GALOIS GROUPS OF CUBICS AND QUARTICS IN ALL CHARACTERISTICS

KEITH CONRAD

1. Introduction

We want to describe Galois groups of separable irreducible cubic and quartic polynomials in characteristic 2. For instance, if F is a field of characteristic 2 and u is transcendental over F, the polynomials $X^3 + uX + u$ and $X^4 + uX + u$ are irreducible in $F(u)[X]$ by Eisenstein's criterion at u. What are their Galois groups over $F(u)$? This is the kind of question we want to answer.

For perspective, we begin by recalling the classical results outside of characteristic 2.

Theorem 1.1. *Let K not have characteristic 2 and $f(X)$ be a separable*[1] *irreducible cubic in $K[X]$. If $\operatorname{disc} f = \square$ in K then the Galois group of $f(X)$ over K is A_3. If $\operatorname{disc} f \neq \square$ in K then the Galois group of $f(X)$ over K is S_3.*

Theorem 1.2. *Let K not have characteristic 2 and*

$$f(X) = X^4 + aX^3 + bX^2 + cX + d$$

be irreducible[2] *in $K[X]$. The Galois group G_f of $f(X)$ over K can be described in terms of whether or not its discriminant is a square in K and whether or not its cubic resolvent*

$$R_3(X) = X^3 - bX^2 + (ac - 4d)X - (a^2d + c^2 - 4bd)$$

factors in $K[X]$, according to Table 1.

$\operatorname{disc} f$	$R_3(X)$ *in* $K[X]$	G_f
$\neq \square$ *in* K	*irreducible*	S_4
$= \square$ *in* K	*irreducible*	A_4
$\neq \square$ *in* K	*reducible*	D_4 *or* $\mathbf{Z}/4\mathbf{Z}$
$= \square$ *in* K	*reducible*	V

Table 1.

The cubic resolvent $R_3(X)$ in Theorem 1.2 has roots $r_1r_2 + r_3r_4$, $r_1r_3 + r_2r_4$, and $r_1r_4 + r_2r_3$, and $\operatorname{disc} R_3 = \operatorname{disc} f$, so when $f(X)$ is separable so is $R_3(X)$. (There is another cubic resolvent for $f(X)$, having roots $(r_1 + r_2)(r_3 + r_4)$, $(r_1 + r_3)(r_2 + r_4)$, and $(r_1 + r_4)(r_2 + r_3)$, whose discriminant is also $\operatorname{disc} f$. We do not use this but it can be found in many treatments of Galois groups of quartics, *e.g.*, [3, p. 614], [4, p. 336] and [6, p. 103].)

Theorem 1.2 does not distinguish between Galois groups D_4 and $\mathbf{Z}/4\mathbf{Z}$. That can be done with the following theorem of Kappe and Warren [5].

[1]This hypothesis is only necessary if K has characteristic 3. Outside of characteristic 3, an irreducible cubic is automatically separable.

[2]Outside of characteristic 2, an irreducible quartic is automatically separable.

Theorem 1.3. *Let K not have characteristic 2 and $f(X)$ be a separable irreducible quartic in $K[X]$ whose discriminant is not a square in K and whose cubic resolvent $R_3(X)$ has a root r' in K. Then $G_f = \mathbf{Z}/4\mathbf{Z}$ if $X^2 + aX + b - r'$ and $X^2 - r'X + d$ split completely over $K(\sqrt{\operatorname{disc} f})$. Otherwise $G_f = D_4$.*

These theorems are all false when K has characteristic 2. How do the proofs break down? The proof of each theorem uses the discriminant to detect when a Galois group contains only even permutations of the roots: this happens if and only if the discriminant is a square. The proof of that relies on the condition $-1 \neq 1$, which is not true in characteristic 2.

There are two roles for the discriminant outside of characteristic 2:

(1) its nonvanishing tells us when a polynomial is separable,
(2) whether or not it is a square in $K^\times$ is related to a Galois group over K being in A_n.

In characteristic 2, (1) is still true while (2) is not. We will use a replacement for the discriminant of a cubic and quartic polynomial to get a version of (2) (that is, a way of deciding when a Galois group is in A_n) that works in characteristic 2, or rather that works in all characteristics by a uniform method.

2. Galois Groups of Cubics in All Characteristics

A separable irreducible cubic polynomial in $K[X]$ has Galois group S_3 or A_3, since these are the only transitive subgroups of S_3. Outside characteristic 2, we can tell these Galois groups apart with the discriminant. Let's review how that works.

The discriminant of a cubic is a construction which, outside of characteristic 2, is A_3-invariant but not S_3-invariant. If we start with $x_1 - x_2$ and apply A_3 to it, we get $x_2 - x_3$ and $x_1 - x_3$. The product of these gives us

$$(x_1 - x_2)(x_1 - x_3)(x_2 - x_3), \tag{2.1}$$

which is A_3-invariant. (We could have added the three differences also to get an A_3-invariant expression, but the sum is 0, which is also S_3-invariant and not useful!) Each transposition in S_3 turns (2.1) into

$$-(x_1 - x_2)(x_1 - x_3)(x_2 - x_3). \tag{2.2}$$

Outside of characteristic 2, when $-1 \neq 1$, (2.1) is A_3-invariant but not S_3-invariant while the *square* of (2.1) is S_3-invariant. The square is the discriminant, and this accounts for the relevance of the discriminant being a square or not in K as the test which distinguishes A_3 and S_3 as the Galois group of a cubic outside of characteristic 2.

In characteristic 2, (2.1) is S_3-invariant. In fact, in characteristic 2 we can write (2.1) as $(x_1 + x_2)(x_1 + x_3)(x_2 + x_3)$, which is visibly symmetric in the x_i's. Substituting the roots of a cubic in characteristic 2 into this product, it will be a polynomial in the coefficients of the cubic and therefore when we square it we see the discriminant of every cubic in characteristic 2 is a square.

To find a uniform test for the Galois group of a cubic to be A_3 in all characteristics, we want an A_3-invariant polynomial in x_1, x_2, x_3 which is not S_3-invariant in all characteristics. We begin with a different expression than $x_1 - x_2$. Starting with $x_1^2x_2$ and acting A_3 on it, we get $x_2^2x_3$ and $x_3^2x_1$. Let's add these together:

$$x_1^2x_2 + x_2^2x_3 + x_3^2x_1. \tag{2.3}$$

This is A_3-invariant, but under every transposition in S_3 it changes into

$$x_2^2x_1 + x_1^2x_3 + x_3^2x_2, \tag{2.4}$$

which is a different polynomial in the x_i's. (If we had multiplied instead of adding, we'd get $x_1^3x_2^3x_3^3$, which is S_3-invariant and thus useless for distinguishing A_3 and S_3.) The sums (2.3) and (2.4) are naturally paired together and will be roots of a common quadratic polynomial in $K[X]$ when we specialize the x_i's to roots r_i of a cubic in $K[X]$.

Theorem 2.1. *Let K be a field and $f(X) = X^3 + aX^2 + bX + c \in K[X]$ have roots r_1, r_2, and r_3 in a splitting field. The numbers*

$$r_1^2r_2 + r_2^2r_3 + r_3^2r_1 \quad \text{and} \quad r_2^2r_1 + r_1^2r_3 + r_3^2r_2 \tag{2.5}$$

are roots of

$$X^2 + (ab - 3c)X + (a^3c + b^3 + 9c^2 - 6abc),$$

which has the same discriminant as $f(X)$.

Proof. Comparing coefficients on both sides of $f(X) = (X - r_1)(X - r_2)(X - r_3)$, we have the relations

$$r_1 + r_2 + r_3 = -a, \quad r_1r_2 + r_1r_3 + r_2r_3 = b, \quad r_1r_2r_3 = -c.$$

Every symmetric polynomial in the r_i's is a polynomial in a, b, and c.

The quadratic polynomial

$$R_2(X) := (X - (r_1^2r_2 + r_2^2r_3 + r_3^2r_1))(X - (r_2^2r_1 + r_1^2r_3 + r_3^2r_2)) \tag{2.6}$$

has linear coefficient

$$-(r_1^2r_2 + r_2^2r_3 + r_3^2r_1 + r_2^2r_1 + r_1^2r_3 + r_3^2r_2) \tag{2.7}$$

and constant term

$$r_1^4r_2r_3 + r_1r_2^4r_3 + r_1r_2r_3^4 + r_1^3r_2^3 + r_2^3r_3^3 + r_1^3r_3^3 + 3r_1^2r_2^2r_3^2, \tag{2.8}$$

which are both S_3-invariant and thus are polynomials in a, b, and c. We want to find those polynomials.

In (2.7), drop the overall sign and collect monomials involving the same r_i's together:

$$r_1r_2(r_1 + r_2) + r_2r_3(r_2 + r_3) + r_1r_3(r_1 + r_3). \tag{2.9}$$

Since $r_1 + r_2 + r_3 = -a$, (2.9) is

$$\begin{aligned} r_1r_2(-a - r_3) + r_2r_3(-a - r_1) + r_1r_3(-a - r_2) &= -a(r_1r_2 + r_1r_3 + r_2r_3) - 3r_1r_2r_3 \\ &= -ab + 3c. \end{aligned}$$

Now put the overall sign back and we get the desired formula for the X-coefficient of $R_2(X)$.

Rewrite (2.8) as

$$r_1r_2r_3(r_1^3 + r_2^3 + r_3^3) + (r_1^3r_2^3 + r_2^3r_3^3 + r_1^3r_3^3) + 3(r_1r_2r_3)^2.$$

This simplifies to

$$-c(r_1^3 + r_2^3 + r_3^3) + (r_1^3r_2^3 + r_2^3r_3^3 + r_1^3r_3^3) + 3c^2. \tag{2.10}$$

Since

$$\begin{aligned} r_1^3 + r_2^3 + r_3^3 &= (r_1 + r_2 + r_3)^3 + 3r_1r_2r_3 - 3(r_1 + r_2 + r_3)(r_1r_2 + r_1r_3 + r_2r_3) \\ &= -a^3 - 3c + 3ab \end{aligned}$$

and similarly

$$r_1^3r_2^3 + r_2^3r_3^3 + r_1^3r_3^3 = b^3 + 3c^2 - 3abc,$$

feeding these into (2.10) gives us the constant term for $R_2(X)$.

