = u_j$. with $\pi : \ker(T^n) \to \ker(T^n)/\ker(T^{n-1}))$. We now consider $\{v_1, \dots v_\ell, Tv_1, \dots Tv_\ell, T^2v_1, \dots T^2v_\ell, \dots T^{n-1}v_1, \dots T^{n-1}v_\ell\}$.

Claim: These vectors are linearly independent.
Proof: Suppose they are not. Then we have a nontrivial linear combination equal to zero. Let j be the smallest number such that there exists a nonzero coefficient of some T^jv_i in our linear combination. Then we apply T^{n-j-1} to our linear combination. This will map all T^kv_i with $k > j$ to zero. Thus we find $c_1T^{n-1}v_1 + \cdots + c_\ell T^{n-1}v_\ell = T^{n-1}(c_1v_1 + \dots c_\ell v_\ell) = 0$. This is a contradiction, because $\{v_1, \dots v_\ell\}$ give a basis (via π from before) of $\ker(T^n)/\ker(T^{n-1})$, i.e. they form a basis of the complement of $\ker(T^{n-1})$, so any nontrivial linear combination cannot be in $\ker(T^{n-1})$. Thus $\{v_1, \dots v_\ell, Tv_1, \dots Tv_\ell, T^2v_1, \dots T^2v_\ell, \dots T^{n-1}v_1, \dots T^{n-1}v_\ell\}$ is a linearly independent set. This gives us the following block in the basis $\{T^{n-1}v_1, \dots v_1, \dots T^{n-1}v_\ell, \dots Tv_\ell\}$:

$$\begin{bmatrix}
\begin{bmatrix}0&1&\cdots&0\\0&0&\ddots&0\\\vdots&\vdots&\ddots&1\\0&0&\cdots&0\end{bmatrix} & 0 & \cdots & 0\\
0 & \begin{bmatrix}0&1&\cdots&0\\0&0&\ddots&0\\\vdots&\vdots&\ddots&1\\0&0&\cdots&0\end{bmatrix} & \cdots & 0\\
\vdots & \vdots & \ddots & \vdots\\
0 & 0 & \cdots & \begin{bmatrix}0&1&\cdots&0\\0&0&\ddots&0\\\vdots&\vdots&\ddots&1\\0&0&\cdots&0\end{bmatrix}
\end{bmatrix}$$

where each block along the diagonal corresponds to $\operatorname{span}(T^{n-1}v_1, \dots v_1)$ through $\operatorname{span}(T^{n-1}v_\ell, \dots T^{n-1}v_\ell)$. Note that this block consists of ℓ blocks on the diagonal of size $n \times n$.

Now we consider $\ker(T^{n-2}) \subset \ker(T^{n-1})$. We consider the complement of $\ker(T^{n-2})$ in $\ker(T^{n-1})$ and $\{Tv_1, \dots Tv_\ell\}$. We would like to form a basis for these combined sets. These are both linearly independent by our proof from before and have a trivial intersection. Let this basis be $\{v_1^1, \dots v_\ell^1\}$. We consider $v_1^1, Tv_1^1, \dots T^{n-2}v_1^1$, etc. By the same process as before, we yield another block. We can apply this same argument repeatedly on $\ker(T^{n-j})$, effectively inducting on j, until we reach our conclusion: We have a decomposition of V into blocks of the form

$$\begin{bmatrix} 0 & 1 & \cdots & 0 \\ 0 & 0 & \ddots & 0 \\ \vdots & \vdots & \ddots & 1 \\ 0 & 0 & \cdots & 0 \end{bmatrix}$$

of any size, 1×1 through $n \times n$. The blocks that come from $\ker(T^{n-1})$ would be of size $n-1 \times n-1$, etc. This is the Jordan Canonical Form for nilpotent matrices.

Theorem (Jordan Normal Form): Given $T : V \to V$, an F-linear map with F algebraically closed, then there exists a block decomposition of T (i.e. a direct sum decomposition of V into T-invariant subspaces where the matrix represents the action of T on each of these subspaces) into blocks of the form

$$\begin{bmatrix} \lambda & 1 & \cdots & 0 \\ 0 & \lambda & \ddots & 0 \\ \vdots & \vdots & \ddots & 1 \\ 0 & 0 & \cdots & \lambda \end{bmatrix}.$$

We could have many blocks of this form for a given λ, each of which could have a different size. For example, for a particular λ we could have

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

which consists of one 2×2 block and two 1×1 blocks.

Decomposition into the direct sum of all the blocks with a given λ is canonical. (It's the generalized eigenspace). However, the further decomposition is not canonical, as we had to choose $\{v_1, \ldots v_\ell\}$

Claim: The number of each size blocks with λ's along the diagonal is determined.
Proof: The largest block is of size $n \times n$ where n is the smallest number such that $\ker((T-\lambda I)^n) = \ker((T-\lambda I)^{n+1}$. The number of largest blocks is equal to $\dim(\ker((T\lambda I)^n)) - \dim(\ker((T\lambda I)^{n-1}))$. Then you can pick out the number of any smaller size block using the dimensions of $\ker((T-\lambda I)^k)$. (Rest as Exercise).

Corollary: The conjugacy classes of $n \times n$ matrices over an algebraically closed field are in one-to-one correspondence with Jordan forms.

Corollary: Given $T : V \to V$, if $T^k = I$ over $F = \mathbb{C}$, then T is diagonalizable.
Proof: Consider a Jordan block. We must show that it is size 1 (Delayed).

Lecture 17
October 16

Orthogonal Groups and Isometries (Toward Symmetries of Figures in $\mathbb{R}^2$ or $\mathbb{R}^3$)

Definition: An inner product on $\mathbb{R}^n$ is a bilinear (i.e. linear in each factor when fixing the other) map $\langle , \rangle : \mathbb{R}^n \times \mathbb{R}^n \to \mathbb{R}$ defined as $\langle v, w \rangle = \sum_i^n v_i w_i$.

Definition: The orthogonal group $O(n)$ is the set of all $n \times n$ invertible matrices with real entries that preserve the inner product, i.e. $O(n) = \{A \in GL_n(\mathbb{R}) \mid \langle Av, Aw \rangle = \langle v, w \rangle \ \forall \ v, w \in \mathbb{R}^n\}$.

Claim: The following are equivalent:
1. A is orthogonal, i.e. $\langle Av, Aw \rangle = \langle v, w \rangle \ \forall \ v, w \in \mathbb{R}^n$.
2. $A^T A = I$.
3. $AA^T = I$.
4. The columns of the matrix of A are othogonal.
5. The rows of the matrix of A are othogonal.

Proof:
$2 \implies 1$: Notice that $\langle v, w \rangle = v^T w$, so $\langle Av, Aw \rangle = (Av)^T (Aw) = v^T A^T Aw$.
$1 \implies 2$: Suppose $A^T A = B \neq I$. Then consider $\langle Ae_i, Ae_j \rangle = e_i^T Be_j = B_{ij}$. Since $B \neq I$ there exists i, j such that $B_{ij} \neq \delta_{ij}$. (This is the Kronecker delta, defined as $\delta_{ij} = 1$ for $i = j$ and $\delta_{ij} = 0$ for $i \neq j$). Then $\langle Ae_i, Ae_j \rangle = e_i^T Be_j = B_{ij} \neq \delta_{ij} = e_i^T e_j = \langle e_i, e_j \rangle$. This is a contradiction.
$2 \implies 4$: The entries of $A^T A$ are the inner products of the columns, so the statement $A^T A = I$ is the statement that the columns are orthonormal (with the norm defined as $||v|| = \sqrt{\langle v, v \rangle}$).
$2 \iff 3$: $A^T A = I$ implies that A is injective. By Rank-Nullity, A is surjective. Thus A is invertible, with A^T as its inverse. (This proof works in both directions).
$3 \implies 5$: Same argument as $2 \implies 4$.

Claim: $\det(A) = \pm 1$ if A is orthogonal.
Proof: $1 = \det I = \det(A^T A) = \det(A^T)\det(A) = \det(A)\det(A) = \det(A)^2$. Thus $\det(A) = \pm 1$.

Now we consider a subgroup defined as the kernel of $\det : O(n) \to \{\pm 1, \cdot\}$. This is the special orthogonal group $SO(n) = \{A \in GL_n(\mathbb{R}) \mid A^T A = I \text{ and } \det(A) = 1\}$. We see that $SO(n)$ is a normal subgroup of $O(n)$, as the determinant is a homomorphism. Note that the index of $SO(n)$ is 2.

We shall consider the elements of $SO(n)$. Let $n > 1$ and let

$$A = \begin{bmatrix} 0 & 1 & \\ 1 & 0 & * \\ & * & I_{n-2} \end{bmatrix}$$

Then $A^2 = I$, $A \in O(n)$ $\det(A) = -1$.

Now we let $n \geq 2$. We have $SO(n) \overset{i}{\hookrightarrow} O(n) \overset{\det}{\twoheadrightarrow} \{1, -1\}$ as a short exact sequence ($\text{im}(i) = \ker(\det)$). We see that there exits a $\sigma : \{1, -1\} \to O(n)$ defined with $\sigma(-1) = A$, as $\det \circ \sigma = id_{\{1,-1\}}$. Thus we have a semidirect product $O(n) \cong SO(n) \underset{\phi}{\rtimes} \{\pm 1\}$ with

$\phi : \{1, -1\} \to \operatorname{Aut}(SO(n))$ defined as $\phi(-1)(C) = ACA^{-1}$. Then $AC = ACA^{-1}A$.

Understanding $SO(2)$ and $SO(3)$

$SO(2)$:

If $C \in SO(2)$, $C = \begin{bmatrix} a & * \\ b & * \end{bmatrix}$. The columns of C are orthonormal, so $a^2 + b^2 = 1$. We see that the choices for the second column that are orthogonal to the first column are multiples of $\begin{bmatrix} -b \\ a \end{bmatrix}$ and our choices of norm 1 are $\begin{bmatrix} -b \\ a \end{bmatrix}$ and $\begin{bmatrix} b \\ -a \end{bmatrix}$. The first choice leads to a matrix of determinant 1, so it is our only choice. Note that the second choice yields a matrix in $O(n)$ of determinant -1. Then there exists a unique $\theta \in [0, 2\pi]$ such that $a \in \cos(\theta)$, $b = \sin(\theta)$. Thus $C = \begin{bmatrix} \cos(\theta) & -\sin(\theta) \\ \sin(\theta) & \cos(\theta) \end{bmatrix}$, which is a counterclockwise rotation by θ.

Remark: $\begin{bmatrix} \cos(\theta) & \sin(\theta) \\ \sin(\theta) & -\cos(\theta) \end{bmatrix}$ (which has determinant -1) is a reflection about the line $y = \tan(\theta/2)x$. This form describes all elements of $O(n)$ with determinant -1.

$SO(3)$:

Claim: If $A \in SO(3)$, then there exists a nonzero v such that $Av = v$ (a fixed vector).
Proof: We need to show that $A - I$ has a nontrivial kernel, i.e., we need to show that $\det(A - I) = 0$. We know that $\det(A) = 1$, so $\det(A - I) = \det((A - I)^T) = \det(A^T - I) = \det(A)\det(A^T - I) = \det(A^TA - A) = \det(I - A) = \det(-(A - I)) = (-1)^3 \det(A - I) = -\det(A - I)$. Thus $\det(A - I) = 0$.

This shows that given $A \in SO(3)$, $\exists$ v such that $Av = v$. Because A preserves the inner product, A preserves the plane $\langle v \rangle^{\perp}$ and A is orthogonal on this plane.

Now we change coordinates to $\vec{v}, \vec{w}_1, \vec{w}_2$, an orthogonal triple, i.e. we consider

$$B = \begin{bmatrix} \vec{v} & \vec{w}_1 & \vec{w}_2 \end{bmatrix} A \begin{bmatrix} \vec{v} & \vec{w}_1 & \vec{w}_2 \end{bmatrix}^{-1}.$$

(This fixes e_1 and preserves the span of e_2 and e_3). Thus B has the following form.

$$B = \left[\begin{array}{c|cc} 1 & 0 & 0 \\ \hline 1 & \multicolumn{2}{c}{\multirow{2}{*}{$*$}} \\ 1 & & \end{array}\right]$$

with $* \in O(2)$. We see that $1 = \det(B) = 1 \cdot \det(*)$, so $\det(*) = 1$ and $* \in SO(2)$.
We conclude that any element of $SO(3)$ is a rotation about some axis.

Isometries of $\mathbb{R}^n$

Definition: An isometry of $\mathbb{R}^n$ is a map $\Phi : \mathbb{R}^n \to \mathbb{R}^n$ that preserves distance, i.e. such that $d(\Phi(v), \Phi(w)) = d(v, w)$ with $d(v, w) = ||v - w||$. (Note that Φ is not necessarily linear).

Theorem: $\mathbb{R}^n \underset{\text{mult}}{\rtimes} O(n) \cong \operatorname{Isom}(\mathbb{R}^n)$ with $\text{mult} : O(n) \to \operatorname{Aut}(\mathbb{R}^n)$ defined with $A \mapsto m_A$.
Proof: The isomorphism between these spaces is the map defined with $(\vec{v}, A) \mapsto \tau_{\vec{v}} \circ m_A$. We shall delay showing that it is an isomorphism for now.

Claim: This map is a homomorphism.
Proof: It suffices to show that $m_a \circ \tau_{\vec{v}} = \tau_{m_A(v)} \circ m_A$. This is clearly true, as $(m_A \circ \tau_{\vec{v}})(w) = m_A(w+v) = Aw + Av$ and $(\tau_{m_A(v)} \circ m_A)(w) = \tau_{m_A(v)}(Aw) = Aw + Av$.

Lecture 18
October 18

<u>More on the Isometries of $\mathbb{R}^n$:</u>

We stated the following last lecture:
Theorem: $\mathbb{R}^n \underset{\text{mult}}{\rtimes} O(n) \cong \text{Isom}(\mathbb{R}^n)$ with mult : $O(n) \to \text{Aut}(\mathbb{R}^n)$ defined with $A \mapsto m_A$.
Proof: The isomorphism ϕ between these spaces is the map defined with $\phi(\vec{v}, A) = \tau_{\vec{v}} \circ m_A$. We have already shown that this is a homomorphism. It is also injective, which we can see by examining its kernel. Clearly the only pair composed of a vector and a transformation that will be sent the identity map is the pair $(0, I)$. Now we must show that ϕ is surjective. It suffices to show the following lemma.

Lemma: Any isometry of $\mathbb{R}^n$ that fixes the origin is an orthogonal transformation.
Proof: We must show that an isometry of $\mathbb{R}^n$ (call it Φ) both preserves the inner product and is linear, i.e. $\langle \Phi(p), \Phi(q) \rangle = \langle p, q \rangle$ and $\Phi(cp) = c\Phi(p)$ and $\Phi(p+q) = \Phi(p) + \Phi(q)$.

To prove the first part, we see that $d(p,q)^2 = \langle p-q, p-q \rangle = \langle p,p \rangle + \langle q,q \rangle - 2\langle p,q \rangle$. We also note that $\langle \Phi(p), \Phi(p) \rangle = d(\Phi(p), 0)^2 = \langle p,p \rangle$. So we can claim $(\Phi(p), \Phi(q))^2 = \langle \Phi(p), \Phi(p) \rangle + \langle \Phi(q), \Phi(q) \rangle - 2\langle \Phi(p), \Phi(q) \rangle$. Since Φ is an isometry, $d(p,q) = d(\Phi(p), \Phi(q))$. We have already seen that the first terms (and the second terms by the same logic) of each expression have to be equal. Thus the third terms must also be equal, so $\langle \Phi(p), \Phi(q) \rangle = \langle p, q \rangle$.

To prove the second statement, we consider $\langle \Phi(cp), \Phi(cp) \rangle = \langle cp, cp \rangle = c^2 \langle p, p \rangle$ and $\langle c\Phi(p), c\Phi(p) \rangle = \langle cp, cp \rangle = c^2 \langle p, p \rangle$. Then we take $\langle \Phi(cp) - c\Phi(p), \Phi(cp) - c\Phi(p) \rangle^2 = \langle \Phi(cp), \Phi(cp) \rangle + \langle c\Phi(p), c\Phi(p) \rangle - 2\langle \Phi(cp), c\Phi(p) \rangle$. We also notice $\langle c\Phi(p), \Phi(cp) \rangle = c \langle \Phi(p), \Phi(cp) \rangle = c \langle p, cp \rangle = c^2 \langle p, p \rangle$. The key step occurs in the second equality, where he used the fact that Φ preserves the inner product. Thus $\langle \Phi(cp) - c\Phi(p), \Phi(cp) - c\Phi(p) \rangle^2 = c^2\langle p,p \rangle + c^2\langle p,p \rangle - 2c^2\langle p,p \rangle = 0$ and $\Phi(cp) = c\Phi(p)$. The proof that Φ is additive (i.e. it preserves addition) is left as an exercise, but it follows a similar argument.

