GALOIS THEORY EXAMPLE 2

Set $f = t^5 - 3 \in \mathbb{Q}[t]$. Set $\alpha = \sqrt[5]{3} \in \mathbb{R}_+$, $\zeta = \mathrm{e}^{2\pi i/5}$. We have discussed why f is irreducible over $\mathbb{Q}$, with roots $\alpha, \alpha\zeta, \alpha\zeta^2, \alpha\zeta^3, \alpha\zeta^4$. Thus with

$$L = \mathbb{Q}(\alpha, \alpha\zeta, \alpha\zeta^2, \alpha\zeta^3, \alpha\zeta^4) = \mathbb{Q}(\alpha, \zeta),$$

$L : \mathbb{Q}$ is a splitting field extension for f. As $\mathrm{char}\mathbb{Q} = 0$, we also know that $L : \mathbb{Q}$ is a separable extension; hence $L : \mathbb{Q}$ is a Galois extension.

Also recall that we saw $\deg m_\alpha(\mathbb{Q}) = \deg f = 5$, and $\deg m_\zeta(\mathbb{Q}) = \deg(t^5 - 1)/(t-1) = 4$. Hence $[Q(\alpha) : \mathbb{Q}] = 5$ and $[\mathbb{Q}(\zeta) : \mathbb{Q}] = 4$. From this we deduced that $[L : \mathbb{Q}] = 20$.

We defined the $\mathbb{Q}$ homomorphisms $\varphi : L \to L$ so that $\varphi(\alpha) = \alpha\zeta$ and $\varphi(\zeta) = \zeta$; we also defined $\tau : L \to L$ so that $\tau(\alpha) = \alpha$ and $\tau(\zeta) = \zeta^3$. We determined that φ has order 5, τ has order 4, and $\varphi\tau = \tau\varphi^2$. Thus with $G = Gal(L : K)$, we can write G as

$$G = \langle \tau, \varphi : \ \tau^4 = 1 = \varphi^5, \ \varphi\tau = \tau\varphi^2 \ \rangle.$$

Also, $G = \{\tau^a\varphi^b : \ 1 \le a \le 4, \ 1 \le b \le 5 \ \}$.

A slight detour: Recall that before defining τ we defined a homomorphism $\psi : L \to L$ so that $\psi(\alpha) = \alpha$ and $\psi(\zeta) = \zeta^4$. We found that ψ has order 2. Could we have anticipated this? The values $\zeta, \zeta^2, \zeta^3, \zeta^4$ are all primitive 5th roots of unity. However, $\zeta^4 = \zeta^{-1}$, and since ψ is a homomorphism, we have

$$\psi(\zeta^4) = \psi(\zeta^{-1}) = \psi(\zeta)^{-1}, \text{ so } \psi^2(\zeta) = \psi(\zeta^{-1}) = (\psi(\zeta))^{-1} = (\zeta^{-1})^{-1} = \zeta.$$

So in hindsight, we could have anticipated that the order of ψ is 2.

Using Sylow theory: We know that $|G|$ is a non-abelian group of order 20. So it has a Sylow 2-subgroup and a Sylow 5-subgroup. Also, with $p = 2$ or 5, we know that all Sylow p-subgroups are conjugate, the number of Sylow p-subgroups divides $|G| = 20$, and the number of Sylow p-subgroups is conjugage to 1 modulo p. This means that we have either 1 or 5 Sylow 2-subgroups, and 1 Sylow 5-subgroup (which is necessarily a normal subgroup of G).

As φ has order 5, $\langle\varphi\rangle$, the subgroup generated by φ, must be the only Sylow 5-subgroup. As τ has order 4, $\langle\tau\rangle$ is a Sylow 2-subgroup. We have $\varphi\tau\varphi^{-1} = \tau\varphi^2\varphi^{-1} = \tau\varphi \notin \langle\tau\rangle$, so $\varphi\langle\tau\rangle\varphi^{-1}$ must be another Sylow 2-subgroup. Thus there must be 5 Sylow 2-subgroups. We know that for $\sigma \in G$, we have

$$\sigma\langle\tau\rangle\sigma^{-1} = \{1, \sigma\tau\sigma^{-1}, \sigma\tau^2\sigma^{-1}, \sigma\tau^3\sigma^{-1}\};$$

also, the order of $\sigma\tau^a\sigma^{-1}$ is the order of τ^a. To help with computing these Sylow 2-subgroups, we can first organise information as in the below table.

