MATH 431 Written Homework 6 Solution Radford 04/13/2009

---

1. Page 377, number 6: (**20 points**) Regard $g(x) \in F[x]$ as a polynomial with coefficients in $F[a]$ and let b be a zero of $g(x)$ belonging to some field extension of $F[a]$. We need only show that $\operatorname{Deg} g(x) = [F[a][b] : F[a]]$ (**4**).

Now $m = [F[a][b] : F[a]] \leq \operatorname{Deg} g(x)$ since $g(b) = 0$ (**3**). By Theorem 21.5 note $[F[a][b] : F] = [F[a][b] : F[a]][F[a] : F] = m\operatorname{Deg} f(x)$ (**3**). On the other hand, from the relations $F \subseteq F[a], F[b] \subseteq F[a,b] = F[a][b]$ we deduce that $\operatorname{Deg} f(x) = [F[a] : F]$ and $\operatorname{Deg} g(x) = [F[b] : F]$ divide $[F[a][b] : F] = m\operatorname{Deg} f(x)$ by the same theorem (**3**). Since $\operatorname{Deg} f(x), \operatorname{Deg} g(x)$ are relatively prime $\operatorname{Deg} g(x)\operatorname{Deg} f(x)$ divides $m\operatorname{Deg} f(x)$ (**3**). Therefore $\operatorname{Deg} g(x) = m = [F[a][b] : F[a]]$ as $m \leq \operatorname{Deg} g(x)$ (**4**).

2. Page 378, number 8: (**20 points**) First of all $\mathbf{Q}[\sqrt{15}] \subseteq \mathbf{Q}[\sqrt{3}+\sqrt{5}]$ since $(\sqrt{3}+\sqrt{5})^2 = 3+2\sqrt{15}+5 = 8+2\sqrt{15}$ implies $\sqrt{15} \in \mathbf{Q}[\sqrt{3}+\sqrt{5}]$ (**3**).

We show that $\mathbf{Q}[\sqrt{3}+\sqrt{5}] = \mathbf{Q}[\sqrt{3},\sqrt{5}]$. The left hand side of the equation is contained in the right. The right hand side is contained in the left as from the calculation $(\sqrt{5}+\sqrt{3})(\sqrt{5}-\sqrt{3}) = 5-2 = 2$ it follows that $\sqrt{5}+\sqrt{3}, \sqrt{5}-\sqrt{3} \neq 0$, $(\sqrt{5}+\sqrt{3})^{-1} = (1/2)(\sqrt{5}-\sqrt{3})$, and thus $\sqrt{5},\sqrt{3} \in \mathbf{Q}[\sqrt{3}+\sqrt{5}]$ as these elements are rational linear combinations of $\sqrt{5}+\sqrt{3}, \sqrt{5}-\sqrt{3}$ (**3**).

Let $a = \sqrt{3}+\sqrt{5}$. We have shown that $a^2 - (8+2\sqrt{15}) = 0$. Thus a is a root of $p(x) = x^2 - (8+2\sqrt{15}) \in \mathbf{Q}[\sqrt{15}]$. Therefore $[\mathbf{Q}[\sqrt{3}+\sqrt{5}] : \mathbf{Q}[\sqrt{15}]] \leq 2$. We will show that this dimension is 2 which means a has degree 2 over $\mathbf{Q}[\sqrt{15}]$ and thus $\{1, \sqrt{3}+\sqrt{5}\}$ is a basis for $\mathbf{Q}[\sqrt{3}+\sqrt{5}]$ over $\mathbf{Q}$ (**3**).

Suppose $[\mathbf{Q}[\sqrt{3}+\sqrt{5}] : \mathbf{Q}[\sqrt{15}]] = 1$. Then $\mathbf{Q}[\sqrt{3}+\sqrt{5}] = \mathbf{Q}[\sqrt{15}] = \mathbf{Q}[\sqrt{3},\sqrt{5}]$. Now $x^2-15, x^2-3, x^2-5 \in \mathbf{Q}[x]$ are irreducible by the Eisenstein Condition with $p = 3,3,5$ respectively. In particular 3, 5, 15 have no rational square roots and $\{1,\sqrt{15}\}$ is a basis for $\mathbf{Q}[\sqrt{15}]$ over $\mathbf{Q}$. Thus $\sqrt{5} = r1 + s\sqrt{15}$ for some $r, s \in \mathbf{Q}$. Squaring both sides of this equation we have $5 = (r^2+15s^2)1 + 2rs\sqrt{15}$. Therefore $5 = r^2+15s^2$ and $2rs = 0$. Exactly one of r and s is zero. If $r = 0$ then $5 = s^{-2}$ and if $s = 0$ then $5 = r^2$. In both cases we have a contradiction. We have shown $[\mathbf{Q}[\sqrt{3}+\sqrt{5}] : \mathbf{Q}[\sqrt{15}]] = 2$ (**3**).

