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

2. Page 389, number 24: (20 points) Write \( p(x) = \alpha p_1(x) \cdots p_r(x) \), where \( p_i(x) \in \mathbb{Z}_p[x] \) is monic irreducible for all \( 1 \leq i \leq r \) and \( \alpha \in \mathbb{Z}_p \) 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 \( \mathbb{Z}_p \) (3). Then \( F \) is finite-dimensional vector space over \( \mathbb{Z}_p \). Thus \( |F| = p^n \) or some positive integer \( n \) and \( x^n - x = \prod_{a \in F} (x - a) \) (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 \( x^n - x \) also (2), \( p_i(x) = \text{irr}(a, \mathbb{Z}) \) and thus divides \( x^n - x \) in \( \mathbb{Z}_p[x] \) by Theorem 21.3 (2). Since \( p_1(x), \ldots, p_r(x) \) are relatively prime and each divides \( x^n - x \) in \( \mathbb{Z}_p[x] \) 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 \( 40^\circ \) is constructible. Then \( a = \cos 40^\circ \) is a constructible number. Now

\[-\frac{1}{2} = \cos 120^\circ = \cos 3\cdot 40^\circ = 4 \cos^3 40^\circ - 3 \cos 40^\circ = 4a^3 - 3a\]

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

We show that \( p(x) \in \mathbb{Q}[x] \) is irreducible. Suppose to the contrary that \( p(x) \in \mathbb{Q}[x] \) is reducible. Then \( p(r) = 0 \) for some \( r \in \mathbb{Q} \) by Theorem 17.1. Set \( s = 2r + 1 \). Then \( s \in \mathbb{Q} \) 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 \( \mathbb{Q} \) (7). But this polynomial is irreducible in \( \mathbb{Q}[x] \) by the Eisenstein Criterion with \( p = 3 \), contradiction. We have shown that \( p(x) \in \mathbb{Q}[x] \) is irreducible; thus

\[\text{irr}(a, \mathbb{Q}) = x^3 - \frac{3}{4}x + \frac{1}{8}\]

which means \( \text{Deg} a = 3 \neq 2^\ell \) for all \( \ell \geq 0 \). Therefore \( a \) is not constructible number (7).
5. Page 396, number 20: \textbf{(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 $\deg a = 3$ and thus is not constructible, by showing that $x^3 - 4 \in \mathbb{Q}[x]$ is irreducible.

Suppose that $x^3 - 4 \in \mathbb{Q}[x]$ is reducible. Then the polynomial has a root $r \in \mathbb{Q}$ (4). Write $r = n/m$, where $n, m \in \mathbb{Z}$ 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 $\ell$. 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 $x^4 - 4 \in \mathbb{Q}[x]$ is irreducible which means $\text{irr}(a, \mathbb{Q}) = x^3 - 4$ (4). Thus $\deg a = 3$ and consequently $a$ is not constructible (4).