## GALOIS THEORY: SOLUTIONS TO HOMEWORK 12

1. Let $L : K$ be a finite Galois extension with Galois group $G$. For any $\alpha \in L$, define the polynomial $f_\alpha(t) = \prod_{\sigma \in G}(t - \sigma(\alpha))$.
   (a) Show that $f_\alpha \in K[t]$.
   **Solution:** Since $L : K$ is Galois, the fixed field of $G$ is $K$. Then $\beta \in K$ if and only if $\tau(\beta) = \beta$ for every $\tau \in G$. Thus, whenever $\tau \in G$, one has
   $$\tau(f_\alpha(t)) = \prod_{\sigma \in G}(t - \tau(\sigma(\alpha))) = \prod_{\rho \in G}(t - \rho(\alpha)) = f_\alpha(t).$$
   Then $f_\alpha(t)$ has each of its coefficients in the fixed field of $G$, so $f_\alpha \in K[t]$.
   (b) Prove that if $\sigma(\alpha) \neq \tau(\alpha)$ whenever $\sigma, \tau \in G$ satisfy $\sigma \neq \tau$, then $f_\alpha = m_\alpha(K)$.
   **Solution:** Since the identity element belongs to $G$, one has $f_\alpha(\alpha) = 0$, whence the minimal polynomial $m_\alpha(K)$ of $\alpha$ over $K$ must divide $f_\alpha$. But over $L[t]$ one has that $t - \alpha$ divides $m_\alpha(K)$. Then since $m_\alpha(K)$ is fixed by the action of $G$ (its coefficients lie in $K$), we find that $t - \sigma(\alpha)$ divides $\sigma(m_\alpha(K)) = m_\alpha(K)$ for each $\sigma \in G$. By hypothesis, moreover, the elements $\sigma(\alpha)$ are distinct for $\sigma \in G$, and thus $\prod_{\sigma \in G}(t - \sigma(\alpha)) = f_\alpha(t)$ divides $m_\alpha(K)$. Thus we find that $m_\alpha(K)$ and $f_\alpha$ divide each other, and this implies that $f_\alpha$ is the minimal polynomial of $\alpha$.
2. Use question 1 to calculate the minimal polynomial of $2\sqrt{-3} - \sqrt{2}$ over $\mathbb{Q}$.
   **Solution:** The field extension $\mathbb{Q}(\sqrt{2}, \sqrt{-3}) : \mathbb{Q}$ is a splitting field extension for the polynomial $(t^2 - 2)(t^2 + 3)$, and hence is finite and Galois. One checks easily (via the Tower Law) that $[\mathbb{Q}(\sqrt{2}, \sqrt{-3}) : \mathbb{Q}] = 4$, and thus the conjugates of $2\sqrt{-3} - \sqrt{2}$ under the action of $\mathrm{Gal}(\mathbb{Q}(\sqrt{2}, \sqrt{-3}) : \mathbb{Q})$ are $\pm(2\sqrt{-3} - \sqrt{2})$ and $\pm(2\sqrt{-3} + \sqrt{2})$. Then applying the conclusion of part (ii), we find that the minimal polynomial of $2\sqrt{-3} - \sqrt{2}$ is
   $$(t^2 - (2\sqrt{-3} - \sqrt{2})^2)(t^2 - (2\sqrt{-3} + \sqrt{2})^2) = t^4 + 20t^2 + 196.$$
3. Let $f$ denote the polynomial $t^3 + t + 1$.
   (a) Write down a splitting field extension for $f$ over $\mathbb{F}_2$.
   **Solution:** If $\alpha$ is a root of $t^3 + t + 1$ lying in a splitting field extension $L$ for this polynomial over $\mathbb{F}_2$, then
$$f(t) = t^3 + t + 1 = (t + \alpha)(t^2 + \alpha t + \alpha^2 + 1) = (t + \alpha)(t + \alpha^2)(t + \alpha^2 + \alpha).$$
   Then $\mathbb{F}_2(\alpha) : \mathbb{F}_2$ is a splitting field extension for $t^3 + t + 1$ over $\mathbb{F}_2$.
   (b) What is $\mathrm{Gal}_{\mathbb{F}_2}(f)$? Justify your answer, and determine all subfields of the splitting field that you wrote down in part (a).
   **Solution:** Observe that $f$ is irreducible over $\mathbb{F}_2$, since otherwise, as a polynomial of degree 3, it would have a linear factor over $\mathbb{F}_2$, and hence have 0 or 1 as a root, which is not the case. It follows that $m_\alpha(\mathbb{F}_2) = f$.

Hence, since $f$ is a separable polynomial, we find that $\mathbb{F}_2(\alpha) : \mathbb{F}_2$ is a Galois extension, with Galois group of order $[\mathbb{F}_2(\alpha) : \mathbb{F}_2] = 3$. Then $\mathrm{Gal}(\mathbb{F}_2)$ must be cyclic.

