I am following Curtis Bright's 2013 notes *Computing the Galois groups of a polynomial*. I will start in Chapter 2.

We will assume f is an irreducible polynomial over $\mathbb{Q}$. Then f is separable and $\mathrm{Gal}(f)$ (which is the Galois group of the splitting field of f) acts transitively on the roots of f.

Proof. We know f is separable because f' has smaller degree than f, and since f has no nontrivial divisors, $\gcd(f, f') = 1$. But if α were a root of multiplicity > 1, then α would be a root of f', therefore the minimal polynomial of α would divide $\gcd(f, f') = 1$, a contradiction.

That is because if f is irreducible, then f is prime. In fact, every irreducible element of a GCD domain is prime. That is, if $f|gh$, then $f|g$ or $f|h$. Irreducibility of f means that $f = ab$ only if a or b is a unit. Let $f|gh$ and let $z = \gcd(fh, gh)$. If $gh = 0$, then $z = fh$ and so $fh|gh$ and by cancellation (if $h \neq 0$), $f|g$. If $h = 0$ then $f|h$.

Now let $gh \neq 0$. Since f and h both divide fh and gh, there are some elements u, v such that $fu = z = hv$. So then $hv = z$ divides fh, so $hv|fh$ and by cancellation (since $h \neq 0$), $v|f$. Then by irreducibility, either v is a unit or $f \sim v$ (that is, f and v are unit multiplies of each other). If v is a unit, then since $fu = hv$, we have $f(uv^{-1}) = h$ and so $f|h$. If $f \sim v$, then there is a unit w such that $f = vw$ and so $z \sim fh$ and also $u \sim h$. Then $fh = \gcd(fh, gh)$ and so $fh|gh$ and by cancellation $f|g$. □

Also, if $g \not\sim h$ are both irreducible, then g and h have no roots in common. This is because if $g(\alpha) = h(\alpha) = 0$, then $m_\alpha | \gcd(g, h)$. But this contradicts g and h both being irreducible and not similar, implying $\gcd(g, h) = 1$.

In general, $\mathrm{Gal}(gh) \subseteq \mathrm{Gal}(g) \times \mathrm{Gal}(h)$. This is a result of the **translation theorem**.

Theorem Translation. Let L/F and M/F be field extensions, with L/F Galois. Then LM/M is a Galois extension with

$$\mathrm{Gal}(LM/M) \cong \mathrm{Gal}(L/L \cap M).$$

Proof. Since L/F is finite Galois, L is the splitting field over F with respect to some polynomial $f(x) \in F[x]$. Then LM is a splitting field of $f(x) \in M[x]$ over M, which is separable over L, so LM/M is Galois. Consider the restriction homomorphism

$$\mathrm{Gal}(LM/M) \to \mathrm{Gal}(L/F),\ \sigma \mapsto \sigma|_L.$$

This has trivial kernel: an automorphism $\sigma \in \mathrm{Gal}(LM/M)$ that is trivial on L must me trivial on all of LM since it is by essence trivial on M ($\sigma \in \mathrm{Gal}(LM/M)$). Thus the function is injective.

Thus $\mathrm{Gal}(LM/M)$ is isomorphic to some subgroup of $\mathrm{Gal}(L/F)$. Thus there is some intermediate field $F \subseteq K \subseteq L$ such that $\mathrm{Gal}(LM/M) \cong \mathrm{Gal}(L/K)$. So

$$K = \{\ell \in L : \sigma(\ell) = \ell, \sigma \in \mathrm{Gal}(LM/M)\}.$$

An element of LM is fixed by $\mathrm{Gal}(LM/M)$ when it belongs to M, so $K = L \cap M$. Therefore the image of $\mathrm{Gal}(LM/M)$ under the restriction map is $\mathrm{Gal}(L/L \cap M)$. □

