GALOIS THEORY: SOLUTIONS TO HOMEWORK 2

1. Let $L : K$ be a field extension, and suppose that $\theta \in L$ satisfies the property that $[K(\theta) : K] = p$, where p is a prime number. Let

$$\alpha = c_0 + c_1\theta + \ldots + c_{p-1}\theta^{p-1},$$

for some $c_0, \ldots, c_{p-1} \in K$, and suppose that $\alpha \notin K$. By considering $[K(\alpha) : K]$, show that $K(\alpha) = K(\theta)$.
Solution: We have $K(\alpha) \subseteq K(\theta)$, so the tower law yields

$$[K(\theta) : K(\alpha)][K(\alpha) : K] = [K(\theta) : K],$$

whence $[K(\alpha) : K]$ divides $[K(\theta) : K] = p$. Since p is a prime, we therefore see that $[K(\alpha) : K] \in \{1, p\}$. But $\alpha \notin K$, by hypothesis, so $[K(\alpha) : K] \neq 1$. Then we conclude that $[K(\alpha) : K] = p$. By the tower law again, it follows that

$$[K(\theta) : K(\alpha)] = [K(\theta) : K]/[K(\alpha) : K] = 1,$$

and thus $K(\theta) = K(\alpha)$.

2. 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 γ 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 γ 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 $K(A) \subseteq \cup_{C\in\mathcal{C}} K(C)$.

We now address the final claim. Take $\alpha \in K(A)$. Then $\alpha \in K(C)$ for some $C \in \mathcal{C}$. Thus we deduce via the tower law that $[K(C) : K(\alpha)][K(\alpha) : K] = [K(C) : K] < \infty$, whence $[K(\alpha) : K] < \infty$. We therefore conclude that α is algebraic over K. Since this holds for all $\alpha \in K(A)$, we have that $K(A) : K$ is an algebraic extension.

3. Let $L : K$ be a field extension, and suppose that $\gamma \in L$ satisfies the property that $\deg m_\gamma(K) = 5$. Suppose that $h \in K[t]$ is a non-zero cubic polynomial. By noting that γ is a root of the cubic polynomial $g(t) = h(t) - h(\gamma) \in K(h(\gamma))[t]$, show that $[K(h(\gamma)) : K] = 5$.
Solution: One has $K \subseteq K(h(\gamma)) \subseteq K(\gamma) \subseteq L$. Then by the tower law, we find that $[K(\gamma) : K] = [K(\gamma) : K(h(\gamma))][K(h(\gamma)) : K]$, whence $[K(\gamma) : K(h(\gamma))]$ divides $[K(\gamma) : K]$. But the degree of the minimal polynomial of γ over K is 5, so that $[K(\gamma) : K] = 5$. We therefore see that $[K(\gamma) : K(h(\gamma))] \in \{1, 5\}$. But over the field $K(h(\gamma))$, the element γ satisifies the cubic equation $h(t) - h(\gamma) = 0$, and thus the minimal polynomial of γ over $K(h(\gamma))$ divides the latter cubic polynomial, so has degree 1, 2 or 3. Consequently, we must have $[K(\gamma) : K(h(\gamma))] \in \{1, 2, 3\}$. In view of our earlier observation, we are forced to conclude that the latter degree is 1, and then the previous application of the tower law implies that $[K(h(\gamma)) : K] = 5$, which is to say that the minimal polynomial of $h(\gamma)$ over K has degree 5.

4. Calculate the minimal polynomial of $\sqrt[5]{7+\sqrt[3]{21}}$ over $\mathbb{Q}$, and hence determine the degree of the field extension $\mathbb{Q}(\sqrt[5]{7+\sqrt[3]{21}}) : \mathbb{Q}$.

