GALOIS THEORY 2019: HW 2 SOLUTIONS

For assessment: Problems 1, 2, 3

Due by noon Tuesday, week 5 of the term

1. Suppose that $L : K$ is a field extension with $K \subseteq L$, and that $\tau : L \to L$ is a K-homomorphism. Also suppose that $f \in K[t]$ with $\deg f \geq 1$, and that $\alpha \in L$. Show that $f(\alpha) = 0$ if and only if $f(\tau(\alpha)) = 0$.

   Solution: [This is Proposition 3.1.]

   For some $a_0, a_1, \ldots, a_n \in K$, we have $f = a_0 + a_1 t + \cdots + a_n t^n$. We know that τ is injective and $\tau(0) = 0$ [since τ is a field homomorphism], so $f(\alpha) = 0$ if and only if $\tau(f(\alpha)) = 0$. Also, since τ is a K-homomorphism, we have

$$\begin{aligned}\tau(f(\alpha)) &= \tau(a_0 + a_1\alpha + \cdots + a_n\alpha^n) \\ &= \tau(a_0) + \tau(a_1)\tau(\alpha) + \cdots + \tau(a_n)\tau(\alpha)^n \\ &= a_0 + a_1\tau(\alpha) + \cdots + a_n\tau(\alpha)^n \\ &= f(\tau(\alpha)).\end{aligned}$$

   Thus

$$f(\alpha) = 0 \iff \tau(f(\alpha)) = 0 \iff f(\tau(\alpha)) = 0.$$

2. Let M be a field. Show that the following are equivalent:
   (i) M is algebraically closed.
   (ii) Every nonconstant 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) Any algebraic extension of M is [isomorphic to] M.

   Solutions: [This is Lemma 4.1; proving that (i) is equivalent to (iii) was on the 2016 exam.] There are many ways to prove this; here we do not present all the possibilities. We first show that (i) implies (ii), (ii) implies (iii), (iii) implies (iv), (iv) implies (i). Then we show the reverse.

   Solution 1:

   Suppose (i) holds. Take $f \in M[t] \setminus M$. Thus f has a root $\alpha_1 \in M$. With $n = \deg f$, define g_i inductively as follows. Take $g_1 \in M[t]$ so that $f = (t - \alpha_1)g_1$. For $1 < i \leq n$, take $g_i \in M[t]$ so that $g_{i-1} = (t - \alpha_i)g_i$. Since $\deg g_i = n - i$, g_{i-1} is nonconstant for $1 < i \leq n$, and hence has a root $\alpha_i \in M$. [Note that $g_n \in M^\times$ is the leading coefficient of f.] Thus

$$f = g_n \prod_{i=1}^{n} (t - \alpha_i).$$

   So (i) implies (ii).

   Suppose (ii) holds, and suppose $f \in M[t]$ is irreducible. So f is nonzero and nonconstant [as the nonzero constants in $M[t]$ are units]. As f factors as a product of $\deg f$ linear factors, we must have $\deg f = 1$. So (ii) implies (iii).

Suppose (iii) holds, and suppose α lies in some algebraic extension field $N : M$, where $N : M$ is an extension relative to a homomorphism $\varphi : M \to N$. Assume $M \subseteq N$. So α is algebraic over M, and hence there is some $m_\alpha(M) \in M[t]$. Since $m_\alpha(M)$ is necessarily irreducible, it has degree 1. Since it is also monic, we have $t - \alpha = m_\alpha(M) \in M[t]$, so $\alpha \in M$. Thus $N = M$. So (iii) implies (iv). [If we don't assume that $M \subseteq N$, there is some monic, irreducible $f \in M[t]$ so that α is a root of $\varphi(f)$. Since $\deg f = 1$, we have $f = t - \beta$ where $\beta \in M$, and $\varphi(f) = t - \varphi(\beta)$ with $\varphi(\beta) = \alpha$ since α is a root of $\varphi(f)$. Hence for all $\alpha \in L$, we have $\alpha \in \varphi(M)$, meaning that $\varphi : M \to L$ is an isomorphism.]

Suppose (iv) holds. Say $f \in M[t] \setminus M$. Let $N : M$ be a splitting field extension for f, and assume that $M \subseteq N$. Thus by assumption, the inclusion map $\varphi : M \to N$ is an isomorphism, so $M = N$. Thus f splits over M, and in particular, M contains a root of f. Hence (iv) implies (i).

This shows the equivalence of (i), (ii), (iii), (iv).

Solution 2:

Suppose (iv) holds. Take $f \in M[t]$ so that f is irreducible over M. Let $L : M$ be a splitting field extension for f, and assume that $M \subseteq L$. By (iv), M isomorphic to L, which means that we must have $M = L$. As f factors into linear factors over $L = M$ and f is irreducible over M, we must have $\deg f = 1$. So (iv) implies (iii).

Suppose (iii) holds. Take nonconstant $f \in M[t]$. We know f factors as a product of irreducible elements of $M[t]$, so f factors as a product of linear factors. So (iii) implies (ii).

Suppose (ii) holds. Suppose $f \in M[t]$ is nonconstant. Then f factors as a product of linear factors. Let $\beta t - \gamma$ be one of these linear factors; so $\beta \neq 0$. Thus $\beta^{-1}\gamma$ is a root of f. So (ii) implies (i).

