Solvability by Radicals

A Brief History. We’ve known the formula for the roots of an arbitrary quadratic polynomial since ancient times. A cubic formula emerged in the beginning of the modern era, followed by a quartic formula a few hundred years later. In these cases, the roots of an arbitrary polynomial are obtained by a series of square and cube roots (and arithmetic operations). The triumph of Galois Theory is to relate the existence of such a formula to the solvability of the Galois group of the polynomial. Thus, the solvability of the groups of $S_2, S_3$ and $S_4$ “explain” the general formulas, but only the quintic polynomials with solvable Galois groups may be solved in this way, so in particular there is no general formula for the roots of a general quintic (or higher degree) polynomial.

Discriminants. Let $\alpha_1, \ldots, \alpha_d \in \overline{\mathbb{Q}}$ be the roots of

$$f(x) = x^d + c_{d-1}x^{d-1} + \cdots + c_0 \in \mathbb{Q}[x]$$

with splitting field $F = \mathbb{Q}(\alpha_1, \ldots, \alpha_d)/\mathbb{Q}$.

Adapting the example from the previous section, we find that the determinant of the Vandermonde matrix (in the roots $\alpha_i$) is:

$$\prod_{i<j}(\alpha_j - \alpha_i) \in F$$

which is a square root of $\Delta = (-1)^{\binom{d}{2}} \prod_{i=1}^{d} f'(\alpha_i)$

where $\Delta$ is the discriminant of the polynomial $f(x)$.

Examples. (a) For a (monic) quadratic polynomial $f(x) = x^2 + bx + c$, we have:

$$\Delta = -(2\alpha_1 + b)(2\alpha_2 + b) = -4(\alpha_1 \alpha_2) - 2(\alpha_1 + \alpha_2)b - b^2 = b^2 - 4c$$

(b) After a substitution $y = x + b$, a monic cubic polynomial in $x$ becomes:

$$f(x) = y^3 + py + q$$

which has the additional pleasant property that the roots (in the $y$ variable) satisfy:

$$\alpha_1 + \alpha_2 + \alpha_3 = 0 \quad \text{in addition to} \quad \alpha_1 \alpha_2 + \alpha_2 \alpha_3 + \alpha_3 \alpha_1 = p \quad \text{and} \quad -\alpha_1 \alpha_2 \alpha_3 = q$$

From this (and a few suppressed calculations), we get

$$\Delta = -(3\alpha_1^2 + p)(3\alpha_2^2 + p)(3\alpha_3^2 + p) = -27q^2 - 4p^3$$

Note that these are polynomial functions of the coefficients of $f(x)$.

**Proposition 1.** Let $f(x) \in \mathbb{Q}[x]$ be a (monic) polynomial. Then:

(a) The discriminant $\Delta$ of $f(x)$ is a rational number.

(b) Either $\Delta = 0$ and there is a repeated root (and $f(x)$ is reducible), or else:

the sign of $\Delta$ is the number of conjugate pairs of complex roots of $f(x)$

**Proof.** Let $\deg(f(x)) = d$. The discriminant $\Delta = \Delta(\alpha_1, \ldots, \alpha_d)$ is a symmetric function of the roots of $f(x)$. In other words, if $g \in S_d$, then:

$$\Delta(\alpha_1, \ldots, \alpha_d) = \Delta(\alpha_{g(1)}, \ldots, \alpha_{g(d)})$$

(the sign of a square root of $\Delta$ is flipped by transpositions so it is not symmetric)
The coefficients of \( f(x) \) are also symmetric functions of the roots. Since
\[
f(x) = x^d + a_{d-1}x^{d-1} + \cdots + a_0 = \prod_{i=1}^{d} (x - \alpha_i)
\]
we see that \( f(x) \) is symmetric in the \( \alpha_i \) so all its (rational) coefficients are symmetric. Explicitly, these coefficients are:
\[
a_{d-1} = (-1) \sum \alpha_i, \quad a_{d-2} = \sum_{i < j} \alpha_i \alpha_j, \ldots, \quad a_0 = (-1)^d \alpha_1 \alpha_2 \cdots \alpha_d
\]
and then (a) follows from the:

