55a Lecture 6 — Wed Sept 16 2020 — reminder: HW 2 due / HW3 available

* **Recall** | a field $(k,+,\times)$ = set with two operations, $(k,+)$ abelian group with identity 0, $(k^* = k \setminus \{0\}, \times)$ abelian group with identity 1, distributive law.

* Given a field k, we always have a ring homomorphism $\varphi: \mathbb{Z} \to k$, $1 \mapsto 1_k$
(this determines φ, since 1 generates $\mathbb{Z}$) $\hookrightarrow \varphi(a+b) = \varphi(a)+\varphi(b)$, $\varphi(ab) = \varphi(a)\varphi(b)$

Is this injective? For most fields we'll consider (eg. $\mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{R}(x), \mathbb{R}((x)), \dots$), it is.
If so, say k has characteristic zero. Otherwise:

Prop: $\ker(\varphi: \mathbb{Z} \to k) = \mathbb{Z}p$ for some prime p.

Pf: $\ker(\varphi)$ is a subgroup of $\mathbb{Z}$, hence of the form $\mathbb{Z}n$. If n is not prime, write $n = ab$ for $1 < a, b < n$. Then $\varphi(n) = \varphi(ab) = \varphi(a)\varphi(b) = 0 \in k$. but this implies $\varphi(a) = 0$ or $\varphi(b) = 0$ (if $\varphi(a) \neq 0$, multiply by $\varphi(a)^{-1}$ to get $\varphi(b) = 0$). Since by assumption n is the smallest positive integer st. $\varphi(n) = 0$, this is a contradiction. $\square$

Def: Say k has characteristic p if $\ker(\varphi) = \mathbb{Z}p$. (This means $p \cdot 1_k = \underbrace{1+\dots+1}_{p \text{ times}} = 0$!)

So far our only example of such a field is $\mathbb{Z}/p$, but there are more.

Theorem: For all $n \geq 1$ and prime p, there exists a unique field with p^n elements (up to isomorphism), and these are all the finite fields.

(There are also infinite fields of characteristic p, for example $\mathbb{Z}/p((x))$!)

Def: A vector space over k is a set V with two operations:
(1) addition $+: V \times V \to V$ making V an abelian group with identity $0 \in V$.
(2) scalar multiplication $\times: k \times V \to V$ associative $(ab)v = a(bv)$; $1v = v$, $0v = 0$; distributive $a(v+v') = av+av'$, $(a+b)v = av+bv$

Def. A subspace of a vector space is a nonempty subset $W \subset V$ that is preserved by addition and scalar multiplication: $W + W \subset W$, $k \cdot W \subset W$.
(So W is also a vector space!) in fact $=W$ $\hookrightarrow$ this implies $0 \in W$.

Examples:
- $\{0\}$ is a vector space
- $k^n = \{(a_1, \dots, a_n) \mid a_i \in k\}$ with componentwise addition / scalar mult.
- $k^\infty = \{(a_i)_{i \in \mathbb{N}} \mid a_i \in k\}$ (sequences in k) $\supset$ {sequences which are eventually zero}
  ($\Leftrightarrow$ polynomials $k[x]$, power series $k[[x]]$)
- given any set S, $k^S = \{\text{maps } f: S \to k\}$
- {functions $f: \mathbb{R} \to \mathbb{R}$} $\supset$ {continuous functions} $\supset$ {differentiable functions}.

Span, linear independence, basis:

Let V be a vector space $/k$.

Def: Given $v_1,\dots,v_n \in V$, the span of $v_1,\dots,v_n$ is the smallest subspace of V which contains $v_1,\dots,v_n$. Concretely, $\mathrm{span}(v_1,\dots,v_n) = \{a_1v_1+\dots+a_nv_n \mid a_i \in k\}$

Def: say $v_1 \dots v_n$ span V if $\mathrm{span}(v_1,\dots,v_n) = V$.

Def: We say $v_1,\dots,v_n \in V$ are linearly independent if
$$a_1v_1+\dots+a_nv_n = 0 \Rightarrow a_1=a_2=\dots=a_n=0.$$

Equivalently, given $v_1,\dots v_n \in V$, we have a linear map $\phi : k^n \longrightarrow V$, $(a_1,\dots,a_n) \mapsto \sum a_iv_i$

$v_1,\dots v_n$ are linearly indep^t $\Leftrightarrow$ ϕ injective

$v_1 \dots v_n$ span V $\Leftrightarrow$ ϕ surjective.

