# GALOIS THEORY AND QUARTIC POLYNOMIALS

MOHABAT TARKESHIAN

Winter Term 2018

## 1. BASIC DEFINITIONS AND RESULTS

Let $K \subseteq L \subseteq \mathbb{C}$ be subfields.

*Definition* 1.1. Let $\Omega_L = \mathrm{Hom}(L, \mathbb{C})$ be the set of embeddings of $L$ into $\mathbb{C}$. Denote the embeddings of $L$ that restrict to the inclusion map on $K$ by $\Omega_{L/K}$:

$$\Omega_{L/K} := \{\varphi \in \Omega_L \mid \varphi|_K = \iota_K\}$$

Define the set of *normal embeddings* $\Omega^{\nu}_{L/K}$ as the embeddings in $\Omega_{L/K}$ such that their image is contained in $L$, i.e.,

$$\Omega^{\nu}_{L/K} := \{\varphi \in \Omega_{L/K} \mid \varphi(L) \subseteq L\}$$

$L \subseteq \overline{K}$ is said to be a *Galois extension* if and only if $\Omega^{\nu}_{L/K} = \Omega_{L/K}$.

Let $f \in K[x]$ be a monic polynomial. Denote the set of zeros of $f$ as $Z_f \subseteq \mathbb{C}$.

*Definition* 1.2. $K(Z_f)$ is called the *splitting field* of $f$ over $K$.

– $L/K$ *splits* $f$ if and only if $Z_f \subseteq L$.

Let $\alpha_1, \alpha_2, \ldots, \alpha_m \in \overline{K}$ and $L = K(\alpha_1, \alpha_2, \ldots, \alpha_m) \subseteq \overline{K}$. Let $\pi_{\alpha_i} \in K[x]$ denote the minimal polynomial for each $\alpha_i$.

**Proposition 1.3.** *The following are equivalent.*

1. *$L/K$ is a Galois extension;*
2. *$L/K$ splits $\pi_{\alpha_1}, \ldots, \pi_{\alpha_m}$;*
3. *$L/K$ is the splitting field of some polynomial $f \in K[x]$;*
4. *$L/K$ splits $\pi_\alpha$ for every $\alpha \in L$.*

*Definition* 1.4. The set of automorphisms of $L$ that fix $K$ is denoted as

$$\mathrm{Aut}_K(L) := \{\varphi : L \overset{\cong}{\to} L \mid \varphi|_K = \mathrm{id}_K\}$$

Given a Galois extension $L/K$, the *Galois group* of $L/K$ is this set of automorphisms.

$$\mathrm{Gal}(L/K) := \mathrm{Aut}_K(L)$$

**Theorem 1.** *Fundamental theorem of Galois theory.*

*Let $M/K$ be a Galois extension and $G = \mathrm{Gal}(M/K)$. There exists a bijection:*

$$\{\textit{subfields } L \textit{ of } M \textit{ containing } K\} \leftrightarrow \{\textit{subgroups } H \textit{ of } G\}$$

*given by:*

$$L \mapsto \{\textit{elements of } G \textit{ fixing } L\} = \mathrm{stab}_G(L)$$
$$\{\textit{fixed field of } H\} \hookleftarrow H \leq G$$

*Definition* 1.5. The *fixed field* of a subgroup $H \leq G$ of a Galois group is the set of all $x \in M$ that are fixed by all elements of the subgroup $H$, i.e.,

$$M^H = \{x \in M \mid \sigma(x) = x \text{ for all } \sigma \in H\}$$

*Definition* 1.6. The *Galois group of a monic polynomial* $f \in K[x]$ is the Galois group of the splitting field of $f$ over $K$:

$$\mathrm{Gal}(f) := \mathrm{Gal}(K(Z_f)/K)$$

**Theorem 2.** *$f(x) \in K[x]$ is irreducible if and only if $\mathrm{Gal}(f) \leq S_n$ is a transitive subgroup.*

*That is, the Galois group of a monic polynomial acts transitively on the roots.*

## 2. DISCRIMINANTS AND GALOIS GROUPS OF CUBICS

Let $K \subseteq \mathbb{C}$ be a subfield as before. Let $f(x) \in K[x]$ be a monic polynomial.