Having proved the lemma, we conclude that any isometry of $\mathbb{R}^n$ that fixes the origin is an orthogonal transformation. Thus our map $\phi : \mathbb{R}^n \underset{\text{mult}}{\rtimes} O(n) \to \text{Isom}(\mathbb{R}^n)$ is surjective, as any isomorphism that shifts the origin can simply be written as an orthogonal transformation composed with a translation to the point to which it maps the origin. Thus ϕ is a bijective homomorphism, i.e. an isomorphism and $\mathbb{R}^n \underset{\text{mult}}{\rtimes} O(n) \cong \text{Isom}(\mathbb{R}^n)$.

Now we shall discuss isometries in $\mathbb{R}^2$. We have seen that $O(2) \cong SO(2) \underset{\phi}{\rtimes} \{-1, 1\}$, where $SO(2) = \{\rho_\theta\}$, the set of counterclockwise rotations around the origin by θ, and $\{-1, 1\} = \{r\}$, the set of reflections about the origin. Thus the group elements can all be written as $1, \rho_\theta$, or $\rho_\theta r$ ($\theta \in [0, 2\pi]$).

Now we shall study the finite subgroups of $\text{Isom}(\mathbb{R}^2)$. These will each be the symmetry group of some object in the plane. For example, we consider an equilateral triangle. The isometries consist of three rotations $(1, \rho_{2\pi/3}, \rho_{4\pi/3})$ and 3 reflections $r, \rho_{2\pi/3}r, \rho_{4\pi/3}r$.

Claim: Given $G \subset \text{Isom}(\mathbb{R}^n)$, if G is finite, then there exists some $p \in \mathbb{R}^n$ such that $g(p) = p \;\forall\; g \in G$.
Proof: We know that $g = \tau_{\vec{v}} \circ m_A$. We can pick any point $q \in \mathbb{R}^n$ and apply all the

isometries to it. The average of these points will be our fixed point, which we can think of as a "center of mass." Thus $p = \frac{1}{|G|}\sum_{i=1}^{|G|} g_i(q)$ where $\{g_i\}$ is a list of all the elements in G and q is any point in $\mathbb{R}^n$. Having defined p, we can now show that $g(p) = p$. We write this as $\tau_{\vec{v}} \circ m_A \left(\frac{1}{|G|}\sum_{i=1}^{|G|} g_i(q) \right) = \tau_{\vec{v}} \left(\frac{1}{|G|}\sum_{i=1}^{|G|} A(g_i(q)) \right) = \frac{1}{|G|}\sum_{i=1}^{|G|} \big(A(g_i(q)) + \vec{v}\big) = \frac{1}{|G|}\sum_{i=1}^{|G|} g(g_i(q))$. This is not quite the same expression we had for p, but it is equivalent, because left multiplication by any $g \in G$ is a bijection. Thus it relabels every term in the sum, but the overall sum remains the same and $p = g(p)$. We conclude that if we choose p to be the origin, then G is a finite subgroup of $O(2)$ (because any isometry that fixes the origin is a orthonormal transformation).

Now we shall consider if G contains a reflection. If G has no reflection, then it is a subgroup of $SO(2) \cong \mathbb{R}/2\pi\mathbb{Z}$ and is a group of rotations.
Claim: If G is a finite subgroup of $O(n)$ with no reflection, then $G = \{\rho_{2\pi k/n} \mid k \in 0, 1, \ldots (n-1)\} \cong C_n$ for some n.
Sketch of Proof: We choose the smallest positive rotation and take multiples of it. If there is some rotation that is not a multiple of it, then we can compose them in such a way that yields a smaller rotation, which contradicts our choice of rotation. (Note that this mimics our proof that all subgroups of $\mathbb{Z}$ were of the form $d\mathbb{Z}$).

If there is some reflection $r \in G$, we can then write $O(2) = SO(2) \underset{\phi}{\rtimes} \{1, r\}$. Then elements can be written as ρ_θ or $\rho_\theta r$. We conclude that $G = \{\rho_{2\pi k/n} \mid k \in 0, 1, \ldots (n-1)\} \underset{\phi}{\rtimes} \{1, r\} \cong \mathbb{Z}/n\mathbb{Z} \underset{\phi}{\rtimes} \{-1, 1\} \cong D_n$.

We conclude that finite subgroups of $O(2)$ are either cyclic groups of rotations or dihedral groups of rotations composed with a reflection.

Discrete Subgroups

Definition: $G \subset \text{Isom}(\mathbb{R}^n)$ is a discrete subgroup if there is a lower bound on the length of the vector $\vec{v}$ and the size of the angle θ in any element $\tau_v \rho_\theta r \in G$.

Consider a discrete subgroup $G \subset \mathbb{R}^2 \underset{\text{mult}}{\rtimes} O(2)$. We then consider $G \cap T$, where T is the group of translations.
Claim: We have three possibilities for $G \cap T$:
1. $G \cap T \cong 1$, which we will see implies that G is finite.
2. $G \cap T \cong \mathbb{Z}$, where every translation is a multiple of one smallest translation.
3. $G \cap T \cong \mathbb{Z}^2$.
Proof: Delayed.

Definition: A planar crystallographic group is a discrete subgroup G of $\text{Isom}(\mathbb{R}^2)$ with $G \cap T \cong \mathbb{Z}^2$.

Lecture 19
October 21

More on Discrete Subgroups of Isom($\mathbb{R}^n$)

We shall consider the isometries of $\mathbb{R}^2$, . We recall that Isom($\mathbb{R}^2$) $\cong \mathbb{R}^2 \underset{\phi}{\rtimes} O(2)$ under the isomorphism $(v, A) \mapsto \tau_v \circ m_A$. We recall that anything in $O(2)$ is a rotation by some θ composed with a reflection about some axis, i.e. it can be written $\rho_\theta \circ r$, while anything in $\mathbb{R}^2$ is a translation $\tau_{\vec{v}}$.

Definition: Given a discrete subgroup $G <$ Isom($\mathbb{R}^2$) let the lattice of G be $L_G = \{v \in \mathbb{R}^2 \mid \tau_v \in G\}$. (Note that this is essentially the set of vectors that correspond to the elements of $G \cap T$).

Remark: $G \cap T$ is normal in G.
To see this, we consider the it general fact that given $H < G$, and $N \lhd G$, $H \cap N \lhd G$. Or we can consider the homomorphism Isom($\mathbb{R}^n$) $\to O(n)$ defined with $\tau_v \circ m_A \mapsto A$. This map has as kernel of $T \subset$ Isom($\mathbb{R}^n$). The kernel of this map restricted to G is $G \cap T$.

Such a map also yields $\overline{G}$, which is the image of G in $O(n)$ under this map, called the point group of G. We see that $\overline{G} \cong G/G \cap T$. This is the set of $A \in O(2)$ such that there exists v such that $\tau_v \circ m_A \in G$. This is not equivalent to the set or orthogonal elements in G. To see the distinction, consider the glide reflection equivalent to a refection over the x axis followed by a horizontal translation. Under our map, this would yield a reflection in $\overline{G}$, even though G might not necessarily have a reflection itself.

Claim: Any discrete subgroup G of $O(n)$ is finite.
Sketch of Proof: We know that $O(n)$ contains only reflections and rotations. We take the smallest rotation angle. We see that all rotations are multiples of this and this is $2\pi/n$ for some n.

Lemma: If $A \in \overline{G} \subset O(n)$ and $\vec{v} \in L_G$, then $A\vec{v} \in L_G$.
Proof: The basic idea comes from the following: $\rho_\theta \tau_v \rho_{-\theta} = \tau_{\rho_\theta v} \rho_\theta \rho_{-\theta} = \tau_{\rho_\theta v}$.
We then have $\tau_w m_A \in G$ (if $A \in \overline{G}$). Then

$$\begin{aligned}
\tau_w m_A \tau_v (\tau_w m_A)^{-1} &= \tau_w m_A \tau_v m_{A^{-1}} \tau_{-w} \\
&= \tau_w \tau_{Av} m_A m_{A^{-1}} \tau_{-w} \\
&= \tau_w \tau_{Av} \tau_{-w} \\
&= \tau_{w+Av-w} \\
&= \tau_{Av}.
\end{aligned}$$

Proposition: A discrete additive subgroup L of $\mathbb{R}^2$ is one of the following:
1. $L = \{0\}$.
2. $L = \mathbb{Z}v$
3. $L = \mathbb{Z}v + \mathbb{Z}w$, where v and w are linearly independent. (This case is the lattice).

Proof: Either we have Case 1 or we can choose a minimal nonzero length vector $v \in L$. Then $\mathbb{Z}v \in L$. Then either we have Case 2 or there are more vectors to consider. We take a minimal nonzero length vector w in $L - \mathbb{Z}v$. We then have two cases to consider. Either $w \in \mathbb{R}v$ or $w \notin \mathbb{R}v$. The fist case leads to a contradiction, because additive subgroups of $\mathbb{R}$ are all multiples of one element because otherwise, there would be gaps smaller than $|v|$, e.g. $|2v - w| < |v|$. Thus $w \in L - \mathbb{Z}v$ cannot also be in $\mathbb{R}v$. In the second case, we consider the triangle formed by w, v, and $v - w$. There is no vector in L inside this region, as w is of minimal length. We see this is true for the triangle formed by w, v, and $v + w$ as well. Thus we conclude that $L = \mathbb{Z}v + \mathbb{Z}w$.

Theorem: $\overline{G} \cong C_n$ or $\overline{G} \cong D_n$ for $n = 1, 2, 3, 4$, or 6.
Sketch of Proof: Let v be the minimal vector in L_G. We know that the subgroups of $O(n)$ are either $\{\rho_{2\pi k/n}\}$ or $\{\rho_{2\pi k/n}\} \cup \{\rho_{2\pi k/n} \circ r\}$. Thus $\rho_{2\pi/n} v \in L_G$. We consider the triangle formed by v, $\rho_{2\pi/n} v$, and $\rho_{2\pi/n} v - v$. We see that $|\rho_{2\pi/n} v - v| < |v|$ for $n > 6$, as at $n = 6$ they form an equilateral triangle. Thus for $n > 6$, $\rho_{2\pi/n} v \notin L_G$, so $\rho_{2\pi/n} \notin \overline{G}$.
We now consider $n = 5$. We can show that $|v + \rho_{4\pi/5} v| < |v|$. (This is left as an exercise).

Planar Crystallographic Groups:
We recall that these are discrete subgroups of $\mathrm{Isom}(\mathbb{R}^2)$ whose the translations correspond to a lattice ($G \cap T \cong \mathbb{Z}^2$). They have point groups isomorphic to C_n or D_n for $n = 1, 2, 3, 4$, or 6.

Theorem: There are 17 total possibilities for G up to isomorphic groups, and all 10 possibilities for C_n and D_n are represented.

Theorem: There are two isomorphism classes of planar crystallographic groups in $\mathrm{Isom}(\mathbb{R}^2)$ with point group D_4.
a. $G = \{\tau_v \circ \rho_{2\pi k/4}\} \cup \{\tau_v \circ \rho_{2\pi k/4} \circ r\}$ with $v \in \mathbb{Z} \oplus \mathbb{Z}$
b. $G = \{\tau_v \circ \rho_{2\pi k/4}\} \cup \{\tau_{v+(1/2,1/2)} \circ \rho)2\pi k/4v \circ r\}$ with $v \in \mathbb{Z} \oplus \mathbb{Z}$
Here the reflections are about the x axis.
Proof: L_G is isomorphic to, up to orthogonal change of coordinates and rescaling, $\mathbb{Z} \oplus \mathbb{Z}$. (This part is left as an exercise). Given that, there exist rotations by multiples of $2\pi k/4$ about some integer lattice point. We take this point to be the origin. Thus such rotations exist around all lattice points.
Remark: $\tau_v \rho_\theta$ is a rotation by θ about some point $p \in \mathbb{R}^2$.
We also find $\tau_w r \in G$ with $r \in \overline{G}$. The reflections in $\overline{G}$ are reflections about the x and y axes and the lines of slope 1 and -1.
Now we pick some element $\tau_{(a,b)} r \in G$. (Let r be reflection about the x axis.) We square it to yield $\tau_{(a,b)} r \tau_{(a,b)} r \in G = \tau_{(a,b)} \tau_{(a,-b)} = \tau_{(2a,0)}$.

Proof continued in next lecture.

Lecture 20
October 23

More on Discrete Subgroups of Isom($\mathbb{R}^2$)

We were considering the two isomorphism classes of planar crystallographic groups in Isom($\mathbb{R}^2$) with point group D_4.

We have $\tau_{\vec{w}}r_x \in G$ for some $\vec{w} \in \mathbb{R}^2$. We write this as $\vec{w} = (a,b)$ and square the expression, yielding $\tau_{(a,b)}r_x\tau_{(a,b)}r_x = \tau_{(a,b)}\tau_{(a,-b)}r_x^2 = \tau_{(2a,0)}$. So $2a \in \mathbb{Z}$. Now we use $r_y = \rho_{\pi/2}r_x\rho_{-\pi/2} = r_x\rho_\pi$ to yield that $2b \in \mathbb{Z}$.

We also have $\rho_{-\pi/2}r_x \in G$, as $\rho_{-\pi/2}r_x = r_x\rho_{\pi/2}$. We consider $\tau_{(a,b)}r_x\rho_{\pi/2} \in G$. We square this to yield

$$\begin{aligned}\tau_{(a,b)}r_x\rho_{\pi/2}\tau_{(a,b)}r_x\rho_{\pi/2} &= \tau_{(a,b)}\rho_{-\pi/2}r_x\tau_{(a,b)}r_x\rho_{\pi/2}\\ &= \tau_{(a,b)}\tau_{(a,-b)}\rho_{\pi/2}r_xr_x\rho_{\pi/2}\\ &= \tau_{(a,b)}\tau_{(-b,a)}\\ &= \tau_{(a-b,b+a)} \in G.\end{aligned}$$

Thus $a-b \in \mathbb{Z}$. So either $G = \{\tau_{(a,b)}\rho_{2\pi k/4} \mid a,b \in \mathbb{Z}\} \cup \{\tau_{(a,b)}\rho_{2\pi k/4} \mid a,b \in \mathbb{Z}\}$ or $G = \{\tau_{(a,b)}\rho_{2\pi k/4} \mid a,b \in \mathbb{Z}\} \cup \{\tau_{(a,b)+(1/2,1/2)}\rho_{2\pi k/4}r \mid a,b \in \mathbb{Z}\}$.

We know draw an interesting conclusion from the second case. We ask the following question: Is there a homomorphism $\overline{G} \cong D_4 \to G$ such that we have a sequence $D_4 \hookrightarrow G \twoheadrightarrow \overline{G}$? (Can we see $\overline{G}$ inside G?) The answer is no, because then there would exist a point $p \in \mathbb{R}^2$ that is fixed by this image of D_4 in G, as any finite subgroup of the isometry group has a fixed point. We then repeat all of the above using this point as the origin. This yields the first case.

We shall eventually discuss possible point groups in $\mathbb{R}^3$, or rather, the finite subgroups of Isom($\mathbb{R}^3$).

Definition: If G is a group and S is a set, a group action of G on S is a map $G \times S \to$ defined by $(g,s) \mapsto g \cdot s$ such that $(g_1, g_2) \cdot s = g_1 \cdot (g_2 \cdot s)$.

This is the same as a homomorphism $G \to \text{Bij}(S,S)$ defined with $g \mapsto \{s \mapsto g \cdot s\}$.

Definition: Given $x \in S$, the stabilizer of x is $\text{Stab}_x = \{g \in G \mid g \cdot x = x\}$. This is a subgroup of G.

Consider D_3 acting on the triangle T. We label the vertices as A, C, and E, the midpoints of the sides as B, D, and F, the center as O, and an arbitrary point on the boundary as P. We see that $\text{Stab}_A = \{id, \text{refl}_{\overline{AD}}\}$, $\text{Stab}_B = \{id, \text{refl}_{\overline{BE}}\}$, $\text{Stab}_P = \{id\}$, and $\text{Stab}_0 = D_3$.

Definition: Given $x \in S$, the orbit of x is $\mathcal{O}_x = \{y \in S \mid \exists\ g \in G \text{ such that } g \cdot x = y\}$.

In our previous example, we see that $\mathcal{O}_A = \{A, C, E\}$, $\mathcal{O}_B = \{B, D, F\}$, $\mathcal{O}_A = \{0\}$, and $\mathcal{O}_P = 6$ points.

