GALOIS GROUPS OF CUBICS AND QUARTICS (NOT IN CHARACTERISTIC 2)

KEITH CONRAD

We will describe a procedure for figuring out the Galois groups of separable irreducible polynomials in degrees 3 and 4 over fields not of characteristic 2. This does *not* include explicit formulas for the roots, *i.e.*, we are not going to derive the classical cubic and quartic formulas.

1. Review

Let K be a field and $f(X)$ be a separable polynomial in $K[X]$. The Galois group of $f(X)$ over K permutes the roots of $f(X)$ in a splitting field, and labeling the roots as $r_1, \ldots, r_n$ provides an embedding of the Galois group into S_n. We recall without proof two theorems about this embedding.

Theorem 1.1. *Let $f(X) \in K[X]$ be a separable polynomial of degree n.*

(a) *If $f(X)$ is irreducible in $K[X]$ then its Galois group over K has order divisible by n.*
(b) *The polynomial $f(X)$ is irreducible in $K[X]$ if and only if its Galois group over K is a transitive subgroup of S_n.*

Definition 1.2. If $f(X) \in K[X]$ factors in a splitting field as

$$f(X) = c(X - r_1) \cdots (X - r_n),$$

the *discriminant* of $f(X)$ is defined to be

$$\operatorname{disc} f = \prod_{i<j} (r_j - r_i)^2.$$

In degree 3 and 4, explicit formulas for discriminants of some monic polynomials are

$$\begin{aligned} \operatorname{disc}(X^3 + aX + b) &= -4a^3 - 27b^2, \\ \operatorname{disc}(X^4 + aX + b) &= -27a^4 + 256b^3, \\ \operatorname{disc}(X^4 + aX^2 + b) &= 16b(a^2 - 4b)^2, \end{aligned}$$

Theorem 1.3. *Let $f(X) \in K[X]$ be a separable polynomial of degree n. If K does not have characteristic 2, the Galois group of $f(X)$ over K is a subgroup of A_n if and only if $\operatorname{disc} f$ is a square in K.*

This theorem is why we will assume *our fields do not have characteristic* 2.

2. Galois groups of cubics

The Galois group of a cubic polynomial is completely determined by its discriminant.

Theorem 2.1. *Let K not have characteristic 2 and $f(X)$ be a separable 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.*

Proof. The permutation action of the Galois group of $f(X)$ on its roots turns the Galois group into a transitive subgroup of S_3 (Theorem 1.1). The only transitive subgroups of S_3 are A_3 and S_3, and we can decide when the Galois group is in A_3 or not using the discriminant (Theorem 1.3). $\square$

Example 2.2. In Table 1 we list the discriminants and Galois groups over $\mathbf{Q}$ of cubics $X^3 - aX - 1$, where $1 \leq a \leq 6$. We skipped $X^3 - 2X - 1$ since it is reducible. The second row, where $a = 3$, has a square discriminant and Galois group A_3. The other Galois groups in the table are S_3. It is a hard theorem that $X^3 - aX - 1$ with $a \in \mathbf{Z}$ has Galois group A_3 *only* when $a = 3$.

$f(X)$	$\operatorname{disc} f$	Galois group
$X^3 - X - 1$	-23	S_3
$X^3 - 3X - 1$	81	A_3
$X^3 - 4X - 1$	229	S_3
$X^3 - 5X - 1$	473	S_3
$X^3 - 6X - 1$	837	S_3

Table 1. Some Galois groups over $\mathbf{Q}$

If a cubic polynomial has Galois group A_3 over $\mathbf{Q}$, its roots all generate the same field extension of $\mathbf{Q}$, so all the roots are real since at least one root is real. But if all the roots are real the Galois group does not have to be A_3. The polynomial $X^3 - 4X - 1$ has all real roots but its Galois group over $\mathbf{Q}$ is S_3. Each real root of $X^3 - 4X - 1$ generates a different cubic field in $\mathbf{R}$.

Remark 2.3. The cubics $X^3 - 2X + 1$ and $X^3 - 7X - 6$ have respective discriminants 5 and $400 = 20^2$, but this does *not* mean by Theorem 2.1 that their Galois groups over $\mathbf{Q}$ are S_3 and A_3. Both polynomials are reducible (factoring as $(X - 1)(X^2 + X - 1)$ and $(X + 1)(X + 2)(X - 3)$). Do not forget to check that a cubic is irreducible before you use Theorem 2.1! You also need to check it is separable if you're working in characteristic 3. Outside characteristic 3, irreducible cubics are automatically separable.

Example 2.4. Let F be a field and u be transcendental over F. In $F(u)[X]$, the polynomial $X^3 + uX + u$ is irreducible by Eisenstein's criterion at u. The discriminant is $-4u^3 - 27u^2 = -u^2(4u+27)$. If F does not have characteristic 2 or 3, this has a simple linear factor $4u+27$, so the discriminant is not a square in $F(u)$. If F has characteristic 3, the discriminant is $-4u^3 = -u^3$, which is not a square in $F(u)$. Therefore when F does not have characteristic 2, the Galois group of $X^3 + uX + u$ over $F(u)$ is isomorphic to S_3.

We can't say anything here about the Galois group of $X^3 + uX + u$ over $F(u)$ when F has characteristic 2. Its discriminant is $-4u^3 - 27u^2 = u^2$, a perfect square, but this does *not* mean the Galois group of X^3+uX+u over $F(u)$ is A_3. Theorem 2.1, and Theorem 1.3 which it depended upon, require the base field K not have characteristic 2. In characteristic 2 we can't tell if the Galois group is in A_n or not by checking if the discriminant is a square.

If you write down a random cubic over $\mathbf{Q}$, it is probably irreducible and has Galois group S_3. Therefore it's nice to have a record of a few irreducible cubics over $\mathbf{Q}$ whose Galois group is A_3. See Table 2, where each discriminant is a perfect square. (The polynomials in the table are all irreducible over $\mathbf{Q}$ since ± 1 are not roots or because they are all irreducible mod 2.) We list in the table all three roots of each cubic in terms of one root we call r. That list of roots is essentially telling us what the three elements of $\mathrm{Gal}(\mathbf{Q}(r)/\mathbf{Q})$ are, as each automorphism is determined by its effect on r.

