Modern Algebra

Chapter V. Fields and Galois Theory

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

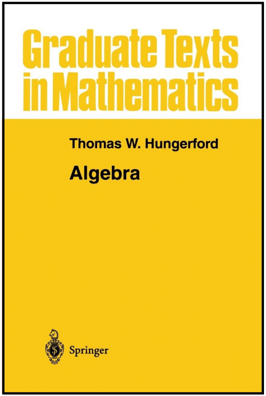

Table of contents

Corollary V.4.3

Corollary V.4.3. The Galois Group of Degree 3 Polynomials.
Let K be a field and $f \in K[x]$ an irreducible polynomial of degree 2 with Galois group G. If f is separable (as is always the case when $\text{char}(K) \neq 2$), then $G \cong \mathbb{Z}_2$; otherwise $G = \{\iota\} = 1$.

Proof. By Theorem V.4.2(ii), if f is separable of degree 2 then G is isomorphic to a transitive subgroup of $S_2 \cong \mathbb{Z}_2$. But the only transitive subgroup of $\mathbb{Z}_2$ is $\mathbb{Z}_2$ itself, so $G \cong \mathbb{Z}_2$.

Corollary V.4.3

Corollary V.4.3. The Galois Group of Degree 3 Polynomials.
Let K be a field and $f \in K[x]$ an irreducible polynomial of degree 2 with Galois group G. If f is separable (as is always the case when $\text{char}(K) \neq 2$), then $G \cong \mathbb{Z}_2$; otherwise $G = \{\iota\} = 1$.

Proof. By Theorem V.4.2(ii), if f is separable of degree 2 then G is isomorphic to a transitive subgroup of $S_2 \cong \mathbb{Z}_2$. But the only transitive subgroup of $\mathbb{Z}_2$ is $\mathbb{Z}_2$ itself, so $G \cong \mathbb{Z}_2$.

If f is not separable, then in a splitting field F of f we have $f(x) = (x - a)^2 \in F[x]$ and for $\sigma \in G - \text{Aut}_K F$ we must have $\sigma(a) = a$ by Theorem V.2.2 and so σ fixes $F = K(a)$. That is, in this case $G = \{\iota\}$.

Corollary V.4.3

Corollary V.4.3. The Galois Group of Degree 3 Polynomials.
Let K be a field and $f \in K[x]$ an irreducible polynomial of degree 2 with Galois group G. If f is separable (as is always the case when $\text{char}(K) \neq 2$), then $G \cong \mathbb{Z}_2$; otherwise $G = \{\iota\} = 1$.

Proof. By Theorem V.4.2(ii), if f is separable of degree 2 then G is isomorphic to a transitive subgroup of $S_2 \cong \mathbb{Z}_2$. But the only transitive subgroup of $\mathbb{Z}_2$ is $\mathbb{Z}_2$ itself, so $G \cong \mathbb{Z}_2$.

If f is not separable, then in a splitting field F of f we have $f(x) = (x - a)^2 \in F[x]$ and for $\sigma \in G - \text{Aut}_K F$ we must have $\sigma(a) = a$ by Theorem V.2.2 and so σ fixes $F = K(a)$. That is, in this case $G = \{\iota\}$.

Finally, suppose $\text{char}(K) \neq 2$ and let $f \in K[x]$ be a degree 2 polynomial. Then $f' \neq 0$; that is, f' is not the zero polynomial in $K[x]$ (since f' is a degree 1 polynomial).

Corollary V.4.3

Corollary V.4.3. The Galois Group of Degree 3 Polynomials.
Let K be a field and $f \in K[x]$ an irreducible polynomial of degree 2 with Galois group G. If f is separable (as is always the case when $\text{char}(K) \neq 2$), then $G \cong \mathbb{Z}_2$; otherwise $G = \{\iota\} = 1$.

Proof. By Theorem V.4.2(ii), if f is separable of degree 2 then G is isomorphic to a transitive subgroup of $S_2 \cong \mathbb{Z}_2$. But the only transitive subgroup of $\mathbb{Z}_2$ is $\mathbb{Z}_2$ itself, so $G \cong \mathbb{Z}_2$.

If f is not separable, then in a splitting field F of f we have $f(x) = (x-a)^2 \in F[x]$ and for $\sigma \in G - \text{Aut}_K F$ we must have $\sigma(a) = a$ by Theorem V.2.2 and so σ fixes $F = K(a)$. That is, in this case $G = \{\iota\}$.

Finally, suppose $\text{char}(K) \neq 2$ and let $f \in K[x]$ be a degree 2 polynomial. Then $f' \neq 0$; that is, f' is not the zero polynomial in $K[x]$ (since f' is a degree 1 polynomial). Since f is hypothesized to be irreducible, then by Theorem III.6.10(iii), f has no multiple roots in any extension field (including a splitting field of f), so f is separable. □

Corollary V.4.3

Corollary V.4.3. The Galois Group of Degree 3 Polynomials.
Let K be a field and $f \in K[x]$ an irreducible polynomial of degree 2 with Galois group G. If f is separable (as is always the case when $\text{char}(K) \neq 2$), then $G \cong \mathbb{Z}_2$; otherwise $G = \{\iota\} = 1$.

Proof. By Theorem V.4.2(ii), if f is separable of degree 2 then G is isomorphic to a transitive subgroup of $S_2 \cong \mathbb{Z}_2$. But the only transitive subgroup of $\mathbb{Z}_2$ is $\mathbb{Z}_2$ itself, so $G \cong \mathbb{Z}_2$.

If f is not separable, then in a splitting field F of f we have $f(x) = (x-a)^2 \in F[x]$ and for $\sigma \in G - \text{Aut}_K F$ we must have $\sigma(a) = a$ by Theorem V.2.2 and so σ fixes $F = K(a)$. That is, in this case $G = \{\iota\}$.

Finally, suppose $\text{char}(K) \neq 2$ and let $f \in K[x]$ be a degree 2 polynomial. Then $f' \neq 0$; that is, f' is not the zero polynomial in $K[x]$ (since f' is a degree 1 polynomial). Since f is hypothesized to be irreducible, then by Theorem III.6.10(iii), f has no multiple roots in any extension field (including a splitting field of f), so f is separable. □

Proposition V.4.5

Proposition V.4.5. Let K, f, F and Δ be as in Definition V.4.4.

(i) The discriminant Δ^2 of f actually lies in K.

(ii) For each $\sigma \in \mathrm{Aut}_k F < S_n$, σ is an even (respectively, odd) permutation if and only if $\sigma(\Delta) = \Delta$ (respectively, $\sigma(\Delta) = -\Delta$).

Proof. **(ii)** In the proof of Theorem I.6.7, it is shown for $\{u_1, u_2, \ldots, u_n\} = \{i_1, i_2, \ldots, i_n\} = \{1, 2, \ldots, n\}$ that for $\sigma \in S_n$ a transposition, $\Delta(\sigma(i_1), \sigma(i_2), \ldots, \sigma(i_n)) = -\Delta(i_1, i_2, \ldots, i_n)$.

Proposition V.4.5

Proposition V.4.5. Let K, f, F and Δ be as in Definition V.4.4.

(i) The discriminant Δ^2 of f actually lies in K.

(ii) For each $\sigma \in \mathrm{Aut}_k F < S_n$, σ is an even (respectively, odd) permutation if and only if $\sigma(\Delta) = \Delta$ (respectively, $\sigma(\Delta) = -\Delta$).

Proof. (ii) In the proof of Theorem I.6.7, it is shown for $\{u_1, u_2, \ldots, u_n\} = \{i_1, i_2, \ldots, i_n\} = \{1, 2, \ldots, n\}$ that for $\sigma \in S_n$ a transposition, $\Delta(\sigma(i_1), \sigma(i_2), \ldots, \sigma(i_n)) = -\Delta(i_1, i_2, \ldots, i_n)$. Similarly (replacing the i's with u's) gives for σ a transposition mapping $\{u_1, u_2, \ldots, u_n\}$ to itself that $\Delta(\sigma(u_1), \sigma(u_2), \ldots, \sigma(u_n)) = -\Delta(u_1, u_2, \ldots, u_n)$. If $\sigma \in \mathrm{Aut}_K F$ then, since F is a splitting field of f and the roots of f are (distinct) $\{u_1, u_2, \ldots, u_n\}$, we have $F = K(u_1, u_2, \ldots, u_n)$, σ is determined by its action on $\{u_1, u_2, \ldots, u_n\}$.

Proposition V.4.5

Proposition V.4.5. Let K, f, F and Δ be as in Definition V.4.4.

(i) The discriminant Δ^2 of f actually lies in K.

(ii) For each $\sigma \in \mathrm{Aut}_k F < S_n$, σ is an even (respectively, odd) permutation if and only if $\sigma(\Delta) = \Delta$ (respectively, $\sigma(\Delta) = -\Delta$).

Proof. (ii) In the proof of Theorem I.6.7, it is shown for $\{u_1, u_2, \ldots, u_n\} = \{i_1, i_2, \ldots, i_n\} = \{1, 2, \ldots, n\}$ that for $\sigma \in S_n$ a transposition, $\Delta(\sigma(i_1), \sigma(i_2), \ldots, \sigma(i_n)) = -\Delta(i_1, i_2, \ldots, i_n)$. Similarly (replacing the i's with u's) gives for σ a transposition mapping $\{u_1, u_2, \ldots, u_n\}$ to itself that $\Delta(\sigma(u_1), \sigma(u_2), \ldots, \sigma(u_n)) = -\Delta(u_1, u_2, \ldots, u_n)$. If $\sigma \in \mathrm{Aut}_K F$ then, since F is a splitting field of f and the roots of f are (distinct) $\{u_1, u_2, \ldots, u_n\}$, we have $F = K(u_1, u_2, \ldots, u_n)$, σ is determined by its action on $\{u_1, u_2, \ldots, u_n\}$.

Proposition V.4.5 (continued)

Proposition V.4.5. Let K, f, F and Δ be as in Definition V.4.4.

(i) The discriminant Δ^2 of f actually lies in K.

(ii) For each $\sigma \in \mathrm{Aut}_k F < S_n$, σ is an even (respectively, odd) permutation if and only if $\sigma(\Delta) = \Delta$ (respectively, $\sigma(\Delta) = -\Delta$).

Proof (continued). (ii) So if σ is even, then σ is a product of an even number of transpositions and so $\Delta(\sigma(u_1), \sigma(u_2), \ldots \sigma(u_n))$ differed from $\Delta(u_1, u_2, \ldots, u_n)$ be a factor of an even power of -1. That is, $\Delta(\sigma(u_1), \sigma(u_2), \ldots \sigma(u_n)) = \Delta(u_1, u_2, \ldots, u_n)$. Similarly, if σ is odd then $\Delta(\sigma(u_1), \sigma(u_2), \ldots \sigma(u_n)) = -\Delta(u_1, u_2, \ldots, u_n)$, and (ii) follows.

