PURDUE UNIVERSITY

Department of Mathematics

# GALOIS THEORY – SOLUTIONS

MA 45401-H01

28th March 2024   75 minutes

*This paper contains* **SIX** *questions.*
*All SIX answers will be used for assessment.*
*Calculators, textbooks, notes and cribsheets are* **not** *permitted in this examination.*

*Do not turn over until instructed.*

1. [3+3+3+3+3+3=18 points] Decide which of the following statements are necessarily true, and which may be false. Mark those which are true with "T", and those which may be false with "F".

**a.** Let $f \in \mathbb{Z}[t]$ be a polynomial, every root of which has multiplicity 2024. Then $f$ is not separable over $\mathbb{Q}$.

**Solution: False** – consider, for example, the polynomial $(t-1)^{2024}$, each irreducible factor of which is linear and hence separable over $\mathbb{Q}$.

**b.** If $L : K$ is an algebraic extension of fields with $K \subseteq L$, then the algebraic closure $\overline{L}$ of $L$ is isomorphic to the algebraic closure $\overline{K}$ of $K$.

**Solution: True** – we have that $\overline{K}$ and $\overline{L}$ are both algebraic closures of $K$, and so Proposition 4.9 shows that $\overline{L}$ is isomorphic to $\overline{K}$.

**c.** Every algebraic extension of $\mathbb{Q}$ is separable.

**Solution: True** – this is a result from class (and holds more generally for every field $K$ of characteristic 0).

**d.** Suppose that $K$ and $L$ are fields with $K \subseteq L$, and $L$ is algebraically closed. Then the field extension $L : K$ is normal.

**Solution: False** – consider, for example $\mathbb{Q} \subseteq \mathbb{C}$. The extension $\mathbb{C} : \mathbb{Q}$ is not normal, because this extension is not algebraic.

**e.** Suppose that $L : M$ and $M : K$ are field extensions with $L : K$ normal. Then $L : M$ is a normal field extension.

**Solution: True** – this is a result from class (Proposition 6.3).

**f.** Let $f \in \mathbb{Z}[x]$ be a polynomial having prime degree $p$, and let $\theta$ be any root of $f$ in a splitting field extension for $f$ over $\mathbb{Q}$. Then $[\mathbb{Q}(\theta) : \mathbb{Q}] = p$.

**Solution: False** – consider $f(x) = x^p$, so that $\theta = 0$ and $[\mathbb{Q}(\theta) : \mathbb{Q}] = [\mathbb{Q} : \mathbb{Q}] = 1$.

2. [3+3+3+3=12 points]

(a) Define what it means for a field extension $L : K$ to be a splitting field extension.

**Solution:** Suppose that $M : K$ is a field extension relative to the embedding $\varphi : K \to M$, and $S \subseteq K[t] \setminus K$ has the property that every $f \in S$ splits over $M$. Let $L$ be a field with $\varphi(K) \subseteq L \subseteq M$. Then $L : K$ *is a splitting field extension for* $S$ if $L$ is the smallest subfield of $M$ containing $\varphi(K)$ over which every polynomial $f \in S$ splits. [Full credit if you assumed that $K \subseteq M$, and worked with a single polynomial instead of a set.]

(b) Define what it means for a field extension $L : K$ to be normal.

**Solution:** The extension $L : K$ is *normal* if it is algebraic, and every irreducible polynomial $f \in K[t]$ either splits over $L$ or has no root in $L$.

(c) Let $L : K$ be a field extension. Define what it means for an element $\alpha \in L$ to be separable over $K$.

**Solution:** An element $\alpha \in L$ is *separable* over $K$ when $\alpha$ is algebraic over $K$ and its minimal polynomial $m_\alpha(K)$ is separable (meaning that it has no multiple roots in $\overline{K}$).

*Continued...*

(d) Define what it means for a field extension $L : K$ to be separable.

**Solution:** An algebraic extension $L : K$ is *separable* if every $\alpha \in L$ is separable over $K$.

3. [8+8+8=24 points] This question concerns the polynomial $f(t) = t^4 - (t+1)^2 \in \mathbb{Q}[t]$.

(a) Find a splitting field extension $L : \mathbb{Q}$ for $f$, justifying your answer.

**Solution:** Working over $\overline{\mathbb{Q}}$, one finds that $f(t) = t^4 - (t+1)^2 = (t^2 - t - 1)(t^2 + t + 1)$, and hence $f(t) = (t - \frac{1}{2}(1+\sqrt{5}))(t - \frac{1}{2}(1-\sqrt{5}))(t + \frac{1}{2}(1+\sqrt{-3})(t + \frac{1}{2}(1-\sqrt{-3}))$. Thus, on taking $L = \mathbb{Q}(\sqrt{-3}, \sqrt{5})$, we find that $L : \mathbb{Q}$ is a splitting field extension for $f$.

