Lior Silberman's Math 501: Problem Set 10 (due 27/11/2020)

Algebraic closures

Fix a field K.

1. (Existence) Let R_d be the set of irreducible monic polynomials $f \in K[x]$ of degree d. For each $f \in R_d$ let $\{t_{f,i}\}_{i=1}^{d}$ be variables and let $T = \bigcup_{d\geq 2} \{t_{f,i} \mid f \in R_d, 1 \leq i \leq d\}$. For $f \in R_d$ with $f = \sum_{k=0}^{d} a_k x^k$ and $1 \leq k \leq d$ set $p_{f,k} = (-1)^k s_k (t_{f,1}, \ldots, t_{f,d}) - a_{d-k}$ where s_k are the elementary symmetric polynomials, and let $I \lhd K[T]$ be the ideal generated by the $p_{f,k}$.
   (a) Show that I is a proper ideal.
   Hint: if $1 \in I$ then we'd have $1 = \sum_{m=1}^{M} q_m p_{f_m, j_m}$ for some $q_m \in K[T]$. Exploit the finiteness of this expression.
   (b) Let $\mathfrak{m} \lhd K[T]$ be a maximal ideal containing I (it exists by the arguments of the previous problem set). Show that every $f \in K[x]$ splits in the field $K[T]/\mathfrak{m}$.
   (c) Show that $K[T]/\mathfrak{m}$ is an algebraic closure of K.Fix a ring R.

2. (Uniqueness) Let $K \hookrightarrow \bar{K}$ and $K \hookrightarrow \bar{K}'$ be two algebraic closures of K. Let $\mathcal{F}$ be the set of functions ρ such that the domain of ρ is a subfield M_ρ of $\bar{K}$ containing K and such that $\rho\colon M_\rho \to \bar{K}'$ is a K-monomorphism.
   (a) Show that $\mathcal{F}$ is closed under unions of chains.
   (b) Show that a maximal element of $\mathcal{F}$ is an isomorphism $\bar{K} \to \bar{K}'$.

*3. Let L, L' be algebraically closed extensions of K, and suppose that $\operatorname{tr}\deg_K L = \operatorname{tr}\deg_K L'$. Show that $L \simeq L'$.

*4. Let L be an algebraically closed extension of K, and let $E \subset L$ be a transcendence basis.
   (a) Let $\sigma \in S_E$ be an arbitrary permutation. Show that σ extends to an K-automorphism of L.
   (b) Show that the group $\{\rho \in \operatorname{Aut}_K(L) \mid \rho(E) = E\}$ surjects on S_E.

OPT This problem is for those who know some set theory.
   (a) Let K be an infinite field. Show that K and $\bar{K}$ have the same cardinality.
   (b) Suppose that either K or T are infinite. Show that $|K(T)| = \max\{|K|, |T|\}$.
   (c) Show that $\overline{\mathbb{F}_p}$ is countable and that if K, T are finite then $K(T)$ is countable.
   (d) Show that $\operatorname{tr}\deg \mathbb{C} = |\mathbb{C}| = \aleph$.
   (e) Show that $|S_\aleph| = \aleph^\aleph = 2^\aleph$. Conclude that $|\operatorname{Aut}(\mathbb{C})| = |\operatorname{Aut}_{\mathbb{Q}}(\mathbb{C})| = 2^\aleph$.

Supplementary problem: semigroup and group rings

Fix a ring R.

A. (Free R-modules). Let R be a ring, and let S be a set. The set $R^S = \{f : S \to R\}$ is naturally an R-module. Recall that the support of $f \in R^S$ is the set $\{s \in S \mid f(s) \neq 0\}$.
   (a) Show that $R^{\oplus S} = \left\{f \in R^S \mid \mathrm{supp}(S) \text{ is finite}\right\}$ is a submodule of R^S.
   (b) Identifying $s \in S$ with the indicator function $e_s(t) = \begin{cases} 1 & t = s \\ 0 & t \neq s \end{cases}$ show that S is a generating set of $R^{\oplus S}$, in other words that the smallest R-submodule of $R^{\oplus S}$ containing S is $R^{\oplus S}$ itself.
   (c) Show that $R^{\oplus S}$ is free on S: for any R-module M, any function $\phi : S \to M$ extends uniquely to a homomorphism $\phi \in \mathrm{Hom}_R\left(R^{\oplus S}, M\right)$.Prince Albert in a can