Proposition V.4.5 (continued)

Proposition V.4.5. Let K, f, F and Δ be as in Definition V.4.4.

(i) The discriminant Δ^2 of f actually lies in K.

(ii) For each $\sigma \in \mathrm{Aut}_k F < S_n$, σ is an even (respectively, odd) permutation if and only if $\sigma(\Delta) = \Delta$ (respectively, $\sigma(\Delta) = -\Delta$).

Proof (continued). (ii) So if σ is even, then σ is a product of an even number of transpositions and so $\Delta(\sigma(u_1), \sigma(u_2), \ldots \sigma(u_n))$ differed from $\Delta(u_1, u_2, \ldots, u_n)$ be a factor of an even power of -1. That is, $\Delta(\sigma(u_1), \sigma(u_2), \ldots \sigma(u_n)) = \Delta(u_1, u_2, \ldots, u_n)$. Similarly, if σ is odd then $\Delta(\sigma(u_1), \sigma(u_2), \ldots \sigma(u_n)) = -\Delta(u_1, u_2, \ldots, u_n)$, and (ii) follows.

(i) From part (ii), for every $\sigma \in \mathrm{Aut}_K F$ we have (since σ is a homomorphism), $\sigma(\Delta^2) = (\sigma(\Delta))^2 = (\pm\Delta)^2 = \Delta^2$. Therefore Δ^2 is part of the fixed field of $\mathrm{Aut}_K F$.

Proposition V.4.5 (continued)

Proposition V.4.5. Let K, f, F and Δ be as in Definition V.4.4.

(i) The discriminant Δ^2 of f actually lies in K.

(ii) For each $\sigma \in \mathrm{Aut}_k F < S_n$, σ is an even (respectively, odd) permutation if and only if $\sigma(\Delta) = \Delta$ (respectively, $\sigma(\Delta) = -\Delta$).

Proof (continued). **(ii)** So if σ is even, then σ is a product of an even number of transpositions and so $\Delta(\sigma(u_1), \sigma(u_2), \ldots \sigma(u_n))$ differed from $\Delta(u_1, u_2, \ldots, u_n)$ be a factor of an even power of -1. That is, $\Delta(\sigma(u_1), \sigma(u_2), \ldots \sigma(u_n)) = \Delta(u_1, u_2, \ldots, u_n)$. Similarly, if σ is odd then $\Delta(\sigma(u_1), \sigma(u_2), \ldots \sigma(u_n)) = -\Delta(u_1, u_2, \ldots, u_n)$, and (ii) follows.

(i) From part (ii), for every $\sigma \in \mathrm{Aut}_K F$ we have (since σ is a homomorphism), $\sigma(\Delta^2) = (\sigma(\Delta))^2 = (\pm\Delta)^2 = \Delta^2$. Therefore Δ^2 is part of the fixed field of $\mathrm{Aut}_K F$. Now by Theorem V.3.11 (the (ii)⇒(i) part), F is Galois over K. So, by the definition of "Galois," the fixed field of $\mathrm{Aut}_K F$ is K itself. Therefore, $\Delta^2 \in K$. □

Proposition V.4.5 (continued)

Proposition V.4.5. Let K, f, F and Δ be as in Definition V.4.4.

(i) The discriminant Δ^2 of f actually lies in K.

(ii) For each $\sigma \in \text{Aut}_k F < S_n$, σ is an even (respectively, odd) permutation if and only if $\sigma(\Delta) = \Delta$ (respectively, $\sigma(\Delta) = -\Delta$).

Proof (continued). (ii) So if σ is even, then σ is a product of an even number of transpositions and so $\Delta(\sigma(u_1), \sigma(u_2), \ldots \sigma(u_n))$ differed from $\Delta(u_1, u_2, \ldots, u_n)$ be a factor of an even power of -1. That is, $\Delta(\sigma(u_1), \sigma(u_2), \ldots \sigma(u_n)) = \Delta(u_1, u_2, \ldots, u_n)$. Similarly, if σ is odd then $\Delta(\sigma(u_1), \sigma(u_2), \ldots \sigma(u_n)) = -\Delta(u_1, u_2, \ldots, u_n)$, and (ii) follows.

(i) From part (ii), for every $\sigma \in \text{Aut}_K F$ we have (since σ is a homomorphism), $\sigma(\Delta^2) = (\sigma(\Delta))^2 = (\pm\Delta)^2 = \Delta^2$. Therefore Δ^2 is part of the fixed field of $\text{Aut}_K F$. Now by Theorem V.3.11 (the (ii)$\Rightarrow$(i) part), F is Galois over K. So, by the definition of "Galois," the fixed field of $\text{Aut}_K F$ is K itself. Therefore, $\Delta^2 \in K$. □

Proposition V.4.7

Corollary V.4.7. The Galois Group of Degree 3 Polynomials.
Let K be a field and $f \in K[x]$ an irreducible, separable polynomial of degree 3. The Galois group of f is either S_3 or A_3. If $\text{char}(K) \neq 2$, it is A_3 if and only if the discriminant $D = \Delta^2$ of f is the square of some element of K.

Proof. By Theorem V.4.2 (really, the note following Corollary V.4.3), the Galois group is either S_3 or A_3. By Corollary V.4.6, G consists of even permutations (and so is A_3) if and only if $\Delta \in K$.

Proposition V.4.7

Corollary V.4.7. The Galois Group of Degree 3 Polynomials.
Let K be a field and $f \in K[x]$ an irreducible, separable polynomial of degree 3. The Galois group of f is either S_3 or A_3. If $\text{char}(K) \neq 2$, it is A_3 if and only if the discriminant $D = \Delta^2$ of f is the square of some element of K.

Proof. By Theorem V.4.2 (really, the note following Corollary V.4.3), the Galois group is either S_3 or A_3. By Corollary V.4.6, G consists of even permutations (and so is A_3) if and only if $\Delta \in K$. If $\Delta \in K$ then D is the square of some element of K. Next, if $D = d^2 = \Delta^2$ where $d \in K$, then (in F) $\Delta^2 - d^2 = 0$ or $(\Delta - d)(\Delta + d) = 0$ and so either $d = \Delta$ or $d = -\Delta$, implying $\Delta \in K$. □

Proposition V.4.7

Corollary V.4.7. The Galois Group of Degree 3 Polynomials.
Let K be a field and $f \in K[x]$ an irreducible, separable polynomial of degree 3. The Galois group of f is either S_3 or A_3. If $\text{char}(K) \neq 2$, it is A_3 if and only if the discriminant $D = \Delta^2$ of f is the square of some element of K.

Proof. By Theorem V.4.2 (really, the note following Corollary V.4.3), the Galois group is either S_3 or A_3. By Corollary V.4.6, G consists of even permutations (and so is A_3) if and only if $\Delta \in K$. If $\Delta \in K$ then D is the square of some element of K. Next, if $D = d^2 = \Delta^2$ where $d \in K$, then (in F) $\Delta^2 - d^2 = 0$ or $(\Delta - d)(\Delta + d) = 0$ and so either $d = \Delta$ or $d = -\Delta$, implying $\Delta \in K$. □

Proposition V.4.8

Proposition V.4.8. Let K be a field with $\text{char}(K) \neq 2, 3$. If $f(x) = x^3 + bx^3 + cx + d \in K[x]$ has three distinct roots in some splitting field, then the polynomial $g(x) = f(x - b/3) \in K[x]$ has the form $x^3 + px + q$ and the discriminant of f is $-4p^3 - 27q^2$.

Proof. Let F be a splitting field of f over K. If $u \in F$ is a root of f then $u + b/3$ is a root of $g(x) = f(x - b/3)$ (and conversely). Let v_1, v_2, v_3 be the roots of g.

Proposition V.4.8

Proposition V.4.8. Let K be a field with $\text{char}(K) \neq 2, 3$. If $f(x) = x^3 + bx^3 + cx + d \in K[x]$ has three distinct roots in some splitting field, then the polynomial $g(x) = f(x - b/3) \in K[x]$ has the form $x^3 + px + q$ and the discriminant of f is $-4p^3 - 27q^2$.

Proof. Let F be a splitting field of f over K. If $u \in F$ is a root of f then $u + b/3$ is a root of $g(x) = f(x - b/3)$ (and conversely). Let v_1, v_2, v_3 be the roots of g. Then the roots of f are $v_1 - b/3$, $v_2 - b/3$, $v_3 - b/3$. So the discriminant of g is the square of

$$\Delta = (v_1 - v_2)(v_1 - v_3)(v_2 - v_3)$$

$$= ((v_1 - b/3) - (v_2 - b/3))((v_1 - b/3) - (v_3 - b/3))((v_2 - b/3) - (v_3 - b/3)),$$

which when squared is also the discriminant of f. So f and g have the same discriminant.

Proposition V.4.8

Proposition V.4.8. Let K be a field with $\mathrm{char}(K) \neq 2, 3$. If $f(x) = x^3 + bx^3 + cx + d \in K[x]$ has three distinct roots in some splitting field, then the polynomial $g(x) = f(x - b/3) \in K[x]$ has the form $x^3 + px + q$ and the discriminant of f is $-4p^3 - 27q^2$.

Proof. Let F be a splitting field of f over K. If $u \in F$ is a root of f then $u + b/3$ is a root of $g(x) = f(x - b/3)$ (and conversely). Let v_1, v_2, v_3 be the roots of g. Then the roots of f are $v_1 - b/3$, $v_2 - b/3$, $v_3 - b/3$. So the discriminant of g is the square of

$$\Delta = (v_1 - v_2)(v_1 - v_3)(v_2 - v_3)$$

$$= ((v_1 - b/3) - (v_2 - b/3))((v_1 - b/3) - (v_3 - b/3))((v_2 - b/3) - (v_3 - b/3)),$$

which when squared is also the discriminant of f. So f and g have the same discriminant.

