SPLITTING FIELDS

KEITH CONRAD

1. Introduction

When K is a field and $f(T) \in K[T]$ is nonconstant, there is a field extension K'/K in which $f(T)$ picks up a root, say α. Then $f(T) = (T-\alpha)g(T)$ where $g(T) \in K'[T]$ and $\deg g = \deg f - 1$. By applying the same process to $g(T)$ and continuing in this way finitely many times, we reach an extension L/K in which $f(T)$ splits into linear factors: in $L[T]$,

$$f(T) = c(T-\alpha_1)\cdots(T-\alpha_n).$$

We call the field $K(\alpha_1, \ldots, \alpha_n)$ that is generated by the roots of $f(T)$ over K a *splitting field of* $f(T)$ *over* K. The idea is that in a splitting field we can find a full set of roots of $f(T)$ and *no smaller field extension of* K has that property. Let's look at some examples.

Example 1.1. A splitting field of T^2+1 over $\mathbf{R}$ is $\mathbf{R}(i, -i) = \mathbf{R}(i) = \mathbf{C}$.

Example 1.2. A splitting field of T^2-2 over $\mathbf{Q}$ is $\mathbf{Q}(\sqrt{2})$, since we pick up two roots $\pm\sqrt{2}$ in the field generated by just one of the roots. A splitting field of T^2-2 over $\mathbf{R}$ is $\mathbf{R}$ since T^2-2 splits into linear factors in $\mathbf{R}[T]$.

Example 1.3. In $\mathbf{C}[T]$, a factorization of T^4-2 is $(T-\sqrt[4]{2})(T+\sqrt[4]{2})(T-i\sqrt[4]{2})(T+i\sqrt[4]{2})$. A splitting field of T^4-2 over $\mathbf{Q}$ is

$$\mathbf{Q}(\sqrt[4]{2}, i\sqrt[4]{2}) = \mathbf{Q}(\sqrt[4]{2}, i).$$

In the second description one of the field generators is not a root of the original polynomial T^4-2. This is a simpler way of writing the splitting field.

A splitting field of T^4-2 over $\mathbf{R}$ is $\mathbf{R}(\sqrt[4]{2}, i\sqrt[4]{2}) = \mathbf{R}(i) = \mathbf{C}$.

These examples illustrate that, as with irreducibility, the choice of base field is an important part of determining the splitting field. Over $\mathbf{Q}$, T^4-2 has a splitting field that is an extension of degree 8, while over $\mathbf{R}$ the splitting field of the same polynomial is an extension (of $\mathbf{R}$!) of degree 2.

The splitting field of a polynomial is a bigger extension, in general, than the extension generated by a single root.[1] For instance, $\mathbf{Q}(\sqrt[4]{2}, i)$ is bigger than $\mathbf{Q}(\sqrt[4]{2})$. If we are dealing with an *irreducible* polynomial, adjoining a single root of it to the base field always leads to a field that, independently of the choice of root, is unique up to isomorphism over K: if $\pi(T)$ is irreducible in $K[T]$ and α is any root of $\pi(T)$ in a field extension of K then $K(\alpha) \cong K[T]/(\pi(T))$ by a field isomorphism fixing K. More precisely, evaluation at α is a surjective homomorphism $K[T] \to K(\alpha)$ fixing K and having kernel $(\pi(T))$, so there is an induced field isomorphism $K[T]/(\pi(T)) \to K(\alpha)$. Adjoining a single root of a *reducible* polynomial to a field might lead to non-isomorphic fields if the root changes. For instance, if $f(T) = (T^2-2)(T^2-3)$ in $\mathbf{Q}[T]$ then adjoining a single root to $\mathbf{Q}$ might result in $\mathbf{Q}(\sqrt{2})$

[1] There is no standard name in English for the extension of a field generated by a single root of a polynomial. One term I have seen used is a "root field," so $\mathbf{Q}(\sqrt[4]{2})$ is a root field for T^4-2 over $\mathbf{Q}$.

or $\mathbf{Q}(\sqrt{3})$, and these fields are not isomorphic. But we should expect that any two ways of creating a splitting field for $(T^2-2)(T^2-3)$ over $\mathbf{Q}$ – using *all* the roots, not just one root – should lead to isomorphic fields. Our main task here is to show that something like this is true in general.

