Math 306, Spring 2012
Homework 4 Solutions

(1) (2 pts/part) Find the minimal polynomials over the smaller field of the following elements in the given extensions.
(a) $3i$ in $\mathbb{C}\colon \mathbb{Q}$
(b) $\sqrt{18}$ in $\mathbb{R}\colon \mathbb{Q}$
(c) $\sqrt{e}$ in $\mathbb{C}\colon \mathbb{Q}(e)$
(d) $\frac{\sqrt{5}+1}{2}$ in $\mathbb{C}\colon \mathbb{Q}$
(e) $e^{2\pi i/11}$ in $\mathbb{C}\colon \mathbb{Q}$

Solution:
(a) x^2+9
(b) x^2-18
(c) x^2-e
(d) x^2-x-1
(e) $x^{10}+x^9+x^8+\cdots+x+1$

(2) (2 pts/part) Construct simple extensions $\mathbb{Q}(\alpha)\colon \mathbb{Q}$ where α has the following minimum polynomial in $\mathbb{Q}[t]$.
(a) t^2-5
(b) $t^4+t^3+t^2+t+1$
(c) t^3+2

Solution:
(a) $\mathbb{Q}(\sqrt{5})$
(b) $\mathbb{Q}(e^{2\pi i/5})$
(c) $\mathbb{Q}(\sqrt[3]{2}e^{\pi i/3})$

(3) (3 pts/part) All the following statements are false. Provide counterexample for each.
(a) For every finite field K, the polynomial x^2+x+1 is irreducible in $K[x]$.
(b) If $K(\alpha)\colon K$ is a simple field extension, then α is algebraic over K.
(c) There is no nontrivial field extension of $\mathbb{C}(t)$, where t is an indeterminate.
(d) If K is a simple extension of $\mathbb{Q}$, then there are no subfields properly containing $\mathbb{Q}$ which are properly contained in K.
(e) If α has minimum polynomial f over $\mathbb{Q}$, then f factors into linear pieces in $\mathbb{Q}(\alpha)$. (Hint: Consider $\alpha=\sqrt[3]{2}$.)

Solution:
(a) The polynomial x^2+x+1 is reducible in $\mathbb{Z}_3[x]$.
(b) If t is an indeterminate, then $\mathbb{C}(t)\colon \mathbb{C}$ is a simple extension but t is not algebraic over $\mathbb{C}$.
(c) The extension $\mathbb{C}(\sqrt{t})\colon \mathbb{C}(t)$ is nontrivial.
(d) The simple extension $\mathbb{Q}(\sqrt[4]{2})\colon \mathbb{Q}$ contains the intermediate subfield $\mathbb{Q}(\sqrt{2})$.
(e) The polynomial x^3-2 is the minimum polynomial of $\alpha=\sqrt[3]{2}$. The other roots of x^3-2 are complex and so do not belong to $\mathbb{Q}(\sqrt[3]{2})$. Therefore the polynomial does not factor into linear pieces in $\mathbb{Q}(\sqrt[3]{2})$.

(4) (4 pts/part) Let p and q be distinct primes in $\mathbb{Z}$.
(a) Prove that $\mathbb{Q}(\sqrt{p},\sqrt{q})$ is a simple extension of $\mathbb{Q}$.
(b) Prove that $\alpha=\sqrt{p}+\sqrt{q}$ is algebraic over $\mathbb{Q}$ by exhibiting an appropriate quartic polynomial in $\mathbb{Q}[x]$ with α as a root.

Solution:
(a) We claim that $\mathbb{Q}(\sqrt{p},\sqrt{q})=\mathbb{Q}(\sqrt{p}+\sqrt{q})$. Clearly $\mathbb{Q}(\sqrt{p}+\sqrt{q})\subseteq\mathbb{Q}(\sqrt{p},\sqrt{q})$. Now $(\sqrt{p}+\sqrt{q})^3=(p+3q)\sqrt{p}+(q+3p)\sqrt{q}$ belongs to $\mathbb{Q}(\sqrt{p}+\sqrt{q})$. Hence $(2p-2q)\sqrt{q}=(p+3q)\sqrt{p}+(q+3p)\sqrt{q}-(p+3q)(\sqrt{p}+\sqrt{q})$ also belongs to $\mathbb{Q}(\sqrt{p}+\sqrt{q})$. Therefore $\sqrt{q}\in\mathbb{Q}(\sqrt{p}+\sqrt{q})$, and so $\sqrt{p}\in\mathbb{Q}(\sqrt{p}+\sqrt{q})$. Therefore $\mathbb{Q}(\sqrt{p},\sqrt{q})\subseteq\mathbb{Q}(\sqrt{p}+\sqrt{q})$.

