MATH 431 Written Homework 7 Solution Radford 04/09/2009

1. Page 388, number 20: (**20 points**) $g(x) \in \mathbf{Z}_p[x]$ is irreducible and divides $x^{p^n} - x$ in $\mathbf{Z}_p[x]$. Let F be a splitting field of $x^{p^n} - x$ over $\mathbf{Z}_p$. Then $|F| = p^n$ and $x^{p^n} - x = \prod_{a\in F}(x - a)$; see the proof of Theorem 22.1 (**4**). Since $g(x)$ divides $x^{p^n} - x$ in $\mathbf{Z}_p[x]$ it follows that $g(a) = 0$ for some $a \in F$ (**4**). Now $\operatorname{Deg} g(x) = [\mathbf{Z}_p[a] : \mathbf{Z}_p]$ by work in class (**4**). From the sequence of field extensions $\mathbf{Z}_p \subseteq \mathbf{Z}_p[a] \subseteq F$ we see that $[\mathbf{Z}_p[a] : \mathbf{Z}_p]$ divides $[F : \mathbf{Z}_p]$ by Theorem 21.5 (**4**). Thus $\operatorname{Deg} g(x)$ divides $[F : \mathbf{Z}_p] = n$ (**4**).

2. Page 389, number 24: (**20 points**) Write $p(x) = \alpha p_1(x)\cdots p_r(x)$, where $p_i(x) \in \mathbf{Z}_p[x]$ is *monic* irreducible for all $1 \leq i \leq r$ and $\alpha \in \mathbf{Z}_p$ is not zero (**3**). Then $p_1(x), \ldots, , p_r(x)$ are distinct since $p(x)$ has no multiple zeros in one (hence all) of its splitting fields (**3**).

Let F be a splitting field of $p(x)$ over $\mathbf{Z}_p$ (**3**). Then F is finite-dimensional vector space over $\mathbf{Z}_p$. Thus $|F| = p^n$ or some positive integer n and $x^{p^n} - x = \prod_{a\in F}(x - a)$ (**3**).

Let $1 \leq i \leq r$. Since $p(x)$ splits into linear factors over F it follows that $p_i(a) = 0$ for some $a \in F$ by the corollary to Theorem 18.3 and Corollary 2 to Theorem 16.2 (**2**). Since a is a root of $x^{p^n} - x$ also (**2**), $p_i(x) = \operatorname{irr}(a, \mathbf{Z})$ and thus divides $x^{p^n} - x$ in $\mathbf{Z}_p[x]$ by Theorem 21.3 (**2**). Since $p_1(x), \ldots, p_r(x)$ are relatively prime and each divides $x^{p^n} - x$ in $\mathbf{Z}_p[x]$ the product $p(x)$ does as well (**2**).

3. Page 389, number 30: (**20 points**) Suppose that F is a finite field and set $p(x) = \prod_{a\in F}(x - a) + 1$. Then $p(a) = 1$ for all $a \in F$ and $p(x)$ has positive degree. Therefore F is not algebraically closed.

4. Page 395, number 10: (**20 points**) Suppose that 40^o is constructible. Then $a = \cos 40^o$ is a constructible number. Now

$$-\frac{1}{2} = \cos 120^o = \cos 3{\cdot}40^o = 4\cos^3 40^o - 3\cos 40^o = 4a^3 - 3a$$

implies that a is a root of $p(x) = 8x^3 - 6x + 1 \in \mathbf{Q}[x]$ (**8**).

We show that $p(x) \in \mathbf{Q}[x]$ is irreducible. Suppose to the contrary that $p(x) \in \mathbf{Q}[x]$ is reducible. Then $p(r) = 0$ for some $r \in \mathbf{Q}$ by Theorem 17.1. Set $s = 2r + 1$. Then $s \in \mathbf{Q}$ and $r = \frac{1}{2}(s - 1)$. Therefore

$$0 = 8r^3 - 6r + 1 = (s-1)^3 - 3(s-1) + 1 = (s^3 - 3s^2 + 3s - 1) + (-3s + 3) + 1 = s^3 - 3s^2 + 3$$

which implies that $x^3 - 3x^2 + 3$ has a root in $\mathbf{Q}$ (**7**). But this polynomial is irreducible in $\mathbf{Q}[x]$ by the Eisenstein Criterion with $p = 3$, contradiction. We have shown that $p(x) \in \mathbf{Q}[x]$ is irreducible; thus

$$\operatorname{irr}(a, \mathbf{Q}) = x^3 - \frac{3}{4}x + \frac{1}{8}$$

which means $\operatorname{Deg} a = 3 \neq 2^\ell$ for all $\ell \geq 0$. Therefore a is not constructible number (**7**).

5. Page 396, number 20: (**20 points**) Suppose that the cube could be quadrupled. Then there an constructible number a which satisfies $a^3 = 4$, or equivalently is a root of $x^3 - 4$. We will show that $\operatorname{Deg} a = 3$ and thus is not constructible, by showing that $x^3 - 4 \in \mathbf{Q}[x]$ is irreducible.

Suppose that $x^3 - 4 \in \mathbf{Q}[x]$ is reducible. Then the polynomial has a root $r \in \mathbf{Q}$ (**4**). Write $r = n/m$, where $n, m \in \mathbf{Z}$ and are relatively prime. Then $r^3 = 4$, or equivalently $n^3 = 4m^3$. Therefore $2|n^3$; hence $2|n$ since 2 is a prime integer (**4**). Thus $n = 2\ell$ for some positive integer ℓ. Therefore $8\ell^3 = 4m^3$, or $2\ell^3 = m^3$. Thus $2|m^3$, and hence $2|m$, since 2 is prime (**4**). This contradicts the fact that n and m are relatively prime. Therefore $x^4 - 4 \in \mathbf{Q}[x]$ is irreducible which means $\operatorname{irr}(a, \mathbf{Q}) = x^3 - 4$ (**4**). Thus $\operatorname{Deg} a = 3$ and consequently a is not constructible (**4**).