Math 594. Composites of radical towers

Let k be a field, and K/k an extension field. Let $k_1, k_2 \subseteq K$ be two subfields containing k, and assume each k_j is "solvable in radicals" in the sense that there exists a k-embedding $k_j \hookrightarrow L_j$ where L_j/k is a radical tower (i.e., L_j/k can be expressed as a finite tower of extensions, each level generated over the level below by a single element which admits some power that lies in the level below). We wish to prove that the composite field $k_1k_2 \subseteq K$ is also solvable in radicals. In other words, we want to construct an extension L/k into which k_1k_2 embeds with L/k a radical tower.

A natural idea is to create a "composite" L of L_1 and L_2 over k (note that, a priori, L_1 and L_2 are not given inside of a common extension of k) and to somehow put k_1k_2 inside of here compatibly with the mechanism by which each k_j is k-embedded into L_j. Such an L/k seems likely to be a radical tower over k, and hence would solve our problem. This is not quite what we will do (it may be impossible to get compatibility with the initial k-embeddings of the k_j's if $k_1 \cap k_2 \subseteq K$ is larger than k), but it gives the general idea.

We emphasize that the concept of composite field k_1k_2 of the k_j's over k inside of K depends very much (in general) on how the k_j's sit in relation to each other inside of K as extensions of k. That is, k_1k_2 is not usually intrinsic to the k_j's as abstract extensions of k (there is an important condition called *linear disjointness* which does render this compositum intrinsic to the k_j's over k, but we won't address this issue here).

1. Some embedding lemmas

The first step is to put the L_j's into a common normal radical tower over k. First, we need to construct an abstract compositum of the L_j's over k, which is to say an extension L/k into which each L_j embeds via some k-embedding $\iota_j : L_j \hookrightarrow L$, with L generated over k by the subfields $\iota_j(L_j)$. Rather more generally, we have the following lemma which has nothing to do with radical towers.

Lemma 1.1. *Let L_1 and L_2 be two finite extensions of a field k. Then there exists a finite extension L/k and k-embeddings $\iota_j : L_j \hookrightarrow L$ such that L is the compositum of the subfields $\iota_j(L_j)$ over k.*

This lemma is true without finiteness (or even algebraicity) conditions, and is easily proven using Zorn's Lemma and tensor products: let L be the quotient of the nonzero k-algebra $L_1 \otimes_k L_2$ by a maximal ideal. The finite case can be handled without using such tools, and this case is all we need, so there seems to be some merit in handling it directly.

Proof. If $L_1 = k(\alpha)$ and α has minimal polynomial f over k, then let $L = L_2[T]/g$ where g is an irreducible factor of f in $L[T]$. Define ι_2 in the obvious way, and define

$$\iota_1 : L_1 \simeq k[T]/f \to L_2[T]/g = L$$

in the obvious way (via $T \mapsto T$). Concretely, we are sending $\alpha \in L_1$ to the residue class $T \bmod g \in L$.

The general case is now easily handled by expressing L_1 is a finite tower of primitive extensions and inducting on the number of steps in the tower. More precisely, we may suppose $L_1 = K(\alpha)$ where K is a subfield over k for which there exists an "abstract compositum" F of K and L_2 over k (i.e., there exist k-embeddings of K and L_2 into F which generate F over k), and then we take L to be an abstract compositum of F and L_1 over K. ∎

Lemma 1.2. *Let L/k be an extension which is a compositum over k of two subextensions $L_1, L_2/k$, with each L_j/k a radical tower. Then L/k is a radical tower.*

Proof. If $L_2 = k(\alpha)$ with $\alpha^d = a \in k$, then $L = L_1(\alpha)$ with $\alpha^d = a \in L_1$, so by expressing L_1/k as a radical tower we get an expression for L/k as a radical tower. In general, L_2 is an n-step radical tower over k and we induct on n (the case $n = 1$ having just been settled). For $n > 1$ we write $L_2 = K(\alpha)$ where $\alpha^d \in K$ and K/k is a radical tower in $n-1$ steps. Then $F = L_1K$ is a radical tower over k by the inductive hypothesis and $L = F(\alpha)$ with $\alpha^d \in K \subseteq F$, so we conclude that L/k is also a radical tower. ∎

