Galois theory, Problems 2

To be handed in 24th October 2017 **SOLUTIONS**

1. Let $L : K$ be a field extension with $K \subseteq L$. Then the following are equivalent:

   (i) one has $[L : K] < \infty$;

   (ii) the extension $L : K$ is algebraic, and there exist $\alpha_1, \ldots, \alpha_n \in L$ having the property that $L = K(\alpha_1, \ldots, \alpha_n)$.

   Solution: To show (i) implies (ii): Suppose that $[L : K] < \infty$. If $L = K$ then $L = K(\alpha_1)$ for any $\alpha_1 \in L$. So suppose that $L \neq K$. Take $m \in \mathbb{N}$ so that $[L : K] \leq 2^m$. Set $K_0 = K$. For $1 \leq i \leq m$, define $K_i \subseteq L$ inductively as follows. If $K_{i-1} \neq L$ then choose $\alpha_i \in L \setminus K_{i-1}$, and set $K_i = K_{i-1}(\alpha_i)$; if $K_{i-1} = L$ then take $\alpha_i \in K_{i-1}$ and set $K_i = K_{i-1}(\alpha_i) = L$. We claim that for some $j \leq m$, we have $K_j = L$. For the sake of contradiction, suppose not; so for $1 \leq i \leq m$, we have $K_i = K_{i-1}(\alpha_i)$ where $\alpha_i \notin K_{i-1}$. Thus for $1 \leq i \leq m$, we have $[K_i : K_{i-1}] \geq 2$. Hence by the Tower Law, we have

   $$[K_m : K] = [K_m : K_{m-1}][K_{m-1} : K_{m-2}] \cdots [K_1 : K_0] \geq 2^m.$$

   We also know that $K_m = K(\alpha_1, \ldots, \alpha_m) \subseteq L$, so

   $$[L : K] = [L : K_m][K_m : K]$$

   with $[L : K_m] > 1$ (since $K_m \subsetneq L$) and $[K_m : K] \geq 2^m \geq [L : K]$. Hence $[L : K] > [K_m : K] \geq 2^m \geq [L : K]$, a contradiction. Hence for some $j \leq m$, we have $L = K_j = K(\alpha_1, \ldots, \alpha_j)$ for some $\alpha_1, \ldots, \alpha_j \in L$.

   [*A less formal argument:* Suppose that $[L : K] < \infty$. Take $\beta \in L$. Then

   $$[L : K(\beta)][K(\beta) : K] = [L : K] < \infty,$$

   so $[K(\beta) : K] < \infty$. Hence β is algebraic over K. As this holds for all $\beta \in L$, $L : K$ is an algebraic extension. If $L = K$ then $L = K(1)$. Suppose $L \neq K$; choose $\alpha_1 \in L \setminus K$. Thus $[K(\alpha_1) : K] \geq 2$; if $K(\alpha_1) = L$ then we are done. Suppose that $L \neq K(\alpha + 1)$. Then we carry on as above, choosing $\alpha_{i+1} \in L \setminus K(\alpha_1, \ldots, \alpha_i)$; thus $[K(\alpha_1, \ldots, \alpha_{i+1}) : K(\alpha_1, \ldots, \alpha_i)] \geq 2$. When we have $L = K(\alpha_1, \ldots, \alpha_n)$ then this process terminates. The process must terminate, since with $\alpha_{j+1} \in L \setminus K(\alpha_1, \ldots, \alpha_j)$ for $1 \leq j \leq i$, we have $2^i \leq [K(\alpha_1, \ldots, \alpha_i) : K] \leq [L : K] < \infty$.]

   To show (ii) implies (i): Suppose $L : K$ is an algebraic extension and $L = K(\alpha_1, \ldots, \alpha_n)$. Thus $\alpha_1, \ldots, \alpha_n$ are algebraic over K, so for $1 \leq i < n$, we have $[K(\alpha_i) : K] < \infty$. Hence

   $$\begin{aligned}[L : K] &= [K(\alpha_1, \ldots, \alpha_n) : K(\alpha_1, \ldots, \alpha_{n-1})] \\ &\qquad \cdot [K(\alpha_1, \ldots, \alpha_{n-1}) : K(\alpha_1, \ldots, \alpha_{n-2})] \cdots [K(\alpha_1) : K] \\ &\leq [K(\alpha_n) : K][K(\alpha_{n-1}) : K] \cdots [K(\alpha_1) : K] \\ &< \infty.\end{aligned}$$

2. (a) Show that when p is a prime number, then for every positive integer n the polynomial $X^n - p$ is irreducible over $\mathbb{Q}$.

(b) By making the substitution $y = X - 1$, or otherwise, show that when p is a prime number, the polynomial $X^{p-1} + X^{p-2} + \cdots + X + 1$ is irreducible over $\mathbb{Q}$.