The discriminant of $R_2(X)$ is the square of the difference of its roots. The difference is

$$(r_1^2r_2 + r_2^2r_3 + r_3^2r_1) - (r_2^2r_1 + r_1^2r_3 + r_3^2r_2).$$

You can check that this equals $(r_1 - r_2)(r_1 - r_3)(r_2 - r_3)$, so its square is $\operatorname{disc} f$. □

Definition 2.2. When $f(X) \in K[X]$ is a cubic polynomial with roots r_1, r_2, r_3, its *quadratic resolvent* is the polynomial $R_2(X)$ in (2.6).

Theorem 2.1 gives us a formula for for the quadratic resolvent of a cubic polynomial in terms of its coefficients when the cubic is monic.

Since $\operatorname{disc} R_2 = \operatorname{disc} f$, outside of characteristic 2

$$\begin{aligned} \operatorname{disc} f = \square \text{ in } K &\iff R_2(X) \text{ splits completely over } K, \\ \operatorname{disc} f \neq \square \text{ in } K &\iff R_2(X) \text{ is irreducible } K. \end{aligned}$$

In characteristic 2, these equivalences are no longer valid and it is the right side, rather than the left side, which provides the extension of Theorem 1.1 into characteristic 2.

Theorem 2.3. *Let K be a field. A separable irreducible cubic $f(X)$ in $K[X]$ has Galois group over K equal to A_3 if its quadratic resolvent $R_2(X)$ is reducible over K and equal to S_3 if $R_2(X)$ is irreducible over K.*

Proof. Let $f(X)$ have roots r_1, r_2, r_3. Since $\operatorname{disc} R_2 = \operatorname{disc} f \neq 0$, $R_2(X)$ has distinct roots.

By construction, the two roots of $R_2(X)$ are fixed by A_3, so if the Galois group of $f(X)$ over K is A_3 then the roots of $R_2(X)$ lie in K.

Conversely, if $R_2(X)$ has its roots in K, all elements of the Galois group of $f(X)$ over K are even permutations of the r_i's: an odd permutation of the r_i's that belongs to the Galois group would send one root of $R_2(X)$ to the other root but these roots are in K and are distinct, so the Galois group must fix both roots. □

Example 2.4. In Table 2 are some irreducible cubics in $\mathbf{Q}[X]$ and their Galois groups over $\mathbf{Q}$. The Galois groups can be found by Theorem 2.3 or more traditionally by Theorem 1.1.

$f(X)$	$\operatorname{disc} f$	$R_2(X)$	G_f
$X^3 - X - 1$	-23	$X^2 + 3X + 8$	S_3
$X^3 - 3X - 1$	9^2	$(X - 3)(X + 6)$	A_3
$X^3 - 4X - 1$	229	$X^2 + 3X - 55$	S_3
$X^3 - 7X + 7$	7^2	$(X - 14)(X + 21)$	A_3

TABLE 2. Cubic Galois groups over $\mathbf{Q}$

Let's look at examples of Theorem 2.3 in characteristic 2, where Theorem 1.1 doesn't apply. By a linear change of variables, each cubic in characteristic 2 (or, in fact, in all characteristics but 3) can have its quadratic term removed. In that case

$$f(X) = X^3 + bX + c \Longrightarrow R_2(X) = X^2 + cX + (b^3 + c^2). \tag{2.11}$$

If $R_2(X)$ is reducible in $K[X]$ then $G_f = A_3$; otherwise $G_f = S_3$. (This description of G_f for cubics in characteristic 2 is in [2, p. 53].)

Example 2.5. We will use $K = F(u)$, where F is a field of characteristic 2 and u is transcendental over F.

The quadratic resolvent of $X^3 + uX + u$ is $X^2 + uX + u^3 + u^2$, which has no root in $F(u)$: a rational function root would be a factor of u^2, but for degree reasons none work. Therefore the Galois group of $X^3 + uX + u$ over $F(u)$ is S_3.

The polynomial $X^3 + (u^2 + u + 1)X + u^2 + u + 1$ is irreducible over $F(u)$ by Eisenstein's criterion at $u^2 + u + 1$ or at one of its linear factors (if $u^2 + u + 1$ has roots in F). Its quadratic resolvent is reducible in $F(u)[X]$: see Table 3. If r is one root of this cubic then its full set of roots is

$$r, \quad r^2 + ur, \quad r^2 + (u+1)r.$$

$f(X)$	$R_2(X)$	G_f
$X^3 + uX + u$	$X^2 + uX + u^3 + u^2$	S_3
$X^3 + (u^2 + u + 1)X + u^2 + u + 1$	$(X + (u^2 + u + 1)u)(X + (u^2 + u + 1)(u + 1))$	A_3

TABLE 3. Cubic Galois groups over $F(u)$

Outside characteristic 2, the splitting field over K of a separable cubic $f(X)$ in $K[X]$ is $K(r, \sqrt{\operatorname{disc} f})$, where r is a root of $f(X)$. Here is an analogous result in all characteristics. The key idea is to replace $\sqrt{\operatorname{disc} f}$ with a root of the quadratic resolvent of $f(X)$.

Theorem 2.6. *Let $f(X) \in K[X]$ be a separable cubic. The splitting field of $f(X)$ over K is $K(r, \delta)$, where r is a root of $f(X)$ and δ is a root of the quadratic resolvent of $f(X)$.*

Proof. Let $f(X)$ have roots r, r', r''. Since δ is a polynomial in r, r', and r'', given by one of the expressions in (2.5), $K(r, r', r'') \supset K(r, \delta)$, so

$$[K(r, r', r'') : K] \geq [K(r, \delta) : K].$$

Taking cases based on how $f(X)$ and $R_2(X)$ factor over K, we will show these degrees are equal all the time, so the containment of fields implies their equality.

$f(X)$ irreducible and $R_2(X)$ irreducible: Here $[K(r) : K] = 3$ and $[K(\delta) : K] = 2$, so $[K(r, \delta) : K] = 6$. Since $[K(r, r', r'') : K] \leq 6$, we get equality.

$f(X)$ irreducible and $R_2(X)$ reducible: Here $[K(r) : K] = 3$ and $\delta \in K$, so $K(r, \delta) = K(r)$ has degree 3 over K. By Theorem 2.3, $[K(r, r', r'') : K] = 3$.

$f(X)$ reducible and $R_2(X)$ irreducible: A root of $f(X)$ is in K and $[K(\delta) : K] = 2$. Since the roots of $R_2(X)$ are not in K, the roots of $f(X)$ are not all in K. Therefore $f(X)$ has a linear factor and a quadratic irreducible factor in $K[X]$, so $[K(r, r', r'') : K] = 2$. Since

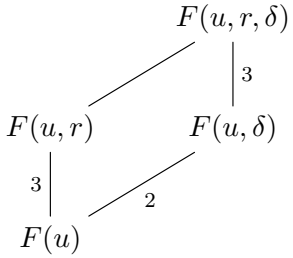
$$K(\delta) \subset K(r, \delta) \subset K(r, r', r'')$$

and the first and last fields have degree 2 over K, $K(r, \delta) = K(r, r', r'')$.

$f(X)$ reducible and $R_2(X)$ reducible: We will show $f(X)$ has all its roots in K, in which case $K(r, r', r'') = K$ and $K(r, \delta) = K$. At least one root of $f(X)$ is in K by hypothesis. If $f(X)$ did not have all of its roots in K then it would have a linear and quadratic irreducible factor in $K[X]$, so its splitting field over K would have degree 2 and its Galois group over K would include a *transposition* on two roots of $f(X)$. If we apply that automorphism to the roots of $R_2(X)$, they are exchanged since each transposition in S_3 sends (2.3) to (2.4) and conversely. However, the roots of $R_2(X)$ are in K by hypothesis and are distinct, so they can't be exchanged by the Galois group of $f(X)$ over K. □

Remark 2.7. Outside of characteristic 2, the quadratic formula says the splitting field of $R_2(X)$ over K is $K(\sqrt{\operatorname{disc} R_2}) = K(\sqrt{\operatorname{disc} f})$. Therefore Theorem 2.6 says the splitting field of $f(X)$ over K is $K(r, \sqrt{\operatorname{disc} f})$, where r is a root of $f(X)$, which recovers the known formula for the splitting field of a cubic outside characteristic 2.

Example 2.8. When F has characteristic 2, the splitting field of $X^3 + uX + u$ over $F(u)$ is $F(u, r, \delta)$, where $r^3 + ur + u = 0$ and $\delta^2 + u\delta + u^3 + u^2 = 0$. By Example 2.5, the field degrees are as in the following diagram.



The extension $F(u, r, \delta)/F(u, \delta)$ is Galois with Galois group A_3. The fields in this A_3-extension can be put into a simpler form. Dividing through the equation $\delta^2+u\delta+u^3+u^2 = 0$ by u^2, we get $(\delta/u)^2 + \delta/u + u + 1 = 0$, so $u = (\delta/u)^2 + \delta/u + 1$. Therefore $F(u, \delta) = F(u, \delta/u) = F(\delta/u)$ and $F(u, r, \delta) = F(\delta/u, r)$. Let $v = \delta/u$, so $u = v^2+v+1$, $F(v, r)/F(v)$ is an A_3-extension, and

$$0 = r^3 + ur + u = r^3 + (v^2 + v + 1)r + v^2 + v + 1.$$

This is a natural way to discover the A_3-cubic from the S_3-cubic in Table 3.

Since $F(u, \delta) = F(v)$ is a rational function field over F, we get an A_3-extension of $F(u)$ if we replace v by u: the polynomial $f(X) = X^3 + (u^2 + u + 1)X + u^2 + u + 1$ is irreducible over $F(u)$ and its Galois group over $F(u)$ is A_3. The quadratic resolvent of $f(X)$ is

$$R_2(X) = (X + (u^2 + u + 1)u)(X + (u^2 + u + 1)(u + 1)),$$

which is reducible, and if r is one root of $f(X)$ then the full set of roots of $f(X)$ is

$$r, \quad r^2 + ur, \quad r^2 + (u + 1)r.$$

3. Galois Groups of Quartics in All Characteristics

To compute the Galois group of a separable irreducible quartic in all characteristics (including characteristic 2), we build on ideas developed in the previous section, only now we're dealing with 4 roots instead of 3 so we're going to meet some longer expressions.