In this case it is not too difficult to write down the automorphisms. If $\phi(x) = x^2$ for $x \in \mathbb{F}_2(\alpha)$, we have seen that this Frobenius monomorphism is an automorphism, with $\phi(\alpha) = \alpha^2$. We get another automorphism by squaring $\phi$, so that $\phi^2(x) = \phi(\phi(x)) = \phi(x^2) = x^4$, and in particular $\phi^2(\alpha) = \alpha^4 = \alpha^2 + \alpha$. Thus, the identity, $\phi$ and $\phi^2$ are the three automorphisms. One can also check directly that $\phi$ has order 3, thus $\phi^3(\alpha) = \alpha^8 = \alpha$.

Since the cyclic group $\langle\phi\rangle$ of order 3 has no proper subgroups, it follows from the Fundamental Theorem of Galois Theory that $\mathbb{F}_2(\alpha)$ has no proper subfields, and hence the only subfields are the trivial ones $\mathbb{F}_2$ and $\mathbb{F}_2(\alpha)$.

4. Let $f$ denote the polynomial $t^4 + t^3 + t^2 + t + 1$.
   (a) Write down a splitting field extension for $f$ over $\mathbb{Q}$.
   **Solution:** If $\alpha$ is a root of $f$, then $\alpha^5 = 1$. Thus, we see that on putting $\zeta = e^{2\pi i/5}$, we have $f(t) = (t-\zeta)(t-\zeta^2)(t-\zeta^3)(t-\zeta^4)$. Then $\mathbb{Q}(\zeta) : \mathbb{Q}$ is a splitting field extension for $f$ over $\mathbb{Q}$.
   (b) Show that $\mathrm{Gal}_{\mathbb{Q}}(f) \cong C_4$, where $C_4$ is the cyclic group of order 4.
   **Solution:** Observe that $f$ is irreducible over $\mathbb{Q}$, since 5 is prime and the polynomial $t^{p-1} + \ldots + t + 1$ is irreducible for primes $p$. Then $m_\zeta(\mathbb{Q}) = f$ and $[\mathbb{Q}(\zeta) : \mathbb{Q}] = \deg(f) = 4$. Moreover, the extension $\mathbb{Q}(\zeta) : \mathbb{Q}$ is separable and normal, and hence Galois, so that $\mathrm{Gal}(f)$ has order $[\mathbb{Q}(\zeta) : \mathbb{Q}] = 4$. The Galois group acts transitively on the roots of $f$, and so there is an automorphism $\sigma \in \mathrm{Gal}(f)$ having the property that $\sigma(\zeta) = \zeta^2$. One then sees that

$$\begin{aligned}
\sigma^2(\zeta) &= \sigma(\zeta^2) = \zeta^4 = -(1 + \zeta + \zeta^2 + \zeta^3),\\
\sigma^3(\zeta) &= \sigma(\zeta^4) = \zeta^8 = \zeta^3,\\
\sigma^4(\zeta) &= \sigma(\zeta^3) = \zeta^6 = \zeta.
\end{aligned}$$

   Thus $\sigma$ is an automorphism of order 4, and one must have $\mathrm{Gal}(f) = \langle\sigma\rangle \cong C_4$.

5. Use the Galois correspondence to determine all subfields of the splitting field that you wrote down in part (a) of question 4. Draw the lattice of subfields and corresponding lattice of subgroups of $C_4$.
   **Solution:** The cyclic group of order 4 given by $G = \langle\sigma^i \,|\, \sigma^4 = 1\rangle$ has the trivial subgroups $\{1\}$ and $G$, and the additional subgroup $H = \{1, \sigma^2\}$ of order 2, and no other subgroups. Then by the Fundamental Theorem of Galois Theory, the field $\mathbb{Q}(\zeta)$ has only one non-trivial subfield, and this is $\mathrm{Fix}_{\mathbb{Q}(\zeta)}(H)$. In this case, we can apply brute force easily enough to determine the fixed field. Given arbitrary rational numbers $a, b, c, d$, one sees that $a + b\zeta + c\zeta^2 + d\zeta^3 = \sigma^2(a + b\zeta + c\zeta^2 + d\zeta^3)$ if and only if

$$a + b\zeta + c\zeta^2 + d\zeta^3 = a - b(1 + \zeta + \zeta^2 + \zeta^3) + c\zeta^3 + d\zeta^2.$$

Thus we must have $a - b = a$, $b = -b$, $c = -b + d$, $d = -b + c$, whence $b = 0$ and $c = d$. We therefore conclude that the fixed field of the group generated by $\sigma^2$ is $\mathbb{Q}(\zeta^2 + \zeta^3)$. The lattices of subfields and corresponding subgroups:

$$\begin{array}{cc} G = \langle \sigma \rangle & \mathbb{Q} \\ | & | \\ \langle \sigma^2 \rangle & \mathbb{Q}(\zeta^2 + \zeta^3) \\ | & | \\ \langle 1 \rangle & \mathbb{Q}(\zeta) \end{array}$$