Now we consider if Stab_x must be normal. It does not. For example, $\rho_{2\pi/3}r_{OA}\rho_{-2\pi/3} = r_{OC}$

does not stabilize A.

Now we consider $y \in \mathcal{O}_x$. We find that if $h \in \mathrm{Stab}_y$ and $y = g \cdot x$, then $hy = y \iff h(gx) = gx \iff (g^{-1}hg)x = x$. We conclude that $g^{-1}(\mathrm{Stab}_y)g = \mathrm{Stab}_x$, i.e. $\mathrm{Stab}_y = g(\mathrm{Stab}_x)g^{-1}$.

Now we consider the set of elements of G that take x to y where $y \in \mathcal{O}_x$. We see $hx = y = gx \iff g^{-1}hx = x \iff g^{-1}h \in \mathrm{Stab}_x \iff h \in g\mathrm{Stab}_x$. Thus the set of elements in G that take x to y is a coset. In fact, we have a one-to-one correspondence between the elements of $\mathcal{O}_x$ and the left cosets of Stab_x.
We conclude that if we restrict the action of G on S to G on $\mathcal{O}_x, x \in S$, then the following diagram commutes:

$$\begin{tikzcd}
G \times \mathcal{O}_x \arrow[r] \arrow[d, leftrightarrow, "\text{1 to 1}"'] & \mathcal{O}_x \arrow[d, leftrightarrow, "\text{1 to 1}"] \\
G \times \{\text{left cosets of } \mathrm{Stab}_x\} \arrow[r] & \{\text{left cosets of } \mathrm{Stab}_x\}
\end{tikzcd} .$$

Orbit-Stabilizer Theorem:
1. $|\mathcal{O}_x| = [G : \mathrm{Stab}_x]$.
2. $|G| = |\mathcal{O}_x| \cdot |\mathrm{Stab}_y|$.

If we consider our previous example of the triangle, we see that $|\mathrm{Stab}_A| = 2$, $|\mathcal{O}_A| = 3$, and $|D_3| = 2 \cdot 3 = 6$. Similarly, we saw that $|\mathrm{Stab}_O| = 6$, $|\mathcal{O}_O| = 1$, $|\mathrm{Stab}_P| = 1$, and $|\mathcal{O}_P| = 6$.

Lecture 21
October 25

Finite Subgroups of $SO(3)$

Suppose $G < SO(3)$ is finite. We consider the set $S = \{p \in S^2$ (the sphere) $\mid \exists\, g \in G,\ g \neq id$ such that $g(p) = p\}$. This is the set of a poles of rotations in G, i.e. the unit eigenvectors of the elements of G. Note that they define the axes of rotations for the elements of G.

Claim: G acts on S with multiplication (of a matrix and a vector).
Proof: We need a map $G \times S \to S$ that is associative. This follows from the associativity of matrix multiplication. We then need to show that if $h \in G$, and $p \in S$, then $hp \in S$, i.e. $\exists\ g \in G$ such that $gp = p$. We need g' such that $g'(hp) = hp$. We choose $g' = hgh^{-1}$, so $g'hp = hgh^{-1}hp = hgp = hp$.

The orbits of the action of G on S partition S. We shall list them as $\mathcal{O}_1, \mathcal{O}_2, \ldots, \mathcal{O}_k$ and their sizes as $n_1, n_2, \ldots, n_k$. Then, given p and $q = gp$ in $\mathcal{O}_i$. Then $\mathrm{Stab}_p \cong \mathrm{Stab}_q$. (We recall that $g\mathrm{Stab}_p g^{-1} < G$ is Stab_q). So they are the same size. We call this size r_i. Then the stabilizer for an element of orbit $\prime_i$ has size r_i. Note that $n_i r_i = |G|$ by the Orbit-Stabilizer Theorem.

Example:
We consider the symmetries of the cube. One type of axis of rotation would pass through two opposite vertices (of different faces). Another type would pass through the midpoints of two adjacent faces. A third type would pass through the midpoints of two adjacent edges of different faces. All axes would be one of these types. Using these axes, we consider the orbits of the poles of the symmetries of the cube.
$\mathcal{O}_1$ is the vertices. It has size $n_1 = 8$. The stabilizer of each vertex has size is $r_1 = 3$.
$\mathcal{O}_2$ is the midpoints of the faces. It has size $n_2 = 6$. The stabilizer of each point has size $r_2 = 4$.
$\mathcal{O}_3$ is the midpoints of the edges. It has size $n_3 = 12$. The stabilizer of each point has size $r_3 = 2$.
Note that each of these orbits and stabilizers shows that $|G| = 24$. We know that group of symmetries of the cube is isomorphic to S_4, which has order $4! = 24$, so this confirms that.

Now let's count the elements of the set $\{(g, p) \mid g \in G, g \neq id, p \in S \text{ and } g(p) = p\}$. This is $2(|G|-1)$. We can find this two ways. We can sum over poles to get $2(|G|-1) = \sum\limits_{p \in S} r_p - 1$. We can also sum over orbits to get $\sum\limits_{i=1}^{k} n_i(r_i - 1) = \sum\limits_{i=1}^{k} |G| - n_i$. Thus we have $2(|G|-1) = \sum\limits_{i=1}^{k} |G| - n_i$. Dividing by $|G|$, we find $2 - \dfrac{2}{|G|} = \sum\limits_{i=1}^{k} \left(1 - \dfrac{1}{r_i}\right)$

Claim: k is 2 or 3.
Proof: We know that r_i is at least 2, because if $p \in S$, then $id(p) = p$, and $g(p) = p$ for some nonidentity $g \in G$. (We assume that $|G| \neq 1$). Thus $2 - \dfrac{2}{|G|} = \sum\limits_{i=1}^{k} \left(1 - \dfrac{1}{r_i}\right) \geq \dfrac{k}{2}$. So $k < 4$. Also, $1 \leq 2 - \dfrac{2}{|G|} = \sum_{i=1}^{k} \left(1 - \dfrac{1}{r_i}\right) < k$. So $1 < k < 4$, so $k = 2$ or 3.

We now consider the two cases.

Case of $k = 2$

We find that $2 - \frac{2}{|G|} = 1 - \frac{1}{r_1} + 1 - \frac{1}{r_2} \implies \frac{1}{r_1} + \frac{1}{r_2} = \frac{2}{|G|}$. Thus $n_1 + n_2 = 2$, so $n_1 = n_2 = 1$, and $r_1 + r_2 = |G|$. This is just C_n $(n = |G|)$, the cyclic group of rotations about one axis. Thus we have only two points, each with a stabilizer of size 2. We shall label this as $(r_1, r_2) = (n, n)$.

Case: $k = 3$

We write $r_1 = r_2 = r_3$. Then we find that $2 - \frac{2}{|G|} = 1 - \frac{1}{r_1} + 1 - \frac{1}{r_2} + 1 - \frac{1}{r_3} \implies \frac{2}{|G|} = \frac{1}{r_1} + \frac{1}{r_2} + \frac{1}{r_3} - 1$. One of the r_i must be 2, or else $\frac{2}{|G|} \leq 0$. Let $r_1 = 2$. Then $r_2 = 2$ or 3. We then examine these two cases.

Case: $(2, 2, r_3)$.

We find that $r_3 = \frac{|G|}{2}$, which we'll label as m. Then the sizes of the corresponding orbits are $(2, 2, m)$.

The case corresponds to the two antipodal points on the sphere with m rotations around each of them. These points are in the same orbit, so we can swap them. The $2m$ points of the other orbits correspond to the vertices and the midpoints of the sides of a m-gon on the equator of the sphere. Thus we have D_m, the set of symmetries of the m-gon.

Case: $(2, 3, r_3)$.

We see that $r_3 = 3, 4$, or 5. We consider each of these cases:

Subcase: (2,3,3).

This implies that $|G| = 12$ and the sizes of the orbits are $(6, 4, 4)$. This case corresponds the the symmetries of a regular tetrahedron. There are 4 vertices with stabilizers of size 3, 6 midponts of edges with stabilizers of size 2, and four midpoints of faces with stabilizers of size 3. This group is called the tetrahedral group T. We claim this is isomorphic to the alternating group A_4 (the kernel of the sign homomorphism from S_4 to $\{\pm 1\}$). We can see this by considering the four vertices as a set of size 4. T acts on the vertices and give a homomorphism $T \to \text{Bij}(\{1, 2, 3, 4\}, \{1, 2, 3, 4\}) = S_4$. A rotation about the a vertex maps to a 3-cycle. A rotation about a pair of opposite edges maps to the composition of 2 2-cycles. We see that this map is injective, and $|A_4| = 12$, so this map is an isomorphism.

Subcase (2,3,4):

We see that $|G| = 24$ and the sizes of the orbits are $(12, 8, 6)$.

This case corresponds to the symmetries of the cube. There are 8 vertices with stabilizers of size 3, 12 midpoints of edges with stabilizers of size 2, and 6 midpoints of faces with stabilizers of size 4. This group is called the octahedral group O, as an octahedron can be made by swapping the faces and vertices of the cube.

Claim: $O \cong S_4$.

Proof: Delayed.

Subcase (2,3,5):

We see that $|G| = 60$ and the sizes of the orbits are $(30, 20, 12)$.

This case corresponds to the symmetries of the icosahedron, or the icosahedral group I.

There are 12 vertices with stabilizers of size 5, 30 midpoints of edges with stabilizers of size 2, and 20 midpoints of faces with stabilizers of size 3.

Claim: $I \cong A_5$.
Proof: Delayed.

Lecture 22
October 28

Sketches of $O \cong S_4$ and $I \cong A_5$

Recall that O is the octahedral group, the orientation-preserving isometries of the octahedron or the cube and that I is the icosahedral group, the orientation-preserving isometries of the icosahedron or the dodecahedron.

The cube has four main diagonals. O permutes these diagonals by rotation around an axis, which yields a homomorphism from O to S_4. Now we must check that no nonidentity element of O preserves all four diagonals. Since O consists of rotations about either an axis through the midpoint of two faces, one through the midpoints of two edges, or one of the main diagonals, this is true.

We can relate the symmetries of the tetrahedron to this group by inscribing a tetrahedron in a cube. In doing so, the tetrahedron uses half of the vertices of the cube, including one out of each end of a main diagonal. This shows that $T \subset O$, and it will turn out that $T \cong A_4 \subset S_4 \cong O$, i.e. T is isomorphic to the group of odd permutations. We also see that the number of edges of the tetrahedron equals the number of faces of the cube.

In a dodecahedron, we have twelve pentagonal faces. This is equivalent to having twelve edges of a cube. We then choose two parallel face diagonals of adjacent pentagonal faces, which allows us to inscribe a cube. Since there are five face diagonals of a pentagon, this yields five regular cubes inscribed in the dodecahedron.

Claim: The action of I on these 5 cubes give an injective homomorphism $I \hookrightarrow S_5$, with image landing in A_5, so $I \cong A_5$ because $|I| = 60$ and $|A_5| = 5!/2 = 60$.
Proof:
We see that rotating the dodecahedron around a face yields a 5-cycle, rotating around a vertex yields a 3-cycle, and rotating around an edge yields the product of two 2-cycles. All of these are even and none are the identity, so we find that $I \cong A_5$.

More Group Theory:

Cayley's Theorem: Every finite group is isomorphic to a subgroup of S_n, where $n = |G|$.
Proof: We use left multiplication: $G \times G \to G$ defined with $\ell_g(h) = gh$. This is an action: $\ell_{g_1 g_2}(h) = (g_1 g_2)h = g_1(g_2 h) = \ell_{g_1}(\ell_{g_2}(h))$. We now consider the orbit of an element. It must be all of G, because for any $h' \in G$, we can use $h'h^{-1} \in G$ to take an arbitrary $h \in G$ to h'. This yields a map $G \to \text{Bij}(G, G) \cong S_n$ where $n \; |G|$ defined with $g \mapsto \ell_g$. Only 1 maps to the identity under this map. Since the kernel is trivial, we have an injective homomorphism $G \hookrightarrow S_n/$, i.e. $G \cong \text{im}(\phi) \cong S_n$.

Theorem: If $H < G$ is a finite group of index p, where p is the smallest prime dividing $|G|$, then $H \triangleleft G$.

Proof: Consider the action of G on the cosets of H. This yields a map $\phi : G \to S_p$. Thus we find $g \in \ker(\phi) \iff g \cdot (g_i H) = g_i H \;\forall\; i \implies g \cdot (1H) = H \iff g \in H$. Thus $N = \ker\phi < H$. We then find the short exact sequence $N \hookrightarrow G \twoheadrightarrow \text{im}(\phi) < S_p$. We know $\text{im}\phi \cong G/N$ and $[G : N] = |G/N|$. We find that $[G : N] \mid |S_p|$, so $[G : N] \mid p!$. We claim that

$[G:N] = p$. We know that $[G:N] \mid |G|$, and $|G|$ has no prime factors less that p, so the index is either 1 or p. But $[G:N] \geq [G:H]$, so $[G:N] = p$. So $N = H$, as they have the same index and $N < H$. So H is normal.

Conjugacy Classes and the Class Equation:

We let G act on itself by conjugation. This is an action, as $g_1 \cdot (g_2 \cdot h) = g_1(g_2 h g_2^{-1}) = g_1 g_2 h g_2^{-1} g_1^{-1} = (g_1 g_2) h (g_1 g_2)^{-1} = (g_1 g_2) \cdot h$.

We consider the orbit and stabilizer of an element $h \in G$.
The orbit of h is $C(h) = \{ghg^{-1} \in G \mid g \in G\}$, known as the conjugacy class of h.
The stabilizer of h is $Z(h) = \{g \in G \mid ghg^{-1} = h\}$, known as the centralizer of h.

We see that $|G| = |C(h)| \cdot |Z(h)|$ from the Orbit-Stabilizer Theorem.

We also have a the Class Equation: $|G| = \sum\limits_{\text{conjugacy classes}} |C|$. ($G$ is finite).

Proof: The orbits of an action partition G, so $|G|$ is the sum of sized of the orbits.

This is often written as $|G| = |C_1| + |C_2| + \cdots + |C_k|$, where k is the number of conjugacy classes and $C_1, C_2, \ldots, C_k$ are the conjugacy classes written in increasing order of size.

Example:
We consider $D_3 = \{1, \rho, \rho^2, r, r\rho, r\rho^2\}$. To multiply these, we use $r\rho = \rho^{-1}r = \rho^2 r$. We find the following:
$r\rho r^{-1} = \rho^{-1} r r^{-1} = \rho^2$.
$\rho r \rho^{-1} = r\rho^{-1}\rho^{-1} = r\rho$.
$\rho r \rho \rho^{-1} = r\rho^2$.
Thus $\{1\}$, $\{\rho, \rho^2\}$, and $\{r, r\rho, r\rho^2\}$ are the conjugacy classes. This agrees with the Class Equation, as $6 = 1 + 2 + 3$.

Lecture 23
October 30

More on Conjugacy Classes and the Class Equation

Last lecture we considered the action of G on itself by conjugation. We now consider $D_4 = \{1, \rho, \rho^2, \rho^3, r, r\rho, \rho^2, r\rho^3\}$.
We find the following:
$r\rho r = rr\rho^3 = \rho^3$
$r\rho^2 r = r\rho r\rho^3 = rr\rho^3\rho^3 = \rho^2$
$\rho\rho^2\rho^{-1} = \rho^2$
$\rho r\rho^{-1} = r\rho^3\rho^3 = r\rho^2$
$\rho(r\rho^2)\rho^{-1} = r\rho^3\rho^2\rho^3 = r$.
Thus $\{1\}$, $\{\rho, \rho^3\}$, $\{\rho^2\}$, $\{r, r\rho^2\}$, and $\{r\rho, r\rho^3\}$ are the conjugacy classes.
Thus the class equation is $1 + 1 + 2 + 2 + 2 = 8$.

Lemma: If $|C(x)| = 1$, then $xg = gx$ for all $g \in G$.
Proof: $gxg^{-1} = x \implies gx = xg$

Theorem: The Class Equation for D_{2m} (with $4m$ elements) is

$$4m = \underbrace{1}_{\text{identity}} + \underbrace{1}_{\text{rotation by } \pi} + \underbrace{2 + \cdots + 2}_{m-1 \text{ rotations by } \pi k/m} + \underbrace{m}_{\text{reflections about midpoints of edges}} + \underbrace{m}_{\text{reflections about vertices}} .$$

The class equation for D_{2m+1} is

$$4m + 2 = \underbrace{1}_{\text{identity}} + \underbrace{2 + \cdots + 2}_{m \text{ rotations by } \pm 2\pi k/2m+1} + \underbrace{2m + 1}_{\text{reflections}} .$$

(Here all the reflections are in the conjugacy class because every reflection about a midpoint of a side of an n-gon with n odd is also a reflection about a vertex).
Proof: $D_{2m} = \{1, \rho, \rho^2, \cdots, \rho^{2m-1}, r, r\rho, \cdots, r\rho^{2m-1}\}$. This yields $r\rho^k r = rr\rho^{-k} = \rho^{-k}$ and $\rho(r\rho^k)\rho^{-1} = r\rho^{-1}\rho^k\rho^{-1} = r\rho^{k-2}$.

