MATHEMATICS S-152, SUMMER 2005
THE MATHEMATICS OF SYMMETRY

Outline #8 (Linear Algebra over Finite Fields)

References

We review important topics from linear algebra, with an emphasis on vector spaces and matrices defined over finite fields.

Biggs presupposes a knowledge of linear algebra, and so there is no relevant reading from Biggs. You will probably find it useful to consult whatever linear algebra textbook you own or to borrow one from the library.

Linear Algebra over Finite Fields

As a model of an n-dimensional vector space over a field F, consider the vector space $F^n = \{(a_1, \ldots, a_n) | a_i \in F, \forall i\}$. For the case where $F = \mathbb{R}$, this is the vector space $\mathbb{R}^n$, with which you should be well acquainted.

1. State the axioms for a vector space V over an arbitrary field F. These can be found in any textbook on linear algebra, but the book is likely to assume that $F = \mathbb{R}$ (or even to assume that $V = \mathbb{R}^n$, in which case the axioms become provable theorems). You should state them for arbitrary F. There is no need to list all the field axioms for F. To be concise, consolidate the axioms for addition into a single axiom by using the concept of group. Then you will only need to write out two distributive laws, the associative law $(ab)\vec{v} = a(b\vec{v})$, and the axiom that the multiplicative identity 1 in F obeys $1\vec{v} = \vec{v}$.

2. State the definitions of *subspace*, *linear independence*, *span*, *basis*, and *dimension* for an arbitrary finite-dimensional vector space V over F. Do not assume that $V = F^n$, but explain how, once you have found a basis, you can identify V with F^n.

3. Given the finite field $F = \mathbb{F}_q$ with $q = p^k$ elements, what is $|F^n|$, the number of elements of F^n as defined above? How many one-dimensional subspaces of F^n are there? List them for the case where $q = 3$ and $n = 2$.

4. State the definition of a linear transformation $T : V \longrightarrow V$. Explain how, once we have introduced a basis for V, we may represent such a linear transformation by an $n \times n$ matrix A, where $T(\vec{v}) = A\vec{v}$. Review how to act on a vector by a matrix. If we write:

$$\vec{v} = \begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix} \text{ and } A = \begin{bmatrix} a_{11} & \dots & a_{1n} \\ \vdots & & \vdots \\ a_{n1} & \dots & a_{nn} \end{bmatrix},$$

then we define

$$A\vec{v} = \begin{bmatrix} a_{11}x_1 + \cdots + a_{1n}x_n \\ \vdots \\ a_{n1}x_1 + \cdots + a_{nn}x_n \end{bmatrix}.$$

Illustrate this operation with examples when F is a finite field and when $n = 2$. Choose one example where F is the field $\mathbb{Z}_5$ and one where F is the field $\mathbb{F}_4$.

5. Show that the collection of $n \times n$ matrices with entries from the field F, denoted $M_n(F)$, forms a ring with appropriate notions of addition and multiplication. When $F = \mathbb{F}_q$ is a finite field, what is $|M_n(F)|$?

6. State the definitions of the *kernel* and *image* of a linear transformation $T : V \longrightarrow V$ for a vector space V. Using the definition of a linear transformation, show that the kernel and image of T are subspaces of V. (The fact that V can be identified with F^n or that T can be represented by an $n \times n$ matrix is not needed for the proof.)

7. State the definition of the *determinant* of a 2×2 matrix, and state the well-known properties of determinants: If $A, B \in M_n(F)$, then the determinant satisfies

   (a) $\det(AB) = \det(A)\det(B)$

   (b) $\det(A^t) = \det(A)$, where A^t is the transpose of A.

   (c) $\det(A) \neq 0$ if and only if A is invertible.

   Explain why the proof of these results (which you have seen in a previous course for the case of matrices over the field $\mathbb{R}$) depends only on the fact that the entries in the matrix are from a field F. (Don't take the time to write out the proof!).

Illustrate determinants for matrices over a finite field by inventing invertible matrices A and B, where F is the finite field $\mathbb{F}_4$ and $n = 2$. Show that $\det(AB) = \det(A)\det(B)$, construct A^{-1} by the rule taught in elementary linear algebra courses, and show that $\det(A)\det(A^{-1}) = 1$.

8. Given a matrix A, define the notions of the *eigenvalues* and *eigenvectors* of A. Define the *characteristic polynomial* of A,

$$f_A(\lambda) = \det(A - \lambda I),$$

and show that its roots are precisely the eigenvalues of A. Illustrate for the case where F is the finite field $\mathbb{Z}_5$ and when $n = 2$ by finding the eigenvectors and eigenvalues of $\left[\begin{smallmatrix} 3 & 4 \\ 2 & 0 \end{smallmatrix}\right]$

9. Define the *general linear group* of matrices:

$$GL_n(F) = \{A \in M_n(F) | \det(A) \neq 0\}.$$

An alternative notation is $GL(n, F)$.

Show that this is a group. For the case $n = 2$, determine the order of this group when $F = \mathbb{F}_q$ is a finite field by counting the number of possibilities for the top row of the matrix and then the number for the bottom row. Using the same strategy, determine the order of the group when $n = 3$, then generalize the result to arbitrary n. The crucial step is the bottom row for $n = 3$: choosing any linear combination of the top two rows would make the determinant zero.

10. Define the following subset of $GL_n(F)$:

$$SL_n(F) = \{A \in GL_n(F) | \det(A) = 1\}.$$

This is the *special linear group*. An alternative notation is $SL(n, F)$.

Show that $SL(n, F)$ is a subgroup of $GL_n(F)$. Illustrate with examples when F is the finite field $\mathbb{Z}_5$ and when $n = 2$ by exhibiting two matrices (not the identity) in $SL_n(\mathbb{Z}_5)$ and their product. What is the order of this group when $F = \mathbb{F}_q$ is a finite field of order q and when $n = 2$ or $n = 3$?