Now the inclusion $\mathrm{Gal}(gh) \subseteq \mathrm{Gal}(g) \times \mathrm{Gal}(h)$ can be proven. Let $\mathrm{spl}(g) = L$ and $\mathrm{spl}(h) = M$. Then $\mathrm{Gal}(LM/M) \cong \mathrm{Gal}(L/L \cap M)$ and $\mathrm{Gal}(LM/L) \cong \mathrm{Gal}(M/L \cap M)$. Note that

$$\mathrm{Gal}(LM/M), \mathrm{Gal}(LM/L) \trianglelefteq \mathrm{Gal}(LM/L \cap M)$$

and their intersection is trivial. Because they are two normal subgroups with trivial intersection,

$$\mathrm{Gal}(LM/L)\mathrm{Gal}(LM/M) \cong \mathrm{Gal}(LM/L) \times \mathrm{Gal}(LM/M).$$

Thus

$$\begin{aligned}\mathrm{Gal}(L/L \cap M) \times \mathrm{Gal}(M/L \cap M) &\cong \mathrm{Gal}(LM/L) \times \mathrm{Gal}(LM/M) \\ &\cong \mathrm{Gal}(LM/L)\mathrm{Gal}(LM/M) \subseteq \mathrm{Gal}(LM/L \cap M).\end{aligned}$$

The **elementary symmetric polynomials** $s_n \in R[x_1, \ldots, x_n]$ are

$$\begin{aligned}s_1 &:= x_1 + \cdots + x_n \ (n \text{ terms}) \\ s_2 &:= x_1x_2 + \cdots + x_{n-1}x_n \ (\binom{n}{2} \text{ terms}) \\ &\vdots \\ s_n &:= x_1x_2 \cdots x_n \ (1 \text{ term}).\end{aligned}$$

Then in $R[x, x_1, \ldots, x_n]$,

$$\prod_{i=1}^{n}(x - x_i) = x^n - s_1x^{n-1} + \cdots + (-1)^n s_n.$$

For example, for $n = 2$, we have

$$(x - x_1)(x - x_2) = x^2 - xx_1 - xx_2 + x_1x_2 = x^2 - (x_1 + x_2)x + x_1x_2 = x^2 - s_1x + s_2.$$

Now let f be an irreducible polynomial with roots $\alpha_1, \ldots, \alpha_n$. Then

$$f(x) = \prod_{i=1}^{n}(x - \alpha_i) = x^n - s_1(\alpha_1, \ldots, \alpha_n)x^{n-1} + \cdots + (-1)^n s_n(\alpha_1, \ldots, \alpha_n)$$

and so $s_i(\alpha_1, \ldots, \alpha_n) \in \mathbb{Q}$ for all s_i.

Theorem FToSP. Let $s(x_1, \ldots, x_n) \in R[x_1, \ldots, x_n]$ be a symmetric polynomial. Then s can be expressed in $R[s_1, \ldots, s_n]$.

Denote by $\mathrm{orb}(p)$ the **orbit** of a polynomial p under the S_n action. Then $1 \leq \#\mathrm{orb}(p) \leq n!$.

Definition 1. Let $f \in \mathbb{Z}[x]$ be irreducible with roots $\alpha_1, \ldots, \alpha_n$ and $p \in \mathbb{Z}[x_1, \ldots, x_n]$. Then the **resolvent** polynomial $R_{f,p} \in \mathbb{Z}[y]$ is defined as

$$R_{f,p}(y) = \prod_{p_i \in \mathrm{orb}(p)} (y - p_i(\alpha_1, \ldots, \alpha_n)).$$

Example 1. Take $p = x_1 + x_2$ and $f(x) = x^3 - 2$. Then

$$\begin{aligned} R_{f,p}(y) &= (y - \sqrt[3]{2} - \zeta_3\sqrt[3]{2})(y - \zeta_3\sqrt[3]{2} - \zeta_3^2\sqrt[3]{2})(y - \sqrt[3]{2} - \zeta_3^2\sqrt[3]{2}) \\ &= (y + \zeta_3^2\sqrt[3]{2})(y + \sqrt[3]{2})(y + \zeta_3\sqrt[3]{2}) = y^3 + 2. \end{aligned}$$

