Math 55a: Honors Abstract Algebra

Homework Assignment #4 (23 September 2016):
Linear Algebra IV — Duality, and connections with projective spaces and linear algebra with polynomials over finite fields

HINT, *n.*: The hardest of several possible ways to do a proof.[1]

For a vector space V over a field F, the *projective space* $\mathbf{P}V$ is the set of 1-dimensional subspaces of V. These are the "points" of $\mathbf{P}V$; its "lines" are the 2-dimensional subspaces, "planes" the 3-dimensional subspaces, and so on. In particular a "hyperplane" is a subspace of codimension 1. All of these may be regarded as projective spaces in their own right, containing some of the points, lines, etc. of $\mathbf{P}V$. In particular, if $\dim V = 3$ then $\mathbf{P}V$ is called a "projective plane", and likewise a "projective space of dimension n" is $\mathbf{P}V$ with $\dim(V) = n + 1$.

1. i) Show that for any two distinct points in a projective space there is a unique line containing them both, and that any two distinct lines in a projective *plane* meet in a unique point.

   ii) Let $\mathbf{P}V$ be a projective space of dimension n. Its *dual projective space* is $\mathbf{P}(V^*)$. The annihilator gives, for each $d = 0, 1, \ldots, n-1$, a natural bijection between the d-dimensional projective subspaces of $\mathbf{P}V$ and the $(n-1-d)$-dimensional projective subspaces of $\mathbf{P}(V^*)$. Show that this bijection is incidence-reversing: for subspaces U, U' of $\mathbf{P}V$, we have $U \subseteq U'$ if and only if $U^0 \supseteq U'^0$.

   iii) A *polarity* of a finite-dimensional projective space $\mathbf{P}V$ is an isomorphism between $\mathbf{P}V$ and $\mathbf{P}(V^*)$ coming from a linear bijection $V \to V^*$. Composing a polarity with the construction of part (ii), we may associate with each "point" of $\mathbf{P}V$ its polar hyperplane. *If n is odd*, construct a polarity for which each point is in its own polar hyperplane. If $F = \mathbf{R}$, construct a polarity for which no point is in its own polar hyperplane.

We shall see that the parity condition in (iii) is necessary. The properties in (i) characterize the points and lines of a combinatorial projective plane. If F is finite, say $|F| = q$, then each line contains $q + 1$ points and each point is on $q + 1$ lines (why?), giving a "finite projective plane of order q". This construction works whenever q is a prime power. It is conjectured that if q is not a prime power then there is no finite projective plane of order q; but even the existence of a finite projective plane of order 12 is still an unsolved problem. It is known that for some prime powers q there are finite projective planes of order q that are not isomorphic with $\mathbf{P}V$.

2. Suppose F is a finite field of q elements.

   i) For a positive integer n, show that if there exists nonzero $a \in F$ such that $a^n \neq 1$ then $\sum_{x \in F} x^n = 0$. Show that $\sum_{x \in F} x^n = 0$ also holds for $n = 0$ (note that, as was the case for problem 10 on the last problem set, "x^0" is interpreted as 1 even for $x = 0$).

[1] *Definitions of Terms Commonly Used in Higher Math*, R. Glover et al.; cf. also Prob. 2ii.

ii) Deduce that $x^{q-1} = 1$ for all nonzero $x \in F$. [Hint: if $0 < n < q - 1$ then there does exist nonzero $x \in F$ with $x^n = 1$ (why?), so part (i) applies; now use problem 9 of the previous problem set. Yes, there are other proofs of this generalization of "Fermat's little theorem" to arbitrary finite fields.]

3. As a special case of polynomial interpolation (PS2 #5), we can identify $\mathcal{P}_{q-1}$ with F^F by evaluation at all elements of F. This also identifies the dual vector space with F^F (as a special case of the identification with F^S with its own dual when S is a finite set), and thus with $\mathcal{P}_{q-1}$. For $d = 0, 1, 2, \ldots, q - 2$, what is the annihilator of $\mathcal{P}_d$ under this identification? [You should start by unwinding our identifications to see how a polynomial $Q \in \mathcal{P}_{q-1}$ is being considered as a functional on $\mathcal{P}_{q-1}$.]

4. Suppose $P(X_1, \ldots, X_d)$ is a polynomial of total degree $< d$ over some finite field F of characteristic p. Prove that the number of solutions in F^d of $P(X_1, \ldots, X_d) = 0$ is a multiple of p. In particular, if P is homogeneous then there is a nonzero solution.

[A polynomial is an F-linear combination of monomials $\prod_{i=1}^d X_i^{e_i}$; it has degree $< D$ if it is such a linear combination with $\sum_{i=1}^d e_i \leq D$ for each monomial; it is *homogeneous* of degree D if it is a linear combination with $\sum_{i=1}^d e_i = D$ for each monomial. What do you get by summing a monomial over all of F^D? See problem 2.]

Finally, some problems from the textbook. 3.D, *jectivity:

5. Solve Exercises 3.D 1,3,4 (page 88) of Axler. As usual, **F** can be any field (likewise for the remaining problems); for #4, remember that Axler's "null (T)" is our "ker (T)".

6. Solve Exercises 3.D 9,11,12 (page 89) of Axler.

3.E, quotient spaces:

7. Solve Exercises 3.E 16,17 (page 100) of Axler. The second of these should be somewhat familiar.

3.F, duality:

8. Solve Exercises 3.F 22 and 23 (page 114, 115) of Axler. Note that in the first of these there is no assumption of finite dimension.

9. Solve Exercise 3.F 34 on page 116. (In general when a mathematical construction is called a "duality" the double dual should be the original object, or at least closely related to it. Naturally problem 1ii is also an example of this.)