# GALOIS THEORY 2019: HW 3 SOLUTIONS

**For assessment: Problems 1, 2, 3**
**Due by noon Tuesday, week 7 of the term**

1. (a) Let $L : \mathbb{Q}$ be a splitting field extension for $f(X) = (X^2-2)(X^2+7)$.
   (i) Determine the degree of the extension $L : \mathbb{Q}$, justifying your answer.
   (ii) Describe the Galois group $\mathrm{Gal}(L : \mathbb{Q})$ (that is, give generators and relations for the Galois group).

   *Solutions:* [This is from the 2015 exam.] (i) We have $L = \mathbb{Q}(\sqrt{2}, \sqrt{-7})$. The polynomials $X^2 - 2$ and $X^2 + 7$ are both irreducible over $\mathbb{Q}$ (by Eisenstein's Criterion with $p = 2$ and $p = 7$ they are irreducible over $\mathbb{Z}$, and then by Gauss' Lemma they are irreducible over $\mathbb{Q}$). The roots of $X^2-2$ are $\pm\sqrt{2}$, and so $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$. Over $\mathbb{Q}(\sqrt{2})$, if $X^2 + 7$ is reducible then it has a linear factor in $\mathbb{Q}(\sqrt{2})[X]$ which means that $\sqrt{-7} \in \mathbb{Q}(\sqrt{2})$. But $\mathbb{Q}(\sqrt{2}) \subseteq \mathbb{R}$ and $\sqrt{-7} \notin \mathbb{R}$, so $X^2 + 7$ must be irreduible over $\mathbb{Q}(\sqrt{2})$. Thus $[\mathbb{Q}(\sqrt{2}, \sqrt{-7}) : \mathbb{Q}(\sqrt{2})] = 2$ and (by the Tower Law) $[\mathbb{Q}(\sqrt{2}, \sqrt{-7}) : \mathbb{Q}] = 4$.
   (ii) $Gal(L : \mathbb{Q})$ is generated by the $\mathbb{Q}$-homomorphisms $\sigma, \tau$ where $\sigma(\sqrt{2}) = -\sqrt{2}, \sigma(\sqrt{-7}) = \sqrt{-7}, \tau(\sqrt{2}) = -\sqrt{2}, \tau(\sqrt{-7}) = \sqrt{-7}$. So $\sigma^2 = 1 = \tau^2$, $\sigma\tau = \tau\sigma$, and $Gal(L : \mathbb{Q}) = \{1, \sigma, \tau, \sigma\tau\}$. We can also present this group as follows:

$$Gal(L : \mathbb{Q}) \simeq \langle \sigma, \tau : \ \sigma^2 = 1 = \tau^2, \ \sigma\tau = \tau\sigma \ \rangle$$
$$\simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}.$$

   (b) Let $K : \mathbb{Q}$ be a splitting field extension for $g(X) = X^4 - 5$.
   (i) Show that $[K : \mathbb{Q}] = 8$.
   (ii) ) Describe the Galois group $\mathrm{Gal}(K : \mathbb{Q})$.

*Solutions:* Let $\alpha = \sqrt[4]{5} \in \mathbb{R}_+$, and let $i = \mathrm{e}^{2\pi i/4}$. The roots of $g$ are $\pm\alpha, \pm i\alpha$. Thus with $L = \mathbb{Q}(\alpha, i)$, $L : \mathbb{Q}$ is a splitting field for $g$. [Note that all roots of $g$ lie in $\mathbb{Q}(\alpha, i)$; also, $i$ is the quotient of two roots of $g$ so $\mathbb{Q}(\alpha, i)$ is contained in a splitting field for $g$.]

(i) By Eisenstein's Criterion (with $p = 5$), $g$ is irreducible over $\mathbb{Z}$, and so by Gauss' Lemma, $g$ is irreducible over $\mathbb{Q}$. Hence $[\mathbb{Q}(\alpha) : \mathbb{Q}] = \deg \mathrm{m}_\alpha(\mathbb{Q}) = 4$. We know that $i$ is a root of $X^2 + 1$, so $\deg \mathrm{m}_i(\mathbb{Q}(\alpha)) \leq 2$. If $\deg \mathrm{m}_i(\mathbb{Q}(\alpha)) = 1$ then $i \in \mathbb{Q}(\alpha)$, but $\mathbb{Q}(\alpha) \subseteq \mathbb{R}$ and $i \notin \mathbb{R}$. Hence $[K : \mathbb{Q}(\alpha)] = \deg \mathrm{m}_i(\mathbb{Q}(\alpha)) = 2$ and so (by the Tower Law) $[K : \mathbb{Q}] = 8$.

