Chapter 4. Galois Theory

Separable Extensions and Galois Extensions

4.1 Definition: Let F be a field. A nonzero polynomial $f \in F[x]$ is called **separable** when it has no repeated roots in its splitting field over F. Let F be a subfield of K. An element $a \in K$ is called **separable** over F when a is algebraic over F and the minimal polynomial of a over F is separable. The field K is **separable** over F when K is algebraic over F and every element $a \in K$ is separable over F.

4.2 Example: When F is a field with $\text{char}(F) = 0$, every algebraic extension field K of F is separable, because irreducible polynomials in $F[x]$ never have repeated roots in their splitting field (by Corollary 3.35). When F is a finite field, every algebraic extension field K of F is separable. Indeed if $a \in K$ then a is algebraic over F, so $[F(a) : F]$ is finite, so $F(a)$ is also a finite field. If $\big|F(a)\big| = p^n$ then a is a root of $f(x) = x^{p^n} - x$, which has no repeated roots, so the minimal polynomial of a over F divides f, and has no repeated roots.

4.3 Theorem: *(The Primitive Element Theorem) Let F be a subfield of K. If $[K : F]$ is finite and K is separable over F then there exists an element $a \in K$ such that $K = F[a]$.*

Proof: Suppose that $[K : F]$ is finite and K is separable over F. If F is finite then K is also finite (since $[K : F]$ is finiute), so the group of units K^* is cyclic, and if we choose $a \in K$ such that $K^* = \langle a \rangle$ then clearly we have $K = F[a]$. Suppose that F is infinite. Let $\{u_1, u_2, \cdots, u_n\}$ be a basis for K over F. Then we have $K = F[u_1, u_2, \cdots, u_n]$. Note that it suffices for us to show that for all $u, v \in K$ we can find $w \in K$ such that $F[u, v] = F[w]$ because then we can find elements w_i such that

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

and so on. Let $u, v \in K$. Let $f(x) \in F[x]$ be the minimal polynomial of u over F and let $g(x) \in F[x]$ be the minimal polynomial of v over F. Let L be the splitting field of fg over F and note that, since K is separable over F, f and g have no repeated roots in L. Let $a_1, a_2, \cdots, a_k$ be the roots of $f(x)$ in L with $a_1 = u$, and let $b_1, b_2, \cdots, b_\ell$ be the roots of $g(x)$ in L with $b_1 = v$. Choose any element $t \in F$ such that $t \neq -\frac{u - a_i}{v - b_j}$ for any indices i, j and let $w = u + tv$. Note that $w = u + tv \in F[u, v]$ so we have $F[w] \subseteq F[u, v]$. We claim that $F[u, v] \subseteq F[w]$. Let $h(x) = f(w - tx) = f(u + t(v - x)) \in F[w][x]$ and let $d(x) = \gcd\big(g(x), h(x)\big) \in F[w][x]$. 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 L. Indeed, given $x \in L$, 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 L it follows that $d(x) = (x - v)$. Since $d(x) = (x - v)$ and $d(x) \in F[w][x]$ it follows that $v \in F[w]$. Since $v \in F[w]$ and $u = w - tv$ we also have $u \in F[w]$. Since $u \in F[w]$ and $v \in F[w]$ it follows that $F[u, v] \subseteq F[w]$, as claimed.

4.4 Definition: Let F be a subfield of K. An **automorphism** of K is a bijective homomorphism $\phi : K \to K$. The set of all such automorphisms is a group (under composition) which we denote by $\mathrm{Aut}K$. An automorphism $\phi \in \mathrm{Aut}K$ is said to be **F-fixing** when $\phi(a) = a$ for every $a \in F$. The set of all F-fixing automorphisms of K is denoted by $\mathrm{Aut}_F K$, so

$$\mathrm{Aut}_F K = \big\{\phi \in \mathrm{Aut}K \,\big|\, \phi(a) = a \text{ for every } a \in F\big\}.$$

Note that $\mathrm{Aut}_F K$ is a subgroup of $\mathrm{Aut}K$. Recall that when $\phi \in \mathrm{Aut}K$, the fixed point set $\mathrm{Fix}(\phi) = \big\{a \in K \,\big|\, \phi(a) = a\big\}$ is a subfield of K. More generally, for any nonempty set $S \subseteq \mathrm{Aut}K$, the **fixed point set** of S is the set

$$\mathrm{Fix}(S) = \big\{a \in K \,\big|\, \phi(a) = a \text{ for every } \phi \in S\big\} = \bigcap_{\phi \in S} \mathrm{Fix}(\phi).$$

Note that $\mathrm{Fix}(S)$ is a subfield of K.

