I.F. Separable, normal, and Galois extensions

At the heart of Galois theory is a correspondence between intermediate fields in an extension and subgroups of its automorphism group. This takes its nicest form for Galois extensions, where the automorphism group has order equal to the degree of the extension. This setting is obtained by imposing on our extensions the separability and normality conditions, alluded to in §I.D, which we now explain in detail.

Separable extensions.

With the understanding (from §I.E) that inseparable polynomials only occur over non-perfect fields \( K \), we now make the

**I.F.1. Definition.** (i) Let \( L/K \) be an extension, and \( \alpha \in L \). We say \( \alpha \) is separable over \( K \) if \( \alpha \) is algebraic over \( K \) and its minimal polynomial \( m_\alpha \) over \( K \) is separable.

(ii) An extension \( L/K \) is separable if it is algebraic and each \( \alpha \in L \) is separable over \( K \).

**I.F.2. Proposition.** Intermediate extensions in separable extensions are separable.

**Proof.** Let \( L/K \) be separable, and \( M \) be a subfield of \( L \) containing \( K \). Obviously \( M/K \) is separable; the issue is \( L/M \).

Take \( \alpha \in L \), and let \( m_\alpha \) and \( p_\alpha \) denote its minimal polynomials over \( K \) resp. \( M \). Then \( p_\alpha \mid m_\alpha \) in \( M[x] \). Let \( N/M \) be a splitting field extension for \( m_\alpha \). Since \( m_\alpha \) is separable over \( K \), and \( N \) contains a splitting field for \( m_\alpha \) over \( K \), we have \( m_\alpha(x) = \prod_i (x - \alpha_i) \) in \( N[x] \), with \( \alpha_i \in N \) distinct. Hence \( p_\alpha(x) = \prod_{\ell} (x - \alpha_{i_{\ell}}) \) in \( N[x] \), with \( \alpha_{i_{\ell}} \in N \) distinct. Conclude that \( p_\alpha \) is separable. \( \square \)

**I.F.3. Theorem.** Let \( M/K \) be an extension of degree \( d := [M:K] \), and fix an embedding \( j : K \hookrightarrow L \). Write \( r \) for the number of embeddings \( M \hookrightarrow L \) extending \( j \). Then \( r \leq d \), with equality \( \iff \) \( M/K \) is separable and \( j(m_\alpha) \) splits over \( L \) for every \( \alpha \in M \).
For the proof, it is helpful to isolate a special case:

I.F.4. LEMMA. Let $K(\alpha)/K$ be a simple extension of degree $d$, with $L$ and $r$ as in the Theorem. Then $r \leq d$, with equality $\iff \alpha$ is separable over $K$ and $j(m_\alpha)$ splits over $L$.

PROOF. By I.C.14, we get exactly one embedding of $K(\alpha)$ into $L$ extending $j$ for each of the (say) $r$ distinct roots of $j(m_\alpha)$ in $L$. Clearly $r \leq \deg(j(m_\alpha)) = d$, with equality $\iff j(m_\alpha)$ splits into distinct linear factors $\iff j(m_\alpha)$ is separable over $K$ and $j(m_\alpha)$ splits over $L$. □

PROOF OF I.F.3. We proceed by induction on $d$:

($\implies$): Let $\alpha \in M \setminus K$, and note that $M/K(\alpha)$ is separable (of degree $< d$) by I.F.2. To each of the $[K(\alpha):K]$ distinct embeddings $\sigma: K(\alpha) \to L$ produced by the Lemma, we may apply the inductive hypothesis to extend $\sigma$ in $[M:K(\alpha)]$ distinct ways to $M \to L$, and conclude by the Tower Law provided $\sigma(\mu_\beta)$ splits over $L$ for every $\beta$ in $M$ (with $\mu_\beta$ its minimal polynomial over $K(\alpha)$). But this is routine: in $K(\alpha)[x]$, $\mu_\beta$ divides the minimal polynomial $m_\beta$ over $K$; and $\sigma(m_\beta)$ (hence $\sigma(\mu_\beta)$) splits over $L$ by hypothesis.

($\impliedby$): If for some $\alpha \in M$, $j(m_\alpha)$ doesn’t split or $\alpha$ is inseparable over $K$, then by the Lemma there are fewer than $[K(\alpha):K]$ ways to extend $j$ to $K(\alpha)$. Applying induction to $M/K(\alpha)$ and the Tower Law, there are thus fewer than $d$ ways to extend $j$ to $M$. □

Normal extensions.

I.F.5. DEFINITION. A field extension $L/K$ is called normal if it is algebraic and each irreducible $f \in K[x]$ either splits over $L$ or has no roots in $L$. Equivalently, $L/K$ is algebraic and, for each $\alpha \in L$, the minimal polynomial $m_\alpha \in K[x]$ splits over $L$.

