Algebra notes

Mauricio Barba da Costa

December 16, 2020

1 September 11, 2020

Group theorists somethings denote $H \leq G$ if H is a subgroup of G (not just a subset). This is what we covered last time.

Definition 1

The index of H in G is denoted $(G : H) :=$ the number of left cosets of H in G.

Theorem 2 (The counting formula)

$|G| = |H|(G : H)$

Corollary 3 (Lagrange's theorem)

If G is finite, then $|H|$ divides $|G|$.

Corollary 4

If $|G|$ is prime then $G \cong C_p$

Corollary 5 (Corollary to the counting formula)

If $\phi : G \to G'$ then $|G| = |\ker \phi||\operatorname{Im} \phi|$

Proof. Let $K = \ker \phi$. The counting formula says that $|G| = |K|(G : K) = |\ker \phi||\operatorname{Im} \phi|$ since the number of cosets of K is in bijection with $\operatorname{Im} \phi$. □

Definition 6

Let G be a group and H a subgroup. H is normal in G if and only if for all $g \in G$ and $g \in H$, $ghg^{-1} \in H$.

Equivalently, for all $g \in G$, $gHg^{-1} \subseteq H$. In particular, $gHg^{-1} = H$. If $gHg^{-1} \subseteq H$ and $g^{-1}Hg \subseteq H$, multiplying both sides gives $H \subseteq gHg^{-1}$. Thus $gHg^{-1} = H$. For all $g \in G$ $\operatorname{inn}_g(H) = H$. For all $g \in G$, $gH = Hg$.

Not all subgroups are normal but we can run through a bunch of examples:

Example 7

The kernel of any homomorphism is normal. This is the reason normal subgroups are important

Proof. Suppose there exists $\phi : G \to G'$ and $H = \ker \phi$. Let $g \in G$ and $h \in H$. Then $\phi(ghg^{-1} = \phi(g)\phi(h)\phi(g)^{-1} = \phi(g)\phi(g)^{-1} = \text{id}$. Hence, the kernel is normal. □

Example 8

If G is abelian, any subgroup H is normal

Proposition 9

Any subgroup of index 2 is normal.

Proof. Let H is a subgroup of G of index 2. The two left cosets is H are H and gH where $g \notin H$. The two right cosets are H and Hg where $g \notin H$. Thus the left and right cosets are the same □

Example 10

The center $Z(G)$ of a group G is a normal subgroup. This is the set $\{z \in G : zg = gz \forall g \in G\}$.

An alternative proof of the fact that $Z(G)$ is normal. If you have an isomorphism $\phi : G \to G'$ maps the center of G to the center of G'. Take ϕ to be $\text{inn}_g : G \to G$. You get $\text{inn}_g(Z) = Z$. This holds for every g. □

Fact 11

Any subgroup that can be described without naming specific elements is a normal subgroup. Such a description respects any isomorphism and in particular the inner automorphisms.

Example 12

The subgroup of G generated by all elements of order 2 is automatically normal because of the above fact.

Example 13 (Subgroups of S_3)

$S_3 = \{1, (12), (13), (23), (123), (132)\}$. You can take the cyclic subgroups $< (12) >, < (13) >, < (23) >, < (123) >$. I claim that these are all the subgroups. If you have any other subgroup H, it must contain $< (12) >$ and it is contained in S_3. Thus $|H||6$ and $2||H|$ so H is either one of the cyclic subgroups or the entire group.

Subgroup lattices are a thing. At the top but the group G. At the bottom put the trivial group. Make rows between the group and the trivial group with the divisors of $|G|$. If a subgroup has order n put it in row n. If a subgroup is a subgroup of another put a line between the two.

Proposition 14

Let $\phi : G \to G'$ be a homomorphism. If $H \leq G$ then $\phi(H) \leq G'$. If H is a normal subgroup of G and ϕ is surjective then $\phi(H)$ is a normal subgroup of G'.

Proposition 15

If $H' \leq G'$ then $\phi^{-1}(H') \leq G$. If H' is a normal subgroup of G' then $\phi(H')$ is a normal subgroup of G.

Proof. Suppose that $g \in G$ and $h \in \phi^{-1}(H')$. Then $\phi(h) \in H'$ so $\phi(ghg^{-1}) = \phi(g)\phi(h)\phi(g)^{-1} \in H'$ since H' is normal in G'. Thus $\phi^{-1}(H')$ is normal in G. □

Theorem 16 (Correspondence theorem)

Let $\phi : G \to G'$ be a surjective homomorphism with $\ker \phi = K$. Then there exists bijective correspondence ψ between the subgroups of G that contain K and the subgroups of G'. In particular, the maps are $\psi : H \mapsto \phi(H)$ and $\psi^{-1} : H' \mapsto \phi^{-1}(H')$

If H corresponds to H' then H is a normal subgroup of G if and only if H' is a normal subgroup of G'. $\phi|_H : H \to H'$ is a surjective homomorphism with kernel K. $|H| = |K||H'|$.

We save the proof for this theorem for next class.

2 September 14, 2020

The hard part about proving the correspondence theorem is finding out what you have to prove. Need to show $\phi(H) \leq G$, $K \leq \phi^{-1}(H') \leq G$, $H \xrightarrow{\phi} G \xrightarrow{\phi^{-1}} H$, $H' \xrightarrow{\phi^{-1}} G \xrightarrow{\phi} H'$.

Definition 17

$G/H = \{\text{left cosets of } H \text{ in } G\}$

$H \backslash G = \{\text{ right cosets of } H \text{ in } G\}$.

We're going to make a group out G/N of the left cosets whose elements are the left cosets.

Definition 18 (The group G/N)

The subgroup N must be normal

The set is G/N

Define the product of aN and bN to be $aNbN = abN$. The binary operation is well-defined.

Theorem 19

G/N is a group

Proof. Associativity:$(aNbN)cN = (ab)cN = a(bc)N = (aNbN)cN$ so associativity works

Identity:$NaN = aNN = aN$ so N is the identity

Inverses:$a^{-1}NaN = a^1aN = N$ so every element has an inverse

Closure follows from the definition of the binary operation □

Definition 20 (The natural homomorphism)

$\pi : G \to G/N$ sends each element of G to its left coset in G/N.

$\ker \pi = \{a \in G : aN = N\} = N$.

Fact 21

The elements of G/N are "the elements of G, except that you consider some of them to be the same". I.e. $a \equiv b \bmod N$.

Example 22

$\mathbb{Z}/3\mathbb{Z} = \{3\mathbb{Z}, 1 + 3\mathbb{Z}, 2 + 3\mathbb{Z}\}$

Definition 23

A **set of coset representatives** fof $H \leq G$ is a subset of G consisting of one element in each left coset

Example 24

$\{0, 1, 2\}$ is a set of coset representatives for $3\mathbb{Z}/\mathbb{Z}$. We also could arbitrarily have chosen $\{0, 4, 2\}$

Theorem 25 (First isomorphism theorem)

Given a surjective homomorphism $\phi : G \to G'$. $G/\ker\phi \sim G'$ under the map $\bar{\phi}$, $\bar{\phi}aN \mapsto \phi(a)$.

Proof. If $a \cong b \bmod N$ then $\bar{\phi}(b^{-1}a) = \text{id}$ so $\bar{\phi}(a) = \bar{\phi}(b)$. $\bar{\phi}$ is surjective since ϕ is surjective. $\bar{\phi}$ is a homomorphism since $\bar{\phi}((aN)(bN)) = \bar{\phi}(abN) = \bar{\phi}(aN)\bar{\phi}(bN)$ so now we have a bijective homomorphism which is an isomorphism. □

Fact 26

If you want to know what G/N looks like, we can try to identify ϕ such that $\phi : G \to G'$ is a surjection and $\ker\phi = N$. Then $G/N \sim G'$

Corollary 27

If $\phi : G \to G'$ is a homomorphism then $G/\ker\phi \sim \operatorname{Im}\phi$.

Corollary 28

If G is finite, then $|G| = |\ker\phi||\operatorname{Im}\phi|$.

Definition 29

Let F be a field, V be a vector space over F, $S \subset V$. A **linear combination** of elements of S is sum

$$\sum_{s \in S} a_s s$$

where $a_s \in F$ for each $s \in S$ and $a_s = 0$ for all but finitely many $s \in S$.

Definition 30 (Span S)
The span of S is the set of vectors that can be obtained from S be addition and scalar multiplication (finitely many times) which is equivalent to the set of linear combinations of S. This smallest subspace of V containing S. If $S = \emptyset$ then the empty sum is zero so the span of S is just the zero vector.

Definition 31
S spans V is $\operatorname{Span} S = V$
S is linearly independent if

$$\sum_{s \in S} a_s s = 0 \implies a_s = 0$$

for all $s \in S$.
S is a basis of V is S spans V and S is linearly independent.

Definition 32
$T : V \to W$ is a homomorphism of vector spaces if $T(av_1 + bv_2) = aT(v_1) + bT(v_2)$. Such a homomorphism is called a linear transformation.

3 September 16, 2020

Example 33
If $A \in F^{m \times n}$ then $F^n \xrightarrow{A} F^m$, $v \mapsto Av$ is a linear transformation. Every linear transformtion $T : F^n \to F^m$ is of this form. Given T let $A = \begin{bmatrix} T\mathbf{e}_1 & \dots & T\mathbf{e}_\mathrm{n} \end{bmatrix}$. Then $T(v) = Av$ for all v.
$\ker A$ is called the nullspace.
$\operatorname{im} A$ is called the column space since it's the span of the columns of A.

Suppose that $S = (v_1, \dots, v_n)$ where the v_is are vectors in V. We can think of S as being a matrix. Define a linear transformation $\phi : F^n \to V$, $\begin{pmatrix} a_1 \\ \dots \\ a_n \end{pmatrix} \mapsto (v_1, \dots, v_n) \begin{pmatrix} a_1 \\ \dots \\ a_n \end{pmatrix} = a_1 v_1 + \dots + a_n v_n$ Then S spans V if and only if ϕ is surjective. S is linearly independent if and only if ϕ is injective. S is a basis if and onlyif ϕ is bijective (and then ϕ^{-1} is a linear transformation. Thus ϕ is an isomorphism of vector spaces. An isomorphism of vector spaces is equivalent to finding a basis for a vector space.

Example 34 ($V = \mathbb{R}^2$)
$S = (\begin{pmatrix} 2 \\ 1 \end{pmatrix} \begin{pmatrix} 1 \\ 3 \end{pmatrix} \begin{pmatrix} 21 \\ 13 \end{pmatrix})$. S spans V since any point of $\mathbb{R}^2$ can be expressed as linear combination of v_1 and v_2. S is not linearly independent since $10v_1 + v_2 + (-1)v_3 = 0$. Deleting v_3 doesn't change the span.

Proposition 35

Suppose that S is finite and S spans V. (When such an S exists, V is called finite dimensional).

Deleting some vectors in S gives a basis.

If L is a linearly independent set that doesn't span V insert some vectors from S gives a basis.

sketch of second claim. If the span of L isn't V, there must be some vector in S not in the span of L. Put this vector into L to get a larger set. This process eventually has to end Since V is finite dimensional this process can't go on forever. □

Corollary 36

Every finite dimensional vector space has a basis. Actually, this is true even if V if infinite dimensional (if you use the axiom of choice).

Proposition 37

If $F^n \xrightarrow{A} F^m$ is an injective linear transformation, then $m \geq n$.

Proof. Since A is injective, $\ker A = \{0\}$ so the system $Av = 0$ has only $v = 0$ as a solution. If $m < n$ then row would show there exist nonzero solution. □

Corollary 38

If F^n is isomorphic to F^m then $n = m$

Proof. Injections in both directions! □

Corollary 39

If V is finite dimensional then every finite basis of V has the same number of elements.

Proof. If $F^m \xrightarrow{\sim} V$ and $F^n \xrightarrow{\sim} V$ then we can furnish an isomorphism between F^n and F^m so $m = n$ □

Definition 40

$\dim V$ is the number of elements in any basis of V.

Definition 41 (Coordinates)

V is an n dimensional vector space. $B = (v_1, \dots, v_n)$ is the basis. $w \in V$. Then there exists a unique $\vec{x} = \begin{pmatrix} x_1 \\ \dots \\ x_m \end{pmatrix} \in F^n$ $x_1v_1 + \dots + x_nv_n = w$. The x_is are called the coordinates of w with respect to B. We can express this as $B\vec{v} = w$.

Definition 42 (Change of basis)
Suppose $B' = (v_1', \ldots, v_n')$ is another basis. How is B' related to B? $B' = BP$ where $P = B^{-1}B'$. Getting the ordering right is kind of tricky. How are coordinates w with respect to B related to coordinates of w with respect to B'? $P\vec{x'} = \vec{x}$.

Theorem 43 (Dimension Formula)
If $\phi : V \to W$ is a linear transformation then $\dim(\ker \phi) + \dim(\operatorname{im} \phi) = \dim V$. This is equivalent to saying that the nullity $(\dim(\ker \phi))$ plus the rank $(\dim(\operatorname{im} \phi))$ is equal to the dimension of V. This is analogous to proving that $|\ker \phi||\operatorname{im} \phi| = |G|$ for groups

Proof. Choose a basis $(v_1, \ldots, v_k)$ of $\ker \phi$. Extend to a basis $(v_1, \ldots, v_k, v_{k+1}, \ldots, v_n)$ of V. The first k vectors are a basis of $\ker \phi$ and the other vectors are going to be a basis of a space Z. $\ker \phi \oplus Z = V$
Claim: $\phi|_Z : Z \xrightarrow{\sim} \operatorname{im} \phi$.
Surjective: $\{0\} \oplus \phi(Z) = \phi(V)$. Thus $\phi(Z) = \operatorname{im} \phi$
Injective: $(\ker(\phi|_Z) = \{0\})$ since if $z \in Z$ and $\phi(Z) = 0$ then $z \in \ker \phi$ so $z = 0$. Then $\dim(\ker \phi) + \dim(\operatorname{im} \phi) = \dim V$. □

Definition 44 (Eigenvector)
Let $\dim V < \infty$ and $T : V \to V$ and $\lambda \in F$ (possibly 0). The vector $\mathbf{x}$ is an eigenvector of T if and only if there exists $\lambda \in F$ such that $T\mathbf{x} = \lambda \mathbf{x}$.

4 September 21, 2020

Last time we talked about V, a finite-dimensional F-vector space. $T : V \to V$ a linear operator. The following are equivalent.

- T is injective
- T is surjective
- T is bijective
- $\det T \neq 0$
- $\ker T = \{\vec{0}\}$
- $\operatorname{im} T = V$
- T is an isomorphism
- T is invertible

Definition 45
Call $v \in C$ an **eigenvector** with eigenvalue λ if $Tv = \lambda v$ and $v \neq 0$. Call λ an **eigenvalue** if there exists $v \neq \vec{0}$ such that $Tv = \lambda v$.

Proposition 46

Let A be an $n \times n$ matrix; get linear operator $F^n \xrightarrow{A} F^n$. Then A is similar to a diagonal matrix if and only if F^n has a basis consisting of eigenvectors of A.

Definition 47

Given λ, the set $\{\text{eigenvectors with eigenvalue } \lambda, \text{including } \vec{0}\} = \ker(\lambda I - T)$

Proof. v an eigenvectof of eigenvalue λ if and only if $Tv = \lambda v$ if and only if $\lambda v - Tv = \vec{0}$ if and only if $(\lambda I - T)v = \vec{0}$ if and only if $v \in \ker(\lambda I - T)$ □

Proposition 48

The eigenvalues of T are the solutions λ to $\det(T - \lambda I) = 0$

Proof. Let λ be an eigenvalue. Then $\ker(\lambda I - T) \neq \{\vec{0}\}$ if and only if $\det(\lambda I - T) = 0$ if and only if the characteristic polynomial of A is zero □

Definition 49

The characteristic polynomial of T is $p(t) := \det(tI - A)$.

Example 50

If A is upper triangular, then $p(t) = \prod(t - a_{ii})$. The eigenvalues of A is its diagonal entries.

Example 51

$A = \begin{pmatrix} 2 & 3 \\ 3 & 2 \end{pmatrix}$. Then $tI = \begin{pmatrix} t & 0 \\ 0 & t \end{pmatrix}$ and $tI - A = \begin{pmatrix} t-2 & -3 \\ -3 & t-2 \end{pmatrix}$. Taking the determinant of this matrix gives $p(t) = t^2 - 4t - 5$. An $n \times n$ matrix cannot have more than n eigenvalues. To find the eigenvectors, with eigenvalue 5. The **eigenspace** is the set of eigenvectors with a given eigenvalue. $\ker(5I - A) = \ker \begin{pmatrix} 3 & -3 \\ -3 & 3 \end{pmatrix}$. This same process can be used to find the eigenvectors of eigenvalue -1.

If $\dim V = n$ then A is $n \times n$ so $p(t) = t^n - (\text{tr}(A))t^{n-1} + ... + (-1)^n \det(A)$. Note that $p(0) = (-1)^n \det(A)$ since $p(0) = \det(0I - A) = (-1)^n \det(A)$. If the vector space is over an algebraically closed field, then there are n eigenvectors (counting multiplicity).

Proposition 52

If $v_1, ..., v_r$ are nonzero eigenvectors of T whose eigenvalues of $\lambda_1, ..., \lambda_r$ are distinct, then $v_1, ..., v_r$ are linearly independent.