4.5 Note: Let F be a subfield of K and let $\phi \in \mathrm{Aut}_F K$. If $K = F(a_1, \cdots, a_n)$, then every ϕ is determined by the values $\phi(a_i) \in K$. Indeed, in the case that each a_k is algebraic over F, every element in $u \in K$ can be written in the form $u = \sum_{k_1,k_2,\cdots,k_n} c_{k_1,k_2,\cdots,k_n} {a_1}^{k_1} {a_2}^{k_2} \cdots {a_n}^{k_n}$ with each $c_{k_1,\cdots,k_n} \in F$, and we have

$$\phi\Big(\sum_{k_1,k_2,\cdots,k_n} c_{k_1,k_2,\cdots,k_n} {a_1}^{k_1} {a_2}^{k_2} \cdots {a_n}^{k_n}\Big) = \sum_{k_1,\cdots,k_n} c_{k_1,\cdots,k_n} \phi(a_1)^{k_1} \cdots \phi(a_n)^{k_n}.$$

4.6 Note: Let F be a subfield of K and let $\phi \in \mathrm{Aut}_F K$. If $f \in F[x]$ and a is a root of f in K, $\phi(a)$ must also be a root of f in K. Indeed, if $f(x) = \sum_{k=0}^{n} c_k x^k$ with $f(a) = 0$, then we have

$$0 = \phi(0) = \phi\big(f(a)\big) = \phi\big(\sum_{k=0}^{n} c_k a^k\big) = \sum_{k=0}^{n} c_k \phi(a)^k = f\big(\phi(a)\big).$$

Since ϕ is bijective, it permutes the roots of f in K.

4.7 Theorem: *Let F be a subfield of K. Suppose that K is the splitting field, over F, of a separable polynomial $f \in F[x]$. Then*

$$\big|\mathrm{Aut}_F K\big| = [K : F].$$

Proof: If $K = F$ then $\mathrm{Aut}_F K = \{I\}$ (where I is the identity map) and $\big|\mathrm{Aut}_F K\big| = [K:F] = 1$. Suppose that $K \neq F$. Choose a root a of f in K with $a \notin F$, and let $g \in F[x]$ be an irreducible factor of f with $g(a) = 0$ in K. Since f is separable, so is g. Let $a = a_1, a_2 \cdots, a_n$ be the roots of g in K. For each $j = 1, 2, \cdots, n$, choose $\phi_j \in \mathrm{Aut}_F K$ with $\phi_j(a) = a_j$ (we can do this by Theorem 3.28: we first extend the identity map $I : F \to F$ to an isomorphism $\phi_j : F(a_1) \to F(a_j)$ with $\phi(a_1) = a_j$, then we extend ϕ_j to an isomorphism $\phi_j : K \to K$). We have $[K : F] = [K : F(a)]\,[F(a) : F]$ with $[F(a) : F] = n$. Say $[K : F(a)] = m$ so that $[K : F] = nm$. Since K is the splitting field of f over F, it is also the splitting field of f over $F(a)$, so we may suppose, inductively, that $\big|\mathrm{Aut}_{F(a)} K\big| = [K : F(a)] = m$.

Say $\mathrm{Aut}_{F(a)} K = \big\{\psi_1, \cdots, \psi_m\big\}$. For each $i \in \{1, \cdots, n\}$ and $j \in \{1, \cdots, m\}$, we have $\phi_i \psi_j \in \mathrm{Aut}_F K$. Note that the automorphisms $\phi_i \psi_j$ are distinct because if $\phi_i \psi_j = \phi_k \psi_\ell$ then we have $a_i = \phi_i(a) = \phi_i \psi_j(a) = \phi_k \psi_\ell(a) = \phi_k(a) = a_k$ so that $i = k$, and hence $\psi_j = {\phi_i}^{-1} \phi_i \psi_j \phi_k {}^{-1} \phi_k \psi_\ell = \psi_\ell$ so that $j = \ell$. Also note that every $\theta \in \mathrm{Aut}_F K$ is of the form $\theta = \phi_i \psi_j$. Indeed, given $\theta \in \mathrm{Aut}_F K$, since θ permutes the roots of g we have $\theta(a) = a_i$ for some i, then $\phi_i^{-1} \theta(a) = a$ so that $\phi_i^{-1} \theta$ fixes $F(a)$, and hence we have $\phi_i^{-1} \theta = \psi_j$ for some j so that $\theta = \phi_i \psi_j$. Thus we have $\big|\mathrm{Aut}_F K\big| = nm = [K : F]$, as required.

4.8 Theorem: (*Characterizations of Galois Extensions) Let F be a subfield of K with $[K:F]$ finite. The following are equivalent.*

(1) $\mathrm{Fix}\big(\mathrm{Aut}_F K\big) = F$.

(2) Every irreducible polynomial in $F[x]$ with a root in K is separable and splits in $K[x]$.

(3) K is the splitting field, over F, of a separable polynomial $f \in F[x]$.

