Math 517 **Spring 2007** **Radford**

Written Homework # 4 Solution [1]

04/25/07

This homework set is a workout in Sections 6.1 and 6.2 of the ClassNotes.

1. (**25 points**) (1) (**5**) By the Eisenstein Criterion $x^{10} - 34 \in \mathbf{Q}[x]$ is irreducible with $p = 2$ (or 17). Therefore $x^{10} - 34$ this is the minimal polynomial of $\sqrt[10]{34}$ over $\mathbf{Q}$ by 6.2.1(5). The degree of $\sqrt[10]{34}$ is 3 by 6.2.1(2).

(**10**) Ditto, by the Eisenstein Criterion $x^3 - 21 \in \mathbf{Q}[x]$ is irreducible with $p = 3$ (or 7). Thus $x^3 - 21$ this is the minimal polynomial of $\sqrt[3]{21}$ over $\mathbf{Q}$ by 6.2.1(5). The degree of $\sqrt[3]{21}$ is 3 by 6.2.1(2). By 6.1.6 both $\mathbf{Q}[\sqrt[10]{34}]$ and $\mathbf{Q}[\sqrt[3]{21}]$ are finite field extensions of $\mathbf{Q}$.

Let $K = \mathbf{Q}[\sqrt[10]{34}][\sqrt[3]{21}] = \mathbf{Q}[\sqrt[3]{21}][\sqrt[10]{34}]$. Since $\sqrt[3]{21}$ is a root of $x^3 - 21 \in \mathbf{Q}[\sqrt[10]{34}]$ it follows that $[K : \mathbf{Q}[\sqrt[10]{34}]] \leq 3$ by 6.1.6. Therefore

$$[K : \mathbf{Q}] = [K : \mathbf{Q}[\sqrt[10]{34}]][\mathbf{Q}[\sqrt[10]{34}] : \mathbf{Q}] \leq 3{\cdot}10 = 30$$

by 6.1.1. Now $10 = [\mathbf{Q}[\sqrt[10]{34}] : \mathbf{Q}]$ and $3 = [\mathbf{Q}[\sqrt[3]{21}] : \mathbf{Q}]$ divide $[K : \mathbf{Q}]$ by 6.2.1(2). Therefore $30 \leq [K : \mathbf{Q}]$. As $[K : \mathbf{Q}] \leq 30$ we conclude $[K : \mathbf{Q}[\sqrt[10]{34}]] = 30$.

(2) (**5**) Since

$$30 = [K : \mathbf{Q}] = [K : \mathbf{Q}[\sqrt[3]{21}]][\mathbf{Q}[\sqrt[3]{21}] : \mathbf{Q}] = [K : \mathbf{Q}[\sqrt[3]{21}]]{\cdot}3$$

it follows that $[K : \mathbf{Q}[\sqrt[3]{21}]] = 10$. Since $x^{10} - 34 \in \mathbf{Q}[\sqrt[3]{21}]$ is monic of degree 10 and has root $\sqrt[10]{34}$ it follows that $\mathrm{m}_{\mathbf{Q}[\sqrt[3]{21}],\ \sqrt[10]{34}}(x) = x^{10} - 34$ by 6.2.1(5).

(3) (**5**) Since

$$30 = [K : \mathbf{Q}] = [K : \mathbf{Q}[\sqrt[10]{34}]][\mathbf{Q}[\sqrt[10]{34}] : \mathbf{Q}] = [K : \mathbf{Q}[\sqrt[10]{34}]]{\cdot}10$$

[1] Slightly revised 04/26/07.

it follows that $[K:\mathbf{Q}[\sqrt[10]{34}]]=3$. Since $x^3-21\in\mathbf{Q}[\sqrt[10]{34}]$ is monic of degree 3 and has root $\sqrt[3]{21}$ it follows that $\mathrm{m}_{\mathbf{Q}[\sqrt[10]{34}],\ \sqrt[3]{21}}(x)=x^3-21$ by 6.2.1(5).

2. (**25 points**) (1) (**10**) By the Eisenstein Criterion $x^3-n\in\mathbf{Q}[x]$ is irreducible. As $a\in\mathbf{R}$ is a root of this polynomial it follows by 6.1.6 that a is algebraic over $\mathbf{Q}$ and by 6.2.1 that $m_{\mathbf{Q},a}(x)=x^3-n$ and $[\mathbf{Q}[a]:\mathbf{Q}]=3$. Now $\{1,a,a^2\}$ is a basis for $K=\mathbf{Q}[a]$ over $\mathbf{Q}$ by 6.1.7.

