Modern Algebra

Chapter V. Fields and Galois Theory

V.4. The Galois Group of a Polynomial (Partial)—Proofs of Theorems

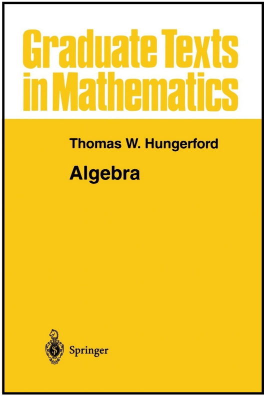

Table of contents

Theorem V.4.2

Theorem V.4.2. Let K be a field and $f \in K[x]$ a polynomial with Galois group G.

(i) G is isomorphic to a subgroup of some symmetric group S_n.

(ii) If irreducible f is separable of degree n, then n divides $|G|$ and G is isomorphic to a transitive subgroup of S_n.

Proof. (i) If $u_1, u_2, \ldots, u_n$ are the distinct roots of f in some splitting field F (so $1 \le n \le \deg(f)$) then Theorem V.2.2 implies that every $\sigma \in \mathrm{Aut}_K F$ induces a unique permutation of $\{u_1, u_2, \ldots, u_n\}$.

Theorem V.4.2

Theorem V.4.2. Let K be a field and $f \in K[x]$ a polynomial with Galois group G.

(i) G is isomorphic to a subgroup of some symmetric group S_n.

(ii) If irreducible f is separable of degree n, then n divides $|G|$ and G is isomorphic to a transitive subgroup of S_n.

Proof. (i) If $u_1, u_2, \ldots, u_n$ are the distinct roots of f in some splitting field F (so $1 \leq n \leq \deg(f)$) then Theorem V.2.2 implies that every $\sigma \in \mathrm{Aut}_K F$ induces a unique permutation of $\{u_1, u_2, \ldots, u_n\}$. Consider S_n as the group of all permutations of $\{u_1, u_2, \ldots, u_n\}$. For $\sigma \in \mathrm{Aut}_K F$, define the mapping $\mathrm{Aut}_K F \to S_n$ by mapping σ to the permutation it induces on $\{u_1, u_2, \ldots, u_n\}$, $\sigma \mapsto \sigma|_{\{u_1, u_2, \ldots, u_n\}}$. Then for $\sigma_1, \sigma_2 \in \mathrm{Aut}_K F$ we have $\sigma_1 \circ \sigma_2 \mapsto \sigma_1|_{\{u_1, u_2, \ldots, u_n\}} \circ \sigma_2|_{\{u_1, u_2, \ldots, u_n\}}$ and so the mapping is a homomorphism.

Theorem V.4.2

Theorem V.4.2. Let K be a field and $f \in K[x]$ a polynomial with Galois group G.

(i) G is isomorphic to a subgroup of some symmetric group S_n.

(ii) If irreducible f is separable of degree n, then n divides $|G|$ and G is isomorphic to a transitive subgroup of S_n.

Proof. (i) If $u_1, u_2, \ldots, u_n$ are the distinct roots of f in some splitting field F (so $1 \le n \le \deg(f)$) then Theorem V.2.2 implies that every $\sigma \in \mathrm{Aut}_K F$ induces a unique permutation of $\{u_1, u_2, \ldots, u_n\}$. Consider S_n as the group of all permutations of $\{u_1, u_2, \ldots, u_n\}$. For $\sigma \in \mathrm{Aut}_K F$, define the mapping $\mathrm{Aut}_K F \to S_n$ by mapping σ to the permutation it induces on $\{u_1, u_2, \ldots, u_n\}$, $\sigma \mapsto \sigma|_{\{u_1, u_2, \ldots, u_n\}}$. Then for $\sigma_1, \sigma_2 \in \mathrm{Aut}_K F$ we have $\sigma_1 \circ \sigma_2 \mapsto \sigma_1|_{\{u_1, u_2, \ldots, u_n\}} \circ \sigma_2|_{\{u_1, u_2, \ldots, u_n\}}$ and so the mapping is a homomorphism. Since F is the splitting field of f then $F = K(u_1, u_2, \ldots, u_n)$ (see Definition V.3.1). We now show the mapping is one to one. Let $\sigma_1, \sigma_2 \in \mathrm{Aut}_K E$ with $\sigma_1 \ne \sigma_2$. Then there is some $g \in F = K(u_1, u_2, \ldots, u_n)$ such that $\sigma_1(g) \ne \sigma_2(g)$.