Proof. Induction on r. Base case: $r = 0$: the empty set is linearly independent. Now suppose $r \geq 1$. Suppose $a_1 v_1 + ... + a_r v_r = 0$. Apply T to both sides to get $a_1 \lambda_1 v_1 + ... + a_r \lambda_r v_r = 0$. Multiply both equations by λ_1 to get

$a_1\lambda_1 v_1 + \ldots + a_r\lambda_1 v_r = 0$. Now subtract the two equations to get $a_2(\lambda_2 - \lambda_1)v_2 + \ldots + a_r(\lambda_r - \lambda_1)v_r = 0$. By the induction hypothesis, this set of $v_2, \ldots, v_r$ is linearly independent. Hence $a_i(\lambda_i - \lambda_1) = 0$ for all $i \geq 2$. $\lambda_i - \lambda_1 \neq 0$ since the λs are all distinct. Hence $a_i = 0$ for all $i \geq 2$. Plug in $a_i = 0$ for all $i \geq 2$ into the equation to see that $a_1 = 0$ too. □

Corollary 53

If you have $p(t)$ and it has n distinct roots, then

- V has a basis of eigenvectors.
- There is a basis with respect to which T is diagonal.
- A is **diagonalizable** (similar to a diagonal matrix). This is equivalent to V having a basis of eigenvectors.

Example 54 (A non-example)

The characteristic polynomial of $\begin{pmatrix} 2 & 1 \\ 0 & 2 \end{pmatrix}$ is $p(t) = (t-2)^2$. The unique eigenvalue is 2. The eigenspace of 2 is $\{\begin{pmatrix} x \\ y \end{pmatrix} : y = 0\} = \text{Span}\{\begin{pmatrix} 1 \\ 0 \end{pmatrix}\}$. This is not enough eigenvectors to get a basis for $\mathbb{R}^2$.

Definition 55

Let $T : V \to V$ and W a subspace of V. W is **T-invariant** if $TW \subset W$. In this case, get $T|_W : W \to W$. Then T with respect to a suitable basis (extend a basis of W to a basis of V) is $\begin{pmatrix} T_w & * \\ 0 & * \end{pmatrix}$.

Definition 56 (Nilpotent Operators)

$T : V \to V$ is nilpotent is $T^n = 0$ for some n.

Example 57

V has basis e_1, e_2, e_3. $e_3 \xrightarrow{T} e_2 \xrightarrow{T} e_1 \xrightarrow{T} 0$. Then $T^3 = 0$. $T = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{pmatrix}$

Example 58

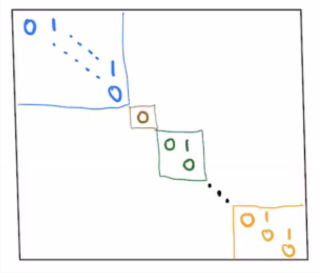
Suppose V has basis $e_1, \ldots, e_5$. Let $V = \text{Span}(e_1, e_2, e_3) \oplus Span(e_4, e_5)$ "Every vector in the space can be expressed uniquely as a linear combination of things in the first span plus a linear combination of things in the second. Consider $T = \begin{pmatrix} 0 & 1 & & & \\ & 0 & 1 & & \\ & & 0 & & \\ & & & 0 & 1 \\ & & & & 0 \end{pmatrix}$. What happens is $e_3 \to e_2 \to e_1 \to 0$ and $e_5 \to e_4 \to 0$. Thus $T^3 = 0$.

5 September 23, 2020

Proposition 59

The following are equivalent.

- T is nilpotent
- All eigenvalues of T are 0
- The characteristic polynomial of T is t^n.
- V has a basis consisting of chains of vectors in which T maps each to the next and eventually to 0.
- T is represented by a block matrix of the following form:



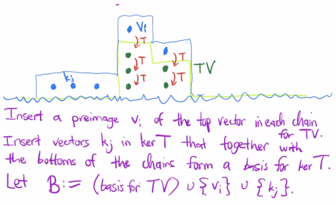
2 9232020.PNG

Proof. 1 $\implies$ 2. Suppose that $Tv = \lambda v$ for some $\lambda \neq 0$ and $v \neq 0$. Then $T^2 v = \lambda^2 v \neq 0$. Continue in this way we get $T^m v \neq 0$ so $T^m \neq 0$ a contradiction since T is nilpotent.

4 $\iff$ 5 $\implies$ 1 Easy

2 $\implies$ 4 We skip it for now

1 $\implies$ 4 By induction on m such that $T^m = 0$. TV is T invariant subspace. $T^{m-1}(TV) = 0$. By the induction hypothesis, TV has a basis of chains:



Insert a preimage v_i of the top vector in each chain for TV.
Insert vectors k_j in ker T that together with the bottoms of the chains form a basis for ker T.
Let $B := (\text{basis for } TV) \cup \{v_i\} \cup \{k_j\}$.

1 9232020.PNG

Also, there are $\dim(\operatorname{im} T) + \dim(\ker T) = \dim V$ basis vectors in B. Thus B is a basis since it has the right number of basis and is linearly independent. □

Proposition 60

B is linearly independent. Suppose there were a linear dependence. If such a dependence existed, you can apply T to get a dependence to the basis vectors in TV, so all the non-bottom coefficients are 0. Now the dependence is between the bottom vectors, which are a basis of $\ker T$, so their coefficients are zero too.

Lemma 61

If $T : V \to V$ then $V = V_0 \oplus W$. $T|_{V_0}$ is nilpotent and $T|_W$ is invertible. You can look at this as $\begin{pmatrix} \text{nilpotent} & \\ & \text{invertible} \end{pmatrix}$

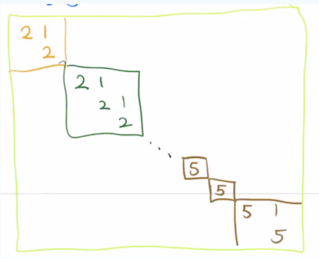
Proof. $V \subset TV \subset T^2V \subset ... \subset T^nV$. The dimension can drop but it can only drop finitely many times so eventually the subspace has to stabilize. There exists $T^nV = T^{n+1}V = T^{n+2}V = ...$ Define $V_0 := \ker(T^n)$ and $W := T^nV$. Thus $W = TW$ so T restricts to something on W that's surjective so $T|_W$ is invertible. T_{V_0} is nilpotent. $\ker(T^n) \cap W = \{w \in W : T^n w = 0\}$ since $T|_W$ is injective. $\dim(\ker T^n) + \dim(\operatorname{im} T^n) = \dim V$. Thus $V_0 \oplus W$ must be all of V. □

Definition 62 (Jordan Block)

(λ), $\begin{pmatrix} \lambda & 1 \\ & \lambda \end{pmatrix}$, $\begin{pmatrix} \lambda & 1 & \\ & \lambda & 1 \\ & & \lambda \end{pmatrix}$

Theorem 63

Let $T : V \to V$ represent a matrix with Jordan blocks along the diagona, unique except for rearranging the blocks. For example:



3 9232020.PNG

The Jordan normal form is the closest you can get to diagonalizing a matrix. Any matrix $A \in \mathbb{C}^{n \times n}$ is similar to a matrix in Jordan normal form, unique except for rearranging the blocks.

Proof. Induction on $\dim V$. Suppose $\dim V \geq 1$. Let $\lambda \in \mathbb{C}$ be a zero of $p(t)$ so λ is an eigenvalue. Replace T by $T - \lambda I$ to assume 0 is an eigenvalue. $V = V_0 \oplus W$ where $V_0 \neq 0$ so $\dim W < \dim V$ $T|_W$ has a JNF by the induction hypothesis. $T|_{V_0}$ has a JNF since it's nilpotent (proposition 59)
Uniqueness. Look at the number of $m \times m$ blocks with diagonal entry λ is determined by $\dim\ker(T - \lambda I)$, $\dim\ker((T - \lambda I)^2)$ □

Definition 64

$v \in V$ is a generalized eigenvector with respect to eigenvalue λ if $(T - \lambda I)^m V = 0$ for some m. Let $V_\lambda = \{\text{generalized eigenvectors with eigenvalue}\lambda\}$

Corollary 65

If $p(t) = (t - \lambda_1)^{e_1} ... (t - \lambda_r)^{e_r}$ with λ_i distinct. Then $V = V_{\lambda_1} \oplus V_{\lambda_2} \oplus ... \oplus V_{\lambda_r}$ with dimensions $n = e_1 + ... + e_r$ where e_i is the number of diagonal entries equal to λ_i which is equivalently equal to the sum of sizes of blocks with diagonal λ_i. Also $\dim \ker(T - \lambda I)$ is the number of blocks with diagonal λ. $\ker(T - \lambda I)$ is the eigenspace of λ.

6 September 24, 2020

Definition 66

Let x and y be vectors. Then $x \cdot y = \begin{pmatrix} x_1 & ... & x_n \end{pmatrix} \begin{pmatrix} y_1 \\ ... \\ y_n \end{pmatrix}$. Observe that $|x \cdot y| = |x||y| \cos\theta$ where θ is the angle between x and y.

Definition 67

$|x| = \sqrt{x \cdot x}$

Definition 68

$x \perp y$ means $x \cdot y = 0$.

Definition 69 (An orthonormal basis)

Suppose we have $v_1, v_2, ..., v_n \in \mathbb{R}^n$. This is an orthonormal basis if and only if $v_i \cdot v_j = \delta_{ij}$ where δ_{ij} is the Kronecker delta function. This is equivalent to $|v_i| = 1$ and $v_i \perp v_j$ for all $i \neq j$.

Theorem 70

The following are equivalent for $A \in \mathbb{R}^{n \times n}$:

- $|Ax| = |x|$
- $(Ax) \cdot (Ay) = x \cdot y$
- $A^t A = I$
- The columns of A form an orthonomral basis

Proof. 1 $\implies$ 2 Use $x \cdot y = (|x + y|^2 - |x|^2 - |y|^2)/2$.
2 $\implies$ 1 Use $|x| = \sqrt{x \cdot x}$
2 $\iff$ 3 $x^t A^t A y = x^t y$ for all x, y and in particular these is best seen by letting x and y be standard basis vectors.
3 $\iff$ 4 $(A^t A)_{ij} = \sum_k A^t_{ik} A_{kj} = \delta_{ij} \iff A^t A = I$ □

Definition 71 (Orthogonal Matrices)

If any of the conditions in theorem 70 hold for a matrix A, then A is called an orthogonal matrix

Definition 72

The orthogonal group O_n is the set of orthogonal $n \times n$ matrices.

Proposition 73

O_n is a subgroup of $GL_n(\mathbb{R})$

Proof. Use condition three of theorem 70 □

Proposition 74

If A is an orthogonal matrix then the determinant of A is plus or minus one. For each $n \geq 1$, both values are possible.

Proof. $A^tA = I$. Take the determinant of both sides to get $\det(A)^2 = 1$. The determinant must be a second root of unity of 1 so $\det(A) = \pm 1$. The I_n has determinant 1 for all n and the matrix that's I everywhere except for the entry in the first row and column where it is negative 1. □

Definition 75

The special orthogonal group is the set of orthogonal matrices of determinant 1. It's the kernel of the determinant homomorphism restricted to O_n. $[O_n : SO_n] = 2$.

Example 76

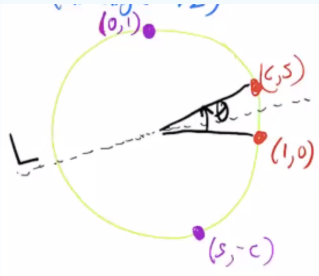
Consider $n = 2$. What are the possible orthonomal bases for $\mathbb{R}^2$?. The first vector has to be in the unit circle so it can be expressed as $\begin{pmatrix} \cos\theta \\ \sin\theta \end{pmatrix}$. The second vector is either $\begin{pmatrix} -\sin\theta \\ \cos\theta \end{pmatrix}$ or $\begin{pmatrix} \sin\theta \\ -\cos\theta \end{pmatrix}$

Corollary 77

$O_2 = \{\begin{pmatrix} c & -s \\ s & c \end{pmatrix}, \begin{pmatrix} c & s \\ s & -c \end{pmatrix}\}$. All the matrices of the first type have determinant one and all the ones of the second type have determinant negative one. $SO_2 = \{\begin{pmatrix} c & -s \\ s & c \end{pmatrix}\}$. This is isomorphic to the units in $\mathbb{C}$.

Proposition 78

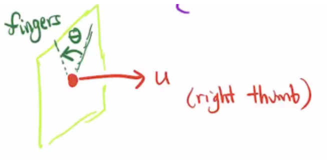
If $A \in S$ where S is the nontrivial coset of SO_2 in O_2 which is $\{\begin{pmatrix} c & s \\ s & -c \end{pmatrix}\}$ then A is a reflection in some line L through the origin (at angle $\theta/2$).



1 9252020.PNG

Proof. This matrix has eigenvalues 1 and -1. Take unit eigenvectors v and w. We claim that $v \perp w$. $(Av)\cdot(Aw) = v \cdot w = v \cdot -w = -(v \cdot w)$. This is possible if and only if $v \cdot w = 0$. □

What happens in three dimensions? Start with a unit vector $u \in \mathbb{R}^3$ and an angle θ. Let $u^\perp$ be the set of all vectors in $\mathbb{R}^3$ that are perpendicular to u. This set forms a plane. Use the below image to deduce what a rotation is:



2 9252020.PNG

$\rho(u,\theta) :=$ the linear operator $\rho : \mathbb{R}^3 \to \mathbb{R}^3$ such that $\rho(u) = u$ and $\rho_{u^\perp}$ is a counterclockwise rotation by θ. It corresponds to a 3 by 3 matrix.

Theorem 79

The 3×3 rotation matrices are SO_3

Proof. First we show that the set of ρs is a subset of SO_3. Let ρ be a rotation $\rho(u,\theta)$. Choose an orthonormal basis $(u,v,w) = P \in O_3$.

$$\begin{tikzcd}
\mathbb{R}^3 \arrow[r, "\rho"] & \mathbb{R}^3 \\
\mathbb{R}^3 \arrow[u, "P"] \arrow[r, "\begin{pmatrix} 1 & 0 & 0 \\ 0 & c & -s \\ 0 & s & c \end{pmatrix}"] & \mathbb{R}^3 \arrow[u, "P"']
\end{tikzcd}$$

3 9252020.PNG

$\rho = P \begin{pmatrix} 1 & & \\ & \cos\theta & -\sin\theta \\ & \sin\theta & \cos\theta \end{pmatrix} P^{-1}$ which is in SO_3. Since SO_3 is a normal subgroup of O_3 (it's the kernel of a homomorphism), $\rho \in SO_3$. Next time we will show the other inclusion. □

7 September 28, 2020

Theorem 80

$SO_3 = \{3 \times 3 \text{ rotation matrices } \rho_{(u,\theta)}\}$.

Proof. We already showed that each 3×3 rotation matrix $\rho_{(u,\theta)}$ is in SO_3. Suppose $A \in SO_3$. Then $A^t A = I$ and $\det A = 1$. First, 1 is an eigenvalue of A. $\det(A - I) = \det(A - I)^t = \det(A^t - I) = \det(A^{-1} - I) = \det(A(A^{-1} - I)) = \det(I - A) = -\det(A - I)$ so the determinant is zero. By performing an orthogonal change of basis, WLOG, $u = \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}$.

Then $u^\perp = \begin{pmatrix} 0 \\ \ \end{pmatrix}$ is A-invariant so $A = \begin{pmatrix} 1 & & \\ & * & * \\ & * & * \end{pmatrix}$. The two by two asterisk portion must also be orthogonal for A to be orthogonal. Hence this little matrix is in $S0_2$. So A is a rotation of $\mathbb{R}^3$. □

Definition 81

Let $f : \mathbb{R}^n \to \mathbb{R}^n$. This map is called an isometry if it preserves distances. $|f(x) - f(y)| = |x - y|$ for all $x, y \in \mathbb{R}^n$.

Example 82

- An orthogonal linear operator. $\mathbb{R}^n \xrightarrow{A} \mathbb{R}^n$, $x \mapsto Ax$ preserves distance for $A \in O_n$.
- "translation by b" $\mathbb{R}^n \xrightarrow{t_b} \mathbb{R}^n$ for $b \in \mathbb{R}^n$, $x \mapsto x + b$.

Theorem 83

Every isomstry $f : \mathbb{R}^n \to \mathbb{R}^n$ is $t_b A$ for some unique $b \in \mathbb{R}^n$ and $A \in O_n$.

Lemma 84

An isometry that fixes 0 is a linear operator.

Proof. First, f preserves distances and zero. We can express dot products in terms of 0 and distances. $u \cdot v = \frac{1}{2}(|u|^2 + |v|^2 - |u - v|^2)$. If an operator preserves distances, then it preserves dot product, $f(u) \cdot f(v) = u \cdot v$ so f preserves dot product. We can express sums in terms of dot products. $z = x + y \iff (z - x - y) \cdot (z - x - y) \iff z \cdot z - 2x \cdot z - \ldots = 0$ so f preserves taking sums. Similarly f preserves scalar multiplication by each $c \in \mathbb{R}$. □

Proof of theorem. Let $b = f(0)$. Then $t_b^{-1} f$ is an isometry mapping 0 to 0. so $t_b^{-1} f = A$ for some orthogonal matrix $f = t_b A$. If $f = t_b A$ then $f(0) = t_b A(0) = t_b = b$ so b is determined by f, and then $A = t_b^{-1} f$ is uniquely determined too. □

Definition 85

The set of all isometries from $\mathbb{R}^n$ to itself is denoted M_n. $M_n = \{t_b A : A \text{ orthogonal } t_b \text{ translation }\}$. which maps $x \mapsto Ax + b | A \in O_n, b \in \mathbb{R}^n$. This is a subgroup of the group of permutations of the plane. The set of translations over $\mathbb{R}^n$ (which is isomorphic to the additive group of $\mathbb{R}^n$) is a normal subgroup of M_n and the group of orthogonal operators is a subgroup of M_n. The mapping $\mathbb{R}^n \times O_n \to M_n$ under $(t_b, A) \mapsto t_b A$ is a bijection between the two sets but it is not an isomorphism since t_b and A don't commute in general. Instead, $At_b = t_{A(b)}A$.

