GALOIS THEORY: SOLUTIONS TO HOMEWORK 4

1. (a) By considering the substitution $t = x + 1$ and applying Eisenstein's criterion, show that the polnomial $t^6 + t^3 + 1$ is irreducible over $\mathbb{Q}[t]$.
(b) Suppose, if possible, that $[\mathbb{Q}(\cos(2\pi/9), \sin(2\pi/9)) : \mathbb{Q}] = 2^r$, for some non-negative integer r. Prove that the 9-th root of unity $\omega = \cos(2\pi/9) + i\sin(2\pi/9)$ satisfies the property that $[\mathbb{Q}(\omega) : \mathbb{Q}]$ divides 2^{r+1}.
(c) By considering the factorisation of $t^9 - 1$ over $\mathbb{Q}[t]$, prove that $[\mathbb{Q}(\omega) : \mathbb{Q}] = 6$. Hence deduce that the angle $2\pi/9$ is not constructible by ruler and compass, whence the regular nonagon cannot be constructed by ruler and compass.

   Solution: (a) We have $(x+1)^6 + (x+1)^3 + 1 = x^6 + 6x^5 + 15x^4 + 21x^3 + 18x^2 + 9x + 3$. This polynomial is irreducible over $\mathbb{Q}[x]$ by Gauss' Lemma and Eisenstein's criterion using the prime 3 (this monic polynomial has all save the leading coefficient divisible by 3, and constant coefficient not divisible by 3^2). But if $(x + 1)^6 + (x + 1)^3 + 1$ is irreducible, then so too is $t^6 + t^3 + 1$.

   (b) Write $K = \mathbb{Q}(\cos(2\pi/9), \sin(2\pi/9))$. Then $\omega \in K(i)$. Hence, by the tower law, one has $[K(i) : \mathbb{Q}(\omega)][\mathbb{Q}(\omega) : \mathbb{Q}] = [K(i) : K][K : \mathbb{Q}] = [K(i) : \mathbb{Q}]$. But i is a root of the polynomial $t^2 + 1$ over K, and hence its minimal polynomial has degree 1 or 2. Thus $[K(i) : K] \in \{1, 2\}$. The question directs us to assume that $[K : \mathbb{Q}] = 2^r$, and thus $[K(i) : \mathbb{Q}(\omega)][\mathbb{Q}(\omega) : \mathbb{Q}] \in \{2^r, 2^{r+1}\}$. Then in any case $[\mathbb{Q}(\omega) : \mathbb{Q}]$ divides 2^{r+1}.

   (c) We have $\omega^3 \neq 1$ and $\omega^9 = 1$, so ω is a root of the polynomial $t^9 - 1 = (t^3 - 1)(t^6 + t^3 + 1)$ but not a root of $t^3 - 1$. Then ω must be a root of the irreducible polynomial $t^6 + t^3 + 1$. Thus $m_\omega(\mathbb{Q}) = t^6 + t^3 + 1$, whence $[\mathbb{Q}(\omega) : \mathbb{Q}] = \deg(t^6 + t^3 + 1) = 6$. But 6 does not divide 2^{r+1} for $r \in \mathbb{Z}_{\geq 0}$, contradicting the assumption that $[K : \mathbb{Q}] = 2^r$. Thus $\cos(2\pi/9)$ and $\sin(2\pi/9)$ are not both constructible by ruler and compass, whence the angle $2\pi/9$ is not constructible. But the construction of a regular nonagon would entail constructing the angle $2\pi/9$, so such cannot be constructed by ruler and compass.

2. (a) Suppose that $P_0, P_1, \ldots, P_n$ are points in $\mathbb{R}^2$ whose coordinates lie in a field extension K of $\mathbb{Q}$. Let $P = (x, y)$ be a point of intersection of two ellipses with equations defined over K. Explain why $[K(x, y) : K] \leq 4$.
(b) Let $P_0 = (0, 0)$ and $P_1 = (1, 0)$, and suppose that $P_2, P_3, \ldots$ are constructed successively by simple cord-and-nail constructions (as discussed in Definition 13 of section 2.3 from the notes). Let j be a positive integer, write $P_j = (x_j, y_j)$, and put $L_j = \mathbb{Q}(x_j, y_j)$. Explain why, for some non-negative integers r and s, one has $[L_j : \mathbb{Q}] = 2^r 3^s$.

   Solution: (a) We can assume that the equations of the two ellipses in question are

$$c_{20}x^2 + c_{11}xy + c_{02}y^2 + c_{10}x + c_{01}y + c_{00} = 0,$$

   with $c_{ij} \in K$, and

$$d_{20}x^2 + d_{11}xy + d_{02}y^2 + d_{10}x + d_{01}y + d_{00} = 0,$$

   with $d_{ij} \in K$. By eliminating the x^2 term, we obtain a new equation of the shape

$$e_{11}xy + e_{02}y^2 + e_{10}x + e_{01}y + e_{00} = 0.$$

   If both e_{11} and e_{10} are zero, then this new equation is independent of x and we may solve for y (or possibly all terms except the constant one are zero, and there is no solution).

Then y lies in a quadratic field extension of K, and by back substitution we find that at worst x lies in a quadratic field extension of this first extension. Otherwise, when one at least of e_{11} and e_{10} is non-zero, then we may substitute for x from this equation into the first so as to obtain a quartic equation for y. Back substituting into the linear equation for x then shows that x lies in the same quartic field extension. The latter conclusion, then, remains true in both cases, and $[K(x,y):K]\le 4$.