Def: $(v_1,\dots,v_n)$ are a basis of V if they are linearly independent and span V.

Then any element of V can be expressed uniquely as $\sum a_iv_i$ for some $a_i \in k$.

Ex: $(1,0)$ and $(0,1)$ are a basis of k^2. So are $(1,1)$ and $(1,-1)$ for most fields k. (what if $\mathrm{char}(k)=2$?)

$\star$ We will see soon: if V has a basis with n elements, then every basis of V has n elements. We say the dimension of V is $\dim(V)=n$.

One can also consider infinite-dimensional vector spaces: for $S \subset V$ any subset,

Def
- $\mathrm{span}(S)$ = smallest subspace of V containing S
$$= \{a_1v_1+\dots+a_kv_k \mid k\in\mathbb{N},\ a_i\in k,\ v_i \in S\}$$
(all finite linear combinations of elements of S.)
- The elements of S are linearly independent if there are no finite linear relations:
$$a_1v_1+\dots+a_kv_k = 0 \quad (a_i\in k,\ v_i\in S) \Rightarrow a_1=\dots=a_k=0.$$
- S is a basis of V if its elements are linearly indep^t and span V.

Example:
- $\{1,x,x^2,x^3,\dots\}$ is a basis of $k[x]$.
- does $k[[x]]$ have a basis? what is it?

Linear maps:

Def. Let V,W be vector spaces $/k$. A homomorphism of vector spaces, or linear map, $\varphi: V\to W$, is any map that is compatible with the operations:
$$\varphi(u+v) = \varphi(u)+\varphi(v), \quad \varphi(\lambda v) = \lambda\varphi(v) \quad \forall \lambda\in k,\ \forall u,v\in V.$$

Prop: The set of linear maps $V \to W$ is itself a vector space/k, denoted $\mathrm{Hom}(V,W)$.

Proof: Given $\varphi, \psi \in \mathrm{Hom}(V,W)$, $\lambda \in k$, define $\begin{cases} \varphi+\psi \text{ by } (\varphi+\psi)(v) = \varphi(v)+\psi(v) \quad \forall v \in V \\ \lambda\varphi \text{ by } (\lambda\varphi)(v) = \lambda\cdot\varphi(v) \end{cases}$

One can check that
- $\varphi+\psi$ and $\lambda\varphi$ defined in this way are linear maps (so we do have operations $+, \cdot$ on $\mathrm{Hom}(V,W)$)
- these operations on $\mathrm{Hom}(V,W)$ satisfy the axioms of a vector space.

(rather boring, but worth checking if you're not sure!) □

- We'll soon see: if $\dim(V) = n$ and $\dim(W) = m$ then $\dim(\mathrm{Hom}(V,W)) = mn$.
  (in bases for V and W, linear maps become $m\times n$ matrices!)

---

* How does the choice of the field k matter when discussing vector spaces?
  Given a subfield $k' \subset k$ (eg. $\mathbb{R}\subset\mathbb{C}$ or $\mathbb{Q}\subset\mathbb{R}$), a vector space over k can also be viewed as a vector space over k', by "restriction of scalars".
  (namely, only look at scalar multiplication restricted to domain $k'\times V \subset k\times V$).
  In particular, k itself is a vector space over k'!

  Ex: $\mathbb{C}$ is a vector space over itself (of dim. 1, $\{1\}$ is a basis)
  It is also a vector space over $\mathbb{R}$ (of dim 2, with basis $\{1, i\}$)

If V, W are $\mathbb{C}$-vector spaces hence also $\mathbb{R}$-vector spaces, any $\mathbb{C}$-linear map is also $\mathbb{R}$-linear, but the converse isn't true: $\mathrm{Hom}_{\mathbb{C}}(V,W) \subsetneq \mathrm{Hom}_{\mathbb{R}}(V,W)$

For example, complex conjugation $\begin{array}{ccc}\mathbb{C} & \longrightarrow & \mathbb{C} \\ z = a+bi & \longmapsto & \bar{z} = a-bi\end{array}$ is $\mathbb{R}$-linear: $\begin{cases}\overline{z_1+z_2} = \bar{z}_1+\bar{z}_2 \\ \overline{az} = a\bar{z} \ \forall a\in\mathbb{R}\end{cases}$ but not $\mathbb{C}$-linear ($\overline{iz} \neq i\bar{z}$).