Example 2. Take $p = x_1 + x_2$ and $f = x^4 + 1$. Then

$$\begin{aligned} &R_{f,p}(y) = (y - \zeta_4 - \zeta_4^3)(y - \zeta_4 - \zeta_4^5)(y - \zeta_4 - \zeta_4^7)(y - \zeta_4^3 - \zeta_4^5)(y - \zeta_4^3 - \zeta_4^7)(y - \zeta_4^5 - \zeta_4^7) \\ &= (y - i\sqrt{2})(y - 0)(y - \sqrt{2})(y + \sqrt{2})(y - 0)(y + i\sqrt{2}) = y^2(y^2 + 2)(y^2 - 2) = y^6 - 4y^2. \end{aligned}$$

Example 3. Take $p = x_1 + x_2$ and $f = x^4 + x^3 + x^2 + 1$. Then

$$\begin{aligned} R_{f,p}(y) &= (y - \zeta_5 - \zeta_5^2)(y - \zeta_5 - \zeta_5^3)(y - \zeta_5 - \zeta_5^4)(y - \zeta_5^2 - \zeta_5^3)(y - \zeta_5^2 - \zeta_5^4)(y - \zeta_5^3 - \zeta_5^4) \\ &= y^6 + 3y^5 + 5y^4 + 5y^3 - 2y - 1 \end{aligned}$$

A useful example is $p = \prod_{i<j}(x_i - x_j)$. Then $\mathrm{orb}(p) = \{p, -p\}$, and

$$R_{f,p} = \left(y - \prod_{i<j}(\alpha_i - \alpha_j)\right)\left(y + \prod_{i<j}(\alpha_i - \alpha_j)\right) = y - \Delta(f).$$

It is worth noting that the coefficients of the resolvent are symmetric polynomials evaluated at $\alpha_1, \ldots, \alpha_n$ (because permuting the roots $\alpha_1, \ldots, \alpha_n$ does not change the resolvent). So as long as $f \in \mathbb{Z}[x]$ and $p \in \mathbb{Z}[x_1, \ldots, x_n]$, then $s_i(\alpha_1, \ldots, \alpha_n) \in \mathbb{Z}$ and so $R_{f,p} \in \mathbb{Z}[y]$.

If $\sigma \in \mathrm{Gal}(f)$ then we can define an action of σ on the roots of $R_{f,p}$ by

$$\sigma(p_i(\alpha_1, \ldots, \alpha_n)) = p_i(\sigma(\alpha_1), \ldots, \sigma(\alpha_n))$$

where $p_i \in \mathrm{orb}(p)$. This is of course well-defined because σ is a permutation of the $\alpha_1, \ldots, \alpha_n$ and so $p_i(\sigma(\alpha_1), \ldots, \sigma(\alpha_n)) = p_j(\alpha_1, \ldots, \alpha_n)$ for some $p_j \in \mathrm{orb}(p)$.

Theorem 2. Let $f \in \mathbb{Z}[x]$ be irreducible with roots $\alpha_1, \ldots, \alpha_n$ and let $p \in \mathbb{Z}[x_1, \ldots, x_n]$. Then there is a group homomorphism

$$\phi : \mathrm{Gal}(f) \to \mathrm{Gal}(R_{f,p})$$

defined by

$$\phi(\sigma)(p_i(\alpha_1, \ldots, \alpha_n)) = p_i(\sigma(\alpha_1), \ldots, \sigma(\alpha_n))$$

for all $p_i \in \mathrm{orb}(p)$. If $R_{f,p}(y) \in \mathbb{Z}[y]$ is separable, then ϕ is surjective.

Note that $\mathrm{Gal}(R_{f,p})$ may still not act transitively on the roots of $R_{f,p}$ if $R_{f,p}$ is not irreducible. For example, with $f = x^4 + x^3 + x^2 + x + 1$ and $p = x_1 + x_2$, we have

$$R_{f,p} = y^6 + 3y^5 + 5y^4 + 5y^3 - 2y - 1 = (y^2 + y - 1)(y^4 + 2y^3 + 4y^2 + 3y + 1),$$

so $\mathrm{Gal}(R_{f,p})$ does not act transitively on the roots of $R_{f,p}$.

