GALOIS THEORY: SOLUTIONS TO HOMEWORK 7

1. Suppose that $\overline{K}$ is an algebraic closure of K, and assume that $K \subseteq \overline{K}$. Take $\alpha \in \overline{K}$ and suppose that $\sigma : K \to \overline{K}$ is a homomorphism.
   (a) Show that σ can be extended to a homomorphism $\tau : \overline{K} \to \overline{K}$.
   (b) Prove that the number of distinct roots of $m_\alpha(K)$ in $\overline{K}$ is equal to the number of distinct roots of $\sigma(m_\alpha(K))$ in $\overline{K}$.
   Solution: (a) Since $\overline{K}$ is an algebraic extension of K with $K \subseteq \overline{K}$, and $\sigma : K \to \overline{K}$ is a homomorphism, Theorem 4.6 shows that σ extends to a homomorphism $\tau : \overline{K} \to \overline{K}$.
   (b) In $\overline{K}[t]$, we have $m_\alpha(K) = \prod_{i=1}^{d}(t - \gamma_i)^{r_i}$, where $\gamma_1, \ldots, \gamma_d$ are distinct, and $r_1, \ldots, r_d \in \mathbb{N}$. By part (b) there is a homomorphism $\tau : \overline{K} \to \overline{K}$ extending σ. Recall that τ is necessarily injective. Then $\sigma(m_\alpha(K)) = \tau(m_\alpha(K)) = \prod_{i=1}^{d}(t - \tau(\gamma_i))^{r_i}$. Since τ is injective, one has that $\tau(\gamma_1), \ldots, \tau(\gamma_d)$ are distinct, and the conclusion follows.
2. Suppose that $L : K$ is an algebraic extension of fields.
   (a) Show that $\overline{L}$ is an algebraic closure of K, and hence $\overline{L} \simeq \overline{K}$.
   (b) Suppose that $K \subseteq L \subseteq \overline{L}$. Show that one may take $\overline{K} = \overline{L}$.
   Solution: (a) Consider $L : K$ as an extension relative to the embedding φ, and $\overline{L} : L$ as an extension relative to the embedding ψ. Then $\overline{L} : K$ is an extension of fields relative to the embedding $\psi \circ \varphi$, and since $\overline{L}$ is algebraically closed, then $\overline{L}$ is an algebraic closure of K. Thus Proposition 4.9 shows that, since $\overline{K}$ is also an algebraic closure of K, then $\overline{L} \simeq \overline{K}$.
   (b) Suppose that there is a smaller algebraic closure $\overline{K}$ of K than $\overline{L}$. We may suppose that $\overline{K}$ is an algebraic extension of K with $K \subseteq \overline{K}$. We have that $\overline{L}$ is an algebraic closure of K and $K \subseteq \overline{L}$. Take $\varphi : K \to \overline{L}$ to be the inclusion mapping. Theorem 4.6 shows that φ can be extended to a homomorphism from $\overline{K}$ into $\overline{L}$. Thus $\overline{L} : \overline{K}$ is a field extension with $[\overline{L} : \overline{K}] > 1$ (since $\overline{K}$ is smaller than $\overline{L}$). But this contradicts the fact that $\overline{K}$ is algebraically closed. Thus we may take $\overline{K} = \overline{L}$, as claimed.
3. For each of the following polynomials, construct a splitting field L over $\mathbb{Q}$ and compute the degree $[L : \mathbb{Q}]$.
   (a) $t^3 - 1$
   (b) $t^7 - 1$
   Solution: (a) One has $t^3 - 1 = (t-1)(t-\omega)(t-\omega^2)$, where $\omega = e^{2\pi i/3} = \frac{1}{2}(-1+\sqrt{-3})$. So $\mathbb{Q}(\omega) : \mathbb{Q}$ is a splitting field extension for $t^3 - 1$. We see that $(t^3-1)/(t-1) = t^2+t+1$ is monic, and it is easy to check that this polynomial has no linear factor and hence is irreducible. Hence $m_\omega(\mathbb{Q}) = t^2 + t + 1$, and $[\mathbb{Q}(\omega) : \mathbb{Q}] = 2$.
   (b) One has $t^7 - 1 = (t-1)(t-\zeta)(t-\zeta^2)\cdots(t-\zeta^6)$, where $\zeta = e^{2\pi i/7}$. So $\mathbb{Q}(\zeta) : \mathbb{Q}$ is a splitting field extension for $t^7 - 1$. We see that $(t^7 - 1)/(t-1) = t^6 + \ldots + t + 1$ is monic, and we have seen that $(t^p - 1)/(t-1)$ is irreducible over $\mathbb{Q}$ when p is prime. Hence $m_\zeta(\mathbb{Q}) = t^6 + \ldots + t + 1$, and $[\mathbb{Q}(\zeta) : \mathbb{Q}] = 6$.
4. For each of the following polynomials, construct a splitting field L over $\mathbb{Q}$ and compute the degree $[L : \mathbb{Q}]$.
   (a) $t^4 + t^2 - 6$
   (b) $t^8 - 16$

