I.C. Splitting fields

Let $f \in \mathbb{Q}[x]$ be a monic polynomial of degree n. We know that f has a unique factorization into irreducibles in $\mathbb{Q}[x]$, $f = f_1 \cdots f_k$. In $\mathbb{C}[x]$, it splits completely into linear factors, $f(x) = \prod_{i=1}^{n}(x - \alpha_i)$, by the Fundamental Theorem of Algebra. But then this also holds over $L := \mathbb{Q}(\alpha_1, \ldots, \alpha_n) \subset \mathbb{C}$, and it can't hold for any smaller field. Several questions arise:

(1) *What is the degree $d := [L{:}\mathbb{Q}]$?* If f is irreducible over $\mathbb{Q}$ (and $n > 2$), this need not be n, which is only the lower bound. For $x^3 - 1$ it is true that $d = 3$, but for $x^3 - 2$ we have $d = 6$, since $\sqrt[3]{2}\zeta_3 \notin \mathbb{Q}(\sqrt[3]{2})$.

(2) *For general K, and $f \in K[x]$, must there exist an L over which f splits into linear factors?* For instance, maybe $K = \mathbb{F}_{p^k}$ is a finite field, or maybe it is the "function field of an algebraic curve" (viz., $\mathbb{C}(x)[y]/(F(x,y))$); in either case, we can't embed K into $\mathbb{C}$ as we did above.

(3) *Is a minimal field extension L/K such that $f \in K[x]$ splits in $L[x]$ unique?* One could both worry about different embeddings of K into L, or about whether L itself is unique. More precisely, the question is: given $\imath \colon K \hookrightarrow L$ and $\imath' \colon K \hookrightarrow L'$ extensions of this type, do we have an isomorphism $\psi \colon L \to L'$ with $\psi \circ \imath = \imath'$?

As we shall see below, (2) and (3) have affirmative answers. (Even for $\mathbb{Q}$, we'll end up getting around the use of $\mathbb{C}$ above.) For (1), we will say more later. First, let's give a rigorous

I.C.1. Definition. Let K be a field, $f \in K[x]$ a polynomial, and L/K an extension.

(i) f **splits over L** if we can write $f(x) = c\prod_{i=1}^{n}(x - \alpha_i)$ with $\alpha_i \in L$ (and $c \in K$).

(ii) $L(/K)$ is a **splitting field (extension) for f** if f splits over L (as $c\prod_i(x - \alpha_i)$) and $L = K(\alpha_1, \ldots, \alpha_n)$.

I.C.2. PROPOSITION. *If f splits over L as above, $L = K(\alpha_1, \ldots, \alpha_n)$ is equivalent to minimality of L: the nonexistence of L'/K, with $L \supsetneq L' \supset K$, over which f splits.*

PROOF. Suppose L is minimal; properness of the containment $L \supset K(\alpha_1, \ldots, \alpha_n)$ would yield a contradiction (take L' to be the smaller field), and so it's an equality.

Conversely, suppose $L = K(\alpha_1, \ldots, \alpha_n) \supset L' \supset K$, with f split over L': i.e., $f = c \prod_i (x - \alpha_i')$, with $\alpha_i' \in L'$. But these will also be n roots (possibly with multiplicity) of f in L, and the roots of f (and their multiplicities) are unique because $L[x]$ is a UFD. They generate L over K by assumption, which forces $L' = L$. □

I.C.3. REMARK. Clearly, if L/K is a splitting field extension, then by the Tower Law L/K is finite, *a fortiori* algebraic.

Existence of splitting fields.

Since there is now no $\mathbb{C}$ in sight, let's remind ourselves of how we can algebraically construct extensions containing a root "out of thin air".

