I.I. Simple extensions

In §I.H we showed that any extension L/K of finite fields is simple; that is, there exists $\alpha \in L$ for which $L = K(\alpha)$. (Recall from I.A.12 that α is then called a *primitive element* for the extension.) More generally, we should wonder for which extensions just one generator α will do. For one thing, automorphisms would then be determined by where α goes.

I.I.1. LEMMA. *Let L/K be an algebraic extension. Then L/K is simple $\iff$ L/K contains only finitely many intermediate fields.*

PROOF. $\underline{(\implies)}$: Assume $K(\alpha) = L$; algebraicity of α yields $m_\alpha \in K[x]$, which we factor into irreducibles $(m_\alpha =)\, g_1 \cdots g_k$ in $L[x]$. Given an intermediate field M, we can consider the minimal polynomial $\mu_\alpha \in M[x]$. Since this divides m_α, we have $\mu_\alpha = g_{i_1} \cdots g_{i_\ell} = a_r + \cdots + a_1 x^{r-1} + x^r$. Since μ_α is also the minimal polynomial over $M_0 := K(a_1, \ldots, a_r)$, we have $M_0(\alpha) = L = M(\alpha) \implies [L{:}M_0] = \deg(\mu_\alpha) = [L{:}M] \implies M = M_0$. So M is determined by the subset $\{i_1, \ldots, i_\ell\} \subset \{1, \ldots, k\}$ and there are only finitely many choices.

$\underline{(\impliedby)}$: Clearly L is finitely generated over K (otherwise, adjoining an infinite sequence of generators contradicts the hypothesis). Each generator has finite degree over K since the extension is algebraic, and so $[L{:}K] < \infty$. So we are done if $|K| < \infty$ by §I.H.

If $|K| = \infty$, suppose $r := \inf\{|\mathcal{S}| \big| K(\mathcal{S}) = L\} > 1$ and write $L = K(\alpha_1, \ldots, \alpha_r)$. As κ ranges over K, the fields $K(\alpha_1 + \kappa\alpha_2)$ cannot all be distinct (without contradicting the hypothesis), and there exist distinct $\kappa, \kappa' \in K$ for which $K(\alpha_1 + \kappa\alpha_2) = K(\alpha_1 + \kappa'\alpha_2)$. So $K(\alpha_1 + \kappa\alpha_2)$ contains $(\alpha_1 + \kappa\alpha_2) - (\alpha_1 + \kappa'\alpha_2) = (\kappa - \kappa')\alpha_2$, hence α_2, hence α_1. This means that $K(\alpha_1 + \kappa\alpha_2) = K(\alpha_1, \alpha_2)$, and we can generate L with $r - 1$ elements, contradicting minimality of r. □

I.I.2. THEOREM OF THE PRIMITIVE ELEMENT. *Any finite and separable extension is simple.*

PROOF. Since L/K is finite, it is certainly finitely generated (and algebraic), and we may write $L = K(\alpha_1, \ldots, \alpha_r)$. The polynomial

$g := \prod_i m_{\alpha_i}$ is separable since each α_i is. If N/L is a SFE for g, then so is N/K, which is thus Galois, making $K = \mathrm{Inv}(\mathrm{Aut}(N/K))$. Since $\mathrm{Aut}(N/K)$ is finite, it has finitely many subgroups, and so by FTGT N/K has finitely many intermediate fields. So the same goes for L/K. Apply the Lemma. $\square$

This leads to an improvement of I.F.22.

I.I.3. COROLLARY. *Any Galois extension is the splitting field extension for a single* ***irreducible*** *polynomial.*

PROOF. Let L/K be Galois. The Theorem yields $\alpha \in L$ such that $L = K(\alpha)$; and $m_\alpha \in K[x]$ splits over L since L/K is normal. No proper subfield contains the root α, and so L/K is a SFE for m_α. $\square$

Say L/K is Galois, and K is an infinite field. Then there is a simple explanation of the Theorem: since the intermediate fields are (proper) K-vector-subspaces of L, and there are only finitely many, their union cannot be all of L. Thus any element of L not in their union is a primitive element. So to find one, we just need to use the Galois correspondence to find all intermediate subfields.

I.I.4. EXAMPLE. For $L = \mathbb{Q}(\sqrt{2}, \sqrt{3})$, which is Galois/$\mathbb{Q}$, we have $\mathrm{Aut}(L/\mathbb{Q}) = \{1, \sigma_2, \sigma_3, \sigma_2\sigma_3\}$ (where $\sigma_j \colon \sqrt{j} \mapsto -\sqrt{j}$). Applying Inv to $\langle\sigma_2\rangle$, $\langle\sigma_3\rangle$, and $\langle\sigma_2\sigma_3\rangle$ gives $\mathbb{Q}(\sqrt{3})$, $\mathbb{Q}(\sqrt{2})$, resp. $\mathbb{Q}(\sqrt{6})$. Since $\sqrt{2} + \sqrt{3}$ is not fixed under σ_2, σ_3, or $\sigma_2\sigma_3$, it is not contained in an intermediate field of the extension. So $L = \mathbb{Q}(\sqrt{2} + \sqrt{3})$.

