

## 1 Vector Spaces

- Reading: Gallian Ch. 19
- Today's main message: linear algebra (as in Math 21) can be done over any field, and most of the results you're familiar with from the case of  $\mathbb{R}$  or  $\mathbb{C}$  carry over.
- **Def:** A *vector space* over a field  $F$  is a set  $V$  with two operations  $+: V \times V \rightarrow V$  (vector addition) and  $\cdot: F \times V \rightarrow V$  (scalar multiplications) that satisfy the following properties:
  1.  $V$  is an abelian group under  $+$ .
  2.  $(ab) \cdot v = a \cdot (b \cdot v)$  for all  $a, b \in F$  and  $v \in V$ .
  3.  $1 \cdot v = v$  for all  $v \in V$ .
  4.  $a \cdot (v + w) = a \cdot v + a \cdot w$  for all  $a \in F$  and  $v, w \in V$ .
  5.  $(a + b) \cdot v = a \cdot v + b \cdot v$  for all  $a, b \in F$  and  $v \in V$ .
- A vector space has more structure than an abelian group, but less structure than a ring (only multiplication by scalars, not multiplication of arbitrary pairs of elements of  $V$ ).
- **Examples and Nonexamples:**
  - $V = F^n$
  - $V = \mathbb{C}, F = \mathbb{R}$
  - $V = \mathbb{Z}^n, F = \mathbb{Z}_2$
  - $V = F[x]$
  - $V = F[x]/\langle p(x) \rangle$
  - $V = R$  for a ring  $R$  containing  $F$ .

- **Def:** Let  $V$  be a vector space over  $F$ . Vectors  $v_1, \dots, v_n \in V$  are *linearly independent* iff for every  $c_1, \dots, c_n \in F$ , if  $c_1v_1 + \dots + c_nv_n = 0$ , then  $c_1 = \dots = c_n = 0$ . The vectors  $v_1, \dots, v_n$  form a *basis* for  $V$  iff they are linearly independent and  $\text{Span}(v_1, \dots, v_n) = V$ , where  $\text{Span}(v_1, \dots, v_n) = \{c_1v_1 + \dots + c_nv_n : c_1, \dots, c_n \in F\}$ .

- **Examples of bases:**

- $(1, 0, 0, \dots, 0), (0, 1, 0, \dots, 0), \dots, (0, 0, 0, \dots, 1)$  is a basis for  $F^n$  for every field  $F$ .
- **Q:** Is  $(1, 1, 0), (1, 0, 1), (0, 1, 1)$  always a basis for  $F^3$ ?
- Bases for other examples above?

- **Def:** The *dimension* of a vector space  $V$  over  $F$  is the size of the largest set of linearly independent vectors in  $V$ . (different than Gallian, but we'll show it to be equivalent)

- A measure of “size” that makes sense even for infinite sets.

- **Prop:** Every finite-dimensional vector space has a basis consisting of  $\dim(V)$  vectors. Later we'll see that all bases have exactly  $\dim(V)$  vectors.

**Proof:** Let  $v_1, \dots, v_k$  be the largest set of linearly independent vectors in  $V$  (so  $k = \dim(V)$ ). To show that this is a basis, we need to show that it spans  $V$ . Let  $w$  be any vector in  $V$ . Since  $v_1, \dots, v_k, w$  has more than  $\dim(V)$  vectors, this set must be linearly dependent, i.e. there exists constants  $c_1, \dots, c_k, d \in F$ , not all zero, such that  $c_1v_1 + \dots + c_kv_k + dw = 0$ . The linear independence of  $v_1, \dots, v_k$  implies that  $d \neq 0$ . Thus, we can write  $w = (c_1/d_1)v_1 + \dots + (c_k/d_k)v_k$ . So every vector in  $V$  is in the span of  $v_1, \dots, v_k$ .

- **Q:** What are the dimensions of the above examples?

- **Corollaries:**

- If  $V$  is an  $n$ -dimensional vector space over a finite field  $F$ , then  $|V| = |F|^n$ .
- If  $E$  is a finite field and  $F$  is a subfield of  $E$ , then  $|E| = |F|^n$  for some  $n \in \mathbb{N}$ . (Much stronger than Lagrange, which only says  $|F|$  divides  $|E|$ .)
- if  $E$  is a finite field of characteristic  $p$ , then  $|E| = p^n$  for some  $n \in \mathbb{N}$ . (Shown on PS7 using Classification of Abelian Groups.)

