Chapter 3. Galois Theory

3.1 Theorem: *(The Separability of Subfields of* $\mathbf{C}$*) Let* K *be a field with* $\mathbf{Q} \subseteq K \subseteq \mathbf{C}$ *and let* $f(x) \in K[x]$*. If* $f(x)$ *is irreducible in* $K[x]$*, then* $f(x)$ *has no multiple roots in* $\mathbf{C}$*.*

Proof: Suppose that $f(x)$ has a multiple root in $\mathbf{C}$. Choose $a \in \mathbf{C}$ such that $(x-a)^2 \big| f(x)$ in $\mathbf{C}[x]$, say $f(x) = (x-a)^2 g(x)$ with $g(x) \in \mathbf{C}[x]$. Since $f'(x) = 2(x-a)g(a) + (x-a)^2 g'(x)$, we see that $(x-a)\big|f'(x)$ in $\mathbf{C}[x]$. Since $(x-a)\big|f(x)$ and $(x-a)\big|f'(x)$ we have $(x-a)\big|d(x)$ where $d(x) = \gcd\big(f(x), f'(x)\big)$ in $\mathbf{C}[x]$. Since $f(x) \in K[x]$ and $f'(x) \in K[x]$, when we calculate $d(x)$ using the Euclidean Algorithm we obtain $d(x) \in K[x]$ and we have $d(x)\big|f(x)$ in $K[x]$ and $d(x)\big|f'(x)$ in $K[x]$. Since $(x-a)\big|d(x)$ in $\mathbf{C}[x]$ we have $\deg(d) \geq 1$. Since $d(x)\big|f'(x)$ and $\deg(f') = \deg(f) - 1$, we have $\deg(d) < \deg(f)$. Since $d(x)\big|f(x)$ in $K[x]$ and $1 \leq \deg(d) < \deg(f)$ it follows that $f(x)$ is reducible in $K[x]$.

3.2 Theorem: *(The Primitive Element Theorem) Let* K *and* L *be fields with* $\mathbf{Q} \subseteq K \subseteq L \subseteq \mathbf{C}$*. If* $[L:K]$ *is finite then there exists an element* $a \in L$ *such that* $L = K[a]$*.*

Proof: Suppose that $[L:K]$ is finite. Let $\{u_1, u_2, \cdots, u_n\}$ be a basis for L over K. Then we have $L = K[u_1, u_2, \cdots, u_n]$. Note that it suffices for us to show that for all $u, v \in L$ we can find $w \in L$ such that $K[u,v] = K[w]$ because then we can find elements w_i such that

$$K[u_1,u_2]=w_2\ ,\ K[u_1,u_2,u_3]=K[w_2,u_3]=K[w_3]\ ,\ K[u_1,u_2,u_3,u_4]=K[w_3,u_4]=K[w_4]$$

and so on. Let $u, v \in L$. Let $f(x) \in K[x]$ be the minimal polynomial of u over K and let $g(x) \in K[x]$ be the minimal polynomial of v over K. Let $a_1, a_2, \cdots, a_k$ be the roots of $f(x)$ in $\mathbf{C}$ with $a_1 = u$, and let $b_1, b_2, \cdots, b_\ell$ be the roots of $g(x)$ in $\mathbf{C}$ with $b_1 = v$. Choose any element $t \in K$ such that $t \neq -\frac{u-a_i}{v-b_j}$ for any indices i, j and let $w = u + tv$. Note that $w = u + tv \in K[u,v]$ so we have $K[w] \subseteq K[u,v]$. We claim that $K[u,v] \subseteq K[w]$. Let $h(x) = f(w - tx) = f(u + t(v-x)) \in K[w][x]$ and let $d(x) = \gcd\big(g(x), h(x)\big) \in K[w][x]$. Note that v is a root of $d(x)$ since $g(v) = 0$ and $h(v) = g(w - tv) = h(u) = 0$. Our choice of t ensures that v is the *only* common root of $g(x)$ and $h(x)$ in $\mathbf{C}$. Indeed, given $x \in \mathbf{C}$, if $g(x) = 0$ then we must have $x = b_j$ for some index j, and if $x = b_j$ and $h(x) = 0$ then we must have $0 = h(b_j) = f\big(u + t(v - b_j)\big)$ so that $u + t(v - b_j) = a_i$ for some index i, but then $t = -\frac{u-a_i}{v-b_j}$. Since v is the only common root of $g(x)$ and $h(x)$ in $\mathbf{C}$ it follows that $d(x) = (x - v)$. Since $d(x) = (x-v)$ and $d(x) \in K[w][x]$ it follows that $v \in K[w]$. Since $v \in K[w]$ and $u = w - tv$ we also have $u \in K[w]$. Since $u \in K[w]$ and $v \in K[w]$ it follows that $K[u,v] \subseteq K[w]$, as claimed.