Theorem V.4.2

Theorem V.4.2. Let K be a field and $f \in K[x]$ a polynomial with Galois group G.

(i) G is isomorphic to a subgroup of some symmetric group S_n.

(ii) If irreducible f is separable of degree n, then n divides $|G|$ and G is isomorphic to a transitive subgroup of S_n.

Proof. (i) If $u_1, u_2, \ldots, u_n$ are the distinct roots of f in some splitting field F (so $1 \leq n \leq \deg(f)$) then Theorem V.2.2 implies that every $\sigma \in \mathrm{Aut}_K F$ induces a unique permutation of $\{u_1, u_2, \ldots, u_n\}$. Consider S_n as the group of all permutations of $\{u_1, u_2, \ldots, u_n\}$. For $\sigma \in \mathrm{Aut}_K F$, define the mapping $\mathrm{Aut}_K F \to S_n$ by mapping σ to the permutation it induces on $\{u_1, u_2, \ldots, u_n\}$, $\sigma \mapsto \sigma|_{\{u_1, u_2, \ldots, u_n\}}$. Then for $\sigma_1, \sigma_2 \in \mathrm{Aut}_K F$ we have $\sigma_1 \circ \sigma_2 \mapsto \sigma_1|_{\{u_1, u_2, \ldots, u_n\}} \circ \sigma_2|_{\{u_1, u_2, \ldots, u_n\}}$ and so the mapping is a homomorphism. Since F is the splitting field of f then $F = K(u_1, u_2, \ldots, u_n)$ (see Definition V.3.1). We now show the mapping is one to one. Let $\sigma_1, \sigma_2 \in \mathrm{Aut}_K E$ with $\sigma_1 \neq \sigma_2$. Then there is some $g \in F = K(u_1, u_2, \ldots, u_n)$ such that $\sigma_1(g) \neq \sigma_2(g)$.

Theorem V.4.2(i)

Theorem V.4.2. Let K be a field and $f \in K[x]$ a polynomial with Galois group G.

(i) G is isomorphic to a subgroup of some symmetric group S_n.

Proof (continued). (i) By Theorem V.1.3(v), $g = h(u_1, u_2, \ldots, u_n)k(u_1, u_2, \ldots, u_n)^{-1}$ for some $h, k \in K[x_1, x_2, \ldots, x_n]$. Since σ_1 and σ_2 are homomorphisms which fix K elementwise, $\sigma_1(g) = h(\sigma_1(u_1), \sigma_1(u_2), \ldots, \sigma_1(u_n))k(\sigma_1(u_1), \sigma_1(u_1), \sigma_1(u_2), \ldots, \sigma_1(u_n))^{-1}$ and $\sigma_2(g) = h(\sigma_2(u_1), \sigma_2(u_2), \ldots, \sigma_2(u_n))k(\sigma_2(u_1), \sigma_2(u_1), \sigma_2(u_2), \ldots, \sigma_2(u_n))^{-1}$. Since $\sigma_1(g) \neq \sigma_2(g)$, then it must be that $\sigma_1|_{\{u_1,u_2,\ldots,u_n\}} \neq \sigma_2|_{\{u_1,u_2,\ldots,u_n\}}$. That is, the mapping $\sigma \mapsto \sigma|_{\{u_1,u_2,\ldots,u_n\}}$ is one to one and so is a monomorphism.

Theorem V.4.2(i)

Theorem V.4.2. Let K be a field and $f \in K[x]$ a polynomial with Galois group G.

(i) G is isomorphic to a subgroup of some symmetric group S_n.

