ALGEBRA II SOLUTIONS

Final Report, 2011.06.08

1.

(1)

$x^6 + x^5 + x^3 + x + 1 = (x^2 + x + 1)^3$ is not irreducible over $\mathbb{Z}_2$.

(2)

$\Sigma_{i=1}^{n} y^{p(n-i)} x^{pi} + 1 = (\Sigma_{i=1}^{n} y^{(ni)} x^i)^p + 1 = (\Sigma_{i=1}^{n} y^{(n-i)} x^i + 1)^p$ is not irreducible over $F(y)$.

(3)

$x^4 - 4x^2 + 5 = (x^2 - 2 - i)(x^2 - 2 + i)$ is not irreducible over $\mathbb{Q}(i)$.

(4)

Let $f(x) = x^4 - 4x^3 + 3x^2 + 2x - 2 + \sqrt{3}$ and $g(x) = f(x+1) = x^4 - 3x^2 + \sqrt{3}$. Since

$$g(x) = (x^2 - \frac{3}{2} + \frac{\sqrt{3}}{2}i)(x^2 - \frac{3}{2} - \frac{\sqrt{3}}{2}i),$$

which has no root in $\mathbb{Q}(\sqrt{3})$.(Since $x^2 - \frac{3}{2} + \frac{\sqrt{3}}{2}i$ and $x^2 - \frac{3}{2} - \frac{\sqrt{3}}{2}i$ has no root in $\mathbb{Q}(\sqrt{3})$.) Assume

$$g(x) = (x^2 + ax + b)(x^2 - ax + c),$$

then $g(x) = x^4 + (b + c - a^2)x^2 + (ac - ab)x + bc$. That is $bc = \sqrt{3}$, $ac - ab = 0$, $b + d - a^2 = -3$. If $a = 0$, then $b = -\frac{3}{2} + \frac{\sqrt{3}}{2}i \notin \mathbb{Q}(\sqrt{3})$, $c = -\frac{3}{2} - \frac{\sqrt{3}}{2}i \notin \mathbb{Q}(\sqrt{3})$. If $b = c$, then $b = c = \sqrt[4]{3} \notin \mathbb{Q}(\sqrt{3})$. So $g(x)$ is irreducible over $\mathbb{Q}(\sqrt{3})$, and hence $f(x)$ is irreducible over $\mathbb{Q}(\sqrt{3})$.

(5)

Let $f(x) = x^4 + 2x^2 + x + 3$. Since $f(1) = 7$, $f(-1) = 5$, $f(3) = 105$ and $f(-3) = 99$, by Gauss Lemma $f(x)$ has no root in $\mathbb{Q}$. Assume

$$f(x) = (x^2 + ax + 1)(x^2 - ax + 3),$$

where $a \in \mathbb{Q}$, then $f(x) = x^4 + (-a^2 + 4)x^2 + 2ax + 3$. That is $2a = 1$ and $-a^2 + 4 = 2$, which is impossible. Assume

$$f(x) = (x^2 + ax - 1)(x^2 - ax - 3),$$

where $a \in \mathbb{Q}$, then $f(x) = x^4 + (-a^2 - 4)x^2 - 2ax + 3$. That is $-2a = 1$ and $-a^2 - 4 = 2$, which is impossible. So $f(x)$ is irreducible over $\mathbb{Q}$.
2.

It's clear that the roots of $x^3 - 2$ are $\sqrt[3]{2}$, $\sqrt[3]{2}\omega$ and $\sqrt[3]{2}\omega^2$, where $\omega = \dfrac{-1 + \sqrt{3}i}{2}$. Note that

(1)

$$\mathbb{Q}(\sqrt[3]{2}, \sqrt[3]{2}\omega, \sqrt[3]{2}\omega^2) = \mathbb{Q}(\sqrt[3]{2})(\sqrt[3]{2}\omega)(\sqrt[3]{2}\omega^2) = \mathbb{Q}(\sqrt[3]{2})(\omega)(\sqrt[3]{2}\omega^2) = \mathbb{Q}(\sqrt[3]{2})(\omega) = \mathbb{Q}(\omega)(\sqrt[3]{2})$$

and the minimal polynomial of ω and $\sqrt[3]{2}$ are $x^2 + x + 1$ and $x^3 - 2$,
(2) The roots of $x^2 + x + 1$ are ω and ω^2.

Since $\forall \varphi \in Aut_{\mathbb{Q}}(\mathbb{Q}(\omega, \sqrt[3]{2}))$ sends the roots of $x^2 + x + 1$ to the roots of itself and sends the roots of $x^3 - 2$ to the roots of itself, $Aut_{\mathbb{Q}}(\mathbb{Q}(\omega, \sqrt[3]{2})) = \{a, b, c, d, e, f\}$, where a satisfies the conditions (I)(a), b satisfies the conditions (I)(b), c satisfies the conditions (I)(c), d satisfies the conditions (II)(a), e satisfies the conditions (II)(b), f satisfies the conditions (II)(c) and (I), (II), (a), (b), (c) in the table below.

(I) $\omega \longmapsto \omega$ (II) $\omega \longmapsto \omega^2$

(a) $\sqrt[3]{2} \longmapsto \sqrt[3]{2}$ (b) $\sqrt[3]{2} \longmapsto \sqrt[3]{2}\omega$ (c) $\sqrt[3]{2} \longmapsto \sqrt[3]{2}\omega^2$

In fact, $a = id$, $b = df = ed = fe$, $c = de = ef = fd$ and $d^2 = id$, $e^2 = id$, $f^2 = id$, hence $Aut_{\mathbb{Q}}(\mathbb{Q}(\omega, \sqrt[3]{2})) = \{id, df, fd, d, e, f\} \cong S_3$ which is Galois (Since the fixed field is $\mathbb{Q}$). And it's has the subgroups $\{id, f\}$, $\{id, e\}$, $\{id, d\}$, $\{id, df, fd\}$, and the intermediate fields are $\{id, f\}' = \mathbb{Q}(\sqrt[3]{2}\omega)$, $\{id, e\}' = \mathbb{Q}(\sqrt[3]{2}\omega^2)$, $\{id, d\}' = \mathbb{Q}(\sqrt[3]{2})$, $\{id, df, fd\}' = \mathbb{Q}(\omega)$.