I.C.4. LEMMA. *If $f \in K[x]$ is irreducible of degree n, then there exists a simple extension $K(\alpha)/K$ with $[K(\alpha){:}K] = n$ and $f(\alpha) = 0$.*

PROOF. We have the natural field extension

$$\imath\colon K \hookrightarrow L := K[x]/(f(x)).$$

Let $\alpha \in L$ denote the image of x under the quotient map $\nu\colon K[x] \twoheadrightarrow L$; then $L = K(\alpha)$, and $f(\alpha) = f(\nu(x)) = \nu(f(x)) = 0$. Hence $f \in (m_\alpha)$, and irreducibility of f then gives $f = km_\alpha$ ($k \in K$). Conclude that $[L{:}K] = \deg(m_\alpha) = \deg(f) = n$. □

I.C.5. THEOREM. *Given $f \in K[x]$ of degree n (not necessarily irreducible), there exists a splitting field extension L/K with $[L{:}K] \big| n!$.*

PROOF. Induce on n (it's clear for $n = 1$). There are two cases:

(a) <u>*f not irreducible over K.*</u> Write $f = gh$ in $K[x]$, with $\deg(g) = s$ and $\deg(h) = t$ both $< n$. By induction, there exists a splitting field

L_0/K for g, with $[L_0{:}K]\big|s!$; so $g = \mu_g(x-\beta_1)\cdots(x-\beta_s)$ with $\mu_g \in K$ and $L_0 = K(\beta_1,\ldots,\beta_s)$.

Now consider h as a polynomial in $L_0[x]$, and apply induction to get a splitting field extension L/L_0 for h with $[L{:}L_0]\big|t!$; that is, $h = \mu_h(x-\gamma_1)\cdots(x-\gamma_t)$ with $\mu_h \in L_0$ and $L = L_0(\gamma_1,\ldots,\gamma_t) = K(\beta_1,\ldots,\beta_s,\gamma_1,\ldots,\gamma_t)$. Moreover, since $\mu_g\mu_h$ is the coefficient of x^n in f, it belongs to K. So we conclude (by I.C.1(ii)) that L/K is a splitting field extension for f, and that $[L{:}K] = [L{:}L_0][L_0{:}K]$ divides $s!t!$ hence divides $(s+t)! = n!$ (since $\frac{(s+t)!}{s!t!} = \binom{s+t}{s} \in \mathbb{N}$).

(b) $\underline{f \text{ irreducible over } K}$. By I.C.4, there exists $K(\alpha)/K$ of degree n, with[9] $f(x) = (x-\alpha)g(x)$ in $K(\alpha)[x]$. Since $\deg(g) = n-1$, we apply induction to get a splitting field extension $L/K(\alpha)$ for g, with $[L{:}K(\alpha)]\big|(n-1)!$. Moreover, we get $g(x) = \mu(x-\beta_1)\cdots(x-\beta_{n-1})$, with $\mu \in K(\alpha)$ and $\beta_i \in L$. Clearly $L = K(\alpha,\beta_1,\ldots,\beta_{n-1})$ and $\mu \in K$. Hence L/K is a splitting field extension, and $[L{:}K] = [L{:}K(\alpha)][K(\alpha){:}K]$ divides $(n-1)!n = n!$. □

I.C.6. REMARK. So for an irreducible polynomial $f \in K[x]$, we see that the degree d of a splitting field extension satisfies $n \leq d \leq n!$ and also divides $n!$. In particular, if $n = 2$, then $d = 2$, which reflects the fact that adjoining one root α of an irreducible quadratic has to give the other, by dividing $f(x)/(x-\alpha)$ in $K(\alpha)$.

Some examples of splitting fields.

I.C.7. EXAMPLE. Keeping K arbitrary, consider a quadratic polynomial $f(x) = x^2 + ax + b \in K[x]$. We break the analysis of the splitting field into two cases.

$\underline{\mathrm{char}(K) \neq 2}$: We may write $f(x) = (x + \frac{a}{2})^2 - \frac{\mu}{4}$, where $\mu := a^2 - 4b$, and replace f by $g(x) := x^2 - \frac{\mu}{4}$. Clearly g splits over K (and the splitting field extension is trivial) iff μ has a square root in K. Otherwise, the splitting field extension has degree 2, and is $K(\sqrt{\mu})$; that is, the quadratic formula tells us that the splitting field is obtained by adjoining a square root.

[9] That $(x-\alpha) \mid f(x)$ in $K(\alpha)[x]$ is [**Algebra I**, III.G.16].

char$(K) = 2$: We can't divide by 2 here, so the quadratic formula doesn't work. For simplicity, let's take $K = \mathbb{Z}_2$, so that there are only four polynomials x^2, $x^2 + x$, $x^2 + 1$, and $x^2 + x + 1$ to analyze, and the first three split over K. That leaves $f(x) := x^2 + x + 1$, which is irreducible (why?). Let L/K be its splitting field extension. This is of degree 2, hence has 4 elements: $0, 1, \alpha, \beta$.

