MATH 81/111: RINGS AND FIELDS
HOMEWORK #7

Problem 7.1. Let $n \in \mathbb{Z}_{\geq 2}$. Let F be a field with $\operatorname{char} F \nmid n$ in which $X^n - 1$ splits. Let $a \in F^\times$ and let $f(X) = X^n - a \in F[X]$. Let K be a splitting field for f and let $\alpha \in K$ be a root of F. Show that the following are equivalent:

(a) $f \in F[X]$ is irreducible;
(b) $a \notin F^{\times d}$ for all $d \mid n$ with $d > 1$; and
(c) n is the smallest positive integer such that $\alpha^n \in F$.

[Hint: Inspiration for a direct proof is in Exercise 2.6. A Galois-theoretic proof is given on page 71, but you will need to unpack this argument.]

Problem 7.2. Let K/F be a finite cyclic extension with $\operatorname{Gal}(K/F) = \langle \sigma \rangle \cong \mathbb{Z}/n\mathbb{Z}$. Define the map

$$\begin{aligned} \operatorname{Tr} : K &\to F \\ \alpha &\mapsto \sum_{i=0}^{n} \sigma^i(\alpha) = \alpha + \sigma(\alpha) + \cdots + \sigma^{n-1}(\alpha). \end{aligned}$$

Let $\alpha \in K$ (and check that indeed $\operatorname{Tr}(\alpha) \in F$). Give two proofs of the additive version of Hilbert's Theorem 90:

$$\operatorname{Tr}(\alpha) = 0 \text{ if and only if there exists } \beta \in K \text{ such that } \alpha = \beta - \sigma(\beta).$$

First, argue directly with Dedekind's linear independence of characters. Then rephrase this by proving (in a similar way) that $H^1(G, K) = \{0\}$ and deducing the result from this.

Problem 7.3 (M5-2). Apply Hilbert's Theorem 90 to the extension $\mathbb{Q}(i)/\mathbb{Q}$ to prove that the rational solutions $x, y \in \mathbb{Q}$ of the Pythagorean equation $x^2 + y^2 = 1$ are of the form

$$x = \frac{s^2 - t^2}{s^2 + t^2}, \quad y = \frac{2st}{s^2 + t^2}, \quad s, t \in \mathbb{Q}.$$

Deduce that a right triangle each with sides $a, b, c \in \mathbb{Z}$ with $\gcd(a, b, c) = 1$ and $a, b < c$ has

$$a, b = m^2 - n^2, 2mn \quad \text{and} \quad c = m^2 + n^2$$

with $m, n \in \mathbb{Z}$. What is the smallest such triple (a, b, c) you have not seen before?

Problem 7.4. Show that the polynomial $f(X) = X^5 + 11X + 11$ is not solvable by radicals over $\mathbb{Q}$, i.e., the roots of f cannot be expressed in terms of radicals, with as nice an argument as possible.

Problem 7.5. Let F an infinite field and let K be an algebraic extension of F (possibly infinite degree over F). Show that $\#F = \#K$, i.e., F and K have the same cardinalities as sets.

Date: 18 February 2015; due Wednesday, 25 February 2015.