(2) (**15**) Since $\{1,a,a^2\}$ is a basis for K over $\mathbf{Q}$ and all $r\in\mathbf{Q}$ can be written $r=r1+0a+0a^2$, it follows that $b=r+sa\notin\mathbf{Q}$ since $s\neq 0$. Now $\operatorname{Deg} m_{\mathbf{Q},a}(x)$ divides $[K:\mathbf{Q}]=3$ by 6.2.1(3). Since $b\notin\mathbf{Q}$ necessarily $\operatorname{Deg} m_{\mathbf{Q},a}(x)=3$. By 6.2.1(5) any monic polynomial $f(x)\in\mathbf{Q}[x]$ of degree 3 which has b as a root is $m_{\mathbf{Q},b}(x)$.

There are a couple of ways to find such an $f(x)$. One is to note that b^3 is a $\mathbf{Q}$-linear of $\{1,b,b^2\}$ by 6.1.7 and then find such a relation. From

$$b=r1+sa,\quad b^2=r^21+2rsa+s^2a^2,$$

and

$$b^3=r^3+3r^2sa+3rs^2a^2+s^3a^3=(r^3+s^3n)1+(3r^2s)a+(3rs^2)a^2$$

we deduce

$$b^3=(r^3+s^3n)1-3r^2b+3rb^2.$$

Another way is to note that $a=\dfrac{1}{s}(b-r)$ and therefore

$$n=a^3=\frac{1}{s^3}(b^3-3b^2r+3br^2-r^3))$$

which leads to

$$b^3-3b^2r+3br^2-r^3-s^3n=0.$$

Therefore

$$\mathrm{m}_{\mathbf{Q},b}(x)=x^3-3rx^2+3r^2x-r^3-ns^3.$$

3. (**25 points**) (1) (**7**) Note that $\sqrt{2}$ is a root of $x^2-2\in\mathbf{Q}[x]$. For the reasons cited in the solution to Problem 2 we can conclude that $\mathbf{Q}[\sqrt{2}]$ is an algebraic extension of $\mathbf{Q}$ of degree 2 and $\mathbf{Q}[\sqrt{2}]$ has $\mathbf{Q}$-basis $\{1,\sqrt{2}\}$.

Suppose that $a = \sqrt{1+\sqrt{2}} \in \mathbf{Q}[\sqrt{2}]$. Then $a = r1 + s\sqrt{2}$ for some $r, s \in \mathbf{Q}$. Squaring a yields

$$1+\sqrt{2} = a^2 = r^2 + 2rs\sqrt{2} + 2s^2 = (r^2+2s^2)1 + 2rs\sqrt{2}$$

which holds if and only if

$$r^2 + 2s^2 = 1 \qquad \text{and} \qquad 2rs = 1.$$

Thus $r \neq 0$ (and incidently $1-2rs = 0$; can't divide by this!!!!!). Substituting $s = \dfrac{1}{2r}$ into the first equation yields

$$2r^4 - 2r^2 + 1 = 0.$$

But then r^2 is a root of $2x^2 - 2x + 1$ which has no real roots by the quadratic formula, contradiction. (One student noted that $2r^2$ is a rational root of $x^2 - 2x + 2$ which is impossible by Eisenstein again.) Therefore $a \notin \mathbf{Q}[\sqrt{2}]$.

(2) (**12**) Since a is a root of $x^2 - (1+\sqrt{2}) \in \mathbf{Q}[\sqrt{2}][x]$ it follows that $[\mathbf{Q}[\sqrt{2}][a] : \mathbf{Q}[\sqrt{2}]] \leq 2$ by 6.1.6. Let $E = \mathbf{Q}[\sqrt{2}][a]$. Since $a \notin \mathbf{Q}[\sqrt{2}]$ necessarily $[E : \mathbf{Q}[\sqrt{2}]] = 2$. Thus $[E : \mathbf{Q}] = 4$ by 6.1.1. By 6.2.1(5) we deduce that $\mathrm{m}_{\mathbf{Q}[\sqrt{2}],a}(x) = x^2 - (1+\sqrt{2})$ and, as $(a^2-1)^2 = 2$, or equivalently $a^4 - 2a^2 - 1 = 0$, $\mathrm{m}_{\mathbf{Q},a}(x) = x^4 - 2x^2 - 1$.

(3) (**6**) We note that

$$\begin{aligned}
\mathrm{m}_{\mathbf{Q},a}(x) &= x^4 - 2x^2 - 1 \\
&= (x^2-1)^2 - 2 \\
&= ((x^2-1) - \sqrt{2})((x^2-1) + \sqrt{2}) \\
&= (x^2 - (1+\sqrt{2}))(x^2 + (\sqrt{2}-1)) \\
&= (x - \sqrt{1+\sqrt{2}})(x + \sqrt{1+\sqrt{2}})(x - \imath\sqrt{\sqrt{2}-1})(x + \imath\sqrt{\sqrt{2}-1})
\end{aligned}$$

Since $E \subseteq \mathbf{R}$ and $\imath\sqrt{\sqrt{2}-1} \notin \mathbf{R}$ and is a root of $x^2 + (\sqrt{2}-1) \in E[x]$, $[K : E] = 2$ and therefore $[K : \mathbf{Q}] = [K : E][E : \mathbf{Q}] = 8$ by 6.1.1.