$f(X)$	$\operatorname{disc} f$	Roots
X^3-3X-1	9^2	$r,\ r^2-r-2,\ -r^2+2$
X^3-X^2-2X+1	7^2	$r,\ r^2-r-1,\ -r^2+2$
X^3+X^2-4X+1	13^2	$r,\ r^2+r-3,\ -r^2-2r+2$
X^3+2X^2-5X+1	19^2	$r,\ r^2+2r-4,\ -r^2-3r+2$

TABLE 2. Some cubics with Galois group A_3 over $\mathbf{Q}$

Here is an infinite family of A_3-cubics over $\mathbf{Q}$.

Corollary 2.5. *For any integer k, set $a=k^2+k+7$. The polynomial X^3-aX+a is irreducible over $\mathbf{Q}$ and has Galois group A_3.*

Proof. For any odd number a, $X^3-aX+a\equiv X^3+X+1 \bmod 2$, which is irreducible mod 2, so X^3-aX+a is irreducible over $\mathbf{Q}$. Its discriminant is $-4(-a)^3-27a^2=a^2(4a-27)$. To have Galois group A_3 we need $4a-27$ to be a square. Writing $4a-27=c^2$, we get $a=\frac{1}{4}(c^2+27)$. To make this integral we need c odd, and writing $c=2k+1$ gives us $a=\frac{1}{4}(4k^2+4k+28)=k^2+k+7$. For any integer k, k^2+k+7 is odd so if we define this expression to be a then X^3-aX+a has Galois group A_3 over $\mathbf{Q}$. $\square$

Without using Galois groups, we can describe the splitting field of any separable cubic (not necessarily irreducible) in terms of one root and the discriminant.

Theorem 2.6. *Let K not have characteristic 2 and $f(X)\in K[X]$ be a separable cubic with discriminant Δ. If r is one root of $f(X)$ then a splitting field of $f(X)$ over K is $K(r,\sqrt{\Delta})$. In particular, if $f(X)$ is a reducible cubic then its splitting field over K is $K(\sqrt{\Delta})$.*

Proof. Without loss of generality, $f(X)$ is monic. Let the roots of $f(X)$ be r, r', and r''. Write $f(X)=(X-r)g(X)$, so r' and r'' are the roots of $g(X)$. In particular, $g(r)\neq 0$. By the quadratic formula for $g(X)$ over $K(r)$, $K(r,r',r'')=K(r)(r',r'')=K(r)(\sqrt{\operatorname{disc} g})$. Since $f(X)$ is monic, so is $g(X)$ and a calculation shows $\operatorname{disc} f=g(r)^2\operatorname{disc} g$, so $K(r,\sqrt{\operatorname{disc} g})=K(r,\sqrt{\operatorname{disc} f})=K(r,\sqrt{\Delta})$.

If $f(X)$ is reducible, we can take for r above a root of $f(X)$ in K. Then $K(r,\sqrt{\Delta})=K(\sqrt{\Delta})$. $\square$

It is crucial here that K does not have characteristic 2. The proof used the quadratic formula, which doesn't work in characteristic 2, but maybe the theorem itself could be proved by a different argument in characteristic 2? No: the theorem as written is wrong in characteristic 2. Here is a counterexample. Let $K = F(u)$, where F has characteristic 2 and u is transcendental over F. The cubic polynomial $X^3 + uX + u$ is irreducible in $K[X]$ with discriminant u^2, so $K(r, \sqrt{\Delta}) = K(r)$. It can be shown that the degree of the splitting field of $X^3 + uX + u$ over K is 6, not 3, so $K(r, \sqrt{\Delta})$ is not the splitting field of the polynomial over K.

3. Galois groups of quartics

To compute Galois groups of separable irreducible quartics, we first list the transitive subgroups of S_4. These are the candidates for the Galois groups, by Theorem 1.1.

Type	S_4	A_4	D_4	$\mathbf{Z}/4\mathbf{Z}$	V
$(1,1,1,1)$	1	1	1	1	1
$(1,1,2)$	6		2		
$(2,2)$	3	3	3	1	3
$(1,3)$	8	8			
(4)	6		2	2	
Sum	24	12	8	4	4

Table 3.

The heading of Table 3 includes all the transitive subgroups of S_4, up to isomorphism, and the entries of the table are the number of permutations of each cycle type in such a subgroup. (We write V for Klein's four-group $\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$.) Inside S_4 there are three transitive subgroups isomorphic to D_4:

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

These are the only subgroups of S_4 with order 8 and they are conjugate to each other. There are three transitive subgroups of S_4 isomorphic to $\mathbf{Z}/4\mathbf{Z}$:

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

These are the the only cyclic subgroups of order 4 in S_4 and they are conjugate to each other. The unique transitive subgroup of S_4 isomorphic to V is

$$\{(1), (12)(34), (13)(24), (14)(23)\}. \tag{3.3}$$

There are other subgroups of S_4 that are isomorphic to V, such as $\{(1), (12), (34), (12)(34)\}$, but they are not transitive so they can't occur as the Galois groups we are looking for. We will henceforth write V for the group (3.3).

We will often treat D_4 and $\mathbf{Z}/4\mathbf{Z}$ as if they are subgroups of S_4 rather than just subgroups known up to conjugation. Since a Galois group as a subgroup of S_n is only determined up to conjugation anyway, this isn't a bad convention provided we are careful when we refer to specific elements of S_4 lying in the Galois group.

A few observations from Table 3:

1. The only transitive subgroups of S_4 which are inside A_4 are A_4 and V. (In fact V is the only subgroup of A_4 with order 4, transitive or not.)
2. The only transitive subgroups of S_4 with size divisible by 3 are S_4 and A_4.
3. The only transitive subgroups of S_4 containing a transposition (cycle type $(1,1,2)$) are S_4 and D_4.

Let $f(X) = X^4 + aX^3 + bX^2 + cX + d$ be monic irreducible[1] in $K[X]$, so $\operatorname{disc} f \neq 0$. Write the roots of $f(X)$ as r_1, r_2, r_3, r_4, so

$$X^4 + aX^3 + bX^2 + cX + d = (X - r_1)(X - r_2)(X - r_3)(X - r_4). \tag{3.4}$$

The Galois group of a separable irreducible cubic polynomial in $K[X]$ is determined by whether or not its discriminant Δ is a square in K, which can be thought of in terms of the associated quadratic polynomial $X^2 - \Delta$ having a root in K. We will see that the Galois group of a quartic polynomial depends on the behavior of an associated cubic polynomial.

