Math 128B, Mon Mar 15

- Use a laptop or desktop with a large screen so you can read these words clearly.
- In general, please turn off your camera and mute yourself.
- Exception: When we do groupwork, please turn both your camera and mic on. (Groupwork will not be recorded.)
- Please always have the chat window open to ask questions.
- Reading for today: Ch. 19; for Wed: Ch. 20.
- PS05 due tonight; PS06 outline due Wed night.
- Problem session Fri Mar 19, 10am–noon.

Unique factorization in $\mathbf{Z}[x]$

Theorem

Every nonzero non-unit $f(x) \in \mathbf{Z}[x]$ can be written **uniquely** *as*

$$f(x) = b_1 b_2 \cdots b_s p_1(x) p_2(x) \cdots p_m(x),$$

where the b_i are prime integers and the $p_j(x)$ are primitive and irreducible over $\mathbf{Q}$.

As usual, uniqueness is up to associates (i.e., ± 1) and order of the factors.

Why: Follows from two facts of independent interest:

1. The irreducible elements of $\mathbf{Z}[x]$ are prime integers and primitive polynomials that are irreducible over $\mathbf{Q}$.
2. Every irreducible of $\mathbf{Z}[x]$ is prime in $\mathbf{Z}[x]$.

(relies on Gauss' Lemma)

Generalization

Theorem

If D is a UFD, then $D[x]$ is a UFD.

Most notably:

$F[x, y] = (F[x])[y]$ = the ring of polynomials in the variable y, with coefficients in the ring F[x].

UFD so $F[x,y]$ is UFD

(Not PID b/c $\langle x, y \rangle$)

$F[x,y,z] = (F[x,y])[z]$

so UFD.

UFD

By induction, see that we have unique factorization in F[any # of vars].

Linear algebra over F (in one class)

F a field.

Definition

V is a **vector space over** F means:

vector add

- $(V, +)$ is an abelian group;
- For $a \in F$ and $\mathbf{v} \in V$, there exists $a\mathbf{v} \in V$ (scalar mult); and
- For all $a, b \in F$ and $\mathbf{u}, \mathbf{v} \in V$:

DLs

$$a(\mathbf{u}+\mathbf{v}) = a\mathbf{u} + a\mathbf{v} \qquad (a+b)\mathbf{v} = a\mathbf{v} + b\mathbf{v}$$

$$\underbrace{a(b\mathbf{v}) = (ab)\mathbf{v}}_{\text{sc mult assoc}} \qquad 1\mathbf{v} = \mathbf{v}$$

nontriviality

$(1 \in F)$

Examples

$\dim F^n = n$

Example: F^n

$x + y =$ coord. wise

$$V = F^n = \left\{ \begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix} \middle| x_i \in F \right\} \qquad a \begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix} = \begin{bmatrix} ax_1 \\ \vdots \\ ax_n \end{bmatrix}$$

Example: $F[x]$

Vectors: Polynomials with coeffs in F
Vector addition: Addition of polynomials
Scalar multiplication: af(x) is defined as it is in F[x].

$\dim F[x] = \infty$

F[x] satisfies axioms of a v.s. because F[x] is a ring
So F[x] is a v.s. over F.

Basis $\{1, x, x^2, \ldots\}$

Example: F is a subfield of E; aka E is an **extension field** of F.

Vector + in E: Field addition
F-scalar mult: Field multiplication
Axioms satisfied because E is a field and F is a ~~subfield~~ field of E.
So: E is a v.s. over F.

$\boxed{\text{Case: } \mathbb{C} \text{ is v.s. over } \mathbb{R}}$

Subspace, linear combination, span

V a v.s. over F, $\mathbf{v}_1, \ldots, \mathbf{v}_k \in V$.
To say that $U \subseteq V$ is a sub**space** of V means that U is also a v.s. under the operations of V. (There is a subspace test, similar to ideal test.)
A **linear combination** of $\mathbf{v}_1, \ldots, \mathbf{v}_k$ has the form

$$a_1\mathbf{v}_1 + \cdots + a_k\mathbf{v}_k$$

for $a_i \in F$.

(n.) **Span** of $\{\mathbf{v}_1, \ldots, \mathbf{v}_k\}$ is $\langle \underline{v}_1, \ldots, \underline{v}_k \rangle$ $\|$

$$\text{span}\{\mathbf{v}_1, \ldots, \mathbf{v}_k\} = \{a_1\mathbf{v}_1 + \cdots + a_k\mathbf{v}_k \mid a_i \in F\}.$$

cf: ideal generated by....

(v.) To say that $\{\mathbf{v}_1, \ldots, \mathbf{v}_k\}$ **spans** U means:

1. Each of the vectors $\mathbf{v}_1, \ldots, \mathbf{v}_k$ is contained in U.
2. Every $\mathbf{x} \in U$ is a linear combination of $\mathbf{v}_1, \ldots, \mathbf{v}_k$.

