Math 521 – Homework 9

Due Thursday, November 7, 2019 at 10:15am

Problem 1. Consider the field $K = \mathbb{Q}(\sqrt{5}, \sqrt{7})$.

(a) Show that $x^2 - 7$ is irreducible in $\mathbb{Q}(\sqrt{5})[x]$.

(b) What is $[K : \mathbb{Q}]$?

(c) Find the minimal polynomial for $\sqrt{5} + \sqrt{7}$ over $\mathbb{Q}$.

Problem 2. Let p be prime and suppose that $f(x) \in \mathbb{F}_p[x]$ is an irreducible polynomial of degree n and let $K = \mathbb{F}_p[x]/\langle f(x)\rangle$.

(a) How many elements belong to K?

(b) Show that for every $\alpha \in K^*$, the minimal polynomial of α over $\mathbb{F}_p$ divides $x^N - 1$ where $N = p^n - 1$.

(c) Show that $\varphi : K \to K$ given by $\varphi(\alpha) = \alpha^p$ is an automorphism of the ring K.

(d) Show that for $\alpha \in K^*$, the roots of the minimal polynomial $m_{\alpha,\mathbb{F}_p}(x)$ are $\alpha, \alpha^p, \alpha^{p^2}, \dots, \alpha^{p^d}$ where $d = \deg(m_{\alpha,\mathbb{F}_p}(x))$.

Problem 3. Let $f(x) = x^3 + x + 1 \in \mathbb{F}_2[x]$ and $K = \mathbb{F}_2[\alpha]/\langle f(\alpha)\rangle$.

(a) Show that f is irreducible in $\mathbb{F}_2[x]$.

(b) Find a cyclic generator for the group K^*.

(c) Find multiplicative inverse for $\alpha^2 + \alpha$.

(d) Find the minimal polynomial over $\mathbb{F}_2$ for every element in K^*.

(e) Write down a matrix representing the $\mathbb{F}_2$-linear map $K \to K$ given by multiplication by α with respect to the basis $\{1, \alpha, \alpha^2\}$ of K over $\mathbb{F}_2$.