Modern Algebra

Chapter V. Fields and Galois Theory

V.9.Appendix. The General Equation of Degree *n*—Proofs of Theorems

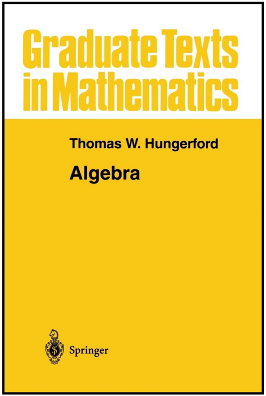

Table of contents

Proposition V.9.8

Proposition V.9.8. Abel's Theorem. Let K be a field and $n \in \mathbb{N}$. The general equation of degree n is solvable by radicals only if $n \leq 4$.

Proof. Let $p_n(x) \in K(t_1, t_2, \ldots, t_n)$ be the general polynomial of degree n over K. Let $u_1, u_2, \ldots, u_n$ be the roots of $p_n(x)$ is some splitting field $F = K(t_1, t_2, \ldots, t_n)(u_1, u_2, \ldots, u_n)$. In F, $p_n(x) = (x - u_1)(x - u_2) \cdots (x - u_n)$ and so the coefficients of $p_n(x)$ satisfy

Proposition V.9.8

Proposition V.9.8. Abel's Theorem. Let K be a field and $n \in \mathbb{N}$. The general equation of degree n is solvable by radicals only if $n \leq 4$.

Proof. Let $p_n(x) \in K(t_1, t_2, \ldots, t_n)$ be the general polynomial of degree n over K. Let $u_1, u_2, \ldots, u_n$ be the roots of $p_n(x)$ is some splitting field $F = K(t_1, t_2, \ldots, t_n)(u_1, u_2, \ldots, u_n)$. In F, $p_n(x) = (x - u_1)(x - u_2) \cdots (x - u_n)$ and so the coefficients of $p_n(x)$ satisfy

$$\begin{aligned} t_1 &= \sum_{i=1}^{n} u_i \\ t_2 &= \sum_{1 \leq i \leq j \leq n} u_i u_j \\ t_3 &= \sum_{1 \leq i \leq j \leq k \leq n} u_i u_j u_k \\ &\vdots \end{aligned}$$

Proposition V.9.8

Proposition V.9.8. Abel's Theorem. Let K be a field and $n \in \mathbb{N}$. The general equation of degree n is solvable by radicals only if $n \leq 4$.

Proof. Let $p_n(x) \in K(t_1, t_2, \ldots, t_n)$ be the general polynomial of degree n over K. Let $u_1, u_2, \ldots, u_n$ be the roots of $p_n(x)$ is some splitting field $F = K(t_1, t_2, \ldots, t_n)(u_1, u_2, \ldots, u_n)$. In F, $p_n(x) = (x - u_1)(x - u_2) \cdots (x - u_n)$ and so the coefficients of $p_n(x)$ satisfy

$$\begin{aligned} t_1 &= \sum_{i=1}^{n} u_i \\ t_2 &= \sum_{1 \leq i \leq j \leq n} u_i u_j \\ t_3 &= \sum_{1 \leq i \leq j \leq k \leq n} u_i u_j u_k \\ &\vdots \end{aligned}$$

Proposition V.9.8 (continued 1)

Proof (continued).

$$\begin{aligned} &\vdots \\ t_k &= \sum_{1 \le i_1 \le i_2 \le \cdots \le i_k \le n} u_{i_1} u_{i_2} \cdots u_{i_k} \\ &\vdots \\ t_n &= u_1 u_2 \cdots u_n. \end{aligned}$$

(this is why the powers of -1 are included in the definition of the general polynomial). That is, $t_i = f_i(u_1, u_2, \ldots, u_n)$ where f_i is the ith elementary symmetric function in n indeterminates (see the appendix to Section V.2). So a field containing each root $u_1, u_2, \ldots, u_n$ of $p_n(x)$ must also contain each $t_1, t_2, \ldots, t_n$. That is, $F = K(u_1, u_2, \ldots, u_n)$. Now consider the indeterminates $\{x_1, x_2, \ldots, x_n\}$ and the field of rational functions $K(x_1, x_2, \ldots, x_n)$.