At least one of α, β must be a root, say α. But then $(\alpha + 1)^2 + (\alpha + 1) + 1 = \alpha^2 + 1 + \alpha + 1 + 1 = \alpha^2 + \alpha + 1 = 0 \implies \alpha + 1$ is a root; since it can't be 0, 1, or α, we have $\alpha + 1 = \beta$. So $f(x) = (x - \alpha)(x - \beta)$, and we also get $\alpha + \beta = 1 = \alpha\beta$. To finish off the multiplication table, $\alpha^2 = \alpha + 1 = \beta$ and $\beta^2 = \beta + 1 = \alpha$.

This also reveals that L is not obtained from K by adjoining a square root: because α and β are not square roots of anything in $K = \{0, 1\}$! (On the other hand, $0 = (\alpha - 1)f(\alpha) = \alpha^3 - 1 \implies \alpha$ is a cube root of 1.)

Next we turn to several examples with $K = \mathbb{Q}$. You should make sure you can draw the tower diagrams of §I.A for each of them.

I.C.8. EXAMPLE. Let $f(x) := x^p - 1 \in \mathbb{Q}[x]$. Of course, we have $f(x) = (x - 1)\Phi_p(x)$, with $\Phi_p(x) = \sum_{j=0}^{p-1} x^j$ irreducible. Consider the field $L = \mathbb{Q}[y]/(\Phi_p(y))$. If we write ζ for the image of y under the quotient map $K[y] \twoheadrightarrow L$, then $\zeta, \zeta^2, \ldots, \zeta^{p-1}$ are all roots of Φ_p, and distinct in L.[10] So in $L[x]$, we have $f(x) = \prod_{j=0}^{p-1}(x - \zeta^j)$, and $L = K(\zeta)$ is the splitting field, of degree $p - 1$ over K.

Of course, L embeds in $\mathbb{C}$ as $\mathbb{Q}(\zeta_p)$, by sending $\zeta \mapsto \zeta_p$ (or more generally, to ζ_p^k, for any $k \in \{1, \ldots, p-1\}$). While it's easier to construct the splitting field inside $\mathbb{C}$, the more abstract approach allows us to embed it more easily into in other extensions of $\mathbb{Q}$.

[10]To see that each ζ^k, $k \in \mathbb{Z}_p^*$, is a root, use $\zeta^p = 1$ to work mod p in exponents; and note that in $\Phi_p(\zeta^k) = 1 + \sum_{j=1}^{p-1} \zeta^{jk}$, the exponents run over all elements of $\mathbb{Z}_p^*$ since multiplication by k is invertible there. That these roots are all distinct is just the fact that they are represented by different polynomials mod $(\Phi_p(x))$.

I.C.9. EXAMPLE. Put $f(x) := x^p - 2 \in \mathbb{Q}[x]$. This is irreducible by Eisenstein and Gauss, and is the minimal polynomial of $2^{\frac{1}{p}} \in \mathbb{R}$ over $\mathbb{Q}$; so we have $[\mathbb{Q}(2^{\frac{1}{p}}){:}\mathbb{Q}] = p$.

But the splitting field is bigger than $\mathbb{Q}(2^{\frac{1}{p}})$. Given $\alpha \in \mathbb{C}$ any root of f, we have $(\alpha/2^{\frac{1}{p}})^p = \alpha^p/2 = 1$; hence $\alpha = 2^{\frac{1}{p}}\zeta_p^j$ for some $j \in \{0, 1, \ldots, p-1\}$, and this gives the list of roots of f in $\mathbb{C}$. Conclude that f splits over $L := \mathbb{Q}(2^{\frac{1}{p}}, \zeta_p)$.

