Section V.4. The Galois Group of a Polynomial (Supplement)

Note. In this supplement to the Section V.4 notes, we present the results from Corollary V.4.3 to Proposition V.4.11 and some examples which use these results. These results are rather specialized in that they will allow us to classify the Galois group of a 2nd degree polynomial (Corollary V.4.3), a 3rd degree polynomial (Corollary V.4.7), and a 4th degree polynomial (Proposition V.4.11). In the event that we are low on time, we will only cover the main notes and skip this supplement. However, most of the exercises from this section require this supplemental material.

Note. The results in this supplement deal primarily with polynomials all of whose roots are distinct in some splitting field (and so the irreducible factors of these polynomials are separable [by Definition V.3.10, only irreducible polynomials are separable]). By Theorem V.3.11, the splitting field F of such a polynomial $f \in K[x]$ is Galois over K. In Exercise V.4.1 it is shown that if the Galois group of such polynomials in $K[x]$ can be calculated, then it is possible to calculate the Galois group of an arbitrary polynomial in $K[x]$.

Note. As shown in Theorem V.4.2, the Galois group G of $f \in K[x]$ is isomorphic to a subgroup of some symmetric group S_n (where $G = \text{Aut}_K F$ for $F = K(u_1, u_2, \ldots, u_n)$ where the roots of f are $u_1, u_2, \ldots, u_n$). Notationally, we do not distinguish between G and the subgroups of S_n (such as A_n), so we treat the elements of G as elements of S_n.

Note. The following result classifies the Galois group of 2nd degree polynomials in terms of the polynomial's separability (and the characteristic of the field).

Corollary V.4.3. The Galois Group of a Degree 2 Polynomial.
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 $G = \{\iota\} = 1$.

Note. For f a degree 3 irreducible, separable polynomial, Theorem V.4.2(ii) implies that the Galois group is a transitive subgroup of S_3. Since $|S_3| = 6$, a proper subgroup of S_3 must have order 1, 2, or 3. A subgroup of order 1 or 2 cannot be transitive. The only subgroup of order 3 is $A_3 \cong \mathbb{Z}_3$, which is transitive. So the only transitive subgroups of S_3 are S_3 itself and $A_3 \cong \mathbb{Z}_3$. Hence, the only possible Galois group for an irreducible, separable degree 3 polynomial is either S_3 or A_3. In order to determine which of these is the Galois group for a given degree 3 polynomial, we need more equipment.

Definition V.4.4. Let K be a field with $\text{char}(K) \neq 2$ and $f \in K[x]$ a polynomial of degree n with n distinct roots $u_1, u_2, \ldots, u_n$ is some splitting field F of f over K. Let $\Delta = \prod_{i<j}(u_i - u_j) = (u_1 - u_2)(u_1 - u_3)\cdots(u_{n-1} - u_n) \in F$. The *discriminant* of f is the element $D = \Delta^2 \in F$. (Some texts include a factor of a_n^{2n-2} in D, where f is degree n with x^n coefficient of a_n. We'll discuss this more below.)

Note. From classical algebra (with $K = \mathbb{R}$) you are familiar with the "discriminant" of the quadratic equation: $ax^2 + bx + c = 0$ implies $x = \dfrac{-b \pm \sqrt{b^2 - 4ac}}{2a}$ and the "discriminant" is $D = b^2 - 4ac$. If $a = 1$ (so the polynomial is monic) and the zeros of the polynomial are $u_1, u_2 \in \mathbb{C}$, then $x^2 + bx + c = (x - u_1)(x - u_2) = x^2 + (-u_1 - u_2)x + u_1u_2$ and we have $D = b^2 - 4ac = (-u_1 - u_2)^2 - 4(u_1u_2) = (u_1 - u_2)^2$ and $\Delta = (u_1 - u_2)$.

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, $\sigma(\Delta) = -\Delta$).

Corollary V.4.6. Let K, f, F, Δ be as in Definition V.4.4 (so that F is Galois over K) and consider $G = \mathrm{Aut}_K F$ as a subgroup of S_n. In the Galois correspondence (Theorem V.2.5) the subfield $K(\Delta)$ corresponds to the subgroup $G \cap A_n$. In particular, G consists of even permutations if and only if $\Delta \in K$.