Proposition V.9.8 (continued 1)

Proof (continued).

$$\begin{aligned} &\vdots \\ t_k &= \sum_{1 \le i_1 \le i_2 \le \cdots \le i_k \le n} u_{i_1} u_{i_2} \cdots u_{i_k} \\ &\vdots \\ t_n &= u_1 u_2 \cdots u_n. \end{aligned}$$

(this is why the powers of -1 are included in the definition of the general polynomial). That is, $t_i = f_i(u_1, u_2, \ldots, u_n)$ where f_i is the ith elementary symmetric function in n indeterminates (see the appendix to Section V.2). So a field containing each root $u_1, u_2, \ldots, u_n$ of $p_n(x)$ must also contain each $t_1, t_2, \ldots, t_n$. That is, $F = K(u_1, u_2, \ldots, u_n)$. Now consider the indeterminates $\{x_1, x_2, \ldots, x_n\}$ and the field of rational functions $K(x_1, x_2, \ldots, x_n)$.

Proposition V.9.8 (continued 2)

Proof (continued). Let E be the subfield of $K(x_1, x_2, \ldots, x_n)$ consisting of all symmetric rational functions in $K(x_1, x_2, \ldots, x_n)$ (that is, the rational functions fixed by any permutation of the indeterminates).

The basic idea of the proof is to construct an isomorphism θ mapping F to $K(x_1, x_2, \ldots, x_n)$ such that $K(t_1, t_2, \ldots, t_n)$ is mapped onto E. Then the Galois group of $p_n(x)$, $\text{Aut}_{K(t_1,t_2,\ldots,t_n)}F$ would be isomorphic to $\text{Aut}_E K(x_1, x_2, \ldots, x_n)$.

Proposition V.9.8 (continued 2)

Proof (continued). Let E be the subfield of $K(x_1, x_2, \ldots, x_n)$ consisting of all symmetric rational functions in $K(x_1, x_2, \ldots, x_n)$ (that is, the rational functions fixed by any permutation of the indeterminates).

The basic idea of the proof is to construct an isomorphism θ mapping F to $K(x_1, x_2, \ldots, x_n)$ such that $K(t_1, t_2, \ldots, t_n)$ is mapped onto E. Then the Galois group of $p_n(x)$, $\text{Aut}_{K(t_1,t_2,\ldots,t_n)}F$ would be isomorphic to $\text{Aut}_E K(x_1, x_2, \ldots, x_n)$. By the "Observation" in the notes on the Appendix to Section V.2 (see page 253 of Hungerford) $K(x_1, x_2, \ldots, x_n)$ is a Galois extension of E with Galois group S_n. S_n is solvable if and only if $n \leq 4$ by Corollary II.7.12 and Exercise II.7.10.

Proposition V.9.8 (continued 2)

Proof (continued). Let E be the subfield of $K(x_1, x_2, \ldots, x_n)$ consisting of all symmetric rational functions in $K(x_1, x_2, \ldots, x_n)$ (that is, the rational functions fixed by any permutation of the indeterminates).

The basic idea of the proof is to construct an isomorphism θ mapping F to $K(x_1, x_2, \ldots, x_n)$ such that $K(t_1, t_2, \ldots, t_n)$ is mapped onto E. Then the Galois group of $p_n(x)$, $\mathrm{Aut}_{K(t_1,t_2,\ldots,t_n)}F$ would be isomorphic to $\mathrm{Aut}_E K(x_1, x_2, \ldots, x_n)$. By the "Observation" in the notes on the Appendix to Section V.2 (see page 253 of Hungerford) $K(x_1, x_2, \ldots, x_n)$ is a Galois extension of E with Galois group S_n. S_n is solvable if and only if $n \leq 4$ by Corollary II.7.12 and Exercise II.7.10. Therefore, if $p_n(x) = 0$ is solvable by radicals then $n \leq 4$ by Corollary V.9.5.