Theorem 1.4. *Let K be a field and $f(T)$ be nonconstant in $K[T]$. If L and L' are splitting fields of $f(T)$ over K then $[L:K]=[L':K]$, there is a field isomorphism $L \to L'$ fixing all of K ($c \mapsto c$ for all $c \in K$), and the number of such isomorphisms $L \to L'$ is at most $[L:K]$.*

$$\begin{tikzcd} L \arrow[rr, dashed] \arrow[dr, dash] & & L' \arrow[dl, dash] \\ & K & \end{tikzcd}$$

Example 1.5. Every splitting field of T^4-2 over $\mathbf{Q}$ has degree 8 over $\mathbf{Q}$ and is isomorphic to $\mathbf{Q}(\sqrt[4]{2}, i)$.

Example 1.6. Every splitting field of $(T^2-2)(T^2-3)$ over $\mathbf{Q}$ has degree 4 over $\mathbf{Q}$ and is isomorphic to $\mathbf{Q}(\sqrt{2},\sqrt{3})$.

This theorem is not only saying that two splitting fields of $f(T)$ over K are isomorphic, but that they are isomorphic *by an isomorphism fixing all of K*. Our interest in the splitting fields is not as abstract fields, but as extensions of K, and an isomorphism fixing all of K respects this viewpoint.

In Theorem 1.4 we are *not* saying the isomorphism $L \to L'$ fixing K is unique. For instance, $\mathbf{C}$ and $\mathbf{R}[x]/(x^2+1)$ are both splitting fields of T^2+1 over $\mathbf{R}$ and there are two different isomorphisms $\mathbf{R}[x]/(x^2+1) \to \mathbf{C}$ that fix all real numbers: $f(x) \bmod x^2+1 \mapsto f(i)$ and $f(x) \bmod x^2+1 \mapsto f(-i)$.

Our proof of Theorem 1.4 will use an inductive argument that will only work by proving a *stronger* theorem, where the single base field K is replaced by two isomorphic base fields K and K'. Some preliminary ideas needed in the proof are introduced in Section 2 before we get to the proof itself in Section 3.

2. Homomorphisms on Polynomial Coefficients

To prove Theorem 1.4 we will use an inductive argument involving homomorphisms between polynomial rings. Any field homomorphism $\sigma\colon F \to F'$ extends to a function $\sigma\colon F[T] \to F'[T]$ as follows: for $f(T) = \sum_{i=0}^n c_i T^i \in F[T]$, set $(\sigma f)(T) = \sum_{i=0}^n \sigma(c_i)T^i \in F'[T]$. We call this map "applying σ to the coefficients." Writing $f(T) = c_nT^n + c_{n-1}T^{n-1} + \cdots + c_1T + c_0$, with $c_i \in F$, for $\alpha \in F$ we have

$$\begin{aligned} \sigma(f(\alpha)) &= \sigma\left(c_n\alpha^n + c_{n-1}\alpha^{n-1} + \cdots + c_1\alpha + c_0\right) \\ &= \sigma(c_n)\sigma(\alpha)^n + \sigma(c_{n-1})\sigma(\alpha)^{n-1} + \cdots + \sigma(c_1)\sigma(\alpha) + \sigma(c_0) \\ &= (\sigma f)(\sigma(\alpha)). \qquad (2.1) \end{aligned}$$

If $f(\alpha) = 0$ then $(\sigma f)(\sigma(\alpha)) = \sigma(f(\alpha)) = \sigma(0) = 0$, so σ sends any root of $f(T)$ in F to a root of $(\sigma f)(T)$ in F'.