(c) Let p be a prime number with $p \equiv 3 \pmod 4$, and consider the polynomial $\pi = t^2 + 1$ in the ring $\mathbb{K} = \mathbb{F}_p[t]$. Show that the polynomial $X^{2016} - \pi X + \pi$ is irreducible over $\mathbb{F}_p(t)$.

Solution: (a) The polynomial $X^n - p$ has leading coefficient not divisible by p, all other coefficients divisible by p, and final coefficient not divisible by p^2. Then Eisenstein's criterion applies, and establishes that $X^n - p$ is irreducible.

(b) Write $f(x) = x^{p-1} + x^{p-2} + \cdots + 1$. Then one has $(x-1)f(x) = x^p - 1$. Now substitute $x = y + 1$, and we find that

$$yf(y+1) = (y+1)^p - 1 = y^p + \sum_{i=1}^{p-1} \binom{p}{i} y^i = yg(y),$$

say. But since each binomial coefficient $\binom{p}{i}$ is divisible by p for $1 \leq i \leq p-1$, we find that g has leading coefficient not divisible by p, all other coefficients divisible by p, and final coefficient p not divisible by p^2. Then Eisenstein's criterion applies, and shows that g is irreducible. But by uniqueness of factorisation, one has $g(x-1) = f(x)$, and thus f must also be irreducible.

(c) On noting that -1 is a quadratic non-residue modulo p for $p \equiv 3 \pmod 4$, we see that the polynomial $t^2 + 1$ has no root over $\mathbb{F}_p$. Thus π is irreducible over $\mathbb{F}_p[t]$, and thus by Gauss' Lemma, also over $\mathbb{F}_p(t)$. But now, over $K[X]$, we see that the leading coefficient of $g = X^{2016} - \pi X + \pi$ is not divisible by π, all other coefficients are divisible by π, and the final coefficient is not divisible by π^2. We thus deduce via Eisenstein's criterion that g is irreducible over $K[X]$. [A variant of this argument also applies when $p \equiv 1 \pmod 4$].

3. (a) Show that the polynomial $f(t) = t^7 - 7t^5 + 14t^3 - 7t - 2$ factorises over $\mathbb{Q}[t]$ in the form $f = g_1 g_3^2$, where $g_1, g_3 \in \mathbb{Z}[t]$ have the property that g_1 is linear, and g_3 is cubic and irreducible.

(b) Using the identity

$$\cos 7\theta = 64\cos^7\theta - 112\cos^5\theta + 56\cos^3\theta - 7\cos\theta,$$

together with the conclusion of part (a), show that the angle $2\pi/7$ is not constructible by ruler and compass. Hence deduce that the regular heptagon is not constructible by ruler and compass.

Solution: (a) By Gauss' Lemma, any linear factor of f must have the shape $t \pm 1$ or $t \pm 2$. Since $f(2) = 0$, we find that f is divisible by $t - 2$, and by long division we find further that

$$\begin{aligned} f &= (t-2)(t^6 + 2t^5 - 3t^4 - 6t^3 + 2t^2 + 4t + 1) \\ &= (t-2)(t^3 + t^2 - 2t - 1)^2. \end{aligned}$$

We therefore have $f = g_1 g_3^2$, with $g_1 = t - 2$ and $g_3 = t^3 + t^2 - 2t - 1$. It remains only to check that g_3 is irreducible. But if it has a factor of positive degree, then it must have a linear factor, and this would necessarily have the shape $t \pm 1$. Since neither of these possibilities is a factor of g_3, we see that g_3 is indeed irreducible.

(b) We seek to derive a contradiction. If $\theta = 2\pi/7$ were constructible, then so too would be the point $(\cos\theta, \sin\theta) \in \mathbb{R}^2$, and hence $[\mathbb{Q}(\cos\theta) : \mathbb{Q}] = 2^r$ for some $r \in \mathbb{Z}_{\geq 0}$. Putting $\sigma = 2\cos\theta$, we deduce via the provided polynomial identity that

$$\begin{aligned}\sigma^7 - 7\sigma^5 + 14\sigma^3 - 7\sigma - 2 &= 2(64\cos^7\theta - 112\cos^5\theta + 56\cos^3\theta - 7\cos\theta - 1)\\ &= 2(\cos 2\pi - 1) = 0,\end{aligned}$$

whence $f(\sigma) = 0$. Since $\sigma \neq 2$, we deduce that σ is a root of the irreducible polynomial g_3, whence $[\mathbb{Q}(\sigma) : \mathbb{Q}] = \deg g_3 = 3$. This contradicts the assumption that $[\mathbb{Q}(\cos\theta) : \mathbb{Q}]$ is a power of 2, and thus we deduce that θ is not constructible. If the regular heptagon were to be constructible, then $2\pi/7$ would be constructible, contradicting the last conclusion (consider the angle suspended by one of the sides). Thus regular heptagons are not constructible.