Proposition V.4.8 (continued 1)

Proof (continued). Now

$$\begin{aligned} g(x) &= f(x-b/3) = (x-b/3)^3 + b(b-b/3)^2 + c(x-b/3) + d \\ &= x^3 - 3x^2 b/3 + 3x(b/3) - (b/3)^3 + bx^2 - 2bx(b/3) \\ &\qquad + b(b/3)^2 + cx - bc/3 + d \\ &= x^3 + (-b+b)x^2 + (b^2/3 - 2b^2/3 + c)x \\ &\quad + (-b^3/27 + b^3/9 - bc/3 + d) \\ &= x^3 + (-b^2/3 + c)x + (2b^3/27 - bc/3 + d) \\ &= x^3 + px + q \end{aligned}$$

where $p = -b^2/3 + c \in K$ and $q = 2b^3/27 - bc/3 + d \in K$. Since we assumed that the roots of g are v_1, v_2, v_3 then

$$g(x) = x^3 - px + q = (x-v_1)(x-v_2)(x-v_3)$$

$$= x^3 + (-v_1 - v_2 - v_3)x^2 + (v_1v_2 + v_1v_3 + v_2v_3)x + (-v_1v_2v_3).$$

Proposition V.4.8 (continued 1)

Proof (continued). Now

$$\begin{aligned} g(x) &= f(x-b/3) = (x-b/3)^3 + b(b-b/3)^2 + c(x-b/3) + d \\ &= x^3 - 3x^2 b/3 + 3x(b/3) - (b/3)^3 + bx^2 - 2bx(b/3) \\ &\qquad\qquad +b(b/3)^2 + cx - bc/3 + d \\ &= x^3 + (-b+b)x^2 + (b^2/3 - 2b^2/3 + c)x \\ &\quad +(-b^3/27 + b^3/9 - bc/3 + d) \\ &= x^3 + (-b^2/3 + c)x + (2b^3/27 - bc/3 + d) \\ &= x^3 + px + q \end{aligned}$$

where $p = -b^2/3 + c \in K$ and $q = 2b^3/27 - bc/3 + d \in K$. Since we assumed that the roots of g are v_1, v_2, v_3 then

$$g(x) = x^3 - px + q = (x - v_1)(x - v_2)(x - v_3)$$

$$= x^3 + (-v_1 - v_2 - v_3)x^2 + (v_1 v_2 + v_1 v_3 + v_2 v_3)x + (-v_1 v_2 v_3).$$

Proposition V.4.8 (continued 2)

Proof (continued). Hungerford declares the establishing of the fact that $D = \Delta^2 = -4p^3 - 27q^2$ where $p = -b^2/3 + c \in K$ and $q = 2b^3/27 - bc/3 + d \in K$ (as above), "a gruesome computation." Instead of hacking through the gruesome computation, we follow the proof in Dummit and Foote's *Abstract Algebra*, Third Edition, Wiley and Sons (2004), pages 609 and 612.

Proposition V.4.8 (continued 2)

Proof (continued). Hungerford declares the establishing of the fact that $D = \Delta^2 = -4p^3 - 27q^2$ where $p = -b^2/3 + c \in K$ and $q = 2b^3/27 - bc/3 + d \in K$ (as above), "a gruesome computation." Instead of hacking through the gruesome computation, we follow the proof in Dummit and Foote's *Abstract Algebra*, Third Edition, Wiley and Sons (2004), pages 609 and 612.

First, in the notation of the appendix to Section V.2 (see page 252), with $g(x) = (x - v_1)(x - v_2)(x - v_3)$, we have $g_1 = v_1 + v_2 + v_3$, $g_2 = v_1 v_2 + v_1 v_3 + v_2 v_3$, and $g_3 = v_1 v_2 v_3$.

Proposition V.4.8 (continued 2)

Proof (continued). Hungerford declares the establishing of the fact that $D = \Delta^2 = -4p^3 - 27q^2$ where $p = -b^2/3 + c \in K$ and $q = 2b^3/27 - bc/3 + d \in K$ (as above), "a gruesome computation." Instead of hacking through the gruesome computation, we follow the proof in Dummit and Foote's *Abstract Algebra*, Third Edition, Wiley and Sons (2004), pages 609 and 612.

First, in the notation of the appendix to Section V.2 (see page 252), with $g(x) = (x - v_1)(x - v_2)(x - v_3)$, we have $g_1 = v_1 + v_2 + v_3$, $g_2 = v_1v_2 + v_1v_3 + v_2v_3$, and $g_3 = v_1v_2v_3$. We then have

$$\begin{aligned} g_1^2 - 2g_2 &= (v_1 + v_2 + v_3)^2 - 2(v_1v_2 + v_1v_3 + v_2v_3) \\ &= (v_1^2 + 2v_1v_2 + 2v_1v_3 + v_2^2 + 2v_2v_3 + v_3^2) \\ &\qquad -2(v_1v_2 + v_1v_3 + v_2v_3) \\ &= v_1^2 + v_2^2 + v_3^2 \end{aligned}$$

Proposition V.4.8 (continued 2)

Proof (continued). Hungerford declares the establishing of the fact that $D = \Delta^2 = -4p^3 - 27q^2$ where $p = -b^2/3 + c \in K$ and $q = 2b^3/27 - bc/3 + d \in K$ (as above), "a gruesome computation." Instead of hacking through the gruesome computation, we follow the proof in Dummit and Foote's *Abstract Algebra*, Third Edition, Wiley and Sons (2004), pages 609 and 612.

First, in the notation of the appendix to Section V.2 (see page 252), with $g(x) = (x - v_1)(x - v_2)(x - v_3)$, we have $g_1 = v_1 + v_2 + v_3$, $g_2 = v_1 v_2 + v_1 v_3 + v_2 v_3$, and $g_3 = v_1 v_2 v_3$. We then have

$$\begin{aligned} g_1^2 - 2g_2 &= (v_1 + v_2 + v_3)^2 - 2(v_1 v_2 + v_1 v_3 + v_2 v_3) \\ &= (v_1^2 + 2v_1 v_2 + 2v_1 v_3 + v_2^2 + 2v_2 v_3 + v_3^2) \\ &\qquad -2(v_1 v_2 + v_1 v_3 + v_2 v_3) \\ &= v_1^2 + v_2^2 + v_3^2 \end{aligned}$$

Proposition V.4.8 (continued 3)

Proof (continued). and

$$\begin{aligned} g_2^2 - 2g_1g_2 &= (v_1v_2 + v_1v_2 + v_2v_3)^2 - 2(v_1 + v_2 + v_3)(v_1v_2v_3) \\ &= (v_1^2v_2^2 + 2v_1^2v_2v_3 + 2v_1v_2^2v_3 + v_1^2v_3^2 + 2v_1v_2v_3^2 + v_2^2v_3^2) \\ &\quad -2v_1^2v_2v_3 - 2v_1v_2^2v_3 - 2v_1v_2v_3^2 \\ &= v_1^2v_2^2 + v_2^2v_3^2 + v_2^2v_3^2. \end{aligned}$$

So we have

$$v_1^2 + v_2^2 + v_3^2 = g_1^2 - 2g_2 \qquad (1)$$

$$v_1^2v_2^2 + v_1^2v_3^2 + v_2^2v_3^2 = g_2^2 - 2g_1g_3. \qquad (2)$$

Proposition V.4.8 (continued 3)

Proof (continued). and

$$\begin{aligned} g_2^2 - 2g_1g_2 &= (v_1v_2 + v_1v_2 + v_2v_3)^2 - 2(v_1 + v_2 + v_3)(v_1v_2v_3) \\ &= (v_1^2v_2^2 + 2v_1^2v_2v_3 + 2v_1v_2^2v_3 + v_1^2v_3^2 + 2v_1v_2v_3^2 + v_2^2v_3^2) \\ &\qquad -2v_1^2v_2v_3 - 2v_1v_2^2v_3 - 2v_1v_2v_3^2 \\ &= v_1^2v_2^2 + v_2^2v_3^2 + v_2^2v_3^2. \end{aligned}$$

So we have

$$v_1^2 + v_2^2 + v_3^2 = g_1^2 - 2g_2 \tag{1}$$

$$v_1^2v_2^2 + v_1^2v_3^2 + v_2^2v_3^2 = g_2^2 - 2g_1g_3. \tag{2}$$

By the Product Rule (Lemma V.6.9(iii)) we have

$$g'(x) = (x - v_1)(x - v_2) + (x - v_1)(x - v_3) + (x - v_2)(x - v_3).$$

Proposition V.4.8 (continued 3)

Proof (continued). and

$$\begin{aligned} g_2^2 - 2g_1g_2 &= (v_1v_2 + v_1v_2 + v_2v_3)^2 - 2(v_1 + v_2 + v_3)(v_1v_2v_3) \\ &= (v_1^2v_2^2 + 2v_1^2v_2v_3 + 2v_1v_2^2v_3 + v_1^2v_3^2 + 2v_1v_2v_3^2 + v_2^2v_3^2) \\ &\qquad -2v_1^2v_2v_3 - 2v_1v_2^2v_3 - 2v_1v_2v_3^2 \\ &= v_1^2v_2^2 + v_2^2v_3^2 + v_2^2v_3^2. \end{aligned}$$

So we have

$$v_1^2 + v_2^2 + v_3^2 = g_1^2 - 2g_2 \tag{1}$$

$$v_1^2v_2^2 + v_1^2v_3^2 + v_2^2v_3^2 = g_2^2 - 2g_1g_3. \tag{2}$$

By the Product Rule (Lemma V.6.9(iii)) we have

$$g'(x) = (x - v_1)(x - v_2) + (x - v_1)(x - v_3) + (x - v_2)(x - v_3).$$

Proposition V.4.8 (continued 4)

Proof (continued). Then

$$\begin{aligned} g'(v_1) &= (v_1 - v_2)(v_1 - v_3) \\ g'(v_2) &= (v_2 - v_1)(v_2 - v_3) = -(v_1 - v_2)(v_2 - v_3) \\ g'(v_3) &= (v_3 - v_1)(v_3 - v_1) + (v_1 - v_3)(v_2 - v_3). \end{aligned}$$

By the definition of "discriminant," the discriminant of g is

$$\begin{aligned} D &= (v_1 - v_2)^2(v_1 - v_3)^2(v_2 - v_3)^2 \\ &= g'(v_1)(-g'(v_2))g'(v_3) \\ &= -g'(v_1)g'(v_2)g'(v_3)v \\ &= -g'(v_1)g'(v_2)g'(v_3). \qquad (3) \end{aligned}$$

Proposition V.4.8 (continued 4)

Proof (continued). Then

$$\begin{aligned} g'(v_1) &= (v_1 - v_2)(v_1 - v_3) \\ g'(v_2) &= (v_2 - v_1)(v_2 - v_3) = -(v_1 - v_2)(v_2 - v_3) \\ g'(v_3) &= (v_3 - v_1)(v_3 - v_1) + (v_1 - v_3)(v_2 - v_3). \end{aligned}$$

By the definition of "discriminant," the discriminant of g is

$$\begin{aligned} D &= (v_1 - v_2)^2(v_1 - v_3)^2(v_2 - v_3)^2 \\ &= g'(v_1)(-g'(v_2))g'(v_3) \\ &= -g'(v_1)g'(v_2)g'(v_3)v \\ &= -g'(v_1)g'(v_2)g'(v_3). \qquad (3) \end{aligned}$$

Since $g(x) = x^3 + px + q$, then $g'(x) = 3x^2 + p$, then

$$g'(v_i) = 3v_i^2 + p \text{ for } i = 1, 2, 3. \qquad (4)$$

Proposition V.4.8 (continued 4)

Proof (continued). Then

$$\begin{aligned} g'(v_1) &= (v_1 - v_2)(v_1 - v_3) \\ g'(v_2) &= (v_2 - v_1)(v_2 - v_3) = -(v_1 - v_2)(v_2 - v_3) \\ g'(v_3) &= (v_3 - v_1)(v_3 - v_1) + (v_1 - v_3)(v_2 - v_3). \end{aligned}$$