ALTERNATIVELY: We can realise $K$ as $\mathbb{Q}(\alpha, i\alpha)$, and follow essentially the above procedure with $i\alpha$ in place of $i$.

(ii) We can construct the elements of $G = Gal(K : \mathbb{Q})$ by first extending the identity map on $\mathbb{Q}$ to a homomorphism $\sigma : \mathbb{Q}(\alpha) \to K$ by mapping $\alpha$ to another root of $g$ [this gives us 4 choices]. Then we extend $\sigma$ to a homomorphism $\tau : K \to K$ by mapping $i$ to $\pm i$ [or by mapping $i\alpha$ to $\pm i\alpha$]. Let $\varphi, \psi : K \to K$ be the $\mathbb{Q}$-homomorphisms from $K$ into $K$ where $\varphi(\alpha) = i\alpha$, $\varphi(i) = i$, $\psi(\alpha) = \alpha$, $\psi(i) = -i$. [Note that as $K : \mathbb{Q}$ is an algebraic extension, by Theorem 3.4, $\varphi, \psi \in Aut(L)$.] So we have $\varphi(i\alpha) = \varphi(i)\varphi(\alpha) = -\alpha$, $\varphi(-\alpha) = -\varphi(\alpha) = -\alpha$, $\varphi(-i\alpha) = -\varphi(i\alpha) = \alpha$. Also, $\psi(i\alpha) = \psi(i)\psi(\alpha) = -i\alpha$, $\psi(-i\alpha) = -\psi(i)\psi(\alpha) = i\alpha$, $\psi(-\alpha) = -\psi(\alpha) = -\alpha$. As well, we have $\varphi\psi(\alpha) = \varphi(\alpha) = i\alpha$, $\varphi\psi(i) = \varphi(-i) = -\varphi(i) = -i$, $\psi\varphi^3(\alpha) = \psi(-i\alpha) = -\psi(i)\psi(\alpha) = i\alpha$, $\psi\varphi^3(i) = \psi(i) = -i$. Hence

$$Gal(K : \mathbb{Q}) \simeq \left\langle \varphi, \psi : \ \varphi^4 = 1 = \psi^2, \ \varphi\psi = \psi\varphi^3 \ \right\rangle.$$

[Note that since $K : \mathbb{Q}$ is a splitting field for $g$, each element of $Gal(K : \mathbb{Q})$ corresponds to a permutation of the roots of $g$. We can associate $\varphi$ with the permutation

$$(\alpha \ i\alpha \ -\alpha \ -i\alpha),$$

and we can associate $\psi$ with the permutation

$$(i\alpha \ -i\alpha).$$

Using these permuations to represent $\varphi$ and $\psi$, we can discern the relation $\varphi\psi = \psi\varphi^3$.]

2. Suppose that $L : K$ is a normal extension with $K \subseteq L \subseteq \overline{L}$ where $\overline{L}$ is an algebraic closure of $L$.
   (a) Suppose $\tau : L \to \overline{L}$ is a $K$-homomorphism. Show that $\tau(L) = L$.
   (b) Suppose $M : K$ is a normal extension so that $K \subseteq M \subseteq L$ and $\tau \in Gal(L : K)$. Show that $\tau(M) = M$. (Suggestion: use (a).)

*Solutions:* (a) [This is Proposition 6.1.] Take $\alpha \in L$. Since $L : K$ is a normal extension, it is an algebraic extension and hence $m_\alpha(K)$ exists. Let $f = m_\alpha(K)$. So $f(\alpha) = 0$ and hence [by Proposition 3.1]

$$0 = \tau(f(\alpha)) = f(\tau(\alpha)).$$

Since $L : K$ is a nomal extension and $f$ is an irreducible polynomial with a root $\alpha$ in $L$, we know that $f$ must split over $L$. We see above that $\tau(\alpha)$ is a root of $f$, so $\tau(\alpha) \in L$. This argument holds for all $\alpha \in L$, and hence $\tau(L) \subseteq L$. Then by Theorem 3.4, we have $\tau(L) = L$.