*Definition* 2.1. The *discriminant* $\delta$ of $x_1, x_2, \ldots, x_n$ is defined by

$$\delta = \prod_{i<j} (x_i - x_j)^2$$

– The *discriminant of a polynomial*, denoted $\operatorname{disc} f$, is the discriminant of the roots of the polynomial.

**Claim 2.2.** *A permutation $\sigma \in S_n$ is an element of the alternating group $A_n$ if and only if $\sigma$ fixes the product:*

$$\sqrt{\delta} = \prod_{i<j} (x_i - x_j) \in \mathbb{Z}[x_1, x_2, \ldots, x_n]$$

*Then, $\sqrt{\delta}$ generates the fixed field of $A_n$ and generates a quadratic extension of $K$, leading to the following proposition.*

**Proposition 2.3.** *The permutation $\sigma \in S_n$ is an element of $A_n$ if and only if $\sigma(\sqrt{\delta}) = \sqrt{\delta}$.*

**Corollary 2.4.** *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 $K$.*

*Remark* 2.5. The disriminant is symmetric in the roots of a polynomial $f(x) \in K[x]$, hence it is fixed by all the elements of the Galois group of $f(x)$.

– Since $\sqrt{\delta} = \prod_{i<j} (\alpha_i - \alpha_j)$, then $\sqrt{\delta}$ is always an element of the splitting field of $f(x)$.

**Theorem 3.** *Let $f(x) \in K[x]$ be an irreducible cubic polynomial. Then,*

$$\operatorname{Gal}(f) = \begin{cases} A_3 & \text{if } \operatorname{disc} f = \square \text{ in } K \\ S_3 & \text{if } \operatorname{disc} f \neq \square \text{ in } K \end{cases}$$

*Proof.*

The Galois group of the splitting field of $f(x)$ over $K$ is a transitive subgroup of $S_3$ by Theorem 2.

$S_3$ only has two transitive subgroups: the alternating group $A_3$ and the group iteself $S_3$. By Corollary 2.4, the result follows. ☐

## 3. Galois resolvents

- If a cubic polynomial is irreducible, its Galois group is easily determined by the characterization given in Theorem 3.
  - Whether or not $\operatorname{disc} f$ is a square in $K$ is the same as determining whether the quadratic polynomial $(x^2 - \operatorname{disc} f)$ has a root in $K$.
  - That is, the Galois group of a cubic depends on a quadratic polynomial.

- In an analogous way, if a quartic polynomial is irreducible, an associated cubic polynomial aids in the determination of its Galois group. This is called its cubic (or Galois) resolvent.

### 3.1. **General definition.**

*Definition* 3.1. Let $x_1, x_2, \dots, x_n$ be indeterminates. The *elementary simple functions* $y_1, y_2, \dots, y_n$ are defined by:

$$\begin{aligned} y_1 &= x_1 + x_2 + \cdots + x_n \\ y_2 &= x_1x_2 + x_1x_3 + \cdots + x_2x_3 + \cdots + x_{n-1}x_n \\ &\vdots \\ y_n &= x_1x_2\cdots x_n \end{aligned}$$

– That is, the elementary simple function $y_i$ in the indeterminates $x_1, x_2, \dots x_n$ is the sum of all products of distinct $x_j's$ taken $i$ at a time.

Let $\mathbb{Q}(\boldsymbol{x}) = \mathbb{Q}(x_1, x_2, \dots, x_n)$ be the field of *rational* functions in $n$ indeterminates. Then, $S_n$ acts faithfully on $\mathbb{Q}(\boldsymbol{x})$ by permuting the indeterminates. That is, for all $s \neq (1) \in S_n$, there exists $f(\boldsymbol{x}) \in \mathbb{Q}(\boldsymbol{x})$ such that $sf(\boldsymbol{x}) \neq f(\boldsymbol{x})$.