By the definition of "discriminant," the discriminant of g is

$$\begin{aligned} D &= (v_1 - v_2)^2(v_1 - v_3)^2(v_2 - v_3)^2 \\ &= g'(v_1)(-g'(v_2))g'(v_3) \\ &= -g'(v_1)g'(v_2)g'(v_3)v \\ &= -g'(v_1)g'(v_2)g'(v_3). \qquad (3) \end{aligned}$$

Since $g(x) = x^3 + px + q$, then $g'(x) = 3x^2 + p$, then

$$g'(v_i) = 3v_i^2 + p \text{ for } i = 1, 2, 3. \qquad (4)$$

Proposition V.4.8 (continued 5)

Proof (continued). We then have

$$
\begin{aligned}
-D &= g'(v_1)g'(v_2)g'(v_3) \text{ from (3)} \\
&= (3v_1^2 + p)(3v_2 + p)(3v_3 + p) \text{ from (4)} \\
&= 27v_1^2v_2^2v_3^2 + 9p(v_1^2v_2^2 + v_1^2v_3^2 + v_2^2v_3^2) + 3p^2(v_1^2 + v_2^2 + v_3^2) + p^2 \\
&= 27g_3^3 + 9p(g_2^2 - 2g_1g_2) + 3p^2(g_1^2 - 2g_2) + p^3 \text{ by (1) and (2).} \quad (5)
\end{aligned}
$$

Next, we have

$$
\begin{aligned}
g(x) &= (x - v_1)(x - v_2)(x - v_3) \\
&= x^3 + px + q \\
&= x^3 - g_1x^2 + g_2x - g_3 \text{ by Section V.2.Appendix (see page 252).}
\end{aligned}
$$

Proposition V.4.8 (continued 5)

Proof (continued). We then have

$$\begin{aligned}
-D &= g'(v_1)g'(v_2)g'(v_3) \text{ from (3)} \\
&= (3v_1^2 + p)(3v_2 + p)(3v_3 + p) \text{ from (4)} \\
&= 27v_1^2v_2^2v_3^2 + 9p(v_1^2v_2^2 + v_1^2v_3^2 + v_2^2v_3^2) + 3p^2(v_1^2 + v_2^2 + v_3^2) + p^2 \\
&= 27g_3^3 + 9p(g_2^2 - 2g_1g_2) + 3p^2(g_1^2 - 2g_2) + p^3 \text{ by (1) and (2).} \quad (5)
\end{aligned}$$

Next, we have

$$\begin{aligned}
g(x) &= (x - v_1)(x - v_2)(x - v_3) \\
&= x^3 + px + q \\
&= x^3 - g_1x^2 + g_2x - g_3 \text{ by Section V.2.Appendix (see page 252).}
\end{aligned}$$

So $g_1 = 0$, $g_2 = p$, and $g_3 = -q$. Substituting these values into (5) we have. . .

Proposition V.4.8 (continued 5)

Proof (continued). We then have

$$\begin{aligned} -D &= g'(v_1)g'(v_2)g'(v_3) \text{ from (3)} \\ &= (3v_1^2 + p)(3v_2 + p)(3v_3 + p) \text{ from (4)} \\ &= 27v_1^2v_2^2v_3^2 + 9p(v_1^2v_2^2 + v_1^2v_3^2 + v_2^2v_3^2) + 3p^2(v_1^2 + v_2^2 + v_3^2) + p^2 \\ &= 27g_3^3 + 9p(g_2^2 - 2g_1g_2) + 3p^2(g_1^2 - 2g_2) + p^3 \text{ by (1) and (2).} \quad (5) \end{aligned}$$

Next, we have

$$\begin{aligned} g(x) &= (x - v_1)(x - v_2)(x - v_3) \\ &= x^3 + px + q \\ &= x^3 - g_1x^2 + g_2x - g_3 \text{ by Section V.2.Appendix (see page 252).} \end{aligned}$$

So $g_1 = 0$, $g_2 = p$, and $g_3 = -q$. Substituting these values into (5) we have. . .

Proposition V.4.8 (continued 6)

Proposition V.4.8. Let K be a field with $\text{char}(K) \neq 2, 3$. If $f(x) = x^3 + bx^3 + cx + d \in K[x]$ has three distinct roots in some splitting field, then the polynomial $g(x) = f(x - b/3) \in K[x]$ has the form $x^3 + px + q$ and the discriminant of f is $-4p^3 - 27q^2$.

Proof (continued). ...

$$-D = 27(-q)^2 + 9p(p^2 - 2(0)(-q)) + 3p^2((0)^2 - 2(p)) + p^3$$
$$= 27q^2 + 9p^3 - 6p^3 + p^3 = 27q^2 + 4p^3,$$

and so $D = -4p^3 - 27q^2$. □

Lemma V.4.9

Lemma V.4.9. Let K, f, F, u_i, V, and $G = \text{Aut}_K F < S_4$ be as just described. If $\alpha = u_1u_2 + u_3u_4$, $\beta = u_1u_3 + u_2u_4$, $\gamma = u_1u_4 + u_2u_3 \in F$, then under the Galois correspondence of the Fundamental Theorem (Theorem V.2.5) the subfield $K(\alpha, \beta, \gamma)$ corresponds to the normal subgroup $V \cap G$. Hence $K(\alpha, \beta, \gamma)$ is Galois over K and $\text{Aut}_K K(\alpha, \beta, \gamma) \cong G/(G \cap V)$.

Proof. "Clearly" every element in $G \cap V$ fixes α, β, γ and hence $K(\alpha, \beta, \gamma)$. To show the correspondence of the Fundamental Theorem, we need to show that the subgroup of $G = \text{Aut}_K F$ which fixes $K(\alpha, \beta, \gamma)$ is $G \cap V$.

Lemma V.4.9

Lemma V.4.9. Let K, f, F, u_i, V, and $G = \mathrm{Aut}_K F < S_4$ be as just described. If $\alpha = u_1u_2 + u_3u_4$, $\beta = u_1u_3 + u_2u_4$, $\gamma = u_1u_4 + u_2u_3 \in F$, then under the Galois correspondence of the Fundamental Theorem (Theorem V.2.5) the subfield $K(\alpha, \beta, \gamma)$ corresponds to the normal subgroup $V \cap G$. Hence $K(\alpha, \beta, \gamma)$ is Galois over K and $\mathrm{Aut}_K K(\alpha, \beta, \gamma) \cong G/(G \cap V)$.

Proof. "Clearly" every element in $G \cap V$ fixes α, β, γ and hence $K(\alpha, \beta, \gamma)$. To show the correspondence of the Fundamental Theorem, we need to show that the subgroup of $G = \mathrm{Aut}_K F$ which fixes $K(\alpha, \beta, \gamma)$ is $G \cap V$. So we need to show for each $\sigma \in G \setminus V$, σ does not fix one of α, β, γ. Since S_4 consists of $4! = 24$ elements, we need to check 20 permutations.

Lemma V.4.9

Lemma V.4.9. Let K, f, F, u_i, V, and $G = \text{Aut}_K F < S_4$ be as just described. If $\alpha = u_1 u_2 + u_3 u_4$, $\beta = u_1 u_3 + u_2 u_4$, $\gamma = u_1 u_4 + u_2 u_3 \in F$, then under the Galois correspondence of the Fundamental Theorem (Theorem V.2.5) the subfield $K(\alpha, \beta, \gamma)$ corresponds to the normal subgroup $V \cap G$. Hence $K(\alpha, \beta, \gamma)$ is Galois over K and $\text{Aut}_K K(\alpha, \beta, \gamma) \cong G/(G \cap V)$.

Proof. "Clearly" every element in $G \cap V$ fixes α, β, γ and hence $K(\alpha, \beta, \gamma)$. To show the correspondence of the Fundamental Theorem, we need to show that the subgroup of $G = \text{Aut}_K F$ which fixes $K(\alpha, \beta, \gamma)$ is $G \cap V$. So we need to show for each $\sigma \in G \setminus V$, σ does not fix one of α, β, γ. Since S_4 consists of $4! = 24$ elements, we need to check 20 permutations.

Lemma V.4.9 (continued 1)

Proof (continued). Consider the transposition $\sigma = (1,2)$. We have $\sigma(\beta) = \sigma(u_1 u_3 + u_2 u_4) = u_2 u_3 + u_1 u_4$. ASSUME $\sigma(\beta) = \beta$. Then $u_1 u_3 + u_2 u_4 = u_2 u_3 + u_1 u_4$ or $u_1 u_3 - u_1 u_4 = u_2 u_3 - u_2 u_4$ or $u_1(u_3 - u_4) = u_2(u_3 - u_4)$. So either $u_1 = u_2$ or $u_3 = u_4$, both CONTRADICTIONS. So the assumption is incorrect and we have $\sigma(\beta) \neq \beta$.

Lemma V.4.9 (continued 1)

Proof (continued). Consider the transposition $\sigma = (1,2)$. We have $\sigma(\beta) = \sigma(u_1u_3 + u_2u_4) = u_2u_3 + u_1u_4$. ASSUME $\sigma(\beta) = \beta$. Then $u_1u_3 + u_2u_4 = u_2u_3 + u_1u_4$ or $u_1u_3 - u_1u_4 = u_2u_3 - u_2u_4$ or $u_1(u_3 - u_4) = u_2(u_3 - u_4)$. So either $u_1 = u_2$ or $u_3 = u_4$, both CONTRADICTIONS. So the assumption is incorrect and we have $\sigma(\beta) \neq \beta$. A similar contradiction results for the other 3 transpositions $(1,4)$, $(2,3)$, and $(3,4)$. For the remaining transpositions, $(1,3)$ and $(2,4)$, a similar argument shows that $\alpha = u_1u_2 + u_3u_4$ is not fixed by these transpositions. So none of the 6 transpositions in S_4 are in $G \setminus V$.

Lemma V.4.9 (continued 1)

Proof (continued). Consider the transposition $\sigma = (1, 2)$. We have $\sigma(\beta) = \sigma(u_1 u_3 + u_2 u_4) = u_2 u_3 + u_1 u_4$. ASSUME $\sigma(\beta) = \beta$. Then $u_1 u_3 + u_2 u_4 = u_2 u_3 + u_1 u_4$ or $u_1 u_3 - u_1 u_4 = u_2 u_3 - u_2 u_4$ or $u_1(u_3 - u_4) = u_2(u_3 - u_4)$. So either $u_1 = u_2$ or $u_3 = u_4$, both CONTRADICTIONS. So the assumption is incorrect and we have $\sigma(\beta) \neq \beta$. A similar contradiction results for the other 3 transpositions $(1, 4)$, $(2, 3)$, and $(3, 4)$. For the remaining transpositions, $(1, 3)$ and $(2, 4)$, a similar argument shows that $\alpha = u_1 u_2 + u_3 u_4$ is not fixed by these transpositions. So none of the 6 transpositions in S_4 are in $G \setminus V$.

