MATH 114: GALOIS THEORY
SPRING 2008/09
PROBLEM SET 5 SOLUTIONS

K will denote a field throughout this problem set.

1. Let $K \leq \Omega$ be a field extension and $\alpha \in \Omega$. Determine $f_K^\alpha(x)$, the irreducible polynomial of α over K, for the following choices of α, K, Ω. For each case, give a subfield $E \leq \Omega$ such that

$$E \cong K[x]/\langle f_K^\alpha(x)\rangle$$

and state the values of $[E : K]$, $[\Omega : E]$, $[\Omega : K]$, $|K|$, $|E|$, and $|\Omega|$.

(a) $\Omega = \mathbb{C}$, $K = \mathbb{R}$, $\alpha = \sqrt{-1}$.

Solution. $f_{\mathbb{R}}^i(x) = x^2 + 1$, irreducible over $\mathbb{R}$ since it has no zeros in $\mathbb{R}$.

$$\mathbb{R}[x]/\langle x^2 + 1\rangle \cong \mathbb{R}(i) = \mathbb{C}$$

and so $E = \mathbb{C}$. $[E : \mathbb{R}] = [\mathbb{C} : \mathbb{R}] = 2$, $[\mathbb{C} : E] = 1$, $|\mathbb{R}| = |E| = |\mathbb{C}| = \infty$.

(b) $\Omega = \mathbb{C}$, $K = \mathbb{R}$, $\alpha = \sqrt[10]{2}$.

Solution. $f_{\mathbb{R}}^{\sqrt[10]{2}}(x) = x - \sqrt[10]{2}$, irreducible over $\mathbb{R}$ since it has degree 1.

$$\mathbb{R}[x]/\langle x - \sqrt[10]{2}\rangle \cong \mathbb{R}$$

and so $E = \mathbb{R}$. $[E : \mathbb{R}] = 1$, $[\mathbb{C} : \mathbb{R}] = [\mathbb{C} : E] = 2$, $|\mathbb{R}| = |E| = |\mathbb{C}| = \infty$.

(c) $\Omega = \mathbb{C}$, $K = \mathbb{Q}$, $\alpha = \sqrt[10]{2}$.

Solution. $f_{\mathbb{Q}}^{\sqrt[10]{2}}(x) = x^{10} - 2$, irreducible over $\mathbb{Q}$ by Eisenstein criterion with $p = 2$ and Gauss lemma.

$$\mathbb{Q}[x]/\langle x^{10} - 2\rangle \cong \mathbb{Q}(\sqrt[10]{2})$$

and so $E = \mathbb{Q}(\sqrt[10]{2})$. $[E : \mathbb{Q}] = 10$. $[\mathbb{C} : \mathbb{Q}] = \infty$ since $\mathbb{C}$ contains trancendental numbers and so $[\mathbb{C} : E] = \infty$ by Theorem **6** in the lectures. $|\mathbb{Q}| = |E| = |\mathbb{C}| = \infty$.

(d) $\Omega = \mathbb{R}$, $K = \mathbb{Q}$, $\alpha = \sqrt[10]{2}$.

Solution. $f_{\mathbb{Q}}^{\sqrt[10]{2}}(x) = x^{10} - 2$, irreducible over $\mathbb{Q}$ by Eisenstein criterion with $p = 2$ and Gauss lemma.

$$\mathbb{Q}[x]/\langle x^{10} - 2\rangle \cong \mathbb{Q}(\sqrt[10]{2})$$

and so $E = \mathbb{Q}(\sqrt[10]{2})$. $[E : \mathbb{Q}] = 10$. $[\mathbb{R} : \mathbb{Q}] = \infty$ since $\mathbb{R}$ contains trancendental numbers and so $[\mathbb{R} : E] = \infty$ by Theorem **6** in the lectures. $|\mathbb{Q}| = |E| = |\mathbb{R}| = \infty$.

(e) $\Omega = \mathbb{C}$, $K = \mathbb{Q}$, $\alpha = \sqrt{1 + \sqrt{3}}$.

Solution. Since $\alpha = \sqrt{1 + \sqrt{3}}$. So $\alpha^2 = 1 + \sqrt{3}$. So $(\alpha^2 - 1)^2 = 3$. So $\alpha^4 - 2\alpha^2 - 2 = 0$. Hence $f_{\mathbb{Q}}^{\sqrt{1+\sqrt{3}}}(x) = x^4 - 2x^2 - 2$; it is irreducible over $\mathbb{Q}$ by Eisenstein criterion with $p = 2$ and Gauss lemma.

$$\mathbb{Q}[x]/\langle x^4 - 2x^2 - 2\rangle \cong \mathbb{Q}(\sqrt{1 + \sqrt{3}})$$

and so $E = \mathbb{Q}(\sqrt{1 + \sqrt{3}})$. $[E : \mathbb{Q}] = 4$. $[\mathbb{C} : \mathbb{Q}] = \infty$ since $\mathbb{C}$ contains trancendental numbers and so $[\mathbb{C} : E] = \infty$ by Theorem **6** in the lectures. $|\mathbb{Q}| = |E| = |\mathbb{C}| = \infty$.