We want to create a cubic polynomial with roots in the splitting field of $f(X)$ over K by finding an expression in the roots of $f(X)$ which only has 3 possible images under the Galois group. Since the Galois group is in S_4, we look for an polynomial in 4 variables which, under all 24 permutations of the variables, has 3 values. One such expression is

$$x_1x_2 + x_3x_4.$$

Under S_4, acting on $F(x_1, x_2, x_3, x_4)$, $x_1x_2 + x_3x_4$ can be moved to

$$x_1x_2 + x_3x_4, \quad x_1x_3 + x_2x_4, \quad \text{and} \quad x_1x_4 + x_2x_3.$$

When we specialize $x_i \mapsto r_i$, these become

$$r_1r_2 + r_3r_4, \quad r_1r_3 + r_2r_4, \quad \text{and} \quad r_1r_4 + r_2r_3. \tag{3.5}$$

It *might not* be the case that these are all K-conjugates, since not all 24 permutations of the r_i's have to be in the Galois group. But the K-conjugate of a number in (3.5) is also in (3.5), so we are inspired to look at the cubic

$$(X - (r_1r_2 + r_3r_4))(X - (r_1r_3 + r_2r_4))(X - (r_1r_4 + r_2r_3)).$$

Its coefficients are symmetric polynomials in the r_i's because the three factors are permuted amongst themselves by any element of the Galois group (a subgroup of S_4). So the coefficients must be in K by Galois theory. What are the coefficients of this cubic, in terms of the coefficients of $f(X)$?

Write

$$(X - (r_1r_2 + r_3r_4))(X - (r_1r_3 + r_2r_4))(X - (r_1r_4 + r_2r_3)) = X^3 + AX^2 + BX + C. \tag{3.6}$$

We seek expressions for A, B, and C as polynomials in the elementary symmetric functions of the r_i's, which are a, b, c, and d up to sign. The value of A is easy:

$$A = -(r_1r_2 + r_3r_4 + r_1r_3 + r_2r_4 + r_1r_4 + r_2r_3) = -b.$$

The others require more effort. Multiplying out (3.6),

$$\begin{aligned} B \;=\; & r_1^2r_2r_3 + r_1r_2^2r_4 + r_1r_3^2r_4 + r_2r_3r_4^2 + r_1^2r_2r_4 + r_1r_2^2r_3 + r_1r_3r_4^2 + r_2r_3^2r_4 + r_1^2r_3r_4 + \\ & r_1r_2r_3^2 + r_1r_2r_4^2 + r_2^2r_3r_4 \end{aligned}$$

and

$$C = -(r_1r_2 + r_3r_4)(r_1r_3 + r_2r_4)(r_1r_4 + r_2r_3).$$

Using the algorithm in the proof of the symmetric function theorem,

$$B = s_1s_3 - 4s_4 = ac - 4d$$

and

$$C = -(s_1^2s_4 + s_3^2 - 4s_2s_4) = -(a^2d + c^2 - 4bd).$$

[1] Irreducibility of a quartic implies separability outside of characteristic 2, so we don't have to assume separability explicitly since our running hypothesis is that K does not have characteristic 2.

Thus

$$X^3 + AX^2 + BX + C = X^3 - bX^2 + (ac - 4d)X - (a^2d + c^2 - 4bd). \tag{3.7}$$

Definition 3.1. When $f(X)$ is a quartic with roots r_1, r_2, r_3, r_4, its *cubic resolvent* $R_3(X)$ is the cubic polynomial (3.6).

When $f(X)$ is monic, we just checked that

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

This may or may not be irreducible over K.

It is useful to record a special case of the cubic resolvent. Letting $a = b = 0$,

$$f(X) = X^4 + cX + d \Longrightarrow R_3(X) = X^3 - 4dX - c^2. \tag{3.8}$$

Example 3.2. We compute the Galois group of $X^4 - X - 1$ over $\mathbf{Q}$. This polynomial is irreducible over $\mathbf{Q}$ since it is irreducible mod 2. By (3.8), the cubic resolvent of $X^4 - X - 1$ is $X^3 + 4X - 1$, which is irreducible over $\mathbf{Q}$ (± 1 are not roots). That shows the splitting field of $X^4 - X - 1$ contains a cubic subfield (namely $\mathbf{Q}(r_1r_2 + r_3r_4)$), so the Galois group of $X^4 - X - 1$ over $\mathbf{Q}$ has order divisible by 3. The splitting field also contains $\mathbf{Q}(r_1)$, so the Galois group is also divisible by 4. Therefore the Galois group is either A_4 or S_4. The discriminant of $X^4 - X - 1$ is -283, which is not a rational square, so the Galois group must be S_4.

Example 3.3. Let's determine the Galois group of $X^4 + 8X + 12$ over $\mathbf{Q}$. First we show the polynomial is irreducible. If it is reducible then it has a linear factor or is a product of two quadratic irreducibles. There is no rational root (a rational root would be an integer factor of 12, and they are not roots), so there is no linear factor. To rule out two quadratic irreducible factors over $\mathbf{Q}$, consider the mod 5 irreducible factorization

$$X^4 + 8X + 12 \equiv (X - 4)(X^3 + 4X^2 + X + 2) \bmod 5.$$

If $X^4 + 8X + 12$ were a product of two quadratics over $\mathbf{Q}$, it would be a product of two (monic) quadratics over $\mathbf{Z}$, and compatibility with the mod 5 factorization above would force there to be at least two roots mod 5, which there are not.

By (3.8), the cubic resolvent of $X^4+8X+12$ is $X^3-48X-64$, which is irreducible mod 5 and thus is irreducible over $\mathbf{Q}$, so the Galois group of $X^4+8X+12$ over $\mathbf{Q}$ has size divisible by 3 (and 4), so the Galois group is either A_4 or S_4. The discriminant of $X^4 + 8X + 12$ is $331776 = 576^2$, a perfect square, so the Galois group is A_4.

Theorem 3.4. *The quartic $f(X)$ and its cubic resolvent $R_3(X)$ have the same discriminant. In particular, $R_3(X)$ is separable since $f(X)$ is separable.*

Proof. A typical difference of two roots of $R_3(X)$ is

$$(r_1r_2 + r_3r_4) - (r_1r_3 + r_2r_4) = (r_1 - r_4)(r_2 - r_3).$$

Forming the other two differences, multiplying, and squaring, we obtain $\operatorname{disc} R_3 = \operatorname{disc} f$. $\square$

Remark 3.5. There is a second polynomial that can be found in the literature under the name of cubic resolvent for $f(X)$. It's the cubic whose roots are $(r_1 + r_2)(r_3 + r_4)$, $(r_1 + r_3)(r_2 + r_4)$, and $(r_1 + r_4)(r_2 + r_3)$. This amounts to exchanging additions and multiplications in the formation of the resolvent's roots. An explicit formula for the cubic with these roots, in terms of the coefficients of $f(X)$, is

$$X^3 - 2bX^2 + (b^2 + ac - 4d)X + (a^2d + c^2 - abc),$$

which resembles the formula for $R_3(X)$ in (3.7), although the X-coefficient of $R_3(X)$ is a bit simpler. This alternate resolvent, like $R_3(X)$, has the same discriminant as $f(X)$. We will not use it.