Since L contains the fields $\mathbb{Q}(\zeta_p)$ and $\mathbb{Q}(2^{\frac{1}{p}})$, of respective degrees $p-1$ and p over $\mathbb{Q}$, by I.A.9 $d = [L{:}\mathbb{Q}]$ is divisible by both these degrees hence (as they are coprime) by $p(p-1)$. So $d \geq p(p-1)$. On the other hand, the minimal polynomial $\tilde{f}$ of $2^{\frac{1}{p}}$ over $\mathbb{Q}(\zeta_p)$ must divide f, and so

$$[L{:}\mathbb{Q}(\zeta_p)] = [\mathbb{Q}(\zeta_p)(2^{\frac{1}{p}}){:}\mathbb{Q}(\zeta_p)] = \deg(\tilde{f}) \leq \deg(f) = p$$

whence by the Tower Law

$$d = [L{:}\mathbb{Q}] = [L{:}\mathbb{Q}(\zeta_p)][\mathbb{Q}(\zeta_p){:}\mathbb{Q}] \leq p(p-1).$$

This shows that in fact $[L{:}\mathbb{Q}] = p(p-1)$.

I.C.10. EXAMPLE. Take $f(x) := (x^2-5)(x^2-7) \in \mathbb{Q}[x]$. We first consider the intermediate extension $L_0 := \mathbb{Q}[y]/(y^2-5)$ (writing $\sqrt{5}$ for the image of y).

I claim that $x^2 - 7$ is irreducible over L_0. Otherwise, we would have

$$7 = (a + b\sqrt{5})^2 = (a^2 + 5b^2) + 2ab\sqrt{5}$$

for some $a, b \in \mathbb{Q}$, which gives[11] $ab = 0$ hence $a^2 = 7$ or $5b^2 = 7$, which is impossible.

So the splitting field $L := L_0[z]/(z^2-7)$ has degree 2 over L_0, and degree 4 over $\mathbb{Q}$.

I.C.11. EXAMPLE. Let's compare the splitting fields for $f(x) := x^6 - 1$ and $g(x) := x^6 + 1$ over $\mathbb{Q}$.

[11] Why? Think in vector space terms: $1, \sqrt{5}$ is a basis of L_0 over $\mathbb{Q}$.

Of course, f is reducible, and factors as $(x-1)(x+1)(x^2+x+1)(x^2-x+1)$. If we write $L := \mathbb{Q}[y]/(y^2+y+1)$ (with $\omega \in L$ the image of y), then $\omega^2+\omega+1=0 \implies (-\omega)^2-(-\omega)+1=0$. So L is the splitting field (and identifies with $\mathbb{Q}(\zeta_3) \subset \mathbb{C}$).

Working in $\mathbb{C}$, g has roots $\mathbf{i}$, $\mathbf{i}\zeta_3$, $\mathbf{i}\zeta_3^2$, $-\mathbf{i}$, $-\mathbf{i}\zeta_3$, and $-\mathbf{i}\zeta_3^2$. Since $\mathbb{Q}(\zeta_3) \neq \mathbb{Q}(\mathbf{i})$, the splitting field M is a (proper) quadratic extension of L, of degree 4 over $\mathbb{Q}$.

Finally, here are a couple more examples over finite fields.

I.C.12. EXAMPLE. Let L be a splitting field for the irreducible polynomial $f(x) := x^3-x+1 \in \mathbb{Z}_3[x]$, with $\alpha \in L$ a root. One checks that $\alpha+1$ and $\alpha-1$ are also roots. Hence $L = \mathbb{Z}_3(\alpha)$ and $[L{:}\mathbb{Z}_3]=3$.

I.C.13. EXAMPLE. What if we take $f(x) := x^3+x+1 \in \mathbb{Z}_2[x]$? I claim that, as in I.C.12, the degree-3 extension $L := \mathbb{Z}_2[y]/(f(y))$ is already a splitting field. Writing α for the image of y, over L we have

$$f(x) = (x-\alpha)(x^2+ax+b) = x^3+(a-\alpha)x^2+(b-a\alpha)x-b\alpha$$

hence $b = -\frac{1}{\alpha} = 1+\alpha^2$ and $a=\alpha$. It follows that

$$(\alpha^2)^2+a(\alpha^2)+b = \alpha(\alpha^3)+\alpha^3+\alpha^2+1 = \alpha(\alpha+1)+\alpha+1+\alpha^2+1 = 0,$$

so that α^2 is also a root of f, proving the claim.