– The stabilizer of this action is the subfield of rational functions

$$\mathbb{Q}(\boldsymbol{y}) = \mathbb{Q}(y_1, y_2, \dots, y_n)$$

where $y_i$ is the $i^{th}$ *elementary simple function* in $x_1, x_2, \dots, x_n$. For any simple function, permuting the indeterminates does not change the function.

– By the fundamental theorem of Galois theory (Theorem 1), then

$$S_n \equiv \operatorname{Gal}(\mathbb{Q}(\boldsymbol{x})/\mathbb{Q}(\boldsymbol{y})).$$

By the fundamental theorem of Galois theory, for every subgroup $H \leq S_n$, there is a corresponding fixed field of $H$, denoted $\mathbb{Q}(\boldsymbol{x})^H$, consisting of every $f \in \mathbb{Q}(\boldsymbol{x})$ that is fixed by the subgroup $H$.

– Since $[\mathbb{Q}(\boldsymbol{x})^H : \mathbb{Q}(\boldsymbol{y})] < \infty$,

$$\mathbb{Q}(\boldsymbol{x})^H = \mathbb{Q}(\boldsymbol{y}, F(\boldsymbol{x}))$$

where $F(\boldsymbol{x}) = F(x_1, x_2, \dots, x_n) \in \mathbb{Q}(\boldsymbol{x})$ is some rational function. Take $F$ to be a polynomial in $x_1, x_2, \dots, x_n$.

*Definition* 3.2. The minimal polynomial for $F(\boldsymbol{x})$ over $\mathbb{Q}(\boldsymbol{y})$ is denoted $\Phi(z, \boldsymbol{y})$ and it is called the (general) *Galois resolvent of $H$ corresponding to $F(\boldsymbol{x})$*.

The roots of $\Phi(z, \boldsymbol{y})$ are the conjugates of $F(\boldsymbol{x})$ over $S_n$. Hence, over $\mathbb{Q}(\boldsymbol{y})$,

$$\Phi(z, \boldsymbol{y}) = \prod_{h \in S} (z - hF(\boldsymbol{x}))$$

where $S$ is the set of coset representatives of $S_n/H$, and

$$hF(\boldsymbol{x}) = F(h\boldsymbol{x})$$

where $h\boldsymbol{x} = (x_{h1}, x_{h2}, \ldots, x_{hn})$ (i.e., applying the permutation to the indeterminates).

**Claim 3.3.** *The coefficients of $\Phi(z, \boldsymbol{y})$ are polynomials in the elementary simple functions $y_1, y_2, \ldots, y_n$.*

The general Galois resolvent can be specialized to the case of a given polynomial $f(x) \in \mathbb{Q}[x]$. Suppose $f$ is monic such that

$$f(x) = x^n + a_1 x^{n-1} + \cdots + a_n \in \mathbb{Q}[x]$$

and $f$ has distinct roots $\alpha_1, \alpha_2, \ldots, \alpha_n$.

*Definition* 3.4. In definition 3.2, substitute $\boldsymbol{a} = (-a_1, a_2, \ldots, (-1)^n a_n)$ for $\boldsymbol{y}$ and $\boldsymbol{\alpha} = (\alpha_1, \alpha_2, \ldots, \alpha_n)$ for $\boldsymbol{x}$ to obtain the following *specialized Galois resolvent* for a polynomial $f(x) \in \mathbb{Q}[x]$:

$$\Phi(z, \boldsymbol{a}) = \prod_{h \in S} (z - hF(\boldsymbol{\alpha}))$$

- The coefficients of $\Phi(z, \boldsymbol{a})$ are rational numbers.