We first recall the list of transitive subgroups of S_4. They are S_4, A_4, 3 conjugate subgroups isomorphic to D_4:

$$\langle(1234), (13)\rangle, \quad \langle(1324), (12)\rangle, \quad \langle(1243), (14)\rangle, \tag{3.1}$$

3 conjugate subgroups isomorphic to $\mathbf{Z}/4\mathbf{Z}$:

$$\langle(1234)\rangle, \quad \langle(1243)\rangle, \quad \langle(1324)\rangle, \tag{3.2}$$

and one subgroup of S_4 isomorphic to V: $\{(1), (12)(34), (13)(24), (14)(23)\}$. (There are other subgroups of S_4 that are isomorphic to V, but they are not transitive and so would not occur as a Galois group.)

We will refer to D_4 and $\mathbf{Z}/4\mathbf{Z}$ as subgroups of S_4, but they are only determined up to conjugation.

Some properties of the transitive subgroups of S_4 are:

- those with order divisible by 3 are A_4 and S_4,
- those inside A_4 are V and A_4,
- those containing a 3-cycle are A_4 and S_4,
- those containing a 4-cycle are $\mathbf{Z}/4\mathbf{Z}$, D_4, and S_4.

To determine when a Galois group is in A_4 or not, we are going to use a quadratic resolvent. It won't be the quadratic resolvent that was used in the cubic case, since our polynomials now have degree 4 and 4 roots. We seek a polynomial in 4 variables x_1, x_2, x_3, x_4 which is A_4-invariant but not S_4-invariant in all characteristics.

Taking our cue from the construction of the quadratic resolvent of a cubic polynomial in Section 2, we start with the asymmetric monomial $x_1^3x_2^2x_3$ and sum its A_4-orbit as an analogue of (2.3):

$$\begin{aligned}\alpha(x_1,x_2,x_3,x_4) &= x_1^3x_2^2x_3 + x_2^3x_3^2x_1 + x_2^3x_4^2x_3 + x_3^3x_2^2x_4 + x_1^3x_3^2x_4 + x_3^3x_1^2x_2 + x_4^3x_1^2x_3 \\ &\quad + x_4^3x_2^2x_1 + x_1^3x_4^2x_2 + x_2^3x_1^2x_4 + x_3^3x_4^2x_1 + x_4^3x_3^2x_2.\end{aligned}$$

This polynomial is A_4-invariant and each transposition of two x_i's turns it into

$$\begin{aligned}\beta(x_1,x_2,x_3,x_4) &= x_2^3x_1^2x_3 + x_1^3x_3^2x_2 + x_1^3x_4^2x_3 + x_3^3x_1^2x_4 + x_2^3x_3^2x_4 + x_3^3x_2^2x_1 + x_4^3x_2^2x_3 \\ &\quad + x_4^3x_1^2x_2 + x_2^3x_4^2x_1 + x_1^3x_2^2x_4 + x_3^3x_4^2x_2 + x_4^3x_3^2x_1.\end{aligned}$$

All transpositions swap $\alpha(x_1,x_2,x_3,x_4)$ and $\beta(x_1,x_2,x_3,x_4)$, so odd permutations in S_4 exchange $\alpha(x_1,x_2,x_3,x_4)$ and $\beta(x_1,x_2,x_3,x_4)$ while even permutations fix $\alpha(x_1,x_2,x_3,x_4)$ and $\beta(x_1,x_2,x_3,x_4)$.

Theorem 3.1. *Let K be a field and $f(X) = X^4 + aX^3 + bX^2 + cX + d \in K[X]$ have roots r_1, r_2, r_3, r_4 in a splitting field. The quadratic polynomial*

$$R_2(X) = (X - \alpha(r_1,r_2,r_3,r_4))(X - \beta(r_1,r_2,r_3,r_4)) \tag{3.3}$$

equals $X^2 + AX + B$, where

$$A = 3a^2d - abc + 3c^2 - 4bd$$

and

$$\begin{aligned}B &= 9a^4d^2 + a^3c^3 - 6a^3bcd + a^2b^3d + 6a^2c^2d - 42a^2bd^2 + 22ab^2cd - 6abc^3 + 48acd^2 \\ &\quad - 4b^4d + b^3c^2 + 36b^2d^2 - 42bc^2d + 9c^4 - 64d^3.\end{aligned}$$

Moreover, $\operatorname{disc} R_2 = \operatorname{disc} f$.

Proof. We abbreviate $\alpha(r_1,r_2,r_3,r_4)$ as α and $\beta(r_1,r_2,r_3,r_4)$ as β. The polynomial

$$(X - \alpha)(X - \beta) = X^2 - (\alpha + \beta)X + \alpha\beta$$

has coefficients which are S_4-invariant, so $-(\alpha+\beta)$ and $\alpha\beta$ are polynomials in the elementary symmetric functions s_1, s_2, s_3, and s_4 of the r_i's. These polynomials can be determined explicitly using an algorithmic proof of the symmetric function theorem. In the case of $-(\alpha+\beta)$, it equals $3s_1^2s_4 - s_1s_2s_3 + 3s_3^2 - 4s_2s_4$. Setting $s_1 = -a$, $s_2 = b$, $s_3 = -c$, and $s_4 = d$, we obtain the formula for A in the theorem. The expression for $\alpha\beta$ as a polynomial in the s_i's is quite long. When it is worked out and we set $s_1 = -a$, $s_2 = b$, $s_3 = -c$, and $s_4 = d$, we get the long formula for B in the theorem.

The discriminant of $R_2(X)$ is $(\alpha - \beta)^2$. A tedious computation by hand or an easy computation on the computer shows

$$\alpha(x_1, x_2, x_3, x_4) - \beta(x_1, x_2, x_3, x_4) = \prod_{i<j}(x_j - x_i),$$

so when we set $x_i = r_i$ and square both sides, we get $\operatorname{disc} R_2 = \operatorname{disc} f$. □

Definition 3.2. When $f(X) \in K[X]$ is a quartic polynomial with roots r_1, r_2, r_3, r_4, its *quadratic resolvent* is the polynomial $R_2(X)$ in (3.3).

Theorem 3.1 gives us a formula for $R_2(X)$ in terms of the coefficients of $f(X)$ if $f(X)$ is monic. If $f(X)$ is separable, so is $R_2(X)$ since $\operatorname{disc} R_2 = \operatorname{disc} f \neq 0$.

When $f(X) = X^4 + bX^2 + cX + d$ has no cubic term, the long formula for $R_2(X)$ "simplifies":

$$R_2(X) = X^2 + 3c^2X - 4b^4d + b^3c^2 + 36b^2d^2 - 42bc^2d + 9c^4 - 64d^3.$$

In characteristic 2, there is a more substantial simplification:

$$R_2(X) = X^2 + c^2X + (b^3 + c^2)c^2. \tag{3.4}$$

Lemma 3.3. *For a field K, the Galois group over K of a separable irreducible quartic in $K[X]$ lies inside of A_4 if and only if its quadratic resolvent splits completely over K.*

Proof. This is the same as the proof of Theorem 2.3, except we replace "Galois group is A_3" with "Galois group is in A_4." □

Along with this quadratic resolvent $R_2(X)$, $f(X)$ also has a cubic resolvent $R_3(X)$, which is the cubic with roots $r_1r_2 + r_3r_4$, $r_1r_3 + r_2r_4$, and $r_1r_4 + r_2r_3$. It appears in Theorem 1.2, but for convenience we recall its formula here, in terms of the coefficients of $f(X)$ when $f(X)$ is monic:

$$R_3(X) = X^3 - bX^2 + (ac - 4d)X - (a^2d + c^2 - 4bd).$$

This simplifies in characteristic 2 to

$$R_3(X) = X^3 + bX^2 + acX + a^2d + c^2,$$

and if $a = 0$ it simplifies even further to

$$R_3(X) = X^3 + bX^2 + c^2. \tag{3.5}$$

The quartic $f(X)$ and its cubic resolvent $R_3(X)$ each have a quadratic resolvent, and we are going to need both quadratic resolvents in our proofs describing G_f. This could lead to a notational conflict: we write $R_2(X)$ for the quadratic resolvent of $f(X)$ in this section, but is $R_2(X)$ also the quadratic resolvent of $R_3(X)$? Not quite, but it will be close enough. From the way the quadratic resolvent of a cubic is constructed in terms of its roots, one root of the quadratic resolvent of $R_3(X)$ is

$$(r_1r_2 + r_3r_4)^2(r_1r_3 + r_2r_4) + (r_1r_3 + r_2r_4)^2(r_1r_4 + r_2r_3) + (r_1r_4 + r_2r_3)^2(r_1r_2 + r_3r_4).$$

Expanding this and assuming without loss of generality that $f(X)$ is monic, this root equals

$$\alpha(r_1, r_2, r_3, r_4) + 2r_1r_2r_3r_4(r_1r_3 + r_2r_4 + r_1r_4 + r_2r_3 + r_1r_2 + r_3r_4) = \alpha(r_1, r_2, r_3, r_4) + 2bd.$$

The other root is $\beta(r_1, r_2, r_3, r_4) + 2bd$, so $R_3(X)$ has quadratic resolvent $R_2(X - 2bd)$. This is generally not $R_2(X)$, although they are equal when K has characteristic 2. The polynomials $R_2(X)$ and $R_2(X - 2bd)$ **have the same splitting field over** K, and it

is the splitting field of quadratic resolvents that really matter, rather than the quadratic resolvents themselves. (For instance, we will see this in the proof of Corollary 3.5.) So for practical purposes we don't have to sweat too much trying to remember if $R_2(X)$ means the quadratic resolvent of $f(X)$ (it does) or $R_3(X)$ (it doesn't).

Here is a version of Theorem 1.2 that is valid in all characteristics.

Theorem 3.4. *Let $f(X) \in K[X]$ be a separable irreducible quartic. The Galois group G_f of $f(X)$ over K can be described in terms of whether or not its quadratic and cubic resolvents factor in $K[X]$, according to Table 4.*

$R_2(X)$ *in* $K[X]$	$R_3(X)$ *in* $K[X]$	G_f
irreducible	*irreducible*	S_4
reducible	*irreducible*	A_4
irreducible	*reducible*	D_4 *or* $\mathbf{Z}/4\mathbf{Z}$
reducible	*reducible*	V

TABLE 4.

Since $\operatorname{disc} R_2 = \operatorname{disc} f$, outside characteristic 2 Theorem 3.4 becomes Theorem 1.2.

Proof. We will check each row of the table in order.

