Math 121. Characterization of normality

Let k be a field. In class we defined an algebraic extension L of k to be *normal* if any irreducible $g \in k[X]$ with a root in L splits completely in $L[X]$. We showed that if $[L : k]$ is finite then it is equivalent to say that L is the splitting field over k for some non-constant $f \in k[X]$. In this handout, we establish a useful alternative characterization of normality.

Theorem 0.1. *Let L/k be an algebraic extension, and let K/k be a normal extension such that there exists a k-embedding $L \to K$. Then L is normal over k if and only if every k-embedding $L \to K$ has the same image.*

As a special case of this theorem, we can take $K = \overline{k}$ to be an algebraic closure. Indeed, an algebraic closure $\overline{L}$ of L is algebraic over k (by transitivity of algebraicity and the algebraicity of $\overline{L}/L$ and L/k) and algebraically closed, so $\overline{L}$ is also an algebraic closure of k. Thus, there is a k-isomorphism $\overline{L} \simeq \overline{k}$, thereby providing a k-embedding $L \to \overline{k}$. Hence, the hypotheses of the theorem are always satisfied using $K = \overline{k}$, so the theorem says that an algebraic extension L/k is normal if and only if *every* k-embedding $j : L \to \overline{k}$ has image $j(L) \subset \overline{k}$ independent of the choice of j.

It must be kept in mind that this "normality criterion" in the theorem is only applicable for L/k when using a normal extension K/k relative to which there is *some* k-embedding of L. For example, using $k = \mathbf{Q}$ and $L = \mathbf{Q}(2^{1/3})$, we cannot test the normality of L over k using the normal extension $K = \mathbf{Q}(\sqrt{5})$!

Proof. We will only prove the theorem in the special case that $[L : k]$ and $[K : k]$ are finite, as this is all we need for later developments in this course. (The interested reader is invited to adapt the idea to make a proof in general via reduction to the finite-degree case, using a combination of Zorn's Lemma and results we saw in class exhausting a general normal extension of k by normal subextensions of finite degree over k.)

The implication "$\Leftarrow$" is just root-chasing, as follows. Suppose L is normal over k, so L is a splitting field over k for some non-constant $f \in k[X]$ that we may take to be monic. By hypothesis there is *some* k-embedding $L \to K$, so f splits completely over K since it does so over L. Writing $f = \prod_{i=1}^{d}(X - r_i)$ in $K[X]$, we claim that any k-embedding $j : L \to K$ has image $j(L)$ equal to the subfield $k(r_1, \ldots, r_d)$ (which is independent of j!). By definition of what it means to say that L is a splitting field of f over k, in $L[X]$ we have $f = \prod(X - a_i)$ for some $a_1, \ldots, a_d \in L$ such that $L = k(a_1, \ldots, a_d)$. Hence, for any k-embedding $j : L \to K$, applying $j : L[X] \to K[X]$ to the identity $f = \prod(X - a_i)$ yields that $\prod(X - r_i) = f = \prod(X - j(a_i))$ in $K[X]$. Thus, by unique factorization in $K[X]$, the collection of $j(a_i)$'s (with multiplicity) is a rearrangement of the collection of r_i's, so $j(L) = k(j(a_1), \ldots, j(a_d)) = k(r_1, \ldots, r_d)$ for any such j.

Now suppose conversely that all k-embeddings $j : L \to K$ have the same image. We want to deduce that L is normal over k. Recall that by hypothesis there is at least one k-embedding $j_0 : L \to K$. We want to show that if an irreducibe $g \in k[X]$ has a root ρ in L then g splits completely in $L[X]$. We may and do assume g is monic. Using j_0, we see that $r := j_0(\rho) \in K$ is a root of $g \in k[X]$. Hence, by normality of K/k, it follows that g splits completely over K. To show that g splits completely over L, it therefore suffices to prove that all roots r' of g in K lie in the subfield $j_0(L)$ (much as r does), as then g would split completely over $j_0(L)$ and hence over L (via the k-isomorphism $j_0 : L \simeq j_0(L)$).

The hypothesis of normality of K over k with $[K : k]$ finite implies that K is the splitting field over k of some monic non-constant $h \in k[X]$. Let $F = k[T]/(g)$ (a field!), and consider the two k-embeddings $F \rightrightarrows K$ via $T \mapsto r, r'$. Since K is generated over k by a full set of roots of h (exhibiting

h as $\prod(X - b_i)$ in $K[X]$), it is likewise generated over F by such roots using *either* of the two k-embeddings of F into K just mentioned. This realizes K as a splitting field of $h \in k[X]$ over F in *two* ways, so by uniqueness of splittng fields there is an automorphism σ of K which carries one such realization to the other! This says that $\sigma : K \simeq K$ exchanges the two k-embeddings $F \rightrightarrows K$ just mentioned, which is to say $\sigma(r) = r'$. Hence, $\sigma \circ j_0 : L \to K$ is a k-embedding under which ρ is carried to $\sigma(j_0(\rho)) = \sigma(r) = r'$. But by hypothesis all k-embeddings of L into K have the *same* image, namely $j_0(L)$, so $\sigma \circ j_0$ has image $j_0(L)$. Thus, $r' \in j_0(L)$. Since r' was an arbitrary choice of root of g in K, it follows that all roots of g in K lie in $j_0(L)$. As we noted above, this implies that g splits completely over L, as desired. ■