MAT 347
Splitting fields and Normal extensions
March 10, 2020

Suppose F is a field and $f(X) \in F[X]$ a nonzero polynomial.

Definition 1. We say that an extension K/F is a *splitting field of $f(X)$ over F* if $f(X) = c(X-\alpha_1)\cdots(X-\alpha_n)$ and $K = F(\alpha_1, \cdots, \alpha_n)$.

1. Suppose that $\deg(f) = n$. Show that there exists a splitting field K of $f(X)$ over F and that moreover $[K:F] \leq n!$. (*Hint:* What happens when you adjoin just one root of f to F? Then use induction on n.)

In class we will show:

Theorem ("Theorem B")**.** *Let $\phi : F_1 \to F_2$ be a field isomorphism. Let $\tilde{\phi} : F_1[X] \to F_2[X]$ be the ring isomorphism that ϕ induces over the rings of polynomials. Let $f_1 \in F_1[X]$ and let $f_2(X) := \tilde{\phi}(f_1(X))$. Let E_i be a splitting field of $f_i(X)$ over F_i.*
Then there exist a field isomorphism $\sigma : E_1 \to E_2$ such that $\sigma|_{F_1} = \phi$.

2. Suppose that K_1 and K_2 are two splitting fields of $f(X)$ over F. Prove that there exists a field isomorphism $\varphi : K_1 \to K_2$ such that $\varphi(\alpha) = \alpha$ for all $\alpha \in F$. In other words, splitting fields are unique up to isomorphism!

3. Let K/F be a finite field extension. Show that the following are equivalent:

   (a) If $g(X) \in F[X]$ is an irreducible polynomial and it has a root in K, then $g(X)$ splits in K.

   (b) For every $\alpha \in K$, the minimal polynomial of α over F splits in K.

   (c) $K = F(\alpha_1, \ldots, \alpha_n)$ and the minimal polynomial of α_j over F splits in K for all $j = 1, \ldots, n$.

   (d) K is the splitting field of some (not necessarily irreducible) polynomial in $F[X]$.

   (e) For any field $E \supseteq K$ and any F-homomorphism $\phi : K \to E$, $\phi(K) \subseteq K$.

   (f) For any field $E \supseteq K$ and any F-homomorphism $\phi : K \to E$, $\phi(K) = K$.

   (*Note:* an "F-homomorphism" is a homomorphism that fixes every element of F. *Hint:* the hard part is (f)⇒(a). The idea is that if $g(X)$ has roots $\alpha_1 \in K$ and α_2 in some bigger field, you first use Theorems A to construct an F-isomorphism $F(\alpha_1) \cong F(\alpha_2)$ and then try to extend it to a splitting field L using Theorem B. The field L you extend it to should be some splitting field over F that contains K and α_2. It may help to look ahead to Question 5...)

Definition 2. A field extension satisfying the equivalent conditions in the previous theorem is called a *normal extension*.

Notice that these characterizations have different "roles". In a given example, it will be easy for us to check that condition (c) or (d) are satisfied, and we will want to use that condition (a) or (b) are true. Conditions (e) and (f) are convenient as lemmas for theoretical proofs.

Definition 3. Let $F \subseteq K \subseteq N$ be fields. The finite extension N/F is called a *normal closure* of K/F if

- N/F is normal, and
- if M is a field, $K \subseteq M \subseteq N$, and M/F is normal, then $M = N$.

In other words, N/F is a minimal normal extension of F containing K.

4. Show that if $F \subseteq K \subseteq N$ and N/F is normal, then N contains a normal closure of K/F.

5. Assume that $K = F(\alpha_1, \ldots, \alpha_n)$. Show that a normal closure of K/F is the same thing as a splitting field of $f(X) := \prod_{j=1}^{n} m_{\alpha_j, F}(X)$ over K. In particular, normal closures exist and are unique up to isomorphism.

6. What are the normal closures of $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$ and of $\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}$?

7. Let K/F be a finite field extension and let N/F be its normal closure. Then there are fields $K_1, \ldots K_r$ for some $r \geq 1$ such that

   - $F \subseteq K_i \subseteq N$ for all i,
   - $N = K_1 K_2 \cdots K_r$ (i.e. N is the composite of K_1, ..., K_r),
   - for each i there is an F-isomorphism between K_i and K.

   This means that the normal closure of K/F is the composite of finitely many field extensions isomorphic to K/F.
   (*Hint:* Write $K = F(\alpha_1, \ldots, \alpha_n)$. Let $f(X)$ be defined as in Question 5. Let β be a root of $m_{\alpha_i, F}(X)$. Use Theorems A and B to prove that there is some F-automorphism ϕ of N such that $\phi(\alpha_i) = \beta$. Let $L_\beta := \phi(K)$. Then N is the composite of the fields in the set $\{L_\beta \mid \beta \text{ is a root of } f(X)\}$.)

8. What are the fields K_i in the second example K/F of Question 6?

Bonus question: In the first problem, show that in fact $[K : F]$ divides $n!$. (Hint: use induction. First deal with the case where $f(x)$ is irreducible. Otherwise, $f(x)$ splits into two factors of smaller degrees r, $n - r \ldots$.)