(b) Since $L : K$ is a normal extension, it is an algebraic extension. Thus for any $\alpha \in L$, $\alpha$ is algebraic over $K$ and hence is algebraic over $M$. So $L : M$ is an algebraic extension, and thus [by Proposition 4.9], $\overline{L}$ is an algebraic closure of $M$. With $\sigma = \tau_{|_M}$ (the restriction of $\tau$ to $M$), we have that $\sigma$ is a $K$-homomorphism taking $M$ into $\overline{M}$. Thus by (a), $\sigma(M) = M$, and hence $\tau(M) = M$.

3. Suppose that $L : K$ is a splitting field extension for $f$ where $f$ is a monic, separable, irreducible element of $K[t]$ with $\deg f$ prime. Suppose that $M$ is a field so that $K \subsetneq M \subsetneq L$ and $M : K$ is a normal extension. The goal is to show that $f$ is irreducible over $M$.

(a) For the sake of contradiction, suppose that $f = f_1 \cdots f_d$ where $d > 1$ and $f_1, \ldots, f_d$ are monic, irreducible elements of $M[t]$. Show that for each integer $k$ with $1 < k \le d$, we have $\deg f_k = \deg f_1$. (Suggestion: first use $Gal(L : K)$ to show that for $1 < k \le d$, $\deg f_1 = \deg f_k$; in doing this, you may want to use Problem 1.)

(b) Show that the hypothesis of (a) leads to a contradiction (and hence $f$ is irreducible over $M$). (Suggestion: first explain why $M$ contains no root of $f$.)

*Solutions:* [Without the above suggestions, this is essentially a problem from the 2016 exam.]

(a) As $L : K$ is a splitting field extension for $f$ and $f = f_1 \cdots f_d$, we know $f_1, \ldots, f_d$ each split over $L$. Fix $k$ with $1 < k \le d$ and take $\alpha, \beta \in L$ so that $\alpha$ is a root of $f_1$ and $\beta$ is a root of $f_k$. Since $f_1, f_k$ are monic and irreducible over $M$, we have $f_1 = m_\alpha(M)$ and $f_k = m_\beta(M)$. Also, both $\alpha$ and $\beta$ are roots of $f$, and thus by Corollary 3.7, there is some $\tau \in Gal(L : K)$ so that $\tau(\alpha) = \beta$. By Problem 1(b), we know that $\tau(M) = M$ and so $\tau(f_1) \in M[t]$. Also, $f_1$ is monic so $\tau(f_1)$ is monic; since $\tau_{|M}$ is an automorphism of $M$, Proposition 1.4 gives us that $\tau(f_1) = \tau_M(f_1)$ is irreducible over $M$. We have

$$0 = \tau(f_1(\alpha)) = \tau(f)(\tau(\alpha) = \tau(f)(\beta),$$

and hence $\tau(f_1) = m_\beta(M)$, meaning that $\tau(f_1) = f_k$. Thus $\deg f_k = \deg \tau(f_1) = \deg f_1$.

(b) Since $M : K$ is a normal extension, either $f$ has no root in $M$ or $f$ splits over $M$. If $f$ splits over $M$ then $M : K$ is a splitting field of $f$; but $L : K$ is a splitting field of $f$ with $K \subsetneq M \subsetneq L$. Thus $f$ cannot split over $M$, so $f$ has no root in $M$.

Suppose the hypothesis of (a) holds. Then $\deg f = \deg f_1 + \cdots + f_d$, and since $\deg f_1 = \deg f_k$ for each $k$ with $1 < k \le d$, we have $\deg f = d \cdot \deg f_1$. Also, since $f$ has no root in $M$, neither does $f_1$, so $\deg f_1 > 1$. [Recall that if $g \in M[t]$ is monic with degree 1, then $g = t - \gamma$ where $\gamma \in M$.] Hence $\deg f$ is the product of two integers greater than 1, contradicting the assumption that $\deg f$ is prime.