$R_2(X)$ and $R_3(X)$ are irreducible over K: Since $R_2(X)$ is irreducible over K, $G_f \not\subset A_4$ by Lemma 3.3. Since $R_3(X)$ is irreducible over K and its roots are in the splitting field of $f(X)$ over K, adjoining a root of $R_3(X)$ to K gives us a cubic extension of K inside the splitting field of $f(X)$, so $|G_f|$ is divisible by 3. Therefore $G_f = S_4$ or A_4, so $G_f = S_4$.

$R_2(X)$ is reducible and $R_3(X)$ is irreducible over K: We have $G_f \subset A_4$ by Lemma 3.3 and $|G_f|$ is divisible by 3, so $G_f = A_4$.

$R_2(X)$ is irreducible and $R_3(X)$ is reducible over K: Lemma 3.3 tells us G_f is not in A_4, so G_f is S_4, D_4, or $\mathbf{Z}/4\mathbf{Z}$. We will show $G_f \neq S_4$.

What distinguishes S_4 from the other two choices for G_f is that S_4 contains 3-cycles. If $G_f = S_4$ then $(123) \in G_f$. Applying this hypothetical automorphism in the Galois group to the roots of $R_3(X)$ carries them through a single orbit:

$$r_1r_2 + r_3r_4 \mapsto r_2r_3 + r_1r_4 \mapsto r_3r_1 + r_2r_4 \mapsto r_1r_2 + r_3r_4.$$

These numbers are distinct since $R_3(X)$ is separable. At least one root of $R_3(X)$ lies in K, but the G_f-orbit of that root is just itself, not three numbers. We have a contradiction.

$R_2(X)$ and $R_3(X)$ are reducible over K: The group G_f lies in A_4, so $G_f = V$ or $G_f = A_4$. We want to eliminate the second choice. As in the previous case, we can distinguish V from A_4 using 3-cycles. There are 3-cycles in A_4 but not in V. If there were a 3-cycle on the roots of $f(X)$ in G_f then applying it to a root of $R_3(X)$ shows all the roots of $R_3(X)$ are in a single G_f-orbit, which is a contradiction since a root of $R_3(X)$ in K is its own G_f-orbit. Thus G_f contains no 3-cycles. □

Corollary 3.5. *With notation as in Theorem 3.4, $G_f = V$ if and only if $R_3(X)$ splits completely over K and $G_f = D_4$ or $\mathbf{Z}/4\mathbf{Z}$ if and only if $R_3(X)$ has a unique root in K.*

Proof. The condition for G_f to be V is that $R_2(X)$ and $R_3(X)$ are reducible in $K[X]$. The condition for G_f to be D_4 or $\mathbf{Z}/4\mathbf{Z}$ is that $R_2(X)$ is irreducible in $K[X]$ and $R_3(X)$ is reducible in $K[X]$. Since the quadratic resolvent of $R_3(X)$ has the same splitting field over K as $R_2(X)$, the formula for the splitting field of a cubic in Theorem 2.6 ends the proof. □

Example 3.6. Let K be a field and assume $f(X) = X^4+aX^3+bX^2+aX+1$ is irreducible in $K[X]$. It is separable if K doesnt have characteristic 2, or if K has characteristic 2 and a and b are nonzero since the discriminant of $f(X)$ in characteristic 2 is a^4b^2. (Alternatively, in characteristic 2 we have $f'(X) = aX^2 + a = a(X+1)^2$ and $f(1) = b$, so $f(X)$ and $f'(X)$ have no common factor if and only if a and b are nonzero.) Assuming $f(X)$ is separable, what is its Galois group over K?

The polynomial is reciprocal: $X^4 f(1/X) = f(X)$. So the roots of $f(X)$ come in reciprocal pairs (a root is not its own reciprocal since ± 1 are not roots by irreducibility), which implies the splitting field of $f(X)$ over K has degree 4 or 8. Therefore G_f is V, $\mathbf{Z}/4\mathbf{Z}$, or D_4.

The possible Galois groups can also be found from the cubic resolvent of $f(X)$, which is

$$R_3(X) = X^3 - bX^2 + (a^2-4)X - (2a^2-4b) = (X-2)(X^2-(b-2)X+a^2-2b). \tag{3.6}$$

Since this is reducible, the last two rows of Table 4 tell us the possible Galois groups.

By Corollary 3.5, the Galois group is V if and only if $R_3(X)$ splits completely over K.

To illustrate Theorem 3.4, we will use base field $K = F(u)$, where F has characteristic 2 and u is transcendental over F. In characteristic 2, if $f(X) = X^4 + bX^2 + cX + d$ (no cubic term), it is separable if and only if $c \neq 0$, its quadratic resolvent is in (3.4), and its cubic resolvent is in (3.5). Since $R_2(X)$ and $R_3(X)$ have degree 2 and 3, to prove their irreducibility over a field it is enough to show they have no root in the field. Table 5 summarizes all the Galois group computations we will make in characteristic 2 (ω is a nontrivial cube root of unity).

Example	$f(X)$	Condition on F	G_f
3.7	$X^4 + uX + u$	$\omega \in F$	A_4
3.7	$X^4 + uX + u$	$\omega \notin F$	S_4
3.8	$X^4 + uX^2 + uX + u$	none	S_4
3.9	$X^4 + (u^2+u+1)X^2 + X + 1$	none	A_4
3.10, 3.15	$X^4 + (u+1)X^2 + uX + 1$	none	D_4
3.11, 3.16	$X^4 + (u^2+u)X^2 + u^2X + u$	none	$\mathbf{Z}/4\mathbf{Z}$
3.12	$X^4 + (u^2+u+1)X^2 + (u^2+u)X + 1$	none	V

TABLE 5. Galois groups over $F(u)$, char $F = 2$

Example 3.7. Let $f(X) = X^4 + uX + u$, which is irreducible over $F(u)$ by Eisenstein's criterion. You might anticipate, by analogy to Example 2.5, that $G_f = S_4$, but we'll see that is not always true.

The quadratic and cubic resolvents of $f(X)$ are

$$R_2(X) = X^2 + u^2X + u^4 \quad \text{and} \quad R_3(X) = X^3 + u^2.$$

The cubic resolvent is irreducible over $F(u)$. We can write $R_2(X) = u^4(Y^2+Y+1)$, where $Y = X/u^2$. Roots of Y^2+Y+1 are nontrivial cube roots of unity, and if there is one in $F(u)$ then it must be in F. If F contains a nontrivial cube root of unity, then $R_2(X)$ is reducible and $G_f = A_4$. Otherwise $G_f = S_4$. So $G_f = S_4$ if $F = \mathbf{F}_2$ and $G_f = A_4$ if $F = \mathbf{F}_4$.

More generally, if $\pi(u)$ is irreducible in $F[u]$ then the Galois group of $X^4 + \pi(u)X + \pi(u)$ over $F(u)$ is S_4 if F has no nontrivial cube roots of unity and is A_4 otherwise. By contrast

[5, p. 136], if p is a prime number then the Galois group of X^4+pX+p over $\mathbf{Q}$ is S_4 unless $p = 3$ or 5, in which case the Galois group is D_4 or $\mathbf{Z}/4\mathbf{Z}$, respectively.

Example 3.8. If $f(X) = X^4+uX^2+uX+u$, which is irreducible over $F(u)$ by Eisenstein's criterion, its quadratic and cubic resolvents are

$$R_2(X) = X^2 + u^2X + u^4 + u^5 \quad \text{and} \quad R_3(X) = X^3 + uX^2 + u^2.$$

By degree considerations there is no root for $R_2(X)$ or $R_3(X)$ in $F(u)$, except $R_3(X)$ might have a linear root of the form au for some $a \in F$. Since

$$R_3(au) = a^2(a+1)u^3 + u^2,$$

which is not 0, $R_3(X)$ is irreducible in $F(u)[X]$. Therefore the Galois group of $f(X)$ over $F(u)$ is S_4.

Example 3.9. Let $f(X) = X^4 + (u^2+u+1)X^2 + X + 1$. It is left to the reader to check this is irreducible over $F(u)$. Its quadratic and cubic resolvents are

$$R_2(X) = X^2 + X + u^2 + u = (X+u)(X+u+1)$$

and

$$R_3(X) = X^3 + (u^2+u+1)X^2 + 1.$$

The cubic resolvent is irreducible over $F(u)$, so $G_f = A_4$.

Example 3.10. Let $f(X) = X^4 + (u+1)X^2 + uX + 1$. It is left to the reader to check $f(X)$ is irreducible over $F(u)$. Its quadratic and cubic resolvents are

$$R_2(X) = X^2 + u^2X + u^5 + u^3 + u^2$$

and

$$R_3(X) = X^3 + (u+1)X^2 + u^2 = (X+u)(X^2+X+u).$$

From the linear change of variables

$$R_2(X) = (X+u)^2 + u^2(X+u) + u^5 = u^4(Y^2+Y+u),$$

where $Y = (X+u)/u^2$, we see $R_2(X)$ is irreducible over $F(u)$. Therefore $G_f = D_4$ or $\mathbf{Z}/4\mathbf{Z}$.

Example 3.11. Let

$$f(X) = X^4 + (u^2+u)X^2 + u^2X + u.$$

This is irreducible over $F(u)$ by Eisenstein's criterion. Its quadratic resolvent is

$$R_2(X) = X^2 + u^4X + u^{10} + u^9 + u^7.$$

It is left to the reader to check this has no root in $F(u)$, so it is irreducible over $F(u)$, and the cubic resolvent of $f(X)$ is

$$R_3(X) = X^3 + (u^2+u)X^2 + u^4 = (X+u)(X^2+u^2X+u^3),$$

so the Galois group of $f(X)$ over $F(u)$ is D_4 or $\mathbf{Z}/4\mathbf{Z}$.

Example 3.12. Let

$$f(X) = X^4 + (u^2+u+1)X^2 + (u^2+u)X + 1.$$

It is left to the reader to check $f(X)$ is irreducible over $F(u)$. Its quadratic and cubic resolvents are

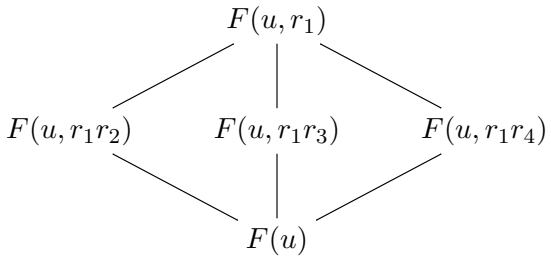
$$\begin{aligned} R_2(X) &= X^2 + (u^2+u)^2X + u^{10} + u^9 + u^3 + u^2 \\ &= (X + u^5 + u^4 + u^3 + u)(X + u^5 + u^3 + u^2 + u) \end{aligned}$$

and

$$R_3(X) = X^3 + (u^2+u+1)X^2 + (u^2+u)^2 = (X+u)(X+u+1)(X+u^2+u). \tag{3.7}$$

Both are reducible, so $G_f = V$.