Example 2.1. If $f(T) \in \mathbf{C}[T]$ and $\alpha \in \mathbf{C}$ then $\overline{f(\alpha)} = \overline{f}(\overline{\alpha})$, where the overline means complex conjugation and $\overline{f}$ is the polynomial whose coefficients are complex conjugates of the coefficients of f. If α is a root of $f(T)$ then $\overline{\alpha}$ is a root of $\overline{f}(T)$.

If $f(T)$ has real coefficients then $\overline{f(\alpha)} = f(\overline{\alpha})$ because $\overline{f} = f$ when f has real coefficients, and in this case if α is a root of $f(T)$ then $\overline{\alpha}$ is also a root of $f(T)$.

Example 2.2. Let $F = F' = \mathbf{Q}(i)$, $\sigma\colon F \to F'$ be complex conjugation, and $f(T) = T^2 + iT + 1 - 3i$. In $F'[T]$, $(\sigma f)(T) = T^2 + \sigma(i)T + \sigma(1-3i) = T^2 - iT + 1 + 3i$.

For any $\alpha \in F$, we have

$$\sigma(f(\alpha)) = \sigma(\alpha^2 + i\alpha + 1 - 3i) = \sigma(\alpha^2) + \sigma(i\alpha) + \sigma(1-3i) = \sigma(\alpha)^2 - i\sigma(\alpha) + 1 + 3i,$$

and observe that this final value is $(\sigma f)(\sigma(\alpha))$, *not* $(\sigma f)(\alpha)$.

Check that applying σ to coefficients is a ring homomorphism $F[T] \to F'[T]$: $\sigma(f+g) = \sigma f + \sigma g$ and $\sigma(fg) = (\sigma f)(\sigma g)$ for any f and g in $F[T]$, and trivially $\sigma(1) = 1$. It also preserves degrees and the property of being monic. If $f(T)$ splits completely in $F[T]$ then $(\sigma f)(T)$ splits completely in $F'[T]$ since linear factors get sent to linear factors. Finally, if σ is a field isomorphism from F to F' then applying it to coefficients gives us a ring isomorphism $F[T] \to F'[T]$, since applying the inverse of σ to coefficients of $F'[T]$ is an inverse of applying σ to coefficients on $F[T]$.

Example 2.3. Continuing with the notation of the previous example, $T^2 + iT + 1 - 3i = (T - (1+i))(T + (1+2i))$ and

$$\sigma(T - (1+i))\sigma(T + (1+2i)) = (T - 1 + i)(T + 1 - 2i) = T^2 - iT + 1 + 3i,$$

which is $\sigma(T^2 + iT + 1 - 3i)$.

3. Proof of Theorem 1.4

Rather than directly prove Theorem 1.4, we formulate a more general theorem where the triangle diagram in Theorem 1.4 is expanded into a square with isomorphic fields at the bottom.

Theorem 3.1. *Let $\sigma\colon K \to K'$ be an isomorphism of fields, $f(T) \in K[T]$, L be a splitting field of $f(T)$ over K and L' be a splitting field of $(\sigma f)(T)$ over K'. Then $[L:K] = [L':K']$, σ extends to an isomorphism $L \to L'$ and the number of such extensions is at most $[L:K]$.*

$$\begin{tikzcd} L \arrow[r, dashed] \arrow[d, dash] & L' \arrow[d, dash] \\ K \arrow[r, "\sigma"] & K' \end{tikzcd}$$

Theorem 1.4 is a special case of Theorem 3.1 where $K' = K$ and σ is the identity on K.

Proof. This proof is long.

We argue by induction on $[L:K]$. If $[L:K] = 1$ then $f(T)$ splits completely in $K[T]$ so $(\sigma f)(T)$ splits completely in $K'[T]$. Therefore $L' = K'$, so $[L':K'] = 1$. The only extension of σ to L in this case is σ, so the number of extensions of σ to L is at most $1 = [L:K]$.

