Problem Set #6: Field Theory II

1. (a) Let G be a cyclic group of order g, and let $n > 0$ be a divisor of g. Prove that the set
$$\{x \in G \mid x^n = e\}$$
is the unique subgroup of order n in G. (Here e denotes the identity in G.)

   (b) Let $F = F_q$ be a finite field of cardinality $|F| = q$, and let n be a positive integer relatively prime to q. Prove that a field K with $F \subset K$ contains a splitting field L (over F) of the polynomial $X^n - 1$ if and only if n divides $|K| - 1$; and deduce that the degree $[L : F]$ is the order of q in the multiplicative group of units of $\mathbb{Z}/(n)$.

   (c) Factor the polynomial $X^{12} - 1 \in F_5[X]$ into irreducibles.

2. Let k be a field and $k(X)$ the field of fractions of the polynomial ring $k[X]$. Let f and g be the unique automorphisms of $k(X)$ fixing k and such that
$$f(X) = 1/X, \quad g(X) = 1 - X.$$
In the group of all automorphisms of $k(X)$, let G be the subgroup generated by f and g.

   (a) Write down explicitly all elements of G.

   (b) Show that the fixed field of G is $k(Y)$, where
$$Y = (X^2 - X + 1)^3/(X^2 - X)^2.$$

   (c) If $k(Y) \subset L \subset k(X)$ is a sequence of proper inclusions of fields with $L/k(Y)$ a normal field extension, then $L = k(Z)$ where
$$Z = X + (1 - 1/X) + \frac{1}{1 - X}.$$

3. Let k be a field of characteristic zero. Assume that every polynomial in $k[X]$ of odd degree and every polynomial in $k[X]$ of degree two has a root in k. Show that k is algebraically closed.

4. Let $n \geq 1$ an integer, F a field. Show that
$$x^n + y^n + z^n$$
is irreducible in $F[x, y, z]$ if and only if $n \in F^\times$.

5. Let K be a field and let G be a finite group acting on K by field automorphisms. Denote by
$$F := \{x \in K \mid gx = x, \forall\, g \in G\}$$
the fixed field of G.

(a) Show that if an irreducible polynomial $f \in F[x]$ has a root in K, then it factors into linear terms in $K[x]$.

(b) Suppose now that K is a subfield of the algebraic numbers $\bar{\mathbb{Q}}$. Use part (a) to show that every automorphism in $\mathrm{Aut}(\bar{\mathbb{Q}}/F)$ stabilizes K.

(c) Find a counterexample to (b) in the following sense: find some tower of extensions

$$\begin{array}{c} L \\ | \\ K \\ | \\ F \end{array} \tag{1}$$

and an element of $\mathrm{Aut}(L/F)$ that does not stabilize K.