(b) If $\alpha = \sqrt{p}+\sqrt{q}$, then $(\alpha - \sqrt{p})^2 = q$, i.e. $\alpha^2 = 2\sqrt{p}\,\alpha + p = q$. Therefore $(\alpha^2 + p - q)^2 = 4p\alpha^2$. Therefore the polynomial $f = x^4 - 2(p+q)x^2 + (p-q)^2$ is a quartic with α as a root.

(5) (3 pts/part) Let $\mathbb{F} = \{a + b\sqrt[3]{2} + c\sqrt[3]{4}\colon\ a, b, c \in \mathbb{Q}\}$.

(a) Prove that $\mathbb{F}$ is closed under multiplication.

(b) Find the multiplicative inverse of $1 - \sqrt[3]{2}$. (Hint: let the inverse be $a + b\sqrt[3]{2} + c\sqrt[3]{4}$ and solve for a, b, c by multiplying out the appropriate equation.)

Solution:

(a) Let $a + b\sqrt[3]{2} + c\sqrt[3]{4}$ and $d + e\sqrt[3]{2} + f\sqrt[3]{4}$ be elements of $\mathbb{F}$. Then $(a + b\sqrt[3]{2} + c\sqrt[3]{4})(d + e\sqrt[3]{2} + f\sqrt[3]{4}) = (ad + 2bf + 2ce) + (bd + ae + 2cf)\sqrt[3]{2} + (af + cd + be)\sqrt[3]{4}$, which belongs to $\mathbb{F}$, so $\mathbb{F}$ is closed under multiplication.

(b) Let $a + b\sqrt[3]{2} + c\sqrt[3]{4}$ be the inverse of $1 - \sqrt[3]{2}$. Then $(a + b\sqrt[3]{2} + c\sqrt[3]{4})(1 - \sqrt[3]{2}) = 1$. Multiply out and collecting coefficients, we have $a - 2c = 1$, $-a + b = 0$ and $c - b = 0$. Therefore $a = b = c = -1$. Therefore the inverse of $1 - \sqrt[3]{2}$ is $-1 - \sqrt[3]{2} - \sqrt[3]{4}$.

(6) (5 pts) Let $\zeta = e^{2\pi i/7}$ be a primitive 7th root of unity. Prove that $\alpha = \zeta + \zeta^{-1}$ is algebraic over $\mathbb{Q}$ by finding a quartic $f \in \mathbb{Q}[x]$ such that $f(\alpha) = 0$. (Hint: Compute α^2, α^3 and α^4 and find a relationship between various powers of α, noticing that $\zeta^3 + \zeta^{-3} = \zeta^4 + \zeta^{-4}$.)

Solution: We compute $\alpha^2 = \zeta^2 + \zeta^{-2} + 2$, $\alpha^3 = \zeta^3 + \zeta^{-3} + 3(\zeta + \zeta^{-1}) = \zeta^3 + \zeta^{-3} + 3\alpha$, $\alpha^4 = \zeta^4 + \zeta^{-4} + 4(\zeta^2 + \zeta^{-2}) + 6 = \alpha^3 - 3\alpha + 4(\alpha^2 - 2) + 6$. Therefore the polynomial $f = x^4 - x^3 - 4x^2 + 3x - 2$ has α as a zero.

(7) (4 pts) Construct fields of order 9 and 125.

Solution: It is easy to see that $x^2 + 1$ is irreducible in $\mathbb{Z}_3[x]$ and $x^3 + x + 1$ is irreducible in $\mathbb{Z}_5[x]$. Hence $\mathbb{Z}_3[x]/(x^2 + 1)$ is a field of order 9 and $\mathbb{Z}_5[x]/(x^3 + x + 1)$ is a field of order 125.