### 3.2. **The Galois resolvent of a quartic.**

Let $f(x) \in K[x]$ be an irreducible monic quartic polynomial such that

$$f(x) = x^4 + ax^3 + bx^2 + cx + d$$

*Definition* 3.5. The *resolvent cubic polynomial* of $f$, denoted $R_3(x)$, is

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

*Remark* 3.6. The derivation of this formula involves looking at the roots of the quartic $f(x) = (x - r_1)(x - r_2)(x - r_3)(x - r_4)$. $R_3(x)$ is then created with roots in the splitting field $K(Z_f)$. An expression in the roots of $f(x)$ which only has three possible images under the Galois group leads to the polynomial:

$$R_3(x) = (x - (r_1 r_2 + r_3 r_4))(x - (r_1 r_3 + r_2 r_4))(x - (r_1 r_4 + r_2 r_3))$$

Then, determining the coefficients of $R_3(x)$ in terms of the coefficients of $f$ involves multiplying and factoring the above expression.

## 4. THE GALOIS GROUP OF A QUARTIC POLYNOMIAL

Let $f(x) \in K[x]$ be an irreducible quartic monic polynomial.

As $f$ is irreducible, the Galois group of $f$ is transitive on the roots of $f$ by Theorem 2 (it is possible to get from one root to any other root by applying some element of the Galois group).

The only transitive subgroups of $S_4$ are as follows:

(i) $S_4$

(ii) Alternating group (order 12): $A_4$

(iii) Klein-4 group: $V = \{1, (12)(34), (13)(24), (14)(23)\} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$
- The Klein-4 group is a normal subgroup of $S_4$.

(iv) Cyclic group of order 4: $C_4 = \{1, (1234), (13)(24), (1432)\} \cong \mathbb{Z}/4\mathbb{Z}$ and its conjugates:
- $\{1, (1324), (12)(34), (1423)\}$ and
- $\{1, (1243), (14)(23), (1342)\}$.

(v) Dihedral group of order 8: $D_8 = \{1, (1324), (12)(34), (1423), (13)(24), (14)(23), (12), (34)\}$ and its conjugates:
- $\{1, (1234), (13)(24), (1432), (12)(34), (14)(23), (13), (24)\}$; and
- $\{1, (1243), (14)(23), (1342), (12)(34), (13)(24), (14), (23)\}$.

Note: The types of cycles determine the conjugacy classes.

**Theorem 4.** *The following table characterizes the Galois group of an irreducible quartic polynomial in terms of its discriminant and resolvent cubic polynomial.*

| disc $f \in K$ | $R_3(x) \in K[x]$ | Gal($f$) |
|---|---|---|
| *not* $\square$ *in* $K$ | *irreducible in* $K[x]$ | $S_4$ |
| $\square$ *in* $K$ | *irreducible in* $K[x]$ | $A_4$ |
| *not* $\square$ *in* $K$ | *reducible in* $K[x]$ | $D_8$ *or* $C_4$ |
| $\square$ *in* $K$ | *reducible in* $K[x]$ | $V$ |

TABLE 1.

*Proof.*

*Row 1:*

If $\operatorname{disc} f$ is not a $\square$ in $K$ and $R_3(x)$ is irreducible over $K$, then $\operatorname{Gal}(f) \not\leq A_4$ by Corollary 2.4.

Now, $3 \mid |\operatorname{Gal}(f)|$ since $R_3(x)$ is irreducible over $K$ and hence adding a root of $R_3(x)$ to $K$ results in a cubic extension of $K$ in $K(Z_f)$. Since the splitting field $K(Z_f)$ also contains $K(r_1)$ for a root $r_1$ of $f$, then $|\operatorname{Gal}(f)|$ is also divisible by 4. The only subgroups of $S_4$ with order divisible by 12 are $S_4$ and $A_4$. Since $\operatorname{Gal}(f) \neq A_4$, then $\operatorname{Gal}(f) = S_4$.