Proof: To prove that (1) $\Longrightarrow$ (2), suppose that $\mathrm{Fix}(\mathrm{Aut}_F K) = F$, let $f \in F[x]$ be irreducible, and let $a \in K$ with $f(a) = 0$. By dividing by the leading coefficient, we may assume that f is monic, so f is the minimal polynomial of a over F. Let $S = \big\{\phi(a) \,\big|\, \phi \in \mathrm{Aut}_F K\big\}$. Note that S is a subset of the set of roots of f in K, and each $\phi \in \mathrm{Aut}_F K$ permutes the elements in S . Let $n = |S|$, and say $S = \big\{a_1, a_2, \cdots, a_n\big\}$ with $a = a_1$. Let $g(x) = \prod_{k=1}^{n}(x - a_k) \in K[x]$. Write $g(x) = \sum_{k=0}^{n} c_k x^k$ with each $c_k \in K$. For each $\phi \in \mathrm{Aut}_F K$, using the associated ring isomorphism $\phi : K[x] \to K[x]$ we have $\phi(g)(x) = \phi\big(\sum_{k=0}^{n} c_k x^k\big) = \sum_{k=0}^{n} \phi(c_k) x^k$. Since ϕ permutes the elements in S we also have $\phi(g)(x) = \phi\big(\prod_{k=1}^{n}(x - a_i)\big) = \prod_{k=1}^{n}\big(x - \phi(a_k)\big) = \prod_{k=1}^{n}(x - a_k) = g(x) = \sum_{k=0}^{n} c_k x^k$. Comparing coefficients, we see that $c_k = \phi(c_k)$ for $0 \le k \le n$. Since this is true for every $\phi \in \mathrm{Aut}_F K$, we have $c_k \in \mathrm{Fix}\big(\mathrm{Aut}_F K\big) = F$. Thus in fact $g \in F[x]$. Since $g \in F[x]$ with $g(a) = 0$, and f is the minimal polynomial of a over F, we have $f \big| g$ in $F[x]$. Since $f \big| g$ in $F[x]$, and g splits in $K[x]$ and has no repeated roots, it follows that f splits in $K[x]$ and has no repeated roots.

To prove that (2) $\Longrightarrow$ (3), suppose that (2) holds, that is every irreducible polynomial in $F[x]$ with a root in K is separable and splits in K. If $K = F$ then K is the splitting field of the separable polynomial $x - 1$. If $K \neq F$ then we choose $a_1 \in K$ with $a_1 \notin F$. Let $f_1 \in F[x]$ be the minimal polynomial of a_1 over F. By (2), f_1 is separable and splits in K. Let F_1 be the splitting field of f_1 over F in K. If $F_1 = K$ we are done. If $F_1 \neq K$ then we choose $a_2 \in K$ with $a_2 \notin F_1$. Let f_2 be the minimal polynomial of a_2 over F. By (2), f_2 is separable and splits in K. Note that $f_1 f_2$ is also separable (if f_1 and f_2 shared a common root b they would both be the minimal polynomial of b, so they would be equal, but f_2 has a root a_2 which is not a root of f_1). Let F_2 be the splitting field of $f_1 f_2$ over F. If $F_2 = K$ we are done, and otherwise we repeat the above procedure.

To prove that (3) $\Longrightarrow$ (1), suppose that K is the splitting field, over F, of a separable polynomial $f \in F[x]$. Let $E = \mathrm{Fix}\big(\mathrm{Aut}_F K\big)$. By the definition of the fixed field, every $\phi \in \mathrm{Aut}_F K$ fixes the elements of E, so we have $\mathrm{Aut}_F K \le \mathrm{Aut}_E K$. By the definition of $\mathrm{Aut}_F K$, every $\phi \in \mathrm{Aut}_F K$ fixes the elements in F, so we have $F \subseteq E$. Since $F \subseteq E$ we have $\mathrm{Aut}_E K \le \mathrm{Aut}_F K$. Thus $\mathrm{Aut}_E K = \mathrm{Aut}_F K$. Since K is the splitting field of f over F, K is also the splitting field of f over E. By the previous theorem, we have $\big|\mathrm{Aut}_F K\big| = [K : F]$ and $\big|\mathrm{Aut}_E K\big| = [K : E]$, and hence $[K : E] = \big|\mathrm{Aut}_E K\big| = \big|\mathrm{Aut}_F K\big| = [K : F]$. Since $[K : E] = [K : F]$ we have $[E : F] = 1$ so that $F = E$, as required.

4.9 Definition: Let F be a subfield of K. The group $\mathrm{Aut}_F K$ is called the **Galois group** of K over F. When $[K:F]$ is finite, we say that K is **Galois** over F when the equivalent conditions of the above theorem are satisfied. Note that when $[K : F]$ is finite and K is Galois over F, the second characterization of Galois extensions (Part 2 of the above theorem) implies that K is separable over F.