**First Theorem of Invariant Theory.** Any symmetric polynomial in \( x_1, \ldots, x_n \) (with integer coefficients) is a polynomial function (also with integer coefficients) of the “elementary symmetric polynomials”
\[
\sigma_1 = \sum x_i, \quad \sigma_2 = \sum x_i x_j, \ldots, \quad \sigma_d = x_1 \cdots x_d
\]
(we’ll investigate this further later). Thus in particular the discriminant of \( f(x) \) is a polynomial in the coefficients of \( f(x) \), with integer coefficients (as a bonus).

Next, the first part of (b) is obvious from:
\[
\Delta = \prod_{i < j} (\alpha_i - \alpha_j)^2
\]
If there are \( p \) pairs of conjugate complex roots \( \alpha_i, \overline{\alpha}_i \) and no repeated roots, then:
\[
\Delta = \left( \prod_{i=1}^{p} (\alpha_i - \overline{\alpha}_i)^2 \right) \cdot \delta^2
\]
where \( \delta \in \mathbb{R}^* \) (so its square is positive) since it is invariant under conjugation and each \( \alpha_i - \overline{\alpha}_i \) is purely imaginary (so its square is negative).

Thus, in particular, the roots of an irreducible \( f(x) = x^2 + bx + c \) are:

- real if \( \Delta = b^2 - 4c \geq 0 \) and both complex if \( \Delta < 0 \)

and similarly, the roots of an irreducible \( f(x) = y^3 + py + q \) are:

- all real if \( \Delta \geq 0 \) and one real and a conjugate pair if \( \Delta < 0 \)

In other words, the roots of \( y^3 + py + q \) are real (and there are three of them) when:
\[
-\Delta = 27q^2 + 4p^3 < 0
\]

**The Quadratic Formula.** From \( \Delta = (\alpha_2 - \alpha_1)^2 \), we get:
\[
\alpha_i = \frac{(\alpha_1 + \alpha_2) \pm (\alpha_1 - \alpha_2)}{2} = \frac{-b \pm \sqrt{\Delta}}{2} \text{ and } \mathbb{Q}(\sqrt{\Delta}) = F
\]

**The Cubic Formula.** From \( f(x) = y^3 + py + q \), we make another substitution:
\[
y = z - \frac{p}{3z} \text{ to obtain } z^3 f(x) = z^6 + qz^3 - \left( \frac{p}{3} \right)^3
\]
from which we conclude (from the quadratic formula) that:
\[
z^3 = -\frac{-q \pm \sqrt{q^2 + 4\left( \frac{p}{3} \right)^3}}{2} = -\left( \frac{q}{2} \pm \sqrt{\left( \frac{q}{2} \right)^2 + \left( \frac{p}{3} \right)^3} \right)
\]
Interestingly, the intermediate solution for \( z^3 \) requires taking the square root:

\[
\sqrt{\left( \frac{q}{2} \right)^2 + \left( \frac{p}{3} \right)^3} = \frac{\sqrt{-3\Delta}}{18}
\]

Thus, in order to find three real roots (positive \( \Delta \)), one needs to pass through the complex numbers (square root of \( -3\Delta \)). This is an essential use of the complex numbers that is often credited as their “discovery” inherent in this cubic formula. Notice also that if we replace \( Q \) with \( Q(\omega_3) \), then a subsequent extension by the square root of \( \Delta \) or of \( -3\Delta \) is the same, since \( \sqrt{-3} \in Q(\omega_3) \).

Inspired by this formula, we make the following:

**Definition.** A separable polynomial \( f(x) \in K[x] \) is **solvable by radicals** if all of its roots are contained in a field \( E \) obtained as a series of “radical” extensions:

\[
K = E_0 \subset E_1 \subset \cdots \subset E_r = E
\]

where \( E_{i+1} = E_i(\beta_i) \) and \( \beta_i^{p_i} = b_i \in E_i \) for some primes \( p_i \).

