**Solutions to Homework 11**

**Problem 1.** Cox, Section 8.1, Exercise 7, variant:
Prove that if $n$ is an integer with $1 \leq n < 60$ that is divisible by at least three distinct primes, then either $n = 30$ or $n = 42$.
Then use Use Burnside's $p^a q^b$ Theorem (Theorem 8.1.8) to prove that any group $G$ with $|G| < 60$ and with $|G| \neq 30, 42$ must be solvable.

**Proof**. Given an integer $n$ with $1 \leq n < 60$ that is divisible by at least three distinct primes, call those primes $p < q < r$. Then there is an integer $k$ such that $n = pqrk$.
If $p \geq 3$, then $q \geq 5$ and hence $r \geq 7$, so $n \geq 3 \cdot 5 \cdot 7 = 105$, a contradiction. Thus, we must have $p = 2$.
If $q \geq 5$, then $r \geq 7$, and hence $n \geq 2 \cdot 5 \cdot 7 = 70$, another contradiction. Thus, we must have $q = 3$.
If $r \geq 11$, then $n \geq 2 \cdot 3 \cdot 11 = 66$, another contradiction. Thus, $r$ must be either 5 or 7.
If $k \geq 2$, then $n \geq 2 \cdot 3 \cdot 5 \cdot 2 = 60$, a contradiction. Thus, $k = 1$.

To summarize, then, we must have $p = 2$, $q = 3$, and $k = 1$, with either $r = 5$ or $r = 7$. If $r = 5$, then we have $n = 2 \cdot 3 \cdot 5 = 30$; otherwise, we have $r = 7$ and hence $n = 2 \cdot 3 \cdot 7 = 42$.

Finally, given any group $G$ as in the statement of the problem, we have just shown that $|G|$ is divisible by at most two primes, and hence can be written in the form $p^a q^b$ with $p, q$ prime and $a, b \geq 0$. Thus, by Burnside's Theorem, $G$ is solvable. QED

---

**Problem 2.** Cox, Section 8.1, Exercise 8, slightly rephrased:
Let $G$ be a finite group, and suppose that there are subgroups

$$\{e\} = G_0 \subseteq G_1 \subseteq \cdots \subseteq G_n = G$$

such that $G_{i-1} \lhd G_i$ for each $1 \leq i \leq n$.

(a) Suppose that $G_i/G_{i-1}$ is abelian for each $1 \leq i \leq n$. Prove that $G$ is solvable.

(b) Suppose that $G_i/G_{i-1}$ is solvable for each $1 \leq i \leq n$. Prove that $G$ is solvable.

**Proof**. **(a)**. We proceed by induction on $n \geq 0$. If $n = 0$, then $G = \{e\}$ is trivially solvable.
For the inductive step, given some $n \geq 1$, suppose the statement is true for $n - 1$. Given a group $G$ with subgroups as in the problem with abelian quotients, let $N = G_{n-1} \lhd G$. Then $N$ has subgroups

$$\{e\} = G_0 \subseteq G_1 \subseteq \cdots \subseteq G_{n-1} = N$$

such that $G_{i-1} \lhd G_i$ with $G_i/G_{i-1}$ abelian for each $1 \leq i \leq n-1$, and therefore $N$ is solvable by the inductive hypothesis.
In addition, $G/N = G_n/G_{n-1}$ is abelian by assumption, and therefore, by Proposition 8.1.5, it is solvable.
Since both $N$ and $G/N$ are solvable, it follows from Theorem 8.1.4 that $G$ is solvable. QED (a)

---

**(b)**. We proceed by induction on $n \geq 0$. If $n = 0$, then $G = \{e\}$ is trivially solvable.
For the inductive step, given some $n \geq 1$, suppose the statement is true for $n - 1$. Given a group $G$ with subgroups as in the problem with solvable quotients, let $N = G_{n-1} \lhd G$. Then $N$ has subgroups

$$\{e\} = G_0 \subseteq G_1 \subseteq \cdots \subseteq G_{n-1} = N$$

such that $G_{i-1} \lhd G_i$ with $G_i/G_{i-1}$ solvable for each $1 \leq i \leq n-1$, and therefore $N$ is solvable by the inductive hypothesis.
In addition, $G/N = G_n/G_{n-1}$ is solvable by assumption.
Since both $N$ and $G/N$ are solvable, it follows from Theorem 8.1.4 that $G$ is solvable. QED (b)

---

**Problem 3.** Cox, Section 8.1, Exercise 5, variant:

The center of a group $G$ is the set $Z(G) = \{g \in G \,|\, xg = gx \text{ for all } x \in G\}$. In this problem, you may assume the following two facts from Math 350:

**Fact 1**. $Z(G)$ is a normal subgroup of $G$.

**Fact 2**. If $|G| = p^n$ for a prime $p$ and integer $n \geq 1$, then $|Z(G)| > 1$.

Use the above facts to prove that for any group $G$ whose order $|G|$ is a power of a prime, $G$ is solvable.

[**Suggestion**: Write $|G| = p^n$ and proceed by induction on $n \geq 0$.]

