Galois theory, Problems 3

To be handed in 8th November 2017 **SOLUTIONS**

1. Let M be a field. Show that the following are equivalent:

   (i) the field M is algebraically closed;

   (ii) every non-constant polynomial $f \in M[t]$ factors in $M[t]$ as a product of linear factors;

   (iii) every irreducible polynomial in $M[t]$ has degree 1;

   (iv) the only algebraic extension of M is M itself.

   (Version 1)

   Solution: Suppose that (i) holds. Consider $f \in M[t] \setminus M$, and note that f has a root $\alpha_1 \in M$. With $n = \deg f$, we define g_i inductively as follows. Define $g_1 \in M[t]$ by means of the relation $f = (t - \alpha_1)g_1$. Then, for $1 < i \leq n$, define $g_i \in M[t]$ by means of the relation $g_{i-1} = (t - \alpha_i)g_i$. Since $\deg g_i = n - i$, we see that g_{i-1} is non-constant for $1 < i \leq n$, and hence has a root $\alpha_i \in M$. We note in this context that $g_n \in M^\times$ is the leading coefficient of f. Thus $f = g_n(t - \alpha_1) \cdots (t - \alpha_n)$, and we conclude that (i) implies (ii).

   Suppose next that (ii) holds, and suppose that $f \in M[t]$ is irreducible. Then f is non-zero and non-constant. Since f factors as a product of $\deg f$ linear factors, we must have $\deg f = 1$, and thus (ii) implies (iii).

   Next suppose that (iii) holds, and suppose that α lies in some algebraic extension field N extending M. Assume $M \subseteq N$. Then α is algebraic over M, and hence there is some irreducible polynomial $m_\alpha(M) \in M[t]$, which, in view of the hypothesis (iii), has degree 1. Since this polynomial is also monic, we infer that $t - \alpha = m_\alpha(M) \in M[t]$, whence $\alpha \in M$. But then $N = M$, and so (iii) implies (iv).

   Finally, suppose that (iv) holds. Suppose that $f \in M[t] \setminus M$, and let N be a field extension of M with $M \subseteq N$ containing a root α of f. Then $M(\alpha) : M$ is an algebraic extension. The hypothesis (iv) thus implies that $M(\alpha) = M$, whence $\alpha \in M$. Then (iv) implies (i).

   We have confirmed the equivalence of (i), (ii), (iii) and (iv).

   (Version 2)

   Suppose that (iv) holds. Let f be an irreducible polynomial in $M[t]$. Since the only algebraic extension of M is M itself, it follows that f has a root $\alpha \in M$. Thus $t - \alpha \in M[t]$ is a factor of f, whence $f = (t - \alpha)h$ for some $h \in M[t]$. The irreducibility of f implies that h is a unit, and hence non-zero. Thus $\deg f = 1$, and so (iv) implies (iii).

   Suppose next that (iii) holds. Let $f \in M[t] \setminus M$. Since f factors as a product of irreducible elements over $M[t]$, it factors as a product of linear factors. Then (iii) implies (ii).

   Next suppose that (ii) holds. Let $f \in M[t] \setminus M$. Then f factors as a product of linear factors. Let $\beta t - \gamma$ be one of these linear factors, so that $\beta \neq 0$. Thus $\beta^{-1}\gamma$ is a root of f, and so M is algebraically closed and (ii) implies (i).

   Finally, suppose that (i) holds. Let N be an algebraic extension of M, assume that $M \subseteq N$, and let $\alpha \in N$. Since $N : M$ is algebraic, the minimal polynomial $m_\alpha(M)$ exists, and by hypothesis (i), it has a root $\beta \in M$. Then $t - \beta \in M[t]$ is a factor of $m_\alpha(M)$. Since $m_\alpha(M)$ is monic and irreducible, we must have $m_\alpha(M) = t - \beta$. But then α is a root of $t - \beta$, whence $\alpha = \beta$. Consequently, one has $\alpha = \beta \in M$. As this holds for all $\alpha \in N$, we deduce that $N \subseteq M$. However, we have also $M \subseteq N$, and thus $M = N$. Hence (i) implies (iv).

   We have again confirmed the equivalence of (i), (ii), (iii) and (iv).