In particular, $K(\alpha)/K$ is normal if and only if $\alpha$ is algebraic over $K$ and $m_\alpha$ splits over $K(\alpha)$. Already one sees that this doesn’t hold for $K = \mathbb{Q}$ and $\alpha = 2^{1/3}$. Unlike separability, normality will routinely fail\footnote{Remember that “splits” always means “into linear factors”.}.
in characteristic zero. Fortunately, as we shall see, there is a “fix” of sorts: if an algebraic extension $L/K$ is non-normal, there will always be a larger extension containing it which is normal.

I.F.6. Definition. $L/K$ is a \textbf{splitting field extension} for a (possibly infinite) subset $S \subset K[x]$ if:

(i) every $f \in S$ splits over $L$; and

(ii) any proper subfield of $L$ fails to split some $f \in S$.

I.F.7. Proposition. $L/K$ is normal $\iff$ $L$ is a splitting field extension for some $S \subset K[x]$.

Proof. ($\Longrightarrow$): Set $S_L := \{m_\alpha \mid \alpha \in L\} \subset K[x]$. Then each $f \in S_L$ splits over $L$; and any proper subfield of $L$ omits some $\alpha \in L$ hence doesn’t split its $m_\alpha$.

($\Longleftarrow$): Set $R_S := \{a \in L \mid f(a) = 0 \text{ for some } f \in S\}$. Then $L = K(R_S)$ by I.F.6(ii), hence is algebraic/$K$ by I.A.21. It remains, given $\beta \in L$, to show that $m_\beta \in K[x]$ splits/$L$. More precisely, we have $\beta \in K(\alpha_1, \ldots, \alpha_n)$ for some $\alpha_i \in R_S$ (with $f_i(\alpha_i) = 0$ for some $f_i \in S$); and writing $g := f_1 \cdots f_n$ and $R_g := \{a \in L \mid g(a) = 0\} \subset L$, we note that $\beta \in K(R_g)$. It will suffice to show that $m_\beta$ splits/$K(R_g)$.

So let $M$ be a splitting field extension for $m_\beta$ over $K(R_g)$, and $\gamma \in M$ a root of $m_\beta$. Since the latter is also the minimal polynomial over $K$ for $\gamma$, by I.C.16(b) we get $\tau$ in

\[
\begin{array}{ccc}
K & \xrightarrow{\text{SFE for } g} & K(R_g) \\
\downarrow \cong & & \downarrow \cong \\
K(\gamma) & \xleftarrow{\tau(g)=g} & K(R_g, \gamma).
\end{array}
\]

hence (from I.C.19) $\sigma$. So $[K(R_g):K(\beta)] = [K(R_g, \gamma):K(\gamma)] \implies$

\[
[K(R_g):K] = [K(R_g):K(\beta)][K(\beta):K] = [K(R_g, \gamma):K(\gamma)][K(\gamma):K] = [K(R_g, \gamma):K]
\]
\[ K(R_g) = K(R_g, \gamma) \implies \gamma \in K(R_g), \]
i.e. \( m_\beta \) splits over \( K(R_g) \) (hence \( L \)). \( \square \)

**I.F.8. Corollary.** Assume \([L:K] < \infty\). Then \( L/K \) is normal \( \iff \) 
\( L \) is a splitting field for some \( g \in K[x] \).

**Proof.** (\( \implies \)): We may write \( L = K(a_1, \ldots, a_d) \) (as a vector space). Since \( L \) is normal, and each \( m_{a_i} \) has a root (namely, \( a_i \)) in \( L \), each \( m_{a_i} \) must split over \( L \). Moreover, \( g := \prod_i m_{a_i} \) splits over no proper subfield of \( L \), since that would not contain all the \( a_i \) so would not contain all the roots of \( g \).

(\( \Leftarrow \)): Immediate from I.F.7. \( \square \)

**I.F.9. Remark.** More explicitly, if \( L/K \) is finite, then for some \( a_1, \ldots, a_k \in L \) we may write \( L = K(a_1, \ldots, a_k) \); and (by the same argument as in I.F.8) \( L/K \) is normal if and only if it is a splitting field extension for \( g := \prod_i m_{a_i} \).