Groups of Order p^2 (p prime)

Claim: There exists a nonidentity element in the center of G
Proof: The class equation is $p^2 = 1 + |C_2| + \cdots + |C_k|$. We claim that at least one of $|C_2|, \ldots, |C_k|$ is one. Clearly some $|C_j|$ is 1, p, or p^2 by Lagrange's Theorem. But $|C_j| \leq p^2 - 1$ since the conjugacy classes partition G, so $|C_j| \neq p^2$. Also, $|C_j|$ cannot be equal to p for every j because the right hand side would equal 1 mod p. Thus there is at least one $|C_j| = 1$, so the element in that conjugacy classes is in the center of G.
Further Claim: G is abelian.
Proof: Let $x \in Z(G)$, $x \neq 1$. The order of x is either p or p^2. If $|x| = p^2$, then G is cyclic, so it is abelian. Otherwise, $|Z(G)|$ is either p or p^2. We assume that it is p. We assume for the sake of contradiction that there exists some $y \notin Z(G)$. We then consider the order of $Z(y)$. We know that $Z(G) \subset Z(y)$ and $y \in Z(y)$. So $|Z(y)| > p$. We also know that $Z(G) < G$ and $|G| = p^2$, so $|Z(y)| \mid p^2$. Thus $Z(y) = Z(G)$, so $y \in Z(G)$, which contradicts our choice of y. Thus $|Z(G)| = p^2$, so G is abelian.

Cauchy's Theorem: Given a finite group G with $p \mid |G|$, $\exists\, x \in G$ of order p.
Proof: First we shall prove that this is true if G is abelian. We shall induct on $|G|$. We take any element $y \in G$. If $p \mid |y|$, we are done, as we can choose some multiple of y with order p. (If $y^{p\ell} = 1$, then $|y^\ell| = p$). If $p \nmid |y|$, we consider $G/\langle y \rangle$, which is of smaller order than G.

By our inductive step, this group must have an element of order p. We then see that if some quotient of G has an element $\overline{x} \in G/H$ of order p, then we can choose x such that $\pi(x) = \overline{x}$ with $\pi : G \to G/H$. Then $p \mid |x|$, so we're done by the same logic as before.

If G is not abelian, we again induct on $|G|$. The Class Equation is $|G| = 1 + |C_2| + \cdots + |C_k|$.
Case 1: $Z(G) \neq \{1\}$. Then either $|Z(G)|$ is a multiple of p or $|G/Z(G)|$ is multiple of p and G has an element of order p by our previous method.
Case 2: $Z(G) = \{1\}$. Not all of the $|C_j|$ can be divisible by p because then $|G| \equiv 1 \bmod p$. Thus there is some C_j such that $1 < |C_j|$ and $p \nmid |C_j|$. Let $x \in C_j$. Then we consider $Z(x)$, which has size $|G|/|C_j|$, which is divisible by p and smaller, so we know that $Z(x)$ has an element of order p and so does G by our previous logic. (Note that the base case where $|G| = p$ implies that all nonidentity elements have order p).

Class Equation for the Icosahedral Group:

We know that $|I| = 60$. An icosahedron has 20 triangular faces, 30 edges, and 12 vertices where 5 edges meet. The elements of I are:
-the identity
-12 rotations about a vertex by $2\pi/5$ (this includes rotations about the antipodal vertex by $-2\pi/5$)
-12 rotations about a vertex by $4\pi/5$ (this includes rotations about the antipodal vertex by $-4\pi/5$)
-20 rotations about centers of faces by $2\pi/3$ (this includes rotations about the center of the antipodal face by $-2\pi/3$)
-15 rotations about edges by π (this includes rotations about the antipodal edge by π)
We see that $60 = 1 + 12 + 12 + 15 + 20$.

Claim: This is the class equation.
Lemma: If $A, B \in SO(3)$ are conjugate, with A being a rotation about an axis v by angle θ and B being a rotation about an axis w by angle ϕ, then $\theta = \pm\phi$

Proof: In two dimensions, we have $\begin{bmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{bmatrix}$ We consider $\det \begin{bmatrix} \lambda - \cos\theta & -\sin\theta \\ \sin\theta & \lambda - \cos\theta \end{bmatrix} = \lambda^2 - (2\cos\theta)\lambda + 1$. To solve this, we consider $e^{i\theta} = \cos\theta + i\sin\theta$. We find that $\left(e^{i\theta}\right)^2 - 2\cos\theta e^{i\theta} + 1 = \cos^2\theta - \sin^2\theta - 2\cos\theta + 1 = 0$. Thus we see that the roots are $\cos\theta \pm i\sin\theta$, which are preserved by conjugation. Thus θ is determined up to a sign. Now we must show that the elements of the sets listed are conjugate. Without loss of generality, we restrict our consideration to the midpoints of the faces. We see that for any two faces, there exists some $g \in I$ that takes face 1 to face 2. We let $\vec{v}_i$ be the midpoint of face i. We conjugate by this g to find that $g\rho_{\vec{v}_1}g^{-1}$ fixes $\vec{v}_2$. This is not the identity, so it must be some rotation about $\vec{v}_2$. The same can be said for $g\rho_{\vec{v}_1}^{-1}g^{-1}$, so these must be the two rotations.

Lecture 24
November 1

We consider the class equation for I in terms of the symmetries of the dodecahedron, which is formed by 12 pentagons that meet in groups of 3. We find:

$$60 = \underbrace{1}_{\text{identity}} + \underbrace{12}_{\substack{\text{rotations about}\\ \text{the midpoint of a face}\\ \text{by } \pm 2\pi/5}} + \underbrace{12}_{\substack{\text{rotations about}\\ \text{the midpoint of a face}\\ \text{by } \pm 4\pi/5}} + \underbrace{15}_{\substack{\text{rotations about}\\ \text{pairs of opposite edges}\\ \text{by } \pi}} + \underbrace{20.}_{\substack{\text{rotations about}\\ \text{opposite vertices}\\ \text{by } \pm 2\pi/3}}$$

We saw before that these are the conjugacy classes of I.

Definition: A group G is simple if its only normal subgroups are $\{1\}$ and G itself. (This means that G can't be broken up into smaller subgroups by quotienting by a normal subgroup. Simple groups are the primes of group theory.)

As an example, we see that C_p is simple. In fact, there are no other simple groups of order less than 60, which we shall see soon.

Theorem: I is simple.
Proof: We note that a normal subgroup is a union of conjugacy classes, as $H \lhd G \iff ghg^{-1} \in H \ \forall \ h \in H, \ g \in G$. We also see that $|H| \mid |G|$. Now we must show that there is no sum of some of 1, 12, 12, 15, and 20 that includes 1 and divides 60 (other than 1 and 60). This is quickly seen.

Theorem: A_n is simple for $n \geq 5$.
Proof: Exercise.

Classification of finite simple groups

There are 18 infinite families, i.e. classes of groups defined with a single parameter. There are 26 sporadic groups that are not in an infinite family. Two examples of infinite families are the alternating groups A_n for $n \geq 5$, and the projective special linear groups in dimension n on the field $\mathbb{Z}/p\mathbb{Z}$, $PSL_n(\mathbb{Z}/p\mathbb{Z})$ (with n large enough). The latter is equal to $SL_n(\mathbb{Z}/p\mathbb{Z})/\{nI\}$, the special linear group modulo the multiples of the identity. An example of a sporadic group is the monster group M, which has a size of $808,017,424,794,512,875,886,459,904,961,710,757,005,754,368,000,000,000 \approx 8 \times 10^{65}$. It is the largest sporadic group.

Definition: Given $H < G$, the normalizer of H is $N_H = \{g \in G \mid gHg^{-1} = H\}$. This is the largest subgroup of G in which H is normal.

This produces an action Φ of G on $S = \{H < G\}$ with $\Phi(g)(H) = gHg^{-1}$. We see that $\text{Stab}_H = N_H$ and $\mathcal{O}_H = \{\text{conjugate subgroups}\}$.

Counting Formula: $|N_H| \cdot \#(\text{conjugate subgroups of } H) = |G|$.

Example: Let $H < G$ be the set of rotations about the midpoints of opposite faces of the dodecahedron. This subgroup has order 5. We see that the number of conjugate subgroups is 6, as there are six pairs of opposite faces and conjugation yields a rotation about another face. Then we see that $|N_H| = 60/6 = 10$. Since $H < N_H$, we consider the 5 remaining elements of N_H. These are the ways to take the a face its opposite.

Sylow Subgroups

First Sylow Theorem: If G is a finite group and $p^k \mid G$ (with p prime and $k \in \mathbb{Z}_{\geq 1}$), but $p^{k+1} \nmid G$, then there exists a subgroup of G of order p^k. This is known as a Sylow p-subgroup.
Proof: Delayed.

Corollary: If $p \mid |G|$, then $\exists\ x \in G$ of order p.
Proof: We take a nonidentity element $y \in H$, with H being a Sylow p-subgroup ($|H| = p^k$). We know that $|y| \mid p^k$, so $|y| = p^\ell$ for $1 \geq \ell \geq k$. Then we simply take $y^{p^\ell} = \left(y^{p^{\ell-1}}\right)^p = 1$, and no smaller power than p^ℓ satisfies this, so we choose $x = y^{p^{\ell-1}}$, which is of order p.

Lemma: If $p^k \mid n$ but $p^{k+1} \nmid n$, then $p \nmid \binom{n}{p^k}$.
Proof: $\binom{n}{p^k} = \dfrac{n(n-1)(n-2)\cdots(n-p^k+1)}{p^k(p^k-1)(p^k-2)\cdots 1}$. We claim that $n - \ell$ and $p^k - \ell$ have the same number of factors of p. This implies that the numerator and denominator have the same number of factors.

Lecture 25
November 4

Sylow Theorems:

First Sylow Theorem: Given a finite group G such that $p^k \mid |G|$ but $p^{k+1} \nmid |G|$ (p prime), then there exists a Sylow p-subgroup $H < G$ of order p^k.
Proof: Let $n = |G|$.
Lemma: $p \nmid \binom{n}{p^k}$.
Let $S = \{A \subset G \mid |A| = p^k\}$ (subsets, not subgroups). G acts on S by left multiplication. We list the orbits $\mathcal{O}_1, \mathcal{O}_2, \ldots, \mathcal{O}_a$. We see that $|S| = |\mathcal{O}_1| + \cdots |\mathcal{O}_a| = \binom{n}{p^k}$, so $p \nmid |S|$, so there exists some $\mathcal{O}_j$ with $|\mathcal{O}_j|$ not divisible by p. Let $A \in \mathcal{O}_j$. Then $|\mathrm{Stab}_A| \cdot |\mathcal{O}_A| = |G| = mp^k$ with $p \nmid m$. So $|\mathrm{Stab}_A| = bp^k$, with $b \mid m$.
Lemma: $|\mathrm{Stab}_A|$ divides $|A|$.
Proof: Stab_A acts on A by left multiplication. Under this action, the stabilizer of an element is just the identity and the size of every orbit is $|\mathrm{Stab}_A|$. We know that $|A| = \sum_{i=1}^{c} |\tilde{\mathcal{O}}_i|$, so $|\mathrm{Stab}_A| \cdot \#(\text{orbits}) = |A|$.
Now, since $|\mathrm{Stab}_A| = bp^k$ and $|\mathrm{Stab}_A| \mid p^k = |A|$, $b = 1$ and $H = \mathrm{Stab}_A$

Second Sylow Theorem: All Sylow p-subgroups in G are conjugate, i.e. given one H, the rest are of the form gHg^{-1}.
We will actually show something even stronger: Given a p-group in G, call is K, and given a Sylow p-group H, $K \subset gHg^{-1}$ for some $g \in G$.
Proof: Consider the action of G on the left cosets of H by left multiplication. Let $S = \{\text{left cosets of } H\}$. Then $|G| = p^k m$ ($p \nmid m$) and $|S| = m$. Then $K < G$ of order p^ℓ. K acts on the cosets of H by left multiplication. We claim that there exists a fixed point of this action, i.e. an element of S, call it gH, such that $\forall\ k \in K, kgH = gH$.
Proposition: Suppose K is a p-group (i.e. a group of order p^ℓ for some ℓ) and S is some set such that $p \nmid |S|$. Then there exists $s \in S$ fixed by all $k \in K$.
Proof: Delayed.
Now we consider $\mathrm{Stab}_{gH} \subset G$ for action of left multiplication by G on the cosets of H. We claim that $\mathrm{Stab}_{gH} = \mathrm{Stab}gHg^{-1}$. This is true, as gHg^{-1} stabilizes gH, i.e. $ghg^{-1}gH = ghH = gH$. We also know that $|gHg^{-1}| = |H|$ and $|\mathcal{O}_{gH}| = |G|/|H|$. Also, $|\mathrm{Stab}_{gH}| \cdot |\mathcal{O}_{gH}| = |G|$, so $|gHg^{-1}| = |\mathrm{Stab}_{gH}|$, and thus $gHg^{-1} = \mathrm{Stab}_{gH}$. Hence $K < \mathrm{Stab}_{gH} = gHg^{-1}$.
Proof Resumed: The size of an orbit is p^d for some $0 \geq d \leq \ell$. We know that $|\mathcal{O}_i||\mathrm{Stab}_i| = |K| = p^\ell$. Not all or the orbits can be of an order divisible by p, so some orbit is of order 1. This is our fixed point.

Third Sylow Theorem: Given G with $|G| = mp^k$, $p \nmid m$, then the number of Sylow p-subgroups divides m and is $1 \bmod p$.
Proof: Consider the action of G on the set of Sylow p-subgroups by conjugation. There is only one orbit by the Second Sylow Theorem, because they are all conjugate. We choose H to be one of our Sylow p-subgroups. We know that $\mathrm{Stab}_H = \{g \in G \mid gHg^{-1} = H\} = N_H$, which is the normalizer of H. We have $H < N_H$, so $|H| \mid |N_H|$ and $|N_H| = bp^k$ for some $b \mid m$. Then $|\mathcal{O}_H| = |G|/|N_H| = mp^k/bp^k = m/b$ and $m/b \mid m$. Now we consider the action of the p-group H on the set of Sylow p-subgroups by conjugation. We see that every orbit is of an order of a power of p. We see that H is of order 1. Suppose K is a Sylow p-subgroup. We claim that if K is fixed by H under conjugation, then $K = H$, i.e. $\forall\ k \in K, h \in H$, $hkh^{-1} \in K$. We have that $H < N_K$ and $|N_K| = fp^k$. We then have that $K \triangleleft N_K$, as group

is normal in its own normalizer. Also, K is a Sylow p-subgroup of N_K and so is H. Then we see that they are conjugate by the Second Sylow Theorem applied to N_K. The conjugate of K by any element of N_K gives K itself, so $H = K$. So all other orbits are of an order divisible by p. Then the $\#$(Sylow p-subgroups) $= \sum$ sizes of orbits $= 1 + jp \equiv 1 \bmod p$.

Example: Groups of Order 15
There must be a Sylow 3-subgroup and a Sylow 5-subgroup. These must be isomorphic to C_3 and C_5. The number of Sylow 3-subgroups divides $15/3 = 5$, and it is equal to 1 mod 3. Thus it is 1 and this subgroup is normal. The number of Sylow 5-subgroups divides $15/5 = 3$ and is equal to 1 mod 5. Thus is it also 1 and this subgroup is also normal.
C_3, C_5 are both normal. $C_3 \cap C_5 = \{1\}$ because any element in the intersection has order dividing 3 and 5, so it has order 1. This implies that $G = C_3 \times C_5$.

Example: Groups of Order 21
We have C_3 and C_7 as Sylow subgroups. The number of Sylow 7-subgroups divides $21/7 = 3$ and is equal to 1 modulo 7, so it is 1. The number of Sylow 3-subgroups divides $21/3 = 7$ and is equal to 1 modulo 3, so it is 1 or 7.
Thus we have $G = C_7 \underset{\phi}{\rtimes} C_3$ mediated by some $\phi : C_3 \to \mathrm{Aut}(C_7) \cong (\mathbb{Z}/7\mathbb{Z})^*$. Let x be the generator of C_3. If $\phi(x) = 1$, then $G = C_3 \times C_7$. Otherwise, $\phi(x)$ is something of order 3 in $(\mathbb{Z}/7\mathbb{Z})^*$, which is either 2 or 4. We shall finish this next time.

