Problem Set 11

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, our course notes, and the textbook.

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). Do not refer to theorems by their number in the course notes or textbook.

Problem 1. Let n be a positive integer and let p be a prime integer. Let $q(x) = x^{p^n} - x \in (\mathbb{Z}/p)[x]$, and let K be the splitting field of q over $\mathbb{Z}/p$.

a) Show that the subset $E \subseteq K$ consisting of all roots of q in K is a subfield of K.

b) Show that $|E| = p^n$ and $E = K$.

c) Let L be any field with $|L| = p^n$, and let F be the prime field of L. Show that $F \cong \mathbb{Z}/p$ and that L is the splitting field of the polynomial $q_F(x) = x^{p^n} - x \in F[x]$ over F.

   Hint: Consider the multiplicative group $(L^\times, \cdot)$.

d) Show that any two fields of order p^n are isomorphic.

Problem 2. Show that every algebraic field extension of a finite field is separable.

Problem 3. Assume F is field and let $f \in F[x]$.

a) Assume $\operatorname{char}(F) = 0$. 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 $\operatorname{char}(F) = 0$ is omitted.

Problem 4. 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 5. Let F be a field, let $a_1, \ldots, a_n$ be elements of an extension of F, and $L = F(a_1, \ldots, a_n)$.

a) Show that

$$F(a_1, \ldots, a_n) = \left\{ \frac{f(a_1, \ldots, a_n)}{g(a_1, \ldots, a_n)} \mid f, g \in F[x_1, \ldots, x_n], g \neq 0 \right\}.$$

b) Let

$$F[a_1, \ldots, a_n] := \{ f(a_1, \ldots, a_n) \mid f \in F[x_1, \ldots, x_n] \}.$$

   Prove that if $a_1, \ldots, a_n$ are algebraic over F, then $L = F[a_1, \ldots, a_n]$.

c) Prove that if $\sigma \in \mathrm{Aut}(L/F)$ and $f \in L[x_1, \ldots, x_n]$, then

$$\sigma(f(a_1, \ldots, a_n)) = f^\sigma(\sigma(a_1), \ldots, \sigma(a_n)),$$

where f^σ denotes the polynomial obtained from f by applying σ to its coefficients and leaving the variables unchanged.

d) Assume that $a_1, \ldots, a_n$ are algebraic over F. Prove that if $\sigma \in \mathrm{Aut}(L/F)$, then σ is uniquely determined by $\sigma(a_1), \ldots, \sigma(a_n)$.