Since the Galois group has order 4, the splitting field of $f(X)$ over $F(u)$ is $F(u, r_1)$. We will show the lattice of intermediate fields is as in the diagram below.



The products r_1r_2 and r_3r_4 are roots of

$$(X - r_1r_2)(X - r_3r_4) = X^2 - (r_1r_2 + r_3r_4)X + r_1r_2r_3r_4 = X^2 + (r_1r_2 + r_3r_4)X + 1. \tag{3.8}$$

We recognize the coefficient of X as a root of $R_3(X)$. The roots are listed in (3.7). By suitable labeling of the roots, we may assume $r_1r_2 + r_3r_4 = u$, $r_1r_3 + r_2r_4 = u+1$, and $r_1r_4 + r_2r_3 = u^2 + u$. Then (3.8) is $X^2 + uX + 1$, which is irreducible over $F(u)$, so $[F(u, r_1r_2) : F(u)] = 2$. It is left to the reader to check that r_1r_3 is a root of $X^2+(u+1)X+1$ and r_1r_4 is a root of $X^2+(u^2+u)X+1$, which are all irreducible over $F(u)$. The subgroups of the Galois group fixing r_1r_2, r_1r_3, and r_1r_4 are different, so these products generate different intermediate fields.

Is one of the quadratic intermediate fields $F(u, r_1 + r_2)$? No, because $r_1 + r_2$ is in $F(u)$. Indeed, the sum of all roots of $f(X)$ is 0, so $r_1 + r_2 = r_3 + r_4$, which implies

$$\begin{aligned} (r_1+r_2)^2 &= (r_1+r_2)(r_3+r_4) \\ &= r_1r_3 + r_2r_4 + r_1r_4 + r_2r_3 \\ &= u + 1 + u^2 + u \\ &= u^2 + 1 \\ &= (u+1)^2, \end{aligned}$$

so $r_1 + r_2 = u + 1$. Similarly, $r_1 + r_3 = u$ and $r_1 + r_4 = 1$.

Remark 3.13. Examples 3.10 and 3.12 are special cases of the following general considerations. Let K be a field of characteristic 2 and $f(X) = X^4 + (c+1)X^2 + cX + d$ be irreducible in $K[X]$, with $c \neq 0$ (so $f(X)$ is separable). Its cubic resolvent is

$$R_3(X) = X^3 + (c+1)X^2 + c^2 = (X+c)(X^2 + X + c),$$

which is reducible, so G_f is D_4, $\mathbf{Z}/4\mathbf{Z}$, or V. Example 3.10 uses $c = u$ and $d = 1$, while Example 3.12 uses $c = u^2 + u$ and $d = 1$.

Examples 3.10 and 3.11 are incomplete: when D_4 or $\mathbf{Z}/4\mathbf{Z}$ is the Galois group which one is it? This will be rectified with the following version of Theorem 1.3 that is valid in all characteristics, where $K(\sqrt{\operatorname{disc} f})$ is replaced with the splitting field of $R_2(X)$ over K.

Theorem 3.14. *Let $f(X) = X^4 + aX^3 + bX^2 + cX + d$ be separable and irreducible in $K[X]$. Assume its quadratic resolvent $R_2(X)$ is irreducible over K and its cubic resolvent*

$R_3(X)$ has a root r' in K. Let K_2 be the splitting field of $R_2(X)$ over K. Then $G_f = \mathbf{Z}/4\mathbf{Z}$ if $X^2 + aX + b - r'$ and $X^2 - r'X + d$ split completely over K_2, and otherwise $G_f = D_4$.

Theorem 1.3, which is Theorem 3.14 with the characteristic explicitly not 2, was proved by Kappe and Warren [5, p. 134] using an average to pass from a sum and difference of two roots of $f(X)$ to the roots themselves. There is no average of two numbers in characteristic 2. Our proof of Theorem 3.14 will avoid averaging by using Galois theory more fully.

Proof. By Corollary 3.5, r' is the unique root of $R_3(X)$ in K. Index the roots r_1, r_2, r_3, r_4 of $f(X)$ so that $r' = r_1r_2 + r_3r_4$. In S_4, D_4 and $\mathbf{Z}/4\mathbf{Z}$ contain a 4-cycle. (Elements of order 4 in S_4 are 4-cycles.) In Table 6 the effect of each 4-cycle in S_4 on $r_1r_2 + r_3r_4$ is given if the 4-cycle were in the Galois group. Each root of $R_3(X)$ is in the second column twice.

$(abcd)$	$(abcd)(r_1r_2 + r_3r_4)$
(1234)	$r_2r_3 + r_4r_1$
(1432)	$r_4r_1 + r_2r_3$
(1243)	$r_2r_4 + r_1r_3$
(1342)	$r_3r_1 + r_4r_2$
(1324)	$r_3r_4 + r_2r_1$
(1423)	$r_4r_3 + r_1r_2$

TABLE 6.

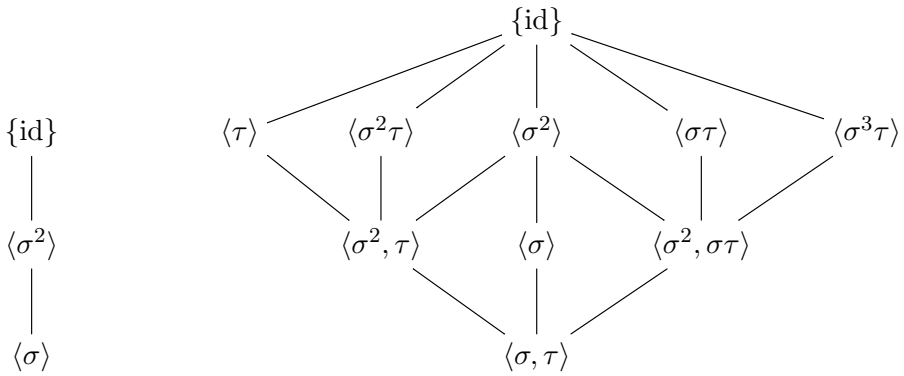
Since $r_1r_2 + r_3r_4$ is fixed by G_f, the 4-cycles in G_f are (1324) and (1423). (Both are in G_f since at least one is and they are inverses.)

Let $\sigma = (1324)$. If $G_f = \mathbf{Z}/4\mathbf{Z}$ then $G_f = \langle\sigma\rangle$. If $G_f = D_4$ then (3.1) tells us $G_f = \langle(1324), (12)\rangle = \{(1), (1324), (12)(34), (1423), (12), (34), (13)(24), (14)(23)\}$ and the elements of G_f fixing r_1 are (1) and (34). Set $\tau = (34)$. Products of σ and τ as disjoint cycles are in Table 7.

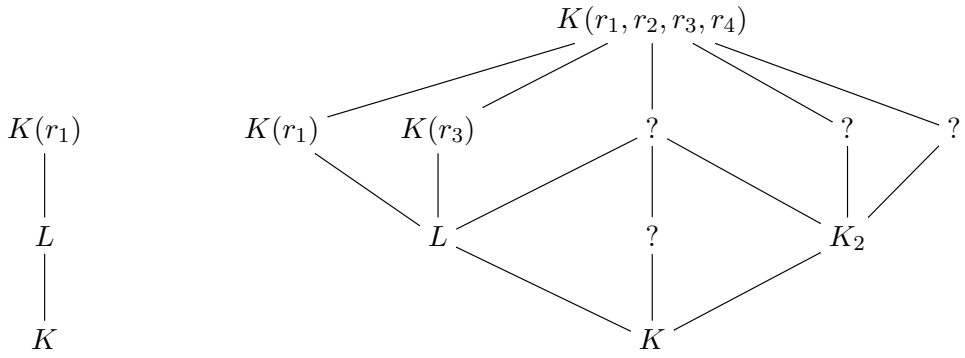
1	σ	σ^2	σ^3	τ	$\sigma\tau$	$\sigma^2\tau$	$\sigma^3\tau$
(1)	(1324)	(12)(34)	(1423)	(34)	(13)(24)	(12)	(14)(23)

TABLE 7.

The lattices of subgroups of $\langle\sigma\rangle$ and $\langle\sigma, \tau\rangle$ look very different. See the diagrams below, where the lattice of subgroups of $\langle\sigma\rangle$ and $\langle\sigma, \tau\rangle$ are listed upside down.



Corresponding to the above lattice of subgroups, we have the following subfield lattice of the splitting field of $f(X)$ over K, where L in both cases denotes the unique quadratic extension of K inside $K(r_1)$ and K_2 is the splitting field of $R_2(X)$ over K.



In the $\mathbf{Z}/4\mathbf{Z}$ case, $L = K_2$ since there is only one quadratic extension of K in the splitting field.

In the D_4 case, let's explain how we know $K(r_1)$ corresponds to $\langle\tau\rangle$, $K(r_3)$ corresponds to $\langle\sigma^2\tau\rangle$, and K_2 corresponds to $\langle\sigma^2, \sigma\tau\rangle$. The degree $[K(r_1) : K]$ is 4, so its corresponding subgroup in $D_4 = \langle\sigma, \tau\rangle$ has order $8/4 = 2$ and $\tau = (34)$ fixes r_1 and has order 2. Similarly, $[K(r_3) : K] = 4$ and $\sigma^2\tau = (12)$ fixes r_3. From the construction of $R_2(X)$ through its roots, the subgroup of G_f corresponding to K_2 is the even permutations of the roots of $f(X)$, and that is $\{(1), (12)(34), (13)(24), (14)(23)\} = \langle\sigma^2, \sigma\tau\rangle$.

Although the two cases are different, we are going to develop some common ideas for both of them concerning the quadratic extensions $K(r_1)/L$ and L/K.

