## GALOIS THEORY 2019: HW 1 SOLUTIONS

Here your are to remember that with $K \subseteq L$ fields and $\alpha \in L$, $\alpha$ is algebraic over $K$ if and only if $[K(\alpha) : K] < \infty$.

1. Let $F = \mathbb{Z}/p\mathbb{Z}$ where $p$ is prime. Recall that for $a \in F$, $a^p = a$.
   (a) For $n \in \mathbb{Z}_+$, use induction on $n$ to show that for $f = a_0 + a_1 t + a_2 t^2 + \cdots + a_n t^n \in F[t]$, we have
   $$f^p = a_0 + a_1 t^p + a_2 t^{2p} + \cdots + a_n t^{np}.$$
   *Solution:* First consider $n = 1$. Then
   $$f^p = (a_0 + a_1 t)^p = \sum_{k=0}^{p} \binom{p}{k} a_0^k a_1^{p-k} t^{p-k} = a_0^p + a_1^p t^p$$
   since $p$ divides $\binom{p}{k}$ for $0 < k < p$. Also, $a_i^p = a_i$ since $a_i \in F$, so $f^p = a_0 + a_1 t^p$.
   Now suppose that $n > 1$ and for $g \in F[t]$ with $g = b_0 + b_1 t + \cdots + b_{n-1} t^{n-1}$, we have $g^p = b_0 + b_1 t^p + \cdots + a_{n-1} t^{(n-1)p}$. With $f = a_0 + a_1 t + a_2 t^2 + \cdots + a_n t^n \in F[t]$, take $g = a_0 + a_1 t + a_2 t^2 + \cdots + a_{n-1} t^{n-1} \in F[t]$. Thus
   $$f^p = (g + a_n t^n)^p = \sum_{k=0}^{p} \binom{p}{k} g^k a_n^{p-k} t^{n(p-k)} = g^p + a_n^p t^{np}$$
   since $\binom{p}{k} = 0$ if $F$ for $0 < k < p$. Since $a_n \in F$ we have $a_n^p = a_n$, and so by the induction hypothesis,
   $$f^p = a_0 + a_1 t^p + a_2 t^{2p} + \cdots + a_n t^{np}.$$
   (b) Suppose that $E : F$ is a field extension with $F \subseteq E$, $[E : F] < \infty$, and $\alpha \in E \setminus F$.
      (i) Briefly explain why $\alpha$ is algebraic over $F$.
      (ii) Let $f = \mathrm{m}_\alpha(F)$, the minimal polynomial of $\alpha$ over $F$. Show that $\alpha^p$ is a root of $f$.
      (iii) Suppose that $|E| = p^m$. Show that every element of $E$ is a root of $t^{p^m} - t$. (Suggestion: use that $E^\times$ is a field under multiplication. Also recall that $E^\times = E \setminus \{0\}$.)

      *Solutions:* [(ii) is part of a problem on the 2018 exam.]
      (i) Since $[E : F] < \infty$ and by the Tower Law, $[E : F] = [E : F(\alpha)][F(\alpha) : F]$, we have $[F(\alpha) : F] = n < \infty$. Thus $\alpha$ is algebraic over $F$.
      (ii) Write $f = b_0 + b_1 t + \cdots + b_d t^d$ (where $b_i \in F$ and $b_d = 1$). By (a) and the fact that $f(\alpha) = 0$, we have
      $$0 = (f(\alpha))^p = b_0 + b_1 \alpha^p + \cdots + b_d \alpha^{dp} = f(\alpha^p).$$
      Hence $\alpha^p$ is a root of $f$.
      (iii) As $E^\times$ is a group (under multiplication) with $|E^\times| = p^m - 1$, we know that the order of every element of $E^\times$ divides $p^m - 1$. Hence for any $\alpha \in E^\times$, we have $\alpha^{p^m - 1} = 1$, and so for every $\alpha \in E$ with $\alpha \neq 0$, we have $\alpha^{p^m} - \alpha = 0$.

Since we also have $0^{p^m} - 0 = 0$, every element of $E$ is a root of $t^{p^m} - t$.

2. Suppose that $L : K$ is a field extension with $K \subseteq L$. Suppose that $\alpha, \beta \in L$ are algebraic over $K$. Show that $\alpha + \beta$ is algebraic over $K$.

