Lior Silberman's Math 501: Problem Set 5 (due 16/10/2020)

Finite fields

1. (The Frobenius map) Let K be a field of characteristic $p > 0$.
   (a) Show that the map $x \mapsto x^p$ defines a monomorphism $K \to K$ fixing the prime field.
   (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.
   (*d) When K is an arbitrary algebraic extension of $\mathbb{F}_p$ show that the Frobenius map is again an automorphism.
   FACT We obtain a group homomorphism $\mathbb{Z} \to \mathrm{Gal}(\bar{\mathbb{F}}_p : \mathbb{F}_p)$. We will later show that the image of this homomorphism is dense.

2. (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 multiplicative subgroup. Show that G is cyclic.

3. (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 $\mathbb{F}_q$.

4. (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 polynomial also splits in the fixed field of σ.
   (b) Conclude that the field F has order q.

5. Let F be a finite field, K/F a finite extension.
   (a) Show that the extension K/F is normal and separable.
   (b) Show that the extension is *simple*: there exists $\alpha \in K$ so that $K = F(\alpha)$.

Simple extensions

*6. Let $K(\alpha) : K$ be a simple extension.
   (a) If α is algebraic, show that there are finitely many subfields M of $K(\alpha)$ containing K.
   Hint: consider the minimal polynomial of α over M.
   (b) If α is transcendental, show that there are infinitely many intermediate fields M.

7. Let $L : K$ be an extension of fields with finitely many intermediate subfields.
   (a) Show that the extension is algebraic.
   (b) Show that the extension is *finitely generated*: there exists a finite subset $S \subset L$ so that $L = K(S)$.
   (c) Show that the extension is finite.

**8. Let $L : K$ be an extension of infinite fields with finitely many intermediate fields. Show that it is a simple algebraic extension.
   RMK We will later show that every separable extension satisfies the hypothesis. For finite fields see 5(b).

Supplementary problem: Algebraicity and algebraic closures

A. Let $L : K$ be an extension of fields
   (a) Let $\alpha \in L$. Show that α is algebraic if and only if there a subset $E \subset L$ such that: (1) E is a subspace of L, thought of as a K-vectorspace; (2) $\alpha E \subset E$.
   (b) Obtain a new proof of Corollary 111 as follows: if $\alpha, \beta \in L$ stabilize $E, F \subset L$ respectively, then the required elements stabilizer an image of $E \otimes_K F$ in L, which is necessarily finite-dimensional.

B. Let $M : L$ and $L : K$ be algebraic extensions of fields. Show that $M : K$ is algebraic.

DEFINITION. A field extension $K \hookrightarrow \bar{K}$ is called an *algebraic closure* if it is algebraic, and if every polynomial in $K[x]$ splits in $\bar{K}[x]$. We also say informally that $\bar{K}$ is an *algebraic closure of* K.

RMK The following problems depend on basic notions from set theory: cardinality and Zorn's Lemma.

C. Let $K \hookrightarrow L$ be an algebraic extension.
   (a) If K is finite, show that $|L| \leq \aleph_0$.
   (b) If K is infinite, show that $|L| = |K|$.

D. Let $K \hookrightarrow \bar{K}$ be an algebraic closure. Show that every algebraic extension of $\bar{K}$ is an isomorphism of fields.

E. (Existence of algebraic closures) Let K be a field, X an infinite set containing K with $|X| > |K|$. Let $0, 1$ denote these elements of $K \subset X$. Let

$$\mathcal{F} = \{(L, +, \cdot) \mid K \subset L \subset X,\ (L, 0, 1, +, \cdot) \text{ is a field with } K \subset L \text{ an algebraic extension}\}\ .$$

   Note that we are assuming that restricting $+, \cdot$ to K gives the field operations of K.

   (a) Show that $\mathcal{F}$ is a set. Note that $\{(\varphi, L) \mid L \text{ is a field and } \varphi\colon K \to L \text{ is an algebraic extension}\}$ is not a set.
   (b) Show that every algebraic extension of K is isomorphic to an element of $\mathcal{F}$.
   (c) Given $(L, +, \cdot)$ and $(L', +', \cdot') \in \mathcal{F}$ say that $(L, +, \cdot) \leq (L', +', \cdot')$ if $L \subseteq L'$, $+ \subseteq +'$, $\cdot \subseteq \cdot'$. Show that this is a transitive relation.
   (d) Let $\bar{K} \in \mathcal{F}$ be maximal with respect to this order. Show that $\bar{K}$ is an algebraic closure of K.
   (e) Show that K has algebraic closures.

F. (Uniqueness of algebraic closures) Let $K \hookrightarrow \bar{K}$ and $K \hookrightarrow L$ be two algebraic closures of K. Show that the two extensions are isomorphic.
   Hint: Let $\mathcal{G}$ be the set of K-embeddings intermediate subfields $K \subset M \subset L$ into $\bar{K}$, ordered by inclusion.