I. GALOIS THEORY

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 \( \alpha \) is then called a \textit{primitive element} for the extension.) More generally, we should wonder for which extensions just one generator \( \alpha \) will do. For one thing, automorphisms would then be determined by where \( \alpha \) goes.

I.I. LEMMA. \textit{Let} \( L/K \) \textit{be an algebraic extension. Then} \( L/K \) \textit{is simple} \iff \( L/K \) \textit{contains only finitely many intermediate fields.}

\textbf{Proof.} \((\implies):\) Assume \( K(\alpha) = L \); algebraicity of \( \alpha \) 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 \( m_\alpha \), we have \( \mu_\alpha = g_{i_1} \cdots g_{i_\ell} = a_r + \cdots + a_1 x^{r-1} + x^r \). Since \( \mu_\alpha \) 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.

\((\iff):\) 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 \( r := \inf\{|S|\mid K(S) = L\} > 1 \) and write \( L = K(a_1, \ldots, a_r) \). As \( \kappa \) ranges over \( K \), the fields \( K(a_1 + \kappa a_2) \) cannot all be distinct (without contradicting the hypothesis), and there exist distinct \( \kappa, \kappa' \in K \) for which \( K(a_1 + \kappa a_2) = K(a_1 + \kappa' a_2) \). So \( K(a_1 + \kappa a_2) \) contains \( (a_1 + \kappa a_2) - (a_1 + \kappa' a_2) = (\kappa - \kappa') a_2 \), hence \( a_2 \), hence \( a_1 \). This means that \( K(a_1 + \kappa a_2) = K(a_1, a_2) \), and we can generate \( L \) with \( r - 1 \) elements, contradicting minimality of \( r \).

I.I.2. THEOREM OF THE PRIMITIVE ELEMENT. \textit{Any finite and separable extension is simple.}

\textbf{Proof.} Since \( L/K \) is finite, it is certainly finitely generated (and algebraic), and we may write \( L = K(a_1, \ldots, a_r) \). The polynomial
\( g := \prod_i m_{\alpha_i} \) is separable since each \( \alpha_i \) is. If \( N / L \) is a SFE for \( g \), then so is \( N / K \), which is thus Galois, making \( K = \Inv(\Aut(N/K)) \). Since \( \Aut(N/K) \) 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 \( m_\alpha \in K[\alpha] \) splits over \( L \) since \( L / K \) is normal. No proper subfield contains the root \( \alpha \), and so \( L / K \) is a SFE for \( m_\alpha \). \( \square \)

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 \( \Aut(L/\mathbb{Q}) = \{1, \sigma_2, \sigma_3, \sigma_2\sigma_3\} \) (where \( \sigma_j : \sqrt{j} \mapsto -\sqrt{j} \)). 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 \( \sigma_2, \sigma_3, \) 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, \( \ell^p \) 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.

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 \( \text{Aut}(L/K) \) is trivial (has fixed field \( L \)) hence entirely fails to “regulate” subfields.

We will not prove the Normal Basis Theorem now, but I would like to explain the idea. Let \( L/K \) be Galois, of degree \( n \), and write 
\[ G := \text{Aut}(L/K) = \{\sigma_1, \ldots, \sigma_n\} \]. Given \( \alpha \in L \), we have \( m_\alpha(x) = \prod_{i=1}^{m_\alpha}(x - \alpha_i) \) (with \( \alpha_1 = \alpha \), and distinct \( \alpha_i \)'s), and the orbit \( G(\alpha) \) is exactly \( \{\alpha_1, \ldots, \alpha_{m_\alpha}\} \). (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 \( \prod_{j}(x - \alpha_{ij}) \) would be invariant under \( G \), hence belong to \( K \), making \( m_\alpha \) reducible in \( K[x] \).) We also have \([K(\alpha):K] = m\). Considering \( m = n \) vs. \( m < n \) yields the

I.I.6. Proposition. \( \alpha \) is a primitive element \( \iff \sigma_1(\alpha), \ldots, \sigma_n(\alpha) \) are distinct.

What the Normal Basis Theorem says is that we can actually choose \( \alpha \) so that these \( \{\sigma_i(\alpha)\} \) are independent over \( K \), giving a basis for \( L/K \).

(1) \( L = \mathbb{Q}(\zeta_5) \): a normal basis \( / \mathbb{Q} \) is given by \( \alpha = \zeta_5 \), since its Galois orbit is \( \zeta_5, \zeta_5^2, \zeta_5^3, \) and \( \zeta_5^4 = -1 - \zeta_5 - \zeta_5^2 - \zeta_5^3 \).
(2) \( L = \mathbb{Q}(\sqrt{2}, \sqrt{3}) \): \( \sqrt{2} + \sqrt{3} \) does not give a normal basis! But \( 1 + \sqrt{2} + \sqrt{3} + \sqrt{6} \) does (why?).