3.3 Definition: Let K, L and M be fields with $K \subseteq L \subseteq M$. An **embedding** of L into M is an injective ring homomorphism $\phi : L \to M$. An **automorphism** of L is a bijective ring homomorphism $\phi : L \to L$. For a ring homomorphism $\phi : L \to M$, we say that ϕ **fixes** K, or that ϕ is K**-fixing**, when $\phi(x) = x$ for all $x \in K$. We use the notation

$$\mathrm{Hom}_K(L,M) = \big\{K\text{-fixing embeddings } \phi : L \to M\big\}$$
$$\mathrm{Aut}_K(L) = \big\{K\text{-fixing automorphhisms } \phi : L \to L\big\}.$$

Note that $\mathrm{Aut}_K(L)$ is a group and we have $\mathrm{Aut}_K(L) \subseteq \mathrm{Hom}_K(L,M)$.

3.4 Note: Let K, L and M be fields with $K \subseteq L \subseteq M$ such that $[L : K]$ finite. For $\phi \in \mathrm{Hom}_K(L, M)$ we have $\phi \in \mathrm{Aut}_K(L) \Longleftrightarrow \phi(L) \subseteq L$.

Proof: Let $\phi \in \mathrm{Hom}_K(L, M)$. If $\phi \in \mathrm{Aut}_K(L)$ then we have $\phi(L) = L$ so $\phi(L) \subseteq L$. Suppose, conversely, that $\phi(L) \subseteq L$. Since ϕ fixes K we have $K \subseteq \phi(L)$. Since ϕ gives a K-fixing isomorphism $\phi : L \to \phi(L)$, if $\{u_1, u_2, \cdots, u_n\}$ is a basis for L over K then $\{\phi(u_1), \cdots, \phi(u_n)\}$ is a basis for $\phi(L)$ over K, and so we have $[\phi(L) : K] = [L : K]$. Since $K \subseteq \phi(L) \subseteq L$ and $[\phi(L) : K] = [L : K]$, it follows that $\phi(L) = L$ and so $\phi \in \mathrm{Aut}_K(L)$.

3.5 Theorem: *(The Embedding Extension Theorem) Let K be a field with $\mathbf{Q} \subseteq K \subseteq \mathbf{C}$. Let $a \in \mathbf{C}$ be algebraic over K and let $n = [K(a) : K]$. Then every embedding of K into $\mathbf{C}$ extends to exactly n embeddings of L into $\mathbf{C}$.*

Proof: Let $\phi : K \to \mathbf{C}$ be an embedding of K into $\mathbf{C}$. Let $f(x) \in K[x]$ be the minimal polynomial of a over K. Say $f(x) = \sum_{i=0}^{n} c_i x^i$ with each $c_i \in K$ and $c_n = 1$. Let $\psi : L \to \mathbf{C}$ be an embedding of L into $\mathbf{C}$. In order for ψ to extend ϕ, we must have $\psi(c_i) = \phi(c_i)$ for all indices i so that

$$0 = \psi(0) = \psi\big(f(a)\big) = \psi\big(\sum_{i=0}^{n} c_i a^i\big) = \sum_{i=0}^{n} \phi(c_i)\psi(a)^i = \sum_{i=0}^{n} \psi(c_i)\psi(a)^i.$$

This shows that for ψ to extend ϕ, the element $\psi(a)$ must be a root of the polynomial $g(x) = \sum_{i-0}^{n} \phi(c_i)x^i$ which lies in $\phi(K)[x]$. Since $\phi : K \to \phi(K)$ is an isomorphism, the map $\Phi : K[x] \to \phi(K)[x]$ given by $\Phi\big(\sum u_i x_i\big) = \sum \phi(u_i)x^i$ is also an isomorphism. Since $f(x)$ is irreducible in $K[x]$ with $\deg(f) = n$, and we have $g(x) = \Phi(f(x))$, it follows that $g(x)$ is irreducible in $\phi(K)[x]$ with $\deg(g) = n$. Let $b_1, b_2, \cdots, b_n$ be the roots of $g(x)$ in $\mathbf{C}$. Thus in order for ψ to extend ϕ, we must have $\psi(a) = b_k$ for some index k. On the other hand, for each index k, there is a unique embedding $\psi_k : L \to \mathbf{C}$ with $\psi_k(a) = b_k$. Indeed the set $\{1, a, a^2, \cdots, a^{n-1}\}$ is a basis for L over K, so each $x \in L$ can be written uniquely in the form $\sum_{i=0}^{n-1} r_i a^i$ with each $r_i \in K$, and the unique embedding $\psi_k : L \to \mathbf{C}$ with $\psi_k(a) = b_k$ must be given by the formula

$$\psi_k\big(\sum_{i=0}^{n-1} r_i a^i\big) = \sum_{i=0}^{n-1} \phi(r_i){b_k}^i,$$

and the above formula does indeed define an embedding $\psi_k : L \to \mathbf{C}$ which extends ϕ. We also remark that the above map ψ_k gives an isomorphism $\psi_k : L = K[a] \to \phi(K)[b_k]$.

