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

K will denote a field throughout this problem set.

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

\[ E \cong K[x]/(f_\Omega^K(x)) \]

and state the values of [E : K], [Ω : E], [Ω : K], |K|, |E|, and |Ω|.

(a) \( Ω = \mathbb{C}, \ K = \mathbb{R}, \ α = \sqrt{-1} \).

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

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

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

(b) \( Ω = \mathbb{C}, \ K = \mathbb{R}, \ α = \sqrt[3]{2} \).

Solution. \( f_{\mathbb{R}}^{\sqrt[3]{2}}(x) = x - \sqrt[3]{2} \), irreducible over \( \mathbb{R} \) since it has degree 1.

\[ \mathbb{R}[x]/(x - \sqrt[3]{2}) \cong \mathbb{R} \]

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

(c) \( Ω = \mathbb{C}, \ K = \mathbb{Q}, \ α = \sqrt[3]{2} \).

Solution. \( f_{\mathbb{Q}}^{\sqrt[3]{2}}(x) = x^3 - 2, \) irreducible over \( \mathbb{Q} \) by Eisenstein criterion with \( p = 2 \) and Gauss lemma.

\[ \mathbb{Q}[x]/(x^3 - 2) \cong \mathbb{Q}(\sqrt[3]{2}) \]

and so \( E = \mathbb{Q}(\sqrt[3]{2}) \). \( [E : \mathbb{Q}] = 3 \) since \( \mathbb{C} \) contains transcendental numbers and so \( [\mathbb{C} : \mathbb{Q}] = \infty \) by Theorem 6 in the lectures. \( |\mathbb{Q}| = |E| = |\mathbb{C}| = \infty \).

(d) \( Ω = \mathbb{R}, \ K = \mathbb{Q}, \ α = \sqrt[3]{2} \).

Solution. \( f_{\mathbb{Q}}^{\sqrt[3]{2}}(x) = x^3 - 2, \) irreducible over \( \mathbb{Q} \) by Eisenstein criterion with \( p = 2 \) and Gauss lemma.

\[ \mathbb{Q}[x]/(x^3 - 2) \cong \mathbb{Q}(\sqrt[3]{2}) \]

and so \( E = \mathbb{Q}(\sqrt[3]{2}) \). \( [E : \mathbb{Q}] = 3 \) since \( \mathbb{R} \) contains transcendental numbers and so \( [\mathbb{R} : \mathbb{Q}] = \infty \) by Theorem 6 in the lectures. \( |\mathbb{Q}| = |E| = |\mathbb{R}| = \infty \).

(e) \( Ω = \mathbb{C}, \ K = \mathbb{Q}, \ α = \sqrt{1 + \sqrt{3}} \).

Solution. Since \( α = \sqrt{1 + \sqrt{3}} \). So \( α^2 = 1 + \sqrt{3} \). So \( (α^2 - 1)^2 = 3 \). So \( α^4 - 2α^2 - 2 = 0 \).

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.

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

and so \( E = \mathbb{Q}(\sqrt{1 + \sqrt{3}}) \). \( [E : \mathbb{Q}] = 4 \). \( [\mathbb{C} : \mathbb{Q}] = \infty \) since \( \mathbb{C} \) contains transcendental numbers and so \( [\mathbb{C} : \mathbb{E}] = \infty \) by Theorem 6 in the lectures. \( |\mathbb{Q}| = |E| = |\mathbb{C}| = \infty \).
(f) \( \Omega = \mathbb{C}, K = \mathbb{R}, \alpha = \sqrt{\pi}. \)

**Solution.** \( f^\sqrt{\pi}_{\mathbb{R}}(x) = x - \sqrt{\pi}, \) irreducible over \( \mathbb{R} \) since it has degree 1.

\[ \mathbb{R}[x]/(x - \sqrt{\pi}) \cong \mathbb{R} \]

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 \( \pi \) is transcendental. Hence \( f^\sqrt{\pi}_{\mathbb{Q}}(x) \) is undefined. So \( E \) does not exist.

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

**Solution.** We need to show that \( \pi^2 \) 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 \( \pi \) is transcendental. Hence \( f^\pi_{\mathbb{Q}}(x) \) 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 \( \pi \) as a zero — a contradiction (since \( \pi \) is transcendental) 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 \( f^\sqrt{\pi}_{\mathbb{Q}(\pi)}(x) = x^2 - \pi; \) it is irreducible over \( \mathbb{Q}(\pi) \) since \( \sqrt{\pi} \notin \mathbb{Q}(\pi) \)