Let $M_n :\xrightarrow{\pi} O_n$ where $(x \mapsto Ax + b) \mapsto A$. This is a homomorphism. The kernel is going to be the translations which proves that the translations are a normal subgroup.

Definition 86

If $x \mapsto Ax + b$ is **orientation preserving** it has $\det A = 1$ and **orientation reversing** if $\det A = -1$.

Theorem 87

Every isometry of $\mathbb{R}^2$ is one of the following:

- translation $x \mapsto x + b$
- rotation around some point
- reflection across r_l a line l. The line is not necessarily through zero.
- glide reflection: $t_b r_l$ for b parallel to l.

Proof. Let f be an isometry under which $x \mapsto Ax + b$. If f is orientation preserving: If $A = I$, then f is a translation. If $A \neq I$ then f has a fixed point. We need to solve $Ax + b = x$ where $A = \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}$. We need to solve $(A - I)x = -b$. If A is a rotation, then it does not fix any nonzero vector so $\ker(A - I) = \{0\}$ so $A - I$ is invertible so we can find a fixed point for A. □

8 September 30, 2020

Last time, we stated that every isometry f or $\mathbb{R}^2$ is one of the following: $x \mapsto x + b$, rotation, reflection t_b, r_l, glide reflection $t_b r_l$ for some line l and nonzero vector b parallel to l.

Proof. $f = t_b A$ where A is a reflection in a line L which contains 0. Change the origin to $b/2$. This is equivalent to $t_{b/2}^{-1} f t_{b/2} = t_{-b/2} t_b A t_{b/2} = t_{b/2} t_{A(b/2)} A = t_m A$ where $m = \frac{1}{2}(b + Ab)$. If $m = 0$, this is a reflection and if $m \neq 0$, then this is a glide reflection. □

Definition 88

A subgroup G or $\mathbb{R}$ is discrete if and only if there exists $\varepsilon > 0$ such that every nonzero element $g \in G$ satisfies $|g| \geq \varepsilon$. Then if $g, h \in G$ are distinct, then $|g - h| \geq \varepsilon$.

Theorem 89

Every discrete subgroup $G \leq \mathbb{R}$ is $\{0\}$ or $a\mathbb{Z}$ for some $a \in \mathbb{R}_{>0}$.

Idea of proof. Assume $G \neq \{0\}$. Then there exists $b \neq 0$ and thus $-b$ or b is positive. There is a least positive real number a since between since the distance between any two points is greater than ε. If there is $b \in G$ and $b \notin a\mathbb{Z}$, then $b' = b - \lfloor \frac{b}{a} \rfloor a$ satisfies $0 < b' < a$, a contradiction. □

Definition 90 (Finite subgroups of O_2)

Let x be the rotation by $2\pi/n$ about O and y the reflection in a line l which contains 0. $C_n =< x >$ and D_n is the subgroup of O_2 generated by x and y. This is equal to $< x, y : x^n = 1, y^2 = 1, yx = x^{-1}y >= \{1, x, x^2, ..., x^{n-1}, y, xy, ..., x^{n-1}y\}$ and these elements are distinct.

Fact 91

$D_1 \cong C_2,\ D_2 \cong C_2 \times C_2,\ D_3 \cong S_3$ for $n \geq 3,\ D_n$ is the set of symmetries of a regular n-gon.

Fact 92

Group game: you name all the groups of order 1, I name all the groups of order 2, you name all the groups of order 3,...

Theorem 93

Every finite subgroup $H \leq SO_2$ is C_n for some $n \geq 1$.

Proof. Let $S = \{\theta \in \mathbb{R}; \rho_\theta \in H\} \leq \mathbb{R}$. Then S is discrete (it has finitely many elements in any bounded interval) so $S = a\mathbb{Z}$ for some $a \in \mathbb{R}_{>0}$. Also $2\pi \in S$ so $2\pi = na$ for some $n \in \mathbb{Z}_{n>0}$ so $a = 2\pi/n$ so $S = (\frac{2\pi}{n})\mathbb{Z}$ which is equal to the set of rotations by multiples of $2\pi/n$ which is C_n □

Theorem 94

Now, we're going to classify all subgroups $\leq O_2$. Every subgroup $G \leq O_2$ is C_n or D_n for some $n \geq 1$.

Proof. We split this into two cases:

Case 1: $G \subset SO_2$. Then $G = C_n$ for some n, by the theorem 94.

Case 2: G is not a subset of SO_2. There are two elements of O_2/SO_2 (remember that $SO_2 = \ker \det : \mathbb{R}^{2\times 2} \to \{-1, 1\}$). Let $H = \ker(G \to \{\pm 1\})$. Then $G \to \{\pm\}$ has two nonempty fibers. Namely, H and Hr for some reflection r. Here, $H \subseteq SO_2$ so $H = C_n$ for some n. Then G is generated by C_n and a reflection r so $G \cong D_n$.

□

Discrete subgroups of O_2 are the same as finite subgroups of O_2. What are the finite subgroups of M_2, the full isometry group? (remember that this is generated by the translations and O_2.

Theorem 95

Every finite subgroup of M_2 has a fixed point x (Taking x to the origin shows that $G \cong C_n$ or D_n for some $n \geq 1$).

9 October 2, 2020

Today, we will classify the discrete subgroups of M_2. Last time we determined the finite subgroups of O_2: the cyclic groups and the dihedral groups. It turns out that the discrete subgroups of O_2 are finite so they are C_n and D_n as well.

Let S be a subset of $\mathbb{R}^n$. Call $s \in S$ **isolated** if some open ball around s contains no other points of S. Call S **discrete** if every point of S is isolated. The discrete subgroups of $\mathbb{R}$ are $\{0\}$ and $a\mathbb{Z}$ for any $a \in \mathbb{R}_{>0}$. Today we will show the following:

Theorem 96

The discrete subgroups of $\mathbb{R}^n$ are $\{0\}$, $a\mathbb{Z}$, and $a\mathbb{Z} + b\mathbb{Z}$ for linearly independent $a, b \in \mathbb{R}^2$. The discrete subgroups of the third type are called full lattices.

Proof. Let $G \leq \mathbb{R}^2$ be a subgroup that is not the trivial group. Choose a one dimensional subspace L such that $G \cap L \neq \{0\}$. Then $G \cap L = a\mathbb{Z}$ for some $a \in L - \{0\}$. If $G = a\mathbb{Z}$, then we're done. Otherwise, there's some other element b in G that's outside $G - a\mathbb{Z}$ closest to L. Observe that any bounded subset B of $\mathbb{R}^2$ contains only finitely many elements of G. Using this fact and closure of subgroups, such a b that's closest to L exists. Then $G = a\mathbb{Z} + b\mathbb{Z}$ since otherwise, by shifting, the parallelogram with sides a and b would contain an element of G closer to L than b is. □

Theorem 97

Every finite subgroup $G \leq M_2$ is isomorphic to to C_n or D_n for some $n \geq 1$.

Proof. We first prove that there is a finite set S such that $gS = S$ for every $g \in S$. Form G_s the G-orbit of s. Then $g(Gs) = (gG)s = Gs$

We now show there there is a unique point x minimizing $|x - s_1|^2 + |x - s_2|^2 + \dots + |x - s_n|^2$. This is equal to $(x - s_1) \cdot (c - s_1) + \dots + (x - s_n) \cdot (x - s_n) = n(x - \frac{s_1 + s_2 + \dots + s_n}{n})^2 +$ constant that depends on the s_i but not on x. The first term is minimized when $x = \frac{s_1 + \dots + s_n}{n}$, which is the centroid of the set S.

x is a fixed point ($gx = x$) for all $g \in G$. g preserves S and preserves distances so g must preserve x.

Now, we show G is isomorphic to C_n or D_n. Make x the new origin. Then $G \leq O_2$. The resule follows from the fact that all finite subgroups of O_2 are C_n and D_n. □

Definition 98

Let $G \leq M_n$. Identify M_n with $\{(A, b) : A \in O_n, b \in \mathbb{R}^n\} \subseteq \mathbb{R}^{n^2+n}$. We can view G as being a subset of this big Euclidean space. Call G discrete if and only if it is discrete as a subset of $\mathbb{R}^{n^2+n}$. This is equivalent to there not existing a sequence $g_1, g_2, \dots$ of distinct elements of G converging to 1.

Proposition 99

Each $A \in \bar{G}$ maps L to L. L is the set of translations in $\bar{G}$.

Proof. Suppose $A \in \bar{G}$ and $t_a \in L$. We need to show that $t_{A_a} \in L$. By definition, A is the image of some $t_b A \in G$. Then $(t_b A) t_a (t_b A)^{-1} \in G$. $t_b A t_a A^{-1} t_b^{-1} = t_b t_{Aa} A^{-1} t_{-b} = t_b t_{Aa} t_{-b} = t_{Aa}$ since translations commute. □

10 October 5, 2020

Let's make some things clear. Let G be a discrete subgroup of M_2. $\bar{G} = \pi(G)$, the point group of G and $L = \ker \pi$

Example 100

If you take a rhombic lattice, every element of $\bar{G}$ preserves this lattice. Thus $\bar{G} \leq D_2$

Theorem 101

Let $G \leq M_2$ be discrete.

(1) L is a discrete subgroup of $\mathbb{R}^2$

(2) If $L \neq \{0\}$, then $\bar{G} = C_n$ or D_n where n is 1,2,3,4 or 6.

(3) If $L = \{0\}$ then G is finite.

Proof. (1): A subset of a discrete set is discrete.
(2): Let a be the shortest nonzero vector in L. If ρ_θ is a rotation in $\bar{G}$, then $\rho a \in L$. Then $\theta \geq 2\pi/6$ since otherwise $\rho a - a$ is shorter than a, a contradiction. Thus $\bar{G}$ is a discrete subgroup of O_2. So $\bar{G} = C_n$ or D_n and $n \leq 6$. If $n = 5$, then $a + \rho_{2(2\pi/5)} a$ is shorter than a, contradiction. If you have a square lattice, $n = 4$ is legit.
(3) Suppose $L = \{0\}$. Let H be the subgroup of orientation preserving isometries in G. If H has rotations around two different points, then there exists a translation in H. But that's impossible since L contains no translations. Thus, after changing origin, H is a discrete subgroup of SO_2, so $h \cong C_n$. Then G is finite: $|G| \leq 2|H|$. So $G \cong C_n$ or D_n. □

10.1 Group Action

Each $A \in GL_n$ gives a bijection $\mathbb{R}^n \xrightarrow{A} \mathbb{R}^n$. Package them all into one function. $GL_n \times \mathbb{R}^n \to \mathbb{R}^n$, $(A, \vec{x}) \mapsto A\vec{x}$. We say GL_n acts on $\mathbb{R}^n$. Similarly, we can say that S_n acts on $\{1, 2, ..., n\}$. M_2 acts on $\mathbb{R}^2$.

Definition 102

Let G be a group and S a set. An action of G on S is a function $G \times S \to S$, $(g, s) \mapsto gs$. It satisfies the following two properties:

(1) $1s = s$ for all $s \in S$.

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

Let G act on S. Fix $g \in G$, get a permutation of S. $m_g : S \to S$, $s \mapsto gs$. The inverse is $m_{g^{-1}}$. This is easy to show using the two axioms of group actions above.
The map $G \to Perm(S)$, $g \mapsto m_g$ is a group homomorphism: $m_g m_h = m_{gh}$ because $m_g(m_h(s)) = g(hs) = (gh)s = m_{gh}s$ for all $s \in S$.
Giving an operation of G and S is the same as giving a a homomorphism from G to the permutation group of S.

Definition 103

The operation is faithful if the only $g \in G$ that acts triviall on S is the identity of G. I.e. $gs = s$ for all s implies that $g = 1$. This is equivalent to $\ker(G \to Perm(S)) = \{0\}$, or that this map is injective

Definition 104

Suppose G acts on S, $s \in S$. The orbit of s is $O_s = Gs = \{gs : g \in G\}$. This is a subset of S.

Definition 105

The stabilizer of s is the set $\text{Stab}_G(s) = \{g \in G : gs = s\}$. This is not the kernel of $G \to Perm(S)$ since this is the set that stabilizes all $s \in S$. The kernel of this homomorphism is $\cap_{s \in S} \text{Stab}_G(s)$.

Example 106

Take S_n. The stabilizer of any element is isomorphic to S_{n-1}.

Proposition 107

The orbits form a partition of S. This can be proved by showing that the the orbit defines an equivalence class on S.

Proposition 108

Let G act on S and $s \in S$. Let $H = \text{Stab}(S)$. There exists a bijection between $G/H \xrightarrow{\varepsilon} O_s$, $gH \mapsto gs$.

Proof. For $g, \gamma \in G$, $\gamma s = gs$ if and only if $g^{-1}s = s$, or equivalently that $g \equiv \gamma(\text{Stab}(s)$. Thus the mapping above is well-defined and the mapping is injective. The map is trivially surjective. □

Corollary 109

$|O_s| = (G : \text{Stab}(s))$ or equivalently $|O_s||\text{Stab}(s)| = |G|$. This is called the orbit stabilizer formula. For any $H \leq G$, normal or not, G acts on G/H by g maps $C \in G/H$ to gC. This turns out to be transitive, stabilizer of the coset $H \in G/H$ is H.

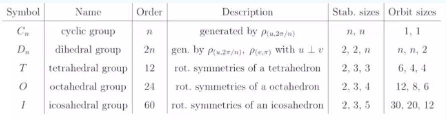
11 October 7, 2020

The orbit of s_1 is in bijection with G/H_1 where $H_1 = \text{Stab}(s_1)$. Suppose $s' = as$. Then $\text{Stab}(s') = a\,\text{Stab}(s)a^{-1}$. Recall that $S0_3$ are the rotations in $\mathbb{R}^3$ that fix the origin.

Theorem 110

The finite subgroups of SO_3 are the following:

1 1072020.PNG



Symbol	Name	Order	Description	Stab. sizes	Orbit sizes
C_n	cyclic group	n	generated by $\rho_{(u,2\pi/n)}$	n, n	1, 1
D_n	dihedral group	$2n$	gen. by $\rho_{(u,2\pi/n)}$, $\rho_{(v,\pi)}$ with $u \perp v$	2, 2, n	n, n, 2
T	tetrahedral group	12	rot. symmetries of a tetrahedron	2, 3, 3	6, 4, 4
O	octahedral group	24	rot. symmetries of a octahedron	2, 3, 4	12, 8, 6
I	icosahedral group	60	rot. symmetries of an icosahedron	2, 3, 5	30, 20, 12

Let G be a finite subgroup. For $g \in G$, g fixes two unit vectors (along the axis of rotation). Let

$$P = \bigcup_{g \neq 1} \{\text{poles of g}$$

. If $G = C_n$ there are two poles. If $G = D_n$, there are 2+2n poles.

Lemma 111

If p is a pole and $g \in G$, then gp is a pole.

Proof of Theorem 110. Since p is a pole, $\mathrm{Stab}(p) \neq \{1\}$. Then $\mathrm{Stab}(gp) = g\,\mathrm{Stab}(p)g^{-1} \neq \{1\}$. Thus G acts on $\mathbb{P}$, the set of poles of G. Let $N = |G|$. Let $r_i = |\mathrm{Stab}(p_i)|$ and $n_i = O_{p_i}$. Then $n_i r_i = N$. We know that $1 < r_i \leq N$. We are going to count pairs (g, p) where $g \neq 1$ and p is a pole of g. This is the same as

$$\sum_{g \in G \cap g \neq 1} 2 = 2N - 2 = \sum_{p \in \mathbb{P}} |(\mathrm{Stab}(p)| - 1) = N \sum_i (1 - r_i)$$

Thus, $\sum_i (1 - r_i) = 2 - 2/N \in [1, 2)$. In the case of two orbits, $\frac{1}{r_1} + \frac{1}{r_2} = \frac{2}{N} \geq \frac{1}{N} + \frac{1}{N}$ so $r_i = N$. Thus n_1 and n_2 are equal to 1 by the orbit stabilizer formula. Geometrically, the total number of poles is 2 and each pole is fixed by the whole group. If there are three orbits, $N - (\frac{1}{r_1} + \frac{1}{r_2} + \frac{1}{r_3}) = 2 - \frac{2}{N}$. Thus $\frac{1}{r_1} + \frac{1}{r_2} + \frac{1}{r_3} = 1 + \frac{2}{N}$. If $r_1 \geq 3$, then the left hand side is less than or equal to $\frac{1}{3} + \frac{1}{3}\frac{1}{3} = 1$. If $r_2 \geq 4$ then the left hand side is less than or equal to $\frac{1}{2}$ a contradiction. Subcase $r_2 = 2:$ Then $\frac{1}{r_3} = \frac{2}{N}$ so $r_3 = \frac{N}{2}$ so that $G = D_{\frac{N}{2}}$. Subcase $r_2 = 3: \frac{1}{r_3} = \frac{1}{6} + \frac{2}{N}$. Subsubcase: $r_3 = 4$. $\frac{1}{4} = \frac{1}{6} + \frac{2}{N}$ so $N = 24$. The r_i are $2, 3, 4$ (stabilizer sizes), The n_i are 12,8,6j (orbit sizes). Thus G preserves the set of vertices of an octahedron. □

12 October 9. 2020

What are the finite subgroups of O_3? O_3 is generated by SO_3 and $\{\pm I\}$ with intersection $\{I\}$ since $\det(-I) = (-1)^3 = -1$ and $gh = hg$ for all $g \in SO_3$ and $h \in \{\pm I\}$, so $O_3 \cong SO_3 \times \{\pm I\}$. We can classify the finite subgroups of O_3 using Goursat's lemma.

