Math 701. Fall 2017.

[office, e-mail, seminars: AG ~~Fri~~ Fri, 317P, ~~2:30~~ 3:30; NT (TBA); Grad colloquium Tuesdays, 4:30. PANTS, Sept. 16-17.]

[Homework discussions.]

[A bit about algebraic topics]

Crash course on linear algebra.

Let F be a field. (can think: $\mathbb{R}$ or $\mathbb{C}$. intro to fields later)

A <u>vector space</u> V over F is a set ~~satisfying the following~~ ~~axioms~~ with an addition law
$$V \times V \to V$$
$$(v, w) \to v + w$$
a scalar multiplication law
$$F \times V \to V$$
$$(c, v) \to cv$$

satisfying:

(1) $(V, +)$ is an <u>abelian</u> group:

* $v + w = w + v$ for all $v, w \in V$.
* There is an elt. $0 \in V$ with $v + 0 = v$ for all $v \in V$.
* Every $v \in V$ has an <u>additive</u> <u>inverse</u> $-v$ with $v + (-v) = 0$
* $(v + w) + x = v + (w + x)$ for all $v, w, x \in V$.

(2) For every $v \in V$ and $c, d \in F$:

* $0v = 0$. (The left 0 is 0_F, right is 0_V.)
* $1v = v$.
* $c(dv) = (cd)v$.

(3) Distributive laws: For all $c, d \in F$ and $x, y \in V$

* $c(x + y) = cx + cy$
* $(c + d)x = cd + cx$.

<u>DON'T MEMORIZE THESE</u>

Examples:

* F^n.
* The set of all polynomials in F.
* The set of all polynomials in F of degree ≤ 37.
* The set of all functions $F \to F$.
* The set of all functions $F \to F$ vanishing at 0.
* $\mathbb{C}/\mathbb{R}$.
* (Invent your own)

In general, we want maps between objects to preserve the structure.

Def. If V and W are vector spaces over a field F, then a function $\phi : V \to W$ is a homomorphism (linear transformation) if:

* $\phi(v_1 + v_2) = \phi(v_1) + \phi(v_2)$ for all $v_1, v_2 \in V$
  (e.g. it is a homomorphism of abelian groups)
* $\phi(av) = a\phi(v)$ for all $a \in F$, $v \in V$.

ϕ is:
injective (one-to-one) if $\phi(v_1) = \phi(v_2)$ implies $v_1 = v_2$;
surjective (onto) if, for all $w \in W$ $\exists$ $v \in V$ with $\phi(v) = w$
(equiv: $\mathrm{Im}(\phi) = W$)
bijective if it is injective and surjective.

The kernel (or nullspace) of ϕ is

$$\mathrm{Ker}(\phi) = \{ v \in V : \phi(v) = 0 \}.$$

701. 1.3.

Proposition. A homomorphism $\phi : V \to W$ is injective iff $\ker(\phi) = \{0\}$.
= if and only if

Proof. $\Longrightarrow$: We must have $\phi(0) = 0$, i.e. $0 \in \ker(\phi)$

why? For example, $\phi(0) = \phi(0+0) = \phi(0) + \phi(0)$

$$\phi(0) - \phi(0) = (\phi(0) + \phi(0)) - \phi(0)$$
$$= \phi(0) + (\phi(0) - \phi(0))$$
$$0 = \phi(0). \quad [\text{*ugh*}]$$

So, $\{0\} \subseteq \ker(\phi)$.
By hypothesis, $\phi(v) = \phi(0) = 0 \Longrightarrow v = 0$.
So $\{0\} = \ker(\phi)$.

$\Longleftarrow$: Suppose $\phi(v_1) = \phi(v_2)$.

Then, $0 = \phi(v_1) - \phi(v_2)$
$= \phi(v_1 - v_2)$, so $v_1 - v_2 = 0$.

Hence $v_1 = v_2$.

Some proofs in this business are genuinely interesting.
Not this one.
This is structure-building. Brick by brick.

701. 1.4 - 2.1

Definitions. A set of vectors $S \subseteq V$:

(1) spans V if each $v \in V$ can be written as

$$v = a_1 v_1 + a_2 v_2 + \cdots + a_n v_n$$

for $a_1, \ldots, a_n \in F$, $v_1, \ldots, v_n \in S$

[a.k.a, if each $v \in V$ can be written as a linear combination of elements of S];

(2) is linearly independent if, whenever we have

$$a_1 v_1 + a_2 v_2 + \cdots + a_n v_n = 0,$$

for some $a_1 \cdots a_n \in F$, $v_1 \cdots v_n \in S$

we have all the a_i equal to 0.

(3) is a basis for V if it spans V and is linearly independent.

(Sometimes we implicitly assume a basis should be ordered.)

Exercise. Prove from scratch that every basis of $\mathbb{R}^2$ has exactly two vectors. This will help you appreciate the theory-building!

Proposition. Assume that $S = \{v_1, \ldots, v_n\}$ spans V and that no proper subset of S spans V. Then S is a basis for V.

Proof. Suppose, by way of contradiction, that it's not; then we have a relation

$$a_1 v_1 + a_2 v_2 + \cdots + a_n v_n = 0$$

with not all the a_i equal to 0. WLOG, $a_1 \neq 0$.

