AM 106/206: Applied Algebra	**Prof. Salil Vadhan**

Lecture Notes 18

November 25, 2009

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 of vector space.
- **Examples:**
  - F^n
  - $F[x]$
  - Any ring containing F
  - $F[x]/\langle p(x)\rangle$
  - $\mathbb{C}$ a vector space over $\mathbb{R}$
- Def of linear (in)dependence, span, basis.
- **Examples in F^n:**
  - $(1,0,0,\cdots,0)$, $(0,1,0,\ldots,0)$, $\ldots$, $(0,0,0,\ldots,1)$ is a basis for F^n
  - $(1,1,0)$, $(1,0,1)$, $(0,1,1)$ is a basis for F^3 iff F has characteristic 2
- **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.
- **Examples:**
  - F^n has dimension n
  - $F[x]$ has infinite dimension ($1, x, x^2, x^3, \ldots$ are linearly independent)
  - $F[x]/\langle p(x)\rangle$ has dimension $\deg(p)$ (basis is (the cosets of) $1, x, x^2, \ldots, x^{\deg(p)-1}$).
  - $\mathbb{C}$ has dimension 2 over $\mathbb{R}$

- **Proof:** Let $v_1, \ldots, v_k$ 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 $v_1, \ldots, v_k, w$ has more than $\dim(V)$ vectors, this set must be linearly dependent, i.e. there exists constants $c_1, \ldots, c_k, d \in F$, not all zero, such that $c_1 v_1 + \cdots + c_k v_k + dw = 0$. The linear independence of $v_1, \ldots, v_k$ implies that $d \neq 0$. Thus, we can write $w = (c_1/d_1)v_1 + \cdots + (c_k/d_k)v_k$. So every vector in V is in the span of $v_1, \ldots, v_k$.

- **Corollaries:**
  - 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 $n \in \mathbb{N}$.

- **Def (vector-space homomorphisms):** Let V and W be two vector spaces over F. $f : V \to W$ is a *linear map* if for every $x, y \in V$ and $c \in F$, we have $f(x + y) = f(x) + f(y)$ (i.e. f is a group homomorphism) and $f(cx) = cf(x)$. 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 $v_1, \ldots, v_n$ be a basis for V.
  Then an isomorphism from F^n to V is given by: $(c_1, \ldots, c_n) \mapsto \sum_i c_i v_i$. Injective because of linear independence (which says the kernel is $\{0\}$), surjective because $(v_1, \ldots, v_n)$ span.

- **Matrices:** A linear map $f : F^n \to F^m$ 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 $v = (v_1, \ldots, v_n) \in F^n$, $f(v)_i = f(\sum_j v_j e_j)_i = \sum_j v_j f(e_j)_i = \sum_i M_{ij} v_j = (Mv)_i$, 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.

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

- When F finite, this says $|V| = |F|^{\dim(V)} = |F|^{\dim(\ker(f))} \cdot |F|^{\dim(\mathrm{im}(f))} = |\ker(f)| \cdot |\mathrm{im}(f)|$, just like for group homomorphisms!

- **Corollaries:**
  - $F^n \ncong F^m$ if $m \neq n$.
  - All bases of a vector space have the same size.
  - A homogenous linear system $Mv = 0$ for $v \in F^n$ given $m \times n$ matrix M always has a nonzero solution 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.

2 Application to Extension Fields

- Reading: parts of Gallian Ch. 21
- **Def:** E is an *extension field* of F is 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:**
  - $[\mathbb{C} : \mathbb{R}] = 2$
  - $[\mathbb{R} : \mathbb{Q}] = \infty$ (not obvious)
  - $[F[x]/\langle p(x)\rangle : F] = \deg(p)$.
- **Thm 21.5:** If K is a finite extension of E, and E is a finite extension of F, then $[K : F] = [K : E][E : F]$.
- **Proof:**