Lemma 112 (Goursat's lemma)

Let G and G' be groups and let H be a subgroup of $G \times G'$ such that the two projections $p_1 : H \to G$ and $p_2 : H \to G'$ are surjective (H is a subdirect product of G and G'). Let N be the kernel of p_2 and N' the kernel of p_1. Once can identify N as a normal subgroup of G and N' as a normal subgroup of G'. Then the image of G in $G/N \times G'/N'$ is the image of an isomorphism $G/N \cong G'/N'$

Two actions of G on $\mathbb{G}$: left multiplication: g does $m_g : \mathbb{G} \to G$, $x \mapsto gx$. We get a homomorphism $G \to Perm(\mathbb{G})$, $g \mapsto m_g$. What is the kernel? If g is the kernel, then $m_g = \mathrm{id}$, so $m_g(1) = 1$, so $g = 1$. Thus $\ker = \{1\}$. Cayley's theorem says that if $|G| = n$, then G is isomorphic to a subgroup of S_n. Conjugation: g does $x \mapsto gxg^{-1}$. The orbit of x is $\{gxg^{-1} : g \in G\}$ which is the **conjugacy class** of x. The stabilizer of x is $\{g \in G : gxg^{-1} = x\} = \{g \in G : gx = xg\} = Z(x)$, the **centralizer** of x (this is a subgroup). Then $|G| = |C(x)||Z(x)|$. $C(x) = \{x\}$ if and only if $Z(x) = G$ if and only if $x \in Z$, the center of G. The class equation is $|\mathbb{G}| = |C_1| + \ldots + |C_k| = |Z| + |G| \sum_{x \notin Z} \frac{1}{|Z(x)|}$.

Definition 113

G is a p-group if and only if $|G|$ is a power of p.

Definition 114

An **Elementary Abelian p-group** is an Abelian group G in which every element has order dividing p.

Example 115

$C_p \times C_p \times C_p \cong \mathbb{F}_p^3$

Proposition 116

If G is a nontrivial p-group, its center is not trivial

Proof. Given $|G| = p^e$ for some $e \geq 1$, each $|C_i|$ divides p^e so it is a power of p. By the class equation, $p^e = |Z| + \sum(\text{ higher powers of p})$ so p divides $|Z|$ (all those C_i with $|C_i| = 1$ go into the center). □

Proposition 117

If $|G| = p^2$, then G is abelian

Proof. The trivial group is a proper subgroup of Z which is a subgroup of G. If $|Z| = p$, choose $x \in G - Z$. Then Z is a proper subgroup of $Z(x)$ since $x \in Z(x)$ so $|Z(x)| = p^2$, a contradiction since $x \in Z$ and $x \notin Z$. □

Proposition 118

If $|G| = p^2$, then $G \cong C_{p^2}$ or $G \cong C_p \times C_p$. If every element of G has order p^2, then G is C_{p^2}. If there is an element of order p, then G must $C_p \times C_p$

If d is a divisor of n, then n factors into d and $\frac{n}{d}$. If N is a normal subgroup of G, then G decomposes into N and G/N.

Definition 119

n is a prime number if and only if $n > 1$ and its only positive divisors are 1 and n.

Definition 120

G is a simple group if and only if $G \neq \{1\}$ and its only normal subgroups are itself and the trivial group.

Next time, we'll prove that $I \cong A_5$ where I is the icosahedral group and its also simple.

13 October 13, 2020

Theorem 121

$I \cong A_5$ and it is simple.

I is the group of rotational symmetries of an icosahedron and it is a subgroup of SO_3.

Pole directionn	$\lvert$Orbit$\rvert$	Stabilizer	Elements in stabilizer	How man elts?
midpoint of face	30	C_2	$\rho_{(u,\pi)}$	15
Center of face	20	C_3	$\rho_{(u,2\pi/3)}$	20
vertex	12	C_5 $\rho_{(u,2\pi/5)}$, $\rho_{(u,4\pi/6)}$	12, 12	

The class equation gives $60 = 1+12+12+15+20$. If N is a normal subgroup of I then N is the union of some of the conjugacy classes. But $|N|$ divides 60 so $N = \{1\}$ or $N = I$. This shows I is simple. Now we show I is isomorphic to A_5. Find a set of cardinality 5 that I acts on. I acts on a dodecahedron. $S :=$ the set of 5 cubes with vertices at the dodecahedron's vertices. I acts on S. You get $\phi : I \to Perm(S)$. But $\ker\phi$ is either 1 or I since I is simple. But $\ker\phi \neq I$ since I doesn't act nontrivially on S. Thus ϕ is injective. Consider $I \to S_5 \xrightarrow{sgn} \{\pm\}$. Call this composition ψ. But $\ker\psi = \{1\}$ or $\ker\psi = I$. In the first case, $\psi : I \to \{\pm\}$ is injective. But this is impossible since $|I| = 60$ and $|\{\pm\}| = 2$. Thus $\ker\psi = I$ so the image of all elements in I is an even permutation, or $\phi(x) \in A_5$. Thus I is isomorphic to A_5.

Next, we'll talk about conjugating in S_n.

Consider $p = (14)(253) \in S_5 = Perm(\{1, 2, ..., 5\} \cong Perm(\{a, b, ..., 3\})$ and $p' = (ab)(cde) \in Perm(\{a, b, ..., 3\})$. Define a bijection $\{1, 2, ..., 5\} \to \{a, b, ..., e\}$. Then $qpq^{-1} = p'$. Instead of going between going between two different sets, consider the case where q is the bijection from $\{1, ..., 5\}$ to itself so that qpq^{-1} is conjugation. View q as a "relabeling" of the numbers. Two elements are conjugate to each other if and only if the lengths of their cycles are the same.

The number of conjugacy classes in $|S_n|$ is the partition function of n. How many elements of S_10 are conjugate to $(123)(456)(78910)$. $|Z(x)| = 2! \times 3 \times 3 \times 4$ the $2!$ comes from the number of ways to decide which 3 cycle comes first and the $3 \times 3 \times 4$ comes from how many ways there are to rotate the other cycles.

14 October 14, 2020

S_4 acts by conjugation on the conjugacy class of $(12)(34)$. Let $a = (12)(34), b = (13)(24), c = (14)(23)$. Get permutation representation $\phi : S_4 \to Perm(\{a, b, c\}) \cong S_3$, $(12) \mapsto (bc), (123) \mapsto (acb), (12)(34) \mapsto 1$. Thus ϕ is surjective. $|\ker\phi| = \frac{|S_4|}{|\operatorname{im}\phi|} = 4$. In fact, $V = \ker\phi = \{1, a, b, c\}$. This is a normal subgroup. $|V| = p^2$ so it is either C_4 or $C_2 \times C_2$. I know that the Klein group is $C_2 \times C_2$.

Example 122

Is A_4 simple? No, because V is a normal subgroup of A_4.

The conjugacy classes in A_4 are 1. the identity, 2. the 3 cycles, and 3. the product of disjoint 2 cycles. Is (123) conjugate to (213) in S_4? Yes, conjugation by (12). However, not in A_4. It's conjugate in A_5 though. If $n \geq 5$ then $\{3 \text{ cycles in } A_n\}$ is one conjugacy class in A_n.

Theorem 123

If $n \geq 5$ then A_n is simple. We did this last time for $n = 5$ by showing it's isomorphic to the icosahedral group.

Proof. Suppose N is not the trivial group and is normal in A_n. We need to show $N = A_n$. Choose $x \in N$, $x \neq 1$. We need only show that A_n contains a 3-cycle. In that case, all 3-cycles are in N. Since the 3-cycles generate A_n from a problem in PSET 1, it will follow that $N = A_n$.

Case 1: x has order $l \geq 5$ where l is prime. Let $x = (1, 2, 3, 4, 5, ..., l)y$ where y stabilizes 1,2,3,4,5. Let $g = (432)$. then $gxg^{-1}x^{-1} = (245)$. The commutator is a 3-cycle.

Case 2: x has order 3. If x contains is a 3-cycle then we're done. If not, then let $x = (123)(456)y$. Let $g = (432)$. Then $gxgg^{-1}x^{-1} = (15243)$. The commutator has order 5. Go back to case 1.

Case 3a: x has order 2 and it contains a 1-cycle. Since it is an even permutation, x must contain at least two 2-cycles, say $x = (12)(34)(5)y$. Let $g = (531)$. Then $gxg^{-1}x^{-1} = (15243)$. The commutator has order 5 so go back to case 1.

Case 3b: x has order $l = 2$ and contains no 1-cycles. Since $n \geq 5$, x contains no more than two 2-cycles. Say $x = (12)(34)(56)y$. Let $g = (531)$. Then $gxg^{-1}x^{-1} = (153)(246)$. The commutator has order 3 and we go back to case 2. These are the possiblities for an even permutation of prime order, so the proof is complete.

□

Definition 124 (The Normalizer)
Suppose G acts on itself by conjugation. Then G acts on the set of subsets of G. For $H \leq G$, $\text{Stab}(H) = \{g \in G : gHg^{-1} = H\}$. This is also called the normalizer of H, $N(H)$.

Example 125
Let $G = S_3$. What is the normalizer of $H =< (12) >$? $|G|$ is the product of the conjugates of H and the order of the normalizer of H. Thus $|N(H)| = 2$ so $N(H) = \{1, (12)\}$ so $N(H) = H$

Theorem 126 (Lagrange's Theorem)
If $H \leq G$ then $|H|$ is a divisor of $|G|$. If d divides $|G|$ must G have a subgroup of order d? No! Then This would lead to too many elements.

However, if d is a prime power, then the answer to the above question is yes.

Theorem 127 (1st Sylow Theorem)
Suppose $|G| = n = p^e m$ where p doesn't divide m. Then there is a subgroup H of G with $|H| = p^e$.

15 October 16, 2020

Theorem 128 (Cauchy's Theorem in Group Theory)
If p divides $|G|$ then G has an element of order p.

Cauchy's theorem for a finite Abelian Group. Let $|G| = n$ and $x_1, ..., x_n$ elements of G. We get a surjective homomorphism $< x_1 > \times < x_2 > \times ... \times < x_n > \to G$ where $y_1, y_1, ..., y_n \mapsto y_1 + ... + y_n$. If p divides $|G|$ then p divides $| < x_1 > \times ... \times < x_n > |$ so p divides $| < x_i > |$ for some i. So $< x_i >$ contains a copy of C_p. □

Proof of Sylow Theorem 1. By induction on the order of G. Assume that p divides $|G|$. Use the class equation:

$$|G| = |Z| + \sum_{\text{conjugacy classes}} |C(x)|$$

.

Case 1: Some $|C(x)| > 1$ is not divisible by p. Then $|G| = |C(x)||Z(x)|$ (orbit stabilizer theorem). This shows that $Z(x)$ is divisible by the same power of p as $|G|$, so a Sylow p-subgroup of $Z(x)$ is a Sylow p-subgroup of G. By the induction hypothesis, $Z(x)$ has a Sylow p-subgroup.

Case 2: Every $|C(x)| > 1$ is divisible by p. Class equation says that $|Z|$ is divisible by p. Cauchy's theorem for $|Z|$ says that there exists $C_p \leq Z$. Get $G \xrightarrow{\pi} G/C_p$. Let S be the Sylow p-subgroup of G/C_p (which exists from the inductive hypothesis) so $|S| = p^{e-1}$ since $|G| = p^e m$ and $|G|/|C_p| = p^{e-1}m$. Then $|\pi^{-1}(S)| = |\ker \pi||S| = p^e$ so this is a Sylow p subgroup for G.

□

Proof of Cauchy's theorem for any finite group. We are given that p divides $|G|$. We want to know that G contains a subgroup of order p. It has a Sylow p-subgroup. If $x \in S$ then the order of x is p^k for some k. Then $x^{p^{k-1}}$ has order p. □

Theorem 129 (2nd Sylow Theorem)

Fix a finite group G and a prime p

1. The Sylow p subgroups are conjugates of each other.
2. Every p subgroup of G is contained in a Sylow p-subgroup.
3. The Sylow p subgroups are normal if and only if G has only one Sylow p subgroup

Lemma 130

Let X be a finite set and P a p-group acting on X. Then $X^P = \{x \in X : px = x \forall p \in P\}$. Then $|X| \equiv |X^P| \bmod p$.

Proof. Every orbit in $X - X^P$ has size p^a for some $a \geq 1$. Add their sizes to get $|X - X^P|$ is divisible by p. □

Proof of 2nd Sylow Theorem. 2. Let S be a Sylow p-subgroup. Let P be any p-subgroup. Let $X = G/S$ so $|X| = |X^P| = m \neq 0(\bmod p)$ so there exists $x \in X$ fixed by P. Then $P \leq \text{Stab}(x) = aSa^{-1}$ for some $a \in G$.

1. If S' is another Sylow p-subgroup, the previous thing we proved shows that $S' \leq aSa^{-1}$ for some a but equality must hold since the orders of the groups are the same

3. If S is normal then $gSg^{-1} = S$ for all $g \in G$. But $\{gSg^{-1} : g \in G\}$ gives every Sylow p-subgroup so there must be only one Sylow p-subgroup.

□

Theorem 131 (3rd Sylow Theorem)

The number of Sylow p subgroups is 1 mod p and divides m

Proof. Let X be the set of Sylow p subgroups. Choose $S \in X$. G acts by conjugation on X. $|G| = |Orbit(S)||\text{Stab}(S)| = |X||\text{Stab}(x)|$. The stabilizer is the normalizer of S. Thus $|X| = \frac{|G|}{|N|}|\frac{|G|}{|S|} = \frac{p^e m}{p^e} = m$. since $S \leq N$ so $|S|||N|$. □

Remark 132. *If Poonen doesn't show the second part of this theorem, I'll try to prove it later.*

16 October 19, 2020

Let's do a quick review of last time: If $H \leq G$ the **normalizer** of H in G is $N(H) = \{g \in G : gHg^{-1} = H\}$. Then H is a normal subgroup of $N(H)$ by the definition of normal subgroup.
Let P be a p group acting on a finite set X. Let $X^P = \{x \in X : gx = x \forall g \in P\}$. Then $|X| = |X^P| (\mod p)$. Let G be a finite group of order $n = p^e m$ where $p^e||n$ and p doesn't divide m. We proved the three Sylow Theorems last time. We're going to show now that the number of Sylow p-subgroups is 1 mod p.

Proof of 1 mod p. $X = \{\text{Sylow p subgroups of G}\}$. We want to show that $|X| = 1 \mod p$. Let S be one Sylow p subgroup. Restrict the conjugaction action of G on X to get an action of S on X. For $s' \in X$, $s' \in X^S \iff S'$ is fixed by every element of $S \iff$ every element of S is in $\text{Stab}(S') \iff S \leq N(S') \iff S' = S$. We claim that S, S' are Sylow p-subgroups If $S \leq N(S')$ then $S = S'$. If S' is a normal subgroup $N(S')$ and S' is a Sylow of $N(S')$. By Sylow 2(c), S' is the only Sylow p-subgroup of $N(S')$. Thus $S = S'$. Thus $X^S = \{S\}$. Finally $|X| = |X^S| = 1 \mod p$. □

Theorem 133

Let F be a finite abelian group. Then G is a product of its Sylow p-subgroups, one for every prime p dividing $|G|$.

Example 134

Let $G = C_6 \times C_4 = (C_2 \times C_4) \times C_3$. The first two terms are from the Sylow 2 subgroup and the third is from the sylow 3 subgroup.

Proof. Write $|G| = p_1^{e_1} ... p_k^{e_k}$. Let S_i be the Sylow p_i subgroup. Since G is abelien $\phi : S_1 \times S_2 \times ... \times S_k \to G$ where $x_1, ..., x_k \mapsto x_1 + ... + x_k$ is a homomorphism. Then $\text{im}\,\phi$ contains each S_i. Thus $|\text{im}\,\phi|$ is divisible by $p_e^{e_i}$ for all i. Hence divisible by $p_1^{e_1} ... p_k^{e_k} = |G|$. So ϕ is an isomorphism. □

Example 135

The multiplicative group of the field with 7 elements is an abelian group order 6. This group is isomorphic to $C_2 \times C_3 \cong C_6$. So it contains a copy of $C_3 : \{1, 2, 4\}$.

Example 136

Consider the $ax + b$ group m under the operation of composition. $m = \{ax + b : a \in \mathbb{F}_7^\times, b \in \mathbb{F}_7\} \leq Perm(\mathbb{F}_7)$. For example $(5x + 2) \circ (3x + 1) = 5(3x + 1) + 2 = 15x + 7 = x = \text{id}$. Look at $m \xrightarrow{\pi} \mathbb{F}_7^\times$, $(x \mapsto ax + b) \mapsto a$. Let $J = \pi^{-1}(\{1, 2, 4\}) = \{(ax + b) \in m : a \in \{1, 2, 4\}, b \in \mathbb{F}_7\}$. It has the following properties: $|J| = 21$, J is nonabelian. If $x = x + 1$ and $y = 2x$ then $x^7 = 1$ and $y^3 = 1$.

Theorem 137

Every group of order 21 is isomorphic to C_{21} or $J = C_3 \times C_7$.