Note. We leave the proof of Corollary V.4.6 as homework. We now have the equipment to deal with determining the Galois group of an irreducible, separable polynomial of degree 3.

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.

Note. If $K = \mathbb{R}$ then the sign of the discriminant determines how many real roots of degree 3 polynomial f has, as shown in Exercise V.4.2. The following is useful in determining whether or not the discriminant of f is a square of some element of K.

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 $-4p^3 - 27q^2$.

Note. In the proof of Proposition V.4.8, we see that the discriminant of $f = x^3 + bx^2 + cx + d$ is $-4p^3 - 27q^2$ where $p = -b^2/3 + c$ and $q = 2b^3/27 - bc/3 + d$. So in terms of b, c, d, the discriminant of f is

$$D = \Delta^2 = -4p^3 - 27q^2 = -4(-b^2/3 + c)^3 - 27(2b^3/27 - bc/3 + d)^2$$

$$= b^2c^2 - 4c^3 - 4b^3d - 27d^2 + 18bcd. \qquad (1)$$

Now the polynomial $ax^3 + bx^2 + cx + d$ has the same roots (and so the same discriminant) as $x^3 + (b/a)x^2 + (c/a)x + (d/a)$. Replacing b with b/a, c with c/a,

and d with d/a in (1) gives that the discriminant of $ax^3 + bx^2 + cx + d$ is

$$b^2c^2/a^4 - 4c^3/a^3 - 4b^3d/a^4 - 27d^2/a^2 + 18bcd/a^3$$

$$= a^{-4}(b^2c^2 - 4ac^3 - 4b^3d - 27a^2d^2 + 18abcd).$$

Some texts define the discriminant of a *monic* polynomial using Hungerford's definition, but for a nonmonic polynomial, say the polynomial is degree n with coefficient a_n of x^n add a multiple of a_n^{2n-2} (which of course is a perfect square of an element in K, namely a_n^{n-1}); see Dummit and Foote's *Abstract Algebra*, Third Edition, John Wiley and Sons (2004), the footnote on page 610. With this definition, the discriminant of $ax^3 + bx^2 + cx + d$ is $b^2c^2 - 4ac^3 - 4b^3d - 27a^2d^2 + 18abcd$. You may see this quoted as the discriminant of a cubic in some other references. Since this value differs from Hungerford's value by a factor of a perfect square, this changes none of the results concerning the Galois group of a polynomial.

Example. Consider $f = x^3 - 3x + 1 \in \mathbb{Q}[x]$. By Proposition III.6.8 (with $C = \mathbb{Z}$ and $F = \mathbb{Q}$), the only possible rational roots of f are ± 1, but neither of these is a root, so f has no rational roots. Since$f$ is degree 3, if it factors in $\mathbb{Q}[x]$ then one of the factors would have to be a linear term in $\mathbb{Q}[x]$, but linear terms in $\mathbb{Q}[x]$ correspond to roots in $\mathbb{Q}$ by the Factor Theorem (Theorem III.6.6). So f does not factor in $\mathbb{Q}[x]$ and f is irreducible in $\mathbb{Q}[x]$. Now $f' = 3x^2 - 3$ is not the zero polynomial, so by Theorem III.6.10(iii), f has no multiple roots, so f is separable. Since f is an irreducible, separable degree 3 polynomial, we apply Corollary V.4.7. The discriminant of f (with $a = 1$, $b = 0$, $c = -3$, and $d = 1$ in Equation (1)) is $(0)^2(-3)^2 - 4(-3)^3 - 4(0)^3(1) - 27(1)^2 + 18(0)(-3)(1) = 81$. Since 81 is a square of $9 \in \mathbb{Q}$, then the Galois group of f is A_3.