The Fundamental Theorem of Galois Theory

4.10 Theorem: (*The Fundamental Theorem of Galois Theory) Let F be a subfield of L with $[L:F]$ finite. Suppose that L is Galois over F. There is a bijective, order-reversing correspondence, between the set of all subfields K of L containing F, and the set of all subgroups H of $\mathrm{Aut}_F K$, which given by $K \mapsto \mathrm{Aut}_F K$ and $H \mapsto \mathrm{Fix}(H)$. Moreover, for each subfield K of L containing F, we have*

(1) $[L:K] = \big|\mathrm{Aut}_K L\big|$ *and* $[K:F] = \Big|\mathrm{Aut}_F L/\mathrm{Aut}_K L\Big|$, *and*

(2) K is Galois over F if and only if $\mathrm{Aut}_K L \trianglelefteq \mathrm{Aut}_F L$ *and, in this case,*

$$\mathrm{Aut}_K F \cong \mathrm{Aut}_F L/\mathrm{Aut}_K L.$$

Proof: Let $\mathcal{K}$ be the set of subfields of L containing F, and let $\mathcal{H}$ be the set of subgroups $H \leq \mathrm{Aut}_F L$, and let $\Phi : \mathcal{K} \to \mathcal{H}$ and $\Psi : \mathcal{H} \to \mathcal{K}$ given by $\Phi(K) = \mathrm{Aut}_K L$ and $\Psi(H) = \mathrm{Fix}(H)$. It is clear that Φ and Ψ are order-reversing. To show that Φ and Ψ are inverses of one another, we show that is $\Psi\Phi = I$ and $\Phi\Psi = I$. Given $K \in \mathcal{K}$, since L is Galois over F it is also Galois over K (if K is the splitting field of the separable polynomial $f \in F[x]$ over F, then K is also the splitting field of f over K) so, by Theorem 4.8, we have $\Psi\Phi(K) = \Psi\big(\mathrm{Aut}_K L\big) = \mathrm{Fix}\big(\mathrm{Aut}_K L\big) = K$. Thus we have $\Psi\Phi = I$.

We claim that $\Phi\Psi = I$, that is $\mathrm{Aut}_{\mathrm{Fix}(H)} L = H$ for all $H \leq \mathrm{Aut}_K L$. Let $H \leq \mathrm{Aut}_F L$ and let $E = \mathrm{Fix}(H)$. We need to show that $\mathrm{Aut}_E L = H$. It is clear that $H \leq \mathrm{Aut}_E L$ because if $\phi \in H$ then, by the definition of $\mathrm{Fix}(H)$, ϕ fixes every element in $E = \mathrm{Fix}(H)$ so that $\phi \in \mathrm{Aut}_E L$. Thus it suffices to show that $|H| \geq \big|\mathrm{Aut}_E L\big|$. Since L is Galois over F, it is also Galois over E so, by Theorem 4.7, we have $\big|\mathrm{Aut}_E L\big| = [L:E]$. Thus it suffices to show that $|H| \geq [L:E]$. We already know that $H \leq \mathrm{Aut}_E L$ so that $|H| \leq \big|\mathrm{Aut}_E L\big| = [L:E]$, so it suffices to show that $|H| \geq [L:E]$. Let $\ell = |H|$ and $n = [L:E]$. Say $H = \big\{\phi_1, \cdots, \phi_\ell\big\}$ with $\phi_1 = I$. Since L is Galois over E, it is separable over E (by Part 2 of Theorem 4.8), so by the Primitive Element Theorem, we can choose $a \in L$ such that $L = E(a)$. Let f be the minimal polynomial of a over E and note that $\deg f = n$. Let $g(x) = \prod_{k=1}^{\ell} \big(x - \phi_k(a)\big) \in L[x]$, and note that $g(a) = 0$ since $\phi_1(a) = a$. For each $\phi \in H$, since left multiplication by ϕ permutes the elements in H (so we have $\{\phi\phi_1, \phi\phi_2, \cdots, \phi\phi_\ell\} = \{\phi_1, \cdots, \phi_\ell\}$) it follows that $\phi(g)(x) = \prod_{k=1}^{\ell} \big(x - \phi\phi_k(a)\big) = \prod_{k=1} \ell\big(x - \phi_k(a)\big) = g(x)$, and hence ϕ fixes all the coefficients of g. This shows that all the coefficients of g lie in $\mathrm{Fix}(H) = E$ so that $g \in E[x]$. Since $g \in E[x]$ with $g(a) = 0$, and f is the minimal polynomial of a over E, we have $f \big| g$, and hence $n \leq \ell$, as required. This completes the proof that Φ and Ψ are inverses, giving an order-reversing bijective correspondence between $\mathcal{K}$ and $\mathcal{H}$.

Note that Part 1 of the theorem follows immediately from Theorem 4.7. Indeed when K is any subfield of L containing F, since L is Galois over F, it is also Galois over K, so we have $\big|\mathrm{Aut}_F L\big| = [L:F]$ and $\big|\mathrm{Aut}_K L\big| = [L:K]$, and hence also

$$[K:F] = [L:F]/[L:K] = \big|\mathrm{Aut}_F L\big| \Big/ \big|\mathrm{Aut}_K L\big| = \Big|\mathrm{Aut}_F L/\mathrm{Aut}_K L\Big|.$$