Proposition V.9.8 (continued 2)

Proof (continued). Let E be the subfield of $K(x_1, x_2, \ldots, x_n)$ consisting of all symmetric rational functions in $K(x_1, x_2, \ldots, x_n)$ (that is, the rational functions fixed by any permutation of the indeterminates).

The basic idea of the proof is to construct an isomorphism θ mapping F to $K(x_1, x_2, \ldots, x_n)$ such that $K(t_1, t_2, \ldots, t_n)$ is mapped onto E. Then the Galois group of $p_n(x)$, $\text{Aut}_{K(t_1,t_2,\ldots,t_n)}F$ would be isomorphic to $\text{Aut}_E K(x_1, x_2, \ldots, x_n)$. By the "Observation" in the notes on the Appendix to Section V.2 (see page 253 of Hungerford) $K(x_1, x_2, \ldots, x_n)$ is a Galois extension of E with Galois group S_n. S_n is solvable if and only if $n \leq 4$ by Corollary II.7.12 and Exercise II.7.10. Therefore, if $p_n(x) = 0$ is solvable by radicals then $n \leq 4$ by Corollary V.9.5.

Proposition V.9.8 (continued 3)

Proof (continued). We now construct the isomorphism discussed in the previous paragraph. By Theorem V.2.18, $E = K(f_1, f_2, \ldots, f_n)$. Consider the mapping of $K[t_1, t_2, \ldots, t_n]$ to $K[f_1, f_2, \ldots, f_n]$ based on the assignment of $g(t_1, t_2, \ldots, t_n) \mapsto g(f_1, f_2, \ldots, f_n)$ for each polynomial $g \in K[x_1, x_2, \ldots, x_n]$. By Theorem III.5.5 this mapping defines a ring homomorphism. "Clearly" this homomorphism is onto (consider the constant polynomials and the fact that $t_i \mapsto f_i$ when considering polynomial $g(x_1, x_2, \ldots, x_n) = x_i$). So the homomorphism is an epimorphism of rings, say θ mapping $K[t_1, t_2, \ldots, t_n]$ to $K[f_1, f_2, \ldots, f_n]$. Suppose $\theta(g(t_1, t_2, \ldots, t_n)) = g(f_1, f_2, \ldots, f_n) = 0$ for some polynomial g.

Proposition V.9.8 (continued 3)

Proof (continued). We now construct the isomorphism discussed in the previous paragraph. By Theorem V.2.18, $E = K(f_1, f_2, \ldots, f_n)$. Consider the mapping of $K[t_1, t_2, \ldots, t_n]$ to $K[f_1, f_2, \ldots, f_n]$ based on the assignment of $g(t_1, t_2, \ldots, t_n) \mapsto g(f_1, f_2, \ldots, f_n)$ for each polynomial $g \in K[x_1, x_2, \ldots, x_n]$. By Theorem III.5.5 this mapping defines a ring homomorphism. "Clearly" this homomorphism is onto (consider the constant polynomials and the fact that $t_i \mapsto f_i$ when considering polynomial $g(x_1, x_2, \ldots, x_n) = x_i$). So the homomorphism is an epimorphism of rings, say θ mapping $K[t_1, t_2, \ldots, t_n]$ to $K[f_1, f_2, \ldots, f_n]$. Suppose $\theta(g(t_1, t_2, \ldots, t_n)) = g(f_1, f_2, \ldots, f_n) = 0$ for some polynomial g. By definition $f_k = f_k(x_1, x_2, \ldots, x_n) = \sum_{1 \le i_1 < i_2 < \cdots < i_k \le n} x_{i_1} x_{i_2} \cdots x_{i_k}$ and hence $0 = g(f_1, f_2, \ldots, f_n) = g(g_1(x_1, x_2, \ldots, x_n), \ldots, f_n(x_1, x_2, \ldots, x_n))$. Since $g(f_1, f_2, \ldots, f_n)$ is a polynomial (since g is a polynomial and each f_i is a polynomial) in the indeterminates $x_1, x_2, \ldots, x_n$ over K.

