GALOIS THEORY: SPLITTING FIELDS AND NORMAL EXTENSIONS

LEO GOLDMAKHER

1. Characterizing normal extensions

Recall that L/K is a *normal extension* if and only if every irreducible $f \in K[x]$ either has no roots in L or splits completely in L. It turns out that finite, normal extensions have a particularly straightforward characterization:

Proposition 1.1. *L/K if finite and normal if and only if L is the splitting field of some $f \in K[x]$.*

Proof. The forward direction is fairly straightforward: write $L = K(\alpha_1, \alpha_2, \ldots, \alpha_n)$, and let f be the product of all the minimal polynomials of the α_i. Then L is the splitting field of f over K.

Thus we focus on the reverse direction. Suppose L is the splitting field of $g \in K[x]$. Then L/K is finite, so it remains to show that the extension must be normal. Accordingly, suppose we're given some irreducible $f \in K[x]$ with a root $\alpha \in L$. Pick some other root β of f. Where does β live? We hope to show that it's in L, but for now all we can say is that $\beta \in L(\beta)$ – not super helpful. Here's a picture of the situation:

$$\begin{tikzcd}
 & L(\beta) \arrow[dd, dash] \\
L \arrow[ur, dash] \arrow[d, dash] & \\
K(\alpha) \arrow[d, dash] & K(\beta) \\
K \arrow[ur, dash] &
\end{tikzcd}$$

Inspired by this diagram, we compute $[L(\beta) : K]$ in two different ways:

$$[L(\beta) : L][L : K(\alpha)][K(\alpha) : K] = [L(\beta) : K] = [L(\beta) : K(\beta)][K(\beta) : K]. \tag{1}$$

Since f is irreducible over K and has roots α and β, it must be the minimal polynomial of both. (Without loss of generality we may assume f is monic.) Thus, Kronecker's theorem implies

$$K(\alpha) \simeq K[x]/(f) \simeq K(\beta).$$

Moreover, $[K(\alpha) : K] = \deg f = [K(\beta) : K]$. Thus (1) simplifies to

$$[L(\beta) : L][L : K(\alpha)] = [L(\beta) : K(\beta)].$$

To conclude the proof, it therefore suffices to show that $[L : K(\alpha)] = [L(\beta) : K(\beta)]$. Why is this true? Here's a proof by picture:

$$\begin{tikzcd}
L \arrow[r, dotted, "\sim"] & L(\beta) \\
K(\alpha) \arrow[u, dash, "\text{Split extn of } g \text{ over } K(\alpha)\rightarrow"] \arrow[r, "\sim"] & K(\beta) \arrow[u, dash, "\leftarrow\text{Split extn of } g \text{ over } K(\beta)"']
\end{tikzcd}$$

Date: April 30, 2018.

Let's consider this a little more carefully. We know from above (by Kronecker) that $K(\alpha) \simeq K(\beta)$, and that L is a splitting field of g over $K(\alpha)$. Furthermore, $L(\beta)$ is a splitting field of g over $K(\beta)$. Intuitively, this should imply that $L \simeq L(\beta)$, and thus, that $[L : K(\alpha)] = [L(\beta) : K(\beta)]$, which concludes the proof! To make this rigorous is a bit painful, and follows immediately from the Isomorphism Lifting Lemma (see next section). □

2. The Isomorphism Lifting Lemma

The goal of this section is to state and prove an important technical result, the *Isomorphism Lifting Lemma*. This result is usually the basis of the proof of the equivalent conditions for an extension to be Galois, and that by itself should already convince you of its utility. However, I also hope it makes you appreciate the elegance of Geck's approach!

We give two additional demonstrations of the power of this lemma. The first is to put the proof of the previous section on rigorous footing; the second is to prove that splitting fields are unique up to isomorphism. Before we can even state the lemma, we require notation for a concept we've been using in class for quite some time.

Definition. Given a field isomorphism $\sigma : K \xrightarrow{\sim} K'$ and a polynomial $f \in K[x]$, we define the polynomial $\sigma f \in K'[x]$ as follows:

$$f(x) = \sum_{0 \le k \le n} a_k x^k \qquad \Longrightarrow \qquad (\sigma f)(x) := \sum_{0 \le k \le n} \sigma(a_k) x^k.$$

In other words, we are abusing notation and letting σ denote the induced ring isomorphism $K[x] \xrightarrow{\sim} K'[x]$ which agrees with σ on K and maps $x \mapsto x$.

Remark. Beware one possible point of confusion: $(\sigma f)(x) \neq \sigma\big(f(x)\big)$! Indeed, writing $f(x) = a_n x^n + \cdots + a_0$ we find

$$\begin{aligned} \sigma\big(f(x)\big) &= \sigma(a_n x^n + \cdots + a_0) \\ &= \sigma(a_n)\sigma(x)^n + \cdots + \sigma(a_1)\sigma(x) + \sigma(a_0) \\ &= (\sigma f)(\sigma x). \end{aligned} \tag{2}$$

Armed with this new notation, we can now state the result.