Let G_f be the Galois group of $f(X)$ over K.

Theorem 3.6. *With notation as above, G_f can be described in terms of whether or not* $\operatorname{disc} f$ *is a square in K and whether or not $R_3(X)$ factors in $K[X]$, according to Table 4.*

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

TABLE 4.

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

disc f is not a square and $R_3(X)$ is irreducible over K: Since $\operatorname{disc} f \neq \square$, $G_f \not\subset A_4$. 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. It's also divisible by 4, so $G_f = S_4$ or A_4, which implies $G_f = S_4$. This is like Example 3.2.

disc f is a square and $R_3(X)$ is irreducible over K: We have $G_f \subset A_4$ and $\#G_f$ is divisible by 3 and 4, so $G_f = A_4$. This is like Example 3.3.

disc f is not a square and $R_3(X)$ is reducible over K: Since $\operatorname{disc} f \neq \square$, 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, so the G_f-orbit of that root is just itself, not three numbers. We have a contradiction.

disc f is a square and $R_3(X)$ is 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 $R_3(X)$ is (separable and) reducible over K. Thus G_f contains no 3-cycles. $\square$

Table 5 gives some examples of Galois group computations over $\mathbf{Q}$ using Theorem 3.6. The discriminant of $f(X)$ is written as a squarefree number times a perfect square and $R_3(X)$ (computed from (3.8)) is factored into irreducibles over $\mathbf{Q}$.

Example 3.7. Let F be a field and u be transcendental over F. In $F(u)[X]$, the polynomial $X^4 + uX + u$ is irreducible. Its discriminant is $-27u^4 + 256u^3 = u^3(256 - 27u)$. When F doesn't have characteristic 2 or 3, the discriminant has a simple factor $256 - 27u$, so it is

$f(X)$	$\operatorname{disc} f$	$R_3(X)$	G_f
$X^4 - X - 1$	-283	$X^3 + 4X - 1$	S_4
$X^4 + 2X + 2$	$101 \cdot 4^2$	$X^3 - 8X - 4$	S_4
$X^4 + 8X + 12$	576^2	$X^3 - 48X - 64$	A_4
$X^4 + 3X + 3$	$21 \cdot 15^2$	$(X + 3)(X^2 - 3X - 3)$	D_4 or $\mathbf{Z}/4\mathbf{Z}$
$X^4 + 5X + 5$	$5 \cdot 55^2$	$(X - 5)(X^2 + 5X + 5)$	D_4 or $\mathbf{Z}/4\mathbf{Z}$
$X^4 + 36X + 63$	4320^2	$(X - 18)(X + 6)(X + 12)$	V

TABLE 5.

not a square. When F has characteristic 3, the discriminant is $256u^3 = u^3$, which is not a square. Therefore the discriminant is not a square when F doesn't have characteristic 2.

The cubic resolvent of $X^4 + uX + u$ is $X^3 - 4uX - u^2$, which is irreducible in $F(u)[X]$ since it is a cubic without roots in $F(u)$ (for degree reasons). Theorem 3.6 tells us the Galois group of $X^4 + uX + u$ over $F(u)$ is S_4.

By Theorem 3.6, $R_3(X)$ is reducible over K only when G_f is D_4, $\mathbf{Z}/4\mathbf{Z}$, or V. In the examples in Table 5 of such Galois groups, $R_3(X)$ has one root in $\mathbf{Q}$ when G_f is D_4 or $\mathbf{Z}/4\mathbf{Z}$ and all three roots are in $\mathbf{Q}$ when G_f is V. This is a general phenomenon.

Corollary 3.8. *With notation as in Theorem 3.6, $G_f = V$ 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: $\operatorname{disc} f = \Box$ and $R_3(X)$ is reducible over K. Since $\operatorname{disc} R_3 = \operatorname{disc} f$, $G_f = V$ if and only if $\operatorname{disc} R_3$ is a square in K and R_3 is reducible over K. By Theorem 2.6, a splitting field of $R_3(X)$ over K is $K(r, \sqrt{\operatorname{disc} R_3})$, where r is any root of $R_3(X)$. Therefore $G_f = V$ if and only if R_3 splits completely over K.

The condition for G_f to be D_4 or $\mathbf{Z}/4\mathbf{Z}$ is: $\operatorname{disc} f \neq \Box$ in K and $R_3(X)$ is reducible over K. These conditions, by Theorem 2.6 for the cubic $R_3(X)$, are equivalent to $R_3(X)$ having a root in K but not splitting completely over K, which is the same as saying $R_3(X)$ has a unique root in K. $\Box$

Theorem 3.6 does not decide between the Galois groups D_4 and $\mathbf{Z}/4\mathbf{Z}$. The following theorem provides a partial way to do this when the base field is $\mathbf{Q}$, by checking the sign of the discriminant.

Theorem 3.9. *Let $f(X)$ be an irreducible quartic in $\mathbf{Q}[X]$. If $G_f = \mathbf{Z}/4\mathbf{Z}$ then $\operatorname{disc} f > 0$. Therefore if G_f is D_4 or $\mathbf{Z}/4\mathbf{Z}$ and $\operatorname{disc} f < 0$, $G_f = D_4$.*

Proof. If $G_f = \mathbf{Z}/4\mathbf{Z}$, the splitting field of $f(X)$ over $\mathbf{Q}$ has degree 4. Any root of $f(X)$ already generates an extension of $\mathbf{Q}$ with degree 4, so the field generated over K by one root of $f(X)$ contains all the other roots. Therefore if $f(X)$ has one real root it has 4 real roots: the number of real roots of $f(X)$ is either 0 or 4.

If $f(X)$ has 0 real roots then they fall into complex conjugate pairs, say z and $\overline{z}$ and w and $\overline{w}$. Then $\operatorname{disc} f$ is the square of

$$(z - \overline{z})(z - w)(z - \overline{w})(\overline{z} - w)(\overline{z} - \overline{w})(w - \overline{w}) = |z - w|^2 |z - \overline{w}|^2 (z - \overline{z})(w - \overline{w}). \tag{3.9}$$

The differences $z - \overline{z}$ and $w - \overline{w}$ are purely imaginary (and nonzero, since z and w are not real), so their product is real and nonzero. Thus when we square (3.9), we find $\operatorname{disc} f > 0$.

