Solutions to Homework 12

Problem 1. Cox, Section 8.3, Exercise 4, rephrased:
Let $m \geq 1$ be an integer, and let F be a field containing a primitive m-th root of unity $\zeta \in F$. Let $a \in F^\times$, and let $K = F(\gamma)$ where γ is a root of $x^m - a$. [That is, $\gamma = \sqrt[m]{a}$.]

(a) For each $\sigma \in \mathrm{Gal}(K/F)$, prove that there is a unique integer n such that $0 \leq n \leq m-1$ and $\sigma(\gamma) = \zeta^n \gamma$.

(b) Define $\varphi : \mathrm{Gal}(K/F) \to \mathbb{Z}/m\mathbb{Z}$ by $\varphi(\sigma) \equiv n \pmod{m}$, where n is the integer from part (a) for which $\sigma(\gamma) = \zeta^n \gamma$. Prove that φ is an injective homomorphism.

(c) Conclude that $\mathrm{Gal}(K/F)$ is cyclic, of order dividing m.

Proof. **(a)**: Given $\sigma \in \mathrm{Gal}(K/F)$, we have $\sigma(\gamma)^m = \sigma(\gamma^m) = \sigma(a) = a$, and hence $\sigma(\gamma)$ is also a root of $x^m - a$. However, we have

$$x^m - a = \prod_{n=0}^{m-1} \big(x - \zeta^n \gamma\big),$$

and hence there is some $0 \leq n \leq m-1$ such that $\sigma(\gamma) = \zeta^n \gamma$.
To see that n is unique, suppose we also have $\sigma(\gamma) = \zeta^k \gamma$ for some $0 \leq k \leq m-1$. Without loss of generality, assume $n