   Solution: Write $\alpha = \sqrt[5]{7+\sqrt[3]{21}}$. Then $\alpha^5 - 7 = \sqrt[3]{21}$, and hence $(\alpha^5-7)^3 = 21$. On putting $f(x) = (x^5-7)^3 - 21 = x^{15} - \ldots - (7^3+21)$, we see that $f(\alpha) = 0$, and thus it follows that the minimal polynomial $m_\alpha(\mathbb{Q})$ of α divides f. But by applying Eisenstein's criterion using the prime 7, we see that f is irreducible: the lead coefficient of f is not divisible by 7, all other coefficients are divisible by 7, and the constant coefficient $-(7^3+21)$ is divisible by 7 but not by 7^2. Hence f is the minimal polynomial of α over $\mathbb{Q}$. The degree of the field extension $\mathbb{Q}(\sqrt[5]{7+\sqrt[3]{21}}) : \mathbb{Q}$ is therefore equal to $\deg f = 15$.

5. Let $\mathbb{Q}(\alpha) : \mathbb{Q}$ be a simple field extension with the property that the minimal polynomial of α is t^3+2t-2. Calculate the minimal polynomials of $\alpha - 1$ and α^2+1 over $\mathbb{Q}$, and express the multiplicative inverses of these elements in $\mathbb{Q}(\alpha)$ in the form $c_0 + c_1\alpha + c_2\alpha^2$ for suitable rational numbers c_0, c_1, c_2.

   Solution: Write $\beta = \alpha - 1$. Then $\alpha = \beta + 1$, so that on substituting into the relation $\alpha^3 + 2\alpha - 2 = 0$ implied by the minimal polynomial of α, we obtain

$$0 = (\beta+1)^3 + 2(\beta+1) - 2 = \beta^3 + 3\beta^2 + 5\beta + 1.$$

   Then the minimal polynomial of β divides $f(t) = t^3 + 3t^2 + 5t + 1$. Since the latter polynomial is cubic, if it is not irreducible it has a linear factor, and by Gauss' Lemma that factor may be written with integral coefficients. But since (consider the leading and final coefficients) $t \pm 1$ are the only possible such factors, and $f(\pm 1) \neq 0$, we must conclude that no such factor exists, and hence $f(t)$ is irreducible. Then $\alpha - 1$ has minimal polynomial $t^3 + 3t^2 + 5t + 1$.

   Next consider $(\alpha-1)^{-1}$. One has $(\alpha-1)^3 + 3(\alpha-1)^2 + 5(\alpha-1) + 1 = 0$, and hence $(\alpha-1)^{-1} = -(\alpha-1)^2 - 3(\alpha-1) - 5 = -\alpha^2 - \alpha - 3$.

   Next write $\gamma = \alpha^2 + 1$. We aim to seek a polynomial relation satisfied by γ in stages. Observe first that since $\alpha^3 + 2\alpha - 2 = 0$, one has

$$\gamma^2 = (\alpha^2+1)^2 = \alpha^4 + 2\alpha^2 + 1 = \alpha(\alpha^3 + 2\alpha - 2) + 2\alpha + 1 = 2\alpha + 1,$$

   and hence

$$\gamma^3 = \gamma(2\alpha+1) = (\alpha^2+1)(2\alpha+1) = 2(\alpha^3 + 2\alpha - 2) + \alpha^2 - 2\alpha + 5 = \gamma - 2\alpha + 4.$$

   Then $\gamma^3 + \gamma^2 = \gamma + 5$, whence the minimal polynomial of γ divides $g(t) = t^3 + t^2 - t - 5$. Since the latter polynomial is cubic, if it is not irreducible it has a linear factor, and by Gauss' Lemma that factor may be written with integral coefficients. But since (consider the leading and final coefficients) $t \pm 1$ and $t \pm 5$ are the only possible such factors, and $f(\pm 1) \neq 0$ and $f(\pm 5) \neq 0$, we must conclude that no such factor exists, and hence $g(t)$ is irreducible. Then $\alpha^2 + 1$ has minimal polynomial $t^3 + t^2 - t - 5$.

   Next consider $(\alpha^2+1)^{-1}$. One has

$$5(\alpha^2+1)^{-1} = \gamma^2 + \gamma - 1 = (2\alpha+1) + (\alpha^2+1) - 1 = \alpha^2 + 2\alpha + 1,$$

   and hence $(\alpha^2+1)^{-1} = \frac{1}{5}(\alpha^2 + 2\alpha + 1)$.