Solution: (a) We have $t^4+t^2-6=(t^2-2)(t^2+3)=(t+\sqrt{2})(t-\sqrt{2})(t+\sqrt{-3})(t-\sqrt{-3})$. Then with $L=\mathbb{Q}(\sqrt{2},\sqrt{-3})$, we have that $L:\mathbb{Q}$ is a splitting field extension for t^4+t^2-6. The polynomial t^2-2 has $\sqrt{2}$ as a root, and t^2-2 is irreducible by Eisenstein's criterion using the prime 2. Thus $m_{\sqrt{2}}(\mathbb{Q})=t^2-2$ and $[\mathbb{Q}(\sqrt{2}):\mathbb{Q}]=\deg m_{\sqrt{2}}(\mathbb{Q})=2$. Put $K=\mathbb{Q}(\sqrt{2})$, and note that $\sqrt{-3}$ is a root of the polynomial t^2+3. This polynomial is irreducible over $K[t]$, since $\sqrt{-3}$ is not real, and yet $K\subset\mathbb{R}$. Thus $m_{\sqrt{-3}}(K)=t^2+3$ and $[K(\sqrt{-3}):K]=\deg m_{\sqrt{-3}}(K)=2$. The tower law thus yields

$$[L:\mathbb{Q}]=[\mathbb{Q}(\sqrt{2},\sqrt{-3}):\mathbb{Q}(\sqrt{2})][\mathbb{Q}(\sqrt{2}):\mathbb{Q}]=2\cdot 2=4.$$

(b) We have $t^8-16=t^8-2^4=(t-\alpha)(t-\zeta\alpha)\cdots(t-\zeta^7\alpha)$, where $\alpha=\sqrt[8]{16}=\sqrt{2}\in\mathbb{R}_+$ and $\zeta=e^{2\pi i/8}$. Thus, with $L=\mathbb{Q}(\alpha,\zeta\alpha,\zeta^2\alpha,\ldots,\zeta^7\alpha)$, we see that $L:\mathbb{Q}$ is a splitting field extension for t^8-16. Note that $\zeta=(\zeta\alpha)/\alpha\in L$, and hence $\mathbb{Q}(\alpha,\zeta)\subseteq L$. Also, for $k\in\mathbb{N}$, one has $\zeta^k\alpha\in\mathbb{Q}(\alpha,\zeta)$, and so $L\subseteq\mathbb{Q}(\alpha,\zeta)$. We therefore conclude that $L=\mathbb{Q}(\alpha,\zeta)$. Next, noting that $m_\alpha(\mathbb{Q})=t^2-2$, we see that $[\mathbb{Q}(\alpha):\mathbb{Q}]=2$. Also, we have $\zeta=(1+i)/\alpha$, so $\alpha\zeta-1$ is a root of the polynomial t^2+1, whence ζ is a root of the polynomial $\alpha^2t^2-2\alpha t+2=2t^2-2\alpha t+2$. But $\zeta\notin\mathbb{R}$, and so this polynomial is irreducible over $\mathbb{Q}(\alpha)$. Thus $m_\zeta(\mathbb{Q}(\alpha))=t^2-\alpha t+1$, and $[\mathbb{Q}(\alpha,\zeta):\mathbb{Q}]=2$. It therefore follows from the tower law that $[L:\mathbb{Q}]=[\mathbb{Q}(\alpha,\zeta):\mathbb{Q}(\alpha)][\mathbb{Q}(\alpha):\mathbb{Q}]=4$.

5. Suppose that $L:K$ is a splitting field extension for the polynomial $f\in K[t]\setminus K$.
(a) Prove that $[L:K]\le(\deg f)!$.
(b) Prove that $[L:K]$ divides $(\deg f)!$.

Solution: (a) The conclusion in part (a) follows of course from that of part (b), but we nonetheless provide the slightly simpler argument available in this case. We use induction on $n=\deg(f)$. In the base case $n=1$, we have $[L:K]=1$, so the conclusion holds. Suppose now that $n>1$ and that the desired conclusion holds for all polynomials of degree smaller than n. Let $\alpha\in L$ be any root of f. Then f factors as $(t-\alpha)g$ for some polynomial $g\in K(\alpha)[t]$ of degree $n-1$. Moreover, we have that L is a splitting field for g over $K(\alpha)$. By induction, we therefore see that $[L:K(\alpha)]\le(n-1)!$. Since $[K(\alpha):K]=n$, the Tower Law shows that $[L:K]\le n\cdot(n-1)!=n$. This confirms the inductive step, and the desired conclusion follows.

(b) In the second case we again proceed by induction on $n=\deg(f)$, and again the case $n=1$ is immediate. Now, when $n>1$, we split the argument according to whether f is reducible or not over K. If f is irreducible, let $\alpha\in L$ be any root of f. Then f again factors as $(t-\alpha)g$ for some other polynomial $g\in K(\alpha)[t]$ of degree $n-1$. Moreover, we have that L is a splitting field for g over $K(\alpha)$. By induction, we therefore see that $[L:K(\alpha)]$ divides $(n-1)!$. Since $[K(\alpha):K]=n$, the Tower Law shows that $[L:K]$ divides $n\cdot(n-1)!=n!$.

On the other hand, if $f=gh$ is reducible, let M be the subfield of L generated by K and the roots of g. Then M is a splitting field for g over K and L is a splitting field for h over M. By induction, we have that $[M:K]$ divides $r!$ and $[L:M]$ divides $(n-r)!$, where $r=\deg(g)$. Hence $[L:K]=[L:M][M:K]$ divides $r!(n-r)!$, which in turn divides $n!$ (with quotient equal to the binomial coefficient $\binom{n}{r}$).

We confirm the inductive step in both cases, and the desired conclusion follows by induction.