Make sure you understand this!

Then $v_1 = \frac{-1}{a_1}(a_2 v_2 + \cdots + a_n v_n)$

and so $\{v_2, \ldots, v_n\}$ spans V. QED.

Corollary. Let S be a finite set spanning V. Then S contains a basis for V.

[Don't write anything down! Solve it by "pure thought".]

Theorem. Suppose V has a finite basis with n elements. Then any linearly independent set in V has $\le n$ vectors, and any spanning set has $\ge n$ vectors.

Cor. Any two bases have the same cardinality.

Replacement Lemma.

Given: a basis $A = \{a_1, \ldots, a_n\}$ for V

a linearly independent set $B = \{b_1, \ldots, b_m\}$ in V.

There is an ordering $a_1 \ldots a_n$ s.t. for each $k \in \{1, \ldots, m\}$,

$$\{b_1, \ldots, b_k, a_{k+1}, \ldots, a_n\} \text{ is a basis for } V.$$

(In particular $n \ge m$.)

2.3

Proof. Induction on k.

Assume $\{b_1, \dots, b_k, a_{k+1}, \dots a_n\}$ is a basis.

Then, $b_{k+1} = \beta_1 b_1 + \dots + \beta_k b_k + \alpha_{k+1} a_{k+1} + \dots + \alpha_n a_n$

(*) for some scalars β_i, α_j.

WLOG, $\alpha_{k+1} \neq 0$. (If all the α_j are 0, $\{b_1, \dots, b_k, b_{k+1}\}$ is linearly dependent.)

So solve a_{k+1} in terms of others, so

$\text{Span}\{b_1, \dots, b_{k+1}, a_{k+2}, \dots, a_n\}$

$= \text{Span}\{b_1, \dots, b_k, a_{k+1}, \dots, a_n\} = V$.

We must prove linear independence too.

Suppose

$$\beta_1' b_1 + \dots + \beta_{k+1}' b_{k+1} + \alpha_{k+2}' a_{k+2} + \dots + \alpha_n' a_n = 0. \quad (**)$$

Then substitute (*) for b_{k+1}, get equ in terms of $b_1 \dots b_k, a_{k+1}, \dots, a_n$.

The a_{k+1} coefficient is $\beta_{k+1}' \cdot \underbrace{\alpha_{k+1}}_{\text{not zero}} = 0$ by linear independence

So $\beta_{k+1}' = 0$.

But other ~~coeffs~~ vectors are linearly independent, so all coeffs 0 in (**). Done.

2.4

This implies:

If V has a basis with n elements, then any LI set has $\leq n$ elements.

Also true:

If V has a basis with n elements, then any spanning set has $\geq n$ elements.

Proof. Let A be a basis w/ n elements

B be a spanning set

Then B contains a basis, which by theorem has at least as many elements as A.

Definition. If a vector space V has a finite basis, the dimension $\dim(V)$ is the number of elements in any basis for V.

Otherwise we say $\dim(V) = \infty$.

Corollary. If A is any set of linearly independent vectors, it can be extended to a basis.

Again immediate by "building up"!

2.5 = 3.1.

Dimensions and linear transformations.

Suppose that $\phi : V \to W$ is a homomorphism of vector spaces. Then: (please check yourself)

* $\mathrm{Ker}(\phi)$ is a subspace of V.

  [Need to check: contains 0; closed under +; closed under scalar multiplication]

* $\mathrm{Im}(\phi)$ is a subspace of W.

  $\{w \in W : w = \phi(v) \text{ for some } v\}$

Theorem. ("rank-nullity") If V is finite dimensional then

$$\dim V = \underbrace{\dim(\ker \phi)}_{\text{in } V} + \underbrace{\dim(\operatorname{im} \phi)}_{\text{in } W}.$$

Proof. Let $u_1, \dots, u_k$ be a basis for $\ker \phi$.

Extend it to a basis $u_1, \dots, u_k, s_1, \dots, s_j$ of V

with $k + j = \dim V$.

Claim. $\phi(s_1), \dots, \phi(s_j)$ is a basis of $\operatorname{im} \phi$.

They span $\operatorname{im} \phi$, because $\phi(u_1), \dots, \phi(u_k), \phi(s_1), \dots, \phi(s_j)$ do and the first ones are all zero.

They are linearly independent, because if

$$a_1 \phi(s_1) + \dots + a_j \phi(s_j) = 0$$

then $0 = \phi(a_1 s_1 + \dots + a_j s_j)$

$\Rightarrow a_1 s_1 + \dots + a_j s_j$ is in $\ker(\phi)$, a LC of the u's and hence zero by linear independence

3.2.

Cor. If $\varphi : V \to W$ is a homo of vector spaces of the same dimension, then TFAE

(1) φ is an isomorphism

(2) φ is injective

(3) φ is surjective

(4) φ sends a basis of V to one of W.

Def. Let V and W be vector spaces. Then:

* $\mathrm{Hom}(V, W) = \{\phi : V \to W\}$
* $\mathrm{End}(V) = \mathrm{Hom}(V, V)$
* $GL(V) = \{\phi \in \mathrm{End}(V) : \phi \text{ is an isomorphism}\}$.

Proposition. $\mathrm{Hom}(V, W)$ is itself a vector space.