Proposition V.9.8 (continued 3)

Proof (continued). We now construct the isomorphism discussed in the previous paragraph. By Theorem V.2.18, $E = K(f_1, f_2, \ldots, f_n)$. Consider the mapping of $K[t_1, t_2, \ldots, t_n]$ to $K[f_1, f_2, \ldots, f_n]$ based on the assignment of $g(t_1, t_2, \ldots, t_n) \mapsto g(f_1, f_2, \ldots, f_n)$ for each polynomial $g \in K[x_1, x_2, \ldots, x_n]$. By Theorem III.5.5 this mapping defines a ring homomorphism. "Clearly" this homomorphism is onto (consider the constant polynomials and the fact that $t_i \mapsto f_i$ when considering polynomial $g(x_1, x_2, \ldots, x_n) = x_i$). So the homomorphism is an epimorphism of rings, say θ mapping $K[t_1, t_2, \ldots, t_n]$ to $K[f_1, f_2, \ldots, f_n]$. Suppose $\theta(g(t_1, t_2, \ldots, t_n)) = g(f_1, f_2, \ldots, f_n) = 0$ for some polynomial g. By definition $f_k = f_k(x_1, x_2, \ldots, x_n) = \sum_{1 \le i_1 < i_2 < \cdots < i_k \le n} x_{i_1} x_{i_2} \cdots x_{i_k}$ and hence $0 = g(f_1, f_2, \ldots, f_n) = g(g_1(x_1, x_2, \ldots, x_n), \ldots, f_n(x_1, x_2, \ldots, x_n))$. Since $g(f_1, f_2, \ldots, f_n)$ is a polynomial (since g is a polynomial and each f_i is a polynomial) in the indeterminates $x_1, x_2, \ldots, x_n$ over K.

Proposition V.9.8 (continued 4)

Proof (continued). Now $F = K(u_1, u_2, \ldots, u_n)$ is a field containing K so if we substitute u_i for x_i then we get (in $K(u_1, u_2, \ldots, u_n)$) that $0 = g(f_1(u_1, u_2, \ldots, u_n), f_2(u_1, u_2, \ldots, u_n), \ldots, f_n(u_1, u_2, \ldots, u_n)) = g(t_1, t_2, \ldots, t_n)$ (by the definition of t_i). So $\mathrm{Ker}(\theta) = \{0\}$ and by Theorem I.2.3(i), θ is one to one. Therefore θ is an isomorphism. Furthermore, by Exercise III.4.7, θ extends to an isomorphism of fields of quotients mapping $K(t_1, t_2, \ldots, t_n)$ to $K(f_1, f_2, \ldots, f_n) = E$.

Proposition V.9.8 (continued 4)

Proof (continued). Now $F = K(u_1, u_2, \ldots, u_n)$ is a field containing K so if we substitute u_i for x_i then we get (in $K(u_1, u_2, \ldots, u_n)$) that $0 = g(f_1(u_1, u_2, \ldots, u_n), f_2(u_1, u_2, \ldots, u_n), \ldots, f_n(u_1, u_2, \ldots, u_n)) = g(t_1, t_2, \ldots, t_n)$ (by the definition of t_i). So $\mathrm{Ker}(\theta) = \{0\}$ and by Theorem I.2.3(i), θ is one to one. Therefore θ is an isomorphism. Furthermore, by Exercise III.4.7, θ extends to an isomorphism of fields of quotients mapping $K(t_1, t_2, \ldots, t_n)$ to $K(f_1, f_2, \ldots, f_n) = E$.