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

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 \( \sqrt[4]{\pi} \) where \( n \) can be arbitrarily large and we may show using the same argument as before that

\[ \mathbb{R} \geq \cdots \geq \mathbb{Q}(\sqrt[4]{\pi}) \geq \mathbb{Q}(\sqrt{\pi}) \geq \mathbb{Q}(\sqrt{\pi}) \geq \mathbb{Q}(\pi) \]

where \( [\mathbb{Q}(\sqrt[4]{\pi}) : \mathbb{Q}(\sqrt[4]{\pi}^{-1})] = 2. \) So \( [\mathbb{R} : \mathbb{Q}(\pi)] \geq [\mathbb{Q}(\sqrt[4]{\pi}) : \mathbb{Q}(\pi)] = 2^n \) and \( [\mathbb{R} : \mathbb{E}] \geq [\mathbb{Q}(\sqrt[4]{\pi}) : \mathbb{E}] = 2^{n+1} \) for any \( n \in \mathbb{N}. \) Hence \( [\mathbb{R} : \mathbb{E}] = [\mathbb{R} : \mathbb{Q}(\pi)] = \infty. \) \( |\mathbb{Q}(\pi)| = |E| = |\mathbb{R}| = \infty. \)

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

**Solution.** \( f^\pi_{\mathbb{Q}(\pi)}(x) = x - \pi^2, \) irreducible over \( \mathbb{Q}(\pi) \) since it has degree 1.

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

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

(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 \( f(x^3) - x^2g(x^3) \in \mathbb{Q}[x] \) has \( \pi \) as a zero — a contradiction (since \( \pi \) is transcendental) unless \( f(x^3) - x^2g(x^3) \) is the zero polynomial. But if

\[ f(x^3) = x^2g(x^3), \]

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

\[ 3x^2f'(x^3) = 2xg(x^3) + 3x^4g'(x^3), \]

\[ 3xf'(x^3) = 2g(x^3) + 3x^3g'(x^3). \]
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 $f_{Q(\pi^3)}^2(x) = x^3 - (\pi^3)^2 = x^3 - \pi^6$; it is irreducible over $Q(\pi)$ since $\pi^2 \notin Q(\pi^3)$.

$Q(\pi^3)[x]/(x^3 - \pi^6) \cong Q(\pi^3)(\pi^2) = Q(\pi^2, \pi^3) = Q(\pi)$

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

(l) $\Omega = R, K = Q(\sin \theta), \alpha = \sin \frac{\theta}{3}$ 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

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

The degree of $f_{Q(\sin \theta)}(x)$ can be $1, 2, 3$ depending on the value of $\theta$. For example, if $\theta \equiv \pi/2 \mod 2\pi$, then

$$f_{Q(\sin \theta)}(x) = f_{Q}^1(x) = x - \frac{1}{2}$$

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

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

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

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

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

(m) $\Omega = Z_2(\phi), K = Z_2, \alpha = \phi$ where $\phi$ is a root of $x^2 + x + 1 \in Z_2[x]$.

**SOLUTION.** Since $1^2 + 1 + 1 \neq 0 \mod 2$ and $0^2 + 0 + 1 \neq 0 \mod 2, x^2 + x + 1$ has no zeros in $Z_2$ and must be irreducible over $Z_2$. Hence $f_{Z_2}^2(x) = x^2 + x + 1$.

$$Z_2[x]/(x^2 + x + 1) \cong Z_2(\phi)$$

and so $E = Z_2(\phi), [E : Z_2] = [Z_2(\phi) : Z_2] = 2, [Z_2(\phi) : E] = 1, |Z_2| = 2$. By Theorem 2 in the lectures, $Z_2(\phi) = Z_2[\phi] = \{a + b\phi \mid a, b \in Z_2\}$ and since there are two choices for the two coefficients $a, b, |E| = |Z_2(\phi)| = 4$.

(n) $\Omega = Z_3(i), K = Z_3, \alpha = i$ where $i$ is a root of $x^2 + 1 \in Z_3[x]$.

**SOLUTION.** Since $(\pm 1)^2 + 1 \neq 0 \mod 3$ and $0^2 + 1 \neq 0 \mod 3, x^2 + 1$ has no zeros in $Z_3$ and must be irreducible over $Z_3$. Hence $f_{Z_3}^1(x) = x^2 + 1$.

$$Z_3[x]/(x^2 + 1) \cong Z_3(i)$$

and so $E = Z_3(i), [E : Z_3] = [Z_3(i) : Z_3] = 2, [Z_3(i) : E] = 1, |Z_3| = 3$. By Theorem 2 in the lectures, $Z_3(i) = Z_3[i] = \{a + bi \mid a, b \in Z_3\}$ and since there are three choices for the two coefficients $a, b, |E| = |Z_3(i)| = 6$.

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 $\beta$ 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 $\beta$ 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 $\alpha$ with coefficients in $K$ which is equal to zero, implying that $\alpha$ is algebraic over $K$, a contradiction.
Therefore there is no such nonzero polynomial expression \( f(\beta) = 0 \), i.e. \( \beta \) is transcendental over \( K \).

(b) Let \( \gamma \in \Omega \) and suppose \( \alpha \) is algebraic over \( K(\gamma) \). Prove that \( \gamma \) is algebraic over \( K(\alpha) \).

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

3. Prove that the set

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

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 \( a + b\sqrt[3]{2} + c\sqrt[4]{4} \) 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 given 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 \( \varphi : \mathbb{Q}[x] \rightarrow \mathbb{Q}(\sqrt[3]{2}) \) in Theorem 2 has \( \ker \varphi = \langle x^3 - 2 \rangle \). If

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

then

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

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

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

and so we have

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