Examples. Each polynomial \( f(x) = x^2 + bx + c \in Q[x] \) is solvable by radicals, with:

\[
Q \subset Q(\sqrt{-3}) \subset E_1(z)
\]

where \( z^3 = -\frac{q}{2} + \frac{\sqrt{-3\Delta}}{18} \). But if we pre-load the cube roots of 1, then:

\[
Q \subset F_0 = Q(\omega_3) = Q(\sqrt{-3}) \subset F_1 = F_0(\sqrt{\Delta}) \subset F_1(z)
\]

contains all of the roots (and so it contains a splitting field for \( f(x) \)). Hence every polynomial of degree 3 is solvable by radicals.

**The Big Theorem of Galois.** Let \( K \) be a field of characteristic zero.

(a) If \( f(x) \in K[x] \) is solvable by radicals, its Galois group \( G \) is solvable.

(b) Conversely, if \( G \) is a solvable group, then \( f(x) \) is solvable by radicals.

The idea is to relate splitting fields with cyclic Galois groups \( C_p \) of prime order to radical extensions. For this, we’ll use the uniquely named Hilbert Theorem 90.

**Definition.** Let \( F/K \) be a separable splitting field with Galois group \( G \). Then:

\[
\text{Nm}(\alpha) := \prod_{g \in G} ga \in K \quad \text{(since it is invariant under } G)\]

and it satisfies \( \text{Nm}(\alpha_1\alpha_2) = \text{Nm}(\alpha_1)\text{Nm}(\alpha_2) \), so \( \text{Nm} : F^* \to K^* \) is a character.

Notice that for each \( \beta \in F \) and \( g \in G \), we have: \( \text{Nm}(\beta) = \text{Nm}(g\beta) \) so that:

\[
\text{Nm}(\beta \cdot (g\beta)^{-1}) = 1
\]

Theorem 90 is the converse to this in the case when \( G \) is cyclic.

**Hilbert’s Theorem 90.** If \( G = C_n \) in the setting of the definition, generated by \( g \in G \), then each element \( \alpha \in F \) of norm 1 may be written as:

\[
\alpha = \beta \cdot (g\beta)^{-1} \quad \text{for some } \beta \in F
\]

Proof. For \( \alpha \in F \) of norm 1, define a sequence of partial norms:

\[
\alpha_1 = \alpha, \quad \alpha_2 = \alpha \cdot ga, \quad \alpha_3 = \alpha \cdot ga \cdot g^2a, \ldots, \quad \alpha_n = \text{Nm}(\alpha) = 1
\]
These obey the recursion:
\[ \alpha_{i+1} = \alpha \cdot g\alpha_i \]
and by the independence of the characters \( \{1, g, \ldots, g^{n-1}\} : F^* \to F^* \), we have:
\[ \alpha_1 \cdot 1 + \alpha_2 \cdot g + \cdots + \alpha_n \cdot g^{n-1} \neq 0 \]
as a function from \( F \) to \( F \)
so that there is a \( \gamma \in F \) for which:
\[ \beta := \sum_{i=1}^{n} \alpha_i \cdot g^{i-1}(\gamma) \neq 0. \]
Then:
\[ \alpha \cdot g\beta = \alpha \cdot \sum_{i=1}^{n} g\alpha_i \cdot g^i(\gamma) = \sum_{i=1}^{n-1} \alpha_{i+1} \cdot g^i(\gamma) + \alpha \cdot \gamma = \alpha \cdot \gamma + \sum_{i=2}^{n} \alpha_i \cdot g^{i-1}(\gamma) = \beta \]
and \( \alpha = \beta \cdot (g\beta)^{-1} \), as desired. \( \square \)

Example. Complex conjugation generates \( \text{Gal}(\mathbb{Q}(i)/\mathbb{Q}) \) and:
\[ \text{Nm}(x + iy) = (x + iy)(x - iy) = x^2 + y^2 \]
so by the Theorem, \( a^2 + b^2 = 1 \) for \( a + bi \in \mathbb{Q}(i) \) if and only if:
\[ a + ib = \frac{c + id}{c - id} = \frac{c^2 - d^2}{c^2 + d^2} + i \frac{2cd}{c^2 + d^2} \]
for some \( c + di \in \mathbb{Q}(i) \). This is a generation formula for Pythagorean triples!