## 2 Maps Between Vector Spaces

- **Def (vector-space homomorphisms):** Let  $V$  and  $W$  be two vector spaces over  $F$ . A function  $f : V \rightarrow W$  is a *linear map* iff for every  $x, y \in V$  and  $c \in F$ , we have

1.  $f(x + y) = f(x) + f(y)$  (i.e.  $f$  is a group homomorphism), and
2.  $f(cx) = cf(x)$ .

$f$  is an *isomorphism* if  $f$  is also a bijection. If there is an isomorphism between  $V$  and  $W$ , we say that they are *isomorphic* and write  $V \cong W$ .

- **Prop:** Every  $n$ -dimensional vector space  $V$  over  $F$  is isomorphic to  $F^n$ .

**Proof:** Let  $v_1, \dots, v_n$  be a basis for  $V$ .

Then an isomorphism from  $F^n$  to  $V$  is given by:

- **Matrices:** A linear map  $f : F^n \rightarrow F^m$  can be described uniquely by an  $m \times n$  matrix  $M$  with entries from  $F$ .
  - $M_{ij} = f(e_j)_i$ , where  $e_j = (000 \cdots 010 \cdots 00)$  has a 1 in the  $j$ 'th position.
  - For  $v = (v_1, \dots, v_n) \in F^n$ ,  $f(v)_i = f(\sum_j v_j e_j)_i = \sum_j v_j f(e_j)_i = \sum_j M_{ij} v_j = (Mv)_i$ , where  $Mv$  is matrix-vector product.
  - Matrix multiplication  $\leftrightarrow$  composition of linear maps.
  - If  $n = m$ , then  $f$  is an isomorphism  $\Leftrightarrow \det(M) \neq 0$ .
  - Solving  $Mv = w$  for  $v$  (when given  $M$  and  $w \in F^m$ ) is equivalent to solving a linear system with  $m$  variables and  $n$  unknowns.
- **Example:**  $f : \mathbb{Z}_3^3 \rightarrow \mathbb{Z}_2^3$  given by  $f(v_1, v_2, v_3) = (v_1 + 2v_2, 2v_1 + v_3)$ .

- **Thm:** If  $f : V \rightarrow W$  is a linear map, then  $\dim(\ker(f)) + \dim(\text{im}(f)) = \dim(V)$ .

**Proof:** omitted.

- When  $F$  finite, this says  $|V| = |F|^{\dim(V)} = |F|^{\dim(\ker(f))} \cdot |F|^{\dim(\text{im}(f))} = |\ker(f)| \cdot |\text{im}(f)|$ , just like for group homomorphisms!
- **Corollaries:**
  - $F^n \not\cong F^m$  if  $m \neq n$ .
  - All bases of a vector space have the same size.
  - A homogenous linear system  $Mv = 0$  for a given  $m \times n$  matrix  $M$  always has a nonzero solution  $v$  if  $n > m$  (more variables than unknowns).
- **Computational issues:** For  $n \times n$  matrices over  $F$ ,
  - Matrix multiplication can be done with  $O(n^3)$  operations in  $F$  using the standard algorithm.
  - The determinant and inverse, and solving a linear system  $Mv = w$  can be done using  $O(n^3)$  operations in  $F$  using Gaussian elimination. (For infinite fields, need to worry about the size of the numbers, or accuracy if doing approximate arithmetic. No such problem in finite fields.)

- Asymptotically fastest known algorithms run in time  $O(n^{2.376})$ . Whether time  $O(n^2)$  is possible is a long-standing open problem.

### 3 Application to Extension Fields

- Reading: parts of Gallian Ch. 21
- **Def:**  $E$  is an *extension field* of  $F$  if  $F$  is a subfield of  $E$ . The *degree of  $E$  over  $F$*  is the dimension of  $E$  as a vector space over  $F$ , and is denoted  $[E : F]$ .  $E$  is a *finite extension* if  $[E : F]$  is finite.
- **Examples:**
  - $[\mathbb{C} : \mathbb{R}] =$
  - $[F[x]/\langle p(x) \rangle : F] =$
  - $[\mathbb{F}(\alpha) : \mathbb{F}] =$
- **Thm 21.5:** If  $K$  is a finite extension of  $E$ , and  $E$  is a finite extension of  $F$ , then  $[K : F] = [K : E][E : F]$ .
- **Example:** The splitting field of  $x^8 - 1$  over  $\mathbb{Q}$ , i.e.  $\mathbb{Q}(\omega) = \mathbb{Q}(i)(\omega)$ , where  $\omega = e^{2\pi i/8}$ .
- **Proof:**
- **Corollary:** If  $E$  is a finite extension of  $F$  and  $\alpha \in E$ , then  $\alpha$  is algebraic over  $F$  and its minimal polynomial has degree dividing  $[E : F]$ .