Suppose $[L:K] > 1$. Since L is generated as a field over K by the roots of $f(T)$, $f(T)$ has a root $\alpha \in L$ that is not in K. Fix this α for the rest of the proof. Let $\pi(T)$ be the minimal polynomial of α over K, so α is a root of $\pi(T)$ and $\pi(T) \mid f(T)$ in $K[T]$. If there's an isomorphism $\widetilde{\sigma}\colon L \to L'$ extending σ, then $\widetilde{\sigma}(\alpha)$ is a root of $(\sigma\pi)(T)$: using (2.1),

$$\pi(\alpha) = 0 \Rightarrow \widetilde{\sigma}(\pi(\alpha)) = \widetilde{\sigma}(0) = 0 \Rightarrow (\widetilde{\sigma}\pi)(\widetilde{\sigma}(\alpha)) = 0 \Rightarrow (\sigma\pi)(\widetilde{\sigma}(\alpha)) = 0,$$

where the last step comes from $\pi(T)$ having coefficients in K (so $\widetilde{\sigma} = \sigma$ on those coefficients). Therefore values of $\widetilde{\sigma}(\alpha)$ – to be determined – must come from roots of $(\sigma\pi)(T)$.

Now we show $(\sigma\pi)(T)$ has a root in L'. Since $\sigma\colon K \to K'$ is an isomorphism, applying σ to coefficients is a ring isomorphism $K[T] \to K'[T]$ (the inverse applies σ^{-1} to coefficients in $K'[T]$), so $\pi(T) \mid f(T) \Rightarrow (\sigma\pi)(T) \mid (\sigma f)(T)$. Since $\pi(T)$ is monic irreducible, $(\sigma\pi)(T)$ is monic irreducible (ring isomorphisms preserve irreducibility). Since $(\sigma f)(T)$ splits completely in $L'[T]$ by the definition of L', its factor $(\sigma\pi)(T)$ splits completely in $L'[T]$. Pick a root $\alpha' \in L'$ of $(\sigma\pi)(T)$. Set $d = \deg \pi(T) = \deg(\sigma\pi)(T)$, so $d > 1$ (since $d = [K(\alpha) : K] > 1$). This information is in the diagram below, and there are at most d choices for α' in L'. The minimal polynomials of α and α' over K and K' (resp.) are $\pi(T)$ and $(\sigma\pi)(T)$.

$$\begin{tikzcd} L \arrow[r, dashed] \arrow[d, dash] & L' \arrow[d, dash] \\ K(\alpha) \arrow[r, dashed] \arrow[d, dash, "d"'] & K'(\alpha') \arrow[d, dash, "d"] \\ K \arrow[r, "\sigma"] & K' \end{tikzcd}$$

There is a *unique* extension of $\sigma\colon K \to K'$ to a field isomorphism $K(\alpha) \to K'(\alpha')$ such that $\alpha \mapsto \alpha'$. First we show uniqueness. If $\sigma'\colon K(\alpha) \to K'(\alpha')$ extends σ and $\sigma'(\alpha) = \alpha'$, then the value of σ' is determined everywhere on $K(\alpha)$ because $K(\alpha) = K[\alpha]$ and

$$\sigma'\left(\sum_{i=0}^{m} c_i\alpha^i\right) = \sum_{i=0}^{m} \sigma'(c_i)(\sigma'(\alpha))^i = \sum_{i=0}^{m} \sigma(c_i)\alpha'^i. \tag{3.1}$$

In other words, a K-polynomial in α goes to the corresponding K'-polynomial in α' where σ is applied to the coefficients. Thus there's at most one σ' extending σ with $\sigma'(\alpha) = \alpha'$.