Quite generally, if F/k is a finite extension and F'/F is a normal closure over k, then F' is a compositum over k of subfields $\sigma(F)$ for $\sigma \in \mathrm{Aut}(F'/k)$. Indeed, this compositum is stable under $\mathrm{Aut}(F'/k)$ and thus must be normal over k since F'/k is normal, and by definition of normal closure it follows that this normal subextension of F' which contains F has to be equal to F'. As a special case, if L/k is a radical tower, then a normal closure L'/k is a compositum over k of finitely many subextensions $\sigma(L)$ each of which is abstractly k-isomorphic to L, so each $\sigma(L)$ is a radical tower. By Lemma 1.2, we obtain:

Theorem 1.3. *If L/k is a finite extension which is a radical tower, then so is a normal closure of L/k.*

The interest of this theorem lies in its role in the proof of:

Corollary 1.4. *If L_1 and L_2 are radical towers over k, then there exist k-embeddings $\iota_j : L_j \hookrightarrow L$ with L/k a radical tower which is normal.*

Proof. By Lemma 1.1, we can find k-embeddings $L_j \hookrightarrow F$ for some finite extension F/k. By replacing F with a normal closure over k, we may assume F/k is normal. The compositum K of L_1 and L_2 over k inside of F is a radical tower, by Lemma 1.2. Since F/k is normal, it contains a normal closure of K/k. By Theorem 1.3, this normal closure is a radical tower, and hence may be taken as L. ■

2. Main result

We have now gathered everything we need to prove the result of interest. Recall the setup: we give ourselves extensions $k_1, k_2/k$ with k-embeddings $k_j \hookrightarrow L_j$ where each L_j/k is a radical tower. We also assume the k_j's are given to us inside of some extension field K/k. We want to prove that the compositum k_1k_2 over k inside of K admits a k-embedding into some radical tower L/k. By Corollary 1.4, we may enlarge the L_j's to reduce to the case $L_1 = L_2$ with this common extension moreover normal over k. In other words, we may assume there exists a finite normal extension L/k which is a radical tower and into which each k_j admits a k-embedding. We shall prove that the compositum $k_1k_2 \subseteq K$ admits a k-embedding into L. Beware that this need not be compatible with the initial k-embeddings of the k_j's into L (e.g., it may happen that $k_1 \cap k_2 \subseteq K$ is strictly bigger than k and the k-embeddings $k_j \hookrightarrow L$ do not agree on this overlap field).

Our problem has nothing to do with radical towers, and is really a problem concerning normal extensions. Namely, we are given k-embeddings of k_1 and k_2 into a normal extension L/k, and we wish to prove that there exists a k-embedding of the subfield $k_1k_2 \subseteq K$ into L. By Lemma 1.1, there exists a finite extension F/L into which K admits a k-embedding. We may even enlarge F so that it is normal over k. We pick a k-embedding $\iota : K \hookrightarrow F$, and it suffices to show that each $\iota(k_j)$ lies in L, for then $\iota(k_1k_2) \subseteq L$. What we know is that there exists *some* k-embedding $\iota_j : k_j \hookrightarrow L$. Viewing this as a k-embedding of k_j into F, and keeping in mind that we wish to show that $\iota|_{k_j} : k_j \hookrightarrow F$ has image inside of L, we are reduced to the following problem: if $F/L/k$ is a tower of fields with F and L normal over k, and κ/k is an extension which admits a k-embedding into L, then we claim that *any* k-embedding $\kappa \hookrightarrow F$ has image inside of F. For each $\alpha \in \kappa$, it suffices to solve this problem for the subfield $k(\alpha) \subseteq \kappa$. But if $f \in k[T]$ is the minimal polynomial of α, then the hypothesis that $k(\alpha)$ admits a k-embedding into L implies that f has a root in L, and then normality of L/k implies that f splits over L. Hence, all roots of f in F lie in L. Thus, any k-embedding of $k(\alpha)$ into F must send α to a root of f in F, and all such roots lie in L. This solves our problem.