   *Solution:* [This is from the 2018 exam.]

   Since $\alpha$ and $\beta$ are algebraic over $K$, there are $f, g \in K[t] \setminus \{0\}$ so that $f(\alpha) = 0 = g(\beta)$. Hence $[K(\alpha) : K] < \infty$. Since $g \in K(\alpha)[t]$, we have that $\beta$ is algebraic over $K(\alpha)$, and so $[K(\alpha, \beta) : K(\alpha)] < \infty$. We know that $\alpha + \beta \in K(\alpha, \beta)$, and by the Tower Law,

$$\begin{aligned}&[K(\alpha,\beta) : K(\alpha+\beta)][K(\alpha+\beta) : K]\\&\quad = [K(\alpha,\beta) : K(\alpha)][K(\alpha) : K] < \infty,\end{aligned}$$

   so $[K(\alpha + \beta) : K] < \infty$. Hence $\alpha + \beta$ is algebraic over $K$.

3. Let $L : K$ be a field extension, and suppose that $\gamma \in L$ satisfies the property that $\deg m_\gamma(K) = 7$. Suppose that $h \in K[t]$ is a non-zero cubic polynomial. By noting that $\gamma$ is a root of the cubic polynomial $g(t) = h(t) - h(\gamma) \in K(h(\gamma))[t]$, show that $[K(h(\gamma)) : K] = 7$.

   *Solution:* [This is a problem on the 2015 exam.]

   We know $h(\gamma) \in K(\gamma)$ and

$$7 = [K(\gamma) : K] = [K(\gamma) : K(h(\gamma))][K(h(\gamma)) : K].$$

   Therefore $[K(h(\gamma)) : K]$ divides 7, and hence this degree is either 1 or 7. For the sake of contradiction, suppose $[K(h(\gamma)) : K] = 1$. This means that $h(\gamma) \in K$, and so $g \in K[t]$. As $h(\gamma)$ is a root of $g$, we must have $g$ in the ideal of $K[t]$ generated by $\mathrm{m}_\gamma(K)$, and hence $\mathrm{m}_\gamma(K)$ divides $g$. As the degree of $g$ is 3, this means that $\deg \mathrm{m}_\gamma(K) \leq 3$, contradicting the fact that

$$7 = \deg \mathrm{m}_\gamma(K) = [K(\gamma) : K].$$

   Thus we cannot have $[K(h(\gamma)) : K] = 1$, so we must have $[K(h(\gamma)) : K] = 7$.

4. Let $L : K$ be a field extension with $K \subseteq L$. Let $A \subseteq L$, and let

$$\mathcal{C} = \{C \subseteq A : C \text{ is a finite set}\}.$$

   Show that $K(A) = \cup_{C \in \mathcal{C}} K(C)$, and further that when $[K(C) : K] < \infty$ for all $C \in \mathcal{C}$, then $K(A) : K$ is an algebraic extension.

   *Solution:* The field $K(A)$ is the smallest subfield of $L$ containing $K$ and $A$. Thus, for all $C \in \mathcal{C}$, the field $K(A)$ must contain $K(C)$. So $\cup_{C \in \mathcal{C}} K(C) \subseteq K(A)$.

   Now take $\gamma \in K(A)$. Then $\gamma$ is a quotient of finite $K$-linear combinations of powers of elements of $A$. Since this $K$-linear combination is finite, there is a finite set $D \subseteq A$ so that $\gamma$ is a quotient of $K$-linear combinations of powers of elements in $D$. We therefore have $D \in \mathcal{C}$ and $\gamma \in K(D)$. Thus $K(A) \subseteq \cup_{C \in \mathcal{C}} K(C)$.

Now suppose that $[K(C) : K] < \infty$ for each $C \in \mathcal{C}$, and take $\alpha \in K(A)$. Thus $\alpha \in K(D)$ for some $D \in \mathcal{C}$, and

$$[K(D) : K(\alpha)][K(\alpha) : K] = [K(C) : K] < \infty,$$

so $[K(\alpha) : K] < \infty$. This means that $\alpha$ is algebraic over $K$, and this argument holds for every $\alpha \in K(A)$. Hence $K(A) : K$ is an algebraic extension.