(b) We expand on the conclusion of part (a) a little. Let $P_i=(x_i,y_i)\in K^2$ $(i\ge 0)$. Then the ellipse defined by taking P_j and P_k as foci, and P_l a third point on the ellipse, has equation given by

$$\sqrt{(x-x_j)^2+(y-y_j)^2}=\sqrt{(x_l-x_i)^2+(y_l-y_i)^2}+\sqrt{(x_l-x_k)^2+(y_l-y_k)^2} - \sqrt{(x-x_k)^2+(y-y_k)^2}.$$

The coefficients here all lie in K, and moreover the distance between any two points from $\{P_1,\dots,P_n\}$ all lie in a field extension K_0 of K with $[K_0:K]=2^m$ for some non-negative integer m. We see this by adjoining the relevant square-roots of elements of K in sequence, making use of the Tower Law. By squaring and cancelling terms, and squaring again to remove the final square-root, we obtain an equation of the first shape described in part (a), with $c_{ij}\in K_0$. The intersection of such a curve with a line generates points lying in a quadratic field extension, as is the case for ruler-and-compass constructions. If instead we consider the intersection of such a curve with a second such curve (of the second shape described in part (a), with $d_{ij}\in K_0$), then we are in the situation considered in part (a). In such circumstances we find that any point of intersection (x,y) satisfies the property that $[K_0(x,y):K_0]\le 4$. Hence, as a consequence of the Tower Law we conclude that $[K_0(x,y):K]=2^m u$ for some integer u with $1\le u\le 4$.

Now put $M_0=\mathbb{Q}$ and $M_j=M_{j-1}(x_j,y_j)$ $(j\ge 1)$. By part (a), one has $[M_j:M_{j-1}]=2^{m_j}3^{n_j}$ for some $m_j\ge 0$ and $n_j\in\{0,1\}$ for each j. Then it follows from the Tower Law that

$$[M_j:\mathbb{Q}]=[M_j:M_{j-1}][M_{j-1}:M_{j-2}]\dots[M_1:M_0]$$

is a product of terms, each of the shape 2^u3^v, and hence divisible only by 2 or 3. Then $[M_j:\mathbb{Q}]=2^a3^b$ for some $a,b\in\mathbb{Z}_{\ge 0}$. But, again by the Tower Law, since $L_j\subseteq M_j$, we have $[M_j:L_j][L_j:\mathbb{Q}]=[M_j:\mathbb{Q}]=2^a3^b$, so that $[L_j:\mathbb{Q}]$ is a divisor of 2^a3^b. Then we are forced to conclude that $[L_j:\mathbb{Q}]=2^r3^s$ for some $r,s\in\mathbb{Z}_{\ge 0}$, as required.

3. (a) Prove that the polynomial t^5-2 is irreducible over $\mathbb{Q}[t]$.
(b) Prove that $2^{1/5}$ is not constructible by cord-and-nail.

Solution: (a) The polynomial t^5-2 is irreducible over $\mathbb{Q}$, by Eisenstein's criterion using the prime 2, since this polynomial is monic, has 2 dividing all coefficients save the leading coefficient, and 2^2 does not divide the constant term.

(b) Let $\theta=2^{1/5}$. Then θ is a root of the monic irreducible polynomial t^5-2, and hence has the latter as its minimal polynomial over $\mathbb{Q}$. Thus $[\mathbb{Q}(\theta):\mathbb{Q}]=\deg(t^5-2)=5$. But if $\theta=2^{1/5}$ lies in some field L constructible by cord-and-nail, then $\mathbb{Q}(\theta)\subseteq L$. By the tower law and question 2(b), therefore, there exist $r,s\in\mathbb{Z}_{\ge 0}$ having the property that $[L:\mathbb{Q}(\theta)][\mathbb{Q}(\theta):\mathbb{Q}]=2^r3^s$, which implies that 5 divides 2^r3^s. The latter yields a contradiction, and so $2^{1/5}$ is not constructible by cord-and-nail.

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 $\deg f\ge 1$, 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) Write $f=c_0+c_1t+\ldots+c_nt^n$, where $c_n\neq 0$, and suppose that $f(\alpha)=0$. Since $f\in K[t]$, we have $c_i\in K$ for each i. Hence, since τ is a K-homomorphism,

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

(b) If τ is a K-automorphism of L, then $\tau^{-1}:L\to L$ exists and is a K-homomorphism. Thus, as in (a), when $f(\tau(\alpha))=0$, we have $0=\tau^{-1}(f(\tau(\alpha)))=f(\tau^{-1}(\tau(\alpha)))=f(\alpha)$. Thus $f(\alpha)=0$ if and only if $f(\tau(\alpha))=0$.

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

Solution: Suppose first that $K\subseteq L$. Since the identity map ι on L is in $\mathrm{Aut}(L)$, and it leaves K pointwise fixed, we have $\iota\in\mathrm{Gal}(L:K)$. 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 we have $\sigma\circ\tau(\alpha)=\sigma(\tau(\alpha))=\sigma(\alpha)=\alpha$. 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 $\mathrm{Aut}(L)$.