MATHEMATICS 152, FALL 2003
METHODS IN DISCRETE MATHEMATICS
Outline #8 (Linear Algebra over Finite Fields)

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. You will probably find it useful to consult whatever linear algebra textbook you own.

1. Given any field F, recall the vector space $V = \{(a_1, \ldots, a_n) | a_i \in F, \forall i\}$. This is a vector space of dimension n over F. State the definitions of *subspace*, *linear independence*, *span*, *basis*, and *dimension*.

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

3. State the definition of a linear transformation $T : V \longrightarrow V$. Recall that we may represent such a linear transformation by an $n \times n$ matrix A, where $T(\mathbf{v}) = A\mathbf{v}$. Recall how to act on a vector by a matrix. If we write:

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

   then we define

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

   Illustrate this 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 $\mathbb{F}_4$.

4. 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 $|M_n(F)|$?

5. State the definitions of the *kernel* and *image* of a matrix/linear transformation. Using the definition of a linear transformation, show that the kernel and image are subspaces of V.

6. State the definition of the *determinant* of a 2×2 matrix. If $A, B \in M_n(F)$, then the determinant satisfies the following facts:

   (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 how 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 with examples of A and B when F is the finite field $\mathbb{F}_4$ and when $n = 2$.

7. 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 with examples when F is the finite field $\mathbb{Z}_5$ and when $n = 2$ by finding the eigenvectors and eigenvalues of $\left[\begin{smallmatrix} 3 & 4 \\ 2 & 0 \end{smallmatrix}\right]$

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

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

   Show that, in fact, 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.

9. Define the following subgroup of $GL_n(F)$:

$$SL_n(F) = \{A \in M_n(F) | \det(A) = 1\}, \text{the } \textit{special linear group}$$

   Show that, in fact, this is a group. 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 $n = 3$?