GALOIS THEORY: SOLUTIONS TO HOMEWORK 3

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

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 $1 \le i \le p-1$, 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.

2. (a) Show that the polynomial $\phi = t^3 - t + 1$ is irreducible over the ring $\mathbb{I} = \mathbb{F}_3[t]$.
(b) Let $\mathbb{K} = \mathbb{F}_3(t)$. Show that the polynomial $X^{2024} + \phi X^2 + \phi$ is irreducible over $\mathbb{K}[X]$.

Solution: (a) If ϕ fails to be irreducible over $\mathbb{I}$, then it has a linear factor, and the only monic such factors over $\mathbb{I}$ are t and $t \pm 1$. But $\phi = t(t+1)(t-1) + 1$, so none of these factors divide f (they leave remainder 1 in each case). Hence ϕ is irreducible over $\mathbb{I}$.
(b) Over $\mathbb{I}[X]$, we see that the leading coefficient of $g = X^{2024} + \phi X^2 + \phi$ is not divisible by ϕ, all other coefficients are divisible by ϕ, and the final coefficient is not divisible by ϕ^2. Since ϕ is irreducible over $\mathbb{I}$, we therefore deduce via Eisenstein's criterion that g is irreducible over $\mathbb{I}[X]$. But then it follows from Gauss' lemma that g is also irreducible over $\mathbb{K}[X]$, since $\mathbb{K}$ is the field of fractions of $\mathbb{I}$.

3. Let $L : K$ be a field extension. Suppose that $\alpha \in L$ is algebraic over K and $\beta \in L$ is transcendental over K. Suppose also that $\alpha \notin K$. Show that $K(\alpha, \beta) : K$ is not a simple field extension.

Solution: Suppose that $K(\alpha, \beta) = K(\gamma)$ for some $\gamma \in L$. Since $\beta \in K(\gamma)$ is transcendental over K, the field extension $K(\gamma) : K$ is not algebraic, and hence γ is transcendental over K. Since $\alpha \in K(\gamma)$, we have $\alpha = f(\gamma)/g(\gamma)$ for some $f, g \in K[t]$ with $g \neq 0$. Thus γ is a root of $h = \alpha g - f \in K(\alpha)[t]$. Since $\alpha \notin K$ and $g \neq 0$, the polynomial h cannot be the zero polynomial, and therefore γ is algebraic over $K(\alpha)$. But then, since α is algebraic over K, this implies that $[K(\gamma) : K] = [K(\gamma) : K(\alpha)][K(\alpha) : K] < \infty$, contradicting the transcendence of γ. So $K(\alpha, \beta) : K$ cannot be a simple extension.

4. (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 is in contradiction to 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. Assume (as has in fact been proved) that $\pi = 3.14159\ldots$ is transcendental over $\mathbb{Q}$.
(a) Show that one cannot "square the circle" – that is, prove that $\sqrt{\pi}$ is not constructible by ruler and compass.
(b) Suppose that a generous benefactor has given you the points $(0,0)$, $(0,1)$ and $(0,\pi)$ in the plane. Can you now construct $\pi^{1/5}$ by ruler and compass from these three points? Explain your answer.

Solution: (a) Suppose that $\sqrt{\pi}$ is construcible by ruler and compass, so that for some non-negative integer r one has $[\mathbb{Q}(\sqrt{\pi}) : \mathbb{Q}] = 2^r$. Observe that $\mathbb{Q}(\pi) \subseteq \mathbb{Q}(\sqrt{\pi})$, and (since π is transcendental over $\mathbb{Q}$), one has $[\mathbb{Q}(\pi) : \mathbb{Q}] = \infty$. Thus

$$2^r = [\mathbb{Q}(\sqrt{\pi}) : \mathbb{Q}] \geq [\mathbb{Q}(\pi) : \mathbb{Q}] = \infty,$$

yielding a contradiction. Hence $\sqrt{\pi}$ is indeed not constructible by ruler and compass.
(b) Write K for the minimal field containing all of the coordinates of the initial points, so that $K = \mathbb{Q}(\pi)$. Suppose that $\pi^{1/5}$ is constructible in the manner asserted. Then $[K(\pi^{1/5}) : K] = 2^r$, for some non-negative integer r. Let f be the minimal polynomial of $\pi^{1/5}$ over K. Then since $\pi^{1/5}$ is a zero of $t^5 - \pi \in K[t]$, it follows that f divides $t^5 - \pi$.

From here one can adopt several strategies. The high-brow approach is to observe that the mapping $\psi : \mathbb{Q}(\pi) \to \mathbb{Q}(x)$, defined by taking a rational function $h(\pi)$ and putting $\psi(h(\pi)) = h(x)$, gives an isomorphism. This follows because π is transcendental over $\mathbb{Q}$, and hence $\ker(\psi)$ is trivial. From here we see that $t^5 - \pi$ is irreducible over K if and only if $t^5 - x$ is irreducible over $\mathbb{Q}(x)$. But $\mathbb{Q}[x]$ is a UFD, so the lemma of Gauss shows that $t^5 - x$ is irreducible over $\mathbb{Q}(x)$ if and only if $t^5 - x$ is irreducible over $\mathbb{Q}[x]$. However, the element x is irreducible over $\mathbb{Q}[x]$, so the irreducibility of $t^5 - x$ follows from Eisenstein's criterion using the irreducible element x. We conclude that $t^5 - \pi$ is also irreducible over K, and hence $[K(\pi^{1/5}) : K] = 5$. Since $5 \neq 2^r$, for any non-negative integer r, we derive a contradiction to our initial assumption, and conclude that π^5 is not construcible from this initial set of points.

An alternate brute force approach proceeds as follows. We have $[K(\pi^{1/5}) : K] = \deg(f)$, and this must divide 2^r, so that $\deg(f) \in \{1, 2, 4\}$. Also, we see that f divides $t^5 - \pi$, so that f has roots of the shape $\omega^i \pi^{1/5}$ for some integer i, where ω is a primitive 5-th root of 1. In all of these cases, the constant term $\beta \in \mathbb{Q}(\pi)$ of f is the product of these roots, and thus $\beta^5 = \pi^c$ where $c \in \{1, 2, 4\}$. Hence there exist $g, h \in \mathbb{Q}[t]$, with g non-zero, such that $\pi^c = g(\pi)/h(\pi)$. There is no loss of generality in supposing that the constant term of either g or h is non-zero, by removing common factors of t between g and h. We now see that $g(\pi)^5 = \pi^c h(\pi)^5$, which gives a polynomial $k(t) = g(t)^5 - t^c h(t)^5 \in \mathbb{Q}[t]$ having the zero π. Since π is transcendental over $\mathbb{Q}$, any such polynomial must be identically zero, and thus we see in particular that its constant term must be 0, whence the constant term of g must also be 0. Examining the coefficient of t, since $g(t)^5$ now is seen to have a factor t^5, we find that $h(t)$ must have constant term 0. Then g and h both have constant term 0, contradicting our earlier assumption. Thus, we see that $\pi^{1/5}$ is not, after all, constructible in the prescribed manner.

©Trevor D. Wooley, Purdue University 2024. This material is copyright of Trevor D. Wooley at Purdue University unless explicitly stated otherwise. It is provided exclusively for educational purposes at Purdue University, and is to be downloaded or copied for your private study only.