Isomorphism Lifting Lemma. Given $f \in K[x]$ and a field isomorphism $\sigma : K \xrightarrow{\sim} K'$. Let L be a splitting field of f over K, and let L' be a splitting field of σf over K'. Then:

(1) $[L : K] = [L' : K']$,
(2) σ lifts to an isomorphism $\widetilde{\sigma} : L \xrightarrow{\sim} L'$ (i.e. there exists a $\widetilde{\sigma}$ such that $\widetilde{\sigma}(\alpha) = \sigma(\alpha)\ \forall \alpha \in K$), and
(3) there are at most $[L : K]$ extensions $\widetilde{\sigma}$ of σ.

The following diagram might clarify the theorem:

$$\begin{tikzcd}
L \arrow[r, dashed, "\widetilde{\sigma}", "\sim"'] & L' \\
K \arrow[u, dash, "\text{splitting ext}^{\text{n}} \text{ of } f \longrightarrow"] \arrow[r, "\sigma", "\sim"'] & K' \arrow[u, dash, "\longleftarrow \text{ splitting ext}^{\text{n}} \text{ of } \sigma f"']
\end{tikzcd}$$

Before proving the result, we derive a couple of corollaries to demonstrate its utility.

Corollary 2.1. *Splitting fields are unique up to isomorphism.*

Proof. Suppose $f \in K[x]$, and let L, L' be two splitting fields of f over K. Applying the Isomorphism Lifting Lemma with $K = K'$ and σ the identity map. □

Corollary 2.2. *Let L/K be the splitting field of $f \in K[x]$ over K. Then $|\mathrm{Aut}(L/K)| \le [L : K]$.*

Proof. Apply the Isomorphism Lifting Lemma to the case $K = K'$ and $\sigma = \mathrm{id}$; from above, we know we can take $L' = L$. Note that any K-automorphism of L must be a lift $\widetilde{\sigma}$ of σ. The third assertion of the Isomorphism Lifting Lemma implies that there are at most $[L : K]$ of these. □

Unfortunately, the proof of the theorem is a bit long and technical, but it's necessary for putting splitting fields (and hence, Galois theory!) on a rigorous foundation. Think of it as a character-building exercise.

Proof of Isomorphism Lifting Lemma. The proof proceeds by induction on $[L : K]$. The base case $[L : K] = 1$ is equivalent to $L = K$. It is an exercise to deduce that $L' = K'$, and all three conclusions of the theorem follow immediately.

We may therefore assume that $[L : K] > 1$. This implies that f has some root $\alpha \notin K$; let $m_\alpha \in K[x]$ denote the minimal polynomial of α over K. We wish to lift the isomorphism $\sigma : K \xrightarrow{\sim} K'$ to an isomorphism $\widetilde{\sigma} : L \xrightarrow{\sim} L'$. How can we do this? What can we say about the behavior of this hypothetical $\widetilde{\sigma}$? We already know its behavior on K, since it's supposed to agree with σ there. What about other elements? For example, where does $\widetilde{\sigma}$ send α?

<u>STEP 1</u>: If $\widetilde{\sigma}$ exists, then it must send α to a root of σm_α.

Proof. By (2), we have

$$\widetilde{\sigma}\big(m_\alpha(x)\big) = (\widetilde{\sigma} m_\alpha)(\widetilde{\sigma} x) = (\sigma m_\alpha)(\widetilde{\sigma} x),$$

where the last equality holds because $m_\alpha \in K[x]$. Plugging in $x = \alpha$ we deduce that

$$(\sigma m_\alpha)(\widetilde{\sigma}\alpha) = \widetilde{\sigma}\big(m_\alpha(\alpha)\big) = 0$$

as claimed. ♣

Inspired by this, we consider the set of all roots of σm_α:

$$\mathcal{Z}_\alpha := \{\beta \in L' : (\sigma m_\alpha)(\beta) = 0\}.$$

In Step 1 we proved that $\widetilde{\sigma}(\alpha) \in \mathcal{Z}_\alpha$. Our strategy is to first lift σ to an isomorphism $\sigma' : K(\alpha) \xrightarrow{\sim} K'(\beta)$ for some $\beta \in \mathcal{Z}_\alpha$, and then to inductively lift σ' the rest of the way to the desired isomorphism $\widetilde{\sigma} : L \xrightarrow{\sim} L'$. For this to be effective, we need to know that $\mathcal{Z}_\alpha$ is nonempty. In fact, we'll prove a bit more:

<u>STEP 2</u>: $1 \leq |\mathcal{Z}_\alpha| \leq \deg m_\alpha$

Proof. $\mathcal{Z}_\alpha$ is the set of roots of the polynomial $\sigma m_\alpha \in K'[x]$. Since L' is a field, the number of roots of this polynomial in L' is $\leq \deg \sigma m_\alpha = \deg m_\alpha$; this proves the claimed upper bound. Next we turn to the lower bound, which is equivalent to showing that σm_α has a root in L'. First observe that $\deg \sigma m_\alpha \geq 2$ (why?), so σm_α must have a root in some extension of K'. I claim that σm_α splits in L'. Indeed, since $\sigma : K[x] \xrightarrow{\sim} K'[x]$ is a ring isomorphism and $m_\alpha \mid f$, we have that $\sigma m_\alpha \mid \sigma f$. By definition, σf splits in L', whence σm_α must as well. ♢

We've now arrived at the heart of the proof.