If $f(X)$ has 4 real roots then the product of the differences of its roots is real and nonzero, so $\operatorname{disc} f > 0$. □

Example 3.10. The polynomial $X^4 + 4X^2 - 2$, which is irreducible by the Eisenstein criterion, has discriminant -18432 and cubic resolvent $X^3-4X^2+8X-32 = (X-4)(X^2+8)$. Theorem 3.6 says its Galois group is D_4 or $\mathbf{Z}/4\mathbf{Z}$. Since the discriminant is negative, Theorem 3.9 says the Galois group must be D_4.

Theorem 3.9 does not distinguish D_4 and $\mathbf{Z}/4\mathbf{Z}$ as Galois groups when $\operatorname{disc} f > 0$, since some polynomials with Galois group D_4 have positive discriminant. For example, we can't decide yet in Table 5 if $X^4 + 5X + 5$ has Galois group D_4 or $\mathbf{Z}/4\mathbf{Z}$ over $\mathbf{Q}$.

Remark 3.11. Any quartic in $\mathbf{Q}[X]$, reducible or not, has its nonreal roots coming in complex-conjugate pairs, so a separable quartic $f(X)$ has either 0, 2, or 4 nonreal roots, and thus 4, 2, or 0 real roots respectively. The computation in the proof of Theorem 3.9 shows $\operatorname{disc} f > 0$ if $f(X)$ has 0 or 4 real roots, whether or not $f(X)$ is irreducible. When $f(X)$ has 2 real roots, $\operatorname{disc} f < 0$.

Remark 3.12. More careful methods lead to a stronger conclusion in Theorem 3.9: if $G_f = \mathbf{Z}/4\mathbf{Z}$ then $\operatorname{disc} f$ is a sum of two rational squares. This is a much stronger constraint on the condition $G_f = \mathbf{Z}/4\mathbf{Z}$ than saying $\operatorname{disc} f > 0$, and can be used quite effectively to show a Galois group is not $\mathbf{Z}/4\mathbf{Z}$ in case $\operatorname{disc} f > 0$. But it is not an if and only if criterion: some quartics with Galois group D_4 have a discriminant that is a sum of two squares.

4. Galois groups of quartics: D_4 and $\mathbf{Z}/4\mathbf{Z}$

In this section we develop a method that separates D_4 from $\mathbf{Z}/4\mathbf{Z}$ as Galois groups of quartics Let $f(X) \in K[X]$ be an irreducible quartic where K does not have characteristic 2. By Theorem 3.6, G_f is D_4 or $\mathbf{Z}/4\mathbf{Z}$ if and only if

$$\Delta := \operatorname{disc} f \neq \square \text{ in } K \text{ and } R_3(X) \text{ is reducible over } K.$$

When this happens, Corollary 3.8 tells us $R_3(X)$ has a unique root r' in K.

Theorem 4.1 (Kappe, Warren)**.** *Let K be a field not of characteristic 2, $f(X) = X^4 + aX^3 + bX^2 + cX + d \in K[X]$, and $\Delta = \operatorname{disc} f$. Suppose $\Delta \neq \square$ in K and $R_3(X)$ is reducible in $K[X]$ with unique root $r' \in K$. Then $G_f = \mathbf{Z}/4\mathbf{Z}$ if the polynomials $X^2 + aX + (b - r')$ and $X^2 - r'X + d$ split over $K(\sqrt{\Delta})$, while $G_f = D_4$ otherwise.*

Proof. Index the roots r_1, r_2, r_3, r_4 of $f(X)$ so that $r' = r_1r_2 + r_3r_4$. Both D_4 and $\mathbf{Z}/4\mathbf{Z}$, as subgoups of S_4, contain a 4-cycle. (The elements of order 4 in S_4 are 4-cycles.) In Table 6 we describe the effect of each 4-cycle in S_4 on $r_1r_2 + r_3r_4$ if the 4-cycle were in the Galois group. The (distinct) roots of $R_3(X)$ are in the second column, each appearing twice.

Since $r_1r_2 + r_3r_4$ is fixed by G_f, the only possible 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.

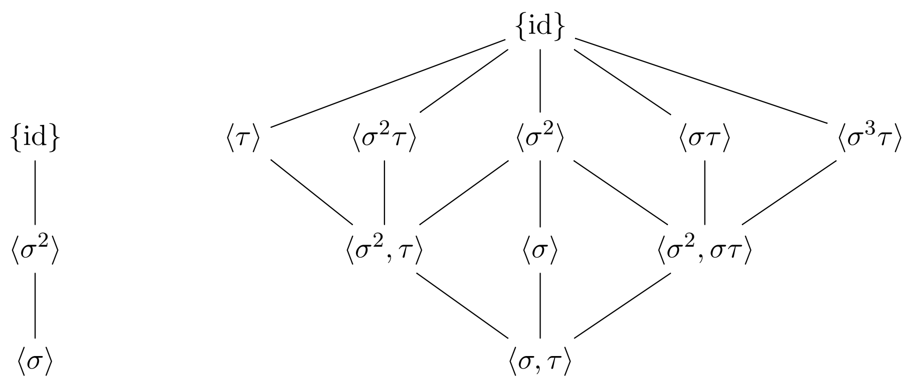
The subgroups of $\langle\sigma\rangle$ and $\langle\sigma, \tau\rangle$ look very different. See the diagrams below, where the subgroup lattices are written upside down.

$(abcd)$	$(abcd)(r_1r_2 + r_3r_4)$
(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)	$r_4r_3 + r_1r_2$

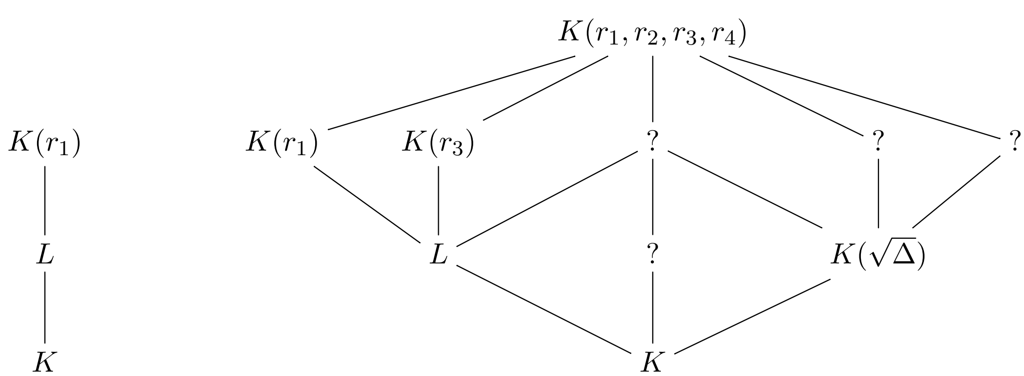
TABLE 6.

