GALOIS THEORY 2019: HW 5

For assessment: Problems 1, 2, 3

Due by noon Tuesday, week 11 of the term

1. ?? LYNNE: there is a problem here, as in the proof of 11.1(b), it states that as an exercise one shows this. So this should be part of the proof of 11.1(b).

   (This is part of the proof of Theorem 11.1(c) – TYPO: this should have said this is part of the proof of Theorem 11.1(b) and (c).) Suppose that $L : K_0$ is a finite Galois extension with $G = Gal(L : K_0)$ and $H \lhd G$. We let ϕ, γ be the maps as defined in section 11 of the notes. Here you show that for any $\sigma \in G$, $\phi(H) = \sigma\phi(H)$ (which by Theorem 11.1(b) is equivalent to showing that for any $\sigma \in G$, $H = \gamma\sigma\phi(H)$).
   (a) Take $\sigma \in G$. Show that $\sigma\phi(H) \subseteq \phi(H)$.
   (b) Show that for $\sigma \in G$, we have $\sigma\phi(H) = \phi(H)$.

2. Let f denote the polynomial $t^3 - 7 \in \mathbb{Q}[t]$.
   (a) Find a splitting field extension $L : \mathbb{Q}$ for f.
   (b) Construct $Gal(L : \mathbb{Q})$; show that $Gal(L : \mathbb{Q}) \simeq S_3$ (where S_3 denotes the symmetric group on 3 letters).
   (c) Find all subgroups H of $Gal(L : \mathbb{Q})$, and for each subgroup H, use the Fundamental Theorem of Galois Theory (Theorem 11.1) to find $Fix_L(H)$, clearly explaining your reasoning. (It may be helpful to draw the lattice of subfields and corresponding lattice of subgroups of S_3.)

3. (Here you prove Theorem 12.2.) Let p be a prime and $q = p^n$ where $n \in \mathbb{Z}_+$. Let $\mathbb{F}_p$ denote a field of order p, and let $\mathbb{F}_q$ denote a field of order q; recall that by Theorem 12.1, $\mathbb{F}_q : \mathbb{F}_p$ is a splitting field extension with $[\mathbb{F}_q : \mathbb{F}_p] = n$. Assume that $\mathbb{F}_p \subseteq \mathbb{F}_q$.
   (a) Briefly explain why $\mathbb{F}_q : \mathbb{F}_p$ is a Galois extension.
   (b) Let ϕ denote the Frobenius map on $\mathbb{F}_q$. Show that $\langle\phi\rangle = Gal(\mathbb{F}_q : \mathbb{F}_p)$, and use this to show that $Gal(\mathbb{F}_q : \mathbb{F}_p) \simeq \mathbb{Z}/n\mathbb{Z}$.

4. (This is a continuation of a problem on HW 3.) Let $g(X) = X^4 - 5 \in \mathbb{Q}[t]$. Let $\alpha = \sqrt[4]{5} \in \mathbb{R}_+$, and let $\zeta = e^{2\pi i/4} = i$; then $L = \mathbb{Q}(\alpha, i)$ is a splitting field for g over $\mathbb{Q}$. We have seen that $[L : \mathbb{Q}] = 8$ and $Gal(L : \mathbb{Q})$ is generated by the $\mathbb{Q}$-homomorphisms σ and τ where $\sigma(\alpha) = i\alpha$, $\sigma(i) = i$, $\tau(\alpha) = \alpha$, $\tau(i) = -i$, and $\sigma\tau = \tau\sigma^3$. Find all subgroups H of $Gal(L : \mathbb{Q})$, and for each subgroup H, use the Fundamental Theorem of Galois Theory (Theorem 11.1) to find $Fix_L(H)$, clearly explaining your reasoning. (It may be helpful to draw the lattice of subfields and corresponding lattice of subgroups of $Gal(L : \mathbb{Q}$.)

5. (This is a continuation of a problem on HW 3.) Let $f = (X^2 - 2)(X^2 + 7)$. We have seen that with $L = \mathbb{Q}(\sqrt{2}, \sqrt{-7}) \subseteq \mathbb{C}$, $L : \mathbb{Q}$ is a splitting field extension for f with $[L : \mathbb{Q}] = 4$. We have also

seen that $Gal(L:\mathbb{Q})$ is generated by the $\mathbb{Q}$-homomorphisms σ and τ where $\sigma(\sqrt{2}) = -\sqrt{2}$, $\sigma(\sqrt{-7}) = \sqrt{-7}$, $\tau(\sqrt{2}) = \sqrt{2}$, $\tau(\sqrt{-7}) = -\sqrt{-7}$, and $\sigma\tau = \tau\sigma$. Find all subgroups H of $Gal(L:\mathbb{Q})$, and for each subgroup H, use the Fundamental Theorem of Galois Theory (Theorem 11.1) to find $Fix_L(H)$, clearly explaining your reasoning. (It may be helpful to draw the lattice of subfields and corresponding lattice of subgroups of $Gal(L:\mathbb{Q}$.)

6. Let p be a prime number, and let $\mathbb{F}_p$ be the finite field with p elements. Put $f(t) = t^p - t + 1$, and let $K = \mathbb{F}_p(\alpha)$, where α is a root of f.
   (a) Show that for all $\xi \in \mathbb{F}_p$, the element $\alpha + \xi$ is a root of f.
   (b) Let σ be the Frobenius map on K. Show that for $1 \leq d < p$, one has that $\sigma^d(\alpha)$ is a root of f.
   (c) Show that f is irreducible over $\mathbb{F}_p$.

7. Let L be a field, G a subgroup of $Aut(L)$, and $K = Fix_L(G)$. Suppose that each G-orbit in L is finite; thus by Theorem 10.2, we know that $L:K$ is a Galois extension.
   (a) Briefly explain why G is a subset of $Gal(L:K)$.
   (b) Take $\alpha \in L$, and let $\alpha, \alpha_2, \ldots, \alpha_r$ be the distinct elements in the G-orbit of α. With

   $$f_\alpha = (t-\alpha)(t-\alpha_2)\cdots(t-\alpha_r),$$

   we have seen in the proof of Theorem 10.2 that $f_\alpha \in K[t]$. Set $g = m_\alpha(K)$; show that $f_\alpha = g$.