To prove σ' exists, we will build an isomorphism from $K(\alpha)$ to $K'(\alpha')$ with the desired behavior on K and α. Any element of $K(\alpha)$ can be written as $f(\alpha)$ where $f(T) \in K[T]$ (a polynomial). It can be like this for more than one polynomial: perhaps $f(\alpha) = g(\alpha)$ where $g(T) \in K[T]$. In that case $f(T) \equiv g(T) \bmod \pi(T)$, so $f(T) = g(T) + \pi(T)h(T)$. Applying σ to coefficients on both sides, which is a ring homomorphism $K[T] \to K'[T]$, we have $(\sigma f)(T) = (\sigma g)(T) + (\sigma\pi)(T)(\sigma h)(T)$, and setting $T = \alpha'$ kills off the second term, leaving us with $(\sigma f)(\alpha') = (\sigma g)(\alpha')$. Therefore it is *well-defined* to set $\sigma'\colon K(\alpha) \to K'(\alpha')$ by $f(\alpha) \mapsto (\sigma f)(\alpha')$. This function is σ on K and sends α to α'. Since applying σ to coefficients is a ring homomorphism $K[T] \to K'[T]$, σ' is a field homomorphism $K(\alpha) \to K'(\alpha')$. For example, if x and y in $K(\alpha)$ are written as $f(\alpha)$ and $g(\alpha)$, then $xy = f(\alpha)g(\alpha) = (fg)(\alpha)$ (evaluation at α is multiplicative) so

$$\sigma'(xy) = \sigma(fg)(\alpha') = ((\sigma f)(\sigma g))(\alpha') = (\sigma f)(\alpha')(\sigma g)(\alpha') = \sigma'(x)\sigma'(y).$$

Using $\sigma^{-1}\colon K' \to K$ to go the other way shows σ' is a field isomorphism.

Place σ' in the field diagram below.

$$\begin{tikzcd} L \arrow[r, dashed] \arrow[d, dash] & L' \arrow[d, dash] \\ K(\alpha) \arrow[r, "\sigma'"] \arrow[d, dash, "d"'] & K'(\alpha') \arrow[d, dash, "d"] \\ K \arrow[r, "\sigma"] & K' \end{tikzcd}$$

Now we can finally induct on degrees of splitting fields. Take as new base fields $K(\alpha)$ and $K'(\alpha')$, which are isomorphic by σ'. Since L is a splitting field of $f(T)$ over K, it's also a splitting field of $f(T)$ over the larger field $K(\alpha)$. Similarly, L' is a splitting field of $(\sigma f)(T)$ over K' and thus also over the larger field $K'(\alpha')$. Since $f(T)$ has its coefficients in K and $\sigma' = \sigma$ on K, $(\sigma' f)(T) = (\sigma f)(T)$. So the top square in the above diagram is like the square in the theorem itself, except the splitting field degrees dropped: since $d > 1$,

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

By induction, $[L : K(\alpha)] = [L' : K'(\alpha')]$ and σ' has an extension to a field isomorphism $L \to L'$. Since σ' extends σ, σ itself has an extension to an isomorphism $L \to L'$ and

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

(If the proof started with $K' = K$, it would usually be false that $K(\alpha) = K'(\alpha')$, so Theorem 1.4 is not directly accessible to our inductive proof.)

It remains to show σ has at most $[L : K]$ extensions to an isomorphism $L \to L'$. First we show every isomorphism $\widetilde{\sigma} \colon L \to L'$ extending σ is the extension of some intermediate isomorphism σ' of $K(\alpha)$ with a subfield of L'. From the start of the proof, $\widetilde{\sigma}(\alpha)$ must be a root of $(\sigma\pi)(T)$. Define $\alpha' := \widetilde{\sigma}(\alpha)$. Since $\widetilde{\sigma}|_K = \sigma$, the restriction $\widetilde{\sigma}|_{K(\alpha)}$ is a field homomorphism that is σ on K and sends α to α', so $\widetilde{\sigma}|_{K(\alpha)}$ is an isomorphism from $K(\alpha)$ to $K'(\widetilde{\sigma}(\alpha)) = K'(\alpha')$. Thus $\widetilde{\sigma}$ on L is a lift of the intermediate field isomorphism $\sigma' := \widetilde{\sigma}|_{K(\alpha)}$.