$$\begin{aligned}
\varphi\tau = \tau\varphi^2, \qquad & \varphi^2\tau = \varphi\tau\varphi^2 = \tau\varphi^4, \\
\varphi^3\tau = \varphi\tau\varphi^4 = \tau\varphi, \qquad & \varphi^4\tau = \varphi\tau\varphi = \tau\varphi^3
\end{aligned}$$

$$\begin{aligned}
\varphi\tau^2 = \tau\varphi^2\tau = \tau^2\varphi^4, \qquad & \varphi^2\tau^2 = \tau\varphi^4\tau = \tau^2\varphi^3, \\
\varphi^3\tau^2 = \tau\varphi\tau = \tau^2\varphi^2, \qquad & \varphi^4\tau^2 = \tau\varphi^3\tau = \tau^2\varphi,
\end{aligned}$$

$$\begin{aligned}
\varphi\tau^3 = \tau^2\varphi^4\tau = \tau^3\varphi^3, \qquad & \varphi^2\tau^3 = \tau^2\varphi^3\tau = \tau^3\varphi, \\
\varphi^3\tau^3 = \tau^2\varphi^2\tau = \tau^3\varphi^4, \qquad & \varphi^4\tau^3 = \tau^2\varphi\tau = \tau^3\varphi^2.
\end{aligned}$$

Thus the 5 Slylow 2-subgroups are

$$\begin{aligned}
\langle\tau\rangle &= \{1, \tau, \tau^2, \tau^3\}, \\
\varphi\langle\tau\rangle\varphi^{-1} &= \{1, \varphi\tau\varphi^{-1}, \varphi\tau^2\varphi^{-1}, \varphi\tau^3\varphi^{-1}\} \\
&= \{1, \tau\varphi, \tau^2\varphi^3, \tau^3\varphi^2\}, \\
\varphi^2\langle\tau\rangle\varphi^{-2} &= \varphi^2\langle\tau\rangle\varphi^3 \\
&= \{1, \tau\varphi^2, \tau^2\varphi, \tau^3\varphi^4\}, \\
\varphi^3\langle\tau\rangle\varphi^{-3} &= \varphi^3\langle\tau\rangle\varphi^2 \\
&= \{1, \tau\varphi^3, \tau^2\varphi^4, \tau^2\varphi\}, \\
\varphi^4\langle\tau\rangle\varphi^{-4} &= \varphi^4\langle\tau\rangle\varphi \\
&= \{1, \tau\varphi^4, \tau^2\varphi^2, \tau^3\varphi^3\}.
\end{aligned}$$

As any subgroup of G with order 2 is contained in a Sylow 2-subgroup, the elements of these Sylow 2-subgroups contain all elements of G of order 2 or 4. The Sylow 5-subgroup contains all elements of G of order 5. So G contains 1 element of order 1, 5 elements of order 2, 10 elements of order 4, and 4 elements of order 5. This accounts for all the elements in G, so if G has a subgroup of order 10 then it is generated by an element of order 2 and an element of order 5. With N a subgroup of G with order 10, N must be a normal subgroup of G as $[G : N] = 2$. The elements in G of order 2 are

$$\tau^2,\ \varphi\tau^2\varphi^{-1} = \tau^2\varphi^3,\ \varphi^2\tau^2\varphi^{-2} = \tau^2\varphi,\ \varphi^3\tau^2\varphi^{-3} = \tau^2\varphi^4,\ \varphi^4\tau^2\varphi^{-4} = \tau^2\varphi^2.$$

With $N_1 = \langle\tau^2, \varphi\rangle$, the subgroup generated by τ^2 and φ, we see that

$$N_1 = \{1, \varphi, \varphi^2, \varphi^3, \varphi^4, \tau^2, \tau^2\varphi, \tau^2\varphi^2, \tau^2\varphi^3, \tau^2\varphi^4\}$$

and that N_1 contains all the elements of G of orders 1, 2, and 10. (We know from our table above that any product of powers of τ^2 and powers of φ can be written as either φ^b or $\tau^2\varphi^b$ for some b, $1 \le b \le t$. This allows us to conclude that N_1 has exactly 10 elements.) Also, N_1 contains all the elements of G of orders 2 and 5; since any subgroup of G of order 10 must contain an element of order 2 and an element of order 5, N_1 is the only subgroup of G of order 10.

