Math 210B. Normal field extensions

1. A definition

In Exercise 7 of HW5 it was shown that for a finite extension of fields $k'/k$, the conditions that $k'/k$ is the splitting field of a monic polynomial is equivalent to the condition that the images of all $k$-embeddings $k' \to \overline{k}$ coincide. This property is the definition of normal for such extensions. Here we wish to take up the generalization of this concept to algebraic extensions of fields $k'/k$ not necessarily of finite degree.

There are (at least) three ways one might generalize normality to an algebraic extension $k'/k$:

(i) All $k$-embeddings $k' \to \overline{k}$ have the same image.

(ii) Every finite subextension of $k'/k$ is contained in a finite subextension that is normal.

(iii) There is a set $S$ of monic polynomials in $k[X]$ such that $k'/k$ splits all $f \in S$ and every finite subextension of $k'/k$ is contained in the splitting field of a product of finitely many elements of $S$.

Note that in (iii) we are forced to consider sets $S$ rather than a single polynomial because for a finite set of monic polynomials $f_1, \ldots, f_m$ we can split all $f_i$’s by splitting the single polynomial $\prod_j f_j$ but no such trick is available to create infinite-degree extensions. Our aim here is to show that (i), (ii), and (iii) are equivalent; any algebraic $k'/k$ satisfying such conditions is called normal. At the end we’ll discuss the analogue of normal closure.

First we show (i) implies (ii). Since a compositum of finite-degree normal extensions is normal (as normality is equivalent to being a splitting field of a single monic polynomial in the finite-degree case, and splitting several polynomials simultaneously is the same as splitting their product), we just have to check that for all $a \in k'$, the field $k(a) \subset k'$ is contained in a finite-degree subextension of $k'/k$ that is normal. Thus, if suffices to show that if $f \in k[X]$ is monic with a root $\rho$ in $k'$ then it splits in $k'$. For any root $r \in \overline{k}$, we can pick a $k$-isomorphism $k(\rho) \simeq k(r) \subset \overline{k}$. This makes $\overline{k}$ an algebraic extension of $k(\rho)$ (by algebraic closure of $k$) that is algebraically closed, so it is an algebraic closure of $k(\rho)$. Thus, the algebraic extension $k'/k(\rho)$ embeds into $\overline{k}$ over this chosen inclusion $k(\rho) \hookrightarrow \overline{k}$. In this way we have made $k$-embeddings $j_r : k' \to \overline{k}$ whose images contain whatever root $r$ of $f$ in $\overline{k}$ we wish. But by (i) all $k$-embeddings $j : k' \to \overline{k}$ have the same image, so in particular if we pick one such $j$ then $j(k')$ contains all such $r$. This implies that the polynomial $f \in k[X]$ splits over $j(k')$, so it splits over the extension $k'/k$ as desired.

Next, we show (ii) implies (iii). For each $a \in k'$, by (ii) the subfield $k(a) \subset k'$ is contained in a normal subextension of $k'/k$ of finite degree, which is to say $k(a) \subset F_a \subset k'$ where $F_a/k$ is the splitting field of some monic polynomial $f_a \in k[X]$. The set $S$ of such $f_a$’s works in (iii).

Finally, we show (iii) implies (i). Let $K \subset \overline{k}$ be the subfield generated over $k$ by the roots of all $f \in S$. By (iii), any $k$-embedding $j : k \to \overline{k}$ has image containing $K$. But in fact the containment $K \subset j(k')$ must be an equality. Indeed, by (iii) every element $a \in k'$ lies in a subfield $F \subset k'$ that is the splitting field of $\prod_j f_j$ for some $f_1, \ldots, f_m \in S$, so $j(a)$ is contained in the splitting field of $\prod_j f_j$ inside $\overline{k}$. But this latter splitting field is the compositum of the splitting fields $F_i \subset \overline{k}$ of each $f_j$, yet $F_i \subset K$ for all $i$ by design of $K$. Thus, $j(a) \in K$. Since $a$ was arbitrary in $k'$, we have $j(k') \subset K$ as desired. This concludes the proof of the equivalence of (i), (ii), and (iii).

