Algebraic Geometry for Theoretical Computer Science

Assignment 2

Lecturer: Gil Cohen *Hand in date: November 13, 2014*

Instructions: Please write your solutions in LaTeX / Word or exquisite handwriting. Submission can be done individually or in pairs.

1. In this exercise we consider a special and important class of codes known as *cyclic codes*. This will give us a good opportunity to practice some notions from algebra since, as we'll see, cyclic codes are related to ideals in a certain ring. A code $C \subseteq \mathbb{F}_q^n$ is said to be cyclic if whenever $(c_0, \ldots, c_{n-1}) \in C$, it also holds that $(c_{n-1}, c_0, \ldots, c_{n-2}) \in C$. Let $R_n = \mathbb{F}_q[x]/(x^n - 1)$. We think of elements of R_n as polynomials of degree at most $n-1$, where multiplication is done as usual except that we identify x^n with 1.

   For a code C we define
   $$I_C = \{c_0 + c_1 x + \cdots + c_{n-1}x^{n-1} \mid (c_0, c_1, \ldots, c_{n-1}) \in C\}.$$

   (a) Prove that R_n is a ring.

   (b) Prove that if C is a cyclic code then I_C is an ideal of R_n.

   (c) Let I be an ideal of R_n and let $g(x) \in I$ be a monic polynomial of minimal degree $\deg g = d$. Prove that $g(x)$ is the unique monic polynomial in I with degree d.

   (d) Prove that $I = (g(x))$.

   (e) Prove that $g(x)$ divides $x^n - 1$ as an element of $\mathbb{F}_q[x]$.

   (f) Assume $I = I_C$ for some cyclic code C. Prove that $\dim(C) = n - d$, where d is as defined above.

   (g) Find all cyclic codes of $\mathbb{F}_2^7$ with dimension 4. Hint:
   $$x^7 - 1 = (x+1)(x^3+x+1)(x^3+x^2+1).$$

2. (a) Let F be a field. Let $\mathcal{O} \subsetneq F$ be a ring that contains 1, with the following property: for any $z \in F$, at least one of z, z^{-1} is contained in $\mathcal{O}$. Let $P = \{z \in \mathcal{O} \mid z^{-1} \notin \mathcal{O}\}$. Prove that P is the unique maximal ideal of $\mathcal{O}$. (A ring with a unique maximal ideal is called a *local ring*.)

   (b) Let k be a field, and $k(x)$ be the field of rational functions on x. For $\alpha \in k$, define the set
   $$\mathcal{O}_\alpha = \left\{ \frac{f}{g} \;\middle|\; f, g \in k[x] \text{ are relatively prime, and } g(\alpha) \neq 0 \right\} \subset k(x).$$

   Prove that $\mathcal{O}_\alpha$ satisfies the condition from the previous item.

(c) What is the unique maximal ideal associated with $\mathcal{O}_\alpha$? Denote this ideal by P_α.

(d) To which field the quotient field $\mathcal{O}_\alpha/P_\alpha$ is isomorphic to? *Hint: consider the mapping $\varphi : \mathcal{O}_\alpha \to k$, defined by $\varphi(z) = z(\alpha)$. That is, φ is the evaluation mapping at point α. Identify* $\ker(\varphi)$*, and apply the first homomorphism theorem.*