Problem Set 10

Due Thursday, April 9

Instructions: You are encouraged to work together on these problems, but each student should hand in their own final draft, written in a way that indicates their individual understanding of the solutions. Never submit something for grading that you do not completely understand. You cannot use any resources besides me, your classmates, and our course notes.

I will post the .tex code for these problems for you to use if you wish to type your homework. If you prefer not to type, please *write neatly*. As a matter of good proof writing style, please use complete sentences and correct grammar. You may use any result stated or proven in class or in a homework problem, provided you reference it appropriately by either stating the result or stating its name (e.g. the definition of ring or Lagrange's Theorem). Please do not refer to theorems by their number in the course notes, as that can change.

Problem 1. Classification of finite fields:

(a) Let F be a finite field; i.e., a field with finitely many elements. Show that $|F| = p^n$ for some prime number p and integer $n \geq 1$.

(b) Let p be a prime number and $n \geq 1$. Show that the polynomial $f(x) = x^{p^n} - x$ has p^n distinct roots in $\overline{\mathbb{F}_p}$, and that the set of roots of f in $\overline{\mathbb{F}_p}$ forms a subfield of $\overline{\mathbb{F}_p}$. Deduce that there exists a field with p^n elements.

(c) Show that[1] if K is any field with p^n elements, then K is a splitting field for $f(x) = x^{p^n} - x$ over $\mathbb{F}_p$. Deduce that all fields with p^n elements are isomorphic.

Problem 2. Let L be the splitting field of $f = x^5 - 11 \in \mathbb{Q}[x]$.

(a) Find the degree of $[L : \mathbb{Q}]$.

(b) Let $F = \mathbb{Q}(\xi)$, where $\xi = e^{\frac{2\pi i}{5}}$ is a primitive 5th root of unity. Show that f is irreducible over F.

Problem 3. Let F be a field and let $f \in F[x]$.

(a) Assume $\mathrm{char}(F) = 0$. Prove that f is not separable if and only if the prime factorization of f in $F[x]$ admits a repeated factor.

(b) Give a counterexample to the previous part when the assumption $\mathrm{char}(F) = 0$ is omitted.

Problem 4. Let $F \subseteq L$ is a field extension and $S \subseteq L$. Show that

$$F(S) = \left\{ \frac{f(s_1, \ldots, s_t)}{g(s_1, \ldots, s_t)} \;\middle|\; t \geq 0,\ s_1, \ldots, s_t \in S,\ f(x_1, \ldots, x_t), g(x_1, \ldots, x_t) \in F[x_1, \ldots, x_t],\ g(s_1, \ldots, s_t) \neq 0 \right\}.$$

[1] Hint: Show the stronger claim that every element of K is a root of $f(x)$. You might find it helpful to recall something you proved earlier about the group $K^\times$.