Let us name the Slylow subgroups as follows.

$$\begin{aligned}
H_0 &= \langle\tau\rangle,\\
H_1 &= \varphi\langle\tau\rangle\varphi^{-1} = \langle\varphi\tau\varphi^{-1}\rangle = \langle\tau\varphi\rangle,\\
H_2 &= \varphi^2\langle\tau\rangle\varphi^{-2} = \langle\varphi^2\tau\varphi^{-2}\rangle = \langle\tau\varphi^2\rangle,\\
H_3 &= \varphi^3\langle\tau\rangle\varphi^{-3} = \langle\varphi^3\tau\varphi^{-3}\rangle = \langle\tau\varphi^3\rangle,\\
H_4 &= \varphi^4\langle\tau\rangle\varphi^{-4} = \langle\varphi^4\tau\varphi^{-4}\rangle = \langle\tau\varphi^4\rangle,\\
N_0 &= \langle\varphi\rangle.
\end{aligned}$$

Let us name the order 2 subgroups as follows.

$$H_5 = \langle\tau^2\rangle,\ H_6 = \langle\tau^2\varphi\rangle,\ H_7 = \langle\tau^2\varphi^2\rangle,\ H_8 = \langle\tau^2\varphi^3\rangle,\ H_9 = \langle\tau^2\varphi^4\rangle.$$

Recall that for a subgroup H of G, we have $[Fix_L(H) : \mathbb{Q}] = [G : H]$, and when H is a normal subgroup of G, $Fix_L(H) : \mathbb{Q}$ is a normal extension. As G has only one subgroup of order 10, there is only one subfield of L with order 2 over $\mathbb{Q}$. We know G has 5 subgroups of order 4, so L has exactly 5 subfields of degree 5 over $\mathbb{Q}$, and these must be $\mathbb{Q}(\alpha)$, $\mathbb{Q}(\alpha\zeta)$, $\mathbb{Q}(\alpha\zeta^2)$, $\mathbb{Q}(\alpha\zeta^3)$, $\mathbb{Q}(\alpha\zeta^4)$ (why?). As G has 5 subgroups of order 2, L has exactly 5 subfields of degree 10 over $\mathbb{Q}$. For each order 2 subgroup H_i ($5 \le i \le 9$), since $H_i \subseteq N_1$, Theorem 10.1 tells us that $Fix_L(H_i) \supseteq Fix_L(N_1)$. Also, for each i with $5 \le i \le 9$, there is some j with $0 \le j \le 4$ so that $H_i \subseteq H_j$ and hence $Fix_L(H_i) \supseteq Fix_L(H_j)$.

Let us now compute some of the fixed fields of subgroups of G. We will start with some easy computations.

(i) First we compute $Fix_L(N_0)$. We know $\varphi(\zeta) = \zeta$, so $\mathbb{Q}(\zeta) \subseteq Fix_L(N_0)$. Since $[Q(\zeta) : \mathbb{Q}] = 4 = [G : N_0]$, we have $\mathbb{Q}(\zeta) = Fix_L(N_0)$. Also, $G/N_0 \simeq Gal(\mathbb{Q}(\zeta) : \mathbb{Q})$.

(ii) Next we compute $Fix_L(H_0)$. We know $\tau(\alpha) = \alpha$, so $\mathbb{Q}(\alpha) \subseteq Fix_L(H_0)$. Since $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 5$ and $[G : H_0] = 5$, we have $\mathbb{Q}(\alpha) = Fix_L(H_0)$.

(iii) We compute $Fix_L(H_5)$. We have $\tau^2(\alpha) = \alpha$. Also, τ^2 has order 2, so τ^2 must fix $\zeta+\tau^2(\zeta) = \zeta+\zeta^9 = \zeta+\zeta^4$. (Also notice that $\zeta^2+\tau^2(\zeta^2) = \zeta^2+\zeta^3$ is fixed by τ^2.) Thus we have $\mathbb{Q}(\alpha, \zeta+\zeta^4) \subseteq Fix_L(H_5)$. By the Tower Law, we know that 5 divides $[\mathbb{Q}(\alpha, \zeta+\zeta^4) : \mathbb{Q}]$. (We want to show that $[\mathbb{Q}(\zeta+\zeta^4) : \mathbb{Q}] = 2$ so that we can argue that $\mathbb{Q}(\alpha, \zeta+\zeta^4) = Fix_L(H_5)$.) We have $1+\zeta+\zeta^2+\zeta^3+\zeta^4 = 0$, and