Let \( K \) be a field of characteristic zero containing a primitive \( p \)th root \( \omega_p \) of \( 1 \).

**Corollary.** Each splitting field \( F/K \) with \( [F : K] = p \) is the splitting field of:
\[ x^p - b \in K[x] \text{ for some } b \in K \]

**Proof.** The Galois group of \( F/K \) has prime order \( p \), so it is cyclic.

Let \( \alpha = \omega_p \in K \) and let \( g \in C_p \) generate the Galois group. Then
\[ \text{Nm}(\alpha) = \omega_p \cdot (g\omega_p) \cdots (g^{p-1}\omega_p) = \omega_p^p = 1 \text{ since } \omega_p \in K \text{ is fixed by } g \]

By the Theorem, we may choose \( \beta \in F \) so that \( \alpha = \beta \cdot (g\beta)^{-1} \). Then in particular \( \beta \notin K \) (since \( \beta \) is not fixed by \( g \)), and:
\[ 1 = \alpha^p = (\beta \cdot (g\beta)^{-1})^p = (\beta^p) \cdot (g\beta)^{-p} = (\beta^p) \cdot (g\beta^p)^{-1} \]
so \( \beta^p = g\beta^p \) is invariant under the Galois group, and \( \beta^p = b \in K \). Thus \( F = K(\beta) \)
is a splitting field of \( x^p - b \) with roots \( \beta, \omega_p \).

We may now prove Galois' Theorem (Part (b)).

Suppose \( K \) has characteristic zero and \( F \) is a splitting field of \( f(x) \in K[x] \) with solvable Galois group \( G = \text{Gal}(F/K) \). Then there is a chain:
\[ 1 \subset G_1 \subset G_2 \subset \cdots \subset G_r = G \]
of normal subgroups \( (G_i \text{ in } G_{i+1}) \) with prime cyclic quotient groups \( G_{i+1}/G_i = C_p \),
and there is a corresponding chain of fixed fields:
\[ K = F^G \subset F^{G_{r-1}} \subset \cdots \subset F^{G_1} \subset F^1 = F \]
For each \( i \), consider the inclusions:
\[ F^{G_{i+1}} \subset F^{G_i} \subset F \text{ with } \text{Gal}(F/F^{G_i}) = G_i \]
Then:

\[ 1 \to G_i \to G_{i+1} \to \text{Gal}(F^{G_i}/F^{G_{i+1}}) \to 1 \]

so \( F^{G_i}/F^{G_{i+1}} \) is a splitting field and an extension of degree \( p_i \). If \( K \) contains \( \omega_{p_i} \), then by the Corollary above, \( F^{G_i} \) is obtained from \( F^{G_{i+1}} \) by adjoining a root \( \beta_i \). Otherwise, we replace \( K \) with:

\[
K(\omega_n) \text{ where } n \text{ is the product of (one of each) prime } p_i
\]

and we replace the fields \( F^{G_i} \) above with \( E_i = F^{G_i}(\omega_n) \).

Then the extensions \( E_i/E_{i+1} \) are still splitting fields, of degree \( p_i \) (or 1), and:

\[
K(\omega_n) = E_r \subset E_{r-1} \subset \cdots \subset E_0 = F(\omega_n)
\]

shows that \( f(x) \) is solvable by radicals as a polynomial in \( K(\omega_n)[x] \). To finish the proof, it suffices to show that if \( \omega_n \notin K \), then the splitting field \( K(\omega_n)/K \) can be solved by radicals. But this is a splitting field with abelian Galois group, and solvability by radicals follows by induction on the largest prime factor of \( n \).

