Math 6020 / Problem Set 12 (three pages)

Compositum of fields

- Recall that given subextension \( L'|K, L''|K \rightarrow L|K \) of a field extension \( L|K \), the subfield of \( L \) generated by \( L', L'' \) is the (internal) compositum of \( L' \) and \( L'' \) and denoted \( L' \cdot L'' \) or simply \( L'L'' \). Obviously, \( L'L''|K \) is the smallest (w.r.t. inclusion \( \subset \)) subextension of \( L|K \) which contains contains \( L'|K \) and \( L''|K \) (WHY). Defining the external or free compositum of two field extensions \( L|K \), which would be the coproduct in the category of \( K \)-field extensions, is not always possible, see below. Here is an approach to try to do that: Recall that given a commutative ring \( R \), the coproduct in the category of \( R \)-algebras is defined. (Namely, if \( R(\Sigma) \) denotes the free \( R \)-algebra on a set \( \Sigma \), one has: If \( \Sigma', \Sigma'' \) are systems of generators of \( S', S'' \), then \( S' = R(\Sigma')/I' \) for some ideal \( I' \subset R(\Sigma') \) (WHY), and similarly for \( S'' \). Then setting \( \Sigma := \Sigma' \sqcup \Sigma'' \) in \( \text{Set} \), one has \( S' \sqcup R S'' = R(\Sigma)/I \) with \( I \subset R(\Sigma) \) is the ideal generated by \( I', I'' \) under the canonical embeddings \( R(\Sigma') \rightarrow R(\Sigma) \) (WHY).

Correspondingly in the category of commutative \( R \)-algebras, one replaces \( R(\Sigma) \) by its commutative variant, namely the polynomial ring \( R[\Sigma] \) on a set of “variables” \( \Sigma \), etc. The coproduct in the category of commutative \( R \)-algebras is denoted \( S' \otimes_R S'' \) and is called the \( R \)-tensor product of \( S', S'' \) with \( S' \rightarrow S' \otimes_R 1_{S''}, S'' \rightarrow 1_{S'} \otimes_R S'' \) as structure \( R \)-morphisms.

Finally, let \( L'|K \) and \( L''|K \) be \( K \)-field extensions. Then working in the category of commutative \( K \)-algebras, one has that \( S := L' \otimes_K L'' \) is a commutative \( K \)-algebra and the structure morphisms \( L' \rightarrow L' \otimes_K 1_{L''}, L'' \rightarrow 1_{L'} \otimes_K L'' \) are injective (WHY), and one identifies \( L', L'' \) with their images \( L' \otimes_K 1_{L''}, 1_{L'} \otimes_K L'' \) inside \( S \). OTOH, in general, \( S \) is not a field and there is no canonical way to attach a field extension \( L|K \) to \( S \) which together with structure morphisms \( L'|K, L''|K \rightarrow L|K \) would satisfy the coproduct universal property(...)

Terminology. If \( L' \sqcup K L'' \) exists, it is called the external/free coproduct of \( L'|K \) and \( L''|K \).

1) In the above notation, give examples of separable finite extensions \( L'|K, L''|K \) for \( K = \mathbb{Q} \), to show that \( L' \sqcup K L'' \) in the category of \( K \)-field extensions does not exist.

[Hint: What about \( K = \mathbb{Q} \) and \( L' = \mathbb{Q}[\sqrt{2}] = L'', \) etc...]

2) In the above notation, let \( S := L' \otimes_K L'' \). Prove/disprove/answer the following:
   a) One has group embeddings \( \text{Aut}_K(L') \times \text{Aut}_K(L'') \rightarrow \text{Aut}_K(S), \text{Aut}_K(L') \rightarrow \text{Aut}_{L''}(S) \) (HOW).
   b) If \( L'|K \) is an algebraic normal extension, then all \( \mathfrak{P} \in \text{Spec}(S) \) are maximal.
   c) \( \text{Aut}_K(L') \) acts transitively on \( \text{Spec}(S) \) under the embedding \( \text{Aut}_K(L') \rightarrow \text{Aut}_{L''}(S) \).

Conclude: If \( L'|K \) is normal, the \( K \)-isomorphism type of \( L_{\mathfrak{P}} := S/\mathfrak{P} \) does not depend on \( \mathfrak{P} \), hence the external field compositum \( L_{\mathfrak{P}} = L' \cdot L'' \) is well defined up to \( K \)-isomorphism.