*Row 2:*

Suppose $\operatorname{disc} f$ is a $\square$ in $K$ and $R_3(x)$ is irreducible over $K$. Since $\operatorname{disc} f = \square$, then by Corollary 2.4, $\operatorname{Gal}(f) \leq A_4$. In the same way as row 1, 3 and 4 divide $|\operatorname{Gal}(f)|$. Hence, since $\operatorname{Gal}(f) \leq A_4$ and $12 \mid |\operatorname{Gal}(f)|$, then $\operatorname{Gal}(f) = A_4$.

*Row 3:*

If $\operatorname{disc} f$ is not a $\square$ in $K$ and $R_3(x)$ is reducible over $K$, then $\operatorname{Gal}(f) \not\leq A_4$ since $\operatorname{disc} f \neq \square$ by Corollary 2.4. Hence,

$$\operatorname{Gal}(f) = S_4, D_8, \text{ or } C_4$$

**Claim 4.1.** *If* $\operatorname{Gal}(f)$ *has a 3-cycle, then* $R_3(x)$ *is irreducible.*

*Proof of claim:* Suppose $\operatorname{Gal}(f)$ has a 3-cycle. Then, applying this 3-cycle to a root of the resolvent $R_3(x)$ yields all the distinct roots of $R_3(x)$ in a single orbit of $\operatorname{Gal}(f)$. This implies that $R_3(x)$ is irreducible over $K$. ∎

In this row, $R_3(x)$ is reducible over $K$, hence by the claim it follows that $\operatorname{Gal}(f)$ has no 3-cycles. Since $S_4$ has 3-cycles, it follows that

$$\operatorname{Gal}(f) = D_8 \text{ or } C_4$$

*Row 4:*

Supose $\operatorname{disc} f$ is a square in $K$ and $R_3(x)$ is reducible over $K$. Again, since $\operatorname{disc} f = \square$, then by Corollary 2.4, $\operatorname{Gal}(f) \leq A_4$. Hence,

$$\operatorname{Gal}(f) = A_4 \text{ or } V$$

Since in this row, $R_3(x)$ is reducible, by claim 4.1, it follows that $\operatorname{Gal}(f)$ has no 3-cycles. Since $A_4$ has 3-cycles and $V$ does not, then it follows that $\operatorname{Gal}(f) = V$.

□

### 4.1. **Distinguishing between $C_4$ and $D_8$.**

– Theorem 4 gives a useful charactierization of Galois groups of irreducible quartics. However, there is some ambiguity when $\operatorname{disc} f \neq \square$ and $R_3(x)$ is reducible. There is a further characterization that can be used to distinguish between these two subgroups.

**Theorem 5.** *Let $f(x) \in \mathbb{Q}[x]$ be an irreducible quartic. If $\operatorname{Gal}(f) = C_4$, then $\operatorname{disc} f > 0$.*

*Therefore, if $\operatorname{Gal}(f)$ is $D_8$ or $C_4$ and $\operatorname{disc} f < 0 \Rightarrow \operatorname{Gal}(f) = D_8$.*

*Proof.*

Suppose $\operatorname{Gal}(f) = C_4$. Since the splitting field of $f(x)$ over $\mathbb{Q}$ has degree 4, any root of $f(x)$ generates an extension of $\mathbb{Q}$ with degree 4. Thus, the field generated by one root of $f$ contains all other roots as well. If $f(x)$ has 1 real root, then it has 4 real roots. Hence, the number of real roots of $f(x)$ is either 0 or 4.

If $f(x)$ has 4 real roots, then $\operatorname{disc} f$ is the product of differences of nonzero real numbers, hence $\operatorname{disc} f > 0$.