So: the choice of field k matters.

Bases and dimension:

* Say V is finite-dimensional if there is a finite subset $\{v_1, .., v_m\}$ which spans V, ie. all elts of V are linear combinations $\sum a_i v_i$.

* **Lemma:** if $\{v_1, .., v_m\}$ spans V, then a subset of $\{v_1 .. v_m\}$ is a basis.

  Proof: If the $\{v_i\}$ are linearly independent, they form a basis.
  Otherwise, there is some linear relation $\sum a_i v_i = 0$, a_i not all zero.
  This can be solved for v_i = a linear combination of the others if $a_i \neq 0$.
  $\to$ remove v_i, $\{v_j \mid j\neq i\}$ still spans V.
  Continue removing elements until the remaining ones are linearly indep^t. □

* Thus, every finite-dimensional vector space has a basis.

* **Lemma:** If $\{v_1, \dots, v_m\}$ are linearly indep^t, there exists a basis of V which contains $\{v_1 \dots v_m\}$

Proof: Let $\{w_1 \dots, w_r\}$ be a spanning set for V. by induction we enlarge $\{v_1, \dots, v_m\}$ to a basis of $W_j = \text{span}(\{v_1, \dots, v_m, w_1, \dots, w_j\}) \subset V$ for each $j = 0, \dots, r$.

For $j=0$: $\{v_1, \dots, v_m\}$ basis of W_0.

Assuming $\{v_1, \dots, v_m, w_{i_1} \dots w_{i_k}\}$ is a basis of $W_{j-1} = \text{span}(\{v_1 \dots v_m, w_1, \dots, w_{j-1}\})$,

if $w_j \in W_{j-1}$ then we already have a basis of $W_j = W_{j-1}$.

otherwise, $\{v_1 \dots v_m, w_{i_1}, \dots, w_{i_k}, w_j\}$ are linearly indep^t. (why?) and span W_j.

This ends with a basis of $W_r = V$ (since $\{w_1, \dots, w_r\}$ span). □

* **Theorem:** If $\{v_1, \dots, v_m\}$ and $\{w_1, \dots, w_n\}$ are bases of V, then $m = n$. (same # elements)

Proof. • We claim $\exists j \in \{1..n\}$ st. $\{v_1, \dots, v_{m-1}, w_j\}$ is a basis.

Indeed, $\{v_1, \dots, v_{m-1}\}$ are linearly independent, but don't span V

(else $v_m \in \text{span}\{v_1 \dots v_{m-1}\}$ gives a linear relation $\sum_{i=1}^{m-1} a_i v_i - v_{m+1} = 0$).

So $\exists j$ st. $w_j \notin \text{span}\{v_1 \dots v_{m-1}\}$ (else $w_1 \dots w_n$ can't span all V).

Now $\{v_1, \dots, v_{m-1}, w_j\}$ are linearly independent (why?),

but using all the v's, can write $w_j = \sum_{i=1}^{m} a_i v_i$ (necess. $a_m \neq 0$)

So $v_m = \frac{1}{a_m}\left(w_j - \sum_{i=1}^{m-1} a_i v_i\right) \in \text{span}(\{v_1 \dots v_{m-1}, w_j\})$

and this implies $\{v_1 \dots v_{m-1}, w_j\}$ span V hence are a basis.

• Repeat this process to exchange one v for one w each time

(we don't use the same w twice since the new w we pick has to be independent of the rest of our basis)

We end up with only w's & get an m-element subset of $\{w_1, \dots, w_n\}$ that is also a basis. Necessarily this is all of $\{w_1 \dots w_n\}$, and $m = n$. □

* **Def:** The <u>dimension</u> of V is the cardinality of any basis.

* Given a basis $(v_1, \dots, v_n)$ of V, we get a linear map $\varphi : k^n \longrightarrow V$
$$(a_1, \dots, a_n) \longmapsto \sum a_i v_i$$

Linear independence $\iff \varphi$ injective

spanning $V \iff \varphi$ surjective , so φ is an isomorphism!

Every finite-dim. vector space $/k$ is isomorphic to k^n for $n = \dim V$.