Lecture 26
November 6

Sylow Subgroup Example: Groups of Order 21
We have already seen that C_3 and C_7 are Sylow subgroups. C_7 is normal, and we see that $C_7 \cdot C_3 = G$ because $C_7 \cap C_3 = \{1\}$ and $|C_7| \cdot |C_3| = |G|$. This can be seen in that all elements are distinct, because if $h_1 k_1 = h_2 k_2$, then $h_2 h_1^{-1} = k_2 k_1^{-1} = 1$ because it is in the intersection. Thus we have a semidirect product $G = C_7 \underset{\phi}{\rtimes} C_3$ with $\phi : C_3 \to \mathrm{Aut}(C_7) \cong (\mathbb{Z}/7\mathbb{Z})^*$. The elements of $\mathbb{Z}/7\mathbb{Z}$ are m_1, m_2, m_3, m_4, m_5, and m_6 taken modulo 7. The orders of these elements are $1, 3, 6, 3, 6$, and 2, respectively. Since ϕ is mapping from C_3, we need the generator of C_3 to map to the identity (in which case we find $G = C_7 \times C_3$) or to something of order 3, i.e. m_2 or m_4. We see that the subgroup (m_1, m_2, m_4) is isomorphic to C_3, so up to relabeling the generator of C_3 (since there are technically two generators), there is only one nontrivial choice for ϕ.

We conclude that there are two isomorphism classes of a group of order 21. The first is $C_7 \times C_3$ and the second is $C_7 \underset{\phi}{\rtimes} C_3$ with ϕ mapping the generator of C_3 to m_2. In particular, if if we let x and y be the generators of C_7 and C_3, respectively, we can write an element of the group as $x^i y^j$ such that $yx = x^2 y$. Then we see that $y^3 x = y^2 x^2 y = yx^4 y^2 = x^8 y^3 = x$. This works because a map that takes the generator of C_3 to m_2 gives a homomorphism.

Example: Groups of Order 12
We see that there is a Sylow 2-subgroup of order 4 and a Sylow 3-subgroup of order 3. The Sylow Theorems also tells us that the number of Sylow 2-subgroups is equivalent to 1 modulo 2 and it divides 3, i.e. it is 1 or 3, and that the number of Sylow 3-subgroups is equivalent to 1 modulo 3 and it divides 4, i.e. it is 1 or 4.
We investigate whether we can have 4 Sylow 3-subgroups and 3 Sylow 2-subgroups in a group of order 12. The Sylow 3-subgroups are all isomorphic to C_3, so their intersection is trivial. If we have four Sylow 3-subgroups, then we have $1 + 4 \cdot 2 = 9$ distinct elements, i.e. we have the identity and 8 elements of order 4. Then the Sylow 2-subgroup is just the remaining 3 elements and the identity, so there is only 1 Sylow 2-subgroup.

Let H be a Sylow 2-subgroup and K be a Sylow 3-subgroup in our group G or order 12. We see that H is isomorphic either to C_4 or $C_2 \times C_2$ and that K is isomorphic to C_3.The possibilities are as follows:
1. $H \lhd G$ and $H \cong C_4$.
2. $H \lhd G$ and $H \cong C_2 \times C_2$.
3. $K \lhd G$ and $H \cong C_4$.
4. $K \lhd G$ and $H \cong C_2 \times C_2$.

We consider each of these in turn.

1. We have $G = C_4 \underset{\phi}{\rtimes} C_3$, with $\phi : C_3 \to \mathrm{Aut}(C_4) = \{m_1, m_3\}$. We find that only the trivial map is allowed, so we find $G = C_4 \times C_3$.

2. We have $G = (C_2 \times C_2) \underset{\phi}{\rtimes} C_3$ with $\phi : C_3 \to \mathrm{Aut}(C_2 \times C_2) \cong S_3$. We can take the trivial map (in which case we find $G = C_2 \times C_2 \times C_3$), or we can map the generator to a 3-cycle (since they are of order 3), which yields the map $C_3 \to \{1, (1\ 2\ 3), (1\ 3\ 2)\}$. It turns

out this group is A_4, the set of even permutations of 4 elements. We then see that $C_2 \times C_2$, as a subgroup of S_4, is the set of compositions of transpositions of distinct elements, i.e. $\{1, (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\}$.

3. We have $G = C_3 \underset{\phi}{\rtimes} C_4$ with $\phi : C_4 \to \mathrm{Aut}(C_3) = \{m_1, m_2\}$. We can take the trivial map (in which case we find $G = C_3 \times C_4$), or we can map the generator to m_2, which yields a semidirect product.

4. We have $G = C_3 \underset{\phi}{\rtimes} (C_2 \times C_2)$ with $\phi : (C_2 \times C_2) \to \mathrm{Aut}(C_3) \cong C_2$. We then have two choices up to relabeling the elements of $C_2 \times C_2$. We can take the trivial map (in which case we find $G = C_2 \times C_2 \times C_3$), or we can project every element of $C_2 \times C_2$ to its second factor in C_2, which yields a semidirect product $G = (C_2 \times C_2) \underset{\phi}{\rtimes} C_3 = C_2 \times (\{\pm 1\} \underset{\text{mult}}{\rtimes} C_3) = C_2 \times D_3$.
We conclude that there are 5 isomorphism classes of groups of order 12. They are:
$C_4 \times C_2 \cong C_{12}$
$C_2 \times C_2 \times C_3 = C_2 \times C_6$
A_4
$C_2 \times D_3$
$C_3 \underset{\phi}{\rtimes} C_4$ such that $yx = x^2y$ (with $x^3 = 1$ and $y^4 = 1$).

Groups of Order 60 or Smaller

We now consider groups of order p^k. These are never simple, as they always have a proper normal subgroup. We also know that p-groups always have nontrivial center (which is normal). We can see this by writing the Class Equation:
$|G| = |Z(G)| + \sum\limits_i p^{k_i}$.
We know that the order of every conjugacy class is some power of p^{k_i}, with $0 < k_i < n$. But since $|G| = p^k$, $p \mid |Z(G)|$, so the center is nontrivial.

We now consider groups of order pq with $p < q$. We see that the number of Sylow q-subgroups is equivalent to 1 modulo q and divides p, so it is 1.

We now consider groups of order $p^k q^\ell$. It turns out that none of these groups are simple, but we need representation theory to prove it. We will have to deal with them case-by-case. We have $p = 2, 3, 5, 7, 11, 13$. The cases are $2^2 \cdot 13$, $2^2 \cdot 11$, $2^3 \cdot 7$, $2^2 \cdot 7$, $2 \cdot 5^2$, $3^2 \cdot 5$, $2^3 \cdot 5$, $2^2 \cdot 5$, $2 \cdot 3^3$, $2^2 \cdot 3^2$, $2 \cdot 3^2$, $2^4 \cdot 3$, $2^3 \cdot 3$, and $2^2 \cdot 3$.

We consider groups of order $2^2 \cdot 13$. We see that the number of Sylow 13-subgroups is equivalent to 1 modulo 13 and divides 2^2, so it is 1. This eliminates $2^2 \cdot 13$.
We find that the same argument works for groups of orders $2^2 \cdot 11$, $2^2 \cdot 7$, and $2^2 \cdot 5$.

We then consider groups of order $2^3 \cdot 5$. We see that the number of Sylow 5-subgroups is equivalent to 1 modulo 5 and divides 2^3, so it is 1. This eliminates $2^3 \cdot 5$.

Similar arguments can eliminate groups of order $2 \cdot 5^2$, $3^2 \cdot 5$, $2 \cdot 3^3$, $2 \cdot 3^2$. This is left as an exercise. Having already dealt with groups of order 12, the remaining cases are $2^3 \cdot 7 = 56$, $2^2 \cdot 3^2 = 36$, $2^4 \cdot 3 = 48$, $2^3 \cdot 3 = 24$, and $2^2 \cdot 3 = 12$.

Lecture 27
November 8

We continue our discussion of groups of order less than 60. We have seen that groups of order p^k and pq always have proper normal subgroups, and are never simple (except if $k = 1$ or $q = 1$, as the group of order p is cyclic and simple). In groups of order $p^k q^\ell$ (with k and ℓ not both 1), we were able to rule out everything except groups of order 12, 24, 36, 48, and 56 by direct application of the Third Sylow Theorem. We ruled out 12 by a counting argument.

Before considering these groups, we shall look at other combinations of primes that are less than 60. For groups of order pqr, the cases are $2 \cdot 3 \cdot 5 = 30$and $2 \cdot 3 \cdot 7 = 42$, and for groups of p^2qr the only case is $2^2 \cdot 3 \cdot 5 = 60$.

We can rule out 56 by considering the number of Sylow 7-subgroups, which must be equivalent to 1 modulo 7 and divide 8. Thus it is either 1 or 8. If it is not normal, it must be 8. Then we have $1 + 8 \cdot 6 = 49$ elements accounted for. We have $56 - 49 = 7$ elements left, and since $1 + 7 = 8$, these must form our Sylow 2-subgroup.

We now consider groups of order 24. The number of Sylow 2-subgroups must be equivalent to 1 modulo 2 and divide 3, so it is 3 if it is not normal. The number of Sylow 3-subgroups must be equivalent to 1 modulo 3 and divide 8, so it is 4 if it is not normal. We then consider the action by conjugation of G on the set of Sylow 2-subgroups. If H is a Sylow p-subgroups, then gHg^{-1} is a Sylow p-subgroup as well. The Second Sylow Theorem tells us that all the Sylow p-subgroups have this form. We now have a homomorphism $\phi\ G \to S_3$, which tells us how the action permutes the 3 Sylow 2-subgroups. If G is simple, then the kernel of ϕ, which is normal, must be trivial or G itself. It can't be G, because some conjugation on H takes it to a different Sylow p-subgroup. We also have that $|\ker(\phi)| \cdot |\text{im}(\phi)| = |G| = 24$, with $|\text{im}(\phi)| \mid |S_3|$ or $|\text{im}(\phi)| \leq 6$, so $|\ker(\phi)| \geq 4$. Thus $4 < |\ker(\phi)| < 24$, so $\ker(\phi)$ is a proper (nontrivial) normal subgroup.

We now consider groups of order 48. The number of Sylow 2-subgroups must be equivalent to 1 modulo 2 and divide 3, so it is 1 or 3. If it is 3, we consider the map $\phi : G \to S_3$ defined as the action by conjugation on the set of Sylow 2-subgroups. This map is not trivial, so $\ker(\phi)$ is a proper nontrivial normal subgroup.

We now consider groups of order 36. The number of Sylow 3-subgroups must be equivalent to 1 modulo 3 and divide 4, so it is 1 or 4. If it is 4, we consider the map $\phi : G \to S_4$, defined similarly to the above. Then $\ker(\phi)$ is normal, and not equal to either $|G|$ or $\{1\}$.

We now consider a group of order 30. The number of Sylow 5-subgroups must be equivalent to 1 modulo 5 and divide 6, so it is 1 or 6. If it is 6, we have $1+6\cdot 4 = 25$ elements accounted for, which leaves 5 remaining. If we assume we have more than one Sylow 2-subgroup and Sylow 3-subgroup, we must have at least 2 elements of order 2 and 4 elements of order 3. This is more than the remaining 5 elements, so there is only one Sylow 5-subgroup and groups of order 30 are not simple.

We now consider groups of order 42. The number of Sylow 7-subgroups must be equivalent to 1 modulo 7 and divide 6, so it is 1. Thus the Sylow 7-subgroup is normal.

We now consider groups of order 60. The number of Sylow 2-subgroups must be equivalent to 1 modulo 2 and divide 3, so it is 3, 5, or 15. The number of Sylow 3-subgroups must be equivalent to 1 modulo 3 and divide 20, so it is 4 or 10. The number of Sylow 5-subgroups must be equivalent to 1 modulo 5 and divide 12, so it is 6. If the number of Sylow 2-subgroups is 3, then we consider the map $\phi : G \to S_3$, defined similar to the above. This map must be nontrivial, so its kernel is a proper nontrivial normal subgroup. Similarly, if the number of Sylow 3-subgroups is 4 , then we consider the map $\phi : G \to S_4$, and this map must be nontrivial. Thus there are 10 Sylow 3-subgroups and there are 5 or 15 Sylow 2-subgroups.

We assume that the number of Sylow 2-subgroups is 5, and we consider the map $\phi : G \to S_5$, defined similar to the above. This map is not trivial, as $\ker \phi \neq G$. So $\ker(\phi) = \{1\}$ if G is simple. We also have $A_5 \subset S_5$. We consider $\text{im}(\phi) \cap A_5$. This must nontrivial, or else $|G| \cdot |A_5| = 3600$. Thus $\text{im}(\phi) \cap A_5 \triangleleft G$. We then consider $\phi^{-1}(A_5) = \{g \in G \mid \phi(g) \in A_5\}$ and claim that it is normal. To prove this, let $g \in \phi^{-1}(A_5)$ and $h \in G$. Then $\phi(hgh^{-1} = \phi(h)\phi(g)\phi(h)^{-1}$. We know $\phi(g) \in A_5$ and A_5 is normal in S_5, so $\phi(h)\phi(g)\phi(h)^{-1} \in A_5$ and $hgh^{-1} \in \phi^{-1}(A_5)$, so $\phi^{-1}(A_5)$ is normal. Thus, if G is simple and $\phi^{-1}(A_5) \neq \{1\}$, then $\phi^{-1}(A_5) = G$. Since $\phi : G \to A_5$ has a trivial kernel, it is an isomorphism and $G \cong A_5$.

Now we assume that the number of Sylow 2-subgroups is 15. G contains the identity, 6 Sylow 5-subgroups, which yield 24 elements of order 5, and 10 Sylow 3-subgroups, which yield 20 elements or order 3. This leaves 15 elements remaining. We see that at least two of the Sylow 2-subgroups, each with order 4, must overlap. Let them be H and K. Then $H \cap K$ is a subgroup of order 2. H and K are abelian because they have order 4. We consider $Z(H \cap K)$, which contains both H and K. Thus $4 \mid |Z(H \cap K)|$. Since $|Z(H \cap K)| \mid |G|$, $|Z(H \cap K)| = 4, 12, 20$ or 60. We know that $|Z(H \cap K)| \neq 60$, as then $H \cap K$ would be a normal subgroup. Also, $|Z(H \cap K)| \neq 4$ because $|H \cup K| > 4$.

We assume that $|Z(H \cap K)| = 12$ or 20, so $Z(H \cap K)$ has an index of 5 or 3. If $Z(H \cap K)$ has index 3, we consider the action of G on the cosets of $Z(H \cap K)$ by left multiplication, which yields the map $\phi : G \to S_3$, which is nontrivial, so this contradicts the fact that G is simple. If $Z(H \cap K)$ has index 5, then we consider the same action, which yields the map $\phi : G \to S_5$. By the same argument as before, we see that $G \cong A_5$. Thus we conclude that the only simple group of order 60 is $I \cong A_5$.

The next smallest nonabelian simple group has order $168 = 2^3 \cdot 3 \cdot 7$. It is the the projective special linear groups in dimension 2 on the field of 7 elements, $PSL_2(\mathbb{F}_7)$. This is equal to $SL_2(\mathbb{F}_7)/\{nI\}$, the special linear group modulo the multiples of the identity. Also, $PSL_2(\mathbb{F}_7) \cong PSL_3(\mathbb{F}_2)$.

Lecture 28
November 11

The Symmetric Group and the Rubik's Cube
We recall that the symmetric group S_n is the set of permutations of n symbols (with composition).

Definition: The cycle type of a permutations is a description of the sizes of its cycles and how many times each size cycle appears.

Definition: A partition of n is a distinct expression of n as a sum $n_1 + n_2 + \cdots + n_k$ with $n_1 \leq n_2 \leq \cdots \leq n_k$.

For example, consider $(3\ 4)(1\ 5\ 2)$ in S_7. There are two 1-cycles ((6) and (7)), one 2-cycle ($(3\ 4)$), and one 3-cycle ($(1\ 5\ 2)$), which corresponds to the partition $7 = 1+1+2+3$.