Proof (continued). (i) By Theorem V.1.3(v),
$g = h(u_1, u_2, \ldots, u_n)k(u_1, u_2, \ldots, u_n)^{-1}$ for some $h, k \in K[x_1, x_2, \ldots, x_n]$.
Since σ_1 and σ_2 are homomorphisms which fix K elementwise, $\sigma_1(g) =$
$h(\sigma_1(u_1), \sigma_1(u_2), \ldots, \sigma_1(u_n))k(\sigma_1(u_1), \sigma_1(u_1), \sigma_1(u_2), \ldots, \sigma_1(u_n))^{-1}$ and
$\sigma_2(g) =$
$h(\sigma_2(u_1), \sigma_2(u_2), \ldots, \sigma_2(u_n))k(\sigma_2(u_1), \sigma_2(u_1), \sigma_2(u_2), \ldots, \sigma_2(u_n))^{-1}$.
Since $\sigma_1(g) \neq \sigma_2(g)$, then it must be that $\sigma_1|_{\{u_1,u_2,\ldots,u_n\}} \neq \sigma_2|_{\{u_1,u_2,\ldots,u_n\}}$.
That is, the mapping $\sigma \mapsto \sigma|_{\{u_1,u_2,\ldots,u_n\}}$ is one to one and so is a monomorphism. So this mapping is an isomorphism with its image. That is, $\mathrm{Aut}_K F$ is isomorphic to some subgroup of S_n.

Theorem V.4.2(i)

Theorem V.4.2. Let K be a field and $f \in K[x]$ a polynomial with Galois group G.

(i) G is isomorphic to a subgroup of some symmetric group S_n.

Proof (continued). (i) By Theorem V.1.3(v), $g = h(u_1, u_2, \ldots, u_n)k(u_1, u_2, \ldots, u_n)^{-1}$ for some $h, k \in K[x_1, x_2, \ldots, x_n]$. Since σ_1 and σ_2 are homomorphisms which fix K elementwise, $\sigma_1(g) = h(\sigma_1(u_1), \sigma_1(u_2), \ldots, \sigma_1(u_n))k(\sigma_1(u_1), \sigma_1(u_1), \sigma_1(u_2), \ldots, \sigma_1(u_n))^{-1}$ and $\sigma_2(g) = h(\sigma_2(u_1), \sigma_2(u_2), \ldots, \sigma_2(u_n))k(\sigma_2(u_1), \sigma_2(u_1), \sigma_2(u_2), \ldots, \sigma_2(u_n))^{-1}$. Since $\sigma_1(g) \neq \sigma_2(g)$, then it must be that $\sigma_1|_{\{u_1,u_2,\ldots,u_n\}} \neq \sigma_2|_{\{u_1,u_2,\ldots,u_n\}}$. That is, the mapping $\sigma \mapsto \sigma|_{\{u_1,u_2,\ldots,u_n\}}$ is one to one and so is a monomorphism. So this mapping is an isomorphism with its image. That is, $\text{Aut}_K F$ is isomorphic to some subgroup of S_n.

Theorem V.4.2(ii)

Theorem V.4.2. Let K be a field and $f \in K[x]$ a polynomial with Galois group G.

(ii) If irreducible f is separable of degree n, then n divides $|G|$ and G is isomorphic to a transitive subgroup of S_n.

Proof. (ii) The splitting field F of $f \in K[x]$ is Galois over K by Theorem V.3.11 (the (iii)$\Rightarrow$(i) part). By Theorem V.1.6(ii) and (iii), $[K(u_1) : K] = n = \deg(f)$. By the Fundamental Theorem of Galois Theory (Theorem V.2.5(i)) Galois group $G = \mathrm{Aut}_K F$ has a subgroup of index $n = [K(u_1) : K]$ (since the subgroups and intermediate fields, such as $K(u_1)$, are in one to one correspondence with the same dimension/index). Whence by Theorem V.1.2, $|G| = |\mathrm{Aut}_K(F)| = [F : K] = [F : K(u_1)][K(u_1) : K] = [F : K(u_1)]n$ and so n divides $|G|$. By Corollary V.1.9, for any $i \neq j$, there is a K-isomorphism $\sigma : K(u_i) \cong K(u_j)$ such that $\sigma(u_i) = u_j$.

Theorem V.4.2(ii)

Theorem V.4.2. Let K be a field and $f \in K[x]$ a polynomial with Galois group G.

