Math 306, Spring 2012
Homework 6 Solutions

(1) (5 pts/part)
   (a) Prove that $\cos(2\pi/5) = \frac{\sqrt{5}-1}{4}$. (Hint: Using the equation $(\cos(2\pi/5) + i\sin(2\pi/5))^5 = 1$, first show that $\alpha = \cos(2\pi/5)$ is a root of $16x^5 - 20x^3 + 5x - 1$, which factors into a linear piece times the square of a quadratic piece.)
   (b) Prove that the regular pentagon is constructible with straightedge and compass.

Solution:
   (a) If we expand $(\cos(2\pi/5) + i\sin(2\pi/5))^5 = 1$ and set the real parts equal, then we have

$$16\cos^5(2\pi/5) - 20\cos^3(2\pi/5) + 5\cos(2\pi/5) - 1 = 0.$$

   Hence $\alpha = \cos(2\pi/5)$ is a root of the polynomial $16x^5 - 20x^3 + 5x - 1 = (x-1)(4x^2+2x-1)^2$. Hence α is a root of $4x^2 + 2x - 1$. Using the quadratic equation, we find that $\alpha = \frac{\sqrt{5}-1}{4}$.
   (b) Let $\alpha = \frac{\sqrt{5}-1}{4}$. Then clearly α is constructible from $\mathbb{Q}$. Therefore $(\cos(2\pi/5), \sin(2\pi/5))$ is constructible, so the regular pentagon is constructible.

(2) (5 pts) Prove that the regular 9-gon is not constructible.

Solution: Suppose that the regular 9-gon is constructible. Then $\cos(2\pi/9)$ is constructible from $\mathbb{Q}$. Using the half-angle formula, we know that $\cos(\pi/9) = \sqrt{\frac{1+\cos(2\pi/9)}{2}}$, so $\cos(\pi/9)$ is constructible, contradicting the result from class.

(3) (3 pts/part) Find subfields of $\mathbb{C}$ which are splitting fields over $\mathbb{Q}$ for the polynomials (i) $t^3 - 1$, (ii) $t^4 - 1$, (iii) $t^4 - 5t^2 + 6$. Please express your answers without using the letter e.

Solution: We have (i) $L = \mathbb{Q}(e^{2\pi i/3}) = \mathbb{Q}(-\frac{1}{2} + \frac{i\sqrt{3}}{2}) = \mathbb{Q}(i\sqrt{3})$, (ii) $L = \mathbb{Q}(i)$, (iii) $L = \mathbb{Q}(\sqrt{2}, \sqrt{3})$.

(4) (2 pts/part) Find the degrees of the field extensions in the previous problem over $\mathbb{Q}$.

Solution: The degrees are (i) $[L\colon \mathbb{Q}] = 2$, (ii) $[L\colon \mathbb{Q}] = 2$, (iii) $[L\colon \mathbb{Q}] = 4$.

(5) (4 pts/part) Determine the splitting field and its degree over $\mathbb{Q}$ for the following polynomials in $\mathbb{Q}[t]$. Here you may use the letter e recklessly.
   (a) $t^4 - 2$
   (b) $t^4 + 2$
   (c) $t^6 - 4$