$$(\zeta+\zeta^4)^2 = \zeta^2 + 2\zeta^5 + \zeta^8 = \zeta^2 + 2 + \zeta^3.$$

Hence $\zeta+\zeta^4$ is a root of t^2+t-1. As this polynomial has no roots modulo 2, it is irreducibe over $\mathbb{Z}$ and hence over $\mathbb{Q}$; so

$$[\mathbb{Q}(\zeta+\zeta^4) : \mathbb{Q}] = 2.$$

Consequently 10 divides $[\mathbb{Q}(\alpha, \zeta+\zeta^4) : \mathbb{Q}]$. As $\mathbb{Q}(\alpha, \zeta+\zeta^4) \subseteq Fix_L(H_5)$ and $[Fix_L(H_5) : \mathbb{Q}] = [G : H_5] = 10$, we must have $\mathbb{Q}(\alpha, \zeta+\zeta^4) = Fix_L(H_5)$.

(iv) Here we find H so that $\mathbb{Q}(\zeta+\zeta^4) = Fix_L(H)$. In (iii), we saw that $[\mathbb{Q}(\zeta+\zeta^4) : \mathbb{Q}] = 2$. So for some subgroup H of G with $[G : H] = 2$, we have $\mathbb{Q}(\zeta+\zeta^4) = Fix_L(H)$. Thus $|H|$ must be 10, and the only

subgroup of G of order 10 is N_1. Hence $\mathbb{Q}(\zeta+\zeta^4) = Fix_L(N_1)$, and $G/N_1 \simeq Gal(\mathbb{Q}(\zeta+\zeta^4):\mathbb{Q})$.

(v) We compute $Fix_L(H_1)$; we know this is $\mathbb{Q}(\alpha\zeta^k)$ for some k, $1 \le k \le 4$ (we know $\mathbb{Q}(\alpha) = Fix_K(H_0)$, and we have a one-to-one correspondence between the subgroups of G of order 4 and the subfields of L with degree $5 = 20/4$ over $\mathbb{Q}$). We have

$$\tau\varphi(\alpha\zeta^k) = \tau(\alpha\zeta^{k+1}) = \alpha(\zeta^3)^{k+1}.$$

We need to find k ($1 \le k \le 4$) with $\zeta^k = \zeta^{3k+3}$, which means we want $k \equiv 3k+3 \pmod 5$. Solving this gives us $k = 1$, and hence $\mathbb{Q}(\alpha\zeta) = Fix_L(H_1)$.

(vi) We compute $Fix_L(\langle(\tau\varphi)^2\rangle)$. (Note that $\langle(\tau\varphi)^2\rangle$ is a subgroup of H_1.) Using our table, we find that $(\tau\varphi)^2 = \tau^2\zeta^3$, and so $H_8 \subseteq H_1$. Thus $Fix_L(H_8) \supseteq Fix_L(H_1) = \mathbb{Q}(\alpha\zeta)$. We also know $Fix_L(H_8) \supseteq Fix_L(N_1) = \mathbb{Q}(\zeta+\zeta^4)$. Thus $\mathbb{Q}(\alpha\zeta, \zeta+\zeta^4) \subseteq Fix_L(H_8)$. As

$$\begin{aligned}
&[\mathbb{Q}(\alpha\zeta, \zeta+\zeta^4) : \mathbb{Q}(\zeta+\zeta^4)][\mathbb{Q}(\zeta+\zeta^4) : \mathbb{Q}] \\
&\quad = [\mathbb{Q}(\alpha\zeta, \zeta+\zeta^4) : \mathbb{Q}] \\
&\quad = [\mathbb{Q}(\alpha\zeta, \zeta+\zeta^4) : \mathbb{Q}(\alpha\zeta)][\mathbb{Q}(\alpha\zeta) : \mathbb{Q}]
\end{aligned}$$

(by the Tower Law), we know 10 divides $[\mathbb{Q}(\alpha\zeta, \zeta+\zeta^4) : \mathbb{Q}]$. Thus we must have $\mathbb{Q}(\alpha\zeta, \zeta+\zeta^4) = Fix_L(H_8)$ as $[Fix_L(H_8) : \mathbb{Q}] = 10 = [G : H_8]$.

Exercise: Find the fixed fields for the subgroups $H_2, H_3, H_4, H_6, H_7, H_9$.