By definition,
$$(\phi + \psi)(v) = \phi(v) + \psi(v)$$
$$(c\phi)(v) = \phi(cv).$$

As a special case, if $W = F$ (the ground field; a one dimensional VS) then $\mathrm{Hom}(V, F) = V^*$, the dual space of V.

Proposition. If V is finite dimensional then $V \cong V^*$.

3.3

<u>Proof.</u> Choose a basis $\{v_1, \dots, v_n\}$ for V.

Then define
$$\phi : V \to V^*$$
$$v_i \to v_i^*$$

where $v_i^*(a_1 v_1 + a_2 v_2 + \dots + a_n v_n) = a_i$.

<u>Exercise.</u> Verify that ~~[illegible]~~ this satisfies all the desired properties.

Note there is <u>no</u> <u>natural</u> ~~[illegible]~~ iso $V \to V^*$
must choose a basis first.

<u>Matrices</u>: You can represent elements of $\mathrm{Hom}(V, w)$ as matrices.

Choose bases $\{v_1, \dots, v_n\}$ for V and $\{w_1, \dots, w_m\}$ for w.

Then, if $\varphi \in \mathrm{Hom}(V, w)$,
$$\varphi(v_j) = \sum_{i=1}^{m} a_{ij} w_i$$
for some scalars a_{ij}.

Since $\varphi(b_1 v_1 + \dots + b_n v_n) = b_1 \varphi(v_1) + \dots + b_n \varphi(v_n)$,
this determines φ.

The <u>matrix</u> <u>of φ</u> w.r.t. these bases is

$$\overbrace{\begin{bmatrix} a_{11} & \cdots & a_{1n} \\ & & \\ a_{m1} & \cdots & a_{mn} \end{bmatrix}}^{\#\text{ columns is } \dim(V)} \left.\vphantom{\begin{bmatrix} a \\ \\ a \end{bmatrix}}\right\} \#\text{ rows is } \dim(w).$$

Image of v_1 ------ Image of v_n

3.4. Properties of matrices:

We can write elements of V as "column vectors"

$$v = b_1 v_1 + \cdots + b_n v_n \longleftrightarrow \begin{bmatrix} b_1 \\ \vdots \\ b_n \end{bmatrix}.$$

Then $\varphi(v)$ is represented by

$$\begin{bmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & & \\ a_{m1} & \cdots & a_{mn} \end{bmatrix} \begin{bmatrix} b_1 \\ \vdots \\ b_n \end{bmatrix}.$$

Write $M_{m\times n}(F)$ for the vector space of $\underbrace{m \times n}_{\substack{m \text{ rows,} \\ n \text{ columns}}}$ matrices with coeffs in F.

If $\dim(V) = n$ and $\dim(W) = m$, then choosing a basis for V and W gives a vector space isomorphism

$$\mathrm{Hom}(V, W) \longrightarrow M_{m\times n}(F) \quad \text{as above.}$$

So, $\dim \mathrm{Hom}(V, W) = (\dim V)(\dim W)$
and in particular $\dim(V^*) = \dim(V)$.

Matrix multiplication. Suppose we have

$$\underset{\dim = n}{V} \xrightarrow{\phi} \underset{\dim = m}{W} \xrightarrow{\psi} \underset{\dim = r}{X}$$

then $\psi \circ \phi$ is a homomorphism $V \to X$.
If ~~these~~ bases are chosen, and matrices A and B represent ψ and ϕ, then $\Longrightarrow$

3.5.

AB represents $\psi \circ \phi$.

$$\overset{A}{\begin{bmatrix} r \times m \\ \cdots \end{bmatrix}} \overset{B}{\begin{bmatrix} m \times n \\ \cdots \end{bmatrix}} = r \times n.$$

You can check the computation.

Cor. Matrix multiplication is associative and distributive.

Because it represents functions.

Change of basis. Suppose V has two different bases

$$\mathcal{B} = \{v_1, \ldots, v_n\}$$
$$\mathcal{E} = \{v_1', \ldots, v_n'\}$$

Write down the identity map $V \to V$ as a matrix using the bases $\mathcal{B}$ and $\mathcal{E}$.

(Write elements of $\mathcal{E}$ in terms of those of $\mathcal{B}$.)

Exercise, If P is the resulting matrix, then

$$P^{-1} M_{\mathcal{B}}^{\mathcal{B}}(\varphi) P = M_{\mathcal{E}}^{\mathcal{E}}(\varphi) \quad \text{for all } \varphi \in \operatorname{End}(V).$$

So: A linear transformation determines the matrix up to conjugacy.

4.1. More on the dual $V^* = \mathrm{Hom}(V, F)$.

Recall, if we have a basis $v_1 \dots v_n$ of V, get a dual basis v_i^* of V^*, defined by

$$v_i^*(v_j) = \delta_{ij}.$$

Now, suppose V, W are vector spaces and $\phi \in \mathrm{Hom}(V, W)$.

We obtain ~~an~~ induced map $\phi^* \in \mathrm{Hom}(W^*, V^*)$, called the pullback of ϕ.

It is defined by, for $f \in W^* = \mathrm{Hom}(W, F)$

$$(\phi^* f) = f \circ \phi.$$

$$\text{i.e. } (\phi^* f)(v) = f(\phi(v)).$$

<< THIS CONSTRUCTION POPS UP ALL THE TIME >>

Claim. ϕ^* is linear.