(b) Determine the degree of your splitting field extension $L : \mathbb{Q}$, justifying your answer.

**Solution:** We have $[\mathbb{Q}(\sqrt{5}) : \mathbb{Q}] = 2$, since the minimal polynomial for $\sqrt{5}$ over $\mathbb{Q}$ is $t^2 - 5$. The minimal polynomial for $\sqrt{-3}$ over $\mathbb{Q}(\sqrt{5})$ divides $t^2 + 3$. Since $\sqrt{-3} \notin \mathbb{R}$ and $\mathbb{Q}(\sqrt{5}) \subset \mathbb{R}$, one sees that $t^2 + 3$ has no root in $\mathbb{Q}(\sqrt{5})$, and hence is irreducible over $\mathbb{Q}(\sqrt{5})$. Thus $[L : \mathbb{Q}(\sqrt{5})] = 2$, and so $[L : \mathbb{Q}] = [L : \mathbb{Q}(\sqrt{5})][\mathbb{Q}(\sqrt{5}) : \mathbb{Q}] = 4$, by the tower law.

(c) Determine the subgroup of $S_4$ to which $\mathrm{Gal}(L : \mathbb{Q})$ is isomorphic.

**Solution:** The group $G = \mathrm{Gal}(L : \mathbb{Q})$ can be identified by extension of $\mathbb{Q}$-homorphisms, first the inclusion map $\mathbb{Q} \to L$ to a $\mathbb{Q}$-homomorphism $\mathbb{Q}(\sqrt{5}) \to L$, and then to a $\mathbb{Q}$-homomorphism $L = \mathbb{Q}(\sqrt{5}, \sqrt{-3}) \to L$. The first extension is defined by an action permuting the roots $\sqrt{5}$ and $-\sqrt{5}$ of the irreducible polynomial $t^2 - 5$ defining the extension $\mathbb{Q}(\sqrt{5}) : \mathbb{Q}$. The second is defined by an action permuting the roots $\sqrt{-3}$ and $-\sqrt{-3}$ of the irreducible polynomial $t^2 + 3$ defining the extension $L : \mathbb{Q}(\sqrt{5})$. Thus we see that $G$ is generated by permutations $\sigma$, $\tau$ and $\sigma\tau = \tau\sigma$ on the roots $\pm\sqrt{5}$ and $\pm\sqrt{-3}$ of the polynomial $f$, where these maps fix $\mathbb{Q}$ pointwise, and $\sigma = (\sqrt{5}, -\sqrt{5})$ and $\tau = (\sqrt{-3}, -\sqrt{-3})$. Thus $\sigma\tau = \tau\sigma = (\sqrt{5}, -\sqrt{5})(\sqrt{-3}, -\sqrt{-3})$, and $G \cong \{\mathrm{id}, (1\ 2), (3\ 4), (1\ 2)(3\ 4)\} \leq S_4$.

4. [14 points] Suppose that $L : K$ is a splitting field extension for the polynomial $f \in K[t] \setminus K$. Prove that $[L : K]$ divides $(\deg f)!$.

**Solution:** We proceed by induction on $n = \deg(f)$, noting that 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 $f$ 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 have confirmed the inductive step in both cases, and the desired conclusion follows.

5. [7+7=14 points] (a) Suppose that $M$ is an algebraically closed field. Show that all polynomials in $M[t]$ are separable.

*Continued...*

**Solution:** Suppose that $f \in M[t]$ is irreducible and $\deg(f) > 1$. Then $f$ is non-zero and non-constant and has a root $\alpha \in M$. Define $g \in M[t]$ by means of the relation $f = (t - \alpha)g$. Then $g$ has degree $\deg(f) - 1 \geq 1$, and thus $f$ is not irreducible over $M[t]$, leading to a contradiction. Thus, every irreducible polynomial in $M[t]$ has degree 1. Such a polynomial cannot have multiple roots, and so must be separable. Every polynomial in $K[X]$ is therefore a product of separable polynomials, and must consequently itself be separable.

(b) Suppose that $p$ is a prime number and $t$ is an indeterminate, and let $L = \overline{\mathbb{F}}_p(t)$, where $\overline{\mathbb{F}}_p$ denotes the algebraic closure of $\mathbb{F}_p$. Are all polynomials in $L[X]$ separable? Justify your answer.