<u>STEP 3</u>: For each $\beta \in \mathcal{Z}_\alpha$ there exists a unique lift of σ to a field isomorphism $\sigma' : K(\alpha) \xrightarrow{\sim} K'(\beta)$ sending $\alpha \mapsto \beta$.

Warm-up to proof. How can we construct σ'? Well, we know one isomorphism involving $K(\alpha)$:

$$K(\alpha) \simeq K[x]/(m_\alpha).$$

Similarly, we have

$$K'(\beta) \simeq K'[x]/(m_\beta),$$

where m_β is the minimal polynomial of β over K. Thus to prove that $K(\alpha) \simeq K'(\beta)$, we need to show that $K[x]/(m_\alpha) \simeq K'[x]/(m_\beta)$. What is m_β? I claim that $m_\beta = \sigma m_\alpha$. Indeed, since m_α is monic irreducible and $\sigma : K[x] \xrightarrow{\sim} K'[x]$ is a ring isomorphism, σm_α must also be monic irreducible. (Make sure you can explain why.) By definition, β is a root of σm_α. This implies that $m_\beta \mid \sigma m_\alpha$, whence (by monicity and irreducibility) $m_\beta = \sigma m_\alpha$ as claimed. This makes it clear how to guess the isomorphism $K[x]/(m_\alpha) \xrightarrow{\sim} K'[x]/(m_\beta)$, and the rest of the proof is straightforward. Here we go.

Proof. Uniqueness is clear, since σ' is completely determined by where it sends α. (Make sure you can explain this.) Now we need to construct an isomorphism $\sigma' : K(\alpha) \xrightarrow{\sim} K'(\beta)$ which sends α to β. Given our warm-up above, the natural guess is to take the composition of three isomorphisms:

$$K(\alpha) \xrightarrow{\sim} K[x]/(m_\alpha) \xrightarrow{\sim} K'[x]/(\sigma m_\alpha) \xrightarrow{\sim} K'(\beta)$$

where the first isomorphism is given by $\alpha \mapsto [x]$ (and maps constants to themselves), the second isomorphism is given by $g \mapsto \sigma g$, and the third and final isomorphism is given by $[x] \mapsto \beta$ (and maps constants to themselves). It is easy to verify that all three of these are isomorphisms, and that their composition maps α to β. ♡

Finally, we arrive at the induction step. First, here's a picture of the situation:

$$\begin{tikzcd}
L \arrow[r, dashed, "\widetilde{\sigma}", "\sim"'] & L' \\
K(\alpha) \arrow[u, dash, "\text{splitting ext}^{\text{n}} \text{ of } f \longrightarrow"] \arrow[r, "\sigma'", "\sim"'] & K'(\beta) \arrow[u, dash, "\longleftarrow \text{ splitting ext}^{\text{n}} \text{ of } \sigma f"'] \\
K \arrow[u, dash, "\deg m_\alpha"] \arrow[r, "\sigma", "\sim"'] & K' \arrow[u, dash, "\deg m_\alpha"']
\end{tikzcd}$$

<u>STEP 4</u>: Induct and win.

Proof. Viewing $f \in K(\alpha)[x]$, we see that L is a splitting field of f over $K(\alpha)$, and L' is a splitting field of $\sigma' f = \sigma f$ over $K'(\alpha)$. Furthermore, since $\alpha \notin K$, we have

$$[L : K(\alpha)] = \frac{[L : K]}{\deg m_\alpha} < [L : K].$$

By induction, we therefore know that

(1) $[L : K(\alpha)] = [L' : K'(\beta)]$,
(2) σ' lifts to an isomorphism $\widetilde{\sigma} : L \xrightarrow{\sim} L'$, and
(3) there are at most $[L : K(\alpha)]$ different lifts $\widetilde{\sigma}$ of σ'.

Now we use these to prove the corresponding claims.

(1) $[L : K] = [L' : K']$
(2) σ lifts to $\widetilde{\sigma}$
(3) For each $\beta \in \mathcal{Z}_\alpha$ there is precisely one lift of σ to an isomorphism $\sigma' : K(\alpha) \xrightarrow{\sim} K'(\beta)$ which sends α to β. Since $|\mathcal{Z}_\alpha| \leq \deg m_\alpha$ by Step 2, there are at most $\deg m_\alpha$ lifts of σ to an isomorphism $\sigma' : K(\alpha) \xrightarrow{\sim} K'(\beta)$. Putting this together with the inductive step, we see that there are at most $[L : K]$ lifts of σ to $\widetilde{\sigma}$. ♠

We've proved all three conclusions! □