Solution:
   (a) The splitting field is $L = \mathbb{Q}(\sqrt[4]{2}, e^{2\pi i/4}) = \mathbb{Q}(\sqrt[4]{2}, i)$, so the degree is 8.
   (b) The roots of $t^4 + 2$ are given by $\sqrt[4]{2}e^{\pi i/4}$, $\sqrt[4]{2}e^{3\pi i/4}$, $\sqrt[4]{2}e^{5\pi i/4}$ and $\sqrt[4]{2}e^{7\pi i/4}$. Notice that the quotient of the first two roots is $e^{\pi i/2} = i$. So the splitting field can be expressed as $\mathbb{Q}(\sqrt[4]{2}e^{\pi i/4}, i)$. Now $\sqrt[4]{2}e^{\pi i/4} = \sqrt[4]{2}(\frac{1}{\sqrt{2}} + \frac{i}{\sqrt{2}}) = \frac{1}{\sqrt[4]{2}}(1+i)$. Since i lies in the splitting field, it is clear that the splitting field can be expressed as $\mathbb{Q}(\sqrt[4]{2}, i)$, which has degree 8 over $\mathbb{Q}$.
   (c) The splitting field is $L = \mathbb{Q}(\sqrt[6]{4}, e^{2\pi i/6}) = \mathbb{Q}(\sqrt[3]{2}, \frac{1}{2} + \frac{i\sqrt{3}}{2}) = \mathbb{Q}(\sqrt[3]{2}, i\sqrt{3})$. The degree is 6.

(6) (4 pts/part) Find a splitting field L for $x^3 - 5$ over (a) $\mathbb{Z}_7$, (b) $\mathbb{Z}_{11}$, (c) $\mathbb{Z}_{13}$. Find the degree $[L\colon \mathbb{Z}_p]$ in each case.

Solution:

(a) The polynomial $x^3 - 5$ has no roots in $\mathbb{Z}_7$. Let α be a root of $x^3 - 5$ in some splitting field. Therefore $x^3 - 5 = (x - \alpha)(x - 2\alpha)(x - 4\alpha)$, so $\mathbb{Z}_7(\alpha)$ is a splitting field for $x^3 - 5$ and $[\mathbb{Z}_7(\alpha)\colon \mathbb{Z}_7] = 3$.
(b) We know that $x^3 - 5 = (x - 3)(x^2 + 3x + 9)$ in $\mathbb{Z}_{11}[x]$. Let α be a root of $x^2 + 3x + 9$. Then $x^3 - 5$ splits in $\mathbb{Z}_{11}(\alpha)[x]$, and $[\mathbb{Z}_{11}(\alpha)\colon \mathbb{Z}_{11}] = 2$.
(c) The polynomial $x^3 - 5 = (x + 2)(x + 5)(x + 6)$ in $\mathbb{Z}_{13}[x]$, so $\mathbb{Z}_{13}$ is the splitting field. The degree is 1.

(7) (5 pts/part)
(a) Let p be prime and let $f = t^p - t + 1$ in $\mathbb{Z}_p[t]$. If α is a root of f, prove that $\mathbb{Z}_p(\alpha)$ is a splitting field for f. (Hint: Prove that $\alpha + 1$ is also a root.)
(b) Determine the possible values of $[\mathbb{Z}_p(\alpha)\colon \mathbb{Z}_p]$.

Solution:
(a) Suppose that α is a root of f, i.e. we have $\alpha^p - \alpha + 1 = 0$. Then for all $b \in \mathbb{Z}_p$ we have $(\alpha+b)^p - (\alpha+b) + 1 = \alpha^p + b^p - \alpha - b + 1 = b^p - b$. But for all $b \in \mathbb{Z}_p$ we have $b^p = b$ (certainly it holds for $b = 0$; otherwise, the order of b divides $p - 1$, the order of $\mathbb{Z}_p^\times$, so $b^{p-1} = 1$, or $b^p = b$). Hence it is clear that $\alpha + b$ is a root of f for all $b \in \mathbb{Z}_p$. Therefore, we have identified p roots of f. Since f has at most p roots, these are exactly the roots of f. Hence $\mathbb{Z}(\alpha)$ is the splitting field for f.
(b) For all $b \in \mathbb{Z}_p$, we have $f(b) = 1$, so f has no roots in $\mathbb{Z}_p$. If α is a root of f, then the splitting field $\mathbb{Z}_p(\alpha)$ is a nontrivial extension of $\mathbb{Z}_p$. We will now show that f is irreducible over $\mathbb{Z}_p$. Suppose that $f = f_1 f_2$ for some monic $f_1, f_2 \in \mathbb{Z}_p[x]$ with $\deg f_1 = d < p$. Now since the set of roots of f is $\{\alpha, \alpha+1, \ldots, \alpha+p-1\}$, it follows that the roots of f_1 are a subset of this collection. The coefficient b_{d-1} of x^{d-1} in f_1 is then of the form $b_{d-1} = -d\alpha + t$, where $t \in \mathbb{Z}_p$ (it should be easy to see that the coefficient of x^{d-1} is the negative of the sum of all the roots). Since $b_{d-1} \in \mathbb{Z}_p$, it follows that $\alpha \in \mathbb{Z}_p$, a contradiction. Therefore f is irreducible, so $[\mathbb{Z}_p(\alpha)\colon \mathbb{Z}_p] = p$.