4. Suppose $K$ is a field, $S \subseteq K[t]$. Suppose that $L : K$ is a splitting field extension for $S$ with $K \subseteq L$, and that $M : K$ is a splitting field extension for $S$ relative to the embedding $\varphi : K \to M$. Assume $L \subseteq \overline{L}$, $M \subseteq \overline{M}$. Set

$$A = \{\alpha \in \overline{L} : \ f(\alpha) = 0 \text{ for some nonconstant } f \in S\ \},$$

and

$$B = \{\beta \in \overline{M} : \ \varphi(f)(\beta) = 0 \text{ for some nonconstant } f \in S\ \}.$$

(So $L = K(A)$ and $M = F(B)$ where $F = \varphi(K)$.)

(a) Explain why there is an isomorphism $\psi : \overline{L} \to \overline{M}$ that extends $\varphi$.

(b) Show that $\psi(A) = B$.

(c) Conclude that $\psi(K(A)) \simeq F(B)$ (and hence $L \simeq M$ since $K(A) = L$ and $F(B) = M$). [Note that the argument used in the proof of Theorem 5.4 shows that $[L : K] = [M : K]$.]

*Solutions:* [This is a proof of Theorem 5.5.]

(a) Since $\overline{L} : K$ is an algebraic extension, $\varphi : K \to M \subseteq \overline{M}$ can be extended to a homomorphism $\psi : \overline{L} :\to \overline{M}$. Since $\overline{L}$ is algebraically closed, so is $\psi(\overline{L})$. Since $\overline{M} : K$ is an algebraic extension, so is $\overline{M} : \overline{L}$ [with the homomorphism $\psi$]; hence $\overline{M} : \psi(\overline{L})$ is an algebraic extension. Since $\psi(\overline{L})$ is algebraically closed, the only algebraic extension of $\psi(\overline{L})$ is $\psi(\overline{L})$. Hence $\overline{M} = \psi(\overline{L})$. Thus $\psi$ is surjective. Since $\overline{L}$ is a field, $\psi$ is necessarily injective. Since $\psi$ is a homomorphism, this shows that $\psi$ is an isomorphism. [Note: $\overline{L} : K$ and $\overline{M} : K$ are both algebraic closures of $K$, so $\overline{L}$ and $\overline{M}$ are isomorphic via some isomorphism $\psi : \overline{L} \to \overline{M}$. But this does not show that $\psi$ extends $\varphi$.]

(b) Using that $\psi(\overline{L}) = \overline{M}$ and that $\psi$ is an isomorphism extending $\varphi$, we have that

$$\begin{aligned}
\psi(A) &= \{\psi(\alpha) \in \overline{M} : \ f(\alpha) = 0 \text{ for some nonzero } f \in S\ \} \\
&= \{\psi(\alpha) \in \overline{M} : \ \psi(f(\alpha)) = 0 \text{ for some nonzero } f \in S\ \} \\
&= \{\psi(\alpha) \in \overline{M} : \ \varphi(f)(\psi(\alpha)) = 0 \text{ for some nonzero } f \in S\ \} \\
&= \{\beta \in \overline{M} : \ \varphi(f)(\beta) = 0 \text{ for some nonzero } f \in S\ \} \\
&= B.
\end{aligned}$$

(c) We know that $\psi(K) = \varphi(K) = F$, and $\psi(A) = B$. We claim this means $\psi(K(A)) = F(B)$: An element $\gamma \in K(A)$ is of the form

$$\gamma = \sum_{k=1}^{m} c_k \alpha_k^{r_k}$$

where $c_k \in K$, $\alpha_k \in A$, $m, r_k \in \mathbb{Z}$ with $m \geq 1$. Thus

$$\psi(\gamma) = \sum_{k=1}^{m} \varphi(c_k) \beta_k^{r_k}$$

where $\beta_k = \psi(\alpha_k) \in \psi(A) = B$. Thus $\psi(\gamma) \in B$, so $\psi((A) \subseteq B$.

Since $\psi$ is an isomorphism, (b) shows that $\psi^{-1}(B) = A$, and an argument virtually identical to the above argument shows that $\psi^{-1}(F(B)) \subseteq K(A)$. Hence $\psi(K(A)) = F(B)$. Since $\psi$ is an injective homomorphism, we have $K(A) \simeq F(B)$.