Now $F = K(a_1, u_2, \ldots, u_n)$ is a splitting field over $K(t_1, t_2, \ldots, t_n)$ of $p_n(x)$, and θ induces a mapping of $p_n(x) \in K(t_1, t_2, \ldots, t_n)[x]$ to $\overline{p}_n(x) \in K(f_1, f_2, \ldots, f_n)[x] = E[x]$ acting as $p_n(x) = x^n - t_1x^{n-1} + t_2x^{n-2} - \cdots + (-1)^{n-1}t_{n-1}x + (-1)^n t_n \mapsto x^n - f_1x^{n-1} + f_2x^{n-2} + \cdots + (-1)^{n-1}f_{n-1}x + (-1)^n f_n = \overline{p}_n(x)$.

Proposition V.9.8 (continued 4)

Proof (continued). Now $F = K(u_1, u_2, \ldots, u_n)$ is a field containing K so if we substitute u_i for x_i then we get (in $K(u_1, u_2, \ldots, u_n)$) that $0 = g(f_1(u_1, u_2, \ldots, u_n), f_2(u_1, u_2, \ldots, u_n), \ldots, f_n(u_1, u_2, \ldots, u_n)) = g(t_1, t_2, \ldots, t_n)$ (by the definition of t_i). So $\mathrm{Ker}(\theta) = \{0\}$ and by Theorem I.2.3(i), θ is one to one. Therefore θ is an isomorphism. Furthermore, by Exercise III.4.7, θ extends to an isomorphism of fields of quotients mapping $K(t_1, t_2, \ldots, t_n)$ to $K(f_1, f_2, \ldots, f_n) = E$.

Now $F = K(a_1, u_2, \ldots, u_n)$ is a splitting field over $K(t_1, t_2, \ldots, t_n)$ of $p_n(x)$, and θ induces a mapping of $p_n(x) \in K(t_1, t_2, \ldots, t_n)[x]$ to $\overline{p}_n(x) \in K(f_1, f_2, \ldots, f_n)[x] = E[x]$ acting as $p_n(x) = x^n - t_1x^{n-1} + t_2x^{n-2} - \cdots + (-1)^{n-1}t_{n-1}x + (-1)^n t_n \mapsto x^n - f_1x^{n-1} + f_2x^{n-2} + \cdots + (-1)^{n-1}f_{n-1}x + (-1)^n f_n = \overline{p}_n(x)$. Since the f_i are the elementary symmetric functions in x indeterminates (say $x_1, x_2, \ldots, x_n$), then $\overline{p}_n(x)$ factors as $\overline{p}_n(x) = (x - x_1)(x - x_2)\cdots(x - x_n)$ (multiply this expression out to confirm that it gives the elementary symmetric functions defined in the Appendix to Section V.2).

Proposition V.9.8 (continued 4)

Proof (continued). Now $F = K(u_1, u_2, \ldots, u_n)$ is a field containing K so if we substitute u_i for x_i then we get (in $K(u_1, u_2, \ldots, u_n)$) that $0 = g(f_1(u_1, u_2, \ldots, u_n), f_2(u_1, u_2, \ldots, u_n), \ldots, f_n(u_1, u_2, \ldots, u_n)) = g(t_1, t_2, \ldots, t_n)$ (by the definition of t_i). So $\text{Ker}(\theta) = \{0\}$ and by Theorem I.2.3(i), θ is one to one. Therefore θ is an isomorphism. Furthermore, by Exercise III.4.7, θ extends to an isomorphism of fields of quotients mapping $K(t_1, t_2, \ldots, t_n)$ to $K(f_1, f_2, \ldots, f_n) = E$.

