MATH 431 Written Homework 5 Solution Radford 04/09/2009

1. Page 349, number 30: (**20 points**) Let $w \in W$ (**5**). Then $T(v) = w$ for some $v \in V$ since T is onto (**5**). Since $\{v_1, \ldots, v_n\}$ spans V there are $a_1, \ldots, a_n \in F$ such that $v = a_1v_1 + \cdots + a_nv_n$ (**5**). Since T is linear $w = T(v) = T(a_1v_1 + \cdots + a_nv_n) = aT(v_1) + \cdots + a_nT(v_n)$ (**5**). Therefore $\{T(v_1), \ldots, T(v_n)\}$ spans W.

2. Page 365, number 2: (**20 points**) First note $\mathbf{Q}(\sqrt{2}, \sqrt{3})$ is the smallest subfield of $\mathbf{R}$ which contains $\mathbf{Q}\cup\{\sqrt{2}, \sqrt{3}\}$, more informally which contains $\mathbf{Q}$, $\sqrt{2}$, and $\sqrt{3}$. Likewise $\mathbf{Q}(\sqrt{2} + \sqrt{3})$ is the smallest subfield of $\mathbf{R}$ which contains $\mathbf{Q}$ and $\sqrt{2} + \sqrt{3}$. To show $\mathbf{Q}(\sqrt{2} + \sqrt{3}) = \mathbf{Q}(\sqrt{2}, \sqrt{3})$ we show both are contained in each other.

Since $\sqrt{2}, \sqrt{3} \in \mathbf{Q}(\sqrt{2}, \sqrt{3})$, $\sqrt{2}+\sqrt{3} \in \mathbf{Q}(\sqrt{2}, \sqrt{3})$ and consequently $\mathbf{Q}(\sqrt{2}+\sqrt{3}) \subseteq \mathbf{Q}(\sqrt{2}, \sqrt{3})$ (**5**).

Now

$$\frac{1}{\sqrt{2}+\sqrt{3}} = \left(\frac{1}{\sqrt{2}+\sqrt{3}}\right)\left(\frac{\sqrt{2}-\sqrt{3}}{\sqrt{2}-\sqrt{3}}\right) = \frac{\sqrt{2}-\sqrt{3}}{2-3} = \sqrt{3}-\sqrt{2}.$$

Since $(\sqrt{2}+\sqrt{3})^{-1} \in \mathbf{Q}(\sqrt{2}+\sqrt{3})$, $\sqrt{3}-\sqrt{2}, \sqrt{3}+\sqrt{2} \in \mathbf{Q}(\sqrt{2}+\sqrt{3})$ which means

$$\sqrt{3} = \frac{1}{2}((\sqrt{3}-\sqrt{2}) + (\sqrt{3}+\sqrt{2})) \in \mathbf{Q}(\sqrt{2}+\sqrt{3}) \ \ (\mathbf{5})$$

and thus $\sqrt{2} = (\sqrt{3}+\sqrt{2}) - \sqrt{3} \in \mathbf{Q}(\sqrt{2}+\sqrt{3})$ also (**5**). Since $\sqrt{2}, \sqrt{3} \in \mathbf{Q}(\sqrt{2}+\sqrt{3})$, $\mathbf{Q}(\sqrt{2}, \sqrt{3}) \subseteq \mathbf{Q}(\sqrt{2}+\sqrt{3})$ (**5**).

Comment: Noting that

$$\begin{aligned}(\sqrt{2}+\sqrt{3})^3 &= \sqrt{2}^3 + 3\sqrt{2}^2\sqrt{3} + 3\sqrt{2}\sqrt{3}^2 + \sqrt{3}^3 \\ &= 2\sqrt{2} + 6\sqrt{3} + 9\sqrt{2} + 3\sqrt{3} \\ &= 11\sqrt{2} + 9\sqrt{3}\end{aligned}$$

one can also show that $\sqrt{2}, \sqrt{3} \in \mathbf{Q}(\sqrt{2}+\sqrt{3})$.

3. Page 365, number 4: (**20 points**) Suppose $\omega \in \mathbf{C}$ satisfies $\omega^4 = -1$. Then ω is a root of $x^4 + 1$. Let $\imath = \sqrt{-1}$. Since $(\imath^\ell)^4 = (\imath^4)^\ell = 1^\ell = 1$ for all $\ell \in \mathbf{Z}$, $(\imath^\ell\omega)^4 = (\imath^\ell)^4\omega^4 = 1(-1) = -1$. Thus $\omega, \imath\omega, \imath^2\omega, \imath^3\omega$ are 4 distinct roots of x^4+1. Therefore

$$x^4 + 1 = (x-\omega)(x-\imath\omega)(x-\imath^2\omega)(x-\imath^3\omega).$$

Thus a splitting field of x^4+1 over $\mathbf{Q}$ is $F = \mathbf{Q}(\omega, \imath\omega, \imath^2\omega, \imath^3\omega)$. Since $\omega^4 = -1$, $\omega^2 = \pm\imath$. Therefore $F = \mathbf{Q}(\omega)$. We may take $\omega = \sqrt{\imath}$.

Comment: Note that $\omega^8 = (\omega^4)^2 = (-1)^2 = 1$. We may take

$$\omega = e^{2\pi\imath/8} = \cos(2\pi/8) + \imath\sin(2\pi/8) = \frac{1}{\sqrt{2}}(1+\imath).$$

Show that the square of $\dfrac{1}{\sqrt{2}}(1+\imath)$ is $\imath$.

4. Page 366, number 12: (**20 points**) This was a challenge. We use the fact that π is transcendental over $\mathbf{Q}$, that is if $f(x) \in \mathbf{Q}[x]$ is not zero then $f(\pi) \neq 0$. Elements of $F = \mathbf{Q}(\pi^3)$ are quotients $f(\pi^3)/g(\pi^3)$, where $f(x), g(x) \in \mathbf{Q}[x]$.

Note that π is a root of $x^3 - \pi^3 \in F[x]$. Thus $\{1, \pi, \pi^2\}$ spans $F(\pi)$ as a vector space over F (**15**).

To show that $\{1, \pi, \pi^2\}$ is independent over F, observe by clearing denominators that a non-trivial dependence relation yields an expression

$$f_0(\pi^3) + f_1(\pi^3)\pi + f_2(\pi^3)\pi^2 = 0 \tag{1}$$

for some $f_0(x), f_1(x), f_2(x) \in \mathbf{Q}[x]$, not all of which are zero. Since $f_i(x^3)x^i$ is in the span of $\{x^{3\ell+i} \,|\, \ell \geq 0\}$ it follows that

$$h(x) = f_0(x^3) + f_1(x^3)x + f_2(x^3)x^2 \neq 0.$$

But $h(\pi) = 0$ by (**??**), a contradiction. Therefore $\{1, \pi, \pi^2\}$ is linearly independent over F. We have shown that $\{1, \pi, \pi^2\}$ is a basis for $F(\pi)$ over F (**5**).

5. Page 366, number 26: (**20 points**) $x^8 - x = x(x-1)(x^3+x^2+1)(x^3+x+1)$. The cubics are irreducible over $\mathbf{Z}_2$ since they have roots in $\mathbf{Z}_2$.