Abstract Algebra in Theoretical Computer Science

Assignment 3

Lecturer: Gil Cohen

Problem 1 - The multplicative group of a finite field is cyclic

In this question, you are going to prove that the multiplicative group of the nonzero elements of a finite field is cyclic. First, we will need to prove a neat group theoretic lemma.

1. Let G be a finite abelian group. Let $m = \max_{g \in G} o(g)$ be the maximal order of elements in G. Prove that $o(g) \mid m$ for every $g \in G$.

2. Let $\mathbb{F}$ be a finite field. Let G be the multiplicative group of the nonzero elements in $\mathbb{F}$. Prove that G is cyclic.

Problem 2 - The ideal generaged by leading terms of polynomials

Let R be an integral domain. For $0 \neq f(x) \in R[x]$ let $\mathrm{LT}(f)$ be the coefficient of the term $x^{\deg(f)}$ in f, that is, $\mathrm{LT}(f)$ is the coefficient of the leading term of f. Let J be an ideal in $R[x]$. Prove that

$$I = \{\mathrm{LT}(f) \mid f \in J \setminus \{0\}\} \cup \{0\}$$

is an ideal in R.

Problem 3 - Double quotient, just for fun!

Let $\mathbb{F}$ be a field and $A = \mathbb{F}[x, y, z]$. Define J to be the ideal in A that is generated by $xy - z^2$, that is, $J = (xy - z^2)A$. Denote $R = A/J$. Let I be the ideal in R that is generated by $x + J$ and $z + J$, that is, $I = (x + J)R + (z + J)R$. Prove that the ring R/I is isomorphic to $\mathbb{F}[w]$.

Problem 4 - Taking the quotient with respect to an irreducible polynomial

Let $m, r > 1$ be integers. Define $R = \mathbb{Z}_m[x]/\langle x^r - 1\rangle$.

1. Prove that R is *not* an integral domain.

2. Prove that for every integer t, the element x^t is not a zero divisor.

Problem 5 - Algebraically closed fields cannot be finite

A field $\mathbb{F}$ is said to be *algebraically closed* if for every $f(x) \in \mathbb{F}[x]$ of positive degree there exists $a \in \mathbb{F}$ such that $f(a) = 0$. Prove that an algebraically closed field cannot be finite.

Problem 6 - Playing with the field of 16 elements and $\mathbb{F}_2^4$

In this question we are going to construct the field of 16 elements in two ways (just because we can!) and use the field to define multiplication between vectors - an extremely useful technique!

1. Prove that $x^4 + x + 1 \in \mathbb{F}_2[x]$ is irreducible. Describe the field of 16 elements as a quotient using this polynomial. We denote this field by $\mathbb{F}_{16}$.

We would like to use the field of 16 elements constructed above, $\mathbb{F}_{16}$, in order to define a multiplication of vectors in $\mathbb{F}_2^4$. To this end we identify the field $\mathbb{F}_{16}$ with the vector space $\mathbb{F}_2^4$ in the following way. Consider the map $m : \mathbb{F}_2^4 \to \mathbb{F}_{16}$ that maps a vector $v = (a, b, c, d) \in \mathbb{F}_2^4$ to the field element $m(v) = a + bx + cx^2 + dx^3$.

2. Prove that m is a bijective $\mathbb{F}_2$-linear map. That is, m is a bijection and $m(\alpha u + \beta v) = \alpha m(u) + \beta m(v)$ for all $u, v \in \mathbb{F}_2^4$ and $\alpha, \beta \in \mathbb{F}_2$ (note that we think of $\mathbb{F}_2$ as a subfield of $\mathbb{F}_{16}$).

We denote m's inverse by $m^{-1} : \mathbb{F}_{16} \to \mathbb{F}_2^4$. Given vectors $u, v \in \mathbb{F}_2^4$ we define $uv \in \mathbb{F}_2^4$ by

$$uv = m^{-1}(m(u)m(v)).$$

That is, informally, we think of u, v as field elements (via the map m), multiply in the field and then transform the result back to a vector.

3. Express the four coordinates of v^3 as a function of a, b, c, d. Before doing so, guess what will be the degree of each coordiante as a polynomial in a, b, c, d. Did you guess right? If not, find an explanation for the answer.

We now turn to give a second construction of a field with 16 elements.

4. We saw that $x^2 + x + 1 \in \mathbb{F}_2[x]$ is irreducible and so $\mathbb{F}_2[x]/\langle x^2 + x + 1\rangle$ is a field with 4 elements. Prove that

$$y^2 + y + x \in \left(\mathbb{F}_2[x]/\langle x^2 + x + 1\rangle\right)[y]$$

is irreducible, where we identify $\mathbb{F}_2[x]$ as a subring of $\mathbb{F}_2[x]/\langle x^2 + x + 1\rangle$ (and so we write x for $x + \langle x^2 + x + 1\rangle$, etc). From this, obtain a second description for the field of 16 elements.

5. Find a generator for the multiplicative cyclic group of the field that you constructed in the previous item.

Problem 7 - A magic trick

- Let K/F be a field extension. Assume that $a, b \in K$ are two algebraic elements over F. Prove that $a+b$ is also algerbaic over F. Hint: what you *shouldn't* try to do is to take the minimal polynomials $f(x), g(x) \in F[x]$ of a and b, respectively, and try to "cook up" from them a new polynomial whose root is $a + b$. The magic is that there is a far simpler, though non-constructive way, of proving that $a + b$ is algebraic over F. Hint^2: prove that $[F(a)(b) : F(a)] < \infty$.

- Let K/F be a field extension. Define L to be the set of all $a \in K$ such that a is algebraic over F. Prove that L is a field.

Problem 8 - Repeated root and derivatives

Let F be a field and $f(x) \in F[x]$. Prove that $f(x)$ has a repeated root (in some field extension of F) if and only if $\langle f(x) \rangle + \langle f'(x) \rangle \neq \langle 1 \rangle$.

Problem 9 - Yet another neat fact about polynomials

Let F be a field, and $f(x), p(x) \in F[x]$ such that $p(x)$ is irreducible. Assume that $f(x), p(x)$ have a common root in some field extension of F. Prove that $p(x)|f(x)$ in $F[x]$.