Embeddings of simple extensions.

I.C.14. PROPOSITION. *Given a simple algebraic extension $K(\alpha)/K$, with $m_\alpha \in K[x]$ the minimal polynomial of α over K; and an embedding $\imath\colon K \hookrightarrow L$, with an element $\beta \in L$. Write $\underline{\imath}\colon K[x] \hookrightarrow L[x]$ for the resulting homomorphism.*[12] *Then the following are equivalent:*

(i) *β is a root of $\underline{\imath}(m_\alpha) \in L[x]$; and*
(ii) *there exists $\jmath\colon K(\alpha) \hookrightarrow L$ with $\jmath(\alpha)=\beta$ and $\jmath|_K = \imath$.*

Moreover, in this case $\jmath$ is unique.

[12]As you have seen, we usually just write $\imath$ for this, but we need the notational distinction here to make the proof intelligible.

PROOF. First we get uniqueness out of the way: suppose $\jmath$ and $\jmath'$ are two such "extensions of $\imath$", and consider

$$K \subseteq \mathbb{F} := \{\gamma \in K(\alpha) \mid \jmath(\gamma) = \jmath'(\gamma)\} \subseteq K(\alpha).$$

Clearly $\alpha \in \mathbb{F}$ since $\jmath(\alpha) = \beta = \jmath'(\alpha)$, and so $\mathbb{F} = K(\alpha)$. Turning to the equivalence:

<u>(ii) $\implies$ (i)</u>: $\underline{\imath}(m_\alpha)(\beta) = \underline{\jmath}(m_\alpha)(\jmath(\alpha)) = \jmath(m_\alpha(\alpha)) = \jmath(0) = 0.$

<u>(i) $\implies$ (ii)</u>: Write m_β for the minimal polynomial of β over $K' := \imath(K)$. Since $\imath\colon K \to K'$ is an isomorphism, $\underline{\imath}(m_\alpha) \in K'[x]$ is irreducible; and so by (i) we have $\underline{\imath}(m_\alpha) = m_\beta$. Now consider the diagram

$$\text{(I.C.15)} \qquad \begin{tikzcd} K \arrow[r, hook] & K[x] \arrow[r, two heads, "\nu"] \arrow[d, "\underline{\imath}"', "\cong"] \arrow[rr, bend left, "\mathrm{ev}_\alpha"] & K[x]/(m_\alpha) \arrow[r, "\overline{\mathrm{ev}}_\alpha", "\cong"'] \arrow[d, dashed, "\tilde{\imath}"', "\cong"] & K(\alpha) \arrow[d, dashed, "\jmath"', "\cong"] & \\ & K'[x] \arrow[r, two heads, "\nu'"] \arrow[rr, bend right, "\mathrm{ev}_\beta"'] & K'[x]/(m_\beta) \arrow[r, "\overline{\mathrm{ev}}_\beta", "\cong"'] & K'(\beta) \arrow[r, hook] & L. \end{tikzcd}$$

Omitting the dotted arrows for the moment, note that the long composition from K to L is just $\imath$. Since $\ker(\nu' \circ \underline{\imath}) = \underline{\imath}^{-1}(\ker(\nu')) = \underline{\imath}^{-1}((m_\beta)) = (m_\alpha)$, the Fundamental Theorem gives $\tilde{\imath}$ as shown (so that the diagram commutes). We then just define $\jmath := \overline{\mathrm{ev}}_\beta \circ \tilde{\imath} \circ \overline{\mathrm{ev}}_\alpha^{-1}$; obviously this sends $k \mapsto \imath(k)$, and it sends $\alpha \mapsto \beta$ because $\tilde{\imath}$ sends $\bar{x} \mapsto \bar{x}$. $\square$

I.C.16. COROLLARY. (a) *Let $K(\alpha)/K$ be algebraic, and $\imath\colon K \hookrightarrow L$ an embedding, such that $\imath(m_\alpha)$ has r distinct roots in L. Then there are exactly r distinct embeddings $\jmath\colon K(\alpha) \hookrightarrow L$ with $\jmath|_K = \imath$.*