If $G_f = \mathbf{Z}/4\mathbf{Z}$, $\mathrm{Gal}(K(r_1)/L) = \{1, \sigma^2\}$. If $G_f = D_4$, $\mathrm{Gal}(K(r_1)/L) = \langle\sigma^2, \tau\rangle/\langle\tau\rangle = \{1, \sigma^2\}$. So in both cases, the L-conjugate of r_1 is $\sigma^2(r_1) = r_2$ and the minimal polynomial of r_1 over L must be

$$(X - r_1)(X - r_2) = X^2 - (r_1 + r_2)X + r_1r_2.$$

Therefore $r_1 + r_2$ and r_1r_2 are in L. Since $[K(r_1) : K] = 4$, this polynomial is not in $K[X]$:

$$r_1 + r_2 \notin K \quad \text{or} \quad r_1r_2 \notin K. \tag{3.9}$$

In the $\mathbf{Z}/4\mathbf{Z}$ case, $\mathrm{Gal}(L/K) = \langle\sigma\rangle/\langle\sigma^2\rangle = \{1, \overline{\sigma}\}$, and in the D_4 case $\mathrm{Gal}(L/K) = \langle\sigma, \tau\rangle/\langle\sigma^2, \tau\rangle = \{1, \overline{\sigma}\}$. The coset of σ represents the nontrivial element both times, so the K-conjugate of $r_1 + r_2$ is $\sigma(r_1 + r_2) = r_3 + r_4$ and the K-conjugate of r_1r_2 is r_3r_4. (If $r_1 + r_2$ or r_1r_2 is in K these K-conjugates equal the original number, but otherwise they have to be different.) If $r_1 + r_2 \notin K$ then its minimal polynomial over K is

$$(X - (r_1 + r_2))(X - (r_3 + r_4)) = X^2 - (r_1 + r_2 + r_3 + r_4)X + (r_1 + r_2)(r_3 + r_4), \tag{3.10}$$

while if $r_1r_2 \notin K$ its minimal polynomial over K is

$$(X - r_1r_2)(X - r_3r_4) = X^2 - (r_1r_2 + r_3r_4)X + r_1r_2r_3r_4. \tag{3.11}$$

Even if $r_1 + r_2$ or r_1r_2 is in K, the coefficients of (3.10) and (3.11) are symmetric in the r_i's and therefore lie in K. The linear coefficient in (3.10) is a and the constant term is

$$(r_1 + r_2)(r_3 + r_4) = r_1r_3 + r_1r_4 + r_2r_3 + r_2r_4 = b - (r_1r_2 + r_3r_4) = b - r',$$

so (3.10) equals $X^2 + aX + (b - r')$. The polynomial (3.11) is $X^2 - r'X + d$. When $r_1 + r_2 \notin K$, (3.10) is irreducible in $K[X]$, and if $r_1 + r_2 \in K$ then (3.10) has a double

root in K. Similarly, (3.11) is irreducible over K or has a double root in K. Therefore the splitting field of (3.10) or (3.11) over K is either L or K and (3.9) tells us at least one of (3.10) and (3.11) is irreducible over K (so has splitting field L).

Since $r_1 + r_2$ and $r_1 r_2$ are in L and $[L : K] = 2$, each one generates L over K if it is not in K. This happens for at least one of the two numbers, by (3.9).

First suppose $G_f = \mathbf{Z}/4\mathbf{Z}$. Then $L = K_2$, so $X^2 + aX + (b - r')$ and $X^2 - r'X + d$ both split completely over K_2, since their roots are in L.

Next suppose $G_f = D_4$. Then $L \neq K_2$. By (3.9) at least one of (3.10) or (3.11) is irreducible over K, so its roots generate L over K and therefore are not in K_2. Thus the polynomial will be irreducible over K_2.

Since the conclusions about the two quadratic polynomials over K_2 are different depending on whether G_f is $\mathbf{Z}/4\mathbf{Z}$ or D_4, these conclusions tell us the Galois group. □

Example 3.15. Return to Example 3.10, where

$$f(X) = X^4 + (u+1)X^2 + uX + 1$$

over $F(u)$ and F has characteristic 2. Its quadratic resolvent is

$$R_2(X) = X^2 + u^2X + u^5 + u^3 + u^2 = u^4(Y^2 + Y + u),$$

where $Y = (X + u)/u^2$, and its cubic resolvent is

$$R_3(X) = X^3 + (u+1)X^2 + u^2 = (X + u)(X^2 + X + u).$$

Therefore $r' = u$ and the quadratic polynomials in Theorem 3.14 are

$$X^2 + aX + b - r' = X^2 + 1 = (X+1)^2 \text{ and } X^2 - r'X + d = X^2 + uX + 1.$$

The splitting field of $R_2(X)$ over $F(u)$ is $F(u, \alpha)$, where $\alpha^2 + \alpha + u = 0$. Therefore $F(u, \alpha) = F(\alpha)$ and $X^2 + uX + 1 = X^2 + (\alpha^2 + \alpha)X + 1$, which is irreducible over $F(\alpha)$, so $G_f = D_4$.

Example 3.16. Return to Example 3.11, where

$$f(X) = X^4 + (u^2 + u)X^2 + u^2X + u$$

has irreducible quadratic resolvent

$$R_2(X) = X^2 + u^4X + u^{10} + u^9 + u^7$$

and reducible cubic resolvent

$$R_3(X) = X^3 + (u^2 + u)X^2 + u^4 = (X + u)(X^2 + u^2X + u^3),$$

so the Galois group of $f(X)$ over $F(u)$ is D_4 or $\mathbf{Z}/4\mathbf{Z}$. Here $r' = u$, so the quadratics we try to factor over the splitting field of $R_2(X)$ are

$$X^2 + aX + b - r' = X^2 + u^2 = (X + u)^2$$

and

$$X^2 - r'X + d = X^2 + uX + u.$$

Letting α be a root of $R_2(X)$, so

$$\alpha^2 + u^4\alpha + u^{10} + u^9 + u^7 = 0,$$

we look for a root of $X^2 + uX + u$ in the field $F(u, \alpha)$. Every element of this field has the form $A + B\alpha$ for some A and B in $F(u)$. Substituting this in for X in $X^2 + uX + u$, we want to solve

$$(uB + u^4B^2)\alpha + (u + uA + A^2 + (u^{10} + u^9 + u^7)B^2) = 0.$$

Therefore $uB + u^4B^2 = 0$, so $B = 1/u^3$. (Or $B = 0$, but this leads to a contradiction on A.) Feeding this into the constant term, which also must be 0,

$$u + uA + A^2 + u^4 + u^3 + u = 0.$$

One solution is $A = u^2$, so $u^2 + (1/u^3)\alpha$ is a root of $R_2(X)$. Therefore $f(X)$ has Galois group $\mathbf{Z}/4\mathbf{Z}$ over $F(u)$.

If r is one root of $f(X)$, it turns out that all the roots of $f(X)$ are

$$r, \quad r+u, \quad r^2+(u+1)r, \quad r^2+(u+1)r+u.$$

A generator of the Galois group is $r \mapsto r^2 + (u+1)r$.

The distinction between $G_f = D_4$ and $G_f = \mathbf{Z}/4\mathbf{Z}$ in Theorem 3.14 depends on irreducibility of $X^2 + aX + b - r'$ and $X^2 - r'X + d$ over K_2. This can be formulated as a criterion entirely inside of K. On account of the different standard "normal forms" for quadratic Galois extensions inside and outside characteristic 2, the criterion will depend on whether or not $\operatorname{char} K = 2$.

Theorem 3.17. *Let the hypotheses and notation be as in Theorem 3.14. When* $\operatorname{char} K \neq 2$, $G_f = \mathbf{Z}/4\mathbf{Z}$ *if* $(a^2 - 4(b-r'))\operatorname{disc} f$ *and* $(r'^2 - 4d)\operatorname{disc} f$ *are squares in* K. *Otherwise* $G_f = D_4$.

When $\operatorname{char} K = 2$, *write* $R_2(X) = X^2 + AX + B$. *Then* $G_f = \mathbf{Z}/4\mathbf{Z}$ *if* $B/A^2 - (b+r')/a^2$ (*when* $a \neq 0$) *and* $B/A^2 - d/r'^2$ (*when* $r' \neq 0$) *are in* $\wp(K) = \{x^2 + x : x \in K\}$. *Otherwise* $G_f = D_4$.

Formulas for A and B are in Theorem 3.1. The case when K does not have characteristic 2 is essentially treated in [5, Theorem 3], but we include it here for completeness.

Proof. From the proof of Theorem 3.14, especially (3.9) and the paragraph following it, the polynomials $X^2 + aX + b - r'$ and $X^2 - r'X + d$ either have double roots in K or are irreducible over K.

First assume $\operatorname{char} K \neq 2$. Since $\operatorname{disc} R_2 = \operatorname{disc} f$, $K_2 = K(\sqrt{\operatorname{disc} f})$ by the quadratic formula. The discriminants of $X^2 + aX + b - r'$ and $X^2 - r'X + d$ are 0 or nonsquares in K. When γ and γ' are two nonsquares in K, $K(\sqrt{\gamma}) = K(\sqrt{\gamma'})$ if and only if $\gamma\gamma' = \square$ in K, so $X^2 + aX + b - r'$ splits over $K(\sqrt{\operatorname{disc} f})$ if and only if $(a^2 - 4(b-r'))\operatorname{disc} f = \square$ in K and $X^2 - r'X + d$ splits over $K(\sqrt{\operatorname{disc} f})$ if and only if $(r'^2 - 4d)\operatorname{disc} f = \square$ in K.

Now assume $\operatorname{char} K = 2$. Since $R_2(X)$ is separable, $A \neq 0$. The splitting field of $R_2(X)$ over K is the same as that of $X^2 + X + B/A^2$ (divide $R_2(X)$ by A^2 and relabel X/A as X). If $a \neq 0$ then $X^2 + aX + b - r'$ is separable and therefore irreducible over K. Its splitting field over K is the same as that of $X^2 + X + (b-r')/a^2$. By Artin-Schreier theory, two quadratics $X^2 + X + C$ and $X^2 + X + C'$ in $K[X]$ have the same splitting field over K if and only if $C - C' \in \wp(K)$. $\square$

Example 3.18. Let $f(X) = X^4 + (u+1)X^2 + uX + 1$. From Example 3.10, $R_2(X) = X^2 + u^2X + u^5 + u^3 + u^2$ and $r' = u$. Since $a = 0$, to decide if G_f is D_4 or $\mathbf{Z}/4\mathbf{Z}$, we need to know if $B/A^2 - d/r'^2$ has the form $g^2 + g$ for some $g \in F(u)$. Since

$$\frac{B}{A^2} - \frac{d}{r'^2} = \frac{u^5 + u^3 + u^2}{u^4} - \frac{1}{u^2} = u + \frac{1}{u},$$

we want to solve $g^2 + g = u + 1/u$. Multiplying through by u^2, this becomes $(ug)^2 + u(ug) + u^3 + u = 0$, which has no solution in $F(u)$ by Eisenstein's criterion. (There is a conceptually

simpler approach using valuation theory: a negative u-adic valuation of g^2+g is even, so $u+1/u$ can't have this form since its u-adic valuation is -1.) Thus $G_f = D_4$, as we saw already in Example 3.15.