$$\begin{tikzcd}
L \arrow[r, "\widetilde{\sigma}"] \arrow[d, dash] & L' \arrow[d, dash] \\
K(\alpha) \arrow[r, "\sigma'"] \arrow[d, dash, "d"'] & K'(\alpha') \arrow[d, dash, "d"] \\
K \arrow[r, "\sigma"] & K'
\end{tikzcd}$$

By induction on degrees of splitting fields, σ' lifts to at most $[L : K(\alpha)]$ isomorphisms $L \to L'$. Since σ' is determined by $\sigma'(\alpha)$, which is a root of $(\sigma\pi)(T)$, the number of maps σ' is at most $\deg(\sigma\pi)(T) = d$. The number of isomorphisms $L \to L'$ that lift σ is the number of homomorphisms $\sigma' \colon K(\alpha) \to L'$ lifting σ times the number of extensions of each σ' to an isomorphism $L \to L'$, and that total is at most $d[L : K(\alpha)] = [L : K]$. $\square$

Example 3.2. Let $K = K' = \mathbf{Q}$ and $f(T) = T^4 - 2$, with splitting field $\mathbf{Q}(\sqrt[4]{2}, i)$ over $\mathbf{Q}$. Let $\alpha = \sqrt[4]{2}$, $\alpha' = i\sqrt[4]{2}$, $\sigma \colon K \to K'$ be the identity (the only field isomorphism of $\mathbf{Q}$ to itself), and $\sigma'(\sqrt[4]{2}) = i\sqrt[4]{2}$. From the proof, there are at most $8/4 = 2$ extensions $\widetilde{\sigma}$ of σ' to a field automorphism of $\mathbf{Q}(\sqrt[4]{2}, i)$. These are determined by whether $\widetilde{\sigma}(i)$ can be i or $-i$.

$$\begin{tikzcd}
\mathbf{Q}(\sqrt[4]{2}, i) \arrow[r, "\widetilde{\sigma}"] \arrow[d, dash] & \mathbf{Q}(\sqrt[4]{2}, i) \arrow[d, dash] \\
\mathbf{Q}(\sqrt[4]{2}) \arrow[r, "\sigma'"] \arrow[d, dash, "4"'] & \mathbf{Q}(i\sqrt[4]{2}) \arrow[d, dash, "4"] \\
\mathbf{Q} \arrow[r, "\sigma"] & \mathbf{Q}
\end{tikzcd}$$

Example 3.3. The field $\mathbf{Q}(\sqrt{2},\sqrt{3})$, a splitting field of $(T^2-2)(T^2-3)$ over $\mathbf{Q}$, has degree 4 over $\mathbf{Q}$. In Theorem 3.1 if we use $K = K' = \mathbf{Q}$, $L = L' = \mathbf{Q}(\sqrt{2},\sqrt{3})$, and $\sigma =$ the identity map on $\mathbf{Q}$, then there are at most 4 field automorphisms of $\mathbf{Q}(\sqrt{2},\sqrt{3})$ that are the identity on $\mathbf{Q}$. This does *not* guarantee that our bound of 4 is achieved (although it is).

4. The Effect of Separability

Now we will add a separability assumption to Theorem 3.1 and get a stronger conclusion: the upper bound $[L : K]$ in Theorem 3.1 for counting isomorphisms $L \to L'$ extending a fixed isomorphism $K \to K'$ is reached.