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.



Corresponding to the above subgroup lattices we have the following subfield lattices of the splitting field, where L in both cases denotes the unique quadratic extension of K inside $K(r_1)$: if $G_f = \mathbf{Z}/4\mathbf{Z}$ then L corresponds to $\langle \sigma^2 \rangle$, while if $G_f = D_4$ then L corresponds to $\langle \sigma^2, \tau \rangle$. Since $\Delta \neq \Box$ in K, $[K(\sqrt{\Delta}) : K] = 2$.



If $G_f = \mathbf{Z}/4\mathbf{Z}$, then $L = K(\sqrt{\Delta})$ since there is only one quadratic extension of K in the splitting field.

If $G_f = D_4$, then let's explain how, in the subgroup and subfield lattice diagrams above, we know $K(r_1)$ corresponds to $\langle\tau\rangle$, $K(r_3)$ corresponds to $\langle\sigma^2\tau\rangle$, and $K(\sqrt{\Delta})$ 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. The subgroup corresponding to $K(\sqrt{\Delta})$ is the even permutations in the Galois group, and that is $\{(1), (12)(34), (13)(24), (14)(23)\} = \langle\sigma^2, \sigma\tau\rangle$.

Although the two cases $G_f = \mathbf{Z}/4\mathbf{Z}$ and $G_f = D_4$ 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 before we distinguish the two cases from each other.

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

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

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

$$r_1 + r_2 \notin K \quad \text{or} \quad r_1 r_2 \notin K. \tag{4.1}$$

If $G_f = \mathbf{Z}/4\mathbf{Z}$ then $\mathrm{Gal}(L/K) = \langle\sigma\rangle/\langle\sigma^2\rangle = \{1, \overline{\sigma}\}$, and if $G_f = D_4$ then $\mathrm{Gal}(L/K) = \langle\sigma, \tau\rangle/\langle\sigma^2, \tau\rangle = \{1, \overline{\sigma}\}$. The coset of σ in $\mathrm{Gal}(L/K)$ represents the nontrivial coset both times, so $L^\sigma = K$. That is, an element of L fixed by σ is in K. Since $\sigma(r_1 + r_2) = r_3 + r_4$ and $\sigma(r_1 r_2) = r_3 r_4$, the polynomials

$$(X - (r_1 + r_2))(X - (r_3 + r_4)) = X^2 - (r_1 + r_2 + r_3 + r_4)X + (r_1 + r_2)(r_3 + r_4), \tag{4.2}$$

and

$$(X - r_1 r_2)(X - r_3 r_4) = X^2 - (r_1 r_2 + r_3 r_4)X + r_1 r_2 r_3 r_4 \tag{4.3}$$

have coefficients in $L^\sigma = K$.

The linear coefficient in (4.2) is a and the constant term is

$$(r_1 + r_2)(r_3 + r_4) = r_1 r_3 + r_1 r_4 + r_2 r_3 + r_2 r_4 = b - (r_1 r_2 + r_3 r_4) = b - r',$$

so (4.2) equals $X^2 + aX + (b - r')$. The quadratic polynomial (4.3) is $X^2 - r'X + d$. When $r_1 + r_2 \notin K$, (4.2) is irreducible in $K[X]$, so its discriminant is a nonsquare in K, and if $r_1 + r_2 \in K$ then (4.2) has a double root and its discriminant is 0. Similarly, (4.3) has a discriminant that is a nonsquare in K or is 0. Therefore the splitting field of (4.2) or (4.3) over K is either L or K and (4.1) tells us at least one of (4.2) and (4.3) has a nonsquare discriminant in 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 (4.1).

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

Next suppose $G_f = D_4$. Then $L \neq K(\sqrt{\Delta})$. By (4.1) at least one of (4.2) or (4.3) is irreducible over K, so its roots generate L over K and therefore are not in $K(\sqrt{\Delta})$. Thus the polynomial in (4.2) or (4.3) will be irreducible over $K(\sqrt{\Delta})$ if it's irreducible over K.

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

Remark 4.2. The proof of Theorem 4.1 by Kappe and Warren shows $G_f = \mathbf{Z}/4\mathbf{Z}$ if and only if $X^2 + aX + (b - r')$ and $X^2 - r'X + d$ split completely over $K(\sqrt{\Delta})$, thereby not having to treat the case $G_f = D_4$ directly.

Corollary 4.3. *When K does not have characteristic 2 and*

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

is an irreducible quartic in $K[X]$, define

$$\Delta = \operatorname{disc} f \text{ and } R_3(X) = X^3 - bX^2 + (ac - 4d)X - (a^2d + c^2 - 4bd).$$

The Galois group of $f(X)$ over K is described by Table 8.

Δ *in* K	$R_3(X)$ *in* $K[X]$	$(a^2 - 4(b - r'))\Delta$ *and* $(r'^2 - 4d)\Delta$	G_f
$\neq \square$	*irreducible*		S_4
$= \square$	*irreducible*		A_4
$\neq \square$	*root* $r' \in K$	*at least one* $\neq \square$ *in* K	D_4
$\neq \square$	*root* $r' \in K$	*both* $= \square$ *in* K	$\mathbf{Z}/4\mathbf{Z}$
$= \square$	*reducible*		V

TABLE 8.