To see Part (a) of Galois’ Theorem, suppose \( f(x) \in K[x] \) is solvable by radicals, i.e. the splitting field \( F/K \) is contained in a field \( E \) obtained by extensions:

\[
K = E_0 \subset E_1 = E_0(\beta_1) \subset \cdots \subset E = E_r = E_{r-1}(\beta_{r-1}) \subset E_r(\beta_r) = E
\]

as in the definition. If \( \omega_n \in K \) and \( E/K \) is a splitting field then each:

\[
E_i \subset E_{i+1} \subset E
\]

is an intermediate splitting field, so \( G_{i+1} = \text{Gal}(E/E_{i+1}) \subset G_i = \text{Gal}(E/E_i) \) is a normal subgroup with quotient \( C_{p_i} \), and the Galois group of \( E/K \) is solvable. Then from the intermediate splitting field \( K \subset F \subset E \) we obtain a surjective map \( \text{Gal}(E/K) \to \text{Gal}(F/K) \) and it follows that \( \text{Gal}(F/K) \) is also solvable.

If \( \omega_n \notin K \), then we may pre-load it via:

\[
K \subset K(\omega_n) \subset E_1(\omega_n) \subset \cdots \subset E_r(\omega_n)
\]

We’ve seen above that \( \omega_n \) is solvable by radicals, and the result follows, assuming that \( E_r(\omega_n)/K \) is a splitting field. Thus to finish, we need to deal with the fact that \( E/K \) may not be a splitting field. To see the problem, consider the following:

**Example.** Let \( \mathbb{Q} \subset \mathbb{Q}(i) \subset \mathbb{Q}(i)(\sqrt{1+i}) = E \). Then \( E/\mathbb{Q} \) is not a splitting field. Complex conjugation, which is an isomorphism \( \sigma : \mathbb{Q}(i) \to \mathbb{Q}(i) \), does not lift to an isomorphism \( \tau : \mathbb{Q}(i)(\sqrt{1+i}) \to \mathbb{Q}(i)(\sqrt{1+i}) \). Instead,

\[
\mathbb{Q} \subset \mathbb{Q}(i) \subset \mathbb{Q}(i)(\sqrt{1+i}) \subset \mathbb{Q}(i)(\sqrt{1+i}, \sqrt{1-i})
\]

is a splitting field for the polynomial:

\[
(x^2 + 1)(x^2 - (1+i))(x^2 - (1-i)) = (x^2 + 1)(x^4 - 2x^2 + 2)
\]

Inspired by this Example, given radical extensions:

\[
K \subset E_1 \subset \cdots \subset E_r = E \subset E(\beta) \text{ with } \beta^{p} = b \in E
\]

and the property that \( E/K \) is a splitting field with Galois group \( H \) and polynomial \( e(x) \in K[x] \), then \( f(x) = \prod_{h \in H} (x^p - hb) \in K[x] \) since \( f(x) \) is invariant under \( H \) and \( E_r \subset E(\beta) \subset E_{r+|H|} = E(..., \sqrt{hb}, ...) \) is a splitting field over \( K \) for \( e(x)f(x) \). □
Example. In the cubic formula for \( f(x) = y^3 + py + q \) (and \( \omega_3 \in K \)), we determined that we could find a splitting field for \( f(x) \) inside a splitting field \( E/K \), where:

\[
K \subset K(\sqrt[3]{\Delta}) \subset K(\sqrt{\Delta}(z_1, z_2)) = E
\]

and

\[
z_1^3 = -\frac{q}{2} + \frac{\sqrt{-3\Delta}}{18} \quad \text{and} \quad z_2^3 = -\frac{q}{2} - \frac{\sqrt{-3\Delta}}{18}
\]

The Galois group of \( K(\sqrt{\Delta})/K \) (assuming it has degree 2) is generated by:

\[
g(\sqrt{\Delta}) = -\sqrt{\Delta}
\]

and so \( E \) is a splitting field for \( (x^2 - \Delta)(x^6 - qx^3 - \frac{q^3}{27}) \) (or, if \( K \) has no primitive cube root of 1, for the polynomial \( (x^2 + x + 1)(x^2 - \Delta)(x^6 - qx^3 - \frac{q^3}{27}) \)).