2. Let $L : K$ be a field extension with $K \subseteq L$. Let $\gamma \in L$ be transcendental over K, and suppose that $K(\gamma) : K$ is a simple field extension. Show that $K(\gamma)$ is not algebraically closed.
Solution: Put $M = K(\gamma)$, and suppose that M is algebraically closed. We show that the polynomial $t^2 - \gamma$ is irreducible over $M[t]$, contradicting that M is algebraically closed, and thereby establishing the desired conclusion. Suppose then that $\alpha \in M$ satisfies the relation $\alpha^2 = \gamma$. Since $\alpha \in M = K(\gamma)$, it follows that there exists $n, m \in \mathbb{Z}_{\geq 0}$ and $a_i, b_i \in K$ $(0 \leq i \leq n)$, with $a_n \neq 0$ and $b_m \neq 0$, having the property that

$$\alpha = \frac{a_0 + a_1\gamma + \ldots + a_n\gamma^n}{b_0 + b_1\gamma + \ldots + b_m\gamma^m},$$

whence

$$(a_0 + a_1\gamma + \ldots + a_n\gamma^n)^2 = \gamma(b_0 + b_1\gamma + \ldots + b_m\gamma^m)^2.$$

Hence

$$a_n^2\gamma^{2n} + \ldots + a_0^2 = b_m^2\gamma^{2m+1} + \ldots + b_0^2\gamma.$$

Either $2n > 2m + 1 \geq 1$, in which case γ is a root of the polynomial

$$a_n^2 t^{2n} + \ldots + a_0^2 \in K[t] \setminus K,$$

or else $2m + 1 > 2n \geq 0$, in which case γ is a root of the polynomial

$$b_m^2 t^{2m+1} + \ldots - a_0^2 \in K[t] \setminus K.$$

We therefore deduce that γ is algebraic over K, contradicting our hypotheses that γ is transcendental over K. Thus $K(\gamma)$ cannot be algebraically closed.

3. For each of the following polynomials, construct a splitting field L over $\mathbb{Q}$ and compute the degree $[L : \mathbb{Q}]$.

   (a) $t^7 - 1$
   Solution: 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 $[\mathbb{Q}(\zeta) : \mathbb{Q}] = 6$.

   (b) $t^4 + t^2 - 6$
   Solution: We have that

$$t^4 + t^2 - 6 = (t^2 - 2)(t^2 + 3) = (t + \sqrt{2})(t - \sqrt{2})(t + i\sqrt{3})(t - i\sqrt{3}).$$

   Then $\mathbb{Q}(\sqrt{2}, i\sqrt{3}) : \mathbb{Q}$ is a splitting field extension for $t^4 + t^2 - 6$. We have that $\sqrt{2}$ is a root of the polynomial $t^2 - 2$, which 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 $i\sqrt{3}$ is a root of the polynomial $t^2 + 3$. This polynomial is irreducible over $K[t]$, since $i\sqrt{3}$ is not real, and yet $K \subset \mathbb{R}$. Thus $m_{i\sqrt{3}}(K) = t^2 + 3$ and $[K(i\sqrt{3}) : K] = \deg m_{i\sqrt{3}}(K) = 2$. The tower law therefore yields the relation

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

4. Construct a splitting field L over $\mathbb{Q}$ for the polynomial $t^8 - 16$, and determine the subgroup of S_4 to which $\mathrm{Gal}(L : \mathbb{Q})$ is isomorphic.
Solution: 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 $K = \mathbb{Q}(\alpha, \zeta\alpha, \zeta^2\alpha, \ldots, \zeta^7\alpha)$, we see that $K : \mathbb{Q}$ is a splitting field extension for $t^8 - 16$. Note that $\zeta = (\zeta\alpha)/\alpha \in K$, and hence $\mathbb{Q}(\alpha, \zeta) \subseteq K$. Also, for $k \in \mathbb{N}$, one has $\zeta^k\alpha \in \mathbb{Q}(\alpha, \zeta)$, and so $K \subseteq \mathbb{Q}(\alpha, \zeta)$. We therefore conclude that $K = \mathbb{Q}(\alpha, \zeta)$. 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 $[K : \mathbb{Q}] = [\mathbb{Q}(\alpha, \zeta) : \mathbb{Q}(\alpha)][\mathbb{Q}(\alpha) : \mathbb{Q}] = 4$.

Take $\tau \in \mathrm{Gal}(L : \mathbb{Q})$. Then τ is determined by its action on α and i. We begin by constructing $\mathbb{Q}$-homomorphisms $\sigma : \mathbb{Q}(\alpha) \to \mathbb{Q}(\alpha, i)$. We know that $\sigma(\alpha)$ must be a root of $m_\alpha(\mathbb{Q}) = t^2 - 2$, so $\sigma(\alpha) = \pm\alpha$. We can extend σ to $\tau : \mathbb{Q}(\alpha, i) \to \mathbb{Q}(\alpha, i)$ by taking $\tau|_{\mathbb{Q}(\alpha)} = \sigma$ and $\tau(i) = \pm i$, with the choice of sign independent of the previous choice. Here, since $m_i(\mathbb{Q}(\alpha)) = t^2 + 1$, we find that $\tau(i)$ must be one of the roots of $t^2 + 1$, explaining the previous assertion. We thus conclude that τ is one of the permutations τ_{lm} $(l, m \in \{0, 1\})$, where $\tau_{lm}(\alpha) = (-1)^l\alpha$ and $\tau_{lm}(i) = (-1)^m i$. Thus τ acts as one of the four permutations

$$(\alpha \ -\alpha)(i \ -i), \quad (\alpha \ -\alpha), \quad (i \ -i), \quad \mathrm{id}.$$