We should check that the hypotheses in the Theorem are really needed. Assume that L/K is algebraic, but *infinite* (like $\bar{\mathbb{Q}}/\mathbb{Q}$); then it is not even finitely generated, let alone simple.

What about the separability hypothesis?

I.I.5. EXAMPLE. Put $J = \mathbb{Z}_p(y)$, $K = J(z)$, with y, z indeterminates; and let L/K be a SFE for $(x^p - y)(x^p - z)$. Then $[L{:}K] = p^2$, and elements $\ell \in L$ take the form $\frac{P(\sqrt[p]{y}, \sqrt[p]{z})}{Q(\sqrt[p]{y}, \sqrt[p]{z})}$, where P, Q are polynomials. By the freshman's dream, ℓ^p is a ratio of polynomials in y, z, and thus belongs to K. Conclude that $[K(\ell){:}K] = p$ for any $\ell \in L \setminus K$, so that L/K is not simple.

$$\begin{tikzcd}
& & L \arrow[dl, dash, "p"'] \arrow[dr, dash, "p"] & \\
& K(\sqrt[p]{y}) \arrow[dl, dash, "\infty"'] \arrow[dr, dash, "p"] & & K(\sqrt[p]{z}) \arrow[dl, dash, "p"] \\
J(\sqrt[p]{y}) \arrow[dr, dash, "p"'] & & K \arrow[dl, dash, "\infty"] & \\
& J & &
\end{tikzcd}$$

Notice that there are infinitely many subfields $K(\ell)$, since $|K| = \infty$ and each has dimension p over K yet their *union* covers a vector space of dimension p^2. This is only possible because $\mathrm{Aut}(L/K)$ is trivial (has fixed field L) hence entirely fails to "regulate" subfields.

Given an extension L/K of degree n, the Theorem of the Primitive Element says we can always find some $\alpha \in L$ for which the powers $\{1, \alpha, \alpha^2, \ldots, \alpha^{n-1}\}$ yields a basis of L as a K-vector space. What more could we ask for?

Well, suppose L/K is Galois, with $G := \mathrm{Aut}(L/K) = \{\sigma_1, \ldots, \sigma_n\}$. For *any* $\alpha \in L$, not necessarily primitive, the minimal polynomial over K factors as $m_\alpha(x) = \prod_{i=1}^m (x - \alpha_i)$ (with $\alpha_1 = \alpha$, and distinct α_i's), and the orbit $G(\alpha)$ is exactly $\{\alpha_1, \ldots, \alpha_m\}$. (Obviously it can't be larger, since roots are sent to roots. It also can't be smaller: otherwise, the coefficients of a partial product $\prod_j (x - \alpha_{i_j})$ would be invariant under G, hence belong to K, making m_α reducible in $K[x]$.) We also have $[K(\alpha){:}K] = m$. Considering $m = n$ vs. $m < n$ yields at once the

I.I.6. PROPOSITION. *α is a primitive element $\iff$ $\sigma_1(\alpha), \ldots, \sigma_n(\alpha)$ are distinct.*

So when α is primitive, $m = n$ and we have two n-element sets, $\{1, \alpha, \alpha^2, \ldots, \alpha^{n-1}\}$ and $G(\alpha) = \{\sigma_1(\alpha), \ldots, \sigma_n(\alpha)\} = \{\alpha_1, \ldots, \alpha_n\}$. The first spans L as a K-vector space, but usually isn't G-invariant, i.e. "normal". (Can you think of an exception?) The second is G-invariant, but need not span L: consider $\alpha = \sqrt{2} + \sqrt{3}$ in $L/K = \mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q}$. What the Normal Basis Theorem says is that *we can actually choose α so that the $\sigma_i(\alpha)$ are independent over K, giving a basis for L/K.*

I.I.7. EXAMPLES. Find such an α (and thus a "normal basis") for $L/\mathbb{Q}$ in each of the following cases:
(1) $L = \mathbb{Q}(\zeta_5)$
(2) $L = \mathbb{Q}(\sqrt{2}, \sqrt{3})$

For the proof, we will make use of I.G.3 as well as the following

I.I.8. LEMMA. *Let R be an infinite subset of a commutative domain S. Then for any $f \in S[x_1, \ldots, x_n] \setminus \{0\}$, there exists $(r_1, \ldots, r_n) \in R^n$ such that $f(r_1, \ldots, r_n) \neq 0$.*