**Postponed Issues.** First, some invariant theory:

Let \( f(x_1, \ldots, x_n) \in \mathbb{Z}[x_1, \ldots, x_n]_d \) be a homogeneous symmetric polynomial of degree \( d \), i.e. \( f \) is a sum of monomials \( a_1 x_1 = a_1 x_1^1 \cdots x_n^1 \) of degree \( d \) and:

\[
f(x_1, \ldots, x_n) = gf := f(x_{g(1)}, \ldots, x_{g(n)}) \text{ for all } g \in S_n
\]

Then we may impose the “lexicographic” order on these monomials, with:

\[
x_1 \prec x_2 \prec \cdots \prec x_n
\]

and \( a_1 x_I \prec a_J x_J \) if \( i_1 = j_1, \ldots, i_k = j_k \) and \( i_{k+1} < j_{k+1} \) for some \( 0 \leq k < n \), so that \( I \) would come before \( J \) if they were words in a dictionary. Then \( f \) is determined by the coefficients \( a_I \) of the “initial, non-increasing” monomials \( x_I \) with \( n \geq i_1 \geq i_2 \geq \cdots \geq i_n \geq 0 \) that appear first in their \( S_n \) orbit, and the elementary polynomials are those with the single initial monomial \( x_I = x_1 \cdots x_k \), so that:

\[
\sigma_0 = 1, \quad \sigma_1 = \sum_i x_i, \quad \sigma_2 = \sum_{i \neq j} x_i x_j = \sum_{i < j} x_i x_j
\]

Now suppose that \( x_I = x_1^{i_1} \cdots x_n^{i_n} \) is a non-increasing monomial. Then:

\[
x_I = \sigma_n^{i_n} \sigma_{n-1}^{i_{n-1} - i_n} \cdots \sigma_1^{i_1 - i_2} + \sum_J a_J x_J
\]

and each monomial in the error \( a_J \neq 0 \) satisfies \( x_I \prec x_J \). It follows that:

\[
f(x_1, \ldots, x_n) \in \mathbb{Z}[\sigma_1, \ldots, \sigma_n] \text{ is a polynomial of (weighted) degree } d \text{ in } \sigma_1, \ldots, \sigma_n
\]

**Examples.**

\[
\sum_{i=1}^n x_i^2 = \sigma_1^2 - 2 \sum_{i < j} x_i x_j = \sigma_1^2 - 2\sigma_2
\]

\[
\sum_{i < j} x_i^2 x_j = \sigma_1 \sigma_2 - 3\sigma_3
\]

\[
\sum_{i=1}^n x_i^3 = \sigma_1^3 - 3 \sum_{i < j} x_i^2 x_j - 6 \sum_{i < j < k} x_i x_j x_k = \sigma_1^3 - 3(\sigma_1\sigma_2 - 3\sigma_3) - 6\sigma_3 = \sigma_1^3 - 3\sigma_1\sigma_2 + 3\sigma_3
\]

These generalize to the “Newton” expansion of the power sum.

We will use this technology in our analysis of the:
Quartic Formula. Since the Galois group of a quartic polynomial

\[ f(x) = y^4 + p y^2 + q y + r = \prod_{i=1}^{4} (x - \alpha_i) \]

is a subgroup of \( S_4 \) which is solvable, Galois’ Theorem explains the existence of a quartic formula solving \( f(x) \) with radicals (and leaving \( p, q, r \) as indeterminants). But more is true. The Theorem tells us how to find the formula. Note that for:

\[ \omega_3 \]

solving \( S_4 \), the only prime cyclic quotient groups \( C_p = G_{i+1}/G_i \) have \( p = 2, 3 \), so our first step is to preload \( \omega_3 \) to replace \( \mathbb{Q} \) with \( K = \mathbb{Q}(\omega_3) \). Also note that there are three choices for the normal subgroup \( C_2 \subset K_4 \), unlike the other normal subgroups, which are uniquely determined and normal subgroups of \( S_4 \).

