HOMEWORK #8
SOLUTIONS TO SELECTED PROBLEMS

Problem 8.4 – Normality of the composite. Let $K \subset L_1, L_2 \subset \bar{K}$ be two finite extensions.

Lemma 1. *If L_1/K and L_2/K are normal, then so is their composite L_1L_2/K.*

First proof. We know that a finite extension L/K is normal if and only if it is a splitting field (over K) of a polynomial $f \in K[t]$. So, by our assumptions, there exist polynomials $f_1, f_2 \in K[t]$ such that L_i/K is a splitting field for f_i ($i = 1, 2$). Now, the composite L_1L_2 is a splitting field of the product f_1f_2, hence L_1L_2/K is normal. $\square$

Lemma 2. $\mathrm{Gal}(\bar{K}/L_1L_2) = \mathrm{Gal}(\bar{K}/L_1) \cap \mathrm{Gal}(\bar{K}/L_2)$.

Proof. If $\sigma \in \mathrm{Gal}(\bar{K}/L_1L_2)$ then it is the identity on L_1L_2 hence on the subfields L_1 and L_2. This shows the inclusion $\subseteq$. In the other direction, if σ is an automorphism of $\bar{K}$ and it is the identity on both L_1, L_2 then it is the identity on L_1L_2 (to see this, write $L_1 = K(\alpha_1, \dots, \alpha_n)$ and $L_2 = K(\beta_1, \dots, \beta_m)$. Then $L_1L_2 = K(\alpha_1, \dots, \alpha_n, \beta_1, \dots, \beta_m)$ and $\sigma(\alpha_i) = \alpha_i$, $\sigma(\beta_j) = \beta_j$ for all i, j). $\square$

Lemma 3. *A finite extension L/K is normal if and only if* $\mathrm{Gal}(\bar{K}/L)$ *is normal in* $\mathrm{Gal}(\bar{K}/K)$.

Proof. Let $\sigma \in \mathrm{Gal}(\bar{K}/K)$. Then $\sigma(L)$ is a subfield of $\bar{K}$, and $\mathrm{Gal}(\bar{K}/\sigma(L)) = \sigma\,\mathrm{Gal}(\bar{K}/L)\sigma^{-1}$ (just check on elements, for example if $x \in \sigma(L)$ then $\sigma^{-1}(x) \in L$ hence for every $\tau \in \mathrm{Gal}(\bar{K}/L)$, $\tau(\sigma^{-1}(x)) = \sigma^{-1}(x)$ so that $\sigma\tau\sigma^{-1}(x) = \sigma\sigma^{-1}(x) = x$ thus $\sigma\tau\sigma^{-1} \in \mathrm{Gal}(\bar{K}/\sigma(L))$).

By Galois theorem we see that all the subfields $\sigma(L)$ are equal to L if and only if all the subgroups $\sigma\,\mathrm{Gal}(\bar{K}/L)\sigma^{-1}$ are equal to $\mathrm{Gal}(\bar{K}/L)$. The latter condition is the definition of the normality of $\mathrm{Gal}(\bar{K}/L)$ in $\mathrm{Gal}(\bar{K}/K)$, while the former condition on L is equivalent to the normality of L/K. $\square$

Second proof of Lemma 1. Let $N_i = \mathrm{Gal}(\bar{K}/L_i)$. By lemma 3, N_1, N_2 are normal in $G = \mathrm{Gal}(\bar{K}/K)$, hence $N = \mathrm{Gal}(\bar{K}/L_1L_2) = N_1 \cap N_2$ (by lemma 2) is normal in G, so by lemma 3 again, L_1L_2/K is normal. $\square$

Corollary. *If L_1/K, L_2/K are Galois, then L_1L_2/K is Galois.*

What can be said about the Galois group of the composite?

Lemma 4. *If L_1/K, L_2/K are Galois, then there is an embedding*

$$\mathrm{Gal}(L_1L_2/K) \hookrightarrow \mathrm{Gal}(L_1/K) \times \mathrm{Gal}(L_2/K)$$

Proof. One can either construct the embedding directly by $\sigma \mapsto (\sigma_{|L_1}, \sigma_{|L_2})$, or use the second proof of Lemma 1 and note the following two facts; first, if $N_1, N_2 \lhd G$ then $G/(N_1 \cap N_2) \hookrightarrow G/N_1 \times G/N_2$. Second, for a Galois extension L/K, $\mathrm{Gal}(L/K) = \mathrm{Gal}(\bar{K}/K)/\mathrm{Gal}(\bar{K}/L)$. $\square$

Problem 8.5. Let K be a field with $\operatorname{char} K \neq 2$. Let $a \in K$. Then the extension $K(\sqrt{a})/K$ obtained by adjoining a square root of a is either of degree 1 (if $a = b^2$ for some $b \in K$) or of degree 2. Since the polynomial $t^2 - a$ has derivative $2t$ and $\operatorname{char} K \neq 2$, the extension is separable. It is also normal (any extension of degree ≤ 2 is normal), hence Galois, and the Galois group is either trivial or $\mathbb{Z}/2\mathbb{Z}$.