3.

It's clear that $K(u^2) \subseteq K(u)$. Let $f(x) = x^2 - u^2 \in K(u^2)[x]$. Since $f(x) = x^2 - u^2 \in K(u^2)[x]$, which is irreducible over $K(u^2)$ and u is a root of $f(x)$. So $[K(u) : K(u^2)] \leq 2$. If $[K(u) : K(u^2)] = 2$, then $[K(u) : K] = [K(u) : K(u^2)]\,[K(u^2) : K] = 2\,[K(u^2) : K]$, but $[K(u) : K]$ is odd, which is impossible. Therefore $[K(u) : K(u^2)] = 1$, that is $K(u) = K(u^2)$ and hence $[K(u^2) : K]$ is odd.

4.

Since every permutation can be split as the product of 2-cycles, S_n is generated by all the two cycles in S_n.

Since $\begin{pmatrix} i & j \end{pmatrix} = \begin{pmatrix} 1 & i \end{pmatrix}\begin{pmatrix} 1 & j \end{pmatrix}\begin{pmatrix} 1 & i \end{pmatrix}$ for each $i \neq j$ and $1 \leq i, j \leq n$, S_n is generated by $\begin{pmatrix} 1 & i \end{pmatrix}$ for $i = 2, ..., n$.

Since $\begin{pmatrix} i-1 & i \end{pmatrix} = \begin{pmatrix} 1 & i-1 \end{pmatrix}\begin{pmatrix} 1 & i \end{pmatrix}\begin{pmatrix} 1 & i-1 \end{pmatrix}$ for $i = 2, ..., n$, S_n is generated by $\begin{pmatrix} i-1 & i \end{pmatrix}$ for $i = 2, ..., n$.

Since $\begin{pmatrix} i-1 & i \end{pmatrix} = \tau^{i-2}\sigma\tau^{-i+2}$ for $i = 2, ..., n$, S_n is generated by σ and τ.

5.

Consider $F = \mathbb{Z}_2(u^2)$, where u is transcendental over $\mathbb{Z}_2$, and consider $K = \mathbb{Z}_2(u)$ which is an extension field of F. Let $f(x) = x^2 - u^2$ in $F[x]$, then $f(x) = (x-u)^2$ in $K[x]$ and u is a root of multiplicity 2

6.

Let $g(x) \in F[x]$ be the minimal polynomial of v, then $q = [F(v) : F] = deg(g)$.
Since $g(x) \in F[x] \subset F(u)[x]$ with root v, $[F(u,v) : F(u)] \leq q$.
So we have

$$[F(u,v) : F] = [F(u,v) : F(u)]\,[F(u) : F] \leq pq.$$

Since

$$[F(u,v) : F] = [F(u,v) : F(u)]\,[F(u) : F] = p\,[F(u,v) : F(u)]$$

and

$$[F(u,v) : F] = [F(u,v) : F(v)]\,[F(v) : F] = q\,[F(u,v) : F(v)]\,,$$

$p \mid [F(u,v) : F]$ and $q \mid [F(u,v) : F]$.
Since $gcd(p,q) = 1$, $pq \mid [F(u,v) : F]$. Hence $[F(u,v) : F] = pq$.

7.

By Theorem 5.6.5, there exists an extension field L of F containing all roots of $x^{p^n} - x$. Let $K \subseteq L$ be the set of all roots of $x^{p^n} - x$, and it's clear that $0, 1 \in K$. Let $a, b, c \in K$ and $a \neq 0, b \neq 0, c \neq 0$, then a, b, c are roots of $x^{p^n} - x$. That is $a^{p^n} - a = 0$, $b^{p^n} - b = 0$, $c^{p^n} - c = 0$.

(1) Since $(a+b)^{p^n} = a^{p^n} + b^{p^n} = a + b$ and $(ab)^{p^n} = a^{p^n} \cdot b^{p^n} = ab$, $a + b$ and ab are roots of $x^{p^n} - x$. That is $a + b, ab \in K$.

(2) Since $(\frac{1}{a})^{p^n} = \frac{1}{a^{p^n}} = \frac{1}{a}$, $\frac{1}{a}$ is a root of $x^{p^n} - x$. That is $\frac{1}{a} \in K$.

(3) Since $a, b, c \in F(a,b,c)$ and $F(a,b,c)$ is a field, $a + b = b + a$, $a + (b + c) = (a + b) + c$, $a(b \cdot c) = (a \cdot b)c$, $a(b + c) = ab + ac$ and $(a + b)c = ac + bc$ are holds.

(4) Note that $(-a)^{p^n} = (-1)^{p^n} \cdot a^{p^n}$. If $p = 2$, then $(-a)^{2^n} = (-1)^{2^n} \cdot a^{2^n} = a^{2^n} = a = -a$. ($-1 = 1$ in the field with characteristic 2) That is $(-a)^{2^n} - (-a) = 0$. If $p > 2$, then $(-a)^{p^n} = -a^{p^n} = -a$. ($p^n$ is odd) That is $(-a)^{p^n} - (-a) = 0$. Hence $(-a) \in K$.

From (1)(2)(3)(4) we conclude that K is a field.