Proof. Let G be a group of order 21. By Sylow theorem 3, the number of Sylow 7-subgroups is 1 mod 7, divides 3. so there is only 1. Let $H_7 =< x >$ be the Sylow 7-subgroup. By Sylow theorem 2(c), H_7 is normal in G. Let $H_3 =< y >$ be a Sylow 3 subgroup. The number of such subgroups is congruent to 1 mod 4 and divides 7 so it is either 1 or 7. Then $H_7 \cap H_3$ is the trivial subgroup. The map $H_7 \cap H_3 \to G$, $(x^i, y^j) \mapsto x^i j^j$ is injective but not necessarily a homomorphism. It is also bijective since the orders are the same. Thus $G = \{x^i y^j : 0 \le i < 7, 0 \le j < 3\}$ as a set. Since H_7 is normal $yxy^{-1} = x^a$ for some $0 < a < 7$. or each a there is at most one possible G up to isomorphism. Given $a, yx = x^a y$. This identity lets us rewrite any products $(x^i y^j)(x^{i'} y^{j'}) = x^c y^d$ so the group law is determined.

We get a homomorphism $\phi : H_3 \to Aut(H_7) \cong \mathbb{F}_7^\times, Y \mapsto \text{(conjugation by Y)} \iff \text{(the b such that } YxY^{-1} = x^b)$.

Case 1: $|\operatorname{im}\phi| = 1$, $\phi(y) = 1$, $yxy^{-1} = x$ so $yx = xy$ so $G \cong < x > \times < y > \cong C_7 \times C_3 \cong C_21$. by Euler's theorem in number theory.

Case 2: $|\operatorname{im}\phi| = 3$. Then $< y > \xrightarrow{\phi} \{1, 2, 4\} \le \mathbb{F}_7^\times$. Choosing a different generator of H_3 if necessary, WLOG $\phi(y) = 2$. Then $yxy^{-1} = x^2$. Does this actually occur? Yes, for $G = J$. The same argument shows that given primes $p < q$ the group of order pq are C_{pq}, if $p|q-1$, also $\{ax + b : a \in \mathbb{F}_p^\times, \operatorname{ord}(a) = p, b \in \mathbb{F}_p\}$.

□

17 October 21, 2020

We're talking about free groups today. Start with symbols x, y, x^{-1}, y^{-1}. A word is a finite string of these symbols, repetition allowed.

Definition 138

A word is reduced if it doesn't have an adjacent pair of symbols that cancel.

Proof. Start with some cancellation sequence. If xx^{-1} gets cancelled at some point, we could have cancelled it. $w \to w_1 \to w_2 \to \ldots \to w_n$. There can be different chains to get to w_n.If not, then some w_i must be $x^{-1}xx^{-1}$. So we might as well cancel xx^{-1} and proceed. □

Definition 139

$F_2 = \{\text{words}\}/\sim$ where $w \sim w'$ if w and w' have the same reduced form.

Multiplication is well-defined on this group.

Proof. Reduce wv by first cancelling as much as possible within w and within v: Then you get $w_{red} v_{red}$. This is well-defined. □

Concatenation is associative. The identity is the empty word. There are inverses. For example the inverse of $xyxxy^{-1}$ is $yx^{-1}x^{-1}y^{-1}x^{-1}$ is the empty word. Thus F_2 is a group.

18 October 23, 2020

The set of words on two letters, F_2 is generated by x and y which satisfy no relations, except those forced by the group axioms. There is the **Universal mapping property** of F_2. Let G be a group. Giving a homomorphism $\phi : F_2 \to G$ is the same as giving $g, h \in G$ (in order, possibly equal).

Sketch of Proof. Given ϕ, let $g = \phi(x)$ and $h = (y)$. Just look where the generators go. For example, given $g, h \in G$, define $\phi : F_2 \to G$ by sending the equivalence class $xyyx^{-1} \mapsto ghhg^{-1}$ evaluated in G. etc. This is well-defined. for example $xyxx^{-1}yx^{-1} \mapsto ghgg^{-1}hg^{-1}$. But these are the same. □

What happens if we have $< x, y : x^3 = 1, y^2 = 1, yx = x^y >$ for example? What does this notation actually mean? $< x, y : R >$ where R is the things that should be one. In the previous example, $R = \{x^3, y^2, yxy^{-1}x^{-2}\} \subseteq F_2$. What quotient should we take of F_2 to make these things equal to 1. If these things are 1 then x^3y^2 should also be one. So should $yx^3y^{-1} = 1$. $< x, y : R >= F_2/\mathcal{R}$ where $\mathcal{R}$ is called the normal subgroup generated by R. It is the set of elements obtained from R by repeatedly taking products, inverses, and conjugated by elements of F_2. It's a group since its closed under taking products and inverses and its a normal subgroup since its closed under conjugation. It is the smallest normal subgroup containing R.

Definition 140

$< x, y : R >= F_2/\mathcal{R}$.

This group also has a universal mapping property.

Definition 141 (Universal Mapping Property of $< x, y : R >$)

Le tG be a group. Giving a homomorphism $\phi :< x, y : R >\to G$ is the same as giving $g, h \in G$ satisfying each relation in G.

Proof. The following data are equivalent: $\phi :< x, y : R >\to G$, $F_2/\mathcal{R} \to G$. By the universal property of the quotient group, this is the same as giving a homomorphism $F_2 \to G$ where all elements of R map to 1. □

ϕ is surjective iff g, h generate G.

Example 142

$< x, y : x^5 = 1, y^2 = 1, yxy^{-1} = x^{-1} \xrightarrow{\phi} D_5$.

Map x to the rotation by $\frac{2\pi}{5}$ and y gets mapped to a reflection in the horizontal axis. The map is well-defined since the rotation and reflection satisfy the relations. It's surjective since the reflections and rotations generates D_5. Is it injective? In G, use $yx = x^{-1}y$ to write every element as x^iy^j and $0 \leq i < 5$ and $0 \leq j < 2$. These elements go to distinct elements in D_5 so ϕ is injective.

Example 143

$< x, y : xy = yx >\cong \mathbb{Z}^2$. This is a free abelian group on two generators.

Example 144

$< x, y : x^7 = 1, y^3 = 1, yxy^{-1} = x^3 >$. But then $yyyxy^{-1}y^{-1}y^{-1} = x^{27}$ so the order of x is one so it's the identity element. Thus this group is the cyclic group with 3 elements.

Example 145

Let $\mathbb{R}^2 \times \mathbb{R}^2 \to \mathbb{R}$, $x, y \mapsto x^T y$. Fix one variable and this map becomes linear in the other.

Example 146

$\mathbb{R}^2 \times \mathbb{R}^2 \to \mathbb{R}$, $x, y \mapsto 2x_1y_1 + 3x_1y_2 + 5x_2y_2 + 7x_2y_2 = x^T \begin{pmatrix} 2 & 3 \\ 5 & 7 \end{pmatrix} y = x^T Ay$

Definition 147 (Bilinear Form)

This is a function $<,>: V \times V \to \mathbb{R}$ such that

$$< v_1 + v_2, w >=< v_1, w > + < v_2, w >$$

and

$$< rv, w >= r < v, w >$$

and the same is true for the other variable.

Proposition 148

There is a bijective correspondence between the $n \times n$ matrices in $\mathbb{R}^n$ and the bilinear forms on $\mathbb{R}^n$. Given A, define $x, y >= x^t Ay$. Given $<,>$ define $A = (a_{ij})$ where $a_{ij} =< e_i, e_j >$.

19 October 26, 2020

Proof of the previous proposition. Given $<,>$ on V and a basis $B = (v_1, ..., v_n)$ of V to get the matrix of $<,>_V$ with respect to B. Take $A = (a_{ij})$ where $a_{ij} =< v_i, v_j >$ or think of it as V $<,>_V$ B is an isomorphism between V and $\mathbb{R}^n$. Define A so that $x^t Ay =< x, y >=< B_x, B_y >_V$.

Suppose B' is another basis. $\mathbb{R}^n \xrightarrow{B \sim} V \xrightarrow{B' \sim} \mathbb{R}^n$. We get a basechange matrix $P : \mathbb{R}^n \xrightarrow{\sim} \mathbb{R}^n$. $< x, y >' =< Px, Py >= (Px)^t A(Py) = x^t(P^t AP)y$ so the matrix of $<,>_V$ with respect to B' is $P^t AP$. □

Definition 149 (Symmetric Bilinear Form)

$<,>$ is symmetric if for all x, y, $< x, y >=< y, x >$.

Definition 150 (Symmetric Matrix)

A matrix $A = (a_{ij})$ is symmetric $\iff$ $a_{ij} = a_{ji}$ for all i, j. This is equivalent to saying $A^t = A$.

Definition 151 (Skew-Symmetric Bilinear Form)

$< v, w >= - < w, v >$ for all vectors v and w.

Definition 152 (Skew-Symmetric Matrix)

$A^t = -A$ or equivalently $a_{ij} = -aij$.

Definition 153 (Positive Definite Bilinear Form)

Let V be a real vector space. $<, >$ is a symmetric form on V. $<, >$ is positive definite if and only if $< v, v >\geq 0$ with $< v, v >= 0 \implies v = 0$. An example of this is the dot product.

Definition 154 (Positive Semidefinite Bilinear Form)

$< v, v >\geq 0$ for all v.

Definition 155 (Negative Definite Bilinear Form)

$< v, v >\leq 0$ for all v and $< v, v >= 0 \implies v = 0$

Definition 156 (Negative Semidefinite Bilinear Form)

$< v, v >\leq 0$ for all v.

Example 157 (Important in Special Relativity)

Let V be space time, $\mathbb{R}^3 \times \mathbb{R} = \mathbb{R}^4$. The Lorentz form: $< (x_1, y_1, z_1, t_1), (x_2, y_2, z_2, t_2) >= x_1x_2 + y_1y_2 + z_1z_2 - t_1t_2$. This is neither positive semidefinite nor negative semidefinite. This is called indefinite.

Definition 158 (Indefinite Bilinear Form)

A bilinear form is indefinite if it is neither positive semidefinite nor negative semidefinite.

Definition 159 (Adjoint of a matrix)

Let A be a matrix with complex entries. The adjoint of A is the complex conjugate of A. $A^* = \bar{A}^t$.

Definition 160 (Hermitian Matrix of Self-Adjoint Matrix)

Let A be a matrix with complex entries such that $A^* = A$. Then it is Hermitian or Self-Adjoint.

Example 161

The matrix below is self-adjoint:

$$\begin{pmatrix} 5 & 2+3i \\ 2-3i & 7 \end{pmatrix}$$

All real symmetric matrices are also Hermitian.

Let $x, y \in \mathbb{C}$. Define x^*y

Definition 162 (Hermitian Form)
This is slightly different from a bilinear form.$<,>: V \times V \to \mathbb{C}$ such that $< v_1 + v_2, w > = < v_1, w > + < v_2, w >$, $< cv, w > = \bar{c} < v, w >$, $< v, w_1 + w_2 > = < v, w_1 > + < v, w_2 >$, $< v, cw > = c < v, w >$, $< w, v > = < \bar{v, w} >$. These constraints can be described as "conjugate linear in the first variable, $\mathbb{C}$ linear in the second variable, and conjugate symmetric"

Definition 163
Every symmetric bilinear form on $\mathbb{R}^n$ is $x, y \mapsto x^tAy$ for some symmetric $A \in \mathbb{R}^{n \times n}$.

Proposition 164
Every Hermitian form on $\mathbb{C}^n$ is $x, y \mapsto x^*Ay$ for some Hermitian matrix A.

Proof. Given $<,>$ on V, $\mathbb{C} - basisB$ of V, you get a matrix $A = (a_{ij})$ where $a_{ij} = < v_i, v_j >$. Changing basis to $B' = BP$ changes the matrix A to $A' = P^*AP$. □

Definition 165 (Standard Hermitian form)
The Standard Hermitian form is the form $< X, Y > = X * Y = \bar{x_1}y_1 + ... + \bar{x_n}y_n$.

20 October 28, 2020

There are a lot of analogs between the matrices in $\mathbb{R}$ and matrices in $\mathbb{C}$. For $P \in GL_n(\mathbb{C})$, $< Px, Py > = < x, y >$ for all $x, y \in \mathbb{C}^n$. The columns of P form an orthonormal basis of $\mathbb{C}^n$. $P^*P = I$. $U_n = \{P \in GL_n(\mathbb{C}) : P^*P = I\}$. The matrices in the special unitary group are the logic gates in quantum computing.

Theorem 166
Let $A \in \mathbb{C}^{n \times n}$ be Hermitian. Then the eigenvalues of A are real numbers.

Proof. Suppose that $Av = \lambda v$. Take adjoints $v^*A = \bar{\lambda}v^*$. Then $v^*Av = \lambda v^*v$ and $\bar{\lambda}v^*v$. Then $\lambda = \bar{\lambda}$. We can divide by v^*v since $v^*v = \sum |v_i|^2 > 0$. Then the imaginary part of λ must be zero. □

Corollary 167
Then $\det A$ and $\operatorname{tr} A$ are real numbers too.

Corollary 168
$A \in \mathbb{R}^{n \times n}$ is symmetric. Then the eigenvalues of A are real.

Let V be a $\mathbb{R}$ valued space equipped with a symmetric bilinear form $<,>$ or V a complex-valued space equipped with the Hermitian form $<,>$.

Definition 169

$v \perp w$ means $< v, w >= 0$. $v \perp W$ means $v \perp w$ for all $w \in W$. $W_1 \perp W_2$ means $w_1 \perp w_2$ for all $w_1 \in W_1$ and $w_2 \in W_2$.

Example 170

Let V be spacetime. $\mathbb{R}^4$ with $x_1x_2 + y_1y_2 + z_1z_2 - t_1t_2$. Let $v = (1, 0, 0, 1)$. Then $< v, v >= 0$

Definition 171

$(v_1, ..., v_n)$ is an **orthogonal basis** if and only if $(v_1, ..., v_n)$ is a basis and $v_i \perp v_j$ whenever $i \neq j$ and is an **orthonormal basis** if and only if $(v_1, ..., v_n)$ is a basis and $v_i \perp v_j$ whenever $i \neq j$ and $< v_i, v_i >= 1$ for all i.

Definition 172

The nulllspace of $<, >$, denoted $V^\perp$ is the set of vectors $v \in V$ that are orthogonal to everything. (kernel, nullspace, whatever).

Example 173

Consider $V = \mathbb{R}^3$ with $< x, y >= x_1y_1 + x_3y_3$. Then $V^\perp = \{(0, a, 0) : a \in \mathbb{R}\}$.

Example 174

Let $V = \mathbb{R}^n$ where $<, >$ is identically zero. Then $V^\perp = V$.

Proposition 175

If $V = \mathbb{R}^n$ or $\mathbb{C}^n$ with $< x, y >= x^*Ay$. Then the kernel of $<, >$ is the kernel of A.

Proof. Let $y \in \ker <, > \iff < x, y >= 0 \forall x \iff x^*Ay = 0 \forall x \iff Ay = 0 \iff y \in \ker A$. □

Definition 176

$<, >$ is **nondegenerate** if $V^\perp = \{0\}$.

Proposition 177

Let $V = \mathbb{R}^n$ or $V = \mathbb{C}^n$ with $< x, y >= x^*Ay$. Then $<, >$ is nondegenerate $\iff$ A is invertible.

Proof. $<, >$ is nondegenerate $\iff \ker <, >= \{0\} \iff \ker A = \{0\} \iff A$ is invertible. □

Example 178

$<,>$ on spacetime is nondegenerate and $A = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix}$ is invertible.

Example 179

If $<,>$ is positive definite then $<,>$ is nondegenerate (and nondegenerate on every subspace).

Proof. If $v \neq 0$ then $< v, v >> 0$ so $v \notin V^\perp$. □

21 October 30, 2020

Theorem 180

Let W be a subspace of V. Then $W \cap W^\perp$ is equivalent to $W \oplus W^\perp = V$.

Proof. Suppose $W \cap W^\perp = \{0\}$. Then $W \oplus W^\perp$ is a direct sum. The only questioni is whether it is all of V. Choose a basis $(w_1, ..., w_k)$ of W, so $\dim W = k$. Define $\phi : V \to \mathbb{C}^k$, $v \mapsto (< w_1, v >, ..., < w_k, v >)$. Then $\ker \phi = W^\perp$ and $\dim V = \dim \operatorname{im} \phi + \dim \ker \phi \leq k + \dim W^\perp = \dim(W + W^\perp) \leq \dim V$. Equality must hold everywhere. $\dim(W \oplus W^\perp) + \dim V$ so $W \oplus W^\perp = V$. □

Theorem 181

V has an orthogonal basis.

Proof. By induction on $\dim V$. Choose $v \in V$. Use inductive hypothesis to get an orthogonal basis for $v^\perp$, append v to it. This was a fake proof.

Case 1: There exists $v \in V$ such that $< v, v > \neq 0$. Let $W = \text{Span}(v)$. Then $<,>$ is nondegenerate on W. So $V = W \oplus W^\perp$.

Case 2: $< v, v >= 0$ for all $v \in V$. Then for all v, w $< v + w, v + w >=< v, v > + < v, w > + < w, v > + < w, w >$. Then $0 =< v, w > + < w, v >$. If it's symmetric, then $2 < v, w >= 0$ so the form is identically zero. If instead $< v, w >$ is Hermitian then $< v, w >$ is purely imaginary for all v, w. $< v, iw >= i < v, w >$ so $< v, w >= 0$. In both cases, $<,>$ is identically zero. Use any basis. □

Corollary 182

V has an orthogonal basis $(v_1, ..., v_n)$ such that $< v_i, v_i >$ is 1,-1,0 for each i.

Corollary 183 (Matrix form of the previous corollary)

Let $A \in \mathbb{R}^{n\times n}$ be symmetric. Then $A \in \mathbb{C}^{n\times n}$ is Hermitian. Then there exists $P \in GL_n(\mathbb{C})$ such that P^*AP is a diagonal matrix with entries 1, -1, and 0. If in addition, A is positive definite, we get $P^*AP = I$ so $A = P^*P$ for some $P \in GL_n(\mathbb{C})$. "Just like in the real numbers, every number is a square, this is saying a similar thing. Everything is expressible in this way."