Consider the 3-cycle $\sigma = (1, 2, 3)$. We have $\sigma(\alpha) = \sigma(u_1 u_2 + u_3 u_4) = u_2 u_3 + u_1 u_4$. ASSUME $\sigma(\alpha) = \alpha$.

Lemma V.4.9 (continued 1)

Proof (continued). Consider the transposition $\sigma = (1,2)$. We have $\sigma(\beta) = \sigma(u_1u_3 + u_2u_4) = u_2u_3 + u_1u_4$. ASSUME $\sigma(\beta) = \beta$. Then $u_1u_3 + u_2u_4 = u_2u_3 + u_1u_4$ or $u_1u_3 - u_1u_4 = u_2u_3 - u_2u_4$ or $u_1(u_3 - u_4) = u_2(u_3 - u_4)$. So either $u_1 = u_2$ or $u_3 = u_4$, both CONTRADICTIONS. So the assumption is incorrect and we have $\sigma(\beta) \neq \beta$. A similar contradiction results for the other 3 transpositions $(1,4)$, $(2,3)$, and $(3,4)$. For the remaining transpositions, $(1,3)$ and $(2,4)$, a similar argument shows that $\alpha = u_1u_2 + u_3u_4$ is not fixed by these transpositions. So none of the 6 transpositions in S_4 are in $G \setminus V$.

Consider the 3-cycle $\sigma = (1,2,3)$. We have $\sigma(\alpha) = \sigma(u_1u_2 + u_3u_4) = u_2u_3 + u_1u_4$. ASSUME $\sigma(\alpha) = \alpha$. Then $u_1u_2 + u_3u_4 = u_2u_3 + u_1u_4$ or $u_1u_2 - u_1u_4 = u_2u_3 - u_3u_4$ or $u_1(u_2 - u_4) = u_3(u_2 - u_4)$. So either $u_1 = u_3$ or $u_2 = u_4$, both CONTRADICTIONS.

Lemma V.4.9 (continued 1)

Proof (continued). Consider the transposition $\sigma = (1,2)$. We have $\sigma(\beta) = \sigma(u_1u_3 + u_2u_4) = u_2u_3 + u_1u_4$. ASSUME $\sigma(\beta) = \beta$. Then $u_1u_3 + u_2u_4 = u_2u_3 + u_1u_4$ or $u_1u_3 - u_1u_4 = u_2u_3 - u_2u_4$ or $u_1(u_3 - u_4) = u_2(u_3 - u_4)$. So either $u_1 = u_2$ or $u_3 = u_4$, both CONTRADICTIONS. So the assumption is incorrect and we have $\sigma(\beta) \neq \beta$. A similar contradiction results for the other 3 transpositions $(1,4)$, $(2,3)$, and $(3,4)$. For the remaining transpositions, $(1,3)$ and $(2,4)$, a similar argument shows that $\alpha = u_1u_2 + u_3u_4$ is not fixed by these transpositions. So none of the 6 transpositions in S_4 are in $G \setminus V$.

Consider the 3-cycle $\sigma = (1,2,3)$. We have $\sigma(\alpha) = \sigma(u_1u_2 + u_3u_4) = u_2u_3 + u_1u_4$. ASSUME $\sigma(\alpha) = \alpha$. Then $u_1u_2 + u_3u_4 = u_2u_3 + u_1u_4$ or $u_1u_2 - u_1u_4 = u_2u_3 - u_3u_4$ or $u_1(u_2 - u_4) = u_3(u_2 - u_4)$. So either $u_1 = u_3$ or $u_2 = u_4$, both CONTRADICTIONS.

Lemma V.4.9 (continued 2)

Proof (continued). So the assumption is incorrect and we have $\sigma(\alpha) \neq \alpha$. A similar contradiction results for the other 7 3-cycles $(1,3,2)$, $(1,2,4)$, $(1,4,2)$, $(1,3,4)$, $(1,4,3)$, $(2,3,4)$, and $(2,4,3)$. So none of the 8 3-cycles in S_4 are in $G \setminus V$.

Lemma V.4.9 (continued 2)

Proof (continued). So the assumption is incorrect and we have $\sigma(\alpha) \neq \alpha$. A similar contradiction results for the other 7 3-cycles $(1,3,2)$, $(1,2,4)$, $(1,4,2)$, $(1,3,4)$, $(1,4,3)$, $(2,3,4)$, and $(2,4,3)$. So none of the 8 3-cycles in S_4 are in $G \setminus V$.

Consider the 4-cycle $(1,2,3,4)$. We have $\sigma(\alpha) = \sigma(u_1 u_2 + u_3 u_4) = u_2 u_3 + u_4 u_1$. ASSUME $\sigma(\alpha) = \alpha$.

Lemma V.4.9 (continued 2)

Proof (continued). So the assumption is incorrect and we have $\sigma(\alpha) \neq \alpha$. A similar contradiction results for the other 7 3-cycles $(1,3,2)$, $(1,2,4)$, $(1,4,2)$, $(1,3,4)$, $(1,4,3)$, $(2,3,4)$, and $(2,4,3)$. So none of the 8 3-cycles in S_4 are in $G \setminus V$.

Consider the 4-cycle $(1,2,3,4)$. We have $\sigma(\alpha) = \sigma(u_1u_2 + u_3u_4) = u_2u_3 + u_4u_1$. ASSUME $\sigma(\alpha) = \alpha$. Then $u_1u_2 + u_3u_4 = u_2u_3 + u_4u_1$ or $u_1u_2 - u_4u_1 = u_2u_3 - u_3u_4$ or $u_1(u_2 - u_4) = u_3(u_2 - u_4)$. So either $u_1 = u_3$ or $u_2 = u_4$, both CONTRADICTIONS. So the assumption is incorrect and we have $\sigma(\alpha) \neq \alpha$.

Lemma V.4.9 (continued 2)

Proof (continued). So the assumption is incorrect and we have $\sigma(\alpha) \neq \alpha$. A similar contradiction results for the other 7 3-cycles $(1,3,2)$, $(1,2,4)$, $(1,4,2)$, $(1,3,4)$, $(1,4,3)$, $(2,3,4)$, and $(2,4,3)$. So none of the 8 3-cycles in S_4 are in $G \setminus V$.

Consider the 4-cycle $(1,2,3,4)$. We have $\sigma(\alpha) = \sigma(u_1u_2 + u_3u_4) = u_2u_3 + u_4u_1$. ASSUME $\sigma(\alpha) = \alpha$. Then $u_1u_2 + u_3u_4 = u_2u_3 + u_4u_1$ or $u_1u_2 - u_4u_1 = u_2u_3 - u_3u_4$ or $u_1(u_2 - u_4) = u_3(u_2 - u_4)$. So either $u_1 = u_3$ or $u_2 = u_4$, both CONTRADICTIONS. So the assumption is incorrect and we have $\sigma(\alpha) \neq \alpha$. A similar contradiction results for the other 5 4-cycles $(1,2,4,3)$, $(1,3,2,4)$, $(1,3,4,2)$, $(1,4,2,3)$, and $(1,4,3,2)$. So none of the 6 4-cycles in S_4 are in $G \setminus V$.

Lemma V.4.9 (continued 2)

Proof (continued). So the assumption is incorrect and we have $\sigma(\alpha) \neq \alpha$. A similar contradiction results for the other 7 3-cycles $(1,3,2)$, $(1,2,4)$, $(1,4,2)$, $(1,3,4)$, $(1,4,3)$, $(2,3,4)$, and $(2,4,3)$. So none of the 8 3-cycles in S_4 are in $G \setminus V$.

Consider the 4-cycle $(1,2,3,4)$. We have $\sigma(\alpha) = \sigma(u_1 u_2 + u_3 u_4) = u_2 u_3 + u_4 u_1$. ASSUME $\sigma(\alpha) = \alpha$. Then $u_1 u_2 + u_3 u_4 = u_2 u_3 + u_4 u_1$ or $u_1 u_2 - u_4 u_1 = u_2 u_3 - u_3 u_4$ or $u_1(u_2 - u_4) = u_3(u_2 - u_4)$. So either $u_1 = u_3$ or $u_2 = u_4$, both CONTRADICTIONS. So the assumption is incorrect and we have $\sigma(\alpha) \neq \alpha$. A similar contradiction results for the other 5 4-cycles $(1,2,4,3)$, $(1,3,2,4)$, $(1,3,4,2)$, $(1,4,2,3)$, and $(1,4,3,2)$. So none of the 6 4-cycles in S_4 are in $G \setminus V$.

Lemma V.4.9 (continued 3)

Lemma V.4.9. Let K, f, F, u_i, V, and $G = \text{Aut}_K F < S_4$ be as just described. If $\alpha = u_1u_2 + u_3u_4$, $\beta = u_1u_3 + u_2u_4$, $\gamma = u_1u_4 + u_2u_3 \in F$, then under the Galois correspondence of the Fundamental Theorem (Theorem V.2.5) the subfield $K(\alpha, \beta, \gamma)$ corresponds to the normal subgroup $V \cap G$. Hence $K(\alpha, \beta, \gamma)$ is Galois over K and $\text{Aut}_K K(\alpha, \beta, \gamma) \cong G/(G \cap V)$.

Proof (continued). So the fixed field of $G \setminus V$ is $(G \setminus V)' = K(\alpha, \beta, \gamma)$ and $K(\alpha, \beta, \gamma)$ and $K(\alpha, \beta, \gamma)$ corresponds to $G \setminus V$ in the correspondence of the Fundamental Theorem. Since $G \setminus V$ is normal in S_4 (and hence in $G < S_4$), then by part (ii) of the Fundamental Theorem (Theorem V.2.5), $K(\alpha, \beta, \gamma)$ is Galois over K and $\text{Aut}_K K(\alpha, \beta, \gamma) \cong G/(G \cap V)$ (in the notation of the Fundamental Theorem, we have $E = K(\alpha, \beta, \gamma)$ and $E' = G \cap V$). □

Lemma V.4.9 (continued 3)

Lemma V.4.9. Let K, f, F, u_i, V, and $G = \mathrm{Aut}_K F < S_4$ be as just described. If $\alpha = u_1 u_2 + u_3 u_4$, $\beta = u_1 u_3 + u_2 u_4$, $\gamma = u_1 u_4 + u_2 u_3 \in F$, then under the Galois correspondence of the Fundamental Theorem (Theorem V.2.5) the subfield $K(\alpha, \beta, \gamma)$ corresponds to the normal subgroup $V \cap G$. Hence $K(\alpha, \beta, \gamma)$ is Galois over K and $\mathrm{Aut}_K K(\alpha, \beta, \gamma) \cong G/(G \cap V)$.