B. A semigroup is a pair $(S, \cdot)$ where S is a non-empty set and $\cdot : S \times S \to S$ is an associative operation. Examples include $(\mathbb{Z}_{\geq 0}, +)$ and $(\mathbb{Z}_{\geq 1}, \times)$, and of course any group is a semigroup.
   DEF Let $R[S] = \left(R^{\oplus S}, +, \cdot\right)$ where $+$ is the addition in $R^{\oplus S}$ and for $f, g \in R^{\oplus S}$ we set
$$(f \cdot g)(s) = \sum_{\substack{r,t \in S \\ rt = s}} f(r) g(t)\,.$$
   (a) Show that the sum in the definition of multiplication is, in fact, finite (i.e. has only finitely many non-zero summands).
   (b) Show that $R[S]$ is an R-algebra: it is an R-module and a ring (possibly non-commutative and without identity) in a compatible fashion. We call $R[S]$ the semigroup ring.
   (c) Show that $R[S]$ is commutative or unital (has an identity element) i S has the same property.
   (d) Show that $R[S]$ has the following universal property: for any R-algebra A, any multiplicative map $\phi : S \to A$ ($f(st) = f(s)f(t)$) extends uniquely to an R-algebra homomorphism $\phi : R[S] \to A$.
   (e) A representation of S (over R) is an R-module M equipped with an action of S by R-module homomorphisms. Construct an equivalence of categories $\{\text{representations of } S\} \leftrightarrow \{R[S]\text{-modules}\}$.

C. (The ring of polynomials and field of rational functions)
   (a) Let T be a set disjoint from R. Show that $E = \{\alpha : T \to \mathbb{Z}_{\geq 0} \mid \#\,\mathrm{supp}(\alpha) < \infty\}$ (the "exponents") is a commutative semigroup with identity element 0.
   (b) Identifying $t \in T$ with the corresponding indicator function, so that E is a free commutative unital semigroup: for any commutative semigroup S, any function $\phi : T \to S$ extends uniquely to a multiplicative map $\phi : E \to S$.
   DEF The polynomial ring $R[T]$ is the semigroup ring $R[E]$.
   (c) Show that $R[T]$ is a free commutative unital R-algebra: for any commutative unital R-algebra A, any function $\phi : T \to A$ extends uniquely to an R-algebra homomorphism $\phi : R[T] \to A$.
   (Hint: combine C(b) and B(d)).
   (d) Show that $T \mapsto R[T]$ is a functor $\{\text{Sets}\} \to \{R\text{-algebras}\}$ mapping injections to injections.
   (e) If $S \subset T$ we often identify $R[S]$ with its image in $R[T]$. Show that
$$R[T] = \bigcup_{\text{finite } S \subset T} R[S]\,.$$
   RMK For the categorical meaning of (e) look up "direct limits".
   (f) Show that $R[T]$ is an integral domain whenever R is.
   DEF When R is an integral domain let k be its fraction field, and write $R(T)$ or $k(T)$ for the field of fractions of $R[T]$, the field of rational functions.

D. (Power series make sense too)
   (a) Call a semigroup S locally finite if for any $s \in S$ the set $\{(r, t) \in S \times S \mid rt = s\}$ is finite. For a locally finite semigroup define a semigroup power series ring $R[[S]]$ by replacing $R^{\oplus S}$ with R^S in the definition of $R[S]$. Show that $R[[S]]$ is indeed a ring.
   (b) In particular show that E of C(a) is locally finite. We write $R[[T]]$ for the resulting ring of power series.

Supplementary problems: Existence of algebraic closures

The idea of this proof of the existence of algebraic closures is the most direct, but the proof is more complicated to bring about.

E. 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 $|L| = |K|$.

F. (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

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

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

   (a) Show that $\mathcal{G}$ 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 $(L', +', \cdot') \in \mathcal{G}$ say that $(L, +, \cdot) \leq (L', +', \cdot')$ if $L \subseteq L'$, $+ \subseteq +'$, $\cdot \subseteq \cdot'$. Show that this is a transitive relation.
   (d) Let $\mathcal{C} \subset \mathcal{G}$ be a chain. Find an element $(L, +, \cdot) \in \mathcal{G}$ which is an upper bound for the chain (in the sense of part (c))
   Hint: morally speaking you need to take the union.

   FACT A more general of Zorn's Lemma shows that $\mathcal{F}$ now has maximal elements with respect to this order.

   (e) Let $\bar{K} \in \mathcal{F}$ be maximal with respect to this order. Show that $\bar{K}$ is an algebraic closure of K.