Proof. The polynomials $X^2 + aX + (b - r')$ and $X^2 - r'X + d$ split completely over $K(\sqrt{\Delta})$ if and only if their discriminants $a^2 - 4(b - r')$ and $r'^2 - 4d$ are squares in $K(\sqrt{\Delta})$. We saw in the proof of Theorem 4.1 that these discriminants are either 0 or nonsquares in K. A nonsquare in K is a square in $K(\sqrt{\Delta})$ if and only if its product with Δ is a square, and this is vacuously true for 0 also. $\square$

In Table 9 we list the Galois groups over $\mathbf{Q}$ of several quartic trinomials $X^4 + cX + d$. All but the last is Eisenstein at some prime; check as an exercise that the last polynomial in the table is irreducible over $\mathbf{Q}$. Verify all of the Galois group computations using Corollary 4.3. If you pick a quartic in $\mathbf{Q}[X]$ at random it probably will be irreducible and have Galois group S_4, or perhaps A_4 if by chance the discriminant is a square, so we only list examples in Table 9 where the Galois group is smaller, which means the cubic resolvent is reducible. Since $a = b = 0$, so $a^2 - 4(b - r') = 4r'$, to decide when G_f is D_4 or $\mathbf{Z}/4\mathbf{Z}$ we need to decide when the rational numbers $4r'\Delta$ and $(r'^2 - 4d)\Delta$ are both squares in $\mathbf{Q}$.

$X^4 + cX + d$	Δ	$X^3 - 4dX - c^2$	$4r'\Delta$ and $(r'^2 - 4d)\Delta$	G_f
$X^4 + 3X + 3$	$21 \cdot 15^2$	$(X + 3)(X^2 - 3X - 3)$	$-56700, \quad -14175$	D_4
$X^4 + 5X + 5$	$5 \cdot 55^2$	$(X - 5)(X^2 + 5X + 5)$	$550^2, \quad 275^2$	$\mathbf{Z}/4\mathbf{Z}$
$X^4 + 8X + 14$	$2 \cdot 544^2$	$(X - 8)(X^2 + 8X + 8)$	$4608^2, \quad 2176^2$	$\mathbf{Z}/4\mathbf{Z}$
$X^4 + 13X + 39$	$13 \cdot 1053^2$	$(X - 13)(X^2 + 13X + 13)$	$27378^2, \quad 13689^2$	$\mathbf{Z}/4\mathbf{Z}$
$X^4 + 36X + 63$	4320^2	$(X - 18)(X + 6)(X + 12)$	irrelevant	V

TABLE 9.

Remark 4.4. Remark 2.3 about cubics also holds for quartics: don't forget to check that your quartic is irreducible before applying Corollary 4.3. For example, X^4+4 has discriminant 128^2 and cubic resolvent $X^3-16X = X(X+4)(X-4)$. Such data (square discriminant, reducible resolvent) suggest the Galois group of X^4+4 over $\mathbf{Q}$ is V, but X^4+4 is *reducible*: it factors as $(X^2+2X+2)(X^2-2X+2)$. Both factors have discriminant -4, so the splitting field of X^4+4 over $\mathbf{Q}$ is $\mathbf{Q}(\sqrt{-4}) = \mathbf{Q}(i)$ and the Galois group of X^4+4 over $\mathbf{Q}$ is cyclic of order 2.

As another example, $X^4+3X+20$ has discriminant $\Delta = 77\cdot 163^2$ and its cubic resolvent is $(X-9)(X^2+9X+1)$, which suggests the Galois group is D_4 or $\mathbf{Z}/4\mathbf{Z}$. Since $r'=9$ and $(r'^2-4d)\Delta = 77\cdot 163^2$ is not a square, it looks like the Galois group is D_4, but the quartic is reducible: it is $(X^2+3X+4)(X^2-3X+5)$. The factors have discriminants -7 and -11, so the splitting field of $X^4+3X+20$ over $\mathbf{Q}$ is $\mathbf{Q}(\sqrt{-7},\sqrt{-11})$, whose Galois group over $\mathbf{Q}$ is V.

Exercise. Show $X^4+24X+36$ has Galois group A_4 over $\mathbf{Q}$ and $X^4+24X+73$ has Galois group V over $\mathbf{Q}$. Remember to prove both polynomials are irreducible over $\mathbf{Q}$ first!

From Corollary 4.3 we obtain the following Galois group test for irreducible quartics of the special form X^4+bX^2+d.

Corollary 4.5. *Let $f(X) = X^4+bX^2+d$ be irreducible in $K[X]$, where K does not have characteristic 2. Its Galois group over K is V, $\mathbf{Z}/4\mathbf{Z}$, or D_4 according to the following conditions.*

(1) *If $d = \square$ in K then $G_f = V$.*
(2) *If $d \neq \square$ in K and $(b^2-4d)d = \square$ in K then $G_f = \mathbf{Z}/4\mathbf{Z}$.*
(3) *If $d \neq \square$ in K and $(b^2-4d)d \neq \square$ in K then $G_f = D_4$.*

In the second condition, we could simplify the hypothesis to just $(b^2-4d)d = \square$ in K since this forces $d \neq \square$: if $(b^2-4d)d = \square$ and $d = \square$ then $b^2-4d = \square$, which contradicts irreducibility of X^4+bX^2+d.

Proof. The discriminant of X^4+bX^2+d is $16d(b^2-4d)^2$. By hypothesis the discriminant is nonzero, so up to square factors it is the same as d.

The cubic resolvent is

$$X^3-bX^2-4dX+4bd = (X-b)(X^2-4d),$$

which is reducible over K with b as a root. In the notation of Corollary 4.3, if Δ is not a square then $r'=b$, so $r'^2-4d = b^2-4d$ and $a^2-4(b-r') = 0$. Translating Corollary 4.3 into the three conditions above is left to the reader. $\square$

In Table 10 are some examples over $\mathbf{Q}$.

The roots of a polynomial X^4+bX^2+d can be written down explicitly, using iterated square roots. Therefore it will come as no surprise that Corollary 4.5 was known before Corollary 4.3. The earliest reference to Corollary 4.5 which I know is an exercise in [1, p. 53].

Appendix A. The Old Distinction Between D_4 and $\mathbf{Z}/4\mathbf{Z}$

Before Kappe and Warren proved Theorem 4.1, the following theorem was the classical procedure to decide between D_4 and $\mathbf{Z}/4\mathbf{Z}$ as Galois groups (outside of characteristic 2).

X^4+bX^2+d	d	$(b^2-4d)d$	G_f
X^4+4X^2+1	1	12	V
X^4-4X^2+2	2	16	$\mathbf{Z}/4\mathbf{Z}$
X^4+4X^2-2	-2	-16	D_4
X^4+5X^2+2	2	34	D_4
X^4-5X^2+5	5	25	$\mathbf{Z}/4\mathbf{Z}$
X^4-5X^2+3	3	13	D_4

TABLE 10.