The subfields may be associated to the homogeneous polynomials:

\[ D = \prod_{i<j} (\alpha_i - \alpha_j), \]

\[ a = (\alpha_1 - \alpha_2)(\alpha_3 - \alpha_4), \quad b = (\alpha_1 - \alpha_3)(\alpha_2 - \alpha_4), \quad c = (\alpha_1 - \alpha_4)(\alpha_2 - \alpha_3) \]

and

\[ u = \alpha_1 + \alpha_2 - \alpha_3 - \alpha_4, \quad v = \alpha_1 - \alpha_2 + \alpha_3 - \alpha_4, \quad w = \alpha_1 - \alpha_2 - \alpha_3 + \alpha_4 \]

of degrees 6, 4 and 1 in the roots of \( f(x) \), respectively.

Our first subfield is familiar. Since \( D \) is invariant for the action of \( A_4 \), and

\[ \Delta = \left( \prod_{i<j} (\alpha_i - \alpha_j) \right)^2 \]

is invariant for the action of \( S_4 \), we have the intermediate field:

\[ K \subset K(D) = F^{A_4} \subset F \]

where \( F/K \) is the splitting field for \( f(x) \) and \( K(D) \) is the splitting field for \( x^2 - \Delta = x^2 - D^2 \).

Next up, notice that \( K_4 \) fixes each of \( a, b \) and \( c \), but that

\[ \gamma(a) = c, \quad \gamma(b) = -a, \quad \gamma(c) = -b \quad \text{for} \quad \gamma = (1 \ 2 \ 3), \]

and \( \tau(a) = -a, \quad \tau(b) = c, \quad \tau(c) = b \quad \text{for} \quad \tau = (1 \ 2) \)

and we conclude that the set \( \{ \pm a, \pm b, \pm c \} \) is fixed by the action of \( S_4 \), and so:

\[ h(x) = (x^2 - a^2)(x^2 - b^2)(x^2 - c^2) \in K[x] \]

This gives us the expected intermediate field:

\[ K \subset K(a, b, c) = F^{K_4} \subset F \]

whose degree \( F^{K_4}/K \) indeed matches \( |S_4/K_4| \), so this has Galois group \( S_3 \).

Moreover, note that \( abc = D \), so we can squeeze in the field:

\[ K \subset K(D) \subset K(a, b, c) \subset F \]

though \( D \) is not the discriminant of \( h(x) \). In fact, \( D(h) = D(a^2 - b^2)(a^2 - c^2)(b^2 - c^2) \) is fixed by the full symmetric group, so it belongs to \( K \).

On the other hand, \( K(D) \subset K(a, b, c) \) is a splitting field, generated by some \( \beta \in K(a, b, c) \) with \( \beta^3 \in K(D) \) by the Corollary to Hilbert Theorem 90.
But we can do better. In $K(D)[x]$, $h(x)$ factors as a product:

$$h_1(x)h_2(x) = ((x - a)(x + b)(x - c))((x + a)(x - b)(x + c))$$

since $\{a, -b, c\}$ is permuted by the alternating group! Thus, the coefficients of:

$$h_1(x) = (x - a)(x + b)(x - c) = x^3 + (b - a - c)x^2 + (ac - ab - bc)x + abc$$

are invariant. But $abc = D$ and $b - a - c = 0$. This leaves an $S_4$-invariant term

$$ac - ab - bc = -\alpha_1^2\alpha_2^2 + \alpha_1^2\alpha_2\alpha_3 - 6\alpha_1\alpha_2\alpha_3\alpha_4 + \text{non-initial terms}$$

$$= -\sigma_2^2 + 3\sigma_1\sigma_3 - 12\sigma_4$$

Keeping in mind that $\sigma_1(\alpha) = 0, \sigma_2(\alpha) = p, \sigma_3(\alpha) = -q, \sigma_4(\alpha) = r$, we get:

$$h_1(x) = (x^3 - (p^2 + 12r)x + D) \text{ and } h_2(x) = (x^3 - (p^2 + 12r)x - D)$$