Sheet 6: Finite Fields

Robert Kropholler

April 7, 2019

1. Let $\mathbb{F}_2$ be the field with 2 elements.
   (a) Show that $x^3 + x + 1$ is irreducible in $\mathbb{F}_2[x]$.
   (b) Consider the field $\mathbb{F}_2(\alpha) = \mathbb{F}_2[x]/(x^3 + x + 1)$, where α is the image of x in $\mathbb{F}_2[x]/(x^3 + x + 1)$. Write down the 8 elements of this field in terms of α.
   (c) Write the multiplication table for $\mathbb{F}_8^\times$.
   (d) Find a generator for $\mathbb{F}_8^\times$.
2. Let L be the splitting field of $x^{p^n} - x$ over $\mathbb{F}_p$. Recall that $[L : \mathbb{F}_p] = n$. Let $g(x) \in \mathbb{F}_p[x]$ be irreducible and divide $x^{p^n} - x$.

   Show that $\deg g(x)$ divides n.

   (Hint: Consider the intermediate field extension where $g(x)$ has a root.)
3. (a) Show that the polynomial $x^{q^n} - x$ does not split over $\mathbb{F}_q$.
   (b) Deduce that for all q, the field $\mathbb{F}_q$ is not algebraically closed.
   (c) Deduce that any algebraically closed field is infinite.
4. Let p be an odd prime. Let $q = p^n$ for some integer $n > 1$.
   (a) Using the fact that $\mathbb{F}_q^\times$ is cyclic or otherwise. Show that there are $\dfrac{q-1}{2}$ non-zero elements in $\mathbb{F}_q$ which are squares.
   (b) Deduce that $S = \{s^2 \mid s \in \mathbb{F}_q\}$ has $\dfrac{q+1}{2}$ elements.
   (c) Let $a \in \mathbb{F}_q$ and $T = \{a - x \mid x \in S\}$. Show that $T \cap S$ is non-empty.
   (d) Deduce that $a = x^2 + y^2$ for some $x, y \in \mathbb{F}_q$.