3.6 Corollary: *Let K and L be fields with $\mathbf{Q} \subseteq K \subseteq L \subseteq \mathbf{C}$. If $[L : K] = n \in \mathbf{Z}^+$ then every embedding of K into $\mathbf{C}$ extends to exactly n embeddings of L into $\mathbf{C}$.*

Proof: Suppose $[L : K] = n$. By the Primitive Element Theorem, we can choose $a \in L$ such that $L = K(a)$. By the above theorem, every embedding of K into $\mathbf{C}$ extends to exactly n embeddings of $L = K(a)$ into $\mathbf{C}$.

3.7 Corollary: *Let K and L be fields with $\mathbf{Q} \subseteq K \subseteq L \subseteq \mathbf{C}$ with $[L : K]$ finite. Then*

$$\big|\mathrm{Hom}_K(L, \mathbf{C})\big| = [L : K].$$

Proof: Let $n = [L : K]$. The identity embedding $I : K \to \mathbf{C}$ (given by $I(x) = x$ for all $x \in K$) extends to exactly n embeddings of L into $\mathbf{C}$. These are precisely the elements in $\mathrm{Hom}_K(L, \mathbf{C})$.

3.8 Definition: Let K and L be a fields with $\mathbf{Q} \subseteq K \subseteq L \subseteq \mathbf{C}$ and let $f(x) \in K[x]$. We say that $f(x)$ **splits** in L when $f(x)$ factors completely into linear factors in $L[x]$. We say that L is the **splitting field** of $f(x)$ when $L = K(a_1, a_2, \cdots, a_n)$ where $a_1, a_2, \cdots, a_n$ are the roots of $f(x)$ in $\mathbf{C}$.

3.9 Theorem: *Let K and L be fields with $\mathbf{Q} \subseteq K \subseteq L \subseteq \mathbf{C}$ such that $[L : K]$ is finite. Then the following statements are equivalent:*

(1) $\left|\mathrm{Aut}_K(L)\right| = [L : K]$,

(2) $\mathrm{Hom}_K(L, \mathbf{C}) = \mathrm{Aut}_K(L)$,

(3) for every $a \in L$, the minimal polynomial of a over K splits in L, and

(4) L is the splitting field of some polynomial $f(x) \in K[x]$.

Proof: First let us show that (1) $\Longleftrightarrow$ (2). Note that $\left|\mathrm{Hom}_K(L, \mathbf{C})\right| = [L : K]$ because the identity embedding $I : K \to \mathbf{C}$ given by $I(x) = x$ for all $x \in K$ extends to exactly $[L : K]$ embeddings from L into $\mathbf{C}$. Since $\mathrm{Aut}_K(L) \subseteq \mathrm{Hom}_K(L, \mathbf{C})$, it follows that (1) $\Longleftrightarrow$ (2).

Next, let us prove that (2) $\Longrightarrow$ (3). Suppose that $\mathrm{Hom}_K(L, \mathbf{C}) = \mathrm{Aut}_K(L)$. Let $a \in L$ and let $f(x) \in K[x]$ be the minimal polynomial for a over K. Let $a_1, a_2, \cdots, a_\ell$ be the roots of $f(x)$ in $\mathbf{C}$ with $a = a_1$. Note that $[K(a) : K] = \deg(f) = \ell$. The identity embedding $I : K \to \mathbf{C}$ extends to the ℓ embeddings $\phi_j : K(a) \to \mathbf{C}$ with $\phi_j(a) = a_j$. Each embedding $\phi_j : K \to \mathbf{C}$ extends to at least one embedding $\psi_j : L \to \mathbf{C}$. Since ϕ_j fixes K and ψ_j extends ϕ_j, it follows that ψ_j also fixes K. Since $\psi_j \in \mathrm{Hom}_K(L, \mathbf{C}) = \mathrm{Aut}_K(L)$, we have $\psi_j(x) \in L$ for all $x \in L$ so, in particular, we have $a_j = \psi_j(a) \in L$. Since $a_j \in L$ for all indices j, it follows that $f(x)$ splits in L.

Now let us prove that (3) $\Longrightarrow$ (4). Suppose that for every $a \in L$ the minimal polynomial of a over K splits in L. Choose $a \in L$ so that $L = K(a)$. Let $f(x) \in K[x]$ be the minimal polynomial of a over K, and let $a_1, a_2, \cdots, a_n$ be the roots of $f(x)$ in $\mathbf{C}$ with $a = a_1$. Since $f(x)$ splits in L, each $a_i \in L$. It follows that $L = K(a) = K(a_1) = K(a_1, a_2, \cdots, a_n)$. Thus L is the splitting field of $f(x)$.