Proof. $(\phi^*(cf))(v) = (cf)(\phi(v)) = c \cdot f(\phi(v)) = c \cdot (\phi^* f)(v)$.

$$= \cancel{f(c\,\phi(v))}$$

$$= \cancel{f(\phi(cv))}.$$

~~(Read it again.)~~

Similarly for addition.

$$\cancel{(\phi^*(f_1 + f_2))(v)} = \cancel{(f_1 + f_2)(\phi(v))}$$

$$= \cancel{f_1(\phi(v)) +}$$

Now, we've chosen bases $\mathcal{B}$ and $\mathcal{E}$ for V, W.

So we can represent ϕ as a matrix.

What is the matrix of ϕ^* w.r.t. the dual bases $\mathcal{B}^*$ and $\mathcal{E}^*$?

4.2 . Proposition.

The matrix of ϕ^* w.r.t. $\mathcal{B}^*$ and $\mathcal{E}^*$ is the transpose of that of ϕ w.r.t. $\mathcal{B}$ and $\mathcal{E}$.

Why? By definition, if $\phi \sim \begin{bmatrix} a_{11} & \text{---} & a_{1n} \\ | & & \\ a_{n1} & \text{---} & a_{nn} \end{bmatrix}$,

then $\phi(v_j) = \sum_{i=1}^{m} a_{ij} w_i$ (with $m = \dim W$).

~~By def~~ Have to compute $\phi^*(w_k^*)$.

By definition,

$$\begin{aligned} \phi^*(w_k^*)\,(v_j) &= (w_k^* \circ \phi)(v_j) \\ &= w_k^*(\phi(v_j)) \\ &= w_k^*\left(\sum_{i=1}^{m} a_{ij} w_i\right) = a_{kj}. \end{aligned}$$

i.e. if $\phi^* \sim \begin{bmatrix} b_{11} & \cdots & b_{1n} \\ \vdots & & \vdots \\ b_{m1} & \cdots & b_{mn} \end{bmatrix}$

with $\phi^*(w_k^*) \cancel{(v_j)} = \sum_{i=1}^{n} b_{ik} w_i^*$

so that $\phi^*(w_k^*)(v_j) = \cancel{(}\sum_{i=1}^{n} b_{ik} w_i^*(v_j) = b_{jk}$

we see that $a_{kj} = b_{jk}$.

4.3. We have additional contravariance properties as well. For example, if $\phi : V \to W$

$\psi : W \to X$,

get $\psi \circ \phi : V \to X$

then what is $(\psi \circ \phi)^*$? a map $X^* \to V^*$

$$
\begin{aligned}
(\psi \circ \phi)^*(x^*) &= x^* \circ \psi \circ \phi \\
&= (\psi^* x^*) \circ \phi \\
&= \phi^* (\psi^* x^*) \\
&= (\phi^* \circ \psi^*)\, x^* .
\end{aligned}
$$

So $(\psi \circ \phi)^* = \phi^* \circ \psi^*$, duality reverses direction.

So we see that $(AB)^T = B^T A^T$

5.1. Recall:

<u>Change of basis</u>. Let $\phi \in \mathrm{End}(V)$ with $\dim(V) = n$.
If A and B are the matrices of ϕ wrt different bases
then $\exists$ ~~$M \in GL_n$~~ a $n \times n$ matrix M s.t.

$$A = M^{-1} B M.$$

We say A is <u>similar</u> or <u>conjugate</u> to B.

<u>Idea</u>: Choose a basis so the matrix is nice.

Throughout assume V is f.d. of dimension n,
and $\phi \in \mathrm{End}(V)$.

<u>Definition</u>. If it happens that

$$\phi v = \lambda v$$

for some vector $v \in V$ and scalar $\lambda \in F$, then we say that v is an <u>eigenvector</u> for ϕ with <u>eigenvalue</u> λ.

<u>Note</u> $\{\phi$ is not invertible$\} \Longleftrightarrow \{0$ is an eigenvalue of $\phi\}$

<u>Theorem</u>. If F is $\left\{\begin{matrix} \mathbb{C} \\ \text{algebraically closed} \end{matrix}\right\}$ then every $\phi \in \mathrm{End}(V)$ has at least one eigenvalue.

<u>Proof</u>. Consider any nonzero $v \in V$ and look at

$$\{v, \phi v, \phi^2 v, \ldots, \phi^n v\}.$$

$n+1$ vectors in an n-dimensional vs, so <u>must</u> be linearly dependent.

5.2.

There exists a relation

$$0 = a_0 v + a_1 \phi v + a_2 \phi^2 v + \cdots + a_n \phi^n v$$

and hence one of the form

$$0 = a_0 v + a_1 \phi v + \cdots + \underbrace{\phi^m}_{(a_m = 1)} v \quad \text{for some } m \leq n.$$

Factor over F:

$$0 = (\phi - \lambda_1)(\phi - \lambda_2) \cdots (\phi - \lambda_m) v.$$

Think about this carefully!

This means $\phi - \lambda_i$ is not injective for some i, so λ_i is an eigenvalue.