Proof (continued). So the fixed field of $G \setminus V$ is $(G \setminus V)' = K(\alpha, \beta, \gamma)$ and $K(\alpha, \beta, \gamma)$ and $K(\alpha, \beta, \gamma)$ corresponds to $G \setminus V$ in the correspondence of the Fundamental Theorem. Since $G \setminus V$ is normal in S_4 (and hence in $G < S_4$), then by part (ii) of the Fundamental Theorem (Theorem V.2.5), $K(\alpha, \beta, \gamma)$ is Galois over K and $\mathrm{Aut}_K K(\alpha, \beta, \gamma) \cong G/(G \cap V)$ (in the notation of the Fundamental Theorem, we have $E = K(\alpha, \beta, \gamma)$ and $E' = G \cap V$). $\square$

Lemma V.4.10

Lemma V.4.10. If K is a field and $f = x^4 + bx^3 + cx^2 + dx + e \in K[x]$, then the resolvant cubic of f is the polynomial
$x^3 - cx^2 + (bd - 4e)x - b^2e + 4ce - d^2 \in K[x]$.

Proof. Let f have roots u_1, u_2, u_3, u_4 in some splitting field F (we know F exists by Corollary V.3.7). Since
$f = (x - u_1)(x - u_2)(x - u_3)(x - u_4) \in F[x]$ then
$b = -u_1 - u_2 - u_3 - u_4$, $c = u_1u_2 + u_1u_3 + u_1u_4 + u_2u_3 + u_2u_4 + u_3u_4$,
$d = -u_1u_2u_3 - u_1u_2u_4 - u_1u_3u_4 - u_2u_3u_4$, and $e = u_1u_2u_3u_4$.

Lemma V.4.10

Lemma V.4.10. If K is a field and $f = x^4 + bx^3 + cx^2 + dx + e \in K[x]$, then the resolvant cubic of f is the polynomial
$x^3 - cx^2 + (bd - 4e)x - b^2e + 4ce - d^2 \in K[x]$.

Proof. Let f have roots u_1, u_2, u_3, u_4 in some splitting field F (we know F exists by Corollary V.3.7). Since
$f = (x - u_1)(x - u_2)(x - u_3)(x - u_4) \in F[x]$ then
$b = -u_1 - u_2 - u_3 - u_4$, $c = u_1u_2 + u_1u_3 + u_1u_4 + u_2u_3 + u_2u_4 + u_3u_4$,
$d = -u_1u_2u_3 - u_1u_2u_4 - u_1u_3u_4 - u_2u_3u_4$, and $e = u_1u_2u_3u_4$.

Next, the resolvant cubic is
$(x-\alpha)(x-\beta)(x-\gamma) = x^3+(-\alpha-\beta-\gamma)x^2+(\alpha\beta+\alpha\gamma+\beta\gamma)x+(-\alpha\beta\gamma)$,
and so from the values of α, β, γ in terms of u_1, u_2, u_3, u_4 (in Lemma V.4.9) we have that the resolvant cubic is. . .

Lemma V.4.10

Lemma V.4.10. If K is a field and $f = x^4 + bx^3 + cx^2 + dx + e \in K[x]$, then the resolvant cubic of f is the polynomial
$x^3 - cx^2 + (bd - 4e)x - b^2e + 4ce - d^2 \in K[x]$.

Proof. Let f have roots u_1, u_2, u_3, u_4 in some splitting field F (we know F exists by Corollary V.3.7). Since
$f = (x - u_1)(x - u_2)(x - u_3)(x - u_4) \in F[x]$ then
$b = -u_1 - u_2 - u_3 - u_4$, $c = u_1u_2 + u_1u_3 + u_1u_4 + u_2u_3 + u_2u_4 + u_3u_4$,
$d = -u_1u_2u_3 - u_1u_2u_4 - u_1u_3u_4 - u_2u_3u_4$, and $e = u_1u_2u_3u_4$.

Next, the resolvant cubic is
$(x-\alpha)(x-\beta)(x-\gamma) = x^3+(-\alpha-\beta-\gamma)x^2+(\alpha\beta+\alpha\gamma+\beta\gamma)x+(-\alpha\beta\gamma)$,
and so from the values of α, β, γ in terms of u_1, u_2, u_3, u_4 (in Lemma V.4.9) we have that the resolvant cubic is. . .

Lemma V.4.10 (continued 1)

Proof (continued).

$$x^3 + [-(u_1u_2 + u_3u_4) - (u_1u_3 + u_2u_4) - (u_1u_4 + u_2u_3)]x^2$$

$$+[(u_1u_2 + u_3u_4)(u_1u_3 + u_2u_4) + (u_1u_2 + u_3u_4)(u_1u_4 + u_2u_3)$$

$$+(u_1u_3 + u_2u_4)(u_1u_4 + u_2u_3)]x$$

$$+[-(u_1u_2 + u_3u_4)(u_1u_3 + u_2u_4)(u_1u_4 + u_2u_3)]. \qquad (*)$$

Notice that the coefficient of x^2 in $(*)$ is $-c$, as claimed. We now confirm the other coefficient of $(*)$ are as required in some lengthy calculations.

Lemma V.4.10 (continued 1)

Proof (continued).

$$x^3 + [-(u_1u_2 + u_3u_4) - (u_1u_3 + u_2u_4) - (u_1u_4 + u_2u_3)]x^2$$
$$+[(u_1u_2 + u_3u_4)(u_1u_3 + u_2u_4) + (u_1u_2 + u_3u_4)(u_1u_4 + u_2u_3)$$
$$+(u_1u_3 + u_2u_4)(u_1u_4 + u_2u_3)]x$$
$$+[-(u_1u_2 + u_3u_4)(u_1u_3 + u_2u_4)(u_1u_4 + u_2u_3)]. \qquad (*)$$

Notice that the coefficient of x^2 in $(*)$ is $-c$, as claimed. We now confirm the other coefficient of $(*)$ are as required in some lengthy calculations.

Consider

$$bd - 4e = (-u_1 - u_2 - u_3 - u_4)(-u_1u_2u_3 - u_1u_2u_4 - u_1u_3u_4 - u_2u_3u_4) - 4(u_1u_2u_3u_4)$$

Lemma V.4.10 (continued 1)

Proof (continued).

$$x^3 + [-(u_1u_2 + u_3u_4) - (u_1u_3 + u_2u_4) - (u_1u_4 + u_2u_3)]x^2$$
$$+[(u_1u_2 + u_3u_4)(u_1u_3 + u_2u_4) + (u_1u_2 + u_3u_4)(u_1u_4 + u_2u_3)$$
$$+(u_1u_3 + u_2u_4)(u_1u_4 + u_2u_3)]x$$
$$+[-(u_1u_2 + u_3u_4)(u_1u_3 + u_2u_4)(u_1u_4 + u_2u_3)]. \qquad (*)$$

Notice that the coefficient of x^2 in $(*)$ is $-c$, as claimed. We now confirm the other coefficient of $(*)$ are as required in some lengthy calculations.

Consider

$$\begin{aligned} bd - 4e &= (-u_1 - u_2 - u_3 - u_4)(-u_1u_2u_3 - u_1u_2u_4 - u_1u_3u_4 - u_2u_3u_4) \\ &\quad -4(u_1u_2u_3u_4) \end{aligned}$$

Lemma V.4.10 (continued 2)

Proof (continued).

$$
\begin{aligned}
&= (u_1+u_2+u_3+u_4)(u_1u_2u_3+u_1u_2u_4+u_1u_3u_4+u_2u_3u_4) \\
&\quad -4u_1u_2u_3u_4 \\
&= u_1(u_1u_2u_3+u_1u_2u_4+u_1u_3u_4)+u_2(u_1u_2u_3+u_1u_2u_4+u_2u_3u_4) \\
&\quad +u_3(u_1u_2u_3+u_1u_3u_4+u_2u_3u_4)+u_4(u_1u_2u_4+u_1u_3u_4+u_2u_3u_4) \\
&= u_1u_2(u_1u_3+u_1u_4)+u_1^2u_3u_4+u_2u_1(u_2u_3+u_2u_4)+u_2^2u_3u_4 \\
&\quad u_3u_4(u_1u_3+u_2u_3)+u_1u_2u_3^2+u_4u_3(u_1u_4+u_2u_4)+u_1u_2u_4^2 \\
&= u_1u_2(u_1u_3+u_2u_4+u_1u_4+u_2u_3)+u_3u_4(u_1u_3+u_2u_4+u_1u_4+u_2u_3) \\
&\quad +u_1u_3(u_1u_4+u_2u_3)+u_2u_4(u_1u_4+u_2u_3) \\
&= (u_1u_2+u_3u_4)[(u_1u_3+u_2u_4)+(u_1u_4+u_2u_3)] \\
&\quad +(u_1u_3+u_2u_4)(u_1u_4+u_2u_3)
\end{aligned}
$$

and so the x coefficient in $(*)$ is $bd-4e$.

Lemma V.4.10 (continued 3)

Proof (continued). Finally, $-b^2e + 4ce - d^2$ equals

$$\begin{aligned}
& -(-u_1 - u_2 - u_3 - u_4)^2(u_1u_2u_3u_4) \\
& +4(u_1u_2 + u_1u_3 + u_1u_4 + u_2u_3 + u_2u_4 + u_3u_4)(u_1u_2u_3u_4) \\
& -(-u_1u_2u_3 - u_1u_2u_4 - u_1u_3u_4 - u_2u_3u_4)^2 \\
= \; & -[u_1^2 + 2u_1u_2 + 2u_1u_3 + 2u_1u_4 + u_2^2 + 2u_2u_3 \\
& +2u_2u_4 + u_3^2 + 2u_3u_4 + u_4^2](u_1u_2u_3u_4) \\
& +4(u_1u_2 + u_1u_3 + u_1u_4 + u_2u_3 + u_2u_4 + u_3u_4)(u_1u_2u_3u_4) \\
& -(u_1u_2u_3 + u_1u_2u_4 + u_1u_3u_4 + u_2u_3u_4)^2 \\
= \; & -[u_1^2 - 2u_1u_2 - 2u_1u_3 - 2u_1u_4 + u_2^2 - 2u_2u_3 - 2u_2u_4 + u_3^2 \\
& -2u_3u_4 + u_4^2](u_1u_2u_3u_4) - [u_1^2u_2^2u_3^2 + 2u_1^2u_2^2u_3u_4 \\
& +2u_1^2u_2u_3^2u_4 + 2u_1u_2^2u_3^2u_4 + u_1^2u_2^2u_4^2 + 2u_1^2u_2u_3u_4^2 \\
& +2u_1u_2^2u_3u_4^2 + u_1^2u_3^2u_4^2 + 2u_1u_2u_3^2u_4^2 + u_2^2u_3^2u_4^2]
\end{aligned}$$

Lemma V.4.10 (continued 4)

Proof (continued).

$$\begin{aligned} &= -(u_1^2+u_2^2+u_3^2+u_4^2)(u_1u_2u_3u_4) \\ &\quad -(u_1^2u_2^2u_3^2+u_1^2u_2^2u_4^2+u_1^2u_3^2u_4^2+u_2^2u_3^2u_4^2) \\ &= -[u_1u_2(u_1^2u_3u_4+u_2^2u_3u_4)+u_3u_4(u_1u_2u_3^2+u_1u_2u_4^2)] \\ &\quad -[u_1u_2(u_1u_2u_3^2+u_1u_2u_4^2)+u_3u_4(u_1^2u_3u_4+u_2^2u_3u_4)] \\ &= -(u_1u_2+u_3u_4)[(u_1^2u_3u_4+u_2^2u_3u_4)+(u_1u_2u_3^2+u_1u_2u_4^2)] \\ &= -(u_1u_2+u_3u_4)[u_1u_3(u_1u_4+u_2u_3)+u_2u_4(u_2u_3+u_1u_4)] \\ &= -(u_1u_2+u_3u_4)(u_1u_3+u_2u_4)(u_1u_4+u_2u_3) \end{aligned}$$

and so the constant term in $(*)$ is $-b^2c+4ce-d^2$.