2. Normal closure

If $k'/k$ is a general algebraic extension, a normal closure of $k'/k$ is an algebraic extension $E/k'$ normal over $k$ with the “minimality” property that any $k$-embedding $k' \to \overline{k}$ into a normal extension $K/k$ extends to an embedding $E \hookrightarrow K$. We claim such an $E/k'$ exists and is unique up to
Thus, the definition of normality. Any root of $E/k$ is algebraically closed, so it is an algebraic closure of $k$. By normality of $F/k$, we claim is an isomorphism (so $i$ is surjective and hence is an isomorphism, so the uniqueness up to isomorphism would be established). By normality of $F/k$, if $a \in E$ is an element and $f \in k[X]$ is its minimal polynomial then $f$ splits in $F$. The injective $i : F \rightarrow E$ then carries the finite set of roots of $f$ in $F$ onto the finite set of such roots in $E$. Since $a$ is one of those roots, it is hit by $i$. Thus, $i$ is surjective as claimed.

Next, we construct a normal closure. In effect, it is a huge union of splitting fields. Pick a $k$-embedding $j_0 : k' \rightarrow \overline{k}$. For each $a \in k'$ we have the splitting field $F_a \subseteq \overline{k}$ of the minimal polynomial $m_a \in k[X]$ of $a$. Let $E$ be the compositum inside $\overline{k}$ of the (huge) set of such extensions $F_a$ of $k$. (That is, an element of $E$ is a ratio of polynomial expressions over $k$ in elements of finitely many $F_a$’s.) We claim that $E$ works. First we show $E/k$ is normal by verifying condition (i) in the definition of normality.

Any $k$-embedding $\iota : E \rightarrow \overline{k}$ makes $\overline{k}$ an algebraic extension of $E$ that is algebraically closed, so it makes $\overline{k}$ an algebraic closure of $E$. But the definition of $E$ as a subfield of $\overline{k}$ does the same, so by uniqueness of algebraic closures there is an automorphism $\sigma$ of $\overline{k}$ carrying the definition inclusion $E \hookrightarrow \overline{k}$ over to $\iota$. Both of these inclusions of $E$ into $\overline{k}$ are $k$-embeddings, so (!) $\sigma$ must be a $k$-automorphism. As such, $\sigma$ restricts to an automorphism of each splitting field $F_a \subseteq \overline{k}$ (of each $m_a \in k[X]$, for $a \in k'$), and hence to their compositum $E$. By design $\sigma(e) = \iota(e)$ for all $e \in E$, yet we just saw that $\sigma(E) = E$, so $\iota(E) = E$. This verifies (i) in the definition of normality, so $E/k'$ is normal over $k$.

Finally, we check the minimality requirement. Suppose $i : k' \rightarrow F$ is a $k$-embedding into a normal extension of $k$. We seek a $k'$-embedding $E \rightarrow F$. Since $F$ is algebraic over $k'$ and $j_0$ in the construction of $E$ realizes $\overline{k}$ as an algebraic closure of $k'$, we can extend $j_0$ through $i$ to an embedding $\tau : F \rightarrow \overline{k}$; in other words, the latter is a $k'$-embedding (where $\overline{k}$ is an extension of $k'$ via $j_0$, and $F$ is an extension of $k'$ via $i$). The image $\tau(F)$ is a subfield of $\overline{k}$ containing $j_0(k')$ and normal over $k$. For any $a \in k'$ the irreducible monic $m_a \in k[X]$ has a root $\tau(i(a)) \in \tau(F)$, so $\tau(F)$ contains the splitting field over $k$ of $m_a$ inside $\overline{k}$. This splitting field is precisely $F_a$ as in the construction of $E$, so $E \subseteq \tau(F)$ as subfields of $\overline{k}$ containing $j_0(k')$. Since $\tau$ is a $k'$-embedding (intertwining $i$ and $j_0$), the composite map $E \hookrightarrow \tau(F) \simeq F$ whose second step is $\tau^{-1}$ is a $k'$-embedding. This is the desired $k'$-embedding of $E$ into any extension $F/k'$ that is normal over $k$. (typically non-unique!) $k'$-isomorphism. (For $k'/k$ of finite degree we make such $E/k'$ as a splitting field; in general we need to do a bit more.)