Proof. Note that $R_{f,p}$'s roots are built out of f's roots, so

$$\text{spl}(R_{f,p}) \subseteq \text{spl}(f).$$

Therefore every automorphism of $\text{spl}(R_{f,p})$ is the restriction of some automorphism of $\text{spl}(f)$. In other words, $\text{Gal}(R_{f,p}) \subseteq \text{Gal}(f)$. □

Let's consider the polynomial $f = x^4 + 2x^3 + 2x + 1$. The four roots of f are

$$r_n = \frac{1}{2}\left(-1 + i^n \sqrt[4]{3}\sqrt{2} + (-1)^{2n+1}\sqrt{3}\right),\ 0 \le n \le 3,\ i^2 = -1.$$

There are four subgroups of S_4 that act transitively on the roots: S_4, A_4, D_4, V_4, and C_4. Therefore $\text{Gal}(f)$ is isomorphic to one of those five groups.

Let $p = x_0 + x_1 \in \mathbb{Z}[x_0, x_1, x_2, x_3]$. Then

$$\begin{aligned} R_{f,p} &= (y - r_0 - r_1)(y - r_0 - r_2)(y - r_0 - r_3)(y - r_1 - r_2)(y - r_1 - r_3)(y - r_2 - r_3) \\ &= y^6 + 6y^5 + 12y^4 + 8y^3 - 8 = (y^2 + 2y - 2)(y^4 + 4y^3 + 6y^2 + 4y + 4). \end{aligned}$$

And so of the six roots of $R_{f,p}$, there is one orbit of size 2 and one orbit of size 4.

Now let $q = x_0 - x_1 \in \mathbb{Z}[x_0, x_1, x_2, x_3]$. Then $\#\text{orb}(q) = 12$, and

$$R_{f,q} = y^{12} - 12y^{10} + 48y^8 + 144y^6 - 576y^4 - 1728 = (y^4 - 12)(y^8 - 12y^6 + 60y^4 + 144)$$

and so $\text{Gal}(R_{f,q})$ acts on the roots of $R_{f,q}$ with one orbit of size 4 and one orbit of size 8.

Of the five groups listed above, only two have the behavior of $R_{f,p}$ yielding one orbit of size two and one orbit of size four: D_4 and C_4. Observe, if $\text{Gal}(f) \cong D_4$, then the two orbits of $\text{Gal}(R_{f,p})$ are

$$\{r_0 + r_1, r_1 + r_2, r_2 + r_3, r_3 + r_0\}, \{r_0 + r_2, r_1 + r_3\},$$

and if $\text{Gal}(f) \cong C_4$, then the two orbits of $\text{Gal}(R_{f,p})$ are $\{r_0 + r_1, r_1 + r_2, r_2 + r_3, r_3 + r_0\}, \{r_0 + r_2, r_1 + r_3\}$ as well.

By contrast, S_4 yields one orbit of size 6, A_4 yields one orbit of size 6, and V_4 yields three orbits of size 2.

Therefore $\text{Gal}(f)$ is isomorphic to either D_4 or C_4. In order to distinguish, we can use $\text{Gal}(R_{f,q})$, which has one orbit of size 4 and one orbit of size 8.

If $\text{Gal}(f) \cong C_4$, then $\text{Gal}(R_{f,q})$ would have the following three orbits of size four:

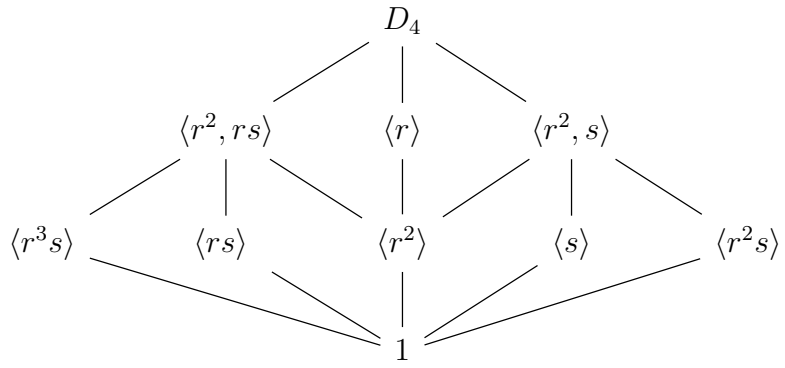
$$\{r_0 - r_1, r_1 - r_2, r_2 - r_3, r_3 - r_0\}, \{r_0 - r_2, r_1 - r_3, r_2 - r_0, r_1 - r_3\}, \{r_0 - r_3, r_1 - r_0, r_2 - r_1, r_3 - r_2\}.$$