Example. If $f(x) = x^3 + 3x^2 - x - 1 \in \mathbb{Q}[x]$, then $g(x) = f(x - 3/3) = f(x - 1) = x^3 - 4x + 2$. Now g is irreducible over $\mathbb{Q}$ by the Eisenstein Criterion (Theorem III.6.15, with $p = 2$), and so f is also irreducible over $\mathbb{Q}$. Now $f' = 3x^2 + 6x - 1$ is not the zero polynomial, so by Theorem III.6.10(iii), f has no multiple roots, so f is separable. The discriminant of f (with $a = 1$, $b = 3$, $c = -1$, and $d = -1$ is in Equation (1)) is $(3)^2(-1)^2 - 4(-1)^3 - 4(3)^3(-1) - 27(-1)^2 + 18(3)(-1)(-1) = 148$. Since 148 is not a square of some element of $\mathbb{Q}$ (since $\sqrt{148} = 2\sqrt{37}$) then by Corollary V.4.7, the Galois group of f is S_2. (Notice that we only used g to show the irreducibility of f; we could have computed the discriminant of g instead of the discriminant of f, as Hungerford does, since f and g have the same determinant. We still need to show the separability of f, which Hungerford omits, to use Corollary V.4.7.)

Note. We now consider degree 4 polynomials (i.e., "quartics"). We let $f \in K[x]$ be a separable quartic with distinct roots u_1, u_2, u_3, u_4 and splitting field $F = K(u_1, u_2, u_3, u_4)$. By Theorem V.3.11 (the (ii)⇒(i) part), F is Galois over K and elements of the Galois group of f, $\text{Aut}_K F$, are determined by their behavior on u_1, u_2, u_3, u_4. So notationally, we treat the elements of $\text{Aut}_K F$ as elements of S_4 (see Theorem V.4.2(ii)). Now the Klein-4 group $V = \{(1), (1,2)(3,4), (1,3)(2,4), (1,4)(2,3)\}$ is normal in S_4 by Exercise I.6.7 and we will see that V arises in this discussion.

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 $\text{Aut}_K K(\alpha, \beta, \gamma) \cong G/(G \cap V)$.

Definition. Let K, f, F, u_i, and α, β, γ be as in Lemma V.4.9. The polynomial $(x - \alpha)(x - \beta)(x - \gamma) \in K(\alpha, \beta, \gamma)[x]$ is the *resolvant cubic* of f.

Note. The next result shows that the resolvant cubic is actually in $K[x]$.

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 $x^3 - cx^2 + (bd - 4e)x - b^2e + 4ce - d^2 \in K[x]$.

Note. We are almost ready to address the Galois group of any irreducible, separable quartic. We need a little more knowledge concerning S_4. By Theorem V.4.2(ii), the Galois group G of a quartic is a transitive subgroup of S_4 with order a multiple of 4. So the subgroup of S_4 must be of order 24 (in which case $G = S_4$), 12, 8, or 4.

Note. With the standard notation for S_4 (though we suppress the commas within the cycles) we can verify that the following are the only subgroups of S_4 of the relevant orders (see `http://users.math.yale.edu/~auel/courses/370f06/docs/solutions5.pdf`):

Order	**Elements**	$\cong$	**Transitive**
12	$\{(1),(12)(34),(13)(24),(14)(23),(123),(132),$ $(124),(142),(134),(143),(234),(243)\}$	A_4	Yes
8	$\{(1),(12),(34),(12)(34),(13)(24),(14)(23),(1324),(1423)\}$	D_4	Yes
8	$\{(1),(13),(24),(13)(24),(12)(34),(14)(23),(1234),(1432)\}$	D_4	Yes
8	$\{(1),(14),(23),(14)(23),(12)(34),(13)(24),(1243),(1342)\}$	D_4	Yes
4	$\{(1),(12),(34),(12)(34)\}$	$\mathbb{Z}_2 \oplus \mathbb{Z}_2$	No
4	$\{(1),(13),(24),(13)(24)\}$	$\mathbb{Z}_2 \oplus \mathbb{Z}_2$	No
4	$\{(1),(14),(23),(14)(23)\}$	$\mathbb{Z}_2 \oplus \mathbb{Z}_2$	No
4	$\{(1),(12)(34),(13)(24),(14)(23)\}$	$V \cong \mathbb{Z}_2 \oplus \mathbb{Z}_2$	Yes
4	$\{(1),(1324),(12)(34),(1423)\}$	$\mathbb{Z}_4$	Yes
4	$\{(1),(1234),(13)(24),(1432)\}$	$\mathbb{Z}_4$	Yes
4	$\{(1),(1243),(14)(23),(1342)\}$	$\mathbb{Z}_4$	Yes

So the only possible Galois groups for a quartic are (up to isomorphism) S_4, A_4, D_4, $V \cong \mathbb{Z}_2 \oplus \mathbb{Z}_2$, or $\mathbb{Z}_4$.

