Homework 1

Topics in Finite Fields (Fall 2019)
Rutgers University
Swastik Kopparty
Last modified: Saturday 21st September, 2019

1. Let p, q be primes $\equiv 1 \mod 4$.
   (a) Let W be the set of roots of $X^p - 1$ in some finite extension $\mathbb{F}_Q$ of $\mathbb{F}_q$. Show that there is an element $\omega \in W$ such that $W = \{1, \omega, \omega^2, \ldots, \omega^{p-1}\}$. Such an ω is called a primitive pth root of unity.
   (b) What is the degree of ω over $\mathbb{F}_q$? (i.e. What is the degree of the minimal polynomial of ω over $\mathbb{F}_q$).
   (c) Show that:
   $$\sum_{0 \leq x < p} \omega^x = 0.$$
   (d) Define
   $$S = \sum_{0 \leq x < p} \omega^{x^2}.$$
   Show that $S^2 = p$.
   (e) Show that $S \in \mathbb{F}_q$ iff q is a quadratic residue mod p.
   (f) Conclude that p is a quadratic residue mod q if and only if q is a quadratic residue mod p. Note where the $1 \mod 4$ condition got used.

2. Let $\beta_1, \ldots, \beta_n$ be a basis for $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$. Having chosen a basis, this gives a $\mathbb{F}_q$-vector space isomorphism $\varphi : \mathbb{F}_{q^n} \to \mathbb{F}_q^n$: for $\alpha \in \mathbb{F}_{q^n}$, if $\alpha = \sum c_i \beta_i$, we define:
   $$\varphi(\alpha) = (c_1, \ldots, c_n).$$
   (a) Show that φ is an $\mathbb{F}_q$-linear map.
   (b) For an element $\alpha \in \mathbb{F}_{q^n}$, consider the linear map $M_\alpha : \mathbb{F}_q^n \to \mathbb{F}_q^n$ defined by:
   $$M_\alpha(x) = \varphi(\alpha \cdot \varphi^{-1}(x)),$$
   (where $\cdot$ represents multiplication in $\mathbb{F}_{q^n}$). We also denote by M_α the corresponding $n \times n$ matrix. In words: if you represent elements of $\mathbb{F}_{q^n}$ by vectors in $\mathbb{F}_q^n$, then M_α is the matrix you multiply with when you want to multiply by $\alpha \in \mathbb{F}_{q^n}$.
   (c) Write some equations between the entries of M_α and the basis $b_1, \ldots, b_n$.
   (d) Show that for $a, b \in \mathbb{F}_q$, $\alpha, \beta \in \mathbb{F}_{q^n}$,
   $$aM_\alpha + bM_\beta = M_{a\alpha + b\beta}.$$
   (e) Everything we did above depended on the choice of $b_1, \ldots, b_n$. Suppose we choose a different basis $b'_1, \ldots, b'_n$, and get matrices M'_α for each $\alpha \in \mathbb{F}_{q^n}$.
   Show that there is an invertible matrix U such that for all $\alpha \in \mathbb{F}_{q^n}$,
   $$M'_\alpha = UM_\alpha U^{-1}.$$
   (Recall that two matrices A, B are called similar if $A = UBU^{-1}$ for some invertible matrix U, and that similarity preserves the characteristic polynomial.)

(f) Thus conclude that $\mathsf{Tr}(M'_\alpha) = \mathsf{Tr}(M_\alpha)$, $\det(M'_\alpha) = \det(M_\alpha)$, and the eigenvalues of M'_α and M_α are the same.

3. Pick a basis $b_1, \dots, b_n$ for $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$.

   (a) Let $\alpha \in \mathbb{F}_{q^n}$. Let M_α be the $n \times n$ $\mathbb{F}_q$-matrix which represents multiplication by α (as in the previous problem). What are the eigenvalues of M_α? What is the trace of M_α? What is the determinant of M_α?

   Hints are footnotes[1] [2].

   (b) Let F be the $n \times n$ $\mathbb{F}_q$-matrix that represents the map: $\alpha \mapsto \alpha^q$. What are the eigenvalues of F? What is the trace of F? What is the determinant of F?

   (c) Let $f(n,k)$ be the largest possible dimension of a linear space V of $n \times n$ $\mathbb{F}_q$-matrices such that every nonzero $M \in V$ has rank $\geq n - k + 1$. Show that $f(n,k) = nk$.

   The problem of finding $f(n,k)$ over $\mathbb{R}$ is significantly more difficult. (For $k = 1$, look up Radon-Hurwitz numbers.)

   (d) Show that there exists an $n \times n$ $\mathbb{F}_q$-matrix A and a point $x \in \mathbb{F}_q^n$, such that

   $$\{A^k \cdot x \mid k \geq 0, k \in \mathbb{Z}\} = \mathbb{F}_q^n \setminus \{0\}.$$

   Not for credit: Can you find a real orthogonal matrix A and a point x on the unit sphere of $\mathbb{R}^n$, such that $\{A^k x \mid k \geq 0, k \in \mathbb{Z}\}$ is dense in the unit sphere?

4. Let $\alpha, \beta \in \mathbb{F}_q$. Show that the polynomial $P(X) = X^q - \alpha X - \beta$ is irreducible if and only if $\beta \neq 0$, $\alpha = 1$ and q is prime.

   In the cases where $P(X)$ is reducible, find the degrees of all its irreducible factors.

[1] Hint for one approach: you can choose any basis you like; by the previous problem, the answer does not depend on the choice of basis. Choose a convenient basis that depends on α. It may help to initially assume that α has degree n over $\mathbb{F}_q$.

[2] Hint for another approach: The eigenvalues of M are those $\lambda \in \overline{\mathbb{F}_q}$ for which there exists x with $Mx = \lambda x$. Use the relationship between the entries of M_α and the basis $b_1, \dots, b_n$.