Suppose (i) holds. Let N be an algebraic extension of M (and assume $M \subseteq N$). Let $\alpha \in N$. Since $N : M$ is an algebraic extension, $m_\alpha(M)$ exists, and by (i), $m_\alpha(M)$ must have a root $\beta \in M$. So in $M[t]$, $t - \beta$ is a factor of $m_\alpha(M)$. Since $m_\alpha(M)$ is monic and irreducible, we must have $m_\alpha(M) = t - \beta$. Hence α is a root of $t - \beta$, which means that $\alpha = \beta$. Thus $\alpha = \beta \in M$. As this holds for all $\alpha \in N$, we have $N \subseteq M$. Since $M \subseteq N$, we have $M = N$. Hence (i) implies (iv).

This shows the equivalence of (i), (ii), (iii), (iv).

3. 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: [This is Proposition 4.7.]

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.

4. [This is a HW problem from years ago; it demonstrates a type of result one can prove with ruler and compass constructions.]
Set $f(t) = t^7 - 7t^5 + 14t^3 - 7t - 2 \in \mathbb{Q}[t]$. With $g_1 = t - 2$ and $g_3 = t^3 + t^2 - 2t - 1$, one can check that $f = g_1 g_3^2$.
   (a) Show that g_3 is irreducible in $\mathbb{Q}[t]$.
   (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.

Solutions: (a) Note that g_3 is primitive in $\mathbb{Z}[t]$. Over $\mathbb{Z}/3\mathbb{Z}$, g_3 has degree 3, the degree of g_3 over $\mathbb{Q}$; hence if g_3 is irreducible over $\mathbb{Z}/3\mathbb{Z}$ then g_3 is irreducible over $\mathbb{Z}$. Recall that if g_3 is reducible over $\mathbb{Z}/3\mathbb{Z}$ then it must have a linear factor, or equivalently, a root in $\mathbb{Z}/3\mathbb{Z}$ [recall that this is not true for polynomials of degree larger than 3]. We see that $g_3(0) \equiv -1 \ (mod\ 3)$, $g_3(1) \equiv -1 \ (mod\ 3)$, and $g_3(2) \equiv 1 \ (\mod 3)$. Hence g_3 is irreducible over $\mathbb{Z}$, and so by Gauss' Lemma, g_3 is irreducible over $\mathbb{Q}$.

(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

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

hence $f(\sigma) = 0$. 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.

5. Let $L : K$ be a field extension. Show that $Gal(L : K)$ is a subgroup of $Aut(L)$.

Solution: Suppose first that $K \subseteq L$. We know that the identity map on L is in $Aut(L)$, 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 $\sigma, \tau \in Aut(L)$, and hence $\sigma \circ \tau$ and σ^{-1} both lie in $Aut(L)$. 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 $Aut(L)$.

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 $Aut(L)$.

6. Suppose K_1, K_2 are fields and $\sigma : K_1 \to K_2$ is an isomorphism. We extend σ to the isomorphism $\sigma : K_1[t] \to K_2[t]$ by setting $\sigma(t) = t$. Suppose that f is an irreducible element of $K_1[t]$.
   (a) Show that $\sigma(f)$ is an irreducible element of $K_2[t]$.
   (b) Define $\varphi : K_1[t] \to K_2[t]/(\sigma(f))$ by $\varphi(g) = \sigma(g) + (\sigma(f))$. Show that $\ker \varphi = (f)$.

   Solutions: [These are results from Algebra 2.]

   (a) Suppose that $\sigma(f) = g'h'$ where $g', h' \in K_2[t]$. Note that g', h' are nonzero since f is nonzero, and since σ is injective, this means that $\sigma(f)$ is nonzero. Since σ is surjective, there are (nonzero) $g, h \in K_1[t]$ so that $\sigma(g) = g'$ and $\sigma(h) = h'$; also, since σ is a homomorphism with $\sigma(t) = t$, we know that $\deg g = \deg g'$ and $\deg h = \deg h'$. Since σ is injective and $\sigma(gh) = \sigma(g)\sigma(h) = g'h' = \sigma(f)$, we have $gh = f$. We have assumed that f is irrediculble over K_1, so either g or h is a unit in $K_1[t]$, meaning either g or h has degree 0. So g' or h' has degree 0, and hence g' or h' is a unit in $K_2[t]$. Thus $\sigma(f)$ is irreducible in $K_2[t]$.
   (b) First suppose that $g \in (f)$; thus $g = fh$ for some $h \in K_1[t]$. Then $\sigma(fh) = \sigma(f)\sigma(h)$ with $\sigma(h) \in K_2[t]$, so $\sigma(fh) \in (\sigma(f))$. Hence $\varphi(g) = \sigma(fh) + (\sigma(f)) = 0 + (\sigma(f))$. Thus $(f) \subseteq \ker \varphi$.

   Now say $g \in \ker \varphi$. Thus $\sigma(g) + (\sigma(f)) = 0 + (\sigma(f))$, so $\sigma(g) \in (\sigma(f))$. This means that $\sigma(g) = \sigma(f)h'$ for some $h' \in K_2[t]$. Since σ is surjective, there is some $h \in K_1[t]$ so that $\sigma(h) = h'$. Hence $\sigma(g) = \sigma(f)\sigma(h) = \sigma(fh)$. Since σ is injective, this means that $g = fh \in (f)$. Hence $\ker \varphi \subseteq (f)$.

   In conclusion, $\ker \varphi = (f)$.