This means: if we choose a basis for V whose first basis elt. is an eigenvector, we can write the matrix as

$$\begin{bmatrix} \lambda & & & \\ 0 & & & \\ \vdots & & ? & \\ 0 & & & \end{bmatrix}$$

5.3.

Proposition. If $\phi \in \mathrm{End}(V)$ and $\{v_1, \dots, v_n\}$ is a basis for V, then TFAE.

(1) The matrix of ϕ wrt $\{v_1 \dots v_k\}$ is upper triangular

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

(2) $\phi v_i \in \mathrm{Span}\{v_1, \dots, v_i\}$ for $i = 1, \dots, n$

(3) $\mathrm{Span}\{v_1, \dots, v_i\}$ is invariant under ϕ for each $i = 1, \dots, n$.

(Proof is easy, do yourself!)

Theorem. If F is $\left\{\begin{matrix} \mathbb{C} \\ \text{algebraically closed} \end{matrix}\right\}$, then there exists a basis of F w.r.t. the above are true.

(Takes a bit more work.)

Diagonalizability. Let $\phi \in \mathrm{End}(V)$ be represented by a diagonal matrix $\begin{bmatrix} \lambda_1 & & 0 \\ & \ddots & \\ 0 & & \lambda_n \end{bmatrix}$.

Then this basis of V consists of eigenvectors with eigenvalues λ_i.

5.4

Def. A matrix is diagonalizable if it is conjugate to a diagonal matrix.

Prop. This is true iff the vector space has a basis of eigenvectors w.r.t. this linear transformation.

In general, the best you can do is that any matrix will be conjugate over an alg closed field to one of the form

$$\begin{bmatrix} \lambda_1 & 1 & & & & & & & & \\ & \ddots & \ddots & & & & & & & \\ & & \ddots & 1 & & & & & & \\ & & & \lambda_1 & 0 & & & & & \\ & & & & \lambda_2 & 1 & & & & \\ & & & & & \ddots & 1 & & & \\ & & & & & & \lambda_2 & & & \\ & & & & & & & \ddots & & \\ & & & & & & & & \lambda_k & 1 \\ & & & & & & & & & \ddots \; 1 \\ & & & & & & & & & \lambda_k \end{bmatrix}$$

i.e. it consists of blocks $\begin{bmatrix} \lambda_i & 1 & & \\ & \ddots & \ddots & \\ & & \ddots & 1 \\ & & & \lambda_i \end{bmatrix}$

with λ_i on the diagonal, and ones immediately above it. The λ_i's don't have to be distinct; these are all the eigenvalues of ϕ.

This is called Jordan canonical form.

~~5~~.5.6.1.

Proposition. Let $n \geq 1$. There exists a function $M_n(F) \to F$, called the determinant, satisfying the following.

(0) It is a homogeneous polynomial of deg n in the entries.

(1) $\det(M) = 0 \longleftrightarrow M$ is not invertible.

(2) If M_1 and M_2 are invertible, then

$$\det(M_1 M_2) = \det(M_1)\det(M_2).$$

(So det is a group homomorphism $GL(n,F) \to F^\times$.)

(3) If A is invertible, $\det(M) = \det(AMA^{-1})$.

(Exercise: follows from above)

So the determinant depends only on the underlying linear transformation.

(4) If M is upper triangular, then $\det(M)$ is the product of the entries on the diagonal.

(5) whatever else you know about determinants.

Definition. If $A \in M_n(F)$, its characteristic polynomial is $\det(xI - A)$.

Example. Let $A = \begin{bmatrix} \lambda_1 & & * \\ & \ddots & \\ 0 & & \lambda_n \end{bmatrix}$ upper triangular.

Then $\det(xI - A) = \det \begin{bmatrix} x-\lambda_1 & & * \\ & \ddots & \\ 0 & & x-\lambda_n \end{bmatrix}$

$= (x-\lambda_1)\cdots(x-\lambda_n)$.

6.2. Note that determinants, and hence charpolys, depend only on the underlying linear transformation.

(invariant under change of basis: $\det(M) = \det(AMA^{-1})$)

~~The other coeffici~~

The coefficients are interesting!

$$\text{charpoly}(A) = X^n - \underbrace{(\lambda_1 + \cdots + \lambda_n)}_{\text{This is called the trace.}} X^{n-1} + \cdots \pm \underbrace{(\lambda_1 \cdots \lambda_n)}_{\det A}$$

Equal to the sum of the diagonal entries even if A is not upper triangular. (Exercise: prove)

All the symmetric polynomials in the ~~eigenvalues~~ λ_i depend only on the LT. ~~Indeed, since~~

Proposition. The roots of the characteristic polynomial are exactly the eigenvalues of A.

Proof. α is an eigenvalue of A

$\Leftrightarrow$ $\alpha I - A$ has nontrivial kernel

$\Leftrightarrow$ $\det(\alpha I - A) = 0$.

6.3.

Theorem. (Cayley - Hamilton)

Suppose F is $\mathbb{C}$ (or more generally algebraically closed), let $\phi \in \mathrm{End}(V)$ with V finite dimensional, and let $f(x)$ be its characteristic polynomial.

Then $f(\phi) = 0$ (as an element of $\mathrm{End}(V)$.)