(ii) If irreducible f is separable of degree n, then n divides $|G|$ and G is isomorphic to a transitive subgroup of S_n.

Proof. (ii) The splitting field F of $f \in K[x]$ is Galois over K by Theorem V.3.11 (the (iii)⇒(i) part). By Theorem V.1.6(ii) and (iii), $[K(u_1) : K] = n = \deg(f)$. By the Fundamental Theorem of Galois Theory (Theorem V.2.5(i)) Galois group $G = \mathrm{Aut}_K F$ has a subgroup of index $n = [K(u_1) : K]$ (since the subgroups and intermediate fields, such as $K(u_1)$, are in one to one correspondence with the same dimension/index). Whence by Theorem V.1.2, $|G| = |\mathrm{Aut}_K(F)| = [F : K] = [F : K(u_1)][K(u_1) : K] = [F : K(u_1)]n$ and so n divides $|G|$. By Corollary V.1.9, for any $i \neq j$, there is a K-isomorphism $\sigma : K(u_i) \cong K(u_j)$ such that $\sigma(u_i) = u_j$.

Theorem V.4.2(ii) (continued)

Theorem V.4.2. Let K be a field and $f \in K[x]$ a polynomial with Galois group G.

(ii) If irreducible f is separable of degree n, then n divides $|G|$ and G is isomorphic to a transitive subgroup of S_n.

Proof (continued). (ii) By Theorem V.3.8, σ extends to a K-automorphism of F; that is, the extended σ is in $\text{Aut}_K F$ and so using the mapping defined in part (i) (which sends the extended σ to the extended σ restricted to $\{u_1, u_2, \ldots, u_n\}$) G is isomorphic to a subgroup of S_n which sends u_i to u_j (recall that we are treating S_n as a permutation on $\{u_1, u_2, \ldots, u_n\}$). That is, G is isomorphic to a transitive subgroup of S_n. □

Theorem V.4.2(ii) (continued)

Theorem V.4.2. Let K be a field and $f \in K[x]$ a polynomial with Galois group G.

(ii) If irreducible f is separable of degree n, then n divides $|G|$ and G is isomorphic to a transitive subgroup of S_n.

Proof (continued). (ii) By Theorem V.3.8, σ extends to a K-automorphism of F; that is, the extended σ is in $\text{Aut}_K F$ and so using the mapping defined in part (i) (which sends the extended σ to the extended σ restricted to $\{u_1, u_2, \ldots, u_n\}$) G is isomorphic to a subgroup of S_n which sends u_i to u_j (recall that we are treating S_n as a permutation on $\{u_1, u_2, \ldots, u_n\}$). That is, G is isomorphic to a transitive subgroup of S_n. □

Theorem V.4.12

Theorem V.4.12. If p is prime and f is an irreducible polynomial of degree p over the field of rational numbers $\mathbb{Q}$ which has precisely two nonreal roots in the field of complex numbers $\mathbb{C}$ and $p-2$ real roots, then the Galois group of f is isomorphic to S_p.

Proof. Let G be the Galois group of f considered as a subgroup of S_p, as described in the note following Theorem V.4.2. By Theorem V.4.2(ii) (notice that f is separable), p divides $|G|$. By Cauchy's Theorem (Theorem II.5.2) G contains an element σ of order p.

Theorem V.4.12

Theorem V.4.12. If p is prime and f is an irreducible polynomial of degree p over the field of rational numbers $\mathbb{Q}$ which has precisely two nonreal roots in the field of complex numbers $\mathbb{C}$ and $p-2$ real roots, then the Galois group of f is isomorphic to S_p.

Proof. Let G be the Galois group of f considered as a subgroup of S_p, as described in the note following Theorem V.4.2. By Theorem V.4.2(ii) (notice that f is separable), p divides $|G|$. By Cauchy's Theorem (Theorem II.5.2) G contains an element σ of order p. By Corollary I.6.4, σ is a p-cycle. Now complex conjugation, $a + bi \mapsto a - bi$, is an $\mathbb{R}$-automorphism of $\mathbb{C}$ that moves every nonreal element of $\mathbb{C}$.