Hence, the resolvant cubic is
$x^3-cx^2+(bd-e)x-b^2e+4ce-d^2 \in K[x]$ as claimed. □

Lemma V.4.10 (continued 4)

Proof (continued).

$$\begin{aligned}
&= -(u_1^2+u_2^2+u_3^2+u_4^2)(u_1u_2u_3u_4) \\
&\quad -(u_1^2u_2^2u_3^2+u_1^2u_2^2u_4^2+u_1^2u_3^2u_4^2+u_2^2u_3^2u_4^2) \\
&= -[u_1u_2(u_1^2u_3u_4+u_2^2u_3u_4)+u_3u_4(u_1u_2u_3^2+u_1u_2u_4^2)] \\
&\quad -[u_1u_2(u_1u_2u_3^2+u_1u_2u_4^2)+u_3u_4(u_1^2u_3u_4+u_2^2u_3u_4)] \\
&= -(u_1u_2+u_3u_4)[(u_1^2u_3u_4+u_2^2u_3u_4)+(u_1u_2u_3^2+u_1u_2u_4^2)] \\
&= -(u_1u_2+u_3u_4)[u_1u_3(u_1u_4+u_2u_3)+u_2u_4(u_2u_3+u_1u_4)] \\
&= -(u_1u_2+u_3u_4)(u_1u_3+u_2u_4)(u_1u_4+u_2u_3)
\end{aligned}$$

and so the constant term in $(*)$ is $-b^2c+4ce-d^2$.

Hence, the resolvant cubic is
$x^3-cx^2+(bd-e)x-b^2e+4ce-d^2 \in K[x]$ as claimed. □

Proposition V.4.11

Proposition V.4.11. Let K be a field and $f \in K[x]$ an irreducible, separable quartic with Galois group G (considered as a subgroup of S_4). Let α, β, γ be the roots of the resolvant cubic of f and let $m = [K(\alpha, \beta, \gamma) : K]$. Then

(i) $m = 6 \Leftrightarrow G = S_4$;

(ii) $m = 3 \Leftrightarrow G = A_4$;

(iii) $m = 1 \Leftrightarrow G = V$;

(iv) $m = 2 \Leftrightarrow G \cong D_4$ or $G \cong \mathbb{Z}_4$; the the case that $G \cong D_4$, if f is irreducible over $K(\alpha, \beta, \gamma)$ and $G \cong \mathbb{Z}_4$.

Proof. Since $K(\alpha, \beta, \gamma)$ is a splitting field over K of a cubic, then by Exercise V.3.5, $m - [K(\alpha, \beta, \gamma) : K]$ divides $3! = 6$ and so can only be 1, 2, 3, or 6. As argued in the note above, the Galois group can only be either S_4, A_4, D_4, V, or $\mathbb{Z}_4$. So the result follows if we can show the $\Leftarrow$ part of the implication (the converse must follow by a process of elimination).

Proposition V.4.11

Proposition V.4.11. Let K be a field and $f \in K[x]$ an irreducible, separable quartic with Galois group G (considered as a subgroup of S_4). Let α, β, γ be the roots of the resolvant cubic of f and let $m = [K(\alpha, \beta, \gamma) : K]$. Then

(i) $m = 6 \Leftrightarrow G = S_4$;

(ii) $m = 3 \Leftrightarrow G = A_4$;

(iii) $m = 1 \Leftrightarrow G = V$;

(iv) $m = 2 \Leftrightarrow G \cong D_4$ or $G \cong \mathbb{Z}_4$; the the case that $G \cong D_4$, if f is irreducible over $K(\alpha, \beta, \gamma)$ and $G \cong \mathbb{Z}_4$.

Proof. Since $K(\alpha, \beta, \gamma)$ is a splitting field over K of a cubic, then by Exercise V.3.5, $m - [K(\alpha, \beta, \gamma) : K]$ divides $3! = 6$ and so can only be 1, 2, 3, or 6. As argued in the note above, the Galois group can only be either S_4, A_4, D_4, V, or $\mathbb{Z}_4$. So the result follows if we can show the $\Leftarrow$ part of the implication (the converse must follow by a process of elimination).

Proposition V.4.11 (continued 1)

Proof (continued). By part (i) of the Fundamental Theorem (Theorem V.2.5(i)), $|\text{Aut}_K K(\alpha, \beta, \gamma)| = [K(\alpha, \beta, \gamma) : K] = m$ and by Lemma V.4.9, $\text{Aut}_K K(\alpha, \beta, \gamma) \cong G/(G \cap V)$, so we have that $m = |G/(G \cap V)|$.

If $G = S_4$, then $G \cap V = V$ and so $m = |G/(G \cap V)| = |G/V| = |G|/|V| = 24/4 = 6$ (by Lagrange's Theorem, Corollary I.4.6) and so (i) follows.

Proposition V.4.11 (continued 1)

Proof (continued). By part (i) of the Fundamental Theorem (Theorem V.2.5(i)), $|\text{Aut}_K K(\alpha, \beta, \gamma)| = [K(\alpha, \beta, \gamma) : K] = m$ and by Lemma V.4.9, $\text{Aut}_K K(\alpha, \beta, \gamma) \cong G/(G \cap V)$, so we have that $m = |G/(G \cap V)|$.

If $G = S_4$, then $G \cap V = V$ and so $m = |G/(G \cap V)| = |G/V| = |G|/|V| = 24/4 = 6$ (by Lagrange's Theorem, Corollary I.4.6) and so (i) follows.

If $G = A_4$, then $G \cap V = V$ (notice from the table in the Note above that each element of of the transitive version of $V \cong \mathbb{Z}_2 \oplus \mathbb{Z}_2$ is an even permutation) and so $m = |G/(G \cap V)| = |G/V| = |G|/|V| = 12/4 = 3$ (by Lagrange's Theorem) and so (ii) follows.

Proposition V.4.11 (continued 1)

Proof (continued). By part (i) of the Fundamental Theorem (Theorem V.2.5(i)), $|\mathrm{Aut}_K K(\alpha,\beta,\gamma)| = [K(\alpha,\beta,\gamma) : K] = m$ and by Lemma V.4.9, $\mathrm{Aut}_K K(\alpha,\beta,\gamma) \cong G/(G \cap V)$, so we have that $m = |G/(G \cap V)|$.

If $G = S_4$, then $G \cap V = V$ and so $m = |G/(G \cap V)| = |G/V| = |G|/|V| = 24/4 = 6$ (by Lagrange's Theorem, Corollary I.4.6) and so (i) follows.

If $G = A_4$, then $G \cap V = V$ (notice from the table in the Note above that each element of of the transitive version of $V \cong \mathbb{Z}_2 \oplus \mathbb{Z}_2$ is an even permutation) and so $m = |G/(G \cap V)| = |G/V| = |G|/|V| = 12/4 = 3$ (by Lagrange's Theorem) and so (ii) follows.

If $G = V$, then $G \cap V = G$ and so $m = |G/(G \cap V)| = |G/G| = |G|/|G| = 4/4 = 1$ (by Lagrange's Theorem) and so (iii) follows.

Proposition V.4.11 (continued 1)

Proof (continued). By part (i) of the Fundamental Theorem (Theorem V.2.5(i)), $|\mathrm{Aut}_K K(\alpha, \beta, \gamma)| = [K(\alpha, \beta, \gamma) : K] = m$ and by Lemma V.4.9, $\mathrm{Aut}_K K(\alpha, \beta, \gamma) \cong G/(G \cap V)$, so we have that $m = |G/(G \cap V)|$.

If $G = S_4$, then $G \cap V = V$ and so $m = |G/(G \cap V)| = |G/V| = |G|/|V| = 24/4 = 6$ (by Lagrange's Theorem, Corollary I.4.6) and so (i) follows.

If $G = A_4$, then $G \cap V = V$ (notice from the table in the Note above that each element of of the transitive version of $V \cong \mathbb{Z}_2 \oplus \mathbb{Z}_2$ is an even permutation) and so $m = |G/(G \cap V)| = |G/V| = |G|/|V| = 12/4 = 3$ (by Lagrange's Theorem) and so (ii) follows.

If $G = V$, then $G \cap V = G$ and so $m = |G/(G \cap V)| = |G/G| = |G|/|G| = 4/4 = 1$ (by Lagrange's Theorem) and so (iii) follows.

Proposition V.4.11 (continued 2)

Proof (continued). If $G \cong D_4$, then we see from the table in the Note above that transitive V is a subgroup of each of the three isomorphic copies of D_4, and so $G \cap V = V$. Hence $m = |G/(G \cap V)| = |G/V| = |G|/|V| = 8/4 = 2$ (by Lagrange's Theorem) and so the first half of (iv) follows.

If $G \cong \mathbb{Z}_4$, then we see from the table in the Note above that transitive V shares two elements with each isomorphic copy of $\mathbb{Z}_4$, and so $|G \cap V| = 2$. Hence $m = |G/(G \cap V)| = |G|/|G \cap V| = 4/2 = 2$ (by Lagrange's Theorem) and so the second half of (iv) follows.

Proposition V.4.11 (continued 2)

Proof (continued). If $G \cong D_4$, then we see from the table in the Note above that transitive V is a subgroup of each of the three isomorphic copies of D_4, and so $G \cap V = V$. Hence $m = |G/(G \cap V)| = |G/V| = |G|/|V| = 8/4 = 2$ (by Lagrange's Theorem) and so the first half of (iv) follows.

If $G \cong \mathbb{Z}_4$, then we see from the table in the Note above that transitive V shares two elements with each isomorphic copy of $\mathbb{Z}_4$, and so $|G \cap V| = 2$. Hence $m = |G/(G \cap V)| = |G|/|G \cap V| = 4/2 = 2$ (by Lagrange's Theorem) and so the second half of (iv) follows.