I.e. $U = \text{span}\{\underline{v}_1, \ldots, \underline{v}_k\}$

Linear independence, basis, dimension

Ex: $\{\mathbf{0}\}$
lin dep
b/c $1\mathbf{0} = \mathbf{0}$

V a v.s. over F, $\mathbf{v}_1, \ldots, \mathbf{v}_k \in V$.
To say $\{\mathbf{v}_1, \ldots, \mathbf{v}_k\}$ is **linearly dependent** means that

$$a_1\mathbf{v}_1 + \cdots + a_k\mathbf{v}_k = \mathbf{0} \tag{1}$$

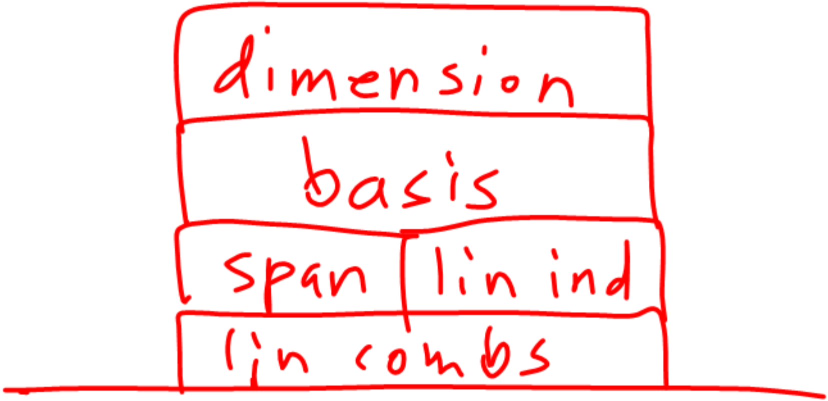
for some choice of $a_1, \ldots, a_k \in F$, not all 0.
Negation: To say that $\{\mathbf{v}_1, \ldots, \mathbf{v}_k\}$ **linearly independent** means that the only time that (1) holds is when all of the a_i are equal to 0. I.e., lin ind means:

If (1), **then** all $a_i = 0$.

A **basis** for V is a linearly independent subset $\{\mathbf{v}_1, \ldots, \mathbf{v}_k\}$ of V that also spans V.

dim $V = k$ means that V has a basis with k vectors in it.

The foundations of linear algebra



Ex. $V = F^n$ Prove: $\dim F^n = n$.

Pf Let $\underline{e}_1 = \begin{bmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{bmatrix}, \underline{e}_2 = \begin{bmatrix} 0 \\ 1 \\ 0 \\ \vdots \end{bmatrix}, \ldots, \underline{e}_n = \begin{bmatrix} 0 \\ \vdots \\ 0 \\ 1 \end{bmatrix}$

$\underline{e}_1 \ldots \underline{e}_n \in F^n$

Span For $\underline{x} \in F^n$,

$$\underline{x} = \begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix} = x_1 \underline{e}_1 + \cdots + x_n \underline{e}_n$$

So {e_i} spans F^n.

Lin ind

(A) $a_1\underline{e}_1 + \cdots + a_n\underline{e}_n = \underline{0}$.

$$\underline{0} = a_1\begin{bmatrix}1\\0\\\vdots\\0\end{bmatrix} + a_2\begin{bmatrix}0\\1\\0\\\vdots\end{bmatrix} + \cdots + a_n\begin{bmatrix}0\\\vdots\\0\\1\end{bmatrix} = \begin{bmatrix}a_1\\a_2\\\vdots\\a_n\end{bmatrix}$$

So

$$\begin{bmatrix}0\\\vdots\\0\end{bmatrix} = \begin{bmatrix}a_1\\\vdots\\a_n\end{bmatrix}$$

(C) $\{\underline{e}_1, \ldots, \underline{e}_n\}$ lin ind

(C) All $a_i = 0$.

So {e_1,..., e_n} is a basis for F^n that contains n vectors.

So by definition, dim (F^n) = n.

$\{v_1 \ldots v_n\}$ span V

$\iff \langle v_1 \ldots v_n \rangle = V$

subspace generated by v_1,...,v_n

Nightmare problem: What if a v.s. has two different dimensions?

How do we know that V can't have both a basis of size 5 and a different basis of size 7?

Theorem

If $\{\mathbf{v}_1, \ldots, \mathbf{v}_s\}$ spans V and $\{\mathbf{w}_1, \ldots, \mathbf{w}_\ell\}$ is linearly independent in V, then $s \geq \ell$.

Proof on PS06.

Theorem

If $\{\mathbf{v}_1, \ldots, \mathbf{v}_n\}$ and $\{\mathbf{w}_1, \ldots, \mathbf{w}_k\}$ are both bases for V, then $n = k$.

Proof:

$\{v_1 \ldots v_n\}$ spans V, $\{\underline{w}_1 \ldots \underline{w}_k\}$ l.i.

so $n \geq k$.

$\{\underline{w}_1, \ldots, \underline{w}_k\}$ spans, $\{\underline{v}_1, \ldots, \underline{v}_n\}$ l.i.

So $k \geq n$.

$\Longrightarrow n = k$

The takeway and a preview

- Anything that satisfies the axioms is a vector space over F.
- Primary case: An extension field of F is a vector space over F.
- If a vector space has a finite basis, then its dimension is well-defined.
- A maximal linearly independent set is a basis (PS06).
- A finite field of characteristic p has $\mathbf{Z}_p$ as a subfield, so is a vector space over $\mathbf{Z}_p$.
- Other extension fields we'll study will be finite-dimensional by construction or by assumption.