Now let $a_1, \ldots, a_n \in K$ and consider the extension $K(\sqrt{a_1}, \ldots, \sqrt{a_n})/K$. Since it is the composite of the extensions $K(\sqrt{a_i})/K$ which are Galois, by the corollary before lemma 4, it is Galois. By lemma 4 we also have

$$G := \operatorname{Gal}(K(\sqrt{a_1}, \ldots, \sqrt{a_n})/K) \hookrightarrow \prod_{i=1}^{n} \operatorname{Gal}(K(\sqrt{a_i})/K)$$

Since each of the factors is either 1 or $\mathbb{Z}/2\mathbb{Z}$, we see that G is embedded in $(\mathbb{Z}/2\mathbb{Z})^m$ for some $m \leq n$. But $(\mathbb{Z}/2\mathbb{Z})^m$ can be viewed as an m-dimensional vector space over the field with 2 elements $\mathbb{F}_2$, and any subgroup is easily seen to be a vector subspace (hence as a vector space of lower dimension). Thus G is isomorphic to a vector space of dimension $r \leq m \leq n$ over $\mathbb{F}_2$, that is, $G \simeq (\mathbb{Z}/2\mathbb{Z})^r$.

Lemma. $[K(\sqrt{a_1}, \ldots, \sqrt{a_n}) : K] = 2^n$ *if and only if none of the* $2^n - 1$ *products* $\prod_{i \in I} a_i$ *(where* I *runs over all subsets* $\phi \neq I \subseteq \{1, 2, \ldots, n\}$*) is a square of an element in* K.

Proof. Let $L_0 = K$ and $L_i = K(\sqrt{a_1}, \ldots, \sqrt{a_i})$ for $1 \leq i \leq n$. Then $L_i = L_{i-1}(\sqrt{a_i})$ so that $[L_i : L_{i-1}] \leq 2$ and $[L_n : K] = 2^n$ if and only if $[L_i : L_{i-1}] = 2$ for all $1 \leq i \leq n$.

Suppose that $[L_n : K] = 2^n$. Then $[L_i : L_{i-1}] = 2$ for all $1 \leq i \leq n$ and $1, \sqrt{a_i}$ is a basis of L_i over L_{i-1}. It follows (Theorem 1.1, Product formula) that $\left\{\prod_{i \in I} \sqrt{a_i}\right\}_{I \subseteq \{1, \ldots, n\}}$ is a basis of L_n over K. Taking $I = \phi$ we see that $1 \in K$ is an element of the basis. Since the elements of the basis are independent over K, we see that $\prod_{i \in I} \sqrt{a_i} \notin K$ for all $\phi \neq I \subseteq \{1, \ldots, n\}$.

We prove the opposite direction by induction on n, the case $n = 1$ being trivial. Since the condition on subsets is obviously satisfied for $\{1, \ldots, n-1\}$, by induction hypothesis we have $[L_{n-1} : K] = 2^{n-1}$. We assume $[L_n : L_{n-1}] < 2$ and arrive at a contradiction. Indeed, we have $L_n = L_{n-1}$ so that $\sqrt{a_n} \in L_{n-1}$. Now $\{1, \sqrt{a_{n-1}}\}$ is a basis of L_{n-1}/L_{n-2}, so we can write

$$\sqrt{a_n} = A + B\sqrt{a_{n-1}}$$

for unique $A, B \in L_{n-2}$. Squaring this, we see that

$$a_n = (A^2 + B^2 a_{n-1}) + 2AB\sqrt{a_{n-1}}$$

But $a_n \in K \subseteq L_{n-2}$, and since $\{1, \sqrt{a_{n-1}}\}$ is a basis of L_{n-1}/L_{n-2}, we must have that $2AB = 0$, so that $A = 0$ or $B = 0$.

If $B = 0$, then $\sqrt{a_n} = A \in L_{n-2}$, but this is impossible as $[L_{n-2}(\sqrt{a_n}) : L_{n-2}] = 2$ by the induction hypothesis on the set $a_1, \ldots, a_{n-2}, a_n$ (with $n-1$ elements).

If $A = 0$, then $\sqrt{a_n} = B\sqrt{a_{n-1}}$ so that $\sqrt{a_{n-1}a_n} \in L_{n-2}$. But again this is impossible since $[L_{n-2}(\sqrt{a_{n-1}a_n}) : L_{n-2}] = 2$ by the induction hypothesis on the $n-1$ element set $a_1, \ldots, a_{n-1}, a_{n-1}a_n$ (all products are products of some a_i-s). $\square$