Example 3.19. Let $f(X) = X^4 + (u^2+u)X^2 + u^2X + u$. From Example 3.11, $R_2(X) = X^2 + u^4X + u^{10} + u^9 + u^7$ and $r' = u$. Here

$$\frac{B}{A^2} - \frac{d}{r'^2} = \frac{u^{10}+u^9+u^7}{u^8} - \frac{u}{u^2} = u^2 + u \in \wp(F(u)),$$

so $G_f = \mathbf{Z}/4\mathbf{Z}$.

Example 3.20. Return to Example 3.6: $f(X) = X^4 + aX^3 + bX^2 + aX + 1$ is irreducible in $K[X]$ for a field K of characteristic 2, with a and b nonzero, so $f(X)$ is separable. The cubic resolvent of $f(X)$ in (3.6) is

$$R_3(X) = X(X^2 + bX + a^2),$$

so $r' = 0$. By the coefficient formulas in Theorem 3.1, the quadratic resolvent of $f(X)$ is

$$R_2(X) = X^2 + a^2bX + a^6 = a^6(Y^2 + (b/a)Y + 1),$$

where $Y = X/a^3$. If $X^2 + (b/a)X + 1$ is reducible over K then $R_2(X)$ is reducible and $G_f = V$. If $X^2 + (b/a)X + 1$ is irreducible over K then $R_2(X)$ is irreducible over K and $G_f = D_4$ or $\mathbf{Z}/4\mathbf{Z}$.

If $R_2(X)$ is ireducible over K, when does $G_f = D_4$ and when does $G_f = \mathbf{Z}/4\mathbf{Z}$? Since $r' = 0$, we need to check if $a^6/(a^2b)^2 - b/a^2 = a^2/b^2 - b/a^2$ is in $\wp(K)$. If it is then $G_f = \mathbf{Z}/4\mathbf{Z}$. Otherwise $G_f = D_4$. See Table 8.

$X^2 + (b/a)X + 1$	$a^2/b^2 - b/a^2$	G_f
reducible over K		V
irreducible over K	$\notin \wp(K)$	D_4
irreducible over K	$\in \wp(K)$	$\mathbf{Z}/4\mathbf{Z}$

TABLE 8. Galois group of sep. irred. $X^4 + aX^3 + bX^2 + aX + 1$ in char. 2

For instance, taking $K = F(u)$ with F of characteristic 2, $f(X) = X^4+uX^3+uX^2+uX+1$ is irreducible over K since $f(X+1)$ is Eisenstein at u. Since $X^2+(b/a)X+1 = X^2+X+1$ and $a^2/b^2 - b/a^2 = 1 - 1/u \notin \wp(K)$, $G_f = V$ if $\omega \in F$ and $G_f = D_4$ if $\omega \notin F$, where ω is a nontrivial cube root of unity.

As another example, let $f(X) = X^4 + uX^3 + u^2X^2 + uX + 1$. This polynomial factors as

$$f(X) = (X^2 + \omega uX + 1)(X^2 + \omega^2 uX + 1),$$

so if $\omega \in F$ then $f(X)$ is reducible over K. (Remember: before determining the Galois group of a quartic you should **first** check if the polynomial is irreducible.) It is left as an exercise to show that if $f(X)$ is reducible over K then $\omega \in F$. So if $\omega \notin F$ then $f(X)$ is irreducible over K. Here $a = u$ and $b = u^2$, so $X^2 + (b/a)X + 1 = X^2 + uX + 1$, which is irreducible over K. And $a^2/b^2 - b/a^2 = 1/u^2 - 1 \equiv 1/u - 1 \not\equiv 0 \bmod \wp(K)$, so $G_f = D_4$ when $\omega \notin F$.

Before Theorem 1.3 was known (from [5]), there was a more complicated procedure to decide between D_4 and $\mathbf{Z}/4\mathbf{Z}$ as the Galois group of a quartic $f(X)$ outside characteristic 2. Unlike Theorem 1.3, it involves testing irreducibility of $f(X)$, instead of two quadratic polynomials, over $K(\sqrt{\operatorname{disc} f})$. Here is that criterion.

Theorem 3.21. *Let K not have characteristic 2 and $f(X) \in K[X]$ be an irreducible quartic. Suppose* disc f *is not a square in K and $R_3(X)$ is reducible in $K[X]$, so G_f is D_4 or $\mathbf{Z}/4\mathbf{Z}$.*

(1) *If $f(X)$ is irreducible over $K(\sqrt{\operatorname{disc} f})$ then $G_f = D_4$.*
(2) *If $f(X)$ is reducible over $K(\sqrt{\operatorname{disc} f})$ then $G_f = \mathbf{Z}/4\mathbf{Z}$.*

An extension of this theorem to all characteristics is easy to guess:

Theorem 3.22. *Let $f(X) \in K[X]$ be a separable irreducible quartic. Suppose $R_2(X)$ is irreducible and $R_3(X)$ is reducible in $K[X]$, so G_f is D_4 or $\mathbf{Z}/4\mathbf{Z}$. Let K_2 be the splitting field of $R_2(X)$ over K.*

(1) *If $f(X)$ is irreducible over K_2 then $G_f = D_4$.*
(2) *If $f(X)$ is reducible over K_2 then $G_f = \mathbf{Z}/4\mathbf{Z}$.*

Proof. We will make reference to the field diagrams in the proof of Theorem 3.14.

When $G_f = D_4$, the field diagram for this Galois group shows the splitting field of $f(X)$ over K is $K_2(r_1)$. Since $[K_2(r_1) : K] = 8$, $[K_2(r_1) : K_2] = 4$, so $f(X)$ must be irreducible over K_2.

When $G_f = \mathbf{Z}/4\mathbf{Z}$, the splitting field of $f(X)$ over K_2 has degree 2, so $f(X)$ is reducible over K_2.

Because the different Galois groups imply different behavior of $f(X)$ over K_2, the behavior of $f(X)$ over K_2 tells us the Galois group. □

4. Quartic Fields with a Quadratic Subfield

If L/K is a separable quartic extension, it may or may not have a quadratic intermediate field. For example, the extension $\mathbf{Q}(\sqrt[4]{2})/\mathbf{Q}$ has the obvious quadratic intermediate field $\mathbf{Q}(\sqrt{2})$. But if α is a root of $X^4 - X - 1$, then the quartic extension $\mathbf{Q}(\alpha)/\mathbf{Q}$ has no quadratic intermediate field.

Outside of characteristic 2, there is a nice description of the quartic extensions L/K that have a quadratic intermediate field.

Theorem 4.1. *If K is a field not of characteristic 2 and $[L : K] = 4$, then there is a quadratic extension of K inside L if and only if $L = K(\theta)$ where θ has minimal polynomial $X^4 + AX^2 + B$ in $K[X]$. When this happens $X^2 + AX + B$ is irreducible over K and $K(\theta^2)$ is such an intermediate field.*

Proof. Suppose L/K is a quartic field and there is an intermediate quadratic extension M/K. Since the fields do not have characteristic 2, we can describe the quadratic extensions L/M and M/K by adjuncation of a square root: $M = K(\sqrt{a})$ where $a \in K^\times$ and $L = M(\sqrt{u + v\sqrt{a}})$ where $u, v \in K$ with $v \neq 0$. Let $\theta = \sqrt{u + v\sqrt{a}}$, so $L = K(\theta)$ and

$$\theta = \sqrt{u + v\sqrt{a}} \Longrightarrow \theta^2 = u + v\sqrt{a} \Longrightarrow (\theta^2 - u)^2 = av^2 \Longrightarrow \theta^4 - 2u\theta^2 + u^2 - av^2 = 0.$$

Conversely, if $L = K(\theta)$ where θ has minimal polynomial $X^4 + AX^2 + B$ in $K[X]$ then $\theta^2 = (-A \pm \sqrt{A^2 - 4B})/2$ and $A^2 - 4B \neq \square$ in K (otherwise $X^4 + AX^2 + B$ would not be irreducible over K), so $K(\sqrt{A^2 - 4B}) = K(\theta^2)$ is a quadratic extension of K lying in L. □

Here is an analogue in characteristic 2.

Theorem 4.2. *If K has characteristic 2 then a separable quartic extension L/K has an intermediate quadratic extension if and only if $L = K(\theta)$ where the minimal polynomial of θ*

over K is $X^4+(A+1)X^2+AX+B$ in $K[X]$ with $A \neq 0$. When this happens X^2+AX+B is irreducible over K and $K(\theta^2+\theta)$ is such an intermediate field.

Proof. First suppose $L \supset M \supset K$ where $[L : M] = 2$ and $[M : K] = 2$. Since L/K is separable, L/M and M/K are separable. By Theorem A.1, $M = K(t)$ where $t^2+t \in K$ and $L = M(\theta)$ where $\theta^2+\theta \in M$. Write $t^2+t = a$ and $\theta^2+\theta = u+vt$ where $u, v \in K$ and $v \neq 0$. Since $t = (\theta^2+\theta-u)/v$, we have $L = K(t,\theta) = K(\theta))$. Expanding the equation

$$a = t^2+t = \left(\frac{\theta^2+\theta-u}{v}\right)^2 + \frac{\theta^2+\theta-u}{v}$$

in terms of θ and clearing the denominator, θ is a root of $X^4+(v+1)X^2+vX+(u^2+uv+av^2)$.

Conversely, suppose $L = K(\theta)$ where θ has minimal polynomial $X^4+(A+1)X^2+AX+B$ in $K[X]$ and $A \neq 0$. Since K has characteristic 2, the derivative of this polynomial is the constant A, which is not 0, so the polynomial is separable and L/K is separable. To show L/K has an intermediate quadratic extension, we rewrite the minimal equation for θ over K:

$$\theta^4+(A+1)\theta^2+A\theta+B = 0 \Longrightarrow (\theta^2+\theta)^2+A(\theta^2+\theta)+B = 0.$$

Therefore $t := \theta^2+\theta$ has degree at most 2 over K and $L = K(\theta) \supset K(t) \supset K$. Since θ has degree at most 2 over $K(t)$ and $[L : K] = 4$, t has degree 2 over K, so X^2+AX+B is irreducible over K. □

The analogies between X^4+AX^2+B outside characteristic 2 and $X^4+(A+1)X^2+AX+B$ in characteristic 2 goes further. Outside characteristic 2, the roots of X^4+AX^2+B come in pairs: $\pm\alpha$ and $\pm\beta$. Similarly, in characteristic 2 the roots of $X^4+(A+1)X^2+AX+B$ come in pairs $\alpha, \alpha+1$ and $\beta, \beta+1$.