On the other hand, if $f(x)$ has 0 real roots, then it has 4 complex roots that are two pairs of complex conjugates. Let $z, \bar{z}, w, \bar{w} \in \mathbb{C} \setminus \mathbb{R}$ be the roots. By definition, then $\sqrt{\operatorname{disc} f}$ is given by

$$\begin{aligned} \sqrt{\operatorname{disc} f} &= (z-\bar{z})(z-w)(z-\bar{w})(\bar{z}-w)(\bar{z}-\bar{w})(w-\bar{w}) \\ \Rightarrow \quad \sqrt{\operatorname{disc} f} &= |z-w|^2|z-\bar{w}|^2(z-\bar{z})(w-\bar{w}) \end{aligned}$$

Since $z \in \mathbb{C} \setminus \mathbb{R}$, then $z - \bar{z} = qi \in \mathbb{C}$ is imaginary and nonzero. In the same way, $w - \bar{w} = ri$ is imaginary and nonzero. Thus,

$$\operatorname{disc} f = |z-w|^4|z-\bar{w}|^4(qi)^2(ri)^2 = |z-w|^4|z-\bar{w}|^4q^2r^2 > 0$$

Thus, $\operatorname{disc} f > 0$ in both cases. □

– To fully distinguish between $C_4$ and $D_8$, the following lemma will be used to show that in this case, the resolvent $R_3(x)$ has a unique root.

**Lemma 4.2.** *If $f \in K[x]$ is a cubic polynomial with discriminant $\delta$, and $r$ is a root of $f$, then a splitting field of $f$ over $K$ is $K(Z_f) = K(r, \sqrt{\delta})$.*

*Proof.* WLOG, suppose $f$ is monic. Let $r, r_2, r_3$ be the roots of $f$. Write

$$f(x) = (x-r)g(x)$$

so $r_2, r_3$ are the roots of $g(x)$. Hence, $g(r) \neq 0$. Using the quadratic formula for $g(x)$ over $K(r)$, then

$$K(r, r_2, r_3) = K(r)(r_2, r_3) = K(r)(\sqrt{\operatorname{disc} g})$$

Since $f$ is monic, then so is $g$ and hence

$$\operatorname{disc} f = g(r)^2 \operatorname{disc} g$$

$$\Rightarrow K(r, \sqrt{\operatorname{disc} g}) = K(r, \sqrt{\operatorname{disc} f})$$

That is, $K(Z_f) = K(r, \sqrt{\delta})$ for a cubic polynomial $f$ with discriminant $\delta$ and root $r \in K$. $\square$

– Lemma 4.2 tells us that if $\delta = \operatorname{disc} f \neq \square$ in $K$ and $R_3(x)$ is reducible over $K$, then $R_3(x)$ has a root in $K$ but does not split completely over $K$ (since $\operatorname{disc} f \neq \square$). Hence, $R_3(x)$ has a unique root $r$ in $K$.

**Theorem 6.** *(Kappe-Warren)*

*Let $f \in K[x]$ be an irreducible quartic where $\delta \neq \square$ in $K$ and $R_3(x) \in K[x]$ is reducible with a unique root $r \in K$. Then, if both polynomials $x^2 + ax + (b - r)$ and $x^2 - rx + d$ split over $K(\sqrt{\delta})$, then $\mathrm{Gal}(f) = C_4$. Otherwise, $\mathrm{Gal}(f) = D_8$.*

– Kappe-Warren is a powerful tool in distinguishing between Galois groups $C_4$ and $D_8$. Using this theorem, Table 1 can be completed into a full characterization as follows.