(b) *Let $K(\alpha)/K$ and $K'(\alpha')/K'$ be algebraic, with $\imath\colon K \xrightarrow{\cong} K'$. Then $m_{\alpha'} = \imath(m_\alpha) \iff \exists\, \jmath\colon K(\alpha) \xrightarrow{\cong} K'(\alpha')$ with $\jmath(\alpha) = \alpha'$ and $\jmath|_K = \imath$ (in which case $\jmath$ is unique).*

PROOF. Both follow directly from I.C.14. (For (b), take $L := K'(\alpha')$ and $\beta := \alpha$.) $\square$

I.C.17. EXAMPLES. (A) Let $K = \mathbb{Q}$, $K(\theta) = \mathbb{Q}[x]/(x^3 - 3x - 1)$, and $L = \mathbb{R}$. Recall from I.A.2 that 3 embeddings $\varphi_i \colon \mathbb{Q}(\theta) \hookrightarrow \mathbb{R}$ were obtained by sending $\theta \mapsto \theta_i$, with $\{\theta_i\}$ the three roots of $x^3 - 3x - 1$ in $\mathbb{R}$. By I.C.16(a), these are *all* of the real embeddings; composing them with the inclusion $\mathbb{R} \hookrightarrow \mathbb{C}$ gives the only embeddings of $\mathbb{Q}(\theta)$ in $\mathbb{C}$ (why?).

(B) If we change the polynomial to $x^3 - 2$ (cf. I.A.3), then there is only one root in $\mathbb{R}$, but two more in $\mathbb{C}$. In this case, by the Corollary there is exactly one embedding $\mathbb{Q}(\theta) \hookrightarrow \mathbb{R}$, but two additional (conjugate) embeddings $\mathbb{Q}(\theta) \hookrightarrow \mathbb{C}$.

(C) What about, say, $K = \mathbb{Z}_p(y)$ and $K(\alpha) := \mathbb{Z}_p(y)[x]/(x^p - y)$? As we will see below, $x^p - y$ is irreducible in $\mathbb{Z}_p(y)[x]$. Moreover, if β is a root in some extension $(\mathbb{Z}_p(y) \overset{\imath}{\hookrightarrow})\, L$, then $\beta^p = y$ and $(x - \beta)^p = x^p - \beta^p = x^p - y$, making β is the *only* root in L. (The "freshman's dream" is obviously crucial here.) So there is *only one embedding* $K(\alpha) \hookrightarrow L$ extending $\imath$.

Uniqueness and automorphisms of splitting fields. First, we prove a general result which appears to have nothing to do with either of these.

I.C.18. THEOREM. *Given $f \in K[x]$ of degree n, with splitting field extension L/K of degree $d := [L{:}K]$. Let $\imath \colon K \hookrightarrow L'$ be an embedding. Then there exists $\jmath \colon L \hookrightarrow L'$ extending[13] $\imath$ if and only if $\imath(f)$ splits over L'. In this case, the number of possible choices for $\jmath$ is $\leq d$, with equality if $\imath(f)$ has n* distinct *roots in L'.*

PROOF. We may assume f monic, with $f(x) = \prod_{i=1}^n (x - \alpha_i)$ in $L[x]$. If $\jmath$ exists, then $\imath(f) = \jmath(f) = \prod_{i=1}^n (x - \jmath(\alpha_i))$ splits over L'.

For the converse direction and the count of possible $\jmath$'s, we induce on d. We need to show that if f splits over L', we can embed its splitting field into L' in $\leq d$ different ways, extending $\imath$. (The case $d = 1$ means that $L = K$, so the extension is the trivial one and there is one way to do it.)

[13]That is, $\jmath|_K = \imath$.

