5-3-1994

Review Problems for the Final - 3.

Example. (a) Show that every finite field has order p^n, where p is prime and $n \ge 1$.

Let F be a finite field. The characteristic of F is a prime number p. (For if F has characteristic n, where $n = ab$, $a, b > 1$, then $a, b \in F$, $a, b \ne 0$, but $ab = n = 0$. This is a contradiction, because fields do not have zero divisors.)

It follows that the set $K = \{0, 1, 2, \ldots, p-1\}$ is a subring of F. Since $K \approx \mathbb{Z}_p$, F becomes a $\mathbb{Z}_p$ vector space if I use the addition and multiplication of F to define addition and scalar multiplication of vectors.

Let n be the dimension of F as a $\mathbb{Z}_p$ vector space. Then $F \approx \mathbb{Z}_p^n$, so $|F| = |\mathbb{Z}_p^n|\ p^n$. □

(b) Construct a finite field of order 8.

Since $8 = 2^3$, I'll use $\mathbb{Z}_2$ as my base field. $\mathbb{Z}_2[x]$ is a PID, so $\langle f(x) \rangle \subset \mathbb{Z}_2[x]$ is maximal if and only if $f(x)$ is irreducible. (Proof?) I need an irreducible polynomial of degree 3 in $\mathbb{Z}_2[x]$.

x^3+x+1 has no roots in $\mathbb{Z}_2$. Since a factorization of a cubic must involve a linear factor, and since linear factors correspond to roots, x^3+x+1 is irreducible. Therefore, $\langle x^3+x+1 \rangle$ is maximal, and $\dfrac{\mathbb{Z}_2[x]}{\langle x^3+x+1 \rangle}$ is a field of order 8. □

Example. Let $\{v_1, \ldots, v_k\}$ be vectors in $\mathbb{R}^n$. Let A be the matrix whose rows are the v_i's. Then the volume of the parallelepiped determined by the v_i's is $\sqrt{\det AA^T}$.

First, observe that AA^T is square: If A is a $p \times q$ matrix, then A^T is a $q \times p$ matrix, so AA^T is a $p \times p$ matrix. Therefore, $\det AA^T$ makes sense.

Induct on k. For $k = 1$, I have one vector v_1, and $A = v_1$. Then AA^T is $v_1 v_1^T = |v_1|^2$, and $\det(v_1 v_1^T) = |v_1|^2$.

Let $k > 1$, and assume the result is true for $k - 1$. Here is A:

$$\begin{bmatrix} \leftarrow & v_1 & \rightarrow \\ \leftarrow & v_2 & \rightarrow \\ & \vdots & \\ \leftarrow & v_k & \rightarrow \end{bmatrix}$$

Write

$$v_1 = x + y,$$

where y is in the subspace spanned by $v_2, \ldots, v_k$, and x is perpendicular to $v_2, \ldots, v_k$. (You can obtain such a decomposition by taking y to be the projection into the subspace, then setting $x = v_1 - y$.

Since $y = c_2 v_2 + \cdots + c_k v_k$, I can perform row operations of the form $v_1 \to v_1 - c_i v_i$ on A to reduce A to

$$B = \begin{bmatrix} \leftarrow & x & \rightarrow \\ \leftarrow & v_2 & \rightarrow \\ & \vdots & \\ \leftarrow & v_k & \rightarrow \end{bmatrix}$$

Notice that each such row operation is implemented by multiplication by a matrix of determinant 1. Thus, there is a matrix P of determinant 1 such that $PA = B$.

Now

$$BB^T = (PA)(PA)^T = PAA^TP^T, \quad \text{and} \quad \det BB^T = \det PAA^TP^T = \det AA^T.$$

But

$$BB^T = \begin{bmatrix} \leftarrow & x & \rightarrow \\ \leftarrow & v_2 & \rightarrow \\ & \vdots & \\ \leftarrow & v_k & \rightarrow \end{bmatrix} \begin{bmatrix} \uparrow & \uparrow & & \uparrow \\ x & v_2 & \cdots & v_k \\ \downarrow & \downarrow & & \downarrow \end{bmatrix} = \begin{bmatrix} |x|^2 & 0 \\ 0 & CC^T \end{bmatrix},$$

where

$$C = \begin{bmatrix} \leftarrow & v_2 & \rightarrow \\ & \vdots & \\ \leftarrow & v_k & \rightarrow \end{bmatrix}.$$

So

$$\det BB^T = |x|^2 \cdot (\det CC^T).$$

$|x|$ is the square of the altitude of the parallelepiped determined by the v_i's, and by induction $\det CC^T$ is the square of the area of the base. Hence, $\det BB^T$ is the square of the volume of the parallelepiped determined by the v_i's, and so the same is true for $\det AA^T$. □