(8) (5 pts) Let $f \in K[x]$ have degree n and let L be a splitting field for f over K. Use induction to prove that $[L\colon K]$ divides $n!$. (Hint: break into two cases, where f is irreducible or reducible; you may use the fact that, if $a, b \in \mathbb{Z}_{\geq 0}$, then $a!\,b!$ divides $(a + b)!$.)

Solution: Clearly, if f has degree 1, then the splitting field for f over K is just K, so $[L\colon K] = 1$, so the claim holds in this case. Suppose that the statement holds for all polynomials g of degree less than n over all fields K'. Now consider a polynomial f of degree n over K.

Case 1: Suppose that f is irreducible in $K[x]$ and let L be its splitting field. Let $\alpha \in L$ be a root of f. Then $f = (x - \alpha)g$ in $K(\alpha)[x]$, where $g \in K(\alpha)[x]$ has degree $n - 1$. Now L is a splitting field for g over $K(\alpha)$, so $[L\colon K(\alpha)]$ divides $(n - 1)!$. Since $[K(\alpha)\colon K] = n$, it follows by the tower law that $[L\colon K]$ divides $n!$.

Case 2: Suppose that f is reducible in $K[x]$, with $f = gh$, where the degrees of g and h are less than n. Let $a = \deg g$ and $b = \deg h$. Let $L' \subseteq L$ be the splitting field of g over K. Then $[L'\colon K]$ divides $a!$ by the induction hypothesis. Clearly L is the splitting field of $h \in L'[x]$. Hence $[L\colon L']$ divides $b!$. By the tower law, we find that $[L\colon K]$ divides $a!\,b!$ which divides $(a + b)! = n!$.

(9) (3 pts/part) Decide which of the following extensions are normal. Give reasons for your answer.
(a) $\mathbb{Q}(t)\colon \mathbb{Q}$, where t is an indeterminate
(b) $\mathbb{Q}(\sqrt[7]{5})\colon \mathbb{Q}$
(c) $\mathbb{Q}(\sqrt{5}, \sqrt[7]{5})\colon \mathbb{Q}$

Solution:
(a) Normal, since $K[t]\colon K$ is normal whenever t is an indeterminate.
(b) Not normal, since $x^7 - 5 \in \mathbb{Q}[x]$ has a root in $\mathbb{Q}(\sqrt[7]{5})$, but does not split.
(c) Not normal, since $x^7 - 5 \in \mathbb{Q}[x]$ has a root in $\mathbb{Q}(\sqrt[7]{5})$, but does not split.

(10) (5 pts) Prove that, if $L\colon K$ is a field extension with $[L\colon K] = 2$, then $L\colon K$ is a normal extension. (Remark: This is analogous to the fact that, if G is a group and H is a subgroup of G with $[G\colon H] = 2$ (the usual index of a subgroup), then H is normal in G.)

Solution: Suppose $L\colon K$ is a field extension with $[L\colon K] = 2$. Suppose that $f \in K[x]$ is irreducible with a root α in L. Then f is quadratic so $f = (x - \alpha)g$ for some $g \in L[x]$. But g is linear, so f must split in $L[x]$. Therefore $L\colon K$ is normal.