So assume $d > 1$. We may then assume $\alpha_1 \notin K$; let m_{α_1} be its minimal polynomial over K, and write $f = m_{\alpha_1} g$. In $L[x]$, for some ordering of the roots, we have $m_{\alpha_1}(x) = \prod_{i=1}^{r}(x - \alpha_i)$. By assumption, $\imath(m_{\alpha_1})\imath(g) = \imath(f)$ splits over L', so that (in $L'[x]$) $\imath(m_{\alpha_1})(x) = \prod_{i=1}^{r}(x - \beta_i)$ and $\imath(f)(x) = \prod_{i=1}^{n}(x - \beta_i)$ for some $\beta_i \in L'$. Notice that $K(\alpha_1)/K$ is simple, and $\{\beta_1, \ldots, \beta_r\}$ are roots of $\imath(m_{\alpha_1})$ in L', so that I.C.14 gives for each $i \in \{1, \ldots, r\}$ a unique $\imath_1 \colon K(\alpha_1) \hookrightarrow L'$ (with $\imath_1|_K = \imath$) sending $\alpha_1 \mapsto \beta_i$. The number of possible choices here is the number of *distinct* β_i with $i \in \{1, \ldots, r\}$.

Setting $K_1 := K(\alpha_1)$ and $f_1 := g \in K_1[x]$, and choosing an $\imath_1 \colon K_1 \hookrightarrow L'$, we note that f_1 splits over L', and L/K_1 is a splitting field extension for f_1, of degree $d_1 := [L{:}K(\alpha_1)] = \frac{[L:K]}{[K(\alpha_1):K]} = \frac{d}{r} < d$. By the inductive hypothesis, there exists a $\jmath \colon L \hookrightarrow L'$ extending $\imath_1$ hence $\imath$. The number of possible choices is $\leq d_1$, with equality iff the $\beta_{r+1}, \ldots, \beta_n$ are distinct.

Conclude that if $\beta_1, \ldots, \beta_n$ are distinct, then there are r choices of $\imath_1$, and for each of those, $\frac{d}{r}$ choices of $\jmath$ extending it, for a total of d choices overall. Clearly in general this is the upper bound. $\square$

I.C.19. COROLLARY. *Given $f \in K[x]$, an isomorphism $\imath \colon K \xrightarrow{\cong} K'$, and L/K resp. L'/K' splitting field extensions for f resp. $\imath(f)$, there exists a $\jmath \colon L \xrightarrow{\cong} L'$ extending $\imath$ (with the same number of choices as in I.C.18).*

PROOF. Applying I.C.18 to $\imath \colon K \xrightarrow{\cong} K' \hookrightarrow L'$ yields $\jmath \colon L \hookrightarrow L'$ extending $\imath$. We need to show that $\jmath$ is onto. Assume f monic.

We have $f(x) = \lambda \prod_{i=1}^{n}(x - \alpha_i)$ in $L[x]$, hence $\imath(f) = \imath(\lambda) \prod_{i=1}^{n}(x - \jmath(\alpha_i))$ in $L'[x]$. Since L' is a splitting field for $\imath(f)$, we have $L' = K'(\jmath(\alpha_1), \ldots, \jmath(\alpha_n)) \subset \jmath(L)$. So $\jmath$ is indeed surjective. $\square$

I.C.20. REMARK. In spite of the non-uniqueness of $\jmath$ in the last Theorem and Corollary, the latter provides an affirmative answer to our uniqueness question (3) from the beginning of the section. If we take $K' = K$ and $\imath = \mathrm{id}_K$ in I.C.19, it says that any two splitting field extensions are isomorphic *over* K (that is, the isomorphism even restricts to the identity on K).

I.C.21. COROLLARY. *Let $f \in K[x]$ be irreducible, L/K a splitting field extension for f.*

(i) *Given $\alpha, \beta \in L$ two roots of f, there exists an*[14] *automorphism $\sigma \colon L \xrightarrow{\cong} L$ with $\sigma(\alpha) = \beta$ and $\sigma|_K = \mathrm{id}_K$.*

(ii) *There are at most $[L{:}K]$ automorphisms of L over K; and there are exactly this number if f has $\deg(f)$ distinct roots.*

PROOF. For (ii), just apply I.C.19 with $K' = K$, $\imath = \mathrm{id}_K$ and $L' = L$.

To see (i), apply I.C.16(b) to produce $\tau \colon K(\alpha) \xrightarrow{\cong} K(\beta)$ (with $\tau|_K = \mathrm{id}_K$) sending $\alpha \mapsto \beta$. But then $L/K(\alpha)$ and $L/K(\beta)$ are splitting field extensions for f, to which we apply I.C.19 (with $\imath = \tau$) to get the result. □

[14]Not necessarily unique, unless $L = K(\alpha)$.