To prove Part 2, let K be a subfield of L which contains F, and suppose first that $\mathrm{Aut}_K L \trianglelefteq \mathrm{Aut}_F L$. We wish to prove that K is Galois over F. Since L is Galois over F, it is separable over F, and hence K is also separable over F. By the Primitive Element Theorem, we can choose $a \in K$ such that $K = F[a]$. Let $f \in F[x]$ be the minimal polynomial of a over F, and note that f is separable. We claim that K is the splitting field of f. Since L is Galois over F, by Condition (2) of the Characterization of Galois Extensions, f is separable and splits in $L[x]$, so all the roots of f lie in L. We need to show that all the roots of f lie in K. Let $b \in L$ be any root of f. Choose $\phi \in \mathrm{Aut}_F K$ with $\phi(a) = b$ (by Theorem 3.28 we can extend the identity map $I : F \to F$ to an isomorphism $\phi : F(a) \to F(b)$ with $\phi(a) = b$, then we can extend ϕ to an automorphism $\phi : K \to K$). Since $\mathrm{Aut}_K L \trianglelefteq \mathrm{Aut}_F L$, for every $\psi \in \mathrm{Aut}_K L$ we have $\phi^{-1}\psi\phi \in \mathrm{Aut}_K L$ so that $\phi^{-1}\psi\phi$ fixes elements in K, so in particular (since $a \in K$) we have $\phi^{-1}\psi\phi(a) = a$, and hence $\psi\phi(a) = \phi(a)$, that is $\psi(b) = b$. Since $\psi(b) = b$ for every $\psi \in \mathrm{Aut}_K L$, we have $b \in \mathrm{Fix}\big(\mathrm{Aut}_K L\big) = K$. This proves that every root of f lies in K, as required.

Suppose, conversely, that K is Galois over F, say K is the splitting field, over F, of the polynomial $g \in F[x]$. Since K is generated, as a field over F, by the roots of g, and since each $\phi \in \mathrm{Aut}_F K$ permutes these roots, it follows that each $\phi \in \mathrm{Aut}_F K$ restricts to an automorphism of K, that is $\phi\big|_K \in \mathrm{Aut}_F K$. Thus the restriction map $R : \mathrm{Aut}_F L \to \mathrm{Aut}_F K$ given by $R(\phi) = \phi\big|_K$, is a well-defined group homomorphism. The map R is surjective by Theorem 3.28 and Corollary 3,29 (every automorphism of K extends to an automorphism of L since L is the splitting field of a polynomial over K), and $\mathrm{Ker} R = \mathrm{Aut}_K L$. By the First Isomorphism Theorem, $\mathrm{Aut}_K L \trianglelefteq \mathrm{Aut}_F L$ and $\mathrm{Aut}_F L / \mathrm{Aut}_K L \cong \mathrm{Aut}_F K$.

4.11 Exercise: Let F be the splitting field of $f(x) = x^4 - 2$ over $\mathbb{Q}$. Find the lattice of subgroups of $\mathrm{Aut}_{\mathbb{Q}} F$ and the lattice of subfields of F.

4.12 Theorem: (*The Fundamental Theorem of Algebra)* $\mathbb{C}$ *is algebraically closed.*

Proof: Let $f \in \mathbb{C}[x]$ be a non-constant polynomial. We must show that f has a root in $\mathbb{C}$. Say $f(x) = \sum_{k=0}^{n} c_k x^k$ and let $\overline{f}(x) = \sum_{k=0}^{n} \overline{c}_k x^k$. Let $g(x) = f(x)\overline{f}(x)$, and verify, as an exercise, that $g \in \mathbb{R}[x]$. Note that for $z \in \mathbb{C}$, if $g(z) = 0$ then either $f(z) = 0$ or $\overline{f}(z) = 0$, and if $\overline{f}(z) = 0$ then $f(\overline{z}) = 0$, so it suffices to show that g has a root in $\mathbb{C}$. Let $h \in \mathbb{R}[x]$ be an irreducible factor of g in $\mathbb{R}[x]$ and note that, since $\mathrm{char}(\mathbb{R}) = 0$, h is separable. If $\pm i$ is a root of h, then of course h has a root in $\mathbb{C}$. Suppose that $\pm i$ are not roots of h and note that $(x^2 + 1)h(x)$ is separable. Let L be the splitting field, over $\mathbb{R}$ of $(x^2 + 1)h(x)$. Note that $i \in L$ so $\mathbb{C} = \mathbb{R}[i] \subseteq L$. Say $[L : \mathbb{R}] = 2^m \ell$ where $\ell, m \in \mathbb{Z}^+$ with ℓ odd (we remark that $m \geq 1$ since $\mathbb{R} \subseteq \mathbb{C} \subseteq L$). By the Galois correspondence we have $\big|\mathrm{Aut}_{\mathbb{R}} L\big| = 2^m \ell$. By the Sylow theorems, $\mathrm{Aut}_{\mathbb{R}} L$ has a Sylow 2-subgroup with 2^m elements, so by the Galois correspondence, there is a subfield F of L containing $\mathbb{R}$ with $[L : F] = 2^m$. Then we have $[F : \mathbb{R}] = \ell$, which is odd. If we had $\ell > 1$ we could choose $a \in F$ with $a \notin \mathbb{R}$, but then the degree of the minimal polynomial of a would be an odd number greater than 1, and this is not possible since every polynomial in $\mathbb{R}[x]$ with odd degree has a root in $\mathbb{R}$. Thus we must have $\ell = 1$ so that $[L : \mathbb{R}] = 2^m$. Since $\mathbb{R} \subseteq \mathbb{C} \subseteq L$ we have $[L : \mathbb{C}] = 2^{m-1}$, and hence $\big|\mathrm{Aut}_{\mathbb{C}} L\big| = 2^{m-1}$. Suppose, for a contradiction, that $m > 1$. By the Sylow theorems, there is a subgroup of $\mathrm{Aut}_{\mathbb{C}} L$ with 2^{m-2} elements. By the Galois correspondence, there is a subfield K of L containing $\mathbb{C}$ with $[L : K] = 2^{m-2}$, and hence $[K : \mathbb{C}] = 2$. This is not possible since if this were the case we could choose $a \in K$ with $a \notin \mathbb{C}$, then the minimal polynomial of a over $\mathbb{C}$ would have degree 2, but every quadratic polynomial in $\mathbb{C}[x]$ has its roots in $\mathbb{C}$ (by the Quadratic Formula). Thus we must have $m = 1$ so that $[L : \mathbb{C}] = 1$. Thus $\mathbb{C} = L$, which is the splitting field of $(x^2 + 1)h(x)$, so the roots of h lie in $\mathbb{C}$.