**Corollary 4.3.** *If $f(x) = x^4 + ax^3 + bx^2 + cx + d \in K[x]$ is an irreducible quartic polynomial with $\operatorname{disc} f = \delta$ and $R_3(x)$ its resolvent cubic, then the following characterization holds.*

| $\delta \in K$ | $R_3(x) \in K[x]$ | $(a^2 - 4(b - r))\delta$ *and* $(r^2 - 4d)\delta$ | $\mathrm{Gal}(f)$ |
|---|---|---|---|
| *not* $\square$ *in* $K$ | *irreducible in* $K[x]$ | | $S_4$ |
| $\square$ *in* $K$ | *irreducible in* $K[x]$ | | $A_4$ |
| *not* $\square$ *in* $K$ | *root* $r \in K$ | *at least one is not* $\square$ *in* $K$ | $D_8$ |
| *not* $\square$ *in* $K$ | *root* $r \in K$ | *both are* $\square$ *in* $K$ | $C_4$ |
| $\square$ *in* $K$ | *reducible in* $K[x]$ | | $V$ |

TABLE 2.

*Proof.*

Referring to Kappe-Warren (6), the polynomials $g = x^2 + ax + (b - r)$ and $h = x^2 - rx + d$ split completely over $K(\sqrt{\delta})$ if and only if their discriminants $\operatorname{disc} g = a^2 - 4(b - r)$ and $\operatorname{disc} h = r^2 - 4d$ are squares in $K(\sqrt{\delta})$.

**Claim 4.4.** *The discriminants $\operatorname{disc} g = a^2 - 4(b - r)$ and $\operatorname{disc} h = r^2 - 4d$ are either 0 or nonsquares in $K$.*

Now, a nonsquare in $K$ is a square in $K(\sqrt{\delta})$ if and only if its product with $\delta$ is a square. Hence, the desired polynomials $g$ and $h$ both split completely over $K(\sqrt{\delta})$ if and only if $\delta \cdot \operatorname{disc} g$ and $\delta \cdot \operatorname{disc} h$ are both square in $K$. That is, if both $\delta \cdot \operatorname{disc} g$ and $\delta \cdot \operatorname{disc} h$ are squares in $K$, then $\operatorname{Gal}(f) = C_4$, and otherwise the Galois group is $D_8$. $\square$

☡ Warning : The above characterizations of Galois groups of quartic polynomials rely on the fact that $f$ must be irreducible over $K$. These results do not hold for reducible quartic polynomials.

## 5. Some example computations

This final section determines the Galois groups of irreducible quartic polynomials using the aforementioned results.

(1) The Galois groups of $f(x) = x^4 + px + p \in \mathbb{Q}[x]$ for all primes $p > 2$.

First, by Eisenstein's criterion, for any prime $p$, $f(x) = x^4 + px + p$ is irreducible over $\mathbb{Q}$.

For arbitrary $p$, the discriminant and cubic resolvent of $f$ is as follows.

$$\delta = 256p^3 - 27p^4 = p^3(256 - 27p) \neq \square$$
$$R_3(x) = x^3 - 4px - p^2$$

Since $\delta \neq \square$ for arbitrary $p$, it remains to analyze the resolvent for varying primes $p$.

Suppose $p > 5$. If $R_3(x)$ were reducible, then it would have a root dividing $p^2$, i.e., $\pm 1,$, $\pm p$ or $\pm p^2$.

$$R_3(1) = 1 - 4p - p^2 < 0 \neq 0$$
$$R_3(-1) = -1 + 4p - p^2 = -1 + p(4 - p) < 0 \text{ since } (4 - p) < 0$$
$$R_3(p) = p^3 - 4p^2 - p^2 = p^3 - 5p^2 = p^2(p - 5) > 0 \text{ since } p > 5$$
$$R_3(-p) = -p^3 + 4p^2 - p^2 = -p^3 + 5p^2 = p^2(5 - p) < 0 \text{ since } p > 5$$
$$R_3(p^2) = p^6 - 4p^3 - p^2 = p^2(p^4 - 4p - 1) > 0$$
$$R_3(-p^2) = -p^6 + 4p^3 - p^2 = p^2(-p^4 + 4p - 1) < 0$$

Hence, $R_3(x)$ is irreducible when $p > 5$. By Theorem 4, then $\text{Gal}(x^4 + px + p) = S_4$ for all primes $p > 5$.