Whereas, if $\text{Gal}(f) \cong D_4$, then $\text{Gal}(R_{f,q})$ has the following orbits of size eight and four:

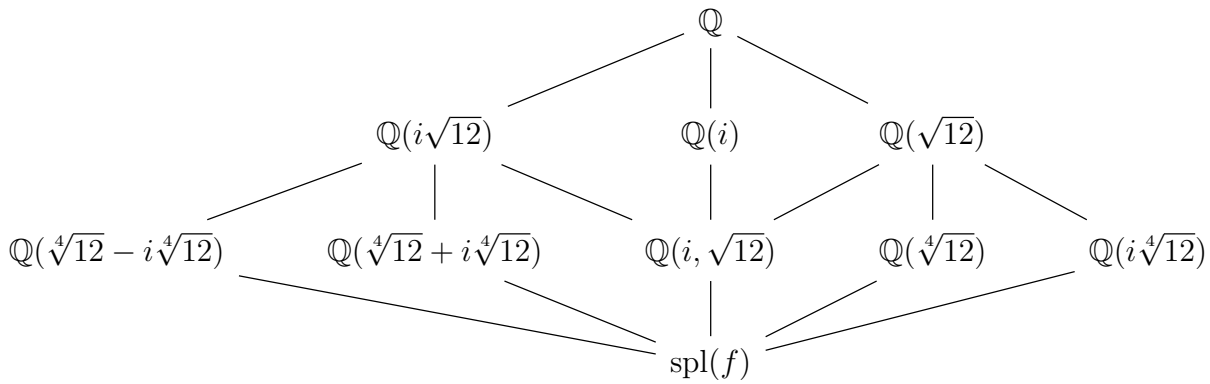
$$\{r_0 - r_1, r_1 - r_2, r_2 - r_3, r_3 - r_0, r_0 - r_3, r_1 - r_0, r_2 - r_1, r_3 - r_2\}, \{r_0 - r_2, r_1 - r_3, r_2 - r_0, r_1 - r_3\}.$$

Therefore we may conclude that $\text{Gal}(f) \cong D_4$, and so $[\text{spl}(f) : \mathbb{Q}] = 8$. Thus, I propose $\text{spl}(f) = \mathbb{Q}(\sqrt{2}\sqrt[4]{3}, i) = \mathbb{Q}(\sqrt[4]{12}, i) = \text{spl}(x^4 - 12)$.

We can construct $\text{Gal}(f) = \langle r, s | r^4, s^2, rsrs \rangle$, where $r(\sqrt[4]{12}) = i\sqrt[4]{12}$ and $r(i) = i$, and $s(\sqrt[4]{12}) = \sqrt[4]{12}$ and $s(i) = i$. Then we have the following hierarchy of groups:



which yields the corresponding hierarchy of field extensions:



Theorem FToGT. Galois extensions correspond to normal subgroups; that is: If K is an intermediate field of L/F and K/F is Galois, then $\mathrm{Gal}(L/K) \trianglelefteq \mathrm{Gal}(L/F)$. If $N \trianglelefteq \mathrm{Gal}(L/F)$, then L^N/F is Galois.

Proof. First let L/F be a Galois extension. Let K be an intermediate field of L/F, and K/F be Galois. Then define

$$\rho_K : \mathrm{Gal}(L/F) \to \mathrm{Gal}(K/F)$$

to be the restriction map: $\rho_K(\sigma) = \sigma|_K$. We would like to prove that $\ker \rho_K = \mathrm{Gal}(L/K)$, and so $\mathrm{Gal}(L/K) \trianglelefteq \mathrm{Gal}(L/F)$. First, let $\sigma \in \ker \rho_K$. Then $\sigma|_K = \mathrm{Id}_K$, and so σ fixes K, and so $\sigma \in \mathrm{Gal}(L/K)$.