4.13 Note: Let $f(x) = ax^2 + bx + c = 0$, where $a, b, c \in \mathbb{C}$ with $a \neq 0$. Recall that we can solve $f(x) = 0$, and obtain the Quadratic Formula, as follows. Divide by a then complete the square by letting $x = y - \frac{b}{2a}$ to get

$$\tfrac{1}{a}\, f(x) = x^2 + \tfrac{b}{a}\, x + \tfrac{c}{a} = \big(y - \tfrac{b}{2a}\big)^2 + \tfrac{b}{a}\big(y - \tfrac{b}{2a}\big) + \tfrac{c}{a} = y^2 + \tfrac{b^2}{4a^2} - \tfrac{b^2}{2a^2} + \tfrac{c}{a} = y^2 - \big(\tfrac{b^2 - 4ac}{4a^2}\big).$$

Thus we have

$$f(x) = 0 \iff y = \pm\tfrac{\sqrt{b^2-4ac}}{2a} \iff x = y - \tfrac{b}{2a} = \tfrac{-b \pm \sqrt{b^2-4ac}}{2a}.$$

4.14 Note: Let $f(x) = ax^3 + bx^2 + cx + d = 0$, where $a, b, c, d \in \mathbb{C}$ with $a \neq 0$. We can solve $f(x) = 0$ as follows. First, divide by a so the equation is converted to the form $x^3 + bx^2 + cx + d = 0$. Next, make the substitution $x = y - \frac{b}{3}$ and rewrite the equation in the form $y^3 + py + q = 0$. Then make the substitution $y = z - \frac{p}{3z}$ to convert the equation to the form $z^3 + q - \frac{p^3}{27} z^{-3} = 0$. Finally, multiply by z^3 to obtain $z^6 + qz^3 - \frac{p^3}{27}$ and solve for z^3 using the Quadratic Formula.

4.15 Exercise: Find the three real roots of $f(x) = x^3 - 3x + 1$.

4.16 Note: Let $f(x) = x^4 + bx^3 + cx^2 + dx + e$ where $b, c, d, e \in \mathbb{C}$. We can solve $f(x) = 0$ as follows. Note that if we can find $s, t, u, v \in \mathbb{C}$ so that

$$f(x) = (x^2 + sx + t)^2 - (ux + v)^2$$

then we can solve $f(x) = 0$ using the Quadratic Formula. Comparing coefficients, we need $2s = b$, $s^2 + 2t - u^2 = c$, $2st - 2uv = d$, and $t^2 - v^2 = e$. The first equation gives $s = \frac{b}{2}$ and the other equations become $u^2 = \frac{b^2}{4} + 2t - c$, $2uv = bt - d$, and $v^2 = t^2 - e$, so we need $(bt - d)^2 = 4u^2v^2 = (b^2 + 8t - 4c)(t^2 - e)$. Thus t must satisfy the cubic equation

$$0 = (8t + b^2 - 4c)(t^2 - e) - (bt - d)^2 = 8t^3 - 4ct^2 + (2bd - 8e)t + (4ce - b^2e - d^2).$$

Equivalently, t must be a root of the cubic polynomial

$$g(x) = 8x^3 - 4c\,x^2 + (2bd - 8e)x + (4ce - b^2e - d^2).$$

$g(x)$ is called a **resolvent cubic** for the quartic polynomial $f(x)$. Thus to solve $f(x) = 0$, we choose $s = \frac{b}{2}$, we solve the cubic equation $g(t) = 0$ to find t, then we choose u and v so that $u^2 = \frac{b^2}{4} + 2t - c$ and $v^2 = t^2 - e$, with the sign of v chosen so that $2uv = bt - d$, and then $f(x) = (x^2 + sx + t)^2 - (ux + v)^2$, so we solve $f(x) = 0$ by the Quadratic Formula.