Now $F = K(a_1, u_2, \ldots, u_n)$ is a splitting field over $K(t_1, t_2, \ldots, t_n)$ of $p_n(x)$, and θ induces a mapping of $p_n(x) \in K(t_1, t_2, \ldots, t_n)[x]$ to $\overline{p}_n(x) \in K(f_1, f_2, \ldots, f_n)[x] = E[x]$ acting as $p_n(x) = x^n - t_1 x^{n-1} + t_2 x^{n-2} - \cdots + (-1)^{n-1} t_{n-1} x + (-1)^n t_n \mapsto x^n - f_1 x^{n-1} + f_2 x^{n-2} + \cdots + (-1)^{n-1} f_{n-1} x + (-1)^n f_n = \overline{p}_n(x)$. Since the f_i are the elementary symmetric functions in x indeterminates (say $x_1, x_2, \ldots, x_n$), then $\overline{p}_n(x)$ factors as $\overline{p}_n(x) = (x - x_1)(x - x_2) \cdots (x - x_n)$ (multiply this expression out to confirm that it gives the elementary symmetric functions defined in the Appendix to Section V.2).

Proposition V.9.8 (continued 5)

Proposition V.9.8. Let K be a field and $n \in \mathbb{N}$. The general equation of degree n is solvable by radicals only if $n \leq 4$.

Proof (continued). Therefore, $K(x_1, x_2, \ldots, x_n)$ is a splitting field of $\overline{p}_n(x)$ over $K(f_1, f_2, \ldots, f_n) = E$. At this stage we have isomorphism $\theta : K(t_1, t_2, \ldots, t_n) \to K(f_1, f_2, \ldots, f_n) = E$. By Theorem V.3.8, θ extends to an isomorphism mapping $F = K(t_1, t_2, \ldots, t_n)(u_1, u_2, \ldots, u_n) = K(u_1, u_2, \ldots, u_n)$ onto $K(x_1, x_2, \ldots, x_n)$.

Proposition V.9.8 (continued 5)

Proposition V.9.8. Let K be a field and $n \in \mathbb{N}$. The general equation of degree n is solvable by radicals only if $n \leq 4$.

Proof (continued). Therefore, $K(x_1, x_2, \ldots, x_n)$ is a splitting field of $\overline{p}_n(x)$ over $K(f_1, f_2, \ldots, f_n) = E$. At this stage we have isomorphism $\theta : K(t_1, t_2, \ldots, t_n) \to K(f_1, f_2, \ldots, f_n) = E$. By Theorem V.3.8, θ extends to an isomorphism mapping
$F = K(t_1, t_2, \ldots, t_n)(u_1, u_2, \ldots, u_n) = K(u_1, u_2, \ldots, u_n)$ onto $K(x_1, x_2, \ldots, x_n)$. So this extension (which we still denote θ) maps F onto $K(x_1, x_2, \ldots, x_n)$ and maps $K(t_1, t_2, \ldots, t_n)$ onto E; θ is the desired isomorphism and the result follows as explained above. □

Proposition V.9.8 (continued 5)

Proposition V.9.8. Let K be a field and $n \in \mathbb{N}$. The general equation of degree n is solvable by radicals only if $n \leq 4$.

Proof (continued). Therefore, $K(x_1, x_2, \ldots, x_n)$ is a splitting field of $\overline{p}_n(x)$ over $K(f_1, f_2, \ldots, f_n) = E$. At this stage we have isomorphism $\theta : K(t_1, t_2, \ldots, t_n) \to K(f_1, f_2, \ldots, f_n) = E$. By Theorem V.3.8, θ extends to an isomorphism mapping
$F = K(t_1, t_2, \ldots, t_n)(u_1, u_2, \ldots, u_n) = K(u_1, u_2, \ldots, u_n)$ onto $K(x_1, x_2, \ldots, x_n)$. So this extension (which we still denote θ) maps F onto $K(x_1, x_2, \ldots, x_n)$ and maps $K(t_1, t_2, \ldots, t_n)$ onto E; θ is the desired isomorphism and the result follows as explained above. □