The group $\mathrm{Gal}(L : \mathbb{Q})$ is therefore isomorphic to the group of permutations

$$\{(1), (1\ 2), (3\ 4), (1\ 2)(3\ 4)\}.$$

5. Suppose that K is a field and that $L : K$ is a splitting field extension for an irreducible polynomial $f \in K[t]$ of degree n. Assume that $K \subseteq L$.

   (a) Show that whenever α and β are roots of f in L, and σ is a K-automorphism of L, then $\sigma(\alpha) = \sigma(\beta)$ if and only if $\alpha = \beta$;
   Solution: Since σ is a K-automorphism of L, it is bijective and hence invertible. Then $\sigma(\alpha) = \sigma(\beta)$ if and only if $\sigma^{-1}(\sigma(\alpha)) = \sigma^{-1}(\sigma(\beta))$, which is to say, if and only if $\alpha = \beta$.

   (b) Show that the elements of $\mathrm{Gal}(L : K)$ act as permutations on the n roots of f, and hence deduce that $\mathrm{Gal}(L : K)$ has order dividing $n!$;
   Solution: Let $\alpha \in L$ be a root of f, and consider $\tau \in \mathrm{Gal}(L : K)$. Then $\tau(f(\alpha)) = f(\tau(\alpha))$. Thus, under the action of any element τ of $\mathrm{Gal}(L : K)$, a root α of f is taken to another root β of f. Since this mapping is bijective, it follows that σ acts as a permutation on the set of roots of f. A permutation group on a set of n objects is a subset of S_n (the permutation group on n letters), and hence by Lagrange's theorem has order dividing $n!$.

   (c) Let g be a degree m polynomial in $K[t]$, not necessarily irreducible, and let $M : K$ be a splitting field extension for g. Show that $|\mathrm{Gal}(M : K)|$ divides $m!$.
   Solution: Let $\alpha \in M$ be a root of g, and consider $\tau \in \mathrm{Gal}(M : K)$. Then again $\tau(g(\alpha)) = g(\tau(\alpha))$. Thus, just as in the discussion for part (b), the mapping τ acts as a permutation on the distinct roots of g. If the number of distinct roots of g is n, then it follows that $|\mathrm{Gal}(M : K)|$ divides $n!$. But $n \leq m$, so $n!$ divides $m!$, whence $|\mathrm{Gal}(M : K)|$ divides $m!$.

6. Suppose that $L : K$ is a normal extension, and that $K \subseteq L \subseteq \overline{K}$. Recall that since $L : K$ is algebraic, then any algebraic closure of K is an algebraic closure of L.

   (a) Show that for any K-homomorphism $\tau : L \to \overline{K}$, one has $\tau(L) = L$;
   Solution: Let $\tau : L \to \overline{K}$ be a K-homomorphism. Let $\alpha \in L$. Then since $L : K$ is algebraic, one sees that α is algebraic over K, and so $m_\alpha(K)$ exists. Write $g = m_\alpha(K)$. Then on noting that g is a K-homomorphism, we deduce that $0 = \tau(g(\alpha)) = g(\tau(\alpha))$. But $L : K$ is normal, so $\tau(\alpha) \in L$. Since this holds for all $\alpha \in L$, we infer that $\tau(L) \subseteq L$. Finally, since $L : K$ is algebraic, it follows from Theorem 3.4 that $\tau(L) = L$.

   (b) Suppose that M is a field satisfying $K \subseteq M \subseteq L$. Show that $L : M$ is a normal extension.
   Solution: Assume $K \subseteq M \subseteq L$, and let $f \in M[t] \setminus M$ be irreducible. Suppose that $\alpha \in L$ is a root of f. Then $f = \lambda m_\alpha(M)$ for some $\lambda \in M^\times$. But $m_\alpha(M)$ divides $m_\alpha(K)$, and since $L : K$ is normal, one has that $m_\alpha(K)$ splits over L. Hence $m_\alpha(M)$ also splits over L, and thus f splits over L. Then $L : M$ is a normal extension.