Proof. (Axler, 8.20) Choose a basis for V so that the matrix of ϕ is of the form

$$\begin{bmatrix} \lambda_1 & & * \\ & \ddots & \\ 0 & & \lambda_n \end{bmatrix}.$$

Want to show $(\phi - \lambda_1) \cdots (\phi - \lambda_n) v = 0$ for all v.
Enough to show it for the basis vectors $v_1, \ldots, v_n$.

Now $\phi v_1 = \lambda_1 v_1$, so true for v_1.

In general, for each $k > 1$

$$\phi v_k = b_{1k} v_1 + b_{2k} v_2 + \cdots + b_{(k-1)k} v_{k-1} + \lambda_k v_k,$$

so $(\phi - \lambda_k) v_k \in \mathrm{Span}\{v_1, \ldots, v_{k-1}\}$.

So $(\phi - \lambda_1)$ kills v_1

$(\phi - \lambda_1)(\phi - \lambda_2)$ kills v_2,

and so on.

//

6.4

Groups: (Dummit - Foote, Ch. 1)

Def. A group is a set G together with a binary operation (write $a \cdot b$ or just ab) satisfying the following:

Identity. There exists an element $e \in G$ (sometimes labeled 1 or 0) with $e \cdot g = g \cdot e = g$ for all g.

Inverses. For all $g \in G$, there exists an element $g^{-1} \in G$ with $g^{-1} \cdot g = g \cdot g^{-1} = e$.

Associativity. For all $a, b, c \in G$, $a \cdot (b \cdot c) = (a \cdot b) \cdot c$.

If in addition G satisfies the commutative law $a \cdot b = b \cdot a$ for all $a, b \in G$, then G is called abelian.

(And the operation is usually written $+$.)

Examples. $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, etc. with addition.

$\mathbb{Q}^\times = \mathbb{Q} - \{0\}$, $\mathbb{R}^\times$, $\mathbb{C}^\times$ with multiplication.

$GL_n(\mathbb{R}) = \{ n \times n$ real matrices A : $\det(A) \neq 0$ [equiv: A is invertible] $\}$

The cyclic group ~~$\mathbb{Z}$~~ $\mathbb{Z}/n$ of integers mod n. One way to describe this: the set $\{0, 1, 2, 3, \ldots, n-1\}$.

when you add, ~~discard~~ subtract n if the result is bigger than n.

6.5–7.1.

Some basic axioms.

1. The identity of G is unique.
2. For each $g \in G$, g^{-1} is uniquely determined.
3. $(g^{-1})^{-1} = g$ for all G.

(4) $(gh)^{-1} = h^{-1}g^{-1}$.

(5) $ab = ac \Rightarrow b = c$; $ba = ca \Rightarrow b = c$.

(6) (Generalized associative law)

The expression $g_1 g_2 \cdots g_n$ is always defined, it doesn't matter where you put parentheses.

Some proofs.

1. If e and f are identities, $ef = e = f$.

~~2. If x and y are both inverses of~~

5. $ab = ac \Rightarrow a^{-1}ab = a^{-1}ac \Rightarrow b = c$.

2. If x and y are both inverses of g,

$xg = yg$.

3. Says g is the inverse of g^{-1}. Read the definition again.

4. $(h^{-1}g^{-1})gh = e$ and ~~tg~~ $gh(h^{-1}g^{-1}) = e$.

6. I refused to write out a proof of this

7.2.

Def. The order of $x \in G$ is the smallest ~~positive~~ positive integer n s.t. $x^n = 1$. (write $|x|$ or $o(x)$).
If no such exists, say it's of infinite order.
Also, we say the order of a group is just its # of elements.

Example. Dihedral groups. D_{2n} in DF but usually D_n.

We'll describe them in multiple ways.

(1) A presentation.

$$D_n = \langle \underbrace{r, s}_{\text{generators}} \mid \underbrace{r^n = s^2 = 1, \ rs = sr^{-1}}_{\text{relation}} \rangle .$$

What does this mean?
D_n consists of strings in r, s, and their inverses.
Includes the empty string. (this is 1.)
So $1, rrrr = r^4, s, s^{-1}, rsr^{-1}s^{-1}r^9 s^{-5} r^{23} s^{-7}, \ldots$

The relations say that some strings are the same.

e.g. suppose $n = 5$,
Look at $r^7 s^3 r^{-2} s^{-8} r^4$. Can we simplify it?

$$= r^5 \cdot r^2 \cdot s^2 \cdot s \cdot r^{-2} (s^2)^{-4} r^4$$

$$= 1 \cdot r^2 \cdot 1 \cdot s \cdot r^{-2} \cdot 1^{-4} \cdot r^4$$

$$= r^2 s r^{-2} r^4 = r^2 s r^2$$

$$= r(sr^{-1}) r^2 = (sr^{-1}) r^{-1} r^{-1} r^2$$

$$= sr^{-1} = sr^{-1} r^5 = sr^4 .$$

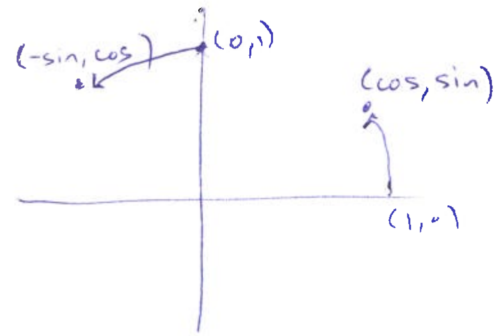
7.3.

