"Field theory" fact used in Q3.

I received some questions about the following fact that I used in the solution of Q3, Ex sheet 4, so here is a proof.

<u>Proposition</u> Let K be a field, M/K a (possibly infinite) Galois extension and let $K \subseteq L, L' \subseteq M$ be subextensions with L'/K finite Galois. Then the image of the restriction map

$$\mathrm{Gal}(M/L) \longrightarrow \mathrm{Gal}(L'|K)$$

is $\mathrm{Gal}(L'/L \cap L')$.

<u>Proof</u>: We factor the map:

$$\mathrm{Gal}(M/L) \longrightarrow \mathrm{Gal}(LL'/L) \longrightarrow \mathrm{Gal}(L'|K)$$

<u>Claim 1</u>: $\operatorname{Im}\left(\mathrm{Gal}(LL'/L) \longrightarrow \mathrm{Gal}(L'|K)\right) =$

$= \mathrm{Gal}(L'/L\cap L')$.

The inclusion $\subseteq$ is clear. Since $L'|K$ is finite Galois, the image is equal to $\mathrm{Gal}(L'/F)$ for some $L'/F/L\cap L'$ by finite Galois theory. It follows that any $\sigma \in \mathrm{Gal}(LL'|L)$ fixes F, and also L by definition, so it fixes $LF \subseteq LL'$. By finite Galois theory again, this implies that $LF = L$ so $F \subseteq L$, and hence $F \subseteq L\cap L'$. Therefore $F = L\cap L'$, as desired.

<u>Claim 2</u>: $\mathrm{Gal}(M|L) \longrightarrow \mathrm{Gal}(LL'|L)$ is surjective.

This "standard" fact from field theory.

Here's a sketch of the proof. let $\sigma \in Gal(LL'|L)$. Define a partially ordered set $\Sigma = \{(E,\psi) \mid M/E/LL', \psi \in Hom_L(E,M), \psi|_{LL'} = \sigma\}$,

$$(E,\psi) \leq (E',\psi') \overset{def}{\Longleftrightarrow} E \subseteq E' \text{ and } \psi'|_E = \psi.$$

One checks that Zorn's Lemma applies to Σ, so $\exists$ maximal (T,φ). First, we claim that $T = M$. If not, pick $\alpha \in M \setminus T$ and let $f(X) \in T[X]$ be the minimal polynomial of α.

We may then extend φ to $T(\alpha)$ by mapping α to a root of $\varphi(f(X))$ in M, contradicting the maximality of (T,φ). Thus $T = M$.

Second, we claim that $\varphi : M \to M$ is surjective. This is a general fact for

Galois extensions:

Let $\beta \in M$ and let $\{\beta = \beta_1, \dots, \beta_m\}$ be the set of L-conjugates of β. Then φ

$$\varphi(\{\beta_1, \dots, \beta_n\}) \subseteq \{\beta_1, \dots, \beta_n\}$$

since φ fixes L, and since φ is injective we have $\varphi(\{\beta_1, \dots, \beta_n\}) = \{\beta_1, \dots, \beta_n\}$.

Therefore $\beta \in \varphi(M)$, so $\varphi(M) = M$.

Claim 1 + Claim 2 then gives the proposition.