**I.F.10. Example.** As previously mentioned, \( \mathbb{Q}(\sqrt[3]{2})/\mathbb{Q} \) is not normal: \( m_{\sqrt[3]{2}}(x) = x^3 - 2 \in \mathbb{Q}[x] \) factors into the irreducible factors \( x - \sqrt[3]{2} \) and \( x^2 + \sqrt[3]{2}x + (\sqrt[3]{2})^2 \) in \( \mathbb{Q}(\sqrt[3]{2})[x] \), so does not split there. How do I know that the quadratic factor is irreducible (and can I see this by pure thought)? Well, by the argument in the proof of I.F.7, you see that any two splitting field extensions have the same degree. We know that \( L := \mathbb{Q}(\sqrt[3]{2}, \zeta_3) \) is a splitting field for \( m_{\sqrt[3]{2}} \) over \( \mathbb{Q} \), since it is what you get by adjoining the complex roots; and by the Tower Law, \( 3 = [\mathbb{Q}(\sqrt[3]{2});\mathbb{Q}] \) and \( 2 = [\mathbb{Q}(\zeta_3);\mathbb{Q}] \) both divide \( [L:\mathbb{Q}] \), which is therefore 6.

**I.F.11. Example.** The cyclotomic extension\(^{19} \) \( \mathbb{Q}(\zeta_m)/\mathbb{Q} \) is normal for any \( m \). The other roots of the minimal polynomial \( m_{\zeta_m} \) are powers of \( \zeta_m \), since \( \zeta_m \mid x^m - 1 \) (and all roots of \( x^m - 1 \) are powers of \( \zeta_m \)). Clearly, these roots also generate the extension.

\(^{19}\)As usual, \( \zeta_m = e^{2\pi i/m} \) denotes a primitive root of 1 in \( \mathbb{C} \).
While we have seen that intermediate fields in a normal extension \(L/K\) need not be normal over \(K\), one can take a different perspective:

I.F.12. **Corollary.** Given \(L/K\) normal, \(M \subset L\) a subfield containing \(K\), \(L/M\) is normal.

**Proof.** By I.F.7 there exists \(S \subset K[x]\) such that \(L/K\) is a SFE for \(S\). But then, if we consider \(S\) as a subset of \(M[x]\), \(L/M\) is evidently a SFE for \(S\). Applying I.F.7 again, we get that \(L/M\) is normal. \(\square\)

We are now ready to consider the relationship between normality and automorphisms, which both suggests the reason for the terminology and provides the first real taste of Galois theory. Write

\[
\text{(I.F.13)} \quad \text{Aut}(L/K) := \{\sigma \in \text{Aut}(L) | \sigma|_K = \text{id}_K\}.
\]

I.F.14. **Theorem.** Let \(L/K\) be finite and normal, and \(M \subset L\) a subfield containing \(K\). Then the following are equivalent:

(i) \(M/K\) is normal;

(ii) \(\sigma \in \text{Aut}(L/K) \implies \sigma(M) \subseteq M\); and

(iii) \(\sigma \in \text{Aut}(L/K) \implies \sigma(M) = M\).

**Proof.** (i) \(\implies\) (ii): Given \(\alpha \in M\), let \(m_\alpha \in K[x]\) be the minimal polynomial, and \(R_{m_\alpha} \subset L\) its roots. If \(M/K\) is normal, we have \(R_{m_\alpha} \subset M\); and \(m_\alpha(\sigma(\alpha)) = \sigma(m_\alpha(\alpha)) = 0 \implies \sigma(\alpha) \in R_{m_\alpha} \subset M\). So \(\sigma(M) \subset M\).

(ii) \(\implies\) (iii): This works because \(L/K\) is finite and \(\sigma\) is injective, since then \(\sigma(M) \subseteq M \implies [M:K] \geq [\sigma(M):K] = [M:K]\) forces \(\sigma(M) = M\). (Think \(K\)-vector spaces.)

(iii) \(\implies\) (i): Given \(\alpha \in M\), we must show that \(m_\alpha \in K[x]\) splits over \(M\), or equivalently that its roots \(R_{m_\alpha} \subset L\) lie in \(M\). Let \(\beta \in R_{m_\alpha}\).

By I.F.8, \(L\) is a splitting field for some \(g \in K[x]\) — over \(K\), hence also over \(K(\alpha)\) and \(K(\beta)\). Moreover, I.C.16(b) gives an isomorphism \(j: K(\alpha) \to K(\beta)\) over \(K\) sending \(\alpha \mapsto \beta\). Since \(j(g) = g\), by I.C.19
there is a $\sigma \in \text{Aut}(L)$ extending $f$ hence fixing $K$; and by assumption of (iii), we have $\sigma(M) = M$. So we have $\beta = f(\alpha) = \sigma(\alpha) \in M$. □

Normal closures.

I.F.15. DEFINITION. A normal closure $L^c$ for an algebraic extension $L/K$ is an extension $L^c/L$ such that

(i) $L^c/K$ is normal; and

(ii) $L^c \supset M \supset L$ and $M/K$ normal $\implies M = L^c$.