There is a simpler description of K. Observe that

$$(\imath\sqrt{\sqrt{2}-1})(\sqrt{1+\sqrt{2}}) = \imath\sqrt{(\sqrt{2}-1)(\sqrt{2}+1)} = \imath\sqrt{2-1} = \imath.$$

Therefore $\imath \in K$ which means

$$K = E[\imath] = \mathbf{Q}[\sqrt{2}, \sqrt{1+\sqrt{2}}, \imath].$$

4. (**25 points**) (1) (**10**) Let $a \in K$. The statement "$a \notin K_{alg}$ implies a is transcendental over K_{alg}", that is "$a \notin K_{alg}$ implies a is not algebraic over K_{alg}", is logically equivalent to its contrapositive "a algebraic over K_{alg} implies $a \in K_{alg}$". We show the latter.

Suppose that a is algebraic over K_{alg}. Then $K_{alg}[a]$ is an algebraic extension of K_{alg} by 6.1.6 and 6.2.2(1). By definition K_{alg} is an algebraic extension of F. Therefore $K_{alg}[a]$ is an algebraic extension of F by 6.2.2(3). By definition of algebraic extension $a \in K_{alg}$.

(2) (**5**) By definition $\{1, a, a^2, \ldots\}$ is linearly independent over F. Generally for vectors spaces over F, non-empty subsets of linearly independent subsets are linearly independent. Therefore $\{1, 1^n, a^{2n}, \ldots\}$ is linearly independent which means that a^n is transcendental over F by definition.

(**10**) Since a is a root of $x^n - a^n \in F(a^n)$ it follows that a is algebraic over $F(a^n)$ and $[F(a^n)[a] : F(a^n)] \leq n$ by 6.1.6. Since a is algebraic over $F(a^n)$ we have $F(a) = F(a^n)(a) = F(a^n)[a]$ by 6.1.5(2). Therefore $[F(a) : F(a^n)] \leq n$. To complete the proof we need only show that $\{1, a, \ldots, a^{n-1}\}$ is linearly independent over $F(a^n)$.

Since a^n is transcendental over F the ring $F[a^n]$ is a polynomial ring in indeterminant a^n over F. The elements of $F(a^n)$ are quotients of polynomials in $F[a^n]$. Suppose that

$$\frac{f_0(a^n)}{g_0(a^n)} + \frac{f_1(a^n)}{g_1(a^n)}a + \cdots + \frac{f_{n-1}(a^n)}{g_{n-1}(a^n)}a^{n-1} = 0,$$

where $f_i(a^n), g_i(a^n) \in F[a^n]$ and $g_i(a^n) \neq 0$ for all $0 \leq i \leq n-1$. "Clearing denominators" by multiplying both sides of the equation above by the product $g_0(a^n) \cdots g_{n-1}(a^n)$ results in

$$\sum_{i=0}^{n-1} g_0(a^n) \cdots g_{i-1}(a^n) \widehat{g_i(a^n)} g_{i+1}(a^n) \cdots g_{n-1}(a^n) f_i(a^n) a^i = 0,$$

where $\widehat{\ }$ means factor omitted. Now

$$g_0(a^n) \cdots g_{i-1}(a^n) \widehat{g_i(a^n)} g_{i+1}(a^n) \cdots g_{n-1}(a^n) f_i(a^n) a^i$$

is an F-linear combination of powers of the type $a^{\ell n+i}$, where $\ell \geq 0$. Since $n\mathbf{Z}$, $1+n\mathbf{Z}, \ldots, (n-1)+n\mathbf{Z}$, the left cosets of $n\mathbf{Z}$ in $\mathbf{Z}$, are disjoint and a is transcendental over F,

$$g_0(a^n)\cdots g_{i-1}(a^n)\widehat{g_i(a^n)}g_{i+1}(a^n)\cdots g_{n-1}(a^n)f_i(a^n)a^i = 0$$

for all $0 \leq i \leq n-1$. Since $F[a]$ is an integral domain $f_i(a^n) = 0$ for all $0 \leq i \leq n-1$. Therefore

$$\frac{f_0(a^n)}{g_0(a^n)} = \frac{f_1(a^n)}{g_1(a^n)} = \cdots = \frac{f_{n-1}(a^n)}{g_{n-1}(a^n)} = 0$$

which shows that $\{1, a, \ldots, a^{n-1}\}$ is linearly independent.