Algebra and Computation (MIT 6.s897) Lecturer: Madhu Sudan
Problem Set 1 Due: Friday, March 6, 2015

Instructions

Goal: The goal of this problem set is to induce some "finite field" thinking. So while it would be great if you can solve the problem without consulting texts, if that makes things better feel free to do so.

Collaboration: Collaboration is allowed, but try to think of the solutions you eventually came up with (possibly collaboratively) in isolation and make sure you understand it (and internalize it).

Writeup: The due date is a recommendation rather than a deadline. It is best if you think of the questions and answers sooner rather than later. The goal of this pset is only to get you to think about potentially weak points in your background. So submission of answers is optional - but I would like to get an email acknowledging that you have thought about the questions and know how to answer them. If you have any questions, email me. If you think you would like to run your solutions by me to verify them or to check if there are alternate solutions, do write them up and send to me by email.

Exercises

1. Prove $\mathbb{F}_q[x]/(g(x))$ is a field of cardinality q^d if and only if g is an irreducible polynomial of degree d.

   Solution: Main thing to do here is to just verify that there are no zero divisors if $g(x)$ is irreducible; and then to count cardinality.

2. Prove that the multiplicative group of the finite field $\mathbb{F}_q$, denoted $\mathbb{F}_q^*$ is cyclic. Conclude that every field has a primitive element.

   Solution: The following shows how you can prove this with some finite field thinking, and truly no counting!

   Let $\mu_n(m)$ denote the number of elements of order m in $\mathbb{Z}_n$ and let $\phi_n(m)$ denote the number of elements of order dividing m in $\mathbb{Z}_n$. If m divides n we have

   $$\phi_n(m) = m \text{ and } \phi_n(m) = \sum_{t|m} \mu_n(t).$$

   We also know that $\mu_n(m) \geq 1$ for every m dividing n (the element n/m has order m).

   (Throughout the below, we will consider m dividing $q-1$.) Now let $\mathbb{F} = \mathbb{F}_q$ be the field of q elements and let $\phi_{\mathbb{F}}(m)$ denote the number of elements of order dividing

m in $\mathbb{F}_q^*$ (th multiplicative subgroup) and let $\mu_{\mathbb{F}}(m)$ denote the number of elements of order exaclty m. We show below that $\mu_{\mathbb{F}}(m) = \mu_{q-1}(m)$ for every m. (This is sufficient since we then have $\mu_{\mathbb{F}}(q-1) \geq 1$.) We do so by noticing that $\phi_{\mathbb{F}}$ and $\mu_{\mathbb{F}}$ satisfy many of the conditions that ϕ_{q-1} and μ_{q-1} do. For instance, we have $\phi_{\mathbb{F}}(m) = \sum_{t|m} \mu_{\mathbb{F}}(t)$. Since every element of order dividing m is a root of the polynomial $x^m - 1$, we have that $\phi_{\mathbb{F}}(m) \leq m = \phi_{q-1}(m)$. Note also that if $\mu_{\mathbb{F}}(m) \geq 1$ then there is an element $\alpha \in \mathbb{F}$ of order m, and so there are at least m elements of order dividing m (all powers of α), and since $\phi_{\mathbb{F}}(m) \leq m$ we have that there are exactly m elements of order dividing m and they form a cyclic subgroup of order m. We conclude that $\mu_{\mathbb{F}}(m) \geq 1$ implies $\mu_{\mathbb{F}}(m) = \mu_{q-1}(m)$, which in turn implies $\mu_{\mathbb{F}}(m) \leq \mu_{q-1}(m)$. But since every non-zero element is a root of $x^{q-1} - 1$ we have $\phi_{\mathbb{F}}(q-1) = q-1$ and so we have $\sum_{t|q-1} \mu_{\mathbb{F}}(t) = \sum_{t|q-1} \mu_{q-1}(t)$. But term by term the left hand side is upper bounded by the right, and so the only way to get equality is if each term on the left equals the corresponding term on the right and so we have $\mu_{\mathbb{F}}(t) = \mu_{q-1}(t)$.

3. If ω is a primitive element in $\mathbb{F}_{q^d}$ then prove that ω is a generator of $\mathbb{F}_{q^d}$ over $\mathbb{F}_q$.

Solution: Recall that $\mathbb{F}_{q^d}$ is a d-dimensional vector space over $\mathbb{F}_q$. Let ω be primitive in $\mathbb{F}_{q^d}$ and consider the elements $1, \omega, \omega^2, \ldots, \omega^d$. Since we have $d+1$ elements here there must be an $\mathbb{F}_q$ relation over them (or else we have a vector space of dimension $d+1$ or larger). But $1, \omega, \ldots, \omega^{d-1}$ must be linearly independent over $\mathbb{F}_q$ or else every power of ω can be expressed in the $\mathbb{F}_q$ span of $1, \omega, \ldots, \omega^{d-2}$ which violates the assumption that there are $q^d - 1$ distinct powers of ω.