PROOF. If $n = 1$, the result is clear: f has finitely many roots in the fraction field F of S, hence in S. So induce on n: writing $f \in S[x_1][x_2, \ldots, x_n]$, the result for $n-1$ (and $S[x_1]$ replacing S) yields $r_2, \ldots, r_n \in R$ for which $f(x, r_2, \ldots, r_n) \neq 0$ in $S[x_1]$. Applying the $n = 1$ case once more to select r_1, we are done. $\square$

I.I.9. NORMAL BASIS THEOREM. *Let L/K be a Galois extension, with $n = [L{:}K]$ and $\mathrm{Aut}(L/K) =: G = \{\sigma_1, \ldots, \sigma_n\}$. Then there exists $\ell \in L$ such that $(\sigma_1(\ell), \ldots, \sigma_n(\ell))$ is a basis for L/K.*

PROOF. <u>Case I ($|K| = \infty$)</u>: Define $\sigma_i \sigma_j =: \sigma_{p(i,j)}$, and form the $n \times n$ matrix $M = [x_{p(i,j)}]$ with entries in $K[\underline{x}] = K[x_1, \ldots, x_n]$, and $f(\underline{x}) := \det(M) \in K[\underline{x}]$. This polynomial is nonzero because (for instance) x_1 occurs exactly once in each row and each column, making the coefficient of x_1^n in f either 1 or -1.

Let $(\beta_1, \ldots, \beta_n) \subset L$ be a basis for L/K. The n "orbit vectors"

$$(\sigma_1(\beta_1), \ldots, \sigma_n(\beta_1)), \ \ldots, \ (\sigma_1(\beta_n), \ldots, \sigma_n(\beta_n))$$

are independent over L in L^n by I.G.3. So the matrix $[\sigma_i(\beta_j)]$ is invertible and we let $[c_{ij}]$ denote its inverse.

Setting $g(\underline{x}) := f(\sum_j \sigma_1(\beta_j)x_j, \ldots, \sum_j \sigma_n(\beta_j)x_j)$, we observe that $f(\underline{x}) = g(\sum_j c_{1j}x_j, \ldots, \sum_j c_{nj}x_j)$, whence $g \in L[\underline{x}]$ is also nonzero. By Lemma I.I.8, there exist $k_1, \ldots, k_n \in K$ such that $g(k_1, \ldots, k_n) \neq 0$. Put $\ell := \sum_{j=1}^n k_j\beta_j$. Then

$$\begin{aligned} 0 \neq g(k_1, \ldots, k_n) &= f(\textstyle\sum_j \sigma_1(\beta_j)k_j, \ldots, \sum_j \sigma_n(\beta_j)k_j) \\ &= f(\sigma_1(\ell), \ldots, \sigma_n(\ell)) \\ &= \det([\sigma_{p(i,j)}(\ell)]) = \det([\sigma_i(\sigma_j(\ell))]) \end{aligned}$$

$\implies$ $[\sigma_i(\sigma_j(\ell))]_{i,j=1,\ldots,n}$ is invertible $\implies$ its columns are linearly independent over L. Since these columns are the orbit vectors of $\Lambda := \{\sigma_1(\ell), \ldots, \sigma_n(\ell)\}$, I.G.3 ensures that Λ is independent over K, hence a basis.

Case II ($|K| < \infty$): Recall that a Galois extension L/K of a finite field is cyclic, with $\mathrm{Aut}(L/K) = \langle \eta \rangle \cong \mathbb{Z}_n$. Consider L as a $K[x]$-module, with x acting by η; the structure theorem then lets us write

$$L \cong K[x]/(\delta_1(x)) \oplus \cdots \oplus K[x]/(\delta_s(x)),$$

with δ_s the minimal polynomial and $\prod_i \delta_i$ the characteristic polynomial of η.

Now as $\eta^n = \mathrm{id}_L$, η satisfies $x^n - 1 = 0$. Moreover, if $\beta_1, \ldots, \beta_n$ is any basis for L/K, then the orbit vectors $\{(\beta_i, \eta(\beta_i), \ldots, \eta^{n-1}(\beta_i))\}_{i=1}^n$ are independent/L by I.G.3. So the matrix $[\eta^{j-1}(\beta_i)]$ is invertible, and its columns $\{(\eta^{j-1}(\beta_1), \ldots, \eta^{j-1}(\beta_n))\}_{j=1}^n$ hence the automorphisms $1, \eta, \eta^2, \ldots, \eta^{n-1}$ are linearly independent/L.[29] Consequently η satisfies no polynomial equation of degree $< n$, and we must have $\delta_s(x) = x^n - 1$, and (since $\deg(\prod_i \delta_i) = \dim_K(L) = n$) also $s = 1$.

Conclude that $L = K[x]/(x^n - 1)$ is a cyclic $K[x]$-module. So there exists $u \in L$ such that $u, \eta(u), \eta^2(u), \ldots, \eta^{n-1}(u)$ is a (normal) basis of L/K. □

[29]More efficiently, one could use the Dedekind Independence Theorem I.L.8 here.