Theorem A.1. *Let $f(X) \in K[X]$ be an irreducible quartic, where K does not have characteristic 2, and set $\Delta = \operatorname{disc} f$. Suppose Δ 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 $K(\sqrt{\Delta})$ then $G_f = D_4$.*
(2) *If $f(X)$ is reducible over $K(\sqrt{\Delta})$ then $G_f = \mathbf{Z}/4\mathbf{Z}$.*

Proof. We will make reference to the field diagrams for the two possible Galois groups in Section 4.

When $G_f = D_4$, the field diagram in this case shows the splitting field of $f(X)$ over K is $K(r_1, \sqrt{\Delta})$. Since $[K(r_1, \sqrt{\Delta}) : K] = 8$, $[K(r_1, \sqrt{\Delta}) : K(\sqrt{\Delta})] = 4$, so $f(X)$ must be irreducible over $K(\sqrt{\Delta})$.

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

Because the different Galois groups imply different behavior of $f(X)$ over $K(\sqrt{\Delta})$, these properties of $f(X)$ over $K(\sqrt{\Delta})$ tell us the Galois group. □

Example A.2. Taking $K = \mathbf{Q}$, the polynomials X^4+3X+3 and X^4+5X+5 from Table 5 both fit the hypotheses of Theorem A.1. We will use Theorem A.1 to show the Galois groups over $\mathbf{Q}$ are as listed in Table 11.

$f(X)$	$\operatorname{disc} f$	$R_3(X)$	G_f
X^4+3X+3	$21 \cdot 15^2$	$(X+3)(X^2-3X-3)$	D_4
X^4+5X+5	$5 \cdot 55^2$	$(X-5)(X^2+5X+5)$	$\mathbf{Z}/4\mathbf{Z}$

TABLE 11.

To compute the Galois groups using Theorem A.1, we need to decide if X^4+3X+3 is irreducible over $\mathbf{Q}(\sqrt{21})$ and if X^4+5X+5 is irreducible over $\mathbf{Q}(\sqrt{5})$. Theorem A.1 says that when the polynomial is irreducible over the quadratic field, its Galois group over $\mathbf{Q}$ is D_4. If it factors over the quadratic field then the Galois group is $\mathbf{Z}/4\mathbf{Z}$.

These quartics are both irreducible over $\mathbf{Q}$, so their roots have degree 4 over $\mathbf{Q}$ and therefore don't lie in a quadratic field. That means if either of these quartics factors over a quadratic field, it must be a product of two quadratic factors rather than into a linear times a cubic.

To decide if X^4+3X+3 is irreducible over $\mathbf{Q}(\sqrt{21})$, we set up a hypothetical factorization

$$X^4 + 3X + 3 = (X^2 + AX + B)(X^2 + CX + D) \tag{A.1}$$

and read off the algebraic conditions imposed on the coefficients:

$$A + C = 0, \quad B + D + AC = 0, \quad AD + BC = 3, \quad BD = 3. \tag{A.2}$$

Therefore $C = -A$ and $D = -AC - B = A^2 - B$, so the third condition in (A.2) becomes $A(A^2 - 2B) = 3$. Necessarily $A \neq 0$ and we can solve for B:

$$B = \frac{A^3 - 3}{2A}.$$

Therefore the condition $BD = 3$ becomes

$$3 = \frac{A^3 - 3}{2A}\left(A^2 - \frac{A^3 - 3}{2A}\right) = \frac{A^6 - 9}{4A^2}.$$

Clearing the denominator,

$$0 = A^6 - 12A^2 - 9 = (A^2 + 3)(A^4 - 3A^2 - 3). \tag{A.3}$$

This equation needs to have a solution A in $\mathbf{Q}(\sqrt{21})$. The condition $A^2 + 3 = 0$ obviously has no solution in $\mathbf{Q}(\sqrt{21}) \subset \mathbf{R}$. Since $X^4 - 3X^2 - 3$ is irreducible over $\mathbf{Q}$, its roots have degree 4 over $\mathbf{Q}$ and therefore can't lie in $\mathbf{Q}(\sqrt{21})$. So we have a contradiction, which proves $X^4 + 3X + 3$ is irreducible over $\mathbf{Q}(\sqrt{21})$, and that means the Galois group of $X^4 + 3X + 3$ over $\mathbf{Q}$ is D_4. Compare the way this method treats $X^4 + 3X + 3$ and the earlier procedure in Table 9!

If we set up a hypothetical factorization of $X^4 + 5X + 5$ over $\mathbf{Q}(\sqrt{5})$ as in (A.1), but with coefficients of 5 in place of 3 on the left side of (A.1), we get constraints similar to (A.2), and the analogue of (A.3) is

$$0 = A^6 - 20A^2 - 25 = (A^2 - 5)(A^4 + 5A^2 + 5), \tag{A.4}$$

which has an obvious solution in $\mathbf{Q}(\sqrt{5})$: $A = \sqrt{5}$. This leads to the factorization

$$X^4 + 5X + 5 = \left(X^2 + \sqrt{5}X + \frac{5 - \sqrt{5}}{2}\right)\left(X^2 - \sqrt{5}X + \frac{5 + \sqrt{5}}{2}\right),$$

so $X^4 + 5X + 5$ has Galois group $\mathbf{Z}/4\mathbf{Z}$ over $\mathbf{Q}$.

It's intriguing that to solve for A, the right sides of both (A.3) and (A.4) equal the cubic resolvent from Table 11 evaluated at A^2. Is A always a root of $R_3(X^2)$? No. For example, if

$$f(X) = X^4 + 2X^3 - 6X^2 - 2X + 1$$

then its cubic resolvent (using (3.7)) is

$$R_3(X) = X^3 + 6X^2 - 8X - 32 = (X + 2)(X^2 + 4X - 16),$$

and in a factorization $f(X) = (X^2 + AX + B)(X^2 + CX + D)$ computations similar to the ones above show A is a root of

$$X^6 - 6X^5 + 40X^3 - 20X^2 - 56X + 16 = (X^2 - 2X - 4)(X^4 - 4X^3 - 4X^2 + 16X - 4),$$

which is not $R_3(X^2)$. But it is $R_3(X^2 - 2X - 6)$. Further investigation into the relationship between factorizations of $f(X)$ and $R_3(X)$ is left to the reader.

As this example illustrates, Theorem A.1 is tedious to use by hand to distinguish between Galois groups D_4 and $\mathbf{Z}/4\mathbf{Z}$. The theorem of Kappe and Warren is a lot nicer. Of course if you have access to a computer algebra package that can factor quartic polynomials over quadratic fields, then Theorem A.1 becomes an attractive method.

References

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

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