Date: April 24, 2009 (Version 1.0).

(f) $\Omega = \mathbb{C}$, $K = \mathbb{R}$, $\alpha = \sqrt{\pi}$.

SOLUTION. $f_{\mathbb{R}}^{\sqrt{\pi}}(x) = x - \sqrt{\pi}$, irreducible over $\mathbb{R}$ since it has degree 1.

$$\mathbb{R}[x]/\langle x - \sqrt{\pi}\rangle \cong \mathbb{R}$$

and so $E = \mathbb{R}$. $[E : \mathbb{R}] = 1$, $[\mathbb{C} : \mathbb{R}] = [\mathbb{C} : E] = 2$, $|\mathbb{R}| = |E| = |\mathbb{C}| = \infty$.

(g) $\Omega = \mathbb{R}$, $K = \mathbb{Q}$, $\alpha = \sqrt{\pi}$.

SOLUTION. We need to show that $\sqrt{\pi}$ is transcendental over $\mathbb{Q}$. If $f(x) \in \mathbb{Q}[x]$ is such that $f(\sqrt{\pi}) = 0$, then we may move all odd degree terms to the RHS and factor out $\sqrt{\pi}$ and square both sides; this gives $g(x) \in \mathbb{Q}[x]$ such that $g(\pi) = 0$ — a contradiction since π is trancendental. Hence $f_{\mathbb{Q}}^{\sqrt{\pi}}(x)$ is undefined. So E does not exist.

(h) $\Omega = \mathbb{R}$, $K = \mathbb{Q}$, $\alpha = \pi^2$.

SOLUTION. We need to show that π^2 is transcendental over $\mathbb{Q}$. If $f(x) \in \mathbb{Q}[x]$ is such that $f(\pi^2) = 0$, then $g(x) = f(x^2) \in \mathbb{Q}[x]$ is such that $g(\pi) = 0$ — a contradiction since π is trancendental. Hence $f_{\mathbb{Q}}^{\pi^2}(x)$ is undefined. So E does not exist.

(i) $\Omega = \mathbb{R}$, $K = \mathbb{Q}(\pi)$, $\alpha = \sqrt{\pi}$.

SOLUTION. We need to first show $\sqrt{\pi} \notin \mathbb{Q}(\pi)$. Let $f(x), g(x) \in \mathbb{Q}[x]$ be such that $\sqrt{\pi} = f(\pi)/g(\pi)$. We may assume $\gcd(f(x), g(x)) = 1$ WLOG. Then $f(x)^2 - xg(x)^2 \in \mathbb{Q}[x]$ has π as a zero — a contradiction (since π is trancendental) unless $f(x)^2 - xg(x)^2$ is the zero polynomial. But if

$$f(x)^2 = xg(x)^2,$$

then $x \mid f(x)^2$; so $x \mid f(x)$; so $x^2 \mid f(x)^2$; so $x^2 \mid xg(x)^2$; so $x \mid g(x)^2$; so $x \mid g(x)$. But $\gcd(f(x), g(x)) = 1$ and we get a contradiction. Hence $f_{\mathbb{Q}(\pi)}^{\sqrt{\pi}}(x) = x^2 - \pi$; it is irreducible over $\mathbb{Q}(\pi)$ since $\sqrt{\pi} \notin \mathbb{Q}(\pi)$.

$$\mathbb{Q}(\pi)[x]/\langle x^2 - \sqrt{\pi}\rangle \cong \mathbb{Q}(\pi)(\sqrt{\pi}) = \mathbb{Q}(\pi, \sqrt{\pi}) = \mathbb{Q}(\sqrt{\pi})(\pi) = \mathbb{Q}(\sqrt{\pi})$$

where the last step follows because $\pi \in \mathbb{Q}(\sqrt{\pi})$. So $E = \mathbb{Q}(\sqrt{\pi})$ and $[E : \mathbb{Q}(\pi)] = 2$. As $\mathbb{R}$ contains $\sqrt[2^n]{\pi}$ where n can be arbitrarily large and we may show using the same argument as before that