Now for the remaining claims of part (iv). Hypothesize that either $G \cong D_4$ or $G \cong \mathbb{Z}_4$. Let u_1, u_2, u_3, u_4 be the roots of f is some splitting field F (which exists by Corollary V.3.7). We establish two claims.

Proposition V.4.11 (continued 2)

Proof (continued). If $G \cong D_4$, then we see from the table in the Note above that transitive V is a subgroup of each of the three isomorphic copies of D_4, and so $G \cap V = V$. Hence $m = |G/(G \cap V)| = |G/V| = |G|/|V| = 8/4 = 2$ (by Lagrange's Theorem) and so the first half of (iv) follows.

If $G \cong \mathbb{Z}_4$, then we see from the table in the Note above that transitive V shares two elements with each isomorphic copy of $\mathbb{Z}_4$, and so $|G \cap V| = 2$. Hence $m = |G/(G \cap V)| = |G|/|G \cap V| = 4/2 = 2$ (by Lagrange's Theorem) and so the second half of (iv) follows.

Now for the remaining claims of part (iv). Hypothesize that either $G \cong D_4$ or $G \cong \mathbb{Z}_4$. Let u_1, u_2, u_3, u_4 be the roots of f is some splitting field F (which exists by Corollary V.3.7). We establish two claims.

Proposition V.4.11 (continued 3)

Proof (continued).

Claim 1. If $G \cong D_4$ then f is irreducible over $K(\alpha, \beta, \gamma)$.

Proof of Claim 1. Suppose $G \cong D_4$ so that $G \cap V = V$ (as described above). Since V is a transitive subgroup (as shown in the table in the note above) and $G \cap V = \mathrm{Aut}_{K(\alpha,\beta,\gamma)}F$ (by Lemma V.4.9 and the "Galois correspondence" part of the Fundamental Theorem), there exists for each pair $i \neq j$ $(1 \leq i, j \leq 4)$ a $\sigma \in G \cap V$ which induces an isomorphism implying $K(\alpha, \beta, \gamma)(u_i) \cong K(\alpha, \beta, \gamma)(u_j)$ such that $\sigma(u_i) = u_j$ and $\sigma|_{K(\alpha,\beta,\gamma)}$ is the identity.

Proposition V.4.11 (continued 3)

Proof (continued).

Claim 1. If $G \cong D_4$ then f is irreducible over $K(\alpha, \beta, \gamma)$.

Proof of Claim 1. Suppose $G \cong D_4$ so that $G \cap V = V$ (as described above). Since V is a transitive subgroup (as shown in the table in the note above) and $G \cap V = \mathrm{Aut}_{K(\alpha,\beta,\gamma)} F$ (by Lemma V.4.9 and the "Galois correspondence" part of the Fundamental Theorem), there exists for each pair $i \neq j$ $(1 \leq i, j \leq 4)$ a $\sigma \in G \cap V$ which induces an isomorphism implying $K(\alpha, \beta, \gamma)(u_i) \cong K(\alpha, \beta, \gamma)(u_j)$ such that $\sigma(u_i) = u_j$ and $\sigma|_{K(\alpha,\beta,\gamma)}$ is the identity. Consequently for each $i \neq j$, u_i and $u_j$are rots of the same irreducible polynomial over $K(\alpha, \beta, \gamma)$ by Corollary V.1.9. So polynomial f must be this irreducible polynomial over $K(\alpha, \beta, \gamma)$. We have shown that $G \cong D_4 \Rightarrow f$ is irreducible over $K(\alpha, \beta, \gamma)$. *QED*

Proposition V.4.11 (continued 3)

Proof (continued).

Claim 1. If $G \cong D_4$ then f is irreducible over $K(\alpha,\beta,\gamma)$.

Proof of Claim 1. Suppose $G \cong D_4$ so that $G \cap V = V$ (as described above). Since V is a transitive subgroup (as shown in the table in the note above) and $G \cap V = \mathrm{Aut}_{K(\alpha,\beta,\gamma)}F$ (by Lemma V.4.9 and the "Galois correspondence" part of the Fundamental Theorem), there exists for each pair $i \neq j$ $(1 \leq i,j \leq 4)$ a $\sigma \in G \cap V$ which induces an isomorphism implying $K(\alpha,\beta,\gamma)(u_i) \cong K(\alpha,\beta,\gamma)(u_j)$ such that $\sigma(u_i) = u_j$ and $\sigma|_{K(\alpha,\beta,\gamma)}$ is the identity. Consequently for each $i \neq j$, u_i and $u_j$are rots of the same irreducible polynomial over $K(\alpha,\beta,\gamma)$ by Corollary V.1.9. So polynomial f must be this irreducible polynomial over $K(\alpha,\beta,\gamma)$. We have shown that $G \cong D_4 \Rightarrow f$ is irreducible over $K(\alpha,\beta,\gamma)$. *QED*

Proposition V.4.11 (continued 4)

Proof (continued).

Claim 2. If $G \cong \mathbb{Z}_4$ then f is reducible over $K(\alpha, \beta, \gamma)$.

Proof of Claim 2. Suppose $G \cong \mathbb{Z}_4$. Then $|G \cap V| = 2$ as argued above. In addition, we see from the table in the Note above, this group of order 2 is not transitive. Now $G \cap V = \mathrm{Aut}K(\alpha, \beta, \gamma)F$ (as justified in Claim 1). Hence: for some $i \neq j$ there is no $\sigma \in G \cap V$ such that $\sigma(u_i) = u_j$ $(*)$

Proposition V.4.11 (continued 4)

Proof (continued).

Claim 2. If $G \cong \mathbb{Z}_4$ then f is reducible over $K(\alpha, \beta, \gamma)$.

Proof of Claim 2. Suppose $G \cong \mathbb{Z}_4$. Then $|G \cap V| = 2$ as argued above. In addition, we see from the table in the Note above, this group of order 2 is not transitive. Now $G \cap V = \mathrm{Aut}K(\alpha, \beta, \gamma)F$ (as justified in Claim 1). Hence: for some $i \neq j$ there is no $\sigma \in G \cap V$ such that $\sigma(u_i) = u_j$ $(*)$

Now F is a splitting field over $J(\alpha, \beta, \gamma)(u_i)$ and over $K(\alpha, \beta, \gamma)(u_j)$ (since F is a splitting field of f over K). ASSUME f is irreducible over $K(\alpha, \beta, \gamma)$. Then by Corollary V.1.9 there is an isomorphism σ' of fields $K(\alpha, \beta, \gamma)(u_i) \cong K(\alpha, \beta, \gamma)(u_j)$ which sends u_i to u_j and is the identity on $K(\alpha, \beta, \gamma)$.

Proposition V.4.11 (continued 4)

Proof (continued).

Claim 2. If $G \cong \mathbb{Z}_4$ then f is reducible over $K(\alpha, \beta, \gamma)$.

Proof of Claim 2. Suppose $G \cong \mathbb{Z}_4$. Then $|G \cap V| = 2$ as argued above. In addition, we see from the table in the Note above, this group of order 2 is not transitive. Now $G \cap V = \text{Aut}K(\alpha, \beta, \gamma)F$ (as justified in Claim 1). Hence: for some $i \neq j$ there is no $\sigma \in G \cap V$ such that $\sigma(u_i) = u_j$ $(*)$ Now F is a splitting field over $J(\alpha, \beta, \gamma)(u_i)$ and over $K(\alpha, \beta, \gamma)(u_j)$ (since F is a splitting field of f over K). ASSUME f is irreducible over $K(\alpha, \beta, \gamma)$. Then by Corollary V.1.9 there is an isomorphism σ' of fields $K(\alpha, \beta, \gamma)(u_i) \cong K(\alpha, \beta, \gamma)(u_j)$ which sends u_i to u_j and is the identity on $K(\alpha, \beta, \gamma)$. By Theorem V.3.8, σ' is extendible to an automorphism of F, say $\sigma \in \text{Aut}_{K(\alpha,\beta,\gamma)}F$. But then for this $\sigma \in G \cap V$ we have $\sigma(u_i) = u_j$, CONTRADICTING $(*)$. So the assumption is false and we have that f is reducible. We have shown that $G \cong \mathbb{Z}_4 \Rightarrow f$ is reducible over $K(\alpha, \beta, \gamma)$. *QED*

Proposition V.4.11 (continued 4)

Proof (continued).
Claim 2. If $G \cong \mathbb{Z}_4$ then f is reducible over $K(\alpha, \beta, \gamma)$.
Proof of Claim 2. Suppose $G \cong \mathbb{Z}_4$. Then $|G \cap V| = 2$ as argued above. In addition, we see from the table in the Note above, this group of order 2 is not transitive. Now $G \cap V = \mathrm{Aut}K(\alpha, \beta, \gamma)F$ (as justified in Claim 1). Hence: for some $i \neq j$ there is no $\sigma \in G \cap V$ such that $\sigma(u_i) = u_j$ $(*)$
Now F is a splitting field over $J(\alpha, \beta, \gamma)(u_i)$ and over $K(\alpha, \beta, \gamma)(u_j)$ (since F is a splitting field of f over K). ASSUME f is irreducible over $K(\alpha, \beta, \gamma)$. Then by Corollary V.1.9 there is an isomorphism σ' of fields $K(\alpha, \beta, \gamma)(u_i) \cong K(\alpha, \beta, \gamma)(u_j)$ which sends u_i to u_j and is the identity on $K(\alpha, \beta, \gamma)$. By Theorem V.3.8, σ' is extendible to an automorphism of F, say $\sigma \in \mathrm{Aut}_{K(\alpha,\beta,\gamma)}F$. But then for this $\sigma \in G \cap V$ we have $\sigma(u_i) = u_j$, CONTRADICTING $(*)$. So the assumption is false and we have that f is reducible. We have shown that $G \cong \mathbb{Z}_4 \Rightarrow f$ is reducible over $K(\alpha, \beta, \gamma)$.
QED

Proposition V.4.11 (continued 5)

Proposition V.4.11. Let K be a field and $f \in K[x]$ an irreducible, separable quartic with Galois group G (considered as a subgroup of S_4). Let α, β, γ be the roots of the resolvant cubic of f and let $m = [K(\alpha, \beta, \gamma) : K]$. Then

(i) $m = 6 \Leftrightarrow G = S_4$;

(ii) $m = 3 \Leftrightarrow G = A_4$;

(iii) $m = 1 \Leftrightarrow G = V$;

(iv) $m = 2 \Leftrightarrow G \cong D_4$ or $G \cong \mathbb{Z}_4$; the the case that $G \cong D_4$, if f is irreducible over $K(\alpha, \beta, \gamma)$ and $G \cong \mathbb{Z}_4$.

Proof (continued). So in case (iv) we have that either $G \cong D_4$ or $G \cong \mathbb{Z}_4$. We have shown that $G \cong D_4 \Rightarrow f$ is irreducible, and $G \cong \mathbb{Z}_4 \Rightarrow f$ is reducible. These are the converses of the additional claims in (iv), but by the process of elimination, the original claims follow. □