Now let $\sigma \in \mathrm{Gal}(L/K)$. Then σ fixes K and so $\sigma|_K = \mathrm{Id}_K$. Thus $\sigma \in \ker \rho_K$. Thus $\ker \rho_K = \mathrm{Gal}(L/K) \trianglelefteq \mathrm{Gal}(L/F)$.

Now let $N \trianglelefteq \mathrm{Gal}(L/F)$. We would like to show that L^N is Galois. We can use the definition of Galois: L^N is Galois if and only if $\#\mathrm{Aut}(L^N/F) = \left[L^N : F\right]$. We know that

$$\left[L : L^N\right]\left[L^N : F\right] = [L : F].$$

Since $[\mathrm{Gal}(L/F) : N] = [L^N : F]$, and since N is normal, we have

$$\#\mathrm{Gal}(L/F)/N = [L^N : F].$$

Now we just want to prove that

$$\#\mathrm{Aut}(L^N/F) = \#\mathrm{Gal}(L/F)/N.$$

We can define a map

$$\psi_N : \mathrm{Gal}(L/F) \to \mathrm{Aut}(L^N/F)$$

by $\psi_N(\sigma) = \sigma|_{L^N}$. Then we want to show that ψ_N is surjective and $\ker \psi_N = N$. For the first, we can take $\nu \in \mathrm{Aut}(L^N/F)$. Then there is some $\sigma \in \mathrm{Gal}(L/F)$ such that $\nu = \sigma|_{L^N}$ since $F \subseteq L^N \subseteq L$ and so $\mathrm{Aut}(L^N/F) \leq \mathrm{Gal}(L/F)$.

Now let $\sigma \in \ker \psi_N$. Then $\sigma|_{L^N} = \mathrm{Id}_{L^N}$, and so by definition of L^N, $\sigma \in N$. Now let $\sigma \in N$. Then by definition, $\sigma|_{L^N} = \mathrm{Id}_{L^N}$ and so $\sigma \in \ker \psi_N$. Thus by the first isomorphism theorem

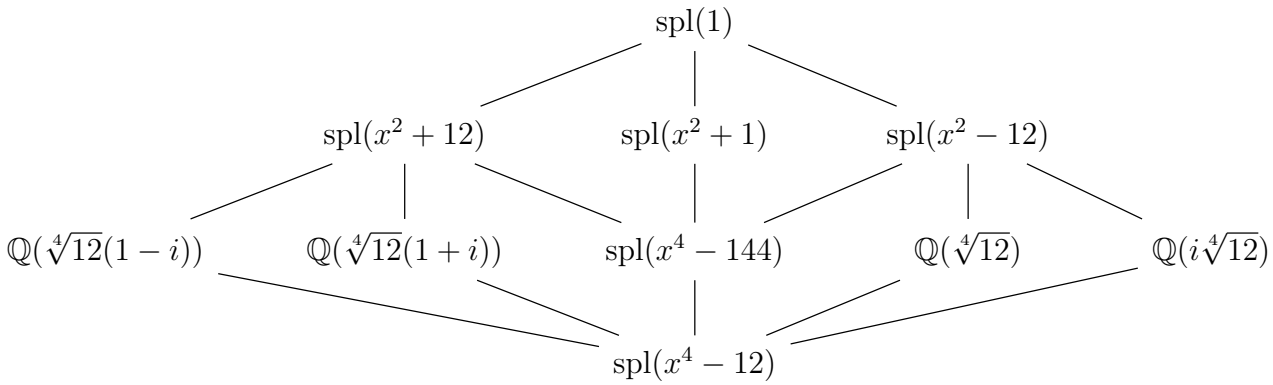
$$\mathrm{Gal}(L/F)/N \cong \mathrm{Aut}(L^N/F)$$

and so

$$\#\mathrm{Aut}(L^N/F) = [L^N : F]$$

and so L^N/F is Galois. □

In the hierarchy of subgroups above, only six of the subgroups are normal and so only six of the field extensions are Galois. Here is the hierarchy of field extensions again, this time with the Galois extensions rewritten in terms of the polynomials of which they are the splitting field.