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 $G \cong \mathbb{Z}_4$.

Note. We now illustrate Proposition V.4.11 with some examples.

Example. Consider $f = x^4 + 4x^2 + 2 \in \mathbb{Q}[x]$. Then f is irreducible in $\mathbb{Q}[x]$ by Eisenstein's Criterion (Theorem III.6.15, with $p = 2$). Since $f' = 3x^2+8x$ is not the zero polynomial then by Theorem III.6.10(iii), f has no multiple roots in a splitting field of F and so f is separable. In the notation of Lemma V.4.10, $b = 0$, $c = 4$, $d = 0$, and $e = 2$, so the resolvant cubic is $x^3 - cx^2 + (bd - 4e)x - b^2e + 4ce - d^2 = x^3 - 4x^2 - 8x + 32 = (x - 4)(x^2 - 8)$, we take $\alpha =$, $\beta = \sqrt{8}$, $\gamma = -\sqrt{8}$. Then $\mathbb{Q}(\alpha, \beta, \gamma) = \mathbb{Q}(\sqrt{8}) = \mathbb{Q}[\sqrt{2})$ and so $m = [\mathbb{Q}(\alpha, \beta, \gamma) : \mathbb{Q}] = [\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$. So the Galois group of f is isomorphic to either D_4 or $\mathbb{Z}_4$. By Proposition V.4.11(iv) we need to determine if f is irreducible or not over $\mathbb{Q}(\alpha, \beta, \gamma) = \mathbb{Q}(\sqrt{2})$. Since f is a quadratic in x^2, we can find the four roots of f (in $\mathbb{C}$) and we find that the roots are $\pm\sqrt{-2 \pm \sqrt{2}} \in \mathbb{R} \subset \mathbb{C}$. So we have

$$f = (x - \sqrt{-2 + \sqrt{2}})(x + \sqrt{-2 + \sqrt{2}})(x - \sqrt{-2 - \sqrt{2}})(-2 + \sqrt{-2 - \sqrt{2}})$$

$$= (x^2 - (-2 + \sqrt{2}))(x^2 - (-2 - \sqrt{2}))$$

and f is reducible in $\mathbb{Q}(\sqrt{2})$ and so by Proposition V.4.11(iv), the Galois group of f is $G \cong \mathbb{Z}_4$.

Example. Let $f = x^4 - 2 \in \mathbb{Q}[x]$. Then f is irreducible by the Eisenstein Criterion (Theorem III.6.15, with $p = 2$). f has four distinct roots in $\mathbb{C}$, $\sqrt[4]{2}, -\sqrt[4]{2}, \sqrt[4]{2}i, -\sqrt[4]{2}i$, and so f is separable. In the notation of Lemma V.4.10, we have $b = c = d = 0$ and $e = -2$, so the resolvant cubic of f is $x^3 + 8x = x(x^2 + 8) = x(x + \sqrt{8}i)(x - \sqrt{8}i) = x(x + 2\sqrt{2}i)(x - 2\sqrt{2}i)$. So $\mathbb{Q}(\alpha, \beta, \gamma) = \mathbb{Q}(\sqrt{2}i)$ and $m = [\mathbb{Q}(\alpha, \beta, \gamma) : \mathbb{Q}] = [\mathbb{Q}(\sqrt{2}i) : \mathbb{Q}] = 2$. So the Galois group of f is isomorphic to either D_4 or $\mathbb{Z}_4$. By Proposition V.4.11(iv) we need to determine if f is irreducible or not over $\mathbb{Q}(\alpha, \beta, \gamma) = \mathbb{Q}(\sqrt{2}i)$. If f is reducible in $\mathbb{Q}(\sqrt{2}i)$ then f must have either a linear or a quadratic factor in $\mathbb{Q}(\sqrt{2}i)[x]$. None of the roots of f, $\sqrt[4]{2}, -\sqrt[4]{2}, \sqrt[4]{2}i, -\sqrt[4]{2}i$ are in $\mathbb{Q}(\sqrt{2}i)$, so by the Factor Theorem (Theorem III.6.6), f has no linear factors in $\mathbb{Q}(\sqrt{2}i)$. If f can be written as a product of two quadratics, we consider all possible quadratic factors of f:

- $(x - \sqrt[4]{2})(x + \sqrt[4]{2}) = x^2 - \sqrt{2}$ and $(x - \sqrt[4]{2}i)(x + \sqrt[4]{2}) = (x^2 + \sqrt{2})$.
- $(x - \sqrt[4]{2})(x - \sqrt[4]{2}i) = x^2 - (\sqrt[4]{2} + \sqrt[4]{2}i)x + \sqrt{2}i$ and $(x + \sqrt[4]{2})(x + \sqrt[4]{2}i) = x^2 + (\sqrt[4]{2} + \sqrt[4]{2}i)x + \sqrt{2}i$.
- $(x - \sqrt[4]{2})(x + \sqrt[4]{2}i) = x^2 + (-\sqrt[4]{2} + \sqrt[4]{2}i)x - \sqrt{2}i$ and $(x + \sqrt[4]{2})(x - \sqrt[4]{2}i) = x^2 + (\sqrt[4]{2} - \sqrt[4]{2}i)x - \sqrt{2}i$.

Now the elements of $\mathbb{Q}(\sqrt{2}i)$ are of the form $q_1 + q_2\sqrt{2}i$ where $q_1, q_2 \in \mathbb{Q}$ by Theorem V.1.6(v), and since neither $\sqrt{2}$ nor $\sqrt[4]{2}$ are in $\mathbb{Q}(\sqrt{2}i)$ and so none of the possible quadratic factors of f are in $\mathbb{Q}(\sqrt{2}i)$ and hence f is irreducible over $\mathbb{Q}(\sqrt{2}i)$. Therefore by Proposition V.4.11(iv), the Galois group of f is isomorphic to D_4.

Note. Hungerford gives another example of a Galois group. Consider $f = x^4 - 5x^2 + 6 \in \mathbb{Q}[x]$. Notice that f is *not* irreducible in $\mathbb{Q}[x]$ since $f = (x^2 - 2)(x^2 - 3)$ and so Proposition V.4.11 does not apply (though f is separable). Hungerford gives a lengthy explanation (using the Fundamental Theorem, Theorem V.4.2, Corollary V.4.3, Corollary V.1.9, and Exercise I.4.5) showing that the Galois group of f is isomorphic to $\mathbb{Z}_2 \oplus \mathbb{Z}_2$. This is not surprising since the roots of f (in $\mathbb{R}$) are $\pm\sqrt{2}$ and $\pm\sqrt{3}$. So we can take $F = \mathbb{Q}(\sqrt{2}, \sqrt{3})$ as a splitting field of F and then $\text{Aut}_K F = \text{Aut}_{\mathbb{Q}}\mathbb{Q}(\sqrt{2}, \sqrt{3})$ must consist of mappings which are the identity on $\mathbb{Q}$ and map $\sqrt{2}$ to $\pm\sqrt{2}$ and map $\sqrt{3}$ to $\pm\sqrt{3}$. In fact, Fraleigh shows that $\text{Aut}_{\mathbb{Q}}\mathbb{Q}(\sqrt{2}, \sqrt{3})$ in his Example 48.17 (though this is not done before Fraleigh addresses splitting fields and Galois groups).

Note. On page 276 Hungerford comments that "Specific techniques for computing Galois groups of polynomials of degree greater than 4 over arbitrary fields are rather scarce." However, Theorem V.4.12 (return to the notes for this section) gives a technique to find the Galois group of a particular type of general polynomial in $\mathbb{Q}[x]$.

Revised 5/2/2016