For the second part observe that $\mathbf{Q}[2^{1/2}, 2^{1/3}, 2^{1/4}] = \mathbf{Q}[2^{1/3}, 2^{1/4}]$ since $(2^{1/4})^2 = 2^{1/2}$. Now $x^3-2, x^4-2 \in \mathbf{Q}[x]$ are irreducible by the Eisenstein condition with $p = 2$. Thus $[\mathbf{Q}[2^{1/3}, 2^{1/4}] : \mathbf{Q}] = 12$ (**2**) by our solution to Problem 1 above; $[\mathbf{Q}[2^{1/3}, 2^{1/4}] : \mathbf{Q}[2^{1/3}]] = 4$ and $\mathbf{Q}[2^{1/3}, 2^{1/4}]$ has basis $\{1, 2^{1/4}, 2^{2/4}, 2^{3/4}\}$ over $\mathbf{Q}[2^{1/3}]$ (**2**); $[\mathbf{Q}[2^{1/3}] : \mathbf{Q}] = 3$ and $\mathbf{Q}[2^{1/3}]$ has basis $\{1, 2^{1/3}, 2^{2/3}\}$ over $\mathbf{Q}$ (**2**). A basis for $\mathbf{Q}[2^{1/3}, 2^{1/4}]$ over $\mathbf{Q}$ is obtained by multiplying these two bases (**2**).

3. Page 378, number 14: (**20 points**) Let $a = \sqrt{-3}+\sqrt{2} = \sqrt{2}+\sqrt{3}\,\imath$ and $F = \mathbf{Q}[a]$. By the calculation $(\sqrt{2}+\sqrt{3}\,\imath)(\sqrt{2}-\sqrt{3}\,\imath) = (\sqrt{2})^2 - (\sqrt{3}\,\imath)^2 = 5$ we deduce neither factor is zero and $a^{-1} = (1/5)(\sqrt{2}-\sqrt{3}\,\imath)$. Therefore $\sqrt{2}+\sqrt{3}\,\imath, \sqrt{2}-\sqrt{3}\,\imath \in F$ which means $\sqrt{2}, \sqrt{3}\,\imath \in F$ and $F = \mathbf{Q}[\sqrt{2}, \sqrt{3}\,\imath]$ (**4**).

Now $\mathbf{Q}[\sqrt{2} : \mathbf{Q}] = 2$ as $\sqrt{2}$ is a root of $x^2 - 2 \in \mathbf{Q}[x]$ and is irreducible by the Eisenstein Criterion with $p = 2$ (**4**). Since $\sqrt{3}\,\imath \notin \mathbf{Q}[\sqrt{2}]$ and $(\sqrt{3}\,\imath)^2 = -3 \in \mathbf{Q}[\sqrt{2}]$ it follows that $[\mathbf{Q}[\sqrt{2}][\sqrt{3}\,\imath] : \mathbf{Q}[\sqrt{2}]] = 2$ (**4**). Therefore $[F : \mathbf{Q}] = 4$ by Theorem 21.5 (**4**).

Therefore the minimal polynomial of a over $\mathbf{Q}$ has degree 4; it is the only monic polynomial of degree 4 which has a as a root. $a^2 = (\sqrt{2} + \sqrt{3}\,\imath)^2 = 2 + 2\sqrt{6}\,\imath - 3$, so $a^2 + 1 = 2\sqrt{6}\,\imath$. Hence $(a^2 + 1)^2 = -24$ so $a^4 + 2a^2 + 25 = 0$. The minimal polynomial of a over $\mathbf{Q}$ is $x^4 + 2x^2 + 25$ (**4**).

4. Page 378, number 18: (**20 points**) We need to assume $E \subseteq \mathbf{C}$ for this problem. Since $[E : \mathbf{Q}] = 2$ there is an $\alpha \in E \backslash \mathbf{Q}$. Choose any such α. Then $E = \mathbf{Q}[\alpha]$ and α is a root of a quadratic $x^2 + bx + c \in \mathbf{Q}[x]$ (**4**). The completing the square calculation

$$0 = \alpha^2 + b\alpha + c = (\alpha + b/2)^2 + (c - b^2/4)$$

shows that $\beta = \alpha + b/2$ is a root of $x^2 - r \in \mathbf{Q}[x]$, where $r = b^2/4 - c$ (**4**). Note $E = \mathbf{Q}[\beta]$.

Write $\beta^2 = m/n$ where $m, n \in \mathbf{Z}$ and $n > 0$ (**4**). Since $\sqrt{m/n} = (1/n)\sqrt{mn}$, $E = \mathbf{Q}[\beta] = \mathbf{Q}[\sqrt{m/n}] = \mathbf{Q}[\sqrt{mn}]$ (**4**). Write $mn = \ell^2 d$, where $\ell, d \in \mathbf{Z}$ and d is square free. Since $\sqrt{mn} = \pm\ell\sqrt{d}$ we have $E = \mathbf{Q}[\sqrt{mn}] = \mathbf{Q}[\sqrt{d}]$ as required (**4**).

5. Page 379, number 28: (**20 points**) Since $a \in \mathbf{C}$ is algebraic over $\mathbf{Q}$, $F = \mathbf{Q}[a]$ is an algebraic extension of $\mathbf{Q}$ (**7**). Write $r = m/n$ where $m, n \in \mathbf{Z}$ and $n > 0$. Since $a^{1/n}$ is a root of $x^n - a \in F[x]$, $E = F[a^{1/n}]$ is an algebraic extension of F (**7**). Therefore E is an algebraic extension of $\mathbf{Q}$ by Theorem 21.7. Since $a^r = (a^{1/n})^m \in E$ it follows that a^r is algebraic over $\mathbf{Q}$ (**6**).