4. Suppose that $L : K$ is a field extension with $K \subseteq L$, and that $\tau : L \to L$ is a K-homomorphism. Suppose also that $f \in K[t]$ has the property that $\deg f \geq 1$, and additionally that $\alpha \in L$.

   (a) Show that when $f(\alpha) = 0$, then $f(\tau(\alpha)) = 0$.

   (b) Deduce that when τ is a K-automorphism of L, we have that $f(\alpha) = 0$ if and only if $f(\tau(\alpha)) = 0$.

   Solution: (a) Suppose that $f(\alpha) = 0$, and write $f = c_0 + c_1 t + \ldots + c_n t^n$, where $n = \deg f$. Since $f \in K[t]$, we know that $c_i \in K$ for each i. Also, in view of the fact that τ is a K-homomorphism, we have that

$$0 = \tau(f(\alpha)) = c_0 + c_1\tau(\alpha) + \ldots + c_n(\tau(\alpha))^n = f(\tau(\alpha)).$$

   (b) If τ is a K-automorphism of L, then $\tau^{-1} : L \to L$ exists and is a K-homomorphism, so the argument above shows that whenever $f(\tau(\alpha)) = 0$, then

$$0 = \tau^{-1}(f(\tau(\alpha))) = f(\tau^{-1}(\tau(\alpha))) = f(\alpha).$$

   Thus $f(\alpha) = 0$ if and only if $f(\tau(\alpha)) = 0$.

1. Let $L : K$ be a field extension. Show that $\mathrm{Gal}(L : K)$ is a subgroup of $\mathrm{Aut}(L)$.
   Solution: Suppose first that $K \subseteq L$. We know that the identity map on L is in $\mathrm{Aut}(L)$, and that it leaves K pointwise fixed, so the identity map on L is in $\mathrm{Gal}(L : K)$. Now consider $\sigma, \tau \in \mathrm{Gal}(L : K)$. Thus $\sigma, \tau \in \mathrm{Aut}(L)$, and hence $\sigma \circ \tau$ and σ^{-1} both lie in $\mathrm{Aut}(L)$. Also, for each $\alpha \in K$, we have $\sigma(\alpha) = \alpha$ and $\tau(\alpha) = \alpha$, since σ and τ leave K pointwise fixed. Thus

$$\sigma \circ \tau(\alpha) = \sigma(\tau(\alpha)) = \sigma(\alpha) = \alpha.$$

   Also, one has $\sigma^{-1}(\alpha) = \alpha$ for all $\alpha \in K$ (for we have $\sigma^{-1}(\beta) = \alpha$ for the value of β satisfying $\sigma(\beta) = \alpha$). Hence $\sigma \circ \tau$ and σ^{-1} both lie in $\mathrm{Gal}(L : K)$, whence $\mathrm{Gal}(L : K)$ is a subgroup of $\mathrm{Aut}(L)$.

   Now suppose that $L : K$ is a field extension relative to an embedding $\varphi : K \to L$. Then in the above argument, for $\alpha \in K$ we have $\sigma(\varphi(\alpha)) = \varphi(\alpha)$ and $\tau(\varphi(\alpha)) = \varphi(\alpha)$, and so $\sigma \circ \tau(\varphi(\alpha)) = \varphi(\alpha)$ and $\sigma^{-1}(\varphi(\alpha)) = \varphi(\alpha)$. Thus the identity map, together with $\sigma \circ \tau$ and σ^{-1} are K-homomorphisms. Thus $\mathrm{Gal}(L : K)$ is a subgroup of $\mathrm{Aut}(L)$.

2. Suppose that L and M are fields with an associated homomorphism $\psi : L \to M$. Show that whenever L is algebraically closed, then $\psi(L)$ is also algebraically closed.

Solution: Suppose that L is algebraically closed, and that $f' \in \psi(L)[t]$ is irreducible. Then we have $f' = \psi(f)$ for some $f \in L[t]$, and $\deg f' = \deg f$. For the sake of deriving a contradiction, suppose that $\deg f' > 1$. Then $\deg f > 1$. Since L is algebraically closed, it follows that irreducible polynomials in $L[t]$ have degree 1. We are forced to conclude, therefore, that f is reducible, and hence that $f = gh$ for some polynomials $g, h \in L[t]$ with $\deg g \geq 1$ and $\deg h \geq 1$. Consequently, we have $f' = g'h'$, where $g' = \psi(g)$ and $h' = \psi(h)$ satisfy the property that $\deg g' \geq 1$ and $\deg h' \geq 1$. However, this contradicts the assumption that f' is irreducible in $\psi(L)[t]$. We must therefore have $\deg f' = 1$. Thus we conclude that $\psi(L)$ is algebraically closed.