4.17 Exercise: Find the complex roots of $f(x) = x^4 + 2x^3 + 5x^2 + 6x + 6$.

4.18 Note: A **radical function** of n variables $x_1, x_2, \cdots, x_n$ is a multi-valued function from $\mathbb{C}^n$ to $\mathbb{C}$ which can be obtained from the constant functions c, the k^{th} coordinate functions x_k, and the n^{th} root multi-functions $\sqrt[n]{x}$, using the operations of addition, subtraction, multiplication, division, and composition of functions. For example, the function

$$g(a, b, c) = \frac{\sqrt{a^2 + \sqrt[3]{b - c^4}}}{1 - \sqrt[5]{c + \sqrt{a}}}$$

is a radical function of a, b and c. Note that when a complex root $z \in \mathbb{C}$ of a polynomial $f \in \mathbb{C}[x]$ can be expressed as a radical function of the coefficients of a radical function of the coefficients of f, the root z lies in the top field F_ℓ in a tower of fields

$$\mathbb{C} = F_0 \subseteq F_1 \subseteq F_2 \subseteq \cdots \subseteq F_\ell$$

such that for $1 \leq k \leq \ell$ we have $F_k = F_{k-1}[a_k]$ for some $a_k \in \mathbb{C}$ with ${a_k}^{n_k} \in F_{k-1}$.

4.19 Definition: Let F be a field and let $f \in F[x]$. We say that f is **solvable by radicals** over F when f has a splitting field which is contained in the top field in a tower of fields

$$F = F_0 \subseteq F_1 \subseteq F_2 \subseteq \cdots \subseteq F_\ell$$

where for $1 \leq k \leq \ell$ we have $F_k = F_{k-1}[a_k]$ with $a_k \in F_k$ and ${a_k}^{n_k} \in F_{k-1}$ for some $n_k \in \mathbb{Z}^+$.

4.20 Definition: Let G be a group. We say that G is **solvable** when there is a tower of subgroups

$$\{e\} = H_0 \leq H_1 \leq H_2 \leq \cdots \leq H_\ell = G$$

such that for $1 \leq k \leq \ell$ we have $H_{k-1} \trianglelefteq H_k$ with H_k/H_{k-1} abelian.

4.21 Theorem: *Let G be a group and let $N \trianglelefteq G$.*
(1) If G is solvable then G/N is solvable.
(2) If N is solvable and G/N is solvable then G is solvable.

Proof: The proof is left as an exercise.

4.22 Definition: Let F be a field. An n^{th} **root of unity** in F is an element $a \in F$ such that $a^n = 1$, that is a root of the polynomial $f(x) = x^n - 1$. The set of n^{th} roots of unity in F is a finite subgroup of the group of units F^*, so it is a cyclic group (as in the proof of Theorem 3.39, which shows that the group of units of a finite field is cyclic). A **primitive** n^{th} **root of unity** in F is an element of order n in the group of n^{th} roots of unity. Note that when $\omega \in F$ is a primitive n^{th} root of unity, the polynomial $x^n - 1$ has n distinct roots in F, namely $1, \omega, \omega^2, \cdots, \omega^{n-1}$.

4.23 Theorem: *Let F be a field with $\text{char}(F) = 0$, let $b \in F$, let $f(x) = x^n - b$, and let L be the splitting field of f over F. Then L contains a primitive n^{th} root of unity, and $\text{Aut}_F L$ is solvable.*

Proof: Suppose, first, that F contains a primitive n^{th} root of unity, say ω. Let $a \in L$ be a root of f. Then $L = F[a]$ and the roots of f in L are $a\omega^k$ with $0 \leq k < n$. Each $\phi \in \text{Aut}_F L$ determines and is determined by $\phi(a)$, and we have $\phi(a) = a\omega^k$ for some k. Given $\phi, \psi \in \text{Aut}_F L$, say $\phi(a) = a\omega^k$ and $\psi(a) = a\omega^\ell$, we have $\phi\psi(a) = \phi(a\omega^\ell) = \phi(a)\phi(\omega)^\ell = a\omega^k\omega^\ell = a\omega^{k+\ell}$ and similarly $\psi\phi(a) = a\omega^{k+\ell}$, and hence $\phi\psi = \psi\phi$. Thus $\text{Aut}_F L$ is abelian.

