PROBLEM SET NINE: DUE MIDNIGHT ON MARCH 29

See the course website for homework policies.

Problem 1. Remember to go to plan an hour to go to Gradescope and do Practice QR Exam 7.

Problem 2. Please write up the proofs of three of **16.3**, **17.1**, **17.2**, **18.5**, **19.3**.

Problem 3. Let $f(x) = 1+8x-16x^2-8x^3+16x^4$. You may trust me that $f(x)$ is irreducible and its roots are $\cos\frac{2\pi}{15}$, $\cos\frac{4\pi}{15}$, $\cos\frac{8\pi}{15}$, $\cos\frac{16\pi}{15}$. Let L be the splitting field of f. Show that $\mathrm{Aut}(L/\mathbb{Q}) \cong C_4$.

Problem 4. Let L be the splitting field of x^4-2 over $\mathbb{Q}$. In this problem, we will show that $\mathrm{Aut}(L/\mathbb{Q})$ is the dihedral group of 8 elements, which we can think of as acting on the square:

$$\begin{array}{ccc} \sqrt[4]{2} & \text{———} & i\sqrt[4]{2} \\ | & & | \\ -i\sqrt[4]{2} & \text{———} & -\sqrt[4]{2} \end{array}$$

(1) Show that $\mathrm{Aut}(L/\mathbb{Q})$, thought of as a permutation group on $\{\sqrt[4]{2}, i\sqrt[4]{2}, -\sqrt[4]{2}, -i\sqrt[4]{2}\}$ is contained in the group of the symmetries of the square above.
(2) Show that $\#\,\mathrm{Aut}(L/\mathbb{Q}) = 8$.

Problem 5. In this problem, we will prove a result which I have promised many times: The group of units modulo p is cyclic. Actually, we will prove a stronger result: If K is a field and A is a finite subgroup of $K^\times$, then A is cyclic.

(1) Let A and K be as above and let n be any positive integer. Show that there are at most n solutions to $a^n = 1$ in A.
(2) Conclude that A is cyclic.

Problem 6. Let n be a positive integer. Let F be a field in which $n \neq 0$ and let K be the splitting field of $x^n - 1$ over F.

(1) Show that $\mathrm{Aut}(K/F)$ is isomorphic to a subgroup of $(\mathbb{Z}/n\mathbb{Z})^\times$.
(2) We specialize to the case where $n = p$ is a prime. Show that $\mathrm{Aut}(K/F) = (\mathbb{Z}/p\mathbb{Z})^\times$ if and only if $1 + x + x^2 + \cdots + x^{p-1}$ is irreducible over F.

Problem 7. Let n be a positive integer. Let K be a field in which $n \neq 0$ and $x^n - 1$ splits. Let a be a nonzero element of K and let L be a splitting field of $x^n - a$ over L. Show that $\mathrm{Aut}(L/K)$ is isomorphic to a subgroup of $\mathbb{Z}/n\mathbb{Z}$.

Problem 8. Let p be a prime integer and let q be a power of p.

(1) Let K be any field of characteristic p. Show that the set of roots of the equation $x^q - x$ in K forms a subfield of K.
(2) Define $\mathbb{F}_q$ to be the splitting field of $x^q - x$ over $\mathbb{F}_p$. Show that there are q elements in $\mathbb{F}_q$.

Problem 9. Let F be a finite field with q elements.

(1) Show that there is a prime integer p such that $\overbrace{1 + 1 + \cdots + 1}^{p \text{ times}} = 0$ in F.
(2) Show that $q = p^n$ for some n.
(3) Show that, for each element x of F, we have $x^q = x$. (Hint: You'll want to handle the case $x = 0$ separately from $x \neq 0$.)
(4) Show that F is the field $\mathbb{F}_q$ of the previous problem.