Proposition: The conjugacy classes of S_n are in one-to-one correspondence with cycle types or alternatively, with partitions of n.
Proof: Consider for example $(1\ 2\ 3)$ and $(2\ 6\ 7)$ in S_7. We must find a g such that $g(1\ 2\ 3)g^{-1} = (2\ 6\ 7)$. We pick a g such that the following takes place under $g(1\ 2\ 3)g^{-1}$:

$$1 \mapsto 4 \mapsto 4 \mapsto 1 \qquad 2 \mapsto 1 \mapsto 2 \mapsto 6 \qquad 3 \mapsto 5 \mapsto 5 \mapsto 3 \qquad 4 \mapsto 7 \mapsto 7 \mapsto 4$$

$$5 \mapsto 6 \mapsto 6 \mapsto 5 \qquad 6 \mapsto 2 \mapsto 3 \mapsto 7 \qquad 7 \mapsto 3 \mapsto 1 \mapsto 2$$

This tells us that $g = (1\ 2\ 6\ 5\ 3\ 7\ 4)$. Note that this g is not unique, as our choice of the action of g^{-1} on 1, 3, 4, and 5 was arbitrary.

In general, given $\sigma \in S_n$ with cycle notation $(a_1^1 a_2^1 \cdots a_{k_1}^1)(a_1^2\ a_2^2 \cdots a_{k_2}^2)\cdots$, we can conjugate by some element to yield $(b_1^1\ b_2^1 \cdots b_{k_1}^1)(b_1^2\ b_2^2 \cdots b_{k_2}^2)\cdots$. We can then form π^{-1} that sends b_i^j to a_i^j, i.e. we can form π sending a_i^j to b_i^j.
We must also show that any conjugate permutations have the same cycle structure, but this can be inferred easily from our previous argument.

Example: The Class Equation for S_4.
The only possible partitions of 4 are $1+1+1+1$, $1+1+2$, $1+3$, $2+2$, and 4. We identify the conjugacy classes that correspond to these partitions as the identity, the transpositions, the 3-cycles, the composition of 2 disjoint 2-cycles, and the 4-cycles. These have 1, $\binom{4}{2} = 6$, $4 \cdot 2 = 8$, $(\binom{4}{2})/2 = 3$, and $3! = 6$ elements, respectively. Thus the Class Equation $24 = 1+6+8+3+6$.

Theorem: A_n is simple for $n \geq 5$.
Steps of Proof:
(1) The 3-cycles generate A_n.
(2) All 3-cycles are conjugate in A_n for $n \geq 5$.
(3) Given any nonidentity element of A_n, it and its conjugates can be composed in some way to yield a 3-cycle.
Proof:
(1) Exercise.
(2) Given 2 2-cycles σ_1 and σ_2, we can write down a formula for g^{-1} that sends the elements

of σ_1 to those of σ_2 and sends the other elements to the remaining elements in an arbitrary fashion. This is the method we used above. Then $g\sigma_1 g^{-1} = \sigma_2$. Note that g is not unique.

For example, consider $\sigma_1 = (1\ 2\ 3)$ and $\sigma_2 = (2\ 4\ 5)$ in A_5. We choose g^{-1} defined with

$$1 \mapsto 4 \qquad 2 \mapsto 1 \qquad 3 \mapsto 5 \qquad 4 \mapsto 2 \qquad 5 \mapsto 3.$$

However, we could replace $g = (1\ 2\ 4)(3\ 5)$ with $g' = g \circ (4\ 5)$, and this would still work, as our choice of the action on 4 and 5 was arbitrary. We see that g and g' have opposite sign, so one of them must be in A_n. This implies that we can always find an even permutation by which we conjugate to take one 3-cycle to another, so all 3-cycles are conjugate in A_n for $n \geq 5$.
(3) Consider for example $(1\ 2\ 3)(4\ 5\ 6) = x$, $g = (4\ 3\ 2)$, and $h = (4/2/5)$. Then we can calculate $\left(gxg^{-1}\right) x^{-1} hx \left(gx^{-1}g^{-1}\right) h^{-1} = (5\ 4\ 3)$, which is a 3-cycle.

Rubik's Group

We have 6 centers (which don't move), 8 corner cubies, and 12 edge cubies. We call the group generated by rotating the faces, i.e., the group of all possible ways to move the corners and edges the Rubik's Cube Group. It would first appear that there is an action of G on S_8 of the positions of the corners, but we need to account for how they rotate. We see that we have $8 \cdot 3 = 24$ small faces. Then $G < S_{48}$. We have $(\mathbb{Z}/3\mathbb{Z})^8$ in this group, which is generated by 3-cycles of faces belonging to the same corner. We claim that the group of possible ways to move the corners is $(\mathbb{Z}/3\mathbb{Z})^8 \underset{\phi}{\rtimes} S_8$ where $\phi : S_8 \to \mathrm{Aut}(\mathbb{Z}/3\mathbb{Z})^8$ sends σ to an automorphism rearranging the factors.

Proposition: The Rubik's Cube group is a subgroup of $((\mathbb{Z}/3\mathbb{Z})^8 \underset{\phi}{\rtimes} S_8) \times ((\mathbb{Z}/2\mathbb{Z})^2 \underset{\phi}{\rtimes} S_{12})$, the semidirect product of the corners times the semidirect product of the edges. This is a called a wreath product.

Theorem: The Rubik's Cube Group has index 12 and in fact is the kernel of $\Phi : ((\mathbb{Z}/3\mathbb{Z})^8 \underset{\phi}{\rtimes} S_8) \times ((\mathbb{Z}/2\mathbb{Z})^2 \underset{\phi}{\rtimes} S_{12}) \to (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/3\mathbb{Z})$ that sends $h = ((a_i), \sigma, (b_j), \tau)$ to $(\mathrm{sign}(\sigma_1) + \mathrm{sign}(\tau), \sum b_j, \sum a_i)$

Lecture 29
November 15

Generators and Relations

Definition: A free group F_n on a set $S = \{a_1, a_2, \cdots, a_n\}$ or more simply, the free group on n symbols, is the set of all words in $(a, b, c, \ldots, n\text{th letter})$ and their inverses with no obvious cancellations.

For example $aba^2b^{-1}c^{-3}b^2$ is in the free group, but not $ab^2b^{-4}c^3a^{-1} = ab^{-2}c^3a^{-1}$, Multiplication in the group is carried out by performing the obvious cancellations, e.g. $(ab^2)(b^{-4}c^3a^{-1}) = ab^{-2}c^3a^{-1}$.

The Universal Property of the Free Group: Given a group G and an ordered list of elements $x_1, \ldots, x_n$, there exists a unique homomorphism $F_n \to G$ that takes the kth letter to x_k, i.e. it takes a to x_1, b to x_2, etc.

Definition: A set of elements $x_1, \ldots, x_n \in G$ generates G if the corresponding map $F_n \to G$ that maps the kth letter to x_k is surjective. This means that every element in G has a corresponding "word" in the free group.

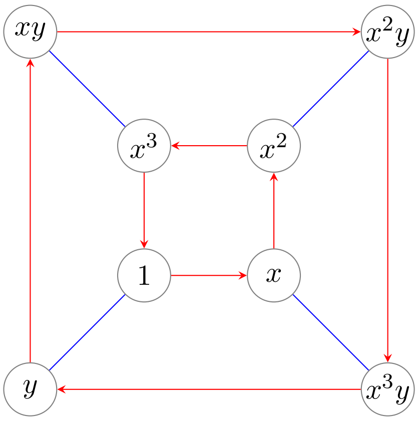
We now consider the dihedral group D_n it is generated by two elements: a rotation x and a reflection y. To understand this group better, we examine some of the relations of these elements. We see that $x^n = 1$, $y^2 = 1$, and $xy = yx^{-1}$. We would like to be able to write a statement describing the complete list of relations for this group, as we did for the generators with the free group. We consider the map $\Phi : F_2 \to D_n$ which takes a to x and b to y. We know that Φ is surjective, so $D_n \cong F_2/\ker(\Phi)$ by the First Isomorphism Theorem. Relations can then be thought of as element of $\ker(\Phi)$. We see that $a^n \in \ker\Phi$, $b^2 \in \ker(\Phi)$, and $abab \in \ker\Phi$.

Definition: A complete set of relations for a group with a generating set is a set of generators of the kernel of the map $\Phi : F_n \to G$.

Definition: A Cayley Graph is a visualization of a group with a generating set. The graph is a collection of vertices and directed edges. The vertices represent the elements of the group and an edge is formed from an element x to gx, where g is in the generating set. The edge is labeled g.

Our Cayley graph for D_n is a tree, i.e. it contains no loops. This is because there is no relation between a and b. Drawn in the plane, it exhibits fractal structure, with four edges at every vertex.

We now consider D_4, whose elements are $1, x, x^2, x^3, y, xy, x^2y, x^3y$. The Cayley graph is the following:



Here the red arrows represent left multiplication by x and the blue line represent left multiplication by y. The blue lines are not directed because $y = y^{-1}$. We observe several loops in this diagram that correspond to relations, such as $xyxy = 1$.

Bilinear Forms

Definition: Given a vector space V over a field K, a bilinear form is a map $B : V \times V \to K$ that is linear in both arguments, i.e. $B(av, w) = aB(v, w)$ and $B(v_1 + v_2, w) = B(v_1, w) + B(v_2, w)$ and $B(v, aw) = aB(v, w)$ and $B(v, w_1 + w_2) = B(v, w_1) + B(v, w_2)$.

Some nice properties B could have:

1) Symmetric: $B(v, w) = B(w, v)$.
Subcategory: Positive-Definite ($K = \mathbb{R}$): $B(v, v) > 0$ for $v \neq 0$.

2) Skew-Symmetric: $B(v, w) = -B(w, v)$.
Caveat: In fields of characteristic 2, this condition is vacuous and we instead require that $B(v, v) = 0$. We see that this would imply the former condition by examining $0 = B(v + w, v + w) = B(v, v) + B(v, w) + B(w, v) + B(w, w) = B(v, w) + B(w, v)$. The previous equation is known as the polarization identity. The polarization identity on a the standard inner product yields the parallelogram identity.

When $K = \mathbb{C}$, our forms are bilinear over $\mathbb{R}$, but sesquilinear over $\mathbb{C}$. This means they are conjugate linear in one argument but linear in the other, i.e. $B(cv, dw) = \bar{c}dB(v, w)$. This leads to a third type of form:

3) Hermitian: $B(v, w) = \overline{B(v, w)}$. A Hermitian form is also called a symmetric sesquilinear form.
Lemma: $B(v, v) \in \mathbb{R}$ if B is Hermitian.
Proof: $B(v, v) = \overline{B(v, v)}$, so $B(v, v) \in \mathbb{R}$.

Lecture 30
November 18

More on Bilinear Forms

Given a bilinear form B on V and a basis $\{v_i\}$, we can associate with B a matrix A with entries $A_{ij} = B(v_i, v_j)$.

Claim A determines the bilinear form.
Proof: $B\left(\sum\limits_{i=1}^{n} a_i vi, \sum b_j v_j\right) = \sum\limits_{i=1}^{n}\sum\limits_{j=1}^{n}(a_i b_j B(v_i, v_j)) = \sum\limits_{i=1}^{n}\sum\limits_{j=1}^{n}(a_i b_j A_{ij})$.

Claim: If each element is expressed in this basis, $B(v, w) = v^T A w$.

Proof: One method is just to compute the product: $\begin{bmatrix} a_1 & \cdots & a_n \end{bmatrix} \begin{bmatrix} A_{ij} \end{bmatrix} \begin{bmatrix} b_1 \\ \vdots \\ b_n \end{bmatrix} = \begin{bmatrix} a_1 & \cdots & a_n \end{bmatrix} \begin{bmatrix} \sum\limits_j b_j A_{1j} \\ \vdots \\ \sum\limits_j b_j A_{nj} \end{bmatrix} =$ $\sum\limits_i \sum\limits_j a_i b_j A_{ij}$. This is the same result we found previously.
Another method is to see that $(v, w) \mapsto v^T A w$ defines a bilinear map, and $v_i^T A v_j = A_{ij}$. Thus we have two bilinear forms that take the same values on the basis vectors, so they must be equivalent.

Now we shall consider a change of basis. We let $w_i = P v_j$, i.e. $w_i = \sum\limits_j P - ijv_j$. If we think of the $\{v_i\}$ as the standard orthonormal basis, then $w_i = \begin{bmatrix} P_{i1} \\ \vdots \\ P_{in} \end{bmatrix}$. We then compute $B(w_i, w_j) = B(Pv_i, Pv_j) = (Pv_i)^T A (Pv_j) = v_i^T \left(P^T A P\right) v_j$. In the $\{v_i\}$ basis, the matrix $P^T A P$ has entries equal to $v_i^T \left(P^T A P\right) v_j$.

Symmetric Forms

Examples:
$A = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$ with form $B\left(\begin{bmatrix} v_1 \\ v_2 \\ v_3 \end{bmatrix}, \begin{bmatrix} w_1 \\ w_2 \\ w_3 \end{bmatrix}\right) = v_1 w_1 + v_2 w_2 + v_3 w_3$. This is the standard inner product.
$A = \begin{bmatrix} -1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$ with form $B\left(\begin{bmatrix} v_1 \\ v_2 \\ v_3 \end{bmatrix}, \begin{bmatrix} w_1 \\ w_2 \\ w_3 \end{bmatrix}\right) = -v_1 w_1 + v_2 w_2 + v_3 w_3$. This form is not positive-definite, as we can see in $B\left(\begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix}, \begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix}\right) = -1$. We can also write $B(v, v) = -v_1^2 + v_2^2 + v_3^2$. The level sets of this expression ($-v_1^2 + v_2^2 + v_3^2 = c$) are hyperboloids with v_1 as their main axis. When $c = 0$, the surface is a degenerate hyperboloid, i.e. a conical surface, known as the null cone. If $c < 0$, the surface is a hyperboloid of two sheets that lies inside the null cone, while if $c > 0$, the surface is a hyperboloid of one sheet that lies outside the null cone.

Theorem: A matrix A is symmetric and positive-definite if and only if $A = P^TP$ for some invertible matrix P, i.e. up to a change of basis, any symmetric positive-definite bilinear form is equivalent to the standard one.
Proof: Delayed.

Nondegenerate Forms and Orthogonality

Definition: A symmetric (or skew-symmetric) form is nondegenerate if there is no vector v (called a null vector) such that $B(v, w) = 0 \; \forall \; w$.

Definition: Given that W is a subspace of V which is endowed with a bilinear form B, the orthogonal subspace $W^\perp = \{v \in V \mid B(v, w) = 0 \; \forall \; w \in W\}$.

Example: Let $W = \text{span}\left(\begin{bmatrix}1\\1\\0\end{bmatrix}\right)$ in $\mathbb{R}^{2,1} = \mathbb{R}^3$ endowed with the previous bilinear form. (This notation means that there are two positive ones on the diagonal and one negative one). We see that $W^\perp = \text{span}\left(\begin{bmatrix}1\\1\\0\end{bmatrix}, \begin{bmatrix}0\\0\\1\end{bmatrix}\right)$. We see that $W \subset W^\perp$.

Proposition: Suppose B is nondegenerate on V. Then B is nondegenerate on $W \subset V$ if and only if $V = W \oplus W^\perp$.
Proof: The backward direction is easy, as $V = W \oplus W^\perp$ implies that $W \cap W^\perp = 0$. This means that there is no nonzero vector in W that yields 0 under the form when paired with every vector in W, i.e. B is nondegenerate on W.
For the forward direction, we use the above fact that the nondegeneracy of B on W implies that $W \cap W^\perp = 0$. We want to express $W^\perp$ in terms of the matrix for the form, A. We begin by describing the set of degenerate vectors in V in terms of A. This is just $\ker(A)$, as w^TAv can only be 0 for all $w \in V$ if $Av = 0$. Now we want to describe the degenerate vectors in $W^\perp$. We can express the condition of degeneracy as $\begin{bmatrix}\vec{w}_1 & \cdots & \vec{w}_k\end{bmatrix}^T Av = 0$, with $v \in W^\perp$ and $\{w_i\}$ being a basis of W, since this implies that $\vec{w}_i^T Av = 0$ for all $\{w_i\}$. We must determine the rank of $\begin{bmatrix}\vec{w}_1 & \cdots & \vec{w}_k\end{bmatrix}^T A$. We know that A is invertible, since B is nondegenerate on V. Since multiplication by an invertible matrix does not change the rank, and the rank of $\begin{bmatrix}\vec{w}_1 & \cdots & \vec{w}_k\end{bmatrix}^T$ is k, the rank of the product is k as well. Thus the dimension of $W^\perp$ is $n - k$ by the Rank-Nullity Theorem. Since $W \cap W^\perp = 0$, $V = W \oplus W^\perp$.

Lecture 31
November 20

Symmetric Forms

Let $B(\cdot,\cdot)$ be a symmetric form on V, a vector space over $\mathbb{R}$ of dimension n. We saw that if B is nondegenerate on v, nondegeneracy on $W \subset V$ implies that $V = W \oplus W^{\perp}$.