Theorem 4.1. *Let $\sigma\colon K \to K'$ be an isomorphism of fields, $f(T) \in K[T]$, L be a splitting field of $f(T)$ over K and L' be a splitting field of $(\sigma f)(T)$ over K'. If $f(T)$ is separable then there are $[L : K]$ extensions of σ to an isomorphism $L \to L'$.*

Proof. The case $[L : K] = 1$ is easy, so assume $[L : K] > 1$. As in the previous proof, let α be a root of $f(T)$ that is not in K, $\pi(T)$ be its minimal polynomial over K, and $d = \deg \pi(T)$.

Because $f(T)$ is separable, $(\sigma f)(T)$ is separable too. One way to show this is with the characterization of separability in terms of relative primality to the derivative: we can write

$$f(T)u(T) + f'(T)v(T) = 1 \tag{4.1}$$

for some $u(T)$ and $v(T)$ in $K[T]$. Applying σ to coefficients commutes with forming derivatives (that is, $\sigma(f') = (\sigma f)'$), so if we apply σ to coefficients in (4.1) then we get

$$(\sigma f)(T)(\sigma u)(T) + (\sigma f)'(T)(\sigma v)(T) = 1,$$

so $(\sigma f)(T)$ and its derivative are relatively prime in $K'[T]$, which proves $(\sigma f)(T)$ is separable. Any factor of a separable polynomial is separable, so $(\sigma\pi)(T)$ is separable and therefore has d roots in L' since it splits completely over L'.

In the proof of Theorem 3.1 we showed the different extensions of σ to a homomorphism $\sigma'\colon K(\alpha) \to L'$ are each determined by choosing different roots α' of $(\sigma\pi)(T)$ in L' and letting $\alpha \mapsto \alpha'$. Since $(\sigma\pi)(T)$ splits completely over L' and is separable, it has d roots in L', so the number of homomorphisms σ' is d (and not just at most d).

$$\begin{tikzcd}
L \arrow[r, dashed] \arrow[d, dash] & L' \arrow[d, dash] \\
K(\alpha) \arrow[r, "\sigma'"] \arrow[d, dash, "d"'] & K'(\alpha') \arrow[d, dash, "d"] \\
K \arrow[r, "\sigma"] & K'
\end{tikzcd}$$

Since $[L : K(\alpha)] < [L : K]$ and L is a splitting field of $f(T)$ over $K(\alpha)$, by induction on the degree of a splitting field (along with the new separability hypothesis on $f(T)$), each σ' has $[L : K(\alpha)]$ extensions to an isomorphism $L \to L'$. Since there are d choices for σ', the total number of extensions of σ to an isomorphism $L \to L'$ is $d[L : K(\alpha)] = [L : K]$. $\square$

Corollary 4.2. *If L/K is the splitting field of a separable polynomial then there are $[L : K]$ automorphisms of L that fix the elements of K.*

Proof. Apply Theorem 4.1 with $K' = K$, $L' = L$, and σ the identity function on K. $\square$

Example 4.3. The extension $\mathbf{Q}(\sqrt{2}, \sqrt{3})/\mathbf{Q}$ is a splitting field of $(T^2-2)(T^2-3)$. Its degree is 4, so there are 4 automorphisms of $\mathbf{Q}(\sqrt{2}, \sqrt{3})$ fixing $\mathbf{Q}$. This improves Example 3.3 from an upper bound of 4 to an exact count of 4. We will use this *a priori* count to find all the automorphisms.

Since $\sqrt{2}$ and $\sqrt{3}$ generate the extension $\mathbf{Q}(\sqrt{2}, \sqrt{3})/\mathbf{Q}$, any automorphism of the extension is determined by $\sigma(\sqrt{2})$ and $\sigma(\sqrt{3})$, which are $\pm\sqrt{2}$ and $\pm\sqrt{3}$. Combining the choices in all possible ways, we get at most 4 choices for σ. See the table below. Corollary 4.2 says there are 4 choices for σ, so every possibility in the table *must* work. Notice that we draw this conclusion because we know in advance how many σ's exist, before computing the possibilities explicitly.