Now, suppose $p = 3$. Then, $f(x) = x^4 + 3x + 3$ and $\delta = 4725$. The cubic resolvent is as follows.

$$R_3(x) = x^3 - 12x - 9$$

Then, $R_3(x)$ is reducible since $R_3(-3) = 0$, and thus $R_3(x)$ has a root, $r = -3$. Then, $\text{Gal}(x^4 + 3x + 3) = D_8$ or $C_4$ by Theorem 4.

To distinguish between $D_8$ and $C_4$, by Corollary 4.3, it remains to compute $(a^2 - 4(b - r))\delta$ and $(r^2 - 4d)\delta$.

$$(a^2 - 4(b - r))\delta = -4(3)(4725) = -56700 \neq \square$$

Since this is non-square in $K$, then $\text{Gal}(x^4 + 3x + 3) = D_8$ by Corollary 4.3.

Lastly, suppose $p = 5$. Then, $f(x) = x^4 + 5x + 5$ and $\delta = 15125$. Its cubic resolvent is

$$R_3(x) = x^3 - 20x - 25$$

Since $R_3(5) = 0$, then $R_3(x)$ is reducible with root $r = 5$. By Theorem 4, then $\text{Gal}(x^4 + 5x + 5) = D_8$ or $C_4$. By Corollary 4.3, it remains to determine whether the following values are squares in $K$.

$$(a^2 - 4(b-r))\delta = -4(-5)(15125) = 302500 = (550)^2 = \square$$
$$(r^2 - 4d)\delta = (25 - 4(5))(15125) = 75625 = (275)^2 = \square$$

As both above values are squares in $\mathbb{Q}$, then by Corollary 4.3, $\text{Gal}(x^4+5x+5) = C_4$.

(2) $f(x) = x^4 - 7$

First, to use any of the results in the previous sections, it must be verified that $f(x) \in \mathbb{Q}[x]$ is indeed irreducible. By applying Eisenstein's criterion with $p = 7$, then $f$ is irreducible over $\mathbb{Z}$, which implies that $f$ is irreducible over $\mathbb{Q}$ (since $f$ is monic).

It remains to compute the discriminant and cubic resolvent of $f$.

$$\delta = 256d^3 = 256(-7)^3 = -87808 \neq \square$$
$$R_3(x) = x^3 + 28x = x(x^2 + 28) = \text{ reducible over } \mathbb{Q}$$

Hence, by Theorem 4, $\text{Gal}(f) = D_8$ or $C_4$. By Theorem 5, since $\delta < 0$, then $\text{Gal}(f) = D_8$.

(3) $f(x) = x^4 + x + 1$

In $\mathbb{F}_2[x]$,

$$f(x) - (x^4 - x) \equiv 1 \mod 2$$

Then, $f(x)$ is relatively prime to every irreducible polynomial over $\mathbb{F}_2$ that has degree dividing 2. Hence, $f(x)$ cannot be factored over $\mathbb{F}_2$. Thus, $f$ is irreducible over $\mathbb{Q}$ (by Proposition 9.12 in Dummit and Foote).

The discriminant and resovlent of $f$ are as follows.

$$\delta = 256d^3 - 27c^4 = 256 - 27 = 229 \neq \square$$
$$R_3(x) = x^3 - 4dx - c^2 = x^3 - 4x - 1 = \text{ irreducible over } \mathbb{Q}$$

Note that $R_3(x)$ is irreducible since if it were reducible, it would have to have a root dividing 1 (i.e., $\pm 1$), but $R_3(\pm 1) \neq 0$.

By Theorem 4, then $\text{Gal}(f) = S_4$.

## References

[1] Keith Conrad. Galois groups of cubics and quartics (not in characteristic 2). *Expository papers by K. Conrad*, 2011.

[2] Phyllis Lefton. Galois resolvents of permutation groups. *Classroom Notes, Manhattanville College*, pages 642–644, October 1977.