$$\mathbb{R} \gneq \cdots \gneq \mathbb{Q}(\sqrt[8]{\pi}) \gneq \mathbb{Q}(\sqrt[4]{\pi}) \gneq \mathbb{Q}(\sqrt{\pi}) \gneq \mathbb{Q}(\pi)$$

where $[\mathbb{Q}(\sqrt[2^n]{\pi}) : \mathbb{Q}(\sqrt[2^{n-1}]{\pi})] = 2$. So $[\mathbb{R} : \mathbb{Q}(\pi)] \geq [\mathbb{Q}(\sqrt[2^n]{\pi}) : \mathbb{Q}(\pi)] = 2^n$ and $[\mathbb{R} : E] \geq [\mathbb{Q}(\sqrt[2^n]{\pi}) : E] \geq 2^{n-1}$ for any $n \in \mathbb{N}$. Hence $[\mathbb{R} : E] = [\mathbb{R} : \mathbb{Q}(\pi)] = \infty$. $|\mathbb{Q}(\pi)| = |E| = |\mathbb{R}| = \infty$.

(j) $\Omega = \mathbb{R}$, $K = \mathbb{Q}(\pi)$, $\alpha = \pi^2$.

SOLUTION. $f_{\mathbb{Q}(\pi)}^{\pi^2}(x) = x - \pi^2$, irreducible over $\mathbb{Q}(\pi)$ since it has degree 1.

$$\mathbb{Q}(\pi)[x]/\langle x - \pi^2\rangle \cong \mathbb{Q}(\pi)$$

and so $E = \mathbb{Q}(\pi)$. $[E : \mathbb{R}] = 1$, $[\mathbb{C} : \mathbb{R}] = [\mathbb{C} : E] = 2$, $|\mathbb{R}| = |E| = |\mathbb{C}| = \infty$.

(k) $\Omega = \mathbb{Q}(\pi)$, $K = \mathbb{Q}(\pi^3)$, $\alpha = \pi^2$.

SOLUTION. We need to first show $\pi^2 \notin \mathbb{Q}(\pi^3)$. Let $f(x), g(x) \in \mathbb{Q}[x]$ be such that $\pi^2 = f(\pi^3)/g(\pi^3)$. We may assume $\gcd(f(x), g(x)) = 1$ WLOG. Then $f(x^3) - x^2 g(x^3) \in \mathbb{Q}[x]$ has π as a zero — a contradiction (since π is trancendental) unless $f(x^3) - x^2 g(x^3)$ is the zero polynomial. But if

$$f(x^3) = x^2 g(x^3),$$

then $x^2 \mid f(x^3)$; so $f(0) = f'(0) = 0$. In particular $x \mid f(x)$. Differentiating the above equation, we get

$$3x^2 f'(x^3) = 2xg(x^3) + 3x^4 g'(x^3),$$
$$3xf'(x^3) = 2g(x^3) + 3x^3 g'(x^3).$$

Plugging in $x = 0$, we get $g(0) = 0$ which means $x \mid g(x)$. But $\gcd(f(x), g(x)) = 1$ and we get a contradiction. Hence $f^{\pi^2}_{\mathbb{Q}(\pi^3)}(x) = x^3 - (\pi^3)^2 = x^3 - \pi^6$; it is irreducible over $\mathbb{Q}(\pi)$ since $\pi^2 \notin \mathbb{Q}(\pi^3)$.

$$\mathbb{Q}(\pi^3)[x]/\langle x^3 - \pi^6\rangle \cong \mathbb{Q}(\pi^3)(\pi^2) = \mathbb{Q}(\pi^2, \pi^3) = \mathbb{Q}(\pi)$$

where the last step follows because $\pi = \pi^3/\pi^2 \in \mathbb{Q}(\pi^2, \pi^3)$. So $E = \mathbb{Q}(\pi)$. $[E : \mathbb{Q}(\pi^3)] = [\mathbb{Q}(\pi) : \mathbb{Q}(\pi^3)] = 3$, $[\mathbb{Q}(\pi) : E] = 1$, $|\mathbb{Q}(\pi)| = |E| = |\mathbb{Q}(\pi^3)| = \infty$.