Theorem: There exists an orthogonal basis for V, and moreover we may take $B(v_i, v_j) = 1, -1$, or 0, where $\{v_i\}$ is the basis of V. Equivalently, if A is a symmetric matrix, then there exists an invertible matrix P such that $P^T AP = \text{diag}(1, \cdots, 1, -1, \cdots, -1, 0, \cdots, 0)$.
Proof: To see the zeroes, we take some basis of $V^{\perp}$. These are degenerate vectors. We then restrict the form to the complement of $V^{\perp}$, where it is nondegenerate. We then claim that given a nondegenerate symmetric form, there exists v such that $B(v, v) \neq 0$. To prove this, we consider $B(v + w, v + w) = B(v, v) + B(w, w) + 2B(w, w)$, so $B(v, w) = 0$, i.e. the form is trivial. We then induct on the dimension of V. There must be some v such that $B(v, v) \neq 0$. We rescale it to λv, which implies that $B(\lambda v, \lambda v) = \lambda^2 v$. We then can choose λ to be ± 1. We then consider $\text{span}(v) \oplus \text{span}(v)^{\perp}$, which gives us a matrix of the form $\begin{bmatrix} *_{1\times 1} & 0_{1\times n-1} \\ 0_{n-1\times 1} & *_{n-1\times n-1} \end{bmatrix}$. We then induct on the dimension of $\text{span}(v)^{\perp}$.

Theorem: The number of 1s, number of -1s, and the number of 0s in the previous theorem are independent of our choice of basis.
Proof: The number of 0s is the dimension of $V^{\perp}$. We realize that the number of 1s and -1s is $\dim(V) - \dim(V^{\perp})$. We claim that the number of -1s is the largest dimension of a negative definite subspace, i.e. a subspace such that $B(v, v) < 0$ for all $v \neq 0$ in the subspace. To prove this, we let $\{v_1, \dots, v_k\}$ be our basis vectors of the k columns with 1s. These are orthogonal. We suppose $\{w_1, \dots, w_{\ell+m}\}$ is a basis for a negative-definite subspace, with $m > 0$. We then claim that $\{v_1, \dots, v_k, w_1, w_{\ell+m}\}$ is a linearly independent set. We assume for the sake of contradiction that it is not. Then there is some linear combination $a_1v_1 + \cdots + a_kv_k = b_1w_1 + \cdots + b_{\ell+m}w_{\ell+m}$ with not all the coefficients equal to 0. We call this combination u. Since u is in the negative-definite subspace, $B(u, u) < 0$ unless $u = 0$. However, since u is a combination of the $\{v_i\}$, which have positive entries, $B(u, u) = \sum a_i^2 > 0$ unless $u = 0$. Thus $u = 0$, so the linear combination is trivial and thus the set is linearly independent. This gives us a classification of the nondegenerate symmetric bilinear forms on $\mathbb{R}^n$ up to a change of basis. We have $B_{k,n-k}$, a form with k 1s, and $n - k$ -1s, and $\mathbb{R}^{k,n-k}$, i.e., $\mathbb{R}^n$ equipped with this form.

We have already considered $O(n)$, the set of matrices the preserved the standard inner product, i.e., $O(n) = \{M \in GL_n(\mathbb{R}) \mid \langle Mv, Mw\rangle = \langle v, w\rangle \ \forall\ v, w\}$. We can extend this to matrices that preserve any bilinear form: $O(k, n-k) = \{M \in GL_n(\mathbb{R}) \mid B_{k,n-k}(Mv, Mw) = B_{k,n-k}(v, w) \ \forall\ v, w\}$. These are matrices M such that $v^T M^T A_{k,n-k} M w = v^T A_{k,n-k} w$, i.e. $M^T A_{k,n-k} M = A_{k,n-k}$, where $A_{n,n-k} = \begin{bmatrix} I_k & 0 \\ 0 & -I_{n-k} \end{bmatrix}$.
Corollary: If $M \in O(n, n-k)$, $\det(M) = \pm 1$.
Proof: $\det(M^T)\det(A_{n,n-k})\det(M) = \det(A_{n,n-k})$ implies that $\det(M)^2 = 1$.

We also see that $SO(k, n-k) < O(k, n-k)$ is the set of matrices with determinant 1.

Theorem: Given a symmetric matrix A, A is positive-definite, i.e. $B(v,w) = v^T Aw$ is positive-definite, if and only if $\det(A_i) > O \ \forall \ i$, where $A = \begin{bmatrix} A_i & * \\ * & * \end{bmatrix}$, i.e. the determinants of all the upper left blocks (known as the principal minors) are positive.

Proof: For the forward direction, we claim that a positive definite matrix has a positive determinant, i.e. A_i is the matrix for the form B on a subspace V_i, spanned by $\{v_1, \ldots, v_i\}$, the first i basis vectors. Since A is positive-definite, we know that $A = P^T IP$ for some invertible matrix P, so $\det(A) = \det(P^2) > 0$. Thus $\det(A) = 1$.

For the backward direction, we induct on the dimension of V_i The base case is simple: if $B(v_1, v_1) > 0$, then B is positive-definite on $V_1 = \text{span}(v_1)$. In our inductive step, we assume B is positive definite on V_{n-1}. We change basis on V_{n-1} to yield the identity for A_i, i.e. the matrix is now $\begin{bmatrix} I_{n-1} & * \\ * & * \end{bmatrix}$.If we change basis, the sign of the determinant does not change. Thus we have two cases.

Case 1: We have that $B(v_n, v_n) = 0$. We change basis so that we have λv_n instead and compute $B(v_i + \lambda v_n, v_i + \lambda v_n) = B(v_i, v_i) + 2\lambda B(v_i, v_n) + 0$ for some $\lambda \neq 0$. This is not 0, so we now have the second case.

Case 2: We have $B(v_n, v_n) \neq 0$. We choose $v_i' = v_i - \frac{B(v_i,v_n)}{B(v_n,v_n)} v_n$ with $B(v_i', v_n) = 0$. In our new basis, we have $\begin{bmatrix} I_{n-1} & 0 \\ 0 & * \end{bmatrix}$, where $* > 0$ because the determinant is greater than 0, so the matrix is positive-definite.

Lecture 32
November 22

Hermitian Forms and Group Theoretic Consequences

We consider a Hermitian form $B : V \times V \to \mathbb{C}$, where V is a vector space of dimension n over $\mathbb{C}$. We have that B is conjugate linear in the one factor (usually the first) and linear in the other factor, i.e. $B(cv, w) = \bar{c}B(v, w)$ and $B(v, cw) = cB(v, w)$. We also add a symmetry condition: $B(v, w) = \overline{B(w, v)}$. For this reason a Hermitian form is also called a symmetric sesquilinear form. We also see that $\mathrm{Re}(B)$ is bilinear and symmetric, while $\mathrm{Im}(B)$ is bilinear and skew-symmetric.

Claim: Let $\{v_i\}$ be a basis over $\mathbb{C}$ and let $a_{ij} = B(v_i, v_j)$. In this basis, $B(v, w) = v^*Aw$, where A is the matrix associated with B, and $v^* = \overline{v^T}$.
Proof: We consider $B(v, w) = B(\sum c_i v_i, \sum d_j v_j) = \sum \overline{c_i} a_{ij} d_j = v^*Aw$. We see that Hermitian symmetry means $B(v_i, v_j) = \overline{B(v_j, v_i}$, i.e. $A^* = A$. (A^* is known as the adjoint). If we change basis, we send A to P^*AP, because $(Pv)^*A(Pw) = v^*(P^*AP)w$..

We see that $(\mathbb{C}^N, \langle \cdot, \cdot \rangle)$ has an operation given by $\langle v, w \rangle = v^*w$. Note that $\langle v, Tw \rangle = \langle T^*v, w \rangle$, as $\langle v, Tw \rangle = v^*Tw$ and $\langle T^*v, w \rangle = (T^*v)^*w = v^*Tw$.

We then consider the other linear maps $T : \mathbb{C}^N \to \mathbb{C}^N$ preserving $\langle \cdot, \cdot \rangle$. We must have $\langle Tv, Tw \rangle = \langle v, w \rangle$, i.e. $v^*T^*Tw = v^*w \ \forall \ v, w$, which implies that $T^* = T^{-1}$.

Definition: A linear map $T : \mathbb{C}^N \to \mathbb{C}^N$ is unitary if $T^* = T^{-1}$, or equivalently if it preserves the operation $\langle \cdot, \cdot \rangle$ described above. The unitary maps form a group $U(n)$

Note that we can now think of the matrix associated with our Hermitian form, A as associated with a linear map from $\mathbb{C}^N$ to $\mathbb{C}^N$, which we also will call Hermitian.

Spectral Theorem: If T is Hermitian, T has an orthonormal basis of eigenvectors. Equivalently, there is a unitary change of basis that diagonalizes T, i.e. there is some $P \in U(n)$ such that $P^{-1}TP$ is diagonal.
Proof: Because our field is $\mathbb{C}$, T must have at least one eigenvector v. We normalize the vector and then extend it to an orthonormal basis of $\mathbb{C}^N$ (using the Graham-Schmidt process). We call our change of basis matrix P_1, so $P_1^*TP_1 = \begin{bmatrix} \lambda & *_{1\times n-1} \\ 0_{n-1\times 1} & *_{n-1\times n-1} \end{bmatrix}$. This matrix must still be Hermitian, so $*_{1\times n-1} = 0_{1\times n-1}$. P_1 is unitary because our basis was orthonormal. We then consider on the subspace spanned by $\{v_2, \dots, v_n\}$, i.e. the subspace associated with $*_{n-1\times n-1}$, and proceed by induction.

Theorem: The eigenvalues of a Hermitian operator are real.
Proof: We consider $\overline{\lambda} \langle v, v \rangle = \langle \lambda v, v, = \rangle \langle Tv, v \rangle = \langle v, Tv \rangle = \langle v, \lambda v \rangle = \lambda \langle v, v \rangle$, so $\lambda = \overline{\lambda}$ and $\lambda \in \mathbb{R}$.

Spectral Theorem over the Reals: If T is symmetric, T has an orthonormal basis of eigenvectors. Equivalently, there is an orthogonal change of basis that diagonalizes T, i.e. there is some $P \in U(n)$ such that $P^{-1}TP$ is diagonal.
Proof: T is Hermitian over $V_{\mathbb{C}}$, so it has a real eigenvalue λ, so $\det(A - \lambda I) = 0$, which implies there is a real eigenvector in V. We then proceed via the same proof as before.

Powers of Positive Symmetric Matrices

Note that all of the following can be done for Hermitian and unitary matrices in place of symmetric and orthogonal. We let A be a positive symmetric matrix, so it will have an orthonormal basis of eigenvectors. (Here a positive matrix is one with an associated positive-definite form). We define A^r with $r \in \mathbb{R}_{>0}$ as $A^r v = \lambda^r v$ if $Av = \lambda v$, which is well-defined. An application of this is the polar decomposition, which begins with the following.

Theorem: If $A \in GL_n(\mathbb{R})$, then AA^T is symmetric, and the eigenvalues of AA^T are positive.
Proof: $\lambda \langle v, v \rangle = \left\langle AA^T v, v \right\rangle = \left\langle A^T v, A^T v \right\rangle \geq 0$. None of the eigenvalues can be zero because A is invertible.

We then consider $(AA^T)^{-1/2}A$. We see that if $AA^T = I$, then A would be orthogonal. We then claim that $(AA^T)^{-1/2}A \in O(n)$. This is just a calculation: $\left((AA^T)^{-1/2}A\right)^T \left((AA^T)^{-1/2}A\right) = A^T T(AA^T)^{-1/2}(AA^T)^{-1/2}A = A^T(AA^T)^{-1}(AA^T)^{-1/2}A = A^T(A^T)^{-1}A^{-1}A = I$.

Corollary: Given $A \in GL_n(\mathbb{R})$, $A = BC$ for a positive and symmetric matrix $B = (AA^T)^{1/2}$ and an orthogonal matrix $C = (AA^T)^{-1/2}A$. In fact, this decomposition is unique.
Proof: To show uniqueness, we suppose $A = B_1C_1 = B_2C_2$. with B_i positive and symmetric and C_i arbitrary. Then $\left(B_1C_1(B_1C_1)^T\right)^{1/2} = \left(B_1C_1C_1^TB_1^T\right)^{1/2} = \left(B^2\right)^{1/2} = B$.

Theorem: The cosets of $O(n)$ in $GL_n(\mathbb{R})$ are in one-to-one correspondence with the set of positive symmetric matrices. This also works for $SO(n)$ in $SL_2(\mathbb{R})$.

Example: We know that $SL_2(\mathbb{R}) = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$ such that $ad - bc = 1$ and $SO_2(\mathbb{R}) = \begin{bmatrix} \cos\theta & -\sin\theta \\ \cos\theta & \sin\theta \end{bmatrix}$, which we can think of as a circle. The positive symmetric matrices in $SL_2(\mathbb{R})$ must be of the form $\begin{bmatrix} a & b \\ b & c \end{bmatrix}$ such that $ac - b^2 = 1$. Thus $b \in \mathbb{R}$, $c \in \mathbb{R}_{>0}$, and $a = (1 + b^2)/c$. Thus $SL_2(\mathbb{R})$ is topologically equivalent to an open solid torus with core $SO_2(\mathbb{R})$.

Lecture 33
November 25

Sample Solutions from Exam 2

2. Let V be a vector space over $\mathbb{C}$ of dimension n and let $T : V \to V$ be a linear map. Suppose that the only eigenvalues of T are 0 and 1. Show that the $\ker((T-I)^n) = \operatorname{im}(T^n)$.

We know that $V^{(\lambda)} = \ker((T-\lambda I)^n)$ and $V = \bigoplus\limits_{\operatorname{Spec}(T)} V^{(\lambda_i)}$. If our eigenvalues are 0 and 1, this tells us that $V = V^{(0)} \oplus V^{(1)} = \ker((T-I)^n) \oplus \ker(T^n)$. We also know that $V = \operatorname{im}(T^n) \oplus \ker(T^n)$. This does not immediately imply that $\ker((T-I)^n) = \operatorname{im}(T^n)$, however. As a counterexample, we could have two lines that span the plan, and we could rotate one without chaning the span. Thus we use the fact that $\ker(T^n)$ and $\operatorname{im}(T^n)$ are T-invariant. We then consider $v \in \ker((T-I)^n)$. Then $v = v_i + v_k$, with $v_i \in \operatorname{im}(T^n)$ adn $v_k =\in \ker(T^n)$. We also see that $\ker(T^n)$ and $\operatorname{im}(T^n)$ are $(T-I)^n$-invariant. This means that v_i and v_k are in $\ker((T-I)^n)$, because $(T-I)^n v = 0$ and $\operatorname{im}(T^n) \cap \ker(T^n) = \{0\}$. Thus $v_k \in \ker(T^n) \cap \ker((T-I)^n) = \{0\}$, so $v = v_i$ and thus $\ker((T-I)^n) = \operatorname{im}(T^n)$.

3. (a) List all isomorphism classes of groups of order 20.
(b) How many distinct isomorphism classes are there?

We see that $20 = 2^2 \cdot 5$. The number of Sylow 2-subgroups is equivalent to 1 modulo 2 and divides 5, so it is either 5 or 1. The Sylow 2-subgroup(s) must have order 4, so they are C_4 or $C_2 \times C_2$. The number of Sylow 5-subgroups is equivalent to 1 modulo 5 and divides 4, so it is 1. The Sylow 5-subgroup must have order 4, so it is C_5. This must be normal, because it has no proper conjugate subgroups. Thus we have 2 cases, because the product of the Sylow subgroups is the whole group and one is normal:
1. $C_5 \underset{\phi}{\rtimes} (C_2 \times C_2)$
2. $C_5 \underset{\phi}{\rtimes} C_4$

In the first case, we consider $\phi : (C_2 \times C_2) \to \operatorname{Aut}(C_5) \cong C_4$. Every element in C_2 maps to something in C_4 of order 2. One option is the trivial map that maps every element to the identity. This yields a direct product $G = C_2 \times C_2 \times C_5$. Note that we can also look at this map as $\phi : (C_2 \times C_2) \to C_2 = \{1, x^2\} \subset C_4$. Other than the trivial map, the only other option is the maps that sends two elements to the identity and two elements to x^2. If we choose the latter options, we find $G = C_2 \times (C_2 \underset{\phi}{\rtimes} C_5) = C_2 \times D_5 = D_{10}$.

In the second case, we consider $\phi : C_4 \to \operatorname{Aut}(C_5) \cong C_4$. There are four possible maps. If x maps to 1, then $G = C_4 \times C_5$. The maps that map x to x or x^3 are equivalent up to renaming C_4. If x maps to x^2, we find something different. Showing that it is not isomorphic to any other case is let as an exercise.