When K does not have characteristic 2 and $f(X) = X^4+AX^2+B$ is irreducible in $K[X]$, its possible Galois groups over K are D_4, $\mathbf{Z}/4\mathbf{Z}$, or V according to the following rules:

- $B = \square$ in $K \Longrightarrow G_f = V$,
- $B \neq \square$ and $(A^2-4B)B = \square$ in $K \Longrightarrow G_f = \mathbf{Z}/4\mathbf{Z}$,
- $B \neq \square$ and $(A^2-4B)B \neq \square$ in $K \Longrightarrow G_f = D_4$.

This is a standard exercise in Galois theory (*e.g.*, [1, p. 277] and [2, p. 53]). In [5, Theorem 3], Kappe and Warren prove these rules using their criterion (Theorem 1.3) for distinguishing $\mathbf{Z}/4\mathbf{Z}$ and D_4 as Galois groups outside characteristic 2. Here is the characteristic 2 analogue.

Theorem 4.3. *Let $f(X) = X^4+(A+1)X^2+AX+B$ be separable irreducible in $K[X]$, where K has characteristic 2. If $A \in \wp(K)$ then $G_f = V$. If $A \notin \wp(K)$ and $B/A^2-A \in \wp(K)$ then $G_f = \mathbf{Z}/4\mathbf{Z}$. If $A \notin \wp(K)$ and $B/A^2-A \notin \wp(K)$ then $G_f = D_4$.*

Proof. From separability of $f(X)$, A and B are nonzero in K. We will explain in two ways why the only choices for G_f are D_4, $\mathbf{Z}/4\mathbf{Z}$, and V, and then distinguish among these possibilities.

Since the field $K(\theta)$, where θ is a root of $f(X)$, has a quadratic intermediate extension, the subgroup of G_f corresponding to $K(\theta)$ lies in an index-2 subgroup of G_f. There is no subgroup of index two in A_4, so $G_f \neq A_4$. If $G_f = S_4$ then its only subgroup of index two is A_4. The subgroup of G_f corresponding to $K(\theta)$ is S_3 (by a suitable labeling of the roots) and $S_3 \not\subset A_4$. This is a contradiction, so $G_f \neq S_4$ either.

For a second proof that G_f is D_4, $\mathbf{Z}/4\mathbf{Z}$, or V, the cubic resolvent of $f(X)$ is

$$R_3(X) = X^3+(A+1)X^2+A^2 = (X+A)(X^2+X+A),$$

which is reducible, so G_f is D_4, $\mathbf{Z}/4\mathbf{Z}$, or V by Theorem 3.4.

The quadratic resolvent of $f(X)$ is

$$\begin{aligned} R_2(X) &= X^2 + A^2X + ((A+1)^3 + A^2)A^2 \\ &= X^2 + A^2X + (A^3 + A + 1)A^2 \\ &= A^4\left(\left(\frac{X}{A^2}\right)^2 + \frac{X}{A^2} + A + \frac{1}{A} + \frac{1}{A^2}\right) \\ &= A^4\left(\left(\frac{X}{A^2} + \frac{1}{A}\right)^2 + \left(\frac{X}{A^2} + \frac{1}{A}\right) + A\right), \end{aligned}$$

so K_2, the splitting field of $R_2(X)$ over K, is the same as the splitting field of $X^2 + X + A$ over K.

By Corollary 3.5, $G_f = V$ if and only if $R_3(X)$ splits completely over K, which is equivalent to $A \in \wp(K)$. Suppose that $A \notin \wp(K)$, so $R_2(X)$ is irreducible over K and A is the unique root of $R_3(X)$ in K. By Theorem 3.14, $G_f = \mathbf{Z}/4\mathbf{Z}$ if and only if the polynomials $X^2 + (A + 1 - A)$ and $X^2 + AX + B$ both split completely over K_2. The first polynomial is $(X+1)^2$, so $G_f = \mathbf{Z}/4\mathbf{Z}$ if and only if $X^2 + X + A$ and $X^2 + AX + B$ have the same splitting field over K. Since $X^2 + AX + B = A^2((X/A)^2 + (X/A) + B/A^2)$, $X^2 + AX + B$ and $X^2 + X + A$ have the same splitting field over K if and only if $B/A^2 - A \in \wp(K)$. □

Example 4.4. In Example 3.10, $K = F(u)$, $A = u$ and $B = 1$. Since $u \notin \wp(K)$, Theorem 4.3 says G_f is D_4 or $\mathbf{Z}/4\mathbf{Z}$, and $G_f = \mathbf{Z}/4\mathbf{Z}$ if and only if $B/A^2 - A = 1/u^2 - u$ is in $\wp(K)$. Since $1/u^2 \equiv 1/u \bmod \wp(K)$ and $1/u - u \notin \wp(K)$, $G_f \neq \mathbf{Z}/4\mathbf{Z}$. Thus $G_f = D_4$, which we already found in Example 3.15.

Example 4.5. In Example 3.12, $K = F(u)$, $A = u^2 + u$, and $B = 1$. Obviously $A \in \wp(K)$, so $G_f = V$.

Appendix A. Separable Quadratic Extensions in Characteristic 2

When K does not have characteristic 2, every quadratic extension of K has the form $K(\sqrt{a})$ for some nonsquare a in $K^\times$, and for two nonsquares a and a' in K we have $K(\sqrt{a}) = K(\sqrt{a'})$ if and only if a/a' is a square in K. When K has characteristic 2, quadratic extensions of K usually don't have the form $K(\sqrt{a})$: the polynomial $X^2 - a$ is inseparable, so a field extension $K(\sqrt{a})/K$ is inseparable. Moreover, we can have $K(\sqrt{a}) = K(\sqrt{a'})$ even if a/a' is not a square in K. For example, if $K = F(u)$ where F has characteristic 2 and u is transcendental over F then $K(\sqrt{u}) = K(\sqrt{u+1})$ since $\sqrt{u+1} = \sqrt{u}+1$ in characteristic 2. Artin and Schreier found a clean description of the *separable* quadratic extensions in characteristic 2 using roots of polynomials $X^2 + X - a$ in place of square roots (roots of $X^2 - a$).

Theorem A.1 (Artin–Schreier)**.** *If K has characteristic 2 then every separable quadratic extension of K has the form $K(\alpha)$ where α is the root of an irreducible polynomial X^2+X-a in $K[X]$. Conversely, each root of an irreducible polynomial of the form $X^2 + X - a$ in $K[X]$ generates a separable quadratic extension of K. Finally, two polynomials $X^2 + X - a$ and $X^2 + X - a'$ in $K[X]$ have the same splitting field over K if and only if $a - a' = c^2 + c$ for some $c \in K$.*

Proof. Let L/K be a separable quadratic extension. Pick $t \in L - K$, so $L = K(t)$. Write the minimal polynomial of t over K as $X^2 + AX + B$. This polynomial is separable, so its discriminant $A^2 - 4B = A^2$ is not zero. Since $A \neq 0$,

$$t^2 + At + B = 0 \Longrightarrow \left(\frac{t}{A}\right)^2 + \frac{t}{A} + \frac{B}{A^2} = 0.$$

Replacing t with $\alpha = t/A$, $L = K(\alpha)$ where α is a root of $X^2 + X + B/A^2$. Conversely, every polynomial $X^2 + X - a$ in $K[X]$ is separable (its discriminant is 1, which is not 0), so if such a polynomial is irreducible then a root of it generates a separable quadratic extension of K.

Suppose $X^2 + X - a$ and $X^2 + X - a'$ have the same splitting field over K. $K(\alpha) = K(\alpha')$ where $\alpha^2 + \alpha - a = 0$ and $\alpha'^2 + \alpha' - a' = 0$. If $X^2 + X - a$ is irreducible over K then $X^2 + X - a'$ must also be irreducible over K, so $\alpha' = u + v\alpha$ where u and v are in K and $v \neq 0$. Then

$$\begin{aligned} 0 &= (u + v\alpha)^2 + (u + v\alpha) - a' \\ &= (u^2 + v^2\alpha^2) + (u + v\alpha) - a' \\ &= (u^2 + v^2(a - \alpha)) + u - a' + v\alpha \\ &= (-v^2 + v)\alpha + u^2 + u + av^2 - a'. \end{aligned}$$

Therefore $v^2 = v$ and $u^2 + u + av^2 - a' = 0$. The first equation implies v is 0 or 1, so $v = 1$ since $v \neq 0$. The second equation becomes $u^2 + u + a - a' = 0$, so $a - a' = -u^2 - u = u^2 + u$ since $-1 = 1$ in K.

If $X^2 + X - a$ is reducible over K then $X^2 + X - a'$ is also reducible over K, so α and α' are both in K: Then $a - a' = (\alpha^2 + \alpha) - (\alpha'^2 + \alpha') = (\alpha - \alpha')^2 + (\alpha - \alpha') = c^2 + c$ where $c = \alpha - \alpha' \in K$.

Conversely, if $a - a' = c^2 + c$ for some $c \in K$ then $X^2 + X - a' = (X + c)^2 + (X + c) - a$, so a splitting field of $X^2 + X - a'$ over K is $K(\alpha - c) = K(\alpha)$.

□

References

[1] T. Hungerford, "Algebra", Springer-Verlag, New York, 1980.

[2] I. Kaplansky, "Fields and Rings," 2nd ed., Univ. of Chicago Press, 1972.

[3] D. S. Dummit and R. M. Foote, "Abstract Algebra," 3rd ed., Wiley, 2004.

[4] F. M. Goodman, "Algebra: Abstract and Concrete," 2nd ed., Prentice–Hall, 2003.

[5] L-C. Kappe and B. Warren, *An Elementary Test for the Galois Group of a Quartic Polynomial*, Amer. Math. Monthly **96** (1989), 133–137.

[6] J. Rotman, "Galois Theory," 2nd ed., Springer–Verlag, 1998.