Theorem V.4.12

Theorem V.4.12. If p is prime and f is an irreducible polynomial of degree p over the field of rational numbers $\mathbb{Q}$ which has precisely two nonreal roots in the field of complex numbers $\mathbb{C}$ and $p-2$ real roots, then the Galois group of f is isomorphic to S_p.

Proof. Let G be the Galois group of f considered as a subgroup of S_p, as described in the note following Theorem V.4.2. By Theorem V.4.2(ii) (notice that f is separable), p divides $|G|$. By Cauchy's Theorem (Theorem II.5.2) G contains an element σ of order p. By Corollary I.6.4, σ is a p-cycle. Now complex conjugation, $a+bi \mapsto a-bi$, is an $\mathbb{R}$-automorphism of $\mathbb{C}$ that moves every nonreal element of $\mathbb{C}$. Then by Theorem V.2.2, it interchanges the two nonreal roots of f and fixes the other (real) roots. So G contains a transposition, say $\tau = (c,d)$ where c and d are the complex roots of f.

Theorem V.4.12

Theorem V.4.12. If p is prime and f is an irreducible polynomial of degree p over the field of rational numbers $\mathbb{Q}$ which has precisely two nonreal roots in the field of complex numbers $\mathbb{C}$ and $p-2$ real roots, then the Galois group of f is isomorphic to S_p.

Proof. Let G be the Galois group of f considered as a subgroup of S_p, as described in the note following Theorem V.4.2. By Theorem V.4.2(ii) (notice that f is separable), p divides $|G|$. By Cauchy's Theorem (Theorem II.5.2) G contains an element σ of order p. By Corollary I.6.4, σ is a p-cycle. Now complex conjugation, $a+bi \mapsto a-bi$, is an $\mathbb{R}$-automorphism of $\mathbb{C}$ that moves every nonreal element of $\mathbb{C}$. Then by Theorem V.2.2, it interchanges the two nonreal roots of f and fixes the other (real) roots. So G contains a transposition, say $\tau = (c, d)$ where c and d are the complex roots of f.

Theorem V.4.12 (continued)

Theorem V.4.12. If p is prime and f is an irreducible polynomial of degree p over the field of rational numbers $\mathbb{Q}$ which has precisely two nonreal roots in the field of complex numbers $\mathbb{C}$ and $p-2$ real roots, then the Galois group of f is isomorphic to S_p.

Proof (continued). Since p-cycle σ can be written $\sigma = (c, j_2, j_3, \ldots, j_p)$ (whence the roots of f are $c, j_2, j_3, \ldots, j_p$; notice that one of the j_i's must be equal to d), then some power of σ maps c to d (the power $k = i-1$ if $d = j_i$) and so for some k, $\sigma^k = (c, d, i_3, i_4, \ldots, i_p) \in G$. By changing notation of the set being permuted, denote $\tau = (1, 2)$ and $\sigma^k = (1, 2, 3, \ldots, p)$. By Exercise I.6.4 these two elements of S_p generate S_p. Since G is isomorphic to a subgroup of S_p by Theorem V.4.2 and G contains these two elements, then $G = S_p$ □

Theorem V.4.12 (continued)

Theorem V.4.12. If p is prime and f is an irreducible polynomial of degree p over the field of rational numbers $\mathbb{Q}$ which has precisely two nonreal roots in the field of complex numbers $\mathbb{C}$ and $p-2$ real roots, then the Galois group of f is isomorphic to S_p.

Proof (continued). Since p-cycle σ can be written $\sigma = (c, j_2, j_3, \ldots, j_p)$ (whence the roots of f are $c, j_2, j_3, \ldots, j_p$; notice that one of the j_i's must be equal to d), then some power of σ maps c to d (the power $k = i-1$ if $d = j_i$) and so for some k, $\sigma^k = (c, d, i_3, i_4, \ldots, i_p) \in G$. By changing notation of the set being permuted, denote $\tau = (1, 2)$ and $\sigma^k = (1, 2, 3, \ldots, p)$. By Exercise I.6.4 these two elements of S_p generate S_p. Since G is isomorphic to a subgroup of S_p by Theorem V.4.2 and G contains these two elements, then $G = S_p$ □