$\sigma(\sqrt{2})$	$\sigma(\sqrt{3})$
$\sqrt{2}$	$\sqrt{3}$
$\sqrt{2}$	$-\sqrt{3}$
$-\sqrt{2}$	$\sqrt{3}$
$-\sqrt{2}$	$-\sqrt{3}$

Example 4.4. Let $K = \mathbf{Q}(i)$ and σ be complex conjugation on K. The number $1+2i$ is not a square in K (check $1+2i = (a+bi)^2$ has no solution with $a, b \in \mathbf{Q}$). Thus the field $L = \mathbf{Q}(i, \sqrt{1+2i})$ has degree 2 over K. Complex conjugation on K sends $T^2-(1+2i)$ to $T^2-(1-2i)$ in $K[T]$, so by Theorem 4.1 with $K' = K$, complex conjugation on K extends in two ways to an isomorphism $L \to L'$, where $L' = \mathbf{Q}(i, \sqrt{1-2i})$.

$$\begin{tikzcd} L \arrow[r, dashed] \arrow[d, dash, "2"'] & L' \arrow[d, dash, "2"] \\ K \arrow[r, "\sigma"] & K \end{tikzcd}$$

These two extensions of complex conjugation $K \to K$ to an isomorphism $L \to L'$ are determined by where $\sqrt{1+2i}$ is sent: a root of $T^2-(1+2i)$ must go to a root of $T^2-(1-2i)$, so $\sqrt{1+2i}$ is sent to a square root of $1-2i$ in L'. Theorem 4.1 tells us that both choices work: each choice arises from an isomorphism $L \to L'$ extending complex conjugation.

In Theorem 4.1, it's crucial that L' is the splitting field of the polynomial $(\sigma f)(T)$, and not the splitting field of $f(T)$ itself (unless σ is the identity on K). Theorem 4.1 does *not* say that each automorphism $\sigma\colon K \to K$ extends to an automorphism of a splitting field of a polynomial over K; in fact, such an extension to a splitting field might not exist if σ is not the identity on K.

Example 4.5. Consider the quadratic extension $\mathbf{Q}(\sqrt[4]{2})/\mathbf{Q}(\sqrt{2})$. The top field is a splitting field of $T^2-\sqrt{2}$ over $\mathbf{Q}(\sqrt{2})$. The conjugation automorphism $a+b\sqrt{2} \mapsto a-b\sqrt{2}$ on $\mathbf{Q}(\sqrt{2})$ has no extension to an automorphism of $\mathbf{Q}(\sqrt[4]{2})$. Indeed, we will show every automorphism of $\mathbf{Q}(\sqrt[4]{2})$ fixes $\sqrt{2}$, so it can't restrict to conjugation on $\mathbf{Q}(\sqrt{2})$, which sends $\sqrt{2}$ to $-\sqrt{2}$.

If $\sigma'\colon \mathbf{Q}(\sqrt[4]{2}) \to \mathbf{Q}(\sqrt[4]{2})$ is a field automorphism, then $\sigma'(\sqrt[4]{2})$ must be a fourth root of 2 in $\mathbf{Q}(\sqrt[4]{2})$. This field is inside $\mathbf{R}$, where the only fourth roots of 2 are $\pm\sqrt[4]{2}$, so $\sigma'(\sqrt[4]{2}) = \pm\sqrt[4]{2}$ for some choice of sign. Regardless of which sign occurs, squaring both sides removes it and leaves us with $\sigma'(\sqrt{2}) = \sqrt{2}$ since $\sigma'(\sqrt{2}) = \sigma'(\sqrt[4]{2}^2) = (\sigma'(\sqrt[4]{2}))^2 = (\pm\sqrt[4]{2})^2 = \sqrt{2}$.