Exercise.[1] Every element of D_n can be written as r^i for $0 \le i \le n-1$ or sr^i for $0 \le i \le n-1$, and no two of these elements are the same.

~~Exer~~

Now look inside $GL(2, \mathbb{R})$

Write $a = \begin{bmatrix} \cos\left(\frac{2\pi}{n}\right) & -\sin\left(\frac{2\pi}{n}\right) \\ \sin\left(\frac{2\pi}{n}\right) & \cos\left(\frac{2\pi}{n}\right) \end{bmatrix}$.



This is rotation by $\frac{2\pi}{n}$ radians.

$b = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$, a flip across the x-axis.

Look at the group generated by these matrices inside $GL(2, \mathbb{R})$

Exercise. Verify that $a^n = b^2 = 1$ and $ab = ba^{-1}$.

So this is again the dihedral group.

Indeed: Define D_n as before, and

Note: $GL_2(\mathbb{R})$ and $GL(2, \mathbb{R})$ are the same.

$$\rho : D_n \longrightarrow GL_2(\mathbb{R})$$

by $\rho(r) = a$, $\rho(s) = b$.

The map is well defined, because the relations in D_n are also preserved by the images in GL_2.

This is a homomorphism (which is injective) and indeed a "representation" (a homomorphism into some $GL(n)$.)

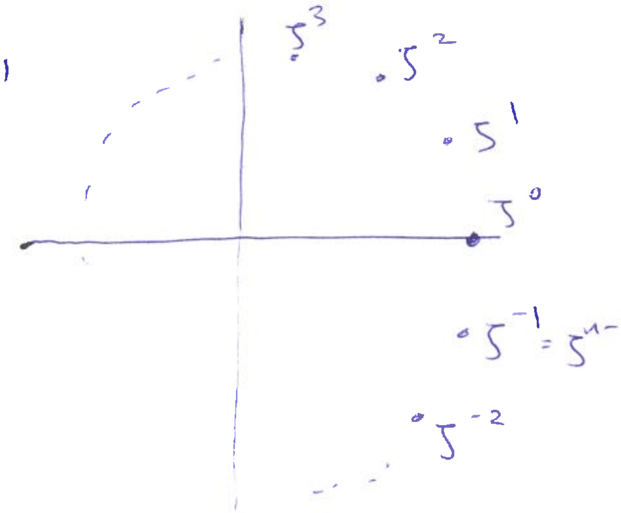
7.4. One more picture. Look inside $GL(2,\mathbb{R})$ again.

Look at the nth roots of unity

$$\zeta^0 = 1,\ \zeta = e^{2\pi i/n},\ \zeta^2 = e^{2\pi i \cdot 2/n},\ \ldots,\ \zeta^n = 1.$$

which we write as elements of $\mathbb{R}^2$,

$$\zeta^k = \begin{bmatrix} \cos\left(\frac{2\pi k}{n}\right) \\ \sin\left(\frac{2\pi k}{n}\right) \end{bmatrix}.$$



Then check: $a \cdot \zeta^k = \zeta^{k+1}$

and $b \cdot \zeta^k = \zeta^{-k}$.

So you can think of D_n as permutations of the set

$$\{\zeta^0, \zeta, \zeta^2, \ldots, \zeta^{n-1}\}.$$

Get another homomorphism

$$\phi : D_n \longrightarrow \mathrm{Sym}(\{\zeta^0, \zeta, \zeta^2, \ldots, \zeta^{n-1}\})$$

Sym(S) is the set, indeed the group, of ~~permutations~~ permutations of S, i.e. of bijections from S to itself

where r maps to the function : $\zeta^0 \to \zeta^1,\ \zeta^1 \to \zeta^2,\ \ldots,$

$\zeta^{n-1} \to \zeta^0$,

i.e. $\zeta^k \to \zeta^{k+1 \pmod n}$.

and s maps to : $\zeta^0 \to \zeta^0,\ \zeta^1 \to \zeta^{-1},$

$\zeta^2 \to \zeta^{-2},\ \ldots,\ \zeta^k \to \zeta^{-k}$.

§.1. Permutation groups.

Definition. If X is any set,

$\mathrm{Sym}(X)$ (or S_X) is $\{$bijections $X \to X\}$.

This is a group under function composition.

We also, write, for positive integers n,

$$\mathrm{Sym}(n) = \mathrm{Sym}(\{1, \cdots, n\}).$$

Note that if $|X| = n$, $\mathrm{Sym}(X) \cong \mathrm{Sym}(n)$. (Prove!)

We know from combinatorics that $|\mathrm{Sym}(n)| = n!$.

Cycle structure.

Consider $\sigma \in \mathrm{Sym}(7)$ given by
$$\begin{array}{c} x \\ \sigma(x) \end{array} \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 5 & 7 & 6 & 4 & 2 & 3 & 1 \end{pmatrix}.$$

Write it in terms of a cycle decomposition

$(1\ 5\ 2\ 7)(3\ 6)(4)$ or just

$(1\ 5\ 2\ 7)(3\ 6)$.

This means $1 \to 5 \to 2 \to 7$ and $3 \to 6$.

It can be checked that disjoint cycles commute.