Now suppose F does not contain a primitive n^{th} of unity. Let K be the splitting field of $g(x) = x^n - 1$ over F. Note that since $\text{char}(F) = 0$ so that $\gcd(g, g') = 1$ and g has n distinct roots in K, the group of n^{th} roots of unity in K is a cyclic group of order n, which has a generator of order n, so K contains a primitive n^{th} root of unity, say ω. The roots of g in K are $1, \omega, \omega^2, \cdots, \omega^{n-1}$, and we have $K = F[\omega]$. Each $\phi \in \text{Aut}_F K$ determines and is determined by $\phi(\omega)$, and we have $\phi(\omega) = \omega^k$ for some k. Given $\phi, \psi \in \text{Aut}_F K$ with say $\phi(\omega) = \omega^k$ and $\psi(\omega) = \omega^\ell$, we have $\phi\psi(\omega) = \phi(\omega^\ell) = (\omega^\ell)^k = \omega^{k\ell}$ and similarly $\psi\phi(\omega) = \omega^{k\ell}$, and hence $\phi\psi = \psi\phi$. Thus $\text{Aut}_F K$ is abelian.

Let M be a splitting field of f over K. By the first paragraph, $\text{Aut}_K M$ is abelian. Let $a \in M$ be a root of f. The roots of f in M are $a, a\omega, a\omega^2, \cdots, a\omega^{n-1}$, and we have $M = F[a, a\omega, \cdots, a\omega^{n-1}] = F[\omega, a]$, so M is also a splitting field of f over F. By the Galois correspondence, for the fields $F \subseteq K \subseteq M$, we have $\text{Aut}_K M \trianglelefteq \text{Aut}_F M$ and $\text{Aut}_F M/\text{Aut}_K M \cong \text{Aut}_F K$. The tower of groups $\{I\} \leq \text{Aut}_K M \leq \text{Aut}_F M$ shows that $\text{Aut}_F M$ is solvable. Since L and M are both splitting fields for f over F, they are isomorphic, so L contains a primitive n^{th} root of unity and $\text{Aut}_F L$ is also solvable.

4.24 Theorem: *(Galois) Let F be a field with $\mathrm{char}(F) = 0$, let $f \in F[x]$, and let K be the splitting field of f over F. If f is solvable by radicals over F then $\mathrm{Aut}_F K$ is solvable.*

Proof: Suppose f is solvable by radicals over F. Let K be the splitting field of f over F, and say $K \subseteq F(a_1, a_2, \cdots, a_\ell)$ where ${a_k}^{n_k} \in F(a_1, \cdots, a_{k-1})$. Consider the case that $\ell = 1$. In this case we have $F \subseteq K \subseteq F(a_1)$ with ${a_1}^{n_1} \in F$. Let L be the splitting field over F of the polynomial $g(x) = x^{n_1} - {a_1}^{n_1}$. Then $F \subseteq K \subseteq F(a_1) \subseteq L$ and $\mathrm{Aut}_F L$ is solvable by the previous theorem. By the Galois correspondence, for the fields $F \subseteq K \subseteq L$, we have $\mathrm{Aut}_K L \trianglelefteq \mathrm{Aut}_F L$ and $\mathrm{Aut}_F L / \mathrm{Aut}_K L \cong \mathrm{Aut}_F K$. By Part 1 of Theorem 4.21 (which states that if $N \trianglelefteq G$ and G is solvable then G/N is solvable) $\mathrm{Aut}_F K$ is solvable.

Now consider the case that $\ell > 1$ and suppose, inductively, that the theorem holds for splitting fields contained in towers of length less than ℓ. Let L be the splitting field of $g(x) = x^{n_1} - {a_1}^{n_1}$ over F, and let M be the splitting field of $g(x)$ over K. Note that $F \subseteq K \subseteq M$ with M being the splitting field of $g(x)f(x)$ over F, and that $F \subseteq L \subseteq M$ with M being the splitting field of $f(x)$ over L. Since $a_1 \in L$ we have $F(a_1) \subseteq L$, and since f splits in $F(a_1, a_2, \cdots, a_\ell)$, it follows that f splits in $L(a_2, \cdots, a_\ell)$. By the induction hypothesis, we may suppose that $\mathrm{Aut}_L M$ is solvable. By the previous theorem, we also know that $\mathrm{Aut}_F L$ and $\mathrm{Aut}_K M$ are solvable.

Using the Galois correspondence for the fields $F \subseteq L \subseteq M$, we have $\mathrm{Aut}_L M \trianglelefteq \mathrm{Aut}_F M$ and $\mathrm{Aut}_F M / \mathrm{Aut}_L M \cong \mathrm{Aut}_F L$. By Part 2 of Theorem 4.21, it follows that $\mathrm{Aut}_F M$ is solvable. Using the Galois correspondence for the fields $F \subseteq K \subseteq M$, we have $\mathrm{Aut}_K M \trianglelefteq \mathrm{Aut}_F M$ and $\mathrm{Aut}_F M / \mathrm{Aut}_K M \cong \mathrm{Aut}_F K$. By Part 1 of Theorem 4.21, it follows that $\mathrm{Aut}_F K$ is solvable, as required.

4.25 Exercise: Let $f \in \mathbb{Q}[x]$ be an irreducible quintic polynomial with three distinct real roots and two conjugate complex roots. Let K be the splitting field of f over $\mathbb{Q}$. Show that $\mathrm{Aut}_{\mathbb{Q}} K \cong S_5$, and hence show that f is not solvable by radicals over $\mathbb{Q}$.