(l) $\Omega = \mathbb{R}$, $K = \mathbb{Q}(\sin\theta)$, $\alpha = \sin\frac{\theta}{3}$ where $\theta \in \mathbb{R}$.
SOLUTION. Using usual trigonometric identities, we see that

$$\sin\theta = 3\sin\frac{\theta}{3} - 4\sin^3\frac{\theta}{3}$$

and so $\sin\frac{\theta}{3}$ is always a zero of

$$4x^3 - 3x + \sin\theta \in \mathbb{Q}(\sin\theta)[x].$$

The degree of $f^{\sin\theta/3}_{\mathbb{Q}(\sin\theta)}(x)$ can be $1, 2, 3$ depending on the value of θ. For example, if $\theta \equiv \pi/2 \bmod 2\pi$, then

$$f^{\sin\theta/3}_{\mathbb{Q}(\sin\theta)}(x) = f^{1/2}_{\mathbb{Q}}(x) = x - \frac{1}{2}$$

(irreducible since linear) and so $E = \mathbb{Q}$ and $[E : \mathbb{Q}] = 1$. If $\theta \equiv \pi \bmod 2\pi$, then

$$f^{\sin\theta/3}_{\mathbb{Q}(\sin\theta)}(x) = f^{\sqrt{3}/2}_{\mathbb{Q}}(x) = x^2 - \frac{3}{4}$$

(irreducible since $\sqrt{3} \notin \mathbb{Q}$) and so $E = \mathbb{Q}(\sqrt{3})$ and $[E : \mathbb{Q}] = 2$. If $\theta \equiv \pi/6 \bmod 2\pi$, then

$$f^{\sin\theta/3}_{\mathbb{Q}(\sin\theta)}(x) = f^{\sin\theta/3}_{\mathbb{Q}}(x) = 4x^3 - 3x + \frac{1}{2}$$

(irreducible by Gauss lemma since $8x^3-6x+1$ has no linear factors over $\mathbb{Z}$ — $\pm1, \pm1/2, \pm1/4, \pm1/8$ are all not zeros of the polynomial) and so $E = \mathbb{Q}(\sin\theta/3)$ has $[E : \mathbb{Q}] = 3$. In all cases, $[\mathbb{R} : \mathbb{Q}] = [\mathbb{R} : E] = \infty$ and $|\mathbb{R}| = |E| = |\mathbb{Q}| = \infty$.

(m) $\Omega = \mathbb{Z}_2(\phi)$, $K = \mathbb{Z}_2$, $\alpha = \phi$ where ϕ is a root of $x^2 + x + 1 \in \mathbb{Z}_2[x]$.
SOLUTION. Since $1^2 + 1 + 1 \not\equiv 0 \bmod 2$ and $0^2 + 0 + 1 \not\equiv 0 \bmod 2$, $x^2 + x + 1$ has no zeros in $\mathbb{Z}_2$ and must be irreducible over $\mathbb{Z}_2$. Hence $f^{\phi}_{\mathbb{Z}_2}(x) = x^2 + x + 1$.

$$\mathbb{Z}_2[x]/\langle x^2 + x + 1\rangle \cong \mathbb{Z}_2(\phi)$$

and so $E = \mathbb{Z}_2(\phi)$. $[E : \mathbb{Z}_2] = [\mathbb{Z}_2(\phi) : \mathbb{Z}_2] = 2$, $[\mathbb{Z}_2(\phi) : E] = 1$. $|\mathbb{Z}_2| = 2$. By Theorem **2** in the lectures, $\mathbb{Z}_2(\phi) = \mathbb{Z}_2[\phi] = \{a + b\phi \mid a, b \in \mathbb{Z}_2\}$ and since there are two choices for the two coefficients a, b, $|E| = |\mathbb{Z}_2(\phi)| = 4$.

(n) $\Omega = \mathbb{Z}_3(i)$, $K = \mathbb{Z}_3$, $\alpha = i$ where i is a root of $x^2 + 1 \in \mathbb{Z}_3[x]$.
SOLUTION. Since $(\pm1)^2 + 1 \not\equiv 0 \bmod 3$ and $0^2 + 1 \not\equiv 0 \bmod 3$, $x^2 + 1$ has no zeros in $\mathbb{Z}_3$ and must be irreducible over $\mathbb{Z}_3$. Hence $f^{i}_{\mathbb{Z}_3}(x) = x^2 + 1$.

$$\mathbb{Z}_3[x]/\langle x^2 + 1\rangle \cong \mathbb{Z}_3(i)$$

and so $E = \mathbb{Z}_3(i)$. $[E : \mathbb{Z}_3] = [\mathbb{Z}_3(i) : \mathbb{Z}_3] = 2$, $[\mathbb{Z}_3(i) : E] = 1$. $|\mathbb{Z}_3| = 3$. By Theorem **2** in the lectures, $\mathbb{Z}_3(i) = \mathbb{Z}_3[i] = \{a + bi \mid a, b \in \mathbb{Z}_3\}$ and since there are three choices for the two coefficients a, b, $|E| = |\mathbb{Z}_3(i)| = 6$.