**Proof**. For any such group, write $|G| = p^n$. We proceed by strong induction on $n \geq 0$. For $n = 0$, we have $|G| = 1$, so $G = \{e\}$ is trivially solvable.

For the inductive step, given some $n \geq 1$, suppose the statement is true for all groups of order $p^m$ satisfying $m < n$. Given a group $G$ with $|G| = p^n$, let $N = Z(G)$, which is a normal subgroup of $G$ by Fact 1. By Lagrange's Theorem, we have $|N| \big| |G|$, and hence $|N| = p^k$ for some integer $k$ with $0 \leq k \leq n$. In addition, we have $|N| > 1$ by Fact 2, and hence $1 \leq k \leq n$.

Consider the quotient group $G/N$, which has order $|G|/|N| = p^m$, where $m = n - k$, so that $0 \leq m < n$. By the inductive hypothesis, then, $G/N$ is solvable.

In addition, $N = Z(G)$ is abelian, since for all $g, h \in Z(G)$, we have $h \in G$ and hence $gh = hg$. Thus, $N$ is also solvable.

Because both $N$ and $G/N$ are solvable, it follows that $G$ is solvable. QED

---

**Problem 4.** Cox, Section 8.2, Exercise 6:
Let $M/L/F$ be finite extensions of fields, and let $\sigma \in \mathrm{Gal}(M/F)$. Assume that $L/F$ is a radical extension. Prove that $(\sigma L)/F$ is also radical.

**Proof**. By hypothesis, there are intermediate fields $F = F_0 \subseteq F_1 \subseteq \cdots \subseteq F_n = L$ such that for each $i = 1, \ldots, n$, there exist an integer $m_i \geq 1$ and $\gamma_i \in F_i$ with $\gamma_i^{m_i} \in F_{i-1}$ and $F_i = F_{i-1}(\gamma_i)$.

For each $i = 0, \ldots, n$, define $E_i = \sigma F_i$. Then clearly $E_n = \sigma L$, and because $\sigma$ fixes all elements of $F$, we also have $E_0 = \sigma F = F$. In addition, for each $i = 1, \ldots, n$, we have $E_{i-1} = \sigma F_{i-1} \subseteq \sigma F_i = E_i$. That is, we have $F = E_0 \subseteq E_1 \subseteq \cdots \subseteq E_n = \sigma L$.

In addition, for each $i = 1, \ldots, n$, let $\delta_i = \sigma(\gamma_i) \in \sigma F_i = E_i$.
Then $\delta_i^{m_i} = \big(\sigma(\gamma_i)\big)^{m_i} = \sigma\big(\gamma_i^{m_i}\big) \in \sigma F_{i-1} = E_{i-1}$.
Finally, we have $E_i = \sigma F_i = \sigma\big(F_{i-1}(\gamma_i)\big) = \big(\sigma F_{i-1}\big)(\sigma(\gamma_i)) = E_{i-1}(\delta_i)$, as desired. QED

---

**Problem 5.** Cox, Section 8.3, Exercise 3, slight variant:
Let $p$ be a prime, let $K$ be a field, and let $\zeta \in K$ be a primitive $p$-th root of unity. [That is, $\zeta^p = 1$ but $\zeta \neq 1$.] For any integer $n \in \mathbb{Z}$ with $p \nmid n$, prove that

$$1 + \zeta^n + \zeta^{2n} + \cdots + \zeta^{(p-1)n} = 0.$$

**Proof**. Let $\xi = \zeta^n \in K$. Since $\gcd(p, n) = 1$, there exist integers $x, y \in \mathbb{Z}$ such that $px + ny = 1$.
Thus, $\xi^y = \zeta^{ny} = 1^x \cdot \zeta^{ny} = \zeta^{px+ny} = \zeta \neq 1$, so $\xi \neq 1$. In addition, $\xi^p = \zeta^{pn} = (\zeta^p)^n = 1$. [That is, $\xi$ is also a primitive $p$-th root of unity.] Since $\xi - 1 \neq 0$, we therefore have

$$1 + \zeta^n + \zeta^{2n} + \cdots + \zeta^{(p-1)n} = 1 + \xi + \xi^2 + \cdots + \xi^{p-1} = \frac{\xi^p - 1}{\xi - 1} = \frac{0}{\xi - 1} = 0. \quad \text{QED}$$

---

**Problem 6.** Cox, Section 8.3, Exercise 6, slight variant:
Let $L$ be a field, let $m \geq n \geq 1$ be integers with $n|m$, and let $\zeta \in L$ be a primitive $m$-th root of unity. [So $\zeta^m = 1$ but for any integer $d$ with $1 \leq d < m$, we have $\zeta^d \neq 1$.] Prove that $\zeta^{m/n}$ is a primitive $n$-th root of unity.

**Proof**. Write $k = m/n$, which is an integer with $1 \leq k \leq m$. Write $\xi = \zeta^k$.
Then $\xi^n = \zeta^m = 1$, so $\xi$ is an $n$-th root of unity.

Given any integer $d$ with $1 \leq d < n$, we have $1 \leq dk < nk = m$, and hence $\xi^d = \zeta^{dk} \neq 1$. QED