[Hint to a: Use the universal property of coproduct, etc...To b): Using Zorn’s Lemma, reduce to the case where \( L' = K_{p(t)} \) is the splitting field of an irreducible \( p(t) \), etc...To c): Last resort, Google it!]

3) In the above notion, suppose that \( L'|K \) is regular, i.e., \( L' \otimes_K \overline{K} \) is a field, thus in particular, \( L := L' \sqcup K \overline{K} = L' \otimes_K \overline{K} \) exists, hence \( L|K \) is field extension (WHY).
   a) Prove that the coproduct \( L' \sqcup K L'' \) of \( L'|K \) with any field extension \( L''|K \) exists.
   b) Does the converse hold, i.e., if \( L' \sqcup K L'' \) exists for all \( L''|K \), must \( L'|K \) be regular?
Algebraic field extensions/Galois theory

- Let $L | K$ be a finite Galois extension with Galois group $G(L|K)$, and recall the notations from the class: $\mathcal{F}(L|K) = \{ L' | L' \text{ subextension of } L | K \}$, $\mathcal{G}(L|K) = \operatorname{Sg}(G(L|K))$, and $\operatorname{gal} : \mathcal{F}(L|K) \to \mathcal{G}(L|K)$, $L' | K \mapsto G(L|L')$ be the Galois correspondence.

4) Prove in all detail the assertions from the class:
   a) $\operatorname{gal}(L' \cdot L'' | K) \to \operatorname{gal}(L' | K) \cap \operatorname{gal}(L'' | K) = G(L|L') \cap \operatorname{gal}(L|L'').$
   b) $\operatorname{gal}(L' \cap L'' | K) \to \langle \operatorname{gal}(L' | K), \operatorname{gal}(L'' | K) \rangle = \langle G(L|L'), G(L|L'') \rangle$.
   c) If $M'|M, M''|K \in \mathcal{F}(L|K)$ are Galois subextensions of $L|K$, then $M = M' \cdot M''$ and $M_0 = M' \cap M''$ are Galois subextensions on $L|K$. What are the Galois groups?

5) Let $f(t) \in K[t]$ of degree $d = \deg(f) > 0$ and $K_{f(t)} \subset K$ be the splitting field of $f(t)$ in some algebraic closure $\overline{K}|K$. Prove/disprove the following:
   a) $\operatorname{Aut}_K(K_{f(t)})$ acts transitively on the roots of $f(t)$ iff $f(t)$ is irreducible.
   b) There is an “almost canonical” embedding $\operatorname{Aut}(K_{f(t)}|K) \hookrightarrow S_d$ (HOW).
   c) For $f(t) = t^8 - 2$, describe $\operatorname{Aut}_K(K_{f(t)})$ $\hookrightarrow S_8$ in the cases:
      (i) $K = \mathbb{Q}$.  (ii) $K = \mathbb{Q}(\sqrt{2})$.  (iii) $K = \mathbb{Q}(i)$.

Recall that for a prime number $p$, we denoted $\Sigma_0 = \{ p \}$, $\Sigma_1 = \{ p^i \mid p^i|(p - 1) \}$, $\Sigma_2 = \ldots$ and finally, $\Sigma_p = \bigcup_k \Sigma_k$. Can you give an upper bound for $|\Sigma_p|$ in terms of $p$?

6) Complete the proof of the following assertions from the class:
   a) Let $n = p_1^{e_1} \ldots p_r^{e_r}$. Then $\mu_n$ is solvable by radicals iff each $\mu_{p_i}$ is solvable by radicals.
   b) If $\operatorname{char}(K) \notin \Sigma_p$, then $\mu_p$ is solvable by radicals over $K$.
   c) Prove/disprove: $\forall p \not\exists q \neq p$ prime s.t. $\mu_q$ is not solvable by radicals over $\mathbb{F}_p$.

Trace and Norm

- Let $L|K$ be a finite field extension. For $x \in K[t]$, let $p_x(t) = \text{Mipo}_K(x) \in K[t]$ be the minimal polynomial of $x$. Then setting $p_x(t) = t^n + a_{n-1}t^{n-1} + \ldots + a_1t + a_0$, we define: $\operatorname{Tr}_K(x) := -a_{n-1}$, the absolute trace, and $\operatorname{N}_K(x) := (-1)^n a_0$, the absolute norm of $x$ over $K$.