So $(1\ 5\ 2\ 7)(3\ 6) = (3\ 6)(1\ 5\ 2\ 7)$.

Example. In $\mathrm{Sym}(3)$, compute $(1\ 2)(1\ 3)$ and $(1\ 3)(1\ 2)$.
(not disjoint)

$(1\ 2)(1\ 3) = (1\ 3\ 2)$ $\quad$ $(1\ 3)(1\ 2) = (1\ 2\ 3)$

(read from right to left!!)

Note that $\mathrm{Sym}(3)$ and $\mathrm{Sym}(n)$ for $n \geq 3$ are not abelian.

8.2.

Subgroups. If G is a group and $H \subseteq G$ is a subset, it is called a subgroup if it is itself a group with the same group operation.

Examples. The subgroups of $\mathbb{Z}$ are $\{0\}$ and $n\mathbb{Z}$ for $n \geq 1$.

Easy: These are all subgroups.

Harder: These are the only subgroups.

The subgroups of $\mathrm{Sym}(3)$. [Hack around at board.]

Note the associative law is inherited for free. You just have to check identity and inverses.

(Alternatively: $H \neq \emptyset$ and $x, y \in H \Rightarrow xy^{-1} \in H$.)

Homomorphisms. Let G and H be groups. A map $\varphi : G \to H$ is called a homomorphism if

$$\underbrace{\varphi(xy)}_{\text{mult. in } G} = \underbrace{\varphi(x)\,\varphi(y)}_{\text{mult. in } H} \quad \text{for all } x, y \in G.$$

We say it's an isomorphism if it's a bijection (and that "G and H are isomorphic")

Proposition. If φ is an isomorphism then its inverse is also a homomorphism (and hence an isomorphism).

Exercise. Prove it. (It's not quite immediate)

8.3

Some examples.

1. The identity map $G \to G$ for any G.
2. Our dihedral group examples.

let $D_n = \langle r, s \mid r^n = s^2 = 1,\ rs = sr^{-1} \rangle$

Then we have homomorphisms

$$\begin{aligned} D_n &\longrightarrow GL_2(\mathbb{R}) \\ r &\longrightarrow \begin{bmatrix} \cos(\frac{2\pi}{n}) & -\sin(\frac{2\pi}{n}) \\ \sin(\frac{2\pi}{n}) & \cos(\frac{2\pi}{n}) \end{bmatrix} \\ s &\longrightarrow \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \end{aligned}$$

and

$$\begin{aligned} D_n &\longrightarrow Sym(n) \\ r &\longrightarrow (1\ 2\ 3\ 4\ 5\ 6\ 7\ \cdots\ n) \\ s &\longrightarrow (1\ \ n-1)(2\ \ n-2) \cdots \begin{cases} (\frac{n}{2}-1\ \ \frac{n}{2}+1) & \text{for } n \text{ even} \\ (\frac{n-1}{2}\ \ \frac{n+1}{2}) & n \text{ odd} \end{cases} \end{aligned}$$

Exercises. (1) Neither of these is surjective (except $D_2 \to Sym(2)$)

(2) The subgroup of $Sym(n)$ that's the image is the same as the one generated by $(1\ 2\ 3\ \cdots\ n)$ and "reverse everything" — i.e. $\begin{pmatrix} 1 & 2 & 3 & \cdots & n \\ n & n-1 & n-2 & \cdots & 1 \end{pmatrix}$.

$\S.4.$

3. Let $(\mathbb{R}, +)$ be the ~~~~ usual real numbers
Also have $(\mathbb{R}^+, \times)$ positive real numbers
with multiplication as the group law.

The exponential function induces an isomorphism

$$(\mathbb{R}, +) \longrightarrow (\mathbb{R}^+, \times)$$
$$x \longrightarrow e^x$$

whose inverse is $y \to \log y$.
Note: we are adults here.
No one gives a shit about base 10.

4. If S and T are sets of the same cardinality,
$\mathrm{Sym}(S) \cong \mathrm{Sym}(T)$.
This is "obvious" but a PITA to write out.
You should do it once in your life.

5. Let G be any group, with $g \in G$.
Then the map $G \longrightarrow G$
$$x \longrightarrow gxg^{-1}$$
is an isomorphism, because $(gxg^{-1})(gyg^{-1})$
$= g(xy)g^{-1}$.

(And because it's injective (check!)
as with vector spaces, ETS only 1 maps to 1.

Example. Let $A \in GL_n(\mathbb{R})$.
There exists B ~~~~ $\in GL_n(\mathbb{R})$ with $A = BJB^{-1}$
and J in Jordan form.
~~If~~ we need to compute A^n, $A^n = (BJB^{-1})^n = BJ^nB^{-1}$.
This is computationally much easier!

§.5 6. Let $G = \mathrm{sym}(3)$.

$$G \longrightarrow \{\pm 1\}$$

defined by $1, (1\ 2\ 3), (1\ 3\ 2) \to 1$

everything else $\to -1$.

7. $D_3 \cong \mathrm{Sym}(3)$ as above.

8. $$\mathbb{Z} \longrightarrow C_n = \langle a \mid a^n = 1 \rangle$$

$$1 \longrightarrow a.$$

what is the kernel?

Can you prove that S_3 is not isomorphic to C_6?