Thus we have 5 isomorphism classes:
1. $C_5 \times C_2 \times C_2$
2. $C_5 \times C_4$
3. D_{10}
4. $C_5 \underset{\phi_2}{\rtimes} C_4$, with $\phi_2(x) = x$
5. $C_5 \underset{\phi_3}{\rtimes} C_4$, with $\phi_3(x) = x^2$.

Normal Operators

We have previously considered Hermitian operators, i.e. linear maps from $\mathbb{C}^n$ equipped with the usual inner product to itself, with $T = T^*$. We also looked at unitary operators, which are maps on the same inner product space with $T^{-1} = T^*$. Both are special cases of a normal operator, which is a map that commutes with its adjoint, i.e. $TT^* = T^*T$.

Spectral Theorem (Version 2): T is normal if and only if it is diagonalizable by a unitary transformation, i.e. if there exists an orthonormal eigenbasis.
Proof: Since the field is $\mathbb{C}$, T must have an eigenvector v. We normalize this vector and then extend it to an orthonormal basis. Then we change to this basis by a unitary transformation: $U^{-1}TU$. This is still normal, as $(U^*TU)(U^*T^*U) = U^*TT^*U = U^*T^*TU = (U^*T^*U)(U^*TU)$. Then we see

$$U^*TU = T_1 = \left[\begin{array}{c|ccc} a_1 & a_2 & \cdots & a_n \\ \hline 0 & & & \\ \vdots & & M & \\ 0 & & & \end{array}\right] \text{ and } T_1^* = \left[\begin{array}{c|ccc} a_1 & 0 & \cdots & 0 \\ \hline \overline{a_2} & & & \\ \vdots & & M^* & \\ \overline{a_n} & & & \end{array}\right].$$

We consider the upper left entry of the two products $(T_1T_1^*)_{11} = \sum a_i\overline{a_i} = \sum |a_i|^2$ and $(T_1^*T_1)_{11} = a_i\overline{a_i} = |a_i|^2$. If these are equal, then $a_i = 0 \ \forall\ i > 2$. We then induct, considering M and M^*, which must also commute. This diagonalizes the matrix.

Corollary: Conjugacy classes of $U(n)$ are in one-to-one correspondence with diagonal unitary matrices.

Note that a normal operators N can be represented as $N = U^*DU$, where U is unitary and D is diagonal.

Skew-Symmetric Bilinear Forms

We consider a skew-symmetric bilinear form $B(\cdot,\cdot)$ on V of dimension n over the field $\mathbb{R}$.

Theorem: Suppose B is nondegenerate. Then n is even, and, after a change of basis, $B(v,w) = -v^TJ_nw$, where $J_n = \begin{bmatrix} 0_{m\times m} & -I_m \\ I_m & 0_{m\times m}\end{bmatrix}$. This new basis is called the standard symplectic basis for B. If we write this basis as $\{v_1,\dots,v_m,w_1,\dots,w_m\}$, then it has the following properties:
1. $B(v_i,w_j) = \delta_{ij}$
2. $B(v_i,v_j) = B(w_i,w_j) = 0$.
Proof: We shall prove by induction on the dimension of V. The base cases are that 0 works and 1 doesn't. In the inductive step, we choose $v \in V$ such that there exists $w \in v$ such that $B(v,w) \neq 0$. We rescale one of the vectors such that $B(v,w) = 1$. Then we let $V_1 = \text{span}(v,w)$ and $V_2 = \{u \in V \mid B(u,u') = 0 \ \forall\ u' \in V_1\}$. Because B is nondegenerate, $\dim(V_2) + \dim(V_1) = \dim(V)$ and $V_2 \cap V_1 = \{0\}$. Then the matrix of the form is $\begin{bmatrix} \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} & 0_{n-2\times n-2} \\ 0_{n-2\times n-2} & *_{n-2\times n-2}\end{bmatrix}$. We then proceed by induction and rearrange our basis to yield the correct block form.

Lecture 34
December 2

Representations of Finite Groups

Definition: A representation of a group G on a vector space V is a linear action of G on V (i.e. elements of G act by linear transformations), or equivalently, a homomorphism $R : G \to GL(V)$.

We use R_g to denote $R(g)$, and we see that $g \cdot (h \cdot v) = (gh)v$ is equivalent to $R_g R_h(v) = R_{gh}(v)$.

We'll consider complex representations which are representations of G on $\mathbb{C}^n$, i.e., homomorphisms to $GL_n(\mathbb{C})$.

Definitions:

The trivial representation is $R_g = I \ \forall \ g \in G$.

A representation is faithful if $R_g \neq R_n$ if $g \neq n$, which gives an injection $G \hookrightarrow GL_n(\mathbb{C})$.

The dimension of a representation is the dimension of the vector space.

The character of a representation $R : G \to GL_n(\mathbb{C})$ is a map $\chi_R : G \to \mathbb{C}$ defined by $\chi_R(g) = \text{tr}(R_g)$.

Examples:

We consider a one-dimensional representation $R : G \to GL_1(\mathbb{C}) = \mathbb{C}^*$. Then $[\chi_R(g)] = R_g$, i.e. they are equal in $\mathbb{C}^* \subset \mathbb{C}$.

We consider the group $D_3 = \{1, x, x^2, y, yx, yx^2\}$, where x is a rotation by $2\pi/3$ and y is a reflection. We know that $D_3 \cong S_3$, so we can also represent this way with $x = (1\ 2\ 3)$ and $(1\ 2)$. In terms of generators and relations, D_3 is generated by x and y, with $x^3 = 1$, $y^2 = 1$, and $yx = x^{-1}y$. We consider the one-dimensional trivial representation, $R_{\text{triv}} = [1]$. We then consider the standard two-dimensional representation, defined with $R_{st}(y) = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$ and $R_{st}(x) = \begin{bmatrix} \cos 2\pi/3 & -\sin 2\pi/3 \\ \sin 2\pi/3 & \cos 2\pi/3 \end{bmatrix} = \begin{bmatrix} -1/2 & -\sqrt{3}/2 \\ \sqrt{3}/2 & -1/2 \end{bmatrix}$. We can also consider $\mathbb{R}_{\text{sign}} : S_3 \to \{\pm 1\} \subset \mathbb{C}^*$ defined by $g \mapsto \text{sign}(g)$. In one dimension, $R_{\text{sign}}(x) = [1]$ and $\mathbb{R}_{\text{sign}}(x) = [-1]$. Now let's build a table:

	1	x	x^2	y	yx	yx^2
$\chi_{R_{\text{triv}}}$	1	1	1	1	1	1
$\chi_{R_{\text{sign}}}$	1	1	1	-1	-1	-1
$\chi_{R_{\text{st}}}$	2	-1	-1	0	0	0

Claim: χ_R is constant on conjugacy classes.
Proof: $\chi_R(ghg^{-1}) = \text{tr}(R_{ghg^{-1}}) = \text{tr}(R_g R_h R_{g^{-1}} = \text{tr}(R_h) = \chi_R(h)$

Direct Sums, Irreducible Representations, and Maschke's Theorem

Suppose we have a representation of G on a vector space V.

Definition: $W \subset V$ is invariant under the action of G if $g \cdot w \in W \in W$ forall $w \in G$, $g \in G$.

Definition: A representation if irreducible if there are no proper nontrivial subspaces.

Definition: A direct sum of representations $R_1 : G \to GL_(V_1)$ and $R_2 : G \to GL_(V_2)$ is the map $R : G \to GL(V_1 \oplus V_2)$ where $R_g(v_1 \oplus v_2) = R_{g_1}(v_1) \oplus R_{g_2}(v_2)$, i.e. $R_g = \begin{bmatrix} R_{g_1} & 0 \\ 0 & R_{g_2} \end{bmatrix}$.

Maschke's Theorem: Every representation is isomorphic to a direct sum of irreducible representations.
Proof First we shall show that any complex representation of a finite group preserves some positive definite Hermitian form. We take the standard Hermitian form $\langle \cdot, \cdot \rangle$ on $\mathbb{C}^n$. We let $B(v, w) = \frac{1}{|G|} \sum\limits_{g \in G} \langle g \cdot v, g \cdot w \rangle$. This form is Hermitian, as it is symmetric, linear and conjugate linear in the appropriate arguments, and positive definite, as $g \cdot v \neq 0$ if $v \neq 0$. With $h \in G$, we then claim that $B(v, w) = B(h \cdot v, h \cdot w) = B(R_h(v), R_h(w))$. $B(h \cdot v, h \cdot w) = \frac{1}{|G|} \sum\limits_{g \in G} \langle g \cdot h \cdot v, g \cdot h \cdot w \rangle = \frac{1}{|G|} \sum\limits_{gh^{-1} \in G} \langle gh^{-1} \cdot h \cdot v, gh^{-1} \cdot h \cdot w \rangle = B(v, w)$.
Now, given a reducible representation, we consider $W \subset V$ that is invariant under G. We let $B(\cdot, \cdot)$ be the invariant Hermitian form and let $W^\perp$ be its orthogonal complement with respect to B. If $u \in W^\perp$, then $B(u, w) = 0\ \forall\ w$, so $B(gu, gw) = 0\ \forall\ w$, so $gu \in W^\perp$. Thus $W^\perp$ is also invariant under G.

Morphisms of Representations

We consider $T : V \to W$. Suppose G acts on V and W. Then T is $G-$linear or is a morphism of representations of G if $T \circ R_{V,g} = R_{W,g} \circ T\ \forall\ g \in G$.

Lecture 35
December 4

Representations and Character Tables

Schur's Lemma: Suppose $R : G \to GL(V)$ and $R' : G \to GL(V')$ are two irreducible representations. Then:
1. Given $T : V \to V'$ that commutes with the action of G, then $T = 0$ or T is an isomorphism.
2. If $R = R'$, $V = V'$ and $T = \lambda I$.
Proof: Consider $\ker(T) \subset V$. We claim that this is a G-invariant subspace, i.e. if $v \in \ker(T)$, then $R_g(v) \in \ker(T)\ \forall\ g \in G$. We see that $Tv = 0$, then $TR_g(v) = R'_g Tv = 0$, so $R_g(v) \in \ker(T)$. Thus $\ker(T) = \{0\}$ or V. If $\ker(T) = V$, $T = 0$. If $\ker(T) = 0$, we consider $\mathrm{im}(T) \subset V'$. We claim this is also a G-invariant subspace. Suppose $w = Tv \in \mathrm{im}(T)$. Then $R'_g(w) = R'_g(Tv) = TR_g v \in \mathrm{im}(T)$. Thus $\mathrm{im}(T) = \{0\}$ or V'. It is not $\{0\}$ unless $V = 0$ or $T = 0$. So the only nontrivial case is that $\ker(T) = \{0\}$ and $\mathrm{im}(T) = V$. Thus T is an isomorphism.
Now we assume that $R = R'$, and we consider $T - \lambda I$ with λ an eigenvalue. Then $\ker((T - \lambda I)^n)$ is G-invariant, so it is V, as it can't be $\{0\}$ because there already is an eigenvalue. Thus $T = \lambda I$.

We conclude from this that if V is a general representation, i.e. $V \cong V_1 \oplus \cdots \oplus V_k$ and $V \cong W_1 \oplus \cdots \oplus W_\ell$, where V_i and W_j are irreducible representations, then the lists $\{V_i\}$ and $\{W_j\}$ are, up to reordering, isomorphic.

We recall that the character of a representation $R : G \to GL(V)$ is a map $\chi_R : G \to \mathbb{C}$ defined by $\chi_R(g) = \mathrm{tr}(R_g)$. Note that this is not a homomorphism.

We consider a positive-definite Hermitian form on the space of all maps $G \to \mathbb{C}$ given by $\langle \phi, \phi' \rangle = \dfrac{1}{|G|} \sum\limits_{g \in G} \overline{\phi(g)} \phi'(g)$.

We consider some useful facts about the character $\chi_R : G \to \mathbb{C}$:
1. $\chi_R(ghg^{-1} = \chi_R(h)$ because $\mathrm{tr}(RgR_hR_{g^{-1}} = \mathrm{tr}(R_h)$.
2. $\chi_R(g^{-1}) = \overline{\chi_R(g)}$. This follows because any representation T is unitary with respect to some basis, so the eigenvalues all have a norm of 1. Thus $\chi_R(g)$ is the sum of eigenvalues, weighted by their multiplicities, and $\chi_R(g^{-1})$ is the sum of the reciprocals of the eigenvalues, which is the sum of the conjugates, because $\lambda^{-1} = \overline{\lambda}$ if $\lambda\overline{\lambda} = 1$.

Theorem: The characters of irreducible representations are orthonormal, i.e. $\langle \chi_R, \chi_{R'} \rangle = 1$ if $R \cong R'$ and 0 otherwise. Additionally, the characters of irreducible representations span the space of maps $G \to \mathbb{C}$ which are constant on conjugacy classes (known as class functions).
Proof: We consider two matrices A and B of size $m \times m$ and $n \times n$, respectively. We consider the operator $F_{A,B}$ on $\mathbb{C}^{m\times n}$ (the vector space of $m \times n$ complex matrices) given by $M \mapsto AMB$. Then $\mathrm{tr}(F_{AB}) = \mathrm{tr}(A)\mathrm{tr}(B)$. We see this by taking $M_{ij} = \delta_{ij}$. Then $(AMB)_{ij} = a_{ii}b_{jj}$, so $\mathrm{tr}(F_{A,B}) = \sum_i \sum_j a_{ii}b_{jj} = \sum_i a_{ii} \sum_j b_{jj} = \mathrm{tr}(A)\mathrm{tr}(B)$. We consider R, a representation of dimension m on V and R, a representation of dimension n on V' and define $\Phi : \mathbb{C}^{m\times n} \to \mathbb{C}^{m\times n}$ with $M \mapsto \dfrac{1}{|G|} \sum\limits_{g\in G} R_g^{-1} M R'_g$. Since M corresponds to a linear map from V to V', $\Phi(M)$ commutes with the action of G. Also, if M commutes with the action of G,

then $\Phi(M) = M$. We shall compute the trace of Φ. Its image is the subspace of maps from V to V' that commute with action of G. Thus $\operatorname{tr}(\Phi) = \operatorname{tr}\left(\begin{bmatrix} I_k & *_{mn-k} \\ 0_{mn-k} & 0_{mn-k} \end{bmatrix}\right) = k$, where k is the dimension of the subspaces described above. Alternatively, $\operatorname{tr}(\Phi) = \frac{1}{|G|}\sum \operatorname{tr}(F_{R_g^{-1},R'_g}) = \frac{1}{|G|}\sum \operatorname{tr}(R_g^{-1})\operatorname{tr}(R'_g) = \frac{1}{|G|}\sum \chi_R(g^{-1})\chi_{R'}(g) = \frac{1}{|G|}\sum \overline{\chi_R(g)}\chi_{R'}(g) = \langle \chi_R, \chi_{R'}\rangle$. Then if R and R' are irreducible representations and $R \not\cong R'$, $\langle \chi_R, \chi_R\rangle$ is the dimension of the space of morphism from V to V, which is $\dim(\{\lambda I\}) = 1$ by the second part of Schur's Lemma. Also, $\langle \chi_R, \chi_{R'}\rangle = 0$. Thus the characters of irreducible representations are orthonormal.
Now we consider a useful lemma:
Lemma: If a class function $\phi : G \to \mathbb{C}$ is orthogonal to all maps, then the linear map $\frac{1}{|G|}\sum \overline{\phi(g)}R_g$ is 0.
Proof: Exercise. It suffices to check this for irreducible representations and to show T commutes with the action of G. Then we use Schur's Law.

Continuing the proof, we now consider the regular representation of G. Here V is the complex span of $\{e_g\}$, where $h \cdot e_g = e_{hg}$ and $h \cdot (\sum a_g e_g) = \sum a_g e_{hg}$. We see that the elements of $GL(V)$ are permutation matrices. Then $T = \frac{1}{|G|}\sum \overline{\phi(g)}R_g^{\text{reg}} = 0$, where ϕ is a class function that is orthogonal to all maps by the previous lemma. Then $Te_1 = \frac{1}{|G|}\sum \overline{\phi(g)}R_g^{\text{reg}}(e_1) = \frac{1}{|G|}\sum \overline{\phi(g)}e_g$, which is not zero unless $\overline{\phi(g)}$ is zero for all g. Thus there is a representation that shows that a class function orthogonal or all other maps is 0, which shows that the characters of irreducible representations span the space of class functions $G \to \mathbb{C}$.

Corollary: (a) The number of distinct irreducible representations is the number of conjugacy classes.
(b) If we list the distinct irreducible representations $V_1, \cdots V_k$, then any representations V is uniquely a direct sum of m_i copies of V_i, with $m_i = \langle chi_V, \chi_{V_i}\rangle$
Proof: Exercise.