Let $r = \frac{1}{2}(-1 + \sqrt[4]{12} - \sqrt{3})$, and let $s = r^2$. I want to know if $\mathbb{Q}(s) = \mathbb{Q}(r)$. Since r satisfies $r^4 + 2r^3 + 2r + 1 = 0$, we have $s^2 + 2s\sqrt{2} + 2\sqrt{s} + 1 = 0$, so $(s^2+1)^2 = (2s+2)^2 s$, so $s^4 + 2s^2 + 1 = 4s^3 + 8s^2 + 4s$, so $s^4 - 4s^3 - 6s^2 - 4s + 1 = 0$, so $[\mathbb{Q}(s) : \mathbb{Q}] = [\mathbb{Q}(r) : \mathbb{Q}] = 4$, and $\mathbb{Q}(s) \subseteq \mathbb{Q}(r)$, so $\mathbb{Q}(s) = \mathbb{Q}(r)$. Now how can we write r in the basis $\{1, s, s^2, s^3\} = \{1, r^2, -2r^3 - 2r - 1, -10r^3 + 3r^2 - 6r - 4\}$? Then

$$r = -\frac{1}{4} - \frac{3}{4}s - \frac{5}{4}s^2 + \frac{1}{4}s^3.$$

That way when we find

$$\alpha = \sqrt{-r^2 - 1}$$

we can write

$$s = -\alpha^2 - 1$$

upon constructing $\mathbb{Q}(\alpha)$. So then

$$r = -\frac{1}{4} + \frac{3}{4}(1+\alpha^2) - \frac{5}{4}(1+\alpha^2)^2 - \frac{1}{4}(1+\alpha^2)^3.$$

According to Wolfram, the minimal polynomial of α is

$$x^8 + 8x^6 + 12x^4 + 8x^2 + 4.$$

The splitting field L of $x^8 + 8x^6 + 12x^4 + 8x^2 + 4$ is a degree-2 extension of $\mathbb{Q}(\sqrt[4]{12}, i) = \text{spl}(x^4 - 12)$, so $[L : \mathbb{Q}] = 16$. Furthermore, D_4 is an index-2 subgroup of $\text{Gal}(L/\mathbb{Q})$. This is because the minimal polynomial of α is $x^2 + r^2 + 1 \in \mathbb{Q}(\sqrt[4]{12}, i)[x]$. Furthermore, D_4 is a normal subgroup of $\text{Gal}(L/\mathbb{Q})$ because it corresponds to a Galois extension. According to GroupNames, there are six groups of order 16 that are transitive on a set of eight points, and only four of those have a normal (or any) subgroup isomorphic to D_4. They are:

$$D_8,\ SD_{16},\ C_2 \times D_4,\ C_4 \circ D_4.$$

The eight roots of $x^8 + 8x^6 + 12x^4 + 8x^2 + 4$ are

$$\begin{aligned}
&\pm i\sqrt{2 + \sqrt{3} + \sqrt{3 + 2\sqrt{3}}} \\
&\pm i\sqrt{2 + \sqrt{3} - \sqrt{3 + 2\sqrt{3}}} \\
&\pm\sqrt{-2 + \sqrt{3} + i\sqrt{-3 + 2\sqrt{3}}} \\
&\pm\sqrt{-2 + \sqrt{3} - i\sqrt{-3 + 2\sqrt{3}}}
\end{aligned}$$

If $\text{Gal}(L/\mathbb{Q}) \cong D_8$, then the 28 sums $r_i + r_j$ with $i \neq j$ form three orbits of size 8 and one orbit of size 4. By contrast, if $\text{Gal}(L/\mathbb{Q}) \cong C_2 \times D_4$, then there are three orbits of size 4 and two orbits of size 8.

Unfortunately, the resolvent polynomial is not square-free. It is

$$\begin{aligned}
&u^{28} + 48u^{26} + 960u^{24} + 10432u^{22} + 67584u^{20} + 270336u^{18} \\
&+650368u^{16} + 807936u^{14} + 122880u^{12} - 811008u^{10} - 589824u^8 - 110592u^4
\end{aligned}$$

which factors as

$$(u)^4(u^2+2)^2(u^4+6u^2+12)^2(u^4+12u^2-12)(u^8+20u^6+108u^4-16u^2+16).$$