Example 184

Suppose (x_1, x_2) is an orthogonal basis with $< x_1, x_1 >= 3$. Take $v_1 = \frac{1}{\sqrt{3}}x_1$ so $< v_1, v_1 >= 1$. $< x_2, x_2 >= -5$. $v_2 = \frac{1}{\sqrt{5}}x_2$, $< v_2, v_2 >= -1$. Just scale it down by some number. Ideally, you'd like all pairings to be one but that isn't always the case.

If the form is positive definite, then we can get all 1s. If the form is positive semidefinite, we can get all 1s and 0s.

Theorem 185 (Sylvester's Law)

Count how many 1s, -1s, and 0s. These are invariants of the form. They are determined by V and $<,>$. The signature of $<,>= (\#1s, \# - 1s)$. We can change bases of V but these numbers stay the same.

Example 186

Suppose we take the dot product on $\mathbb{R}^n$. What's the signature of this form? It's $(n, 0)$.

Take the Lorentz form on $\mathbb{R}^4$. It has signature (3,1).

Choosing a basis of an n-dimensional $\mathbb{R}$ vector space V determines an isomorphism $V \xrightarrow{\sim} \mathbb{R}^n$ by many concepts like linear independence can be expressed without choosing a basis.

Definition 187

A Euclidean space is an $\mathbb{R}$ vector space equipped with a positive definite symmetric bilinear form. It has an orthonormal basis, hence is isomorphic to $\mathbb{R}^n$ equipped with the dot product.

Definition 188

A Hermitian space is a $\mathbb{C}$ vector space equipped with a positive definite Hermitian form. It is isomorphic to $\mathbb{C}^n$ with the standard Hermitian form.

Suppose V is nondegenerate with orthogonal basis $v_1, ..., v_n$. Given $x \in V$, $x = c_1v_1 + ... + c_nv_n$ for some scalars c_i. How do we find c_1? Pair with v_1! $< v_1, x >= c_1 < v_1, v_1 > +c_2 < v_1, v_2 > +... + c_n < v_1, v_n >$ so $c_1 = \frac{<v_1,x>}{<v_1,v_1>}$

Definition 189 (Orthogonal Projection)

Suppose $W \leq V$ and $<,>$ on nondegenerate on W.Then $V = W \oplus W^\perp$. Each v is $w + u$. Orthogonal projection $\pi : V \to W$, $v \mapsto w$. Formula for π. Suppose $w_1, ..., w_k$ is a basis for W. Let $v \in V$. Then $v = c_1w_1+...+C_nw_k+u$. where $c_i = \frac{<w_i,v>}{<w_i,w_i>}$

22 November 2, 2020

Last time we went over the projection formula.

Definition 190 (Gram-Schmidt Algorithm)
The gram-schmidt is an algorithm that takes as input a Euclidean space V, a positive definite symmetric or Hermitian form, and a basis $(v_1, ..., v_n)$ of V. The output is an orthonormal basis $(w_1, ..., w_n)$ of V. Let $V_1 = \text{Span}(v_1)$ and $V_2 = \text{Span}(v_1, v_2)$.

Step 1. $w_1 = \frac{1}{|v_1|} v_1$. Then w_1 is an orthonormal for V_1.

Step 2. $t_2 = V_1^\perp$ component of $v_2 = v_2 - (\text{projection of} v_2 \text{onto} V_1) = v_2 - < w_1, v_2 > w_1$. Then $t_2 \perp w_1$. Define $w_2 = \frac{1}{|t_2|} t_2$ and perform the same steps.

Step 3. $t_3 = V_2^\perp$ component of $v_3 = v_3 - (< w_1, v_3 > w_1 + < w_2, v_3 > w_2)$. Then $t_3 \perp w_1, w_2$. Let $w_3 = \frac{1}{t_3} t_3$.

. Let V and W be Hermitian spaces and $<, >_V$ and $<, >_w$ positive definite Hermitian forms.

Proposition 191
For each $\mathbb{C}$-linear transformation $T : V \to W$, there exists a unique linear transformation $T^* : W \to V$ such that $< Tv, w >_W = < v, T^* w >_V$.

Proof. Choose an orthonormal basis for V and W to assume $V = \mathbb{C}^n$ with standard Hermitian form $< x, y >= x^* y$ and let $W = \mathbb{C}^m$ with standard Hermitian form $< x, y >= x^* y$. Then T is given by some $A \in \mathbb{C}^{m \times n}$. We are looking for $B \in \mathbb{C}^{n \times m}$ such that $(Av)^* w = v^* B w$ for all $v \in V$ and $w \in W$. Byt then $B = A^*$ once we evaluate this at $v = e_i$ and $w = e_j$. □

From now on, $T : V \to V$ so $T^* : V \to V$.

Definition 192 (Hermitian linear operator)
T is **Hermitian** if and only if $T^* = T \iff < Tv, w >=< v, Tw >$ for all $v, w \in V$.

Definition 193 (Unitary linear operator)
T is unitary if and only if $T * T = I \iff < Tv, Tw >=< v, w >$

Definition 194 (Normal linear operator)
T is normal if and only if $T^* T = TT^* \iff < Tv, Tw >=< T^* v, T^* w >$

Same definitions follow for $A \in \mathbb{C}^{n \times n}$. Hermitian implies normal and unitary implies normal but the converse is not true. There's a slight distinction between what linear operators are and what matrices are.

Proposition 195
If $TW \leq W$ then $T^* W^\perp \leq W^\perp$.

Proof. Suppose that $u \in W^\perp$. Is $T^* u \in W^\perp$. Well, if $w \in W$, then $< w, T^* u >=< Tw, u >= 0$ by hypothesis. □

Proposition 196

Let T be normal. If $Tv = \lambda v$ then $T^*v = \overline{\lambda} v$.

Proof. First, if $\lambda = 0$, then $Tv = 0$. Then $< T^*v, T^*v > = < Tv, Tv > = 0$ so $T^* = 0$. Now, if λ is an arbitrary eigenvector, then define $S = T - \lambda I$. Then $S^* = T^* - \overline{\lambda} I$ so $SS^* = S^*S$ so S is normal. $Sv = Tv - \lambda v = 0$. By the $\lambda = 0$ case applied to S, we get that $S^*v = 0$ so $T^*v = \overline{\lambda} v$. □

Theorem 197 (Spectral Theorem)

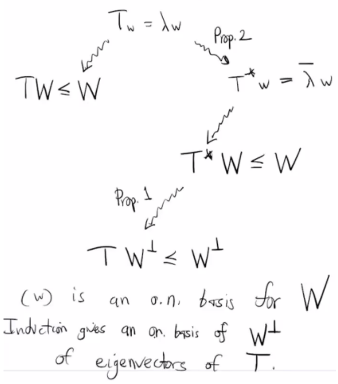
Let V be a Hermitian space. Complex vector space with a positive definite Hermitian form. Let T be normal.

Then V has an orthonormal basis consisting of eigenvectors of T.

Theorem 198 (Matrix Version of the Spectral Theorem)

Let $A \in \mathbb{C}^{n \times n}$ be normal. Then A is diagonalizable. More precisely, there exists a unitary P such that $P^{-1}AP$ is diagonal. This is a basechange matrix from the standard basis to some other on basis of $\mathbb{C}^n$.

Proof. We perform an induction on $\dim V$. Let w be an eigenvector of T. WLOG $|w| = 1$. Let $W = \text{Span}(w)$. Then $V = W \oplus W^\perp$. Then W goes to W under T and $W^\perp$ also goes to itself under T.



(w) is an o.n. basis for W

Induction gives an o.n. basis of $W^\perp$ of eigenvectors of T.

1122020.PNG

□

23 November 4, 2020

Last time we talked about the spectral theorem.

Definition 199

A quadratic form is a homogeneous quadratic polynomial on n variables. This equates to $\sum a_{ii}x_i^2 + 2\sum_{i<j} a_{ij}x_ix_j = \sum = x^tAx$ where A is symmetric.

Performing orthogonal coordinate changes, $x = Px$ where P is in O_n. This changes A to P^tAP. By the spectral theorem for real symmetric matrices, we can make A a diagonal matrix with entries in $\mathbb{R}$. This is equal to $\lambda_1 x_1^2 + \ldots + \lambda_n x_n^2$.

23.1 Plane curves of degree 2

$a_11x_1^2 + 2a_{12}x_1x_2 + a_22X_2^2 + B_1x_1 + b_2x_2 + c = 0 \iff x^tAx + Bx + c = 0.$

Theorem 200

Every possibility is congruent to one of the examples (up to some isometry).

Proof. Given $x^tAx + Bx + c = 0$. WLOG $A = \begin{pmatrix} a & \\ & b \end{pmatrix}$. Then we get $ax_1^2 + bx_2^2 + b_1x_1 + b_2x_2 + c = 0$

Case 1: $a, b \neq 0$. Complete the square. Substitute $x_1 = x_1' - r$ for some $r \in \mathbb{R}$ to eliminate the b_1x_1 term. $r = \frac{b_1}{2a}$ works. Same for x_2. Get $ax_1^2 + bx_2^2 - c = 0$.

Case 1a: $c \neq 0$. Divide equation by c. Get an ellipse or hyperbola

Case 1b: $c = 0$. Get a point or two intersecting lines.

Case 2: $a \neq 0$, $b = 0$. "Left as an exercise to the reader."

□

23.2 Quadric surfaces on on 3d space

A similar analysis leads to $q(x_1, x_2, x_3) = 1$, $x_3 = Q(x_1, x_2)$, and some degenerate cases.

Now, look at skew-symmetric forms. Let F be a field of characteristic not 2. V an F-vector space. $<,>: V \times V \to F$ a bilinear form.

Proposition 201

$< x, y >= - < y, x >$ for all $x, y \iff < x, x >= 0$ for all x.

Proof. Left to right is easy because $< x, x >= - < x, x >$. This is where we use that the characteristic of the field is not 2.

Right to Left. If $< x, x >= 0$ for all x then $0 =< x + y, x + y >=< x, x > + < x, y > + < y, x > + < y, y >$ $\implies < x, y >= - < y, x >$ □

24 November 6, 2020

F is a field, V is an F-vector space. $<,>: V \times V \to F$ is a bilinear form. If the characteristic of F is not 2 (nontrivial field), then the following conditions are equivalent: $< x, y >= - < y, x >$ for all $x, y \in V$, $< x, x >= 0$ for all $x \in V$. If the characteristic of F is 2, the alternating condition is more restrictive, and it is the better notion.

Example 202

On F^2, the determinant form is $< \begin{pmatrix} x_1 \\ x_2 \end{pmatrix}, \begin{pmatrix} y_1 \\ y_2 \end{pmatrix} >= \det \begin{pmatrix} x_1 & y_1 \\ x_2 & y_2 \end{pmatrix} = \mathbf{x}^t \begin{pmatrix} & 1 \\ -1 & \end{pmatrix} \mathbf{y} = 1$ is alternating.

Recall that a real vector space V with a symmetric bilinear form $<,>$ has an orthogonal basis. (Same for a complex vector space with a Hermitian form.) If in addition $<,>$ is positive definite, then $<,>$ has an orthonormal basis.

Alternating always implies symmetric.

Theorem 203

Let $<,>$ be nondegenerate, alternating form on V. A nondegenerate alternating form is also called symplectic. Then there exists a basis $(v_1, w_1, v_2, w_2, ..., v_n, w_n)$ such that $< v_i, w_i >= 1$, $< w_i, v_i >= -1$ and all other pairings of basis vectors give 0.

Remark 204. *Put the images that I saved about conic sections into the previous day's section.*

Theorem 205 (Matrix form of the previous theorem)

Let $A \in GL_m(F)$. Then $A^t = -A$ and zeros on diagonal. Then there exists $p \in GL_n(F)$ such that P^tAP is a matrix with blocks of the form $\begin{pmatrix} & 1 \\ -1 & \end{pmatrix}$ along the diagonal and zeros everywhere else.

Proof. Induction on $\dim v$. If $\dim V = 0$, we're done. Otherwise choose v_1, w_1 with $< v_1, w_1 >\neq 0$. These exist since $<,>$ is nonnegative. Without loss of generality, let $< v_1, w_1 >= 1$ (scale w_1). Since $< v_1, v_1 >= 0$ so $w_1 \notin \text{Span}(v_1)$. Let $W = \text{Span}(v_1, w_1)$ and $<,>$ is nondegenerate on W since its matrix is $\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$, which is invertible. So, just as for symmetric forms, $V = W \oplus W^\perp$. The basis of W is (v_1, w_1) and the basis of $W^\perp$ is $(v_1, w_2, ..., v_n, w_n)$ of $W^\perp$ from inductive hypothesis. □

Also, skew-Hermitian forms. We're on to the LAST CHAPTER.

Definition 206

A **linear group** is a subgroup of $GL_n(\mathbb{R})$ or $GL_n(\mathbb{C})$ for some n.

Example 207

$GL_n = GL_n(\mathbb{R})$ and $O_n = \{P \in GL_n(\mathbb{R}) : P^tP = I\}$. What do its elements preserve? Matrices of O_n preserve dot product, length. Define $I_{3,1} = \begin{pmatrix} 1 & & & \\ & 1 & & \\ & & 1 & \\ & & & -1 \end{pmatrix}$. The Lorentz group is $O_{3,1} = \{P \in GL_n(\mathbb{R}) : P^tI_{3,1}P = I_{3,1}\}$. You get one of these gruops for every signature (p, q). The unitary group $U_n = \{P \in GL_n(\mathbb{C}) : P^*P = I\}$. The symplectic group $SP_{2n} = \{P \in GL_n(\mathbb{R}) : P^tSP = S$ where $S = \begin{pmatrix} 0 & I \\ I & 1 \end{pmatrix}$. "Things that preserve the standard symplectic form. Special linear group $SL_n = \{P \in GL_n(\mathbb{R}) : \det P = 1\}$ "preserves volume, up to a sign". Special orthogonal group $SO_n = O_n \cap SL_n$. You get a bunch of other groups, special lorentz group, special unitary, which are just $SL_n \cap O_{3,1}$ and $SL_n \cap U_n$ respectively. Note that $SSp_{2n} \cap SL_n = SSp_{2n}$.

Example 208 (The General Orthogonal Group)

$GO_n = \{P \in GL_n(\mathbb{R}) : \exists \lambda \in \mathbb{R}^\times s.t. P^tP = \lambda I$. Again, we get a series of other matrices $GU_n = \{P \in GL_n(\mathbb{C}) : \exists \lambda \in \mathbb{R}^\times s.t. P^*P = \lambda I\}$ and $GSp_{2n} = \{P \in GL_n(\mathbb{R}) : \exists \lambda \in \mathbb{R}^\times s.t. P^tSP = \lambda S\}$. Again, we can get an even wider variety of linear groups by looking at the matrices over the complex numbers.

Each of these groups has a geometry.

Example 209

$GL_n(\mathbb{R})$ is an open subset of $\mathbb{R}^{n\times n} \cong \mathbb{R}^{n^2}$ since it's the inverse image under $\det : \mathbb{R}^{n\times n} \to \mathbb{R}$ of the open subset $\mathbb{R}^\times \subset \mathbb{R}$. The inverse image under a continuous map of an open subset is open and we know that the determinant map is continuous since it's a polynomial. We'll say therefore that $\dim GL_n(\mathbb{R}) = n^2$. We can pick almost any n^2 elements in the matrix (with some constraints).

Example 210

The following are isomorphic: $\mathbb{R}/\mathbb{Z}$, $\mathbb{R}/2\pi\mathbb{Z}$, $U_1 = \{z \in \mathbb{C} : z\bar{z} = 1\}, SO_2$. Geomtrically, the're all a circle.

Example 211

SU_2 is homeomorphic to a 3 dimensional sphere S^3. There are continuous maps $SU_2 \to S^3$ and $S^3 \to SU_2$ whose composition in either order is the identity map.

25 November 8, 2020

Proposition 212

$SU_2 = \{\begin{pmatrix} a & b \\ -\bar{b} & \bar{a} \end{pmatrix} : a, b \in \mathbb{C}, \bar{a}a + \bar{b}b = 1\}$.

Proof. Let $P \in \mathbb{C}^{2\times 2}$. Then $P \in SU_2 \iff P^*P = I$ and $\det P = 1 \iff P^* = P^{-1}$ and $ad - bc = 1 \iff \begin{pmatrix} \bar{a} & \bar{c} \\ \bar{b} & \bar{d} \end{pmatrix} = \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$ and $ad - bc = 1 \iff d = \bar{a}, c = \bar{b}$ □

Corollary 213

$SU_2 = \left\{ x_0 \begin{pmatrix} 1 & \\ & 1 \end{pmatrix} + x_1 \begin{pmatrix} i & \\ & -i \end{pmatrix} + x_2 \begin{pmatrix} & 1 \\ -1 & \end{pmatrix} + x_3 \begin{pmatrix} & i \\ i & \end{pmatrix} : x_0, ..., x_3 \in \mathbb{R}, x_0^2 + x_2^2 + x_3^2 = 1 \right\}$ is the unit 3-sphere in the quaternion algebra. The quaternion algebra H satisfies the above rules but no restriction on $x_0^2 + x_1^2 + x_2^2 + x_3^2$.

Fact 214

H satisfies all the axioms of a field except that multiplication is not commutative. $i^2 = j^2 = k^2 = -1$, $ij = k, ji = -k$, ... We can represent this as a chain $i \to j \to k \to i$.

Definition 215

$\mathbb{Q}_8$ is a subgroup of SU_2 called the quaternion group of order 8.