I.F.16. COROLLARY. If $L/K$ is finite, then it has a finite normal closure ($\implies L^c/K$ finite).

PROOF. As in the proof of I.F.8, write $L = K\langle a_1, \ldots, a_d \rangle$, $g = \prod m_{a_i}$, and consider $F/L$ a SPE for $g$. Then $F/K$ is a SFE for $g$, hence normal. Moreover, if $F \supset M \supset L$ with $M/K$ normal, then $g$ splits over $M$, hence $M = F$. □

I.F.17. EXAMPLE. $\mathbb{Q}(\sqrt[3]{2}, \zeta_3)$ is a normal closure for $\mathbb{Q}(\sqrt[3]{2})$.

I.F.18. PROPOSITION. Suppose $L = K(\alpha_1, \ldots, \alpha_r)/K$ is finite, with $\alpha_i$ separable over $K_{i-1} := K(\alpha_1, \ldots, \alpha_{i-1})$ for each $i$. Then $L/K$ is separable.

PROOF. Let $L^c/L$ be a normal closure.

At each stage, by I.F.4 there exist $[K_i:K_{i-1}]$ embeddings $K_i \hookrightarrow L^c$ extending a given embedding $K_{i-1} \hookrightarrow L^c$. (Note that the minimal polynomial of $\alpha_i$ over $K_{i-1}$ divides its minimal polynomial over $K$, hence splits over $L^c$ because the latter does. So I.F.4 does indeed apply.) By the Tower Law, this amounts to $[L:K]$ distinct embeddings of $L$ into $L^c$. Applying I.F.3 (with $M, L$ there replaced by $L, L^c$ here), we find that $L/K$ is separable. □

I.F.19. COROLLARY. A finite extension $L/K$ is separable in any of the following cases:

(a) $L = K(\alpha_1, \ldots, \alpha_r)$ and each $\alpha_i$ is separable over $K$.
(b) $f \in K[x]$ is separable over $K$ and $L/K$ is a SFE for $f$.
(c) $L \supset M \supset K$ with $L/M$ and $M/K$ separable.
PROOF. For (a), note that (with notation from I.F.18) each \( \alpha_i \) being separable over \( K \) makes it also separable over \( K_{i-1} \) (by the proof of I.F.2); now apply I.F.18. For (b), apply (a) to roots of \( f \) in \( L \). For (c), write \( L = M(\{\beta_j\}) \) and \( M = K(\{\alpha_i\}) \); apply I.F.2 to split \( L/M \) and \( M/K \) into successive simple separable extensions; then apply I.F.18 to the whole tower. \( \Box \)

**Galois extensions.**

I.F.20. **Definition.** A **Galois extension** is a finite, normal, separable extension.

I.F.21. **Theorem.** Let \( L/K \) be finite. Then \( |\text{Aut}(L/K)| \leq [L:K] \), with equality \( \iff \) \( L/K \) is Galois.

PROOF. Apply I.F.3 with “\( M, L \)” both \( L \). The “embeddings extending \( \jmath \)” become (by I.A.23) automorphisms fixing \( K \), and I.F.3 says precisely that there are \([L:K] \) of these iff \( L/K \) is separable and normal. \( \Box \)

I.F.22. **Corollary.** An extension \( L/K \) is Galois if and only if it is a splitting field extension for a separable polynomial \( f \in K[x] \).

PROOF. If \( L/K \) is Galois, then it is the SFE for some \( f \in K[x] \) by I.F.8; since this \( f \) is a product of minimal polynomials of its roots, it is separable by I.F.1.

For the other direction, given \( f \in K[x] \), the SFE is finite and normal (cf. I.F.8), and separable if \( f \) is (cf. I.F.19(b)). \( \Box \)

I.F.23. **Definition.** If \( L/K \) is Galois, \( \text{Aut}(L/K) \) is called the **Galois group**\(^{20} \); it is standard to write \( \text{Gal}(L/K) \) for \( \text{Aut}(L/K) \) in this case.

\(^{20}\) Note that [Jacobson] actually calls \( \text{Aut}(L/K) \) the “Galois group” (and writes \( \text{Gal}(L/K) \)) unconditionally. One should be a bit wary here, as some authors (at least, for \( L/K \) separable) define the Galois group of \( L/K \) to be \( \text{Aut}(L^c/K) \). I am happier to drop the finiteness condition on \( L/K \) in favor of algebraicity, so that we can speak of (for example) \( \text{Gal}(\bar{Q}/Q) \), which is very much standard usage. But definitions are definitions and we shall stick with ours.