**Solution:** No, not all polynomials in $L[X]$ separable. Consider, for example, the polynomial $f = X^p - t \in L[X]$, and let $\alpha \in \overline{L}$ be a root of $f$. Thus, we have $\alpha^p = t$. We show first that $f$ is irreducible over $L$. Since $t$ is irreducible in $\overline{\mathbb{F}}_p[t]$, it follows from Eisenstein's criterion via Gauss's Lemma that $f$ is irreducible over $\overline{\mathbb{F}}_p(t) = L$. Finally, to see that $f$ is not separable over $L$, we use the fact that $\mathrm{char}(K) = p$ and $p$ divides the binomial coefficients $\binom{p}{k}$ for $1 \leq k < p$. Hence $(X - \alpha)^p = X^p - t$. Thus $\alpha$ is the only root of $f$, even though $f$ is irreducible over $L$ with $\deg f = p > 1$, and so $f$ is not separable.

6. [8+8=16 points] Throughout, let $f$ denote the polynomial $t^5 - 9t - 3 \in \mathbb{Q}[t]$, let $L$ be a splitting field for $f$ over $\mathbb{Q}$, and let $M$ be a field with $\mathbb{Q} \subsetneq M \subsetneq L$ (that is, a field strictly intermediate between $\mathbb{Q}$ and $L$).

(a) Show that, for any $\sigma \in \mathrm{Gal}(L : \mathbb{Q})$, and for any $\alpha \in M$, the polynomial $\sigma(m_\alpha(\mathbb{Q}))$ is monic and irreducible over $\mathbb{Q}$. Here $m_\alpha(\mathbb{Q})$ denotes the minimal polynomial of $\alpha$ over $\mathbb{Q}$.

**Solution:** Suppose that $\alpha \in M$. Then $m_\alpha(\mathbb{Q})$ is monic and irreducible over $\mathbb{Q}$. Since $\sigma$ is a homomorphism, we know that $\sigma(1) = 1$. Thus $\sigma(m_\alpha(\mathbb{Q}))$ is monic. Also, if $\sigma(m_\alpha(\mathbb{Q}))$ has a proper factorisation $g_1 g_2$, say, then $\sigma^{-1}(g_1) \cdot \sigma^{-1}(g_2)$ gives a factorisation of $m_\alpha(\mathbb{Q})$ over $\mathbb{Q}$, contradicting the irreducibility of $m_\alpha(\mathbb{Q})$. Thus $\sigma(m_\alpha(\mathbb{Q}))$ is indeed irreducible.

(b) Suppose that $M : \mathbb{Q}$ is normal and that $f$ factors as a product of monic irreducibles $f_1, \ldots, f_r$ (of positive degree) over $M[t]$. Show that $\deg(f_i) = \deg(f_1)$ for each $i$.

**Solution:** Let $\alpha \in L$ be a root of $f_1$ and $\beta \in L$ be a root of $f_i$. Since $f_1$ and $f_i$ are monic and irreducible over $M[t]$, we have $f_1 = m_\alpha(M)$ and $f_i = m_\beta(M)$. Also, since $f$ is irreducible over $\mathbb{Q}$, there is some $\sigma \in \mathrm{Gal}(L : \mathbb{Q})$ with $\sigma(\alpha) = \beta$. We have $0 = \sigma(f_1(\alpha)) = \sigma(f_1)(\beta)$. Since $M : K$ is normal, it follows from Theorem 6.4 that $\sigma(M) \subseteq M$, so that $\sigma(f_1) \in M[t]$. Then $\sigma(f_1)$ is a monic polynomial divisible by $m_\beta(M) = f_i$. So $\deg(f_1) \geq \deg(f_i)$. Applying this argument with $\sigma^{-1}$ in place of $\sigma$, we see that $\deg(f_i) \geq \deg(f_1)$. Consequently, we have $\deg(f_i) = \deg(f_1)$ for all $i$.

(c) Show that if $M : \mathbb{Q}$ is normal, then $f$ remains irreducible over $M$.

**Solution:** Observe that $\deg(f) = 5$, and so the proposed factorisation implies that $r \deg(f_1) = 5$, whence $\deg(f_i) = 1$ for all $i$, or $\deg(f_1) = 5$ and $r = 1$. In the former case, the field $M$ is equal to the splitting field $L$ of $f$ over $\mathbb{Q}$, contradicting that $M$ is a proper intermediate field. In the latter case, we see that $f$ remains irreducible over $M$.

*End of examination.*