Fact 216

The eigenvalues of P are $\{\lambda, \overline{\lambda}\}$ for some $\lambda \in \mathbb{C}$ with $|\lambda| = 1$

Proof. Since its unitary, |eigenvalues|=1, the product of the eigenvalues is $\det P = 1$ □

Fact 217

The characteristic polynomial of P is $t^2 - 2x_0 t + 1$ with $-1 \leq x_0 \leq 1$

Proof. $\operatorname{tr} P = 2x_0$ and $\det P = 1$ □

Fact 218

P is conjugate in SU_2 to $\begin{pmatrix} \lambda & \\ & \bar{\lambda} \end{pmatrix}$

Proof. P is unitary so the spectral theorem says there exists $Q \in U_2$ such that $Q^{-1}PQ = \begin{pmatrix} \lambda & \\ & \bar{\lambda} \end{pmatrix}$. Replace Q by α where $\det(\alpha Q) = 1 = \alpha^2 \det(Q)$. □

Fact 219

P and P' are conjugate in SU_2 if and only if $\operatorname{tr} P = \operatorname{tr} P' \iff P, P'$ have the same x_0-value

The center of SU_2 is $\{\pm I\}$.

If $W \leq$ H is a 2 dimensional subspace containing 1, choose an orthonormal basis 1, v. Then $v \in E$ so $v^2 = -1$. $W = \{a1 + bv : a, b \in \mathbb{R}\}$ is a copy of $\mathbb{C}$. You get all of these copies of the complex numbers. What happens when we intersect this with SU_2. $W \cap SU_2$ is teh unit circle in that $\mathbb{C}$.

26 November 13, 2020

Let $V = \operatorname{Span}(\mathbf{i}, \mathbf{j}, \mathbf{k}) \cong \mathbb{R}^3$. If $u, v \in V$ then $uv = (u_1 i + u_2 j + u_3 k)(v_1 i + v_2 j + v_3 k) = (-u \cdot v) + (u \times v)$ so $u \cdot v = -\frac{1}{2}\operatorname{tr}(uv)$. To make sense of this, the $(-u \cdot v)$ part is the real part and the $(u \times v)$ part is the $\mathbf{i}, \mathbf{j}, \mathbf{k}$ part, (nonreal part). For $P \in SU_2$, define "conjugation by P" by $x \mapsto PxP^{-1}$. Elements of the quaternions are just matrices. This map preserves trace so it restricts to a map $\gamma_p : V \to V$, $x \mapsto PxP^{-1}$. Geometrically what is this map?

Theorem 220

$\gamma_p \in SO_3$. More specifically, I can tell you which rotation it is. If $P = \cos\theta + \sin\theta v$ where $v \in E$, then γ_p is a rotation by 2θ about the pole v.

$SU_2 \to SO_3$ is a surjective homomorphism with kernel $\{\pm I\}$ under the map $P \mapsto \gamma_p$.

Proof. Since v is conjugate to $\mathbf{i}$ (both are in the conjugacy class E) by symmetry, we can reduce to the case where $v = \mathbf{i}$ so $P = \cos\theta + \sin\theta\mathbf{i}$. Then $\gamma_p(\mathbf{i}) = P\mathbf{i}P^{-1} = \mathbf{i}$, $\gamma_p(\mathbf{j}) = P\mathbf{j}P^{-1}\cos(2\theta)\mathbf{j} + \sin(2\theta)\mathbf{k}$, $\gamma_p(\mathbf{k}) = PkP^{-1} = -\sin(2\theta)\mathbf{j} + \cos(2\theta)\mathbf{k}$

Every element of SO_3 is a rotation of the previous type so $SU_2 \to SO_3$ is surjective. Also $\gamma_p = I \iff 2\theta \in 2\pi\mathbb{Z} \iff P = \pm I$. □

Corollary 221

$SO_3 \cong \{\text{cosets of } \{\pm I\} \text{ in } SU_2 \cong S^3/\sim$. This is the projective 3-space.

26.1 Differential Equations and the Matrix Exponential

Fix $a \in \mathbb{C}$. The function $x(t) = e^{at}$ for all $t \in \mathbb{R}$ is the unique solution to

$$\frac{dx}{dt} = ax$$
$$x(0) = 1$$

Here are two ways to construct this function:

1. Invoke the general existence and uniqueness theorem for linear ordinary differential equations
2. Proe that $1 + at + \frac{(at)^2}{2!} + \frac{(at)^3}{e!}$ converges to a differentiable function satisfying the above equations.

Example 222

$a = i$. The $e^{it} = \cos t + i \sin t$ because the right hand side satisfies the differential equation.

Definition 223

Let $A \in \mathbb{C}^{n\times n}$. Then $e^A = I + A + \frac{A^2}{2!} + \frac{A^3}{3!} + \dots$. Then e^{tA} is defined. We need to check that this converges for every $t \in \mathbb{R}$, it is differentiable, $\frac{d}{dt} e^{tA} = Ae^{tA}$, $e^0 = I$.

In general, suppose $u_1(t), u_2(t), \dots$ are functions $I \to \mathbb{R}$. Define $||A|| = \max_{i,j} a_{ij}$. Wishful thinking:

1. $$\sum_k u_k(t)$$
   converges.
2. If each u_k is continuous then $u(t) = \sum_k u_k(t)$ is continuous
3. If each u_k is differentiable then u is differentiable and $u'(t) = \sum_k u_k'(t)$.

Then use the Weierstrass M-test here.

27 November 16, 2020

Some theorems from last time The Weierstrass M-test. $\sum_k u_k(t)$ converges uniformly to a function $u : I \to V$ if there exists real numbers M_k such that $|u_k(t)| \leq M_k$ for all $t \in I$ and $\sum M_k < \infty$

If each u_k is continuous and $\sum u_k(t)$ converges uniformly then $\sum u_k(t)$ is continuous.

If each u_k is differentiable and $\sum u_k(t)$ converges and $\sum u_k'(t)$ converges uniformly then $\sum u_k(t)$ is differentiable and its derivative is $\sum u_k'(t)$.

Today, we're going to talk about the matrix exponential function e^{tA} for $A \in \mathbb{C}^{n \times n}$. For $A \in \mathbb{C}^{n \times n}$, define $||A|| = \max_{i,j} |a_{ij}|$. By induction on k, we have $||A^k|| \leq n^{k-1}||A||^k$. Let $I = (-r, r)$. Let $V = \mathbb{C}^{n \times n}$. To define e^{tA}, we want to sum $u_k(t) = \frac{(tA)^k}{k!}$ which has $u_k'(t) == \frac{t^{k-1}A^k}{(k-1)!}$. These are bounded on $(-r, r)$ by $M_k = \frac{r^k n^{k-1}||A||^k}{k!}$ and $N_k = \frac{r^{k-1}n^{k-1}||A||^k}{(k-1)!}$. Then $\sum u_k(t)$ converges uniformly on $(-r, r)$ since $\sum M_k < \infty$ by the ratio test and also $\sum u_k'(t)$ converges uniformly on $(-r, r)$ since $\sum N_k < \infty$ also by the ratio test.

We conclude that e^{tA} converges uniformly on $(-r, r)$ and $\frac{d}{dt}e^{tA} = Ae^{tA}$ at least for $t \in (-r, r)$.

Some properties of e^{tA}

1. $\frac{d}{dt}e^{tA} = Ae^{tA}$
2. $e^0 = I$
3. If $AB = BA$ then $e^A e^B = e^{A+B}$
4. e^A is invertible with inverse e^{-A}
5. If $B = PAP^{-1}$ then $e^B = Pe^A P^{-1}$
6. If $A = \begin{pmatrix} \lambda_1 & & \\ & \dots & \\ & & \lambda_n \end{pmatrix}$ then $e^A = A = \begin{pmatrix} e_1^{\lambda} & & \\ & \dots & \\ & & e_n^{\lambda} \end{pmatrix}$

Proof of the second. If $AB = BA$ then the binomial theorem applies $(A + B)^m = \sum_{k+l=m} \frac{m!}{k!l!} A^k B^l$ so $e^{A+B} = \sum_{m \geq 0} \frac{(A+B)^m}{m!} = \sum_{m \geq 0} \sum_{k+l=m} \frac{1}{m!} \frac{m!}{k!l!} A^k B^l = \sum_{k \geq 0} \sum_{l \geq 0} \frac{A^k}{k!} \frac{B^l}{l!} = e^A e^B$. Rearranging terms is ok because everything converges absolutely. □

Corollary 224

For each $A \in \mathbb{C}^{n \times n}$ $\mathbb{R} \to GL_n(\mathbb{C})$, $t \mapsto e^{tA}$ is a homomorphism.

Proof. $e^{(t+u)A} = e^{tA+uA} = e^{tA}e^{uA}$ since tA and uA commute. □

Definition 225 (One-parameter group)

A one-parameter group in $GL_n(\mathbb{C})$ is a differentiable homomorphism from $\mathbb{R}$ to $GL_n(\mathbb{C})$.

Challenge: continuous homomorphisms from $\mathbb{R}$ to $GL_n(\mathbb{C})$ are automatically differentiable.

Proposition 226

There is a bijection $\mathbb{C}^{n \times n} \to$ one-parameter groups in $GL_n(\mathbb{C})$, $A \mapsto (t \mapsto e^{tA}$, $\phi \mapsto \phi'(0)$.

Proof. We already showed that for each A, $t \mapsto e^{tA}$ is a one-parameter group. Suppose that $\phi : \mathbb{R} \to GL_n(\mathbb{C})$ is any one-parameter group. Let $A = \phi'(0)$. Let $A = \phi'(0)$. We want to show that $\phi(t) = e^{tA}$ for all $t \in \mathbb{R}$. We'll do this by showing that $\phi(t)$ satisfies the same differential equation and initial conditions as e^{tA}. We know that $\phi(s + t) = \phi(s)\phi(t)$. Take the derivative of this w.r.t. s. We get $\phi'(s + t) = \phi'(s)\phi(t)$. Evaluate at $s = 0$ to get $\phi'(t) = A\phi(t)$. Also, $\phi(0) = A$. □

Example 227

Let $A = \mathbf{i} = \begin{pmatrix} i & \\ & -i \end{pmatrix}$. Then $e^{tA} = \begin{pmatrix} e^{it} & \\ & e^{-it} \end{pmatrix} \in SU_2$. This is going to be one of the longitudes.

For which $A \in \mathbb{C}^{n\times n}$ does the one-parameter group $t \mapsto e^{tA}$ land in $GL_n(\mathbb{R})$? We claim that $A \in \mathbb{R}^{n\times n} \iff e^{tA} \in GL_n(\mathbb{R})$ for all $t \in \mathbb{R}$.

Proof. By definition of e^{tA}, $e^{tA} \in GL_n(\mathbb{R})$ when $A \in \mathbb{R}^{n\times n}$. Conversely, if $e^{tA} \in GL_n(\mathbb{R})$ for all t, taking the derivative at $t = 0$ gives $A \in \mathbb{R}$. □

For which $A \in GL_n(\mathbb{C})$ is $e^{tA} \in U_n$ for all $t \in \mathbb{R}$? We claim that this is true if and only if A is skew-Hermitian. In general, $(e^A)^* = e^{A^*} = e^{-A} = (e^A)^{-1}$. Conversely, if $e^{tA} \in U_n$ for all $t \in \mathbb{R}$ then $(e^{tA})^* = (e^{tA})^{-1} \implies e^{tA^*} = e^{-tA} \implies A^* = -A$ after taking the derivative and evaluating at $t = 0$.

28 November 18, 2020

For which A is e^{tA} in O_n for all $t \in \mathbb{R}$? Since $O_n = GL_n(\mathbb{R}) \cap U_n$, we need $A \in \mathbb{R}^{n\times n}$ and $A^* = -A$ or $A^t = -A$. This is equivalent to A being a skew-symmetric matrix.

Lemma 228

For any $A \in \mathbb{C}^{n\times n}$, $\det e^A = e^{\operatorname{tr} A}$.

Proof. Conjugating A by P conjugates e^A by P so it doesn't change e^A. It also doesn't change $\operatorname{tr}(A)$. Therefore, WLOG, let A be in Jordan canonical form. Then

$$e^A = \begin{pmatrix} e^{\lambda_1} & * & \\ & \cdots & \\ & & e^{\lambda_n} \end{pmatrix}$$

so $\det e^A = e^{\operatorname{tr} A}$ □

For which $A \in \mathbb{R}^{n\times n}$ is $e^{tA} \in SL_n(\mathbb{R})$ for all $t \in \mathbb{R}$? The A such that $\operatorname{tr} A = 0$.

Proof. For $A \in \mathbb{R}^{n\times n}$, $\operatorname{tr} tA = 0$ for all $t \in \mathbb{R}$ so $e^{\operatorname{tr} tA} = 1$ so $e^{tA} \in SL_n(\mathbb{R})$. □

Definition 229

A is a d-dimensional manifold is a topologicla space M such that every point $m \in M$ has an open neighborhood in M that is homeomorphic to an open subset of $\mathbb{R}^d$.

Example 230

A circle is a 1-dimensional manifold.

When can you solve for y as a function of x in the equation $ax + by + c = 0$? That is, when does this equation describe the graph of a function. All we need is that $b \neq 0$. In other words, we need $\frac{\partial f}{\partial y} \neq 0$

Theorem 231 (Implicit Function Theorem)
Suppose we are given the following:

1. A system of equations $f(x, y) = 0$ where $x = (x_1, ..., x_m)$ and $y = (y_1, ..., y_r)$ and $f = (f_1, ..., f_r)$ and $f : U \to \mathbb{R}^r$ is a C^1 function.
2. A point $u \in Z(f)$ ($Z(f)$ is the set of solutions to $f = 0$).

If $\frac{\partial f}{\partial y}(u)$ is invertible where $((\frac{\partial f_i}{\partial y_j})(u)) \in \mathbb{R}^{n\times n}$ then $Z(f)$ is a graph near u. This is equivalent to saying that there is an open neighborhood U' of $u \in U$ such that $Z(f) \cap U'$ is a graph of some g for some C^1 function $g : V \to \mathbb{R}^r$, $V \subseteq \mathbb{R}^m$.

Example 232
Let's prove that $S^2 = Z(x^2 + y^2 + z^2 - 1)$ in $\mathbb{R}^3$ is a manifold. We need to check each point $u \in S^2$. At u, not all of x, y, z can be 0. WLOG $z \neq 0$ at u. Try to solve for z:$\frac{\partial f}{\partial z} = 2z$ is nonzero at u, so the implicit function theorem says some neighborhood of u in S^2 is the graph of a function $g(x, y)$. Secretly, $g(x, y) = \sqrt{1 - x^2 - y^2}$ or $-\sqrt{1 - x^2 - y^2}$. We conclude that S^2 is a manifold

29 November 20, 2020

Theorem 233
Let G be a closed subgroup of $GL_n(\mathbb{R})$. Then G is a manifold. In fact, G is $Z(f)$ for some function f and is satisfies the condition of the implicit function theorem at each point.

Definition 234
A **differentiable path** in $G \leq GL_n(\mathbb{R})$ as above is a differentiable function $\phi : \mathcal{I} \to G$ where $\mathcal{I}$ is an open interval. If $0 \in \mathcal{I}$, we get the velocity vector $\phi'(0) \in \mathbb{R}^{n\times n}$ which is tangent to the path, hence tangent to G.

Definition 235 (The Lie Algebra of G)
Here are three ways to describe the Lie Algebra $Lie(G)$.

1. It's the tangent space to G at I. It's the set $\{\phi'(0) : \phi$ is a differentiable path in $G\}$.
2. It's $\{A \in \mathbb{R}^{n\times n}$: the one-parameter group e^{tA} is contained in G.
3. If G is defined by a system of polynomial equations $f = 0$ satisfying the implicit function theorem, the lie algebra is $\{A \in \mathbb{R}^{n\times n} : I + \varepsilon A$ satisfies the system of equations where $\varepsilon^2 = 0$.

Proof that 2. is equivalent to 1. Suppose $A \in S$ where S is the set from 2. Then the one-parameter group $\phi(t) = e^{tA}$ is centered in G. Then $\phi'(0) \in T$ where T is the set from 1. □

Here's an algebraic way to take a derivative. Work in $\mathbb{R}[\varepsilon]$ where $\varepsilon^2 = 0$. If $f(x) = x^2 + 5x$, then $f(x + \varepsilon) = (x + \varepsilon)^2 + 5(x + \varepsilon) = (x^2 + 5x) + (2x + 5)\varepsilon$. We can then say that f' is the ε-component of f.

Example 236

Consider O_n. Then $LieO_n = \{A \in \mathbb{R}^{n\times n} : (I+\varepsilon A)^t(I+\varepsilon A) = I\}$. This is equivalent to $I + \varepsilon A^t + \varepsilon A = I$ or $A^t + A = 0$.

Example 237

Consider SL_2. The equation that defines SL_2 is $\det = 1$. Thus TFAE, $A \in LieSL_2$. Then $\det(I+\varepsilon A) = 1$ so $\operatorname{tr} A = 0$.

Some properties of $LieG$:

- $LieG$ is a vector space.
- If $A, B \in LieG$, then $AB - BA \in LieG$.

Proof. Use $\mathbb{R}[\varepsilon, \varepsilon']$ with $\varepsilon^2 = (\varepsilon')^2 = 0$. If $A, B \in LieG$ then $I + \varepsilon A$, $I + \varepsilon' B$ satisfy the equations of G and then so does their commutator $(I+\varepsilon A)(I+\varepsilon' B)(I+\varepsilon A)^{-1}(I+\varepsilon' B)^{-1} = I + (AB - BA)\varepsilon\varepsilon'$. □

Definition 238 (The Bracket)

Let $A, B \in LieG$. Then $[A, B] = AB - BA$. This measures noncommutativity in some infinitesimal sense.