2. Let $K \leq \Omega$ be a field extension and let $\alpha \in \Omega$ be transcendental over K.

(a) Let $\beta \in K(\alpha)$ and $\beta \notin K$. Show that β is also transcendental over K.
SOLUTION. Since $\beta \in K(\alpha)$, $\beta = p(\alpha)/q(\alpha)$ for some $p(x), q(x) \in K[x]$. Suppose β is algebraic over K. Then we also have $f(\beta) = 0$ for some $f(x) \in K[x]$. Let $\deg f(x) = n \geq 1$. Multiplying the equation $f(p(\alpha)/q(\alpha)) = 0$ by $q(\alpha)^n$, we obtain a polynomial in α with coefficients in K which is equal to zero, implying that α is algebraic over K, a contradiction.

Therefore there is no such nonzero polynomial expression $f(\beta) = 0$, i.e. β is transcendantal over K.

(b) Let $\gamma \in \Omega$ and suppose α is algebraic over $K(\gamma)$. Prove that γ is algebraic over $K(\alpha)$.
SOLUTION. Every element of $K(\gamma)$ can be expressed as a quotient of polynomials in γ with coefficients in K. Because α is algebraic over $K(\gamma)$, there is a polynomial expression in α with coefficients in $K(\gamma)$ which is equal to zero. By multiplying this equation by the polynomial in γ which is the product of the denominators of the coefficients in this equation, we obtain a polynomial in α equal to zero and having as coefficients polynomials in γ. Now a polynomial in α with coefficients that are polynomials in γ can be formally rewritten as a polynomial in γ with coefficients that are polynomials in α. [Recall from the lectures that $(K[x])[y] = (K[y])[x]$.] This polynomial expression is still zero, which shows that is algebraic over $K(\alpha)$.

3. Prove that the set

$$F = \{a + b\sqrt[3]{2} + c\sqrt[3]{4} \in \mathbb{R} \mid a, b, c \in \mathbb{Q}\}$$

is a subfield of $\mathbb{R}$ by showing that $F = \mathbb{Q}(\sqrt[3]{2})$. Show that every element in $\mathbb{Q}(\sqrt[3]{2})$ has a *unique* representation in the form $a + b\sqrt[3]{2} + c\sqrt[3]{4}$ for some $a, b, c \in \mathbb{Q}$. Express $(1 - \sqrt[3]{2})^{-1}$ in this form.
SOLUTION. We know that $x^3 - 2$ is irreducible in $\mathbb{Q}[x]$ by the Eisenstein condition with $p = 2$ and Gauss lemma. Therefore $\sqrt[3]{2}$ is algebraic of degree 3 over $\mathbb{Q}$. By Theorem **2** in the lectures, $\mathbb{Q}(\sqrt[3]{2}) = \mathbb{Q}[\sqrt[3]{2}]$ (as subsets of $\mathbb{R}$) and so $\mathbb{Q}(\sqrt[3]{2})$ consists of all elements of $\mathbb{R}$ of the form $a + b\sqrt[3]{2} + c(\sqrt[3]{2})^2$ for $a, b, c \in \mathbb{Q}$. The give set F consists of precisely these elements of $\mathbb{R}$, so the given set is the field $\mathbb{Q}(\sqrt[3]{2})$. The ring homomorphism $\varphi : \mathbb{Q}[x] \to \mathbb{Q}(\sqrt[3]{2})$ in Theorem **2** has $\ker \varphi = \langle x^3 - 2 \rangle$. If

$$a + b\sqrt[3]{2} + c\sqrt[3]{4} = a' + b'\sqrt[3]{2} + c'\sqrt[3]{4}$$

then

$$(a - a') + (b - b')\sqrt[3]{2} + (c - c')\sqrt[3]{4} = 0.$$

Since $\varphi(x) = \sqrt[3]{2}$,

$$\varphi((a - a') + (b - b')x + (c - c')x^2) = 0,$$

we get

$$(a - a') + (b - b')x + (c - c')x^2 \in \ker \varphi = \langle x^3 - 2 \rangle$$

and thus

$$x^3 - 2 \mid (a - a') + (b - b')x + (c - c')x^2$$

which is only possible if

$$a = a', \quad b = b', \quad c = c'.$$

Hence such expressions are unique. Observe that

$$(1 - \sqrt[3]{2})(-1 - \sqrt[3]{2} - \sqrt[3]{4}) = 1,$$

and so we have

$$(1 - \sqrt[3]{2})^{-1} = -1 - \sqrt[3]{2} - \sqrt[3]{4}.$$