Note: Since $\text{Mipo}_K(x)$ depends in an essential way of $K$, so do $\operatorname{Tr}_K(x)$ and $\operatorname{N}_K(x)$. Finally, if $d_x := [L : K(x)]$, we define the relative trace $\operatorname{Tr}_{L/K}(x) := d_x \operatorname{Tr}_K(x)$ and the relative norm $\operatorname{N}_{L/K}(x) := N_K(x)^{d_x}$ of $x$ over $L|K$. Finally, recall that for $L|K$ we denoted the set of $K$-embeddings $\phi : L \to \overline{K}$ by $\mathcal{S}_{L|K}$. Recall that one has $|\mathcal{S}_{L|L_{\text{sep}}} | = 1$ (WHY) and further:

$\mathcal{S}_{L|K} \to \mathcal{S}_{L_{\text{sep}}|K}$, $\phi \mapsto \phi_{\text{sep}} = \phi|_{L_{\text{sep}}}$ is bijective (WHY) and $|\mathcal{S}_{L|K}| = [L_{\text{sep}}:K] = |\mathcal{S}_{L_{\text{sep}}|K}|$ (WHY).

7) Let $\mathcal{S}_x := S_K(x|K)$, $d_x^i := [K(x) : K(x)_{\text{sep}}]$, and $d_{j_{L|K}}^i := [L : L_{\text{sep}}]$. Prove the following:
   a) $\operatorname{Tr}_K(x) = d_x^i \sum_{\phi_x \in \mathcal{S}_x} \phi_x(x)$ and $\operatorname{N}_K(x) := \prod_{\phi_x \in \mathcal{S}_x} \phi_x(x)^{d_x^i}$.
   b) $\operatorname{Tr}_{L|K}(x) = d_{L_{j_{L|K}}}^i \sum_{\phi_x \in \mathcal{S}_{L_{j_{L|K}}}} \phi(x)$ and $\operatorname{N}_{L|K}(x) := \prod_{\phi \in \mathcal{S}_{L_{j_{L|K}}}} \phi(x)^{d_{L_{j_{L|K}}}^i}$.

Conclude: $\operatorname{Tr}_{L|K}$ is $K$-linear and $\operatorname{N}_{L|K}$ is multiplicative (WHY).

8) Let $M|K$ be a subextension of $L|K$. Prove that relative trace and norm are transitive:

$\operatorname{Tr}_{L|K} = \operatorname{Tr}_{M|K} \circ \operatorname{Tr}_{L|M}$ and $\operatorname{N}_{L|K} = N_{M|K} \circ N_{L|M}$

[Hint: Use Problem 7, b), the surjectivity of the map $\mathcal{S}_{L|K} \to S_{M|K}$, and $d_{L_i|K}^j = d_{M_i|K}^j d_{M_i|M}^j$, etc...]

• In the above notation, set $M := K(x)$. Let $\mathcal{A} = (\alpha_1, \ldots, \alpha_m)$ and $\mathcal{A}' = (\beta_1, \ldots, \beta_n)$ be $K$-basis of $M, +$, respectively $M$-basis of $L, +$. Then $\mathcal{B} = (\alpha_i \beta_j)_{i,j}$ is a $K$-basis of $L, +$. Let $\varphi : M \to M, u \mapsto xu$ and $\psi : L \to L, v \mapsto xv$ have matrices $A_x \in K^{m \times m}$, respectively $B_x \in K^{mn \times mn}$ as $K$-linear maps of $M, +$ and $L, +$, hence $\varphi(\mathcal{A}) = \mathcal{A} \cdot A_x$ and $\psi(\mathcal{B}) = \mathcal{B} \cdot B_x$.

9) Let $p_{A_x}(t), p_{B_x}(t) \in K[t]$ be the characteristic polynomials. Prove/disprove:

a) $\text{Mipo}_K(x) = p_{A_x}(t)$, and further, $\text{Tr}_K(x) = \text{Tr}(A_x)$ and $\text{N}_K(x) = \det(A_x)$.

b) $p_{A_x}(t)$ is also the minimal polynomial of $B_x$, and further, $p_{B_x}(t) = p_{A_x}(t)^n$.

c) $\text{Tr}_L/K(x) = \text{Tr}(B_x)$ and $\text{N}_{L/K}(x) = \det(B_x)$.

Conclude: $\text{Tr}_{L/K} : L \to K$ is $K$ linear, and $\text{N}_{L/K} : L \to K$ is multiplicative.