Math 422/501: Problem set 8 (due 4/11/09)

Monomorphisms of fields

1. (From class)
   (a) Let L/K be a finite extension and $\sigma \in \mathrm{Hom}_K(L,L)$. Show that σ is an automorphism.
   (b) Let L/K be an algebraic extension and $\sigma \in \mathrm{Hom}_K(L,L)$. Show that σ is an automorphism.
   (c) Give an example showing there exist extensions with endomorphisms which are not automorphisms.

2. Let $\varphi : \mathbb{R} \to \mathbb{R}$ be a homomorphism of rings. Show that φ is the identity map.

3. (The Frobenius map) Let K be a field of characteristic $p > 0$
   (a) Show that the map $x \mapsto x^p$ defines a monomorphism $K \to K$.
   (b) Conclude by induction that the same holds for the map $x \mapsto x^{p^r}$ for any $r \geq 1$.
   (c) When K is finite show that the Frobenius map is an automorphism.
   OPT When $K = \bar{\mathbb{F}}_p$ show that the Frobenius map is again an automorphism, and obtain a group homomorphism $\mathbb{Z} \mapsto \mathrm{Gal}(\bar{\mathbb{F}}_p : \mathbb{F}_p)$.
   FACT The image of this homomorphism is dense.

4. (The Galois correspondence for $K = \mathbb{Q}(\sqrt{2}, \sqrt{3})$).
   (a) Find all $\mathbb{Q}$-automorphisms of K and give their group structure.
   (b) Find all subfields of K.
   (c) Show that the map $H \mapsto \mathrm{Fix}(H)$ gives a bijection between subgroups of the automorphism group and subfields of K.

Finite fields

5. (Multiplicative groups)
   (a) Let G be a finite p-group such that for every d, $\left|\left\{g \in G \mid g^d = e\right\}\right| \leq d$. Show that G is cyclic.
   (b) Let G be a finite group such that for every d, $\left|\left\{g \in G \mid g^d = e\right\}\right| \leq d$. Show that G is cyclic.
   (c) Let F be a field, $G \subset F^\times$ a finite group. Show that G is cyclic.

6. (Uniqueness of finite fields) Fix a prime p and let $q = p^r$ for some $r \geq 1$.
   (a) Show that the polynomial $x^q - x \in \mathbb{F}_p[x]$ is separable.
   (b) Let F be a finite field with q elements. Show that F is a splitting field for $x^q - x$ over $\mathbb{F}_p$.
   (c) Conclude that for each q there is at most one isomorphism class of fields of order q. If such a field exists it is denoted $\mathbb{F}_q$.

7. (Existence of finite fields) Fix a prime p and let $q = p^r$ for some $r \geq 1$.
   (a) Let $F/\mathbb{F}_p$ be a splitting field for $x^q - x$, and let $\sigma\colon F \to F$ be the map $\sigma(x) = x^q$. Show that the fixed field of σ is also a splitting field.
   (b) Conclude that the field F has order q.

8. Let F be a finite field, K/F a finite extension.
   (a) Show that the extension K/F is normal and separable.
   Hint: 7(a).
   (b) Show that there exists $\alpha \in K$ so that $K = F(\alpha)$.
   Hint: Consider the group $K^\times$.

Optional – Finite fields

A. (Galois correspondence for finite fields) Fix a prime p.
   (a) Assume that $\mathbb{F}_{p^r}$ embeds in $\mathbb{F}_{p^k}$. Show that $r|k$.
   (b) Let $r|k$. Show that $\mathbb{F}_{p^k}$ has a unique subfield isomorphic to $\mathbb{F}_{p^r}$, consisting of the fixed points of the map $x \mapsto x^{p^r}$.
   (c) Show that $\mathrm{Gal}(\mathbb{F}_{p^k} : \mathbb{F}_{p^r})$ is cyclic and generated by the Frobenius map $x \mapsto x^{p^r}$.
   (d) Obtain the Galois correspondence for extensions of finite fields.