30 November 30, 2020

Let G be a closed subgroup of $GL_n(\mathbb{R})$ or $GL_n(\mathbb{C})$. Then G is a manifold. It is the zero of some function f satisfying the conditions of the implicit function theorem at each point. The **Lie algebra** can be described in three ways:

1. The tangent space to G at I. $LieG = \{\phi'(0) : \phi \text{ is a differentiable path in } G \text{ with } \phi(0) = I\}$
2. $\{A \in \mathbb{R}^{n\times n} : \text{ the one-parameter group } e^{tA} \text{ is contained in } G\}$
3. $\{A \in \mathbb{R}^{n\times n} : f(I+\varepsilon A) = 0\}$ assuming that f is a tuple of polynomials in the matrix entries. Here we're working in $GL_n(\mathbb{R})[\varepsilon]$ where $\varepsilon^2 = 0$.

Some properties of $LieG$ are that $LieG$ is a vector space, the dimension of $LieG$ is $\dim G$, if $A, B \in LieG$ then $AB - BA \in LieG$.

Definition 239

The **bracket** of two matrices is $[A, B] = AB - BA$.

If G is abelian then all matrices $A, B \in LieG$ satisfy $[A, B] = 0$.

Definition 240

A **Lie algebra** is a vector space V equipped with a binary operation $[,] : V \times V \to V$ such that

- bilinearity
- $[A, A] = 0$ ($\iff$ $[B, A] = -[A, B]$)
- The Jacobi Identity $[A, [B, C]] + [B, [C, A]] + [C, [A, B]] = 0$ for all A, B, C.

Given $g \in G$, the translation map $G \to G$, $x \mapsto gx$. This map is usually not a homomorphism, but it is a homeomorphism and it sends 1 to g.

Example 241

By definition, G is a d-dimensional manifold if and only if every $g \in G$ has an open neighborhood homeomorphic to an open subset of $\mathbb{R}^d$. By homogeneity, it's enough to check this for $g = 1$.

Fact 242

Any closed subgroup $G \subseteq GL_n(\mathbb{R})$ is a manifold of the same dimension as its Lie algebra $\mathfrak{g}$.

Idea of Proof. $e : \mathbb{R}^{n \times n} \to GL_n(\mathbb{R})$, $A \mapsto e^A$. It maps small neighbborhood of 0 to small neighborhood of I under a homeomorphism. It restricts to a differentiable map $\mathfrak{g} \to G$, $A \mapsto e^A$. It sends small neiborhoods of 0 in $\mathfrak{g}$ to small neighborhoods of I in G. □

Proposition 243

If H is an open subgroup of a linear group G then it is closed in G.

Proof. G consists of H and all its cosets. H is open. G is the disjoint union of all the cosets, all of which have to be open. Take the union of all cosets of H except for itself. This is open. Take the set difference of this union and G. This is closed because it's the complement of an open set and it is equal to H. Thus H is closed. Note that the converse doesn't work since the infinite union of closed sets isn't necessarily closed. The converse works if we can also guarantee that $[G : H]$ is finite. □

Example 244

Let $G = \mathbb{R}^\times$ and $H = \mathbb{R}_{>0}$

Definition 245

G is **path connected** if for every $x, y \in G$ there exists a continuous map $\phi : [0, 1] \to G$ with $\phi(0) = x$, $\phi(1) = y$.

Fact 246

If G is path connected, then G is not a disjoing union of two nonempty open subsets.

Proposition 247

Let G be a path-connected linear group. Any nonempty open subset U of G generates the whole group G.

Proof. Let H be the subgroup generated by U. We need to prove $H = G$. Choose $g \in U$. Then $g^{-1}U$ is an open neighborhood of I and is contained in H. For each $h \in H$, $hg^{-1}U$ is an open neighborhood of h in G and is contained in H. Thus H is open. G is a disjoint union of open cosets. Since G is path connected, all cosets of H must be the same thing, or equivalently $H = G$. □

Remember that G is simple if and only if $G \neq \{1\}$ and the only normal subgroup are itself and $\{1\}$.

Theorem 248

Is SU_2 is not simple because the center is normal. Its only normal subgroups are $\{I\}$ and $\{\pm I\}$.

Proof. Let N be a normal subgroup of SU_2. Suppose that N is not $\{I\}$ or $\{\pm I\}$, so N contains some $g \neq I$. Since N is normal, N contains the conjugacy class of g, a lattitude Λ. Then $I \in g^{-1}\Lambda \subseteq N$. N contains all these lattitudes too so N contains an open neighborhood of I. By the previous proposition, $N = SU_2$. □

31 December 2, 2020

Corollary 249

SO_3 is simple.

Proof. We have $\gamma : SU_2 \to SO_3$ with kernel $\{\pm I\}$. The correspondence theorem says there is a bijection between the normal subgroups of SU_2 and the normal subgroups of SO_3. $\{\pm I\}$ is the only normal subgroup in SU_2 and it gets mapped to the trivial group in SO_3. □

Theorem 250

Let F be a field with $|F| \geq 4$. Then the only normal subgroups of $SL_2(F)$ are $\{I\}$, $\{\pm\}$, and $SL_2(F)$. If the characteristic of F is 2, then $-1 = 1$, $-I = I$, and $\{\pm I\} = \{I\}$. We'll prove it for $|F|$.

The square root lemma: For $a \in F$, the equation $x^2 = a$ has less than or equal to 2 solutions. If $|F| > 5$ then there exists $r \in F$ such that $r^2 \neq \{0, 1, -1\}$.

Suppose N is a normal subgroup of $SL_2(F)$ and N is not conatined in $\{\pm I\}$. We need to show that $N = SL_2(F)$. First, N contains come matrix B with distinct eigenvalues. Choose $N - \{\pm I\}$. Then A is not a scalar times I. Choose v_1 such that v_1 is not an eigenvector of A. Let $v_2 = Av_1$ so (v_1, v_2) is a basis of F^2. Choose $r \in F$ such that $r^2 \notin \{0, 1, -1, \}$. Let $P \in GL_2$ be such that $Pv_1 = rv_1$ and $Pv_2 = r^{-1}v_2$. Then the determinant of P is 1 so $P \in SL_2(F)$. Then PAP^{-1}, $APA^{-1}P^{-1} \in N$. Call $B = APA^{-1}P^{-1}$. Then $APA^{-1}P^{-1}v_2 = r^2 v_2$. Thus $Bv^2 = r^2 v_2$. The eigenvalues of B are r^2 and r^{-2} since $\det B = 1$. Since $r^2 \notin \{0, 1, -1, \}$ B is not the zero, identity, or -identity matrix. Next, let C be the setf of matrices in $SL_2(F)$ with eigenvalues s, s^{-1}. Then C is a single conjugacy class of $SL_2(F)$. Let $S = \begin{pmatrix} s & \\ & s^{-1} \end{pmatrix}$. Then conjugacy class of S is a subset of C. We want to show the other inclusion now. Suppose that $Q \in C$. Then Q has distinct eigenvalues so it is diagonalizable. It is conjugate to S in $GL_2(F)$. We know that $Q = LSL^{-1}$ for some $L \in GL_2(F)$. Then

$$Q = L \begin{pmatrix} a & \\ & 1 \end{pmatrix} S \begin{pmatrix} a^{-1} & \\ & 1 \end{pmatrix} L^{-1}$$

for any $a \in F^\times = MSM^{-1}$. Choose $a = (\det L^{-1}$ so that $\det M = 1$ so $M \in SL_2(F)$. So Q is conjugate to S in $SL_2(F)$. Next, we show that $\begin{pmatrix} 1 & * \\ & 1 \end{pmatrix} \in N$ for all $x \in F$.

Proof. $\begin{pmatrix} 1 & * \\ & 1 \end{pmatrix} = \begin{pmatrix} s^{-1} & \\ & s \end{pmatrix} \begin{pmatrix} s & sx \\ & s^{-1} \end{pmatrix} \in N$. Next, we show that $\begin{pmatrix} 1 & \\ y & \end{pmatrix} \in N$ for all $y \in F$. the proof is similar. Consequently, $N = SL_2$. The matrices in step 3 and 4 generate $SL_2(F)$. This somes from some old PSET :). □

Let Z be the center of $SL_2(F)$. Then $\{\pm I\} \subseteq Z$ is a proper normal subgroup of $SL_2(F)$. So $Z = \{\pm I\}$

Definition 251

$PSL_2(F) = SL_2(F)/Z$

Corollary 252

If $|F| \geq 4$, then $PSL_2(F)$ is simple. The proof follows from the correspondence theorem.

q	$PSL_2(F)$	simple?
2	S_3	no
3	A_4	no
4	A_5	yes
5	A_5	yes
6		yes
7		yes
8		yes
9	A_6	yes

Table 1: Accidental Isomorphisms

32 December 4, 2020

Classification of finite simple groups: every finite simple group is one of the following:

- C_p for some prime p
- A_n for some $n \geq 5$
- $PSL_2(F_q)$ for some prime power $q \geq 4$
- One of 26 "sporadic" groups, the largest of which is called the Monster group

Definition 253

A sequence of homomorphisms

$$A \xrightarrow{\alpha} B \xrightarrow{\beta} C$$

is exact (at B) if $\operatorname{im} \alpha = \ker \beta$.

Example 254

$$\mathbb{R} \xrightarrow{\alpha} \mathbb{C}^\times \xrightarrow{\beta} \mathbb{R}^\times$$

$$t \mapsto e^{it} \mapsto |e^{it}|$$

is exact, since $\operatorname{im} \alpha = \ker \beta$, the unit circle.

Definition 255

$$G_0 \xrightarrow{\alpha_1} G_1 \xrightarrow{\alpha_2} G_2 \to \dots \xrightarrow{\alpha_n} G_n$$

is exact if it is exact at each joint. $\operatorname{im}\alpha_1 = \ker\alpha_{i+1}$.

Example 256

The following are equivalent

- $1 \to A \xrightarrow{\phi} B$ is exact
- $\ker\phi = 1$
- ϕ is injective

Example 257

TFAE

- $B \xrightarrow{\psi} C \to 1$ is exact
- $\operatorname{im}\psi = C$
- ψ is surjective

Definition 258

An exact sequence of the form $1 \to A \to B \to C \to 1$ is called a short exact sequence.

Example 259

If $\phi : B \to C$ is a surjective homomorphism, then

$$1 \to \ker\phi \xrightarrow{i} B \xrightarrow{\phi} C \to 1$$

is a short exact sequence.

33 December 7, 2020

Definition 260

$Aut(G)$ is the group of automorphisms of G.

Example 261

C_5. For each integer r, there is a homomorphism $\alpha_r : C_5 \to C_5$, $g \mapsto g^r$. If $5|r$, then $g^r = 1$ so α_r sends C_5 to 1 so α_r is not an automorphism. If $5 \nmid r$, then g^r generates C_5 so α_r is an automorphism. Then $\alpha_r = \alpha_{r'} \iff g^r = g^{r'} \iff r \equiv r'(\mod 5)$. And $\alpha_r \circ \alpha_s = \alpha_{rs}$. We conclude that $C_5 \cong (\mathbb{Z}/5Z)^\times$. There are 4 such automorphisms.

Example 262

Every finite abelian group is a product of cyclic groups. C_p^n is a vector space of over the field F_p of dimension p. $Aut(C_p^n) = GL_n(F_p)$.

Definition 263

A **complement of N in G** is a subgroup $H \leq G$ such that $NH = G$ and $N \cap H = 1$.

Proposition 264

If H is a completement of N which is a normal subgroup of G then the map $N \times H \to G$, $(x, h) \mapsto xh$ is a bijection of sets.

Definition 265

Given groups N and H and a homomorphism $H \to AutN$ and $h \mapsto \phi_h$, define $N \rtimes H$ to be the set $N \times H$ with the binary operation $(x, h)(x', h') = (x\phi_h(x'), hh')$.

Proposition 266

$N \rtimes H$ is a group. It's called the semidirect product of N and H with respect to ϕ. The proof is just a matter of checking the group axioms.

The group $N \rtimes H$ has two obvious subgroups: $\{(x, 1) : x \in N\}$ is a copy of N in $N \rtimes H$ and $\{(1, h) : h \in H\}$ is a copy of H. We get a short exact sequence: $1 \to N \to N \rtimes H \to H \to 1$.

Proposition 267

If H is a complement of N which is a normal subgroup of H then H acts on N by conjugation via $\phi : H \to AutN$, $h \mapsto (x \mapsto hxh^{-1}$ and $G \xrightarrow{\sim} N \rtimes H$, $(x, h) \mapsto xh$.

Example 268

Start with $C_n = N$. We have a homomorphism $\phi : \{\pm I\} \to AutC_n$, $1 \mapsto (x \mapsto x)$, $-1 \mapsto (x \mapsto x^{-1})$. We can form the semidirect product $C_n \rtimes \{\pm I\}$. What is it? D_n.

Example 269

$\mathbb{R}^n$ is a normal subgroup of the group of isometries. Thus O_n acts on $\mathbb{R}^n$ under matrix-vector multiplication so $M_n \cong \mathbb{R}^n \rtimes O_n$.

34 December 9, 2020

Today, we're going to talk about tensor products. polyhedra and the Dehn invariant (time-permitting). Let V, W be $\mathbb{R}$-vector spaces. Given $v \in V$ and $w \in W$, can we multiply to get $v \otimes w$? Yes. In which vector space would $v \otimes w$ lie? $V \otimes W$. We define $\mathbb{R}^m \otimes \mathbb{R}^n = \mathbb{R}^{mn}$. This is not to be confused with $\mathbb{R}^3 \oplus \mathbb{R}^2 = \mathbb{R}^5$.

There is a unique way to extend the $\otimes$ on basis vectors to all vectors, to define $v \otimes w$ for all $v \in \mathbb{R}^3$, $w \in \mathbb{R}^2$ in such a way that $\mathbb{R}^2 \times \mathbb{R}^3 \to \mathbb{R}^2 \otimes \mathbb{R}^3$, $(v, w) \mapsto v \otimes w$ is a bilinear form. For example, if $v = 2e_1 + 5e_3$ and $w = 3f_1 + 7f_2$. Then $v \otimes w = 6e_1 \otimes f_1 + 14e_1 \otimes f_2 + 15e_3 \otimes f_1 + 35e_3 \otimes f_2$.

Given V and W, $\mathbb{R}$ vector spaces. How do we define $V \otimes W$? Wrong: G is an $\mathbb{R}$-vector space with one basis vector for each pair (v, w) with $v \in V$ and $w \in W$, and define $v \otimes w$ is the basis vector (v, w) of G. This makes G infinite dimensional and $(v_1 + v_2) \otimes w = v_1 \otimes w + v_2 \otimes w$ won't hold. The three vectors will all be different bases (and consequently linearly independent). This is a contradiction since there is an obvious linear dependency among the three elements. Let $\mathcal{R}$ be the subspace of G spanned by

- $(v_1 + v_2, w) - (v_1, w) - (v_2, w)$
- $(cv, w) - c(v, w)$
- $(v, w_1 + w_2) - (v, w_1) - (v, w_2)$
- $(v, cw) - c(v, w)$

for all $v_1, v_2 \in V$ and $w \in W$ for all $c \in \mathbb{R}$, $v \in V$ and $w \in W$. Finally, define $V \otimes W = G/\mathcal{R}$. Then the things in $\mathcal{R}$ get identified to zero so it's bilinear and stuff.

The same construction works over any field $\mathbb{F}$. If V and W are $F - vectorspaces$, then we can form $V \otimes W$.

Example 270

$\mathbb{C} \otimes \mathbb{C}$ is a 4-dimensional $\mathbb{R}$ vector space and $\mathbb{C} \otimes \mathbb{C}$ is a 1-dimensional $\mathbb{C}$-vector space. $\mathbb{R}$ is a $\mathbb{Q}$-vector space (under addition and scalar multiplication) of infinite dimension. $\sqrt{2}, \sqrt{3}, \ldots,$ are $\mathbb{Q}$-linearly dependent. $\mathbb{Q}\pi$ is a 1-dimensional $\mathbb{Q}$-subspace of $\mathbb{R}$. $\mathbb{R}/\mathbb{Q}\pi$ is another infinite-dimensional vector space.

34.1 The Dehn Invariant

Suppose we have a polyhedron. Slice the polyhedra. Get all the pieces. Glue the pieces again and you get a new polyhedron. Suppose you called the polyedron you started with P and the one you ended with P'. Obviously, the areas of P and P' will stay the same. There's another quantity that's preserved. Fix your attention on one of the edges of P. There is such thing as the dihedral angle. The angle between two faces that meet along an edge e. Call this angle θ_e. Call the length of e l_e. Then

$$\sum_{e \text{ an edge}} l_e \otimes \theta_e \in \mathbb{R} \otimes \mathbb{R}/\mathbb{Q}\pi$$

.

Theorem 271

Two polyhedra are scissor-congruent if and only if they have the same volume and have the same Dehn-invarant.

- The regular tetrahedron has dihedral angles $\cos^{-1}(\frac{1}{3}) \in \mathbb{Q}\pi$ and hence Dehn invariant

$$\sum_{i=1}^{6} 1 \otimes \cos^{-1}(\frac{1}{3}) \neq 0$$

  in $\mathbb{R}_{\mathbb{Q}} \otimes \mathbb{R}/\mathbb{Q}\pi$

- The cube has dihedral angles $\pi/2 \in \mathbb{Q}\pi$ and hence the Dehn invariant 0.

Some non-regular tetrahedra have Dehn invariant 0. An open problem is to classify them all.