(+ basis gives a specific <u>choice</u> of such an isomorphism).

* Given bases $(v_1 \dots v_n)$ of V and $(w_1 \dots w_m)$ of W, we can represent a linear map $\varphi \in \text{Hom}(V, W)$ by an $m \times n$ <u>matrix</u> $A \in M_{m,n}$. This amounts to:

$$\begin{tikzcd} V \arrow[r, "\varphi"] & W \\ k^n \arrow[u, "\simeq", "\text{basis}"'] \arrow[r, "A"] & k^m \arrow[u, "\simeq \text{basis}"'] \end{tikzcd}$$

Write $A = (a_{ij})_{\substack{1 \le i \le m \text{ rows} \\ 1 \le j \le n \text{ columns}}} = \begin{pmatrix} a_{11} & \dots & a_{1n} \\ a_{21} & & \\ \vdots & & \\ a_{m1} & \dots & a_{mn} \end{pmatrix}$

$A : k^n \to k^m$ by multiplication w/ column vectors $\begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \mapsto A \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$

<u>Notation</u>: $A = \mathcal{M}(\varphi, (v), (w))$

* The entries of A are characterized by : $\varphi(v_j) = \sum_{i=1}^{m} a_{ij} w_i$.

  Ie: the <u>columns</u> of A give the components of $\varphi(v_1), \dots, \varphi(v_n)$ in the basis $\{w_1, \dots, w_m\}$.

  Representing any element $x \in V$ as $x = \sum_{i=1}^{n} x_i v_i \leftrightarrow$ column vector $X = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$

  and similarly for $y = \varphi(x) \in W$, $y = \sum y_i w_i \leftrightarrow Y = \begin{pmatrix} y_1 \\ \vdots \\ y_m \end{pmatrix} = AX$.

* As a memory aid, the isom. $k^n \xrightarrow{\sim} V$ given by the basis can be written symbolically as multiplication of row & column vectors $\underbrace{(v_1 \dots v_n)}\begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = \sum x_i v_i$.

  ⚠ these aren't numbers !!

$\varphi\big((v_1 \dots v_n) X\big) = (w_1 \dots w_n) AX$.

* This construction gives an isomorphism between the vector spaces $\mathrm{Hom}(V, W)$ and $\mathcal{M}_{m,n}$! In particular $\dim \mathrm{Hom}(V, W) = \dim \mathcal{M}_{m,n} = mn$.

  linear maps $\longleftrightarrow$ matrices

* How do things change if we choose different basis for V and/or W?

  If we change basis from $(v_1 \dots v_n)$ to $(v'_1 \dots v'_n)$, write $v'_j = \sum_{i=1}^{n} p_{ij} v_i$

  and get an $n \times n$ matrix P whose j^{th} column gives the components of v'_j in the basis $(v_1 \dots v_n)$. Symbolically $(v'_1 \dots v'_n) = (v_1 \dots v_n) P$.

  So : $(v'_1 \dots v'_n) X' = (v_1 \dots v_n) PX'$ ie. the element of V described by a column vector X' in new basis is described by $X = PX'$ in old basis.

  More conceptually: $P = \mathcal{M}(\mathrm{id}_V, (v'), (v))$!

  Do the same for W, but proceed in inverse direction, let $Q = \mathcal{M}(\mathrm{id}_W, (w), (w'))$

  ie. $(w_1 \dots w_m) = (w'_1 \dots w'_m) Q$.

Hence: $\varphi\big((v'_1 \dots v'_n) X'\big) = \varphi\big((v_1 \dots v_n) PX'\big) = (w_1 \dots w_m) APX'$

$$= (w'_1 \dots w'_m) QAPX'$$

ie. $\mathcal{M}(\varphi, (v'), (w')) = QAP$.

In particular, if $V = W$ and change basis, for $\varphi \in \mathrm{Hom}(V,V)$,

$$\begin{aligned} A &= \mathcal{M}(\varphi, (v), (v)) \\ A' &= \mathcal{M}(\varphi, (v'), (v')) \end{aligned} \quad \text{are related by } A' = P^{-1}AP.$$

But... the whole point of linear algebra is to <u>avoid all this</u> and work with linear maps in a coordinate-free language as much as possible.

<u>Next up:</u> sums of subspaces, direct sums, dimension formulas.