4. Let $\alpha \in \mathbb{F}_{q^d}$ have $g \in \mathbb{F}_q[x]$ as it minimal polynomial. Prove that $\mathbb{K} = \mathbb{F}_q[x]/(g)$ is a subfield of $\mathbb{F}_{q^d}$ and so the degree of g divides d.

Solution: Since g is the minimal polynomial it must be irreducible. So we know from Problem 1 that $\mathbb{K}$ is a field of size q^k where k is a degree of g. Since $\mathbb{K}$ is generated by elements of $\mathbb{F}_{q^d}$ it is a subfield of $\mathbb{F}_{q^d}$. Now using the fact that if some field $\mathbb{F}$ extends some field $\mathbb{K}$ then $\mathbb{F}$ forms a vector space over $\mathbb{K}$ and so $|\mathbb{F}| = |\mathbb{K}|^r$, we have that $q^d = |\mathbb{K}|^r$ for some integer r. Using $|\mathbb{K}| = q^k$ we have $d = k \cdot r$ or in other words, k, the degree of g, divides d.

5. Prove the identity $x^q - x = \prod_{a \in \mathbb{F}_q} (x - a)$.

Solution: From the fact that $\mathbb{F}_q[x]$ is a UFD, and the division algorithm, this is equivalent to showing that $a^q = a$ for every $a \in \mathbb{F}_q$ which is equivalent to showing $a^{q-1} = 1$ for every non-zero a, which in turn follows from Lagrange's theorem in group theory.

6. Prove $x^{q^d} - x = \prod_{g \in \mathcal{P}_{q,d}} g(x)$ where

$$\mathcal{P}_{q,d} = \{g \in \mathbb{F}_q[x] | g \text{ irreducible, monic, with } \deg(g) | d\}.$$

Solution: Consider a irreducible polynomial g of degree k dividing d. Consider the field $\mathbb{K} = \mathbb{F}_q[x]/(g(x))$. Note that for every $\alpha \in \mathbb{K}$ we have $\alpha^{q^k} = \alpha$ and hence $\alpha^{q^d} = \alpha$ (since k divides d). We conclude that for every polynomial $p(x) \in \mathbb{F}_q[x]$ we have $p(x)^{q^d} = p(x) \pmod{g(x)}$. In particular we have this for the polynomial $p(x) = x$ from which we get $x^{q^d} = x \pmod{g(x)}$ or equivalently $g(x)$ divides $x^{q^d} - x$. We conclude that the polynomial on the right hand side divides the one on the left.

To prove the reverse direction, first consider any irreducible monic polynomial h dividing $x^{q^d} - x$. Since all roots of $x^{q^d} - x$ are in $\mathbb{F}_{q^d}$ (Problem 5), h has a root $\alpha \in \mathbb{F}_{q^d}$ and so h is a minimal polynomial of α. By Problem 4 we have that h is of degree dividing d. Thus all irreducible factors of $x^{q^d} - x$ appear in the polynomial on the right. It only remains to note that $x^{q^d} - x$ has no repeated factors and this is immediate since its derivative is the constant polynomial -1 which has no common factors with $x^{q^d} - x$.

7. Prove that if $g \in \mathbb{F}_q[x]$ is irreducible of degree d, then it splits completely in $\mathbb{F}_{q^d}$. (In class we claimed that g has a root in $\mathbb{F}_q[x]/(g)$, and if one combines this with the assertion that fields of cardinality q^d are unique then it follows that $\mathbb{F}_{q^d}$ has a root of $g(x)$. But the way to prove the uniqueness is by proving that g has a root in $\mathbb{F}_{q^d}$.)

   Solution: By Problem 6 we have that $g(x)$ divides $x^{q^d} - x$, and by Problem 5, we have that $x^{q^d} - x$ splits into linear factors over $\mathbb{F}_{q^d}$. It follows that $g(x)$ splits into linear factors over $\mathbb{F}_{q^d}$.

8. Prove that there is a unique field of any given cardinality: In particular suppose $g \in \mathbb{F}_p[x]$ is irreducible of degree $a \cdot b$ and $h \in \mathbb{F}_{p^a}[x]$ is irreducible of degree b. Then prove that $\mathbb{F}_p[x]/(g(x)) \cong \mathbb{F}_{p^a}[x]/(h(x))$.

   Solution: Let $q = p^a$ and let $\mathbb{K}$ be any field of cardinality q^b. Note that it suffices to show that $\mathbb{F}_q[x]/(h(x)) \cong \mathbb{K}$. By Problem 7, h has a root in $\alpha \in \mathbb{K}$. It can be verified that the map ϕ that maps $p(x)$ to $p(\alpha)$ is a bijection among polynomials of degree less than b and preserves addition and multiplication modulo h.

9. Write down the full details of the reduction alluded to in the beginning of Lecture 7 reducing factorization of a polynomial $f \in \mathbb{F}_q[x]$ with all irreducible factors having degree d, to root finding in $\mathbb{F}_{q^d}$.

Solution: TBD