Finally, let us prove that (4) $\Longrightarrow$ (1). Let L be the splitting field of $f(x) \in K[x]$ over K. Let $a_1, a_2, \cdots, a_n$ be the roots of $f(x)$ in $\mathbf{C}$ and note that each $a_i \in L$. If $f(x)$ has only linear factors in $K[x]$ then we have $K = L$ and $|\mathrm{Aut}_K(L)| = 1 = [L : K]$. Otherwise, let $g_1(x) \in K[x]$ be a nonlinear irreducible factor of $f(x)$ in $K[x]$. Let $a_{1,1}, a_{1,2}, \cdots, a_{1,\ell_1}$ be the roots of $g_1(x)$ in $\mathbf{C}$. Note that $\{a_{1,1}, \cdots, a_{1,\ell_1}\} \subseteq \{a_1, a_2, \cdots, a_n\}$ and that $\deg(g_1) = \ell_1 = [K(a_{1,1}) : K]$. The identity embedding $I : K \to \mathbf{C}$ extends to the ℓ_1 embeddings $\phi_{j_1} : K(a_{1,1}) \to K(a_{1,j_1}) \subseteq L$ determined by $\phi_{j_1}(a_{1,1}) = a_{1,j_1}$. Note that since L is the splitting field of $f(x)$ over K, it is also the splitting field of $f(x)$ over $K(a_{1,1})$. If $f(x)$ splits in $K(a_{1,1})$ then $L = K(a_{1,1}) = L(a_{1,j_1})$ and we are done. Otherwise, let $g_2(x) \in K(a_{1,1})[x]$ be a nonlinear irreducible factor of $f(x)$ in $K(a_{1,1})[x]$. Let $a_{2,1}, a_{2,2}, \cdots, a_{2,\ell_2}$ be the roots of $g_2(x)$ in $\mathbf{C}$. Note that $\{a_{1,1}, \cdots, a_{1,\ell_1}, a_{2,1}, \cdots, a_{2,\ell_2}\} \subseteq \{a_1, \cdots, a_n\}$ and that $\deg(g_2) = \ell_2 = [K(a_{1,1}, a_{2,1}) : K(a_{1,1})]$. The ℓ_1 embeddings $\phi_{j_1} : K(a_{1,1}) \to \mathbf{C}$ extend to give a total of $\ell_1\ell_2$ embeddings $\phi_{j_1,j_2} : K(a_{1,1}, a_{2,1}) \to \mathbf{C}$ where $\phi_{j_1,j_2}(a_{2,1}) = a_{2,j_2}$. Repeating this procedure inductively, we eventually obtain $L = K(a_{1,1}, a_{2,1}, \cdots, a_{m,1})$ after m steps giving a total of $\ell_1\ell_2\cdots\ell_m$ embeddings $\phi_{j_1,j_2,\cdots,j_m} : K(a_{1,1}, \cdots, a_{m,1}) \to \mathbf{C}$ with $\left[K(a_{1,1}, \cdots, a_{i,1}) : K(a_{1,1}, \cdots, a_{i-1,1})\right] = \ell_i$ and $\ell_1\ell_2\cdots\ell_m = n = [L : K]$. Since the image of the embedding $\phi_{j_1,\cdots,j_\ell} : L \to \mathbf{C}$ is a field E with $K \subseteq E \subseteq L$ and $[E : K] = n = [L : K]$, we must have $E = L$ so that $\phi_{j_1,\cdots,j_\ell}$ is an automorphism of L. This procedure produces every possible K-fixing embedding of L in $\mathbf{C}$, and every one of them is an automorphism of L, so we have $\left|\mathrm{Hom}_K(L, \mathbf{C})\right| = \left|\mathrm{Aut}_K(L)\right| = \ell_1\ell_2\cdots\ell_m = n = [L : K]$.

3.10 Definition: When K and L are fields with $\mathbf{Q} \subseteq K \subseteq L \subseteq \mathbf{C}$ and $[L : K]$ is finite, we say that L is **Galois** over K when the equivalent statements in the above theorem hold.

3.11 Definition: Let K and L be fields with $\mathbf{Q} \subseteq K \subseteq L \subseteq \mathbf{C}$. The **Galois group** of L over K is the group $\mathrm{Aut}_K(L)$. For a subgroup $H \subseteq G$, the **fixed field** of H is the set

$$\mathrm{Fix}(H) = \big\{ x \in L \,\big|\, \sigma(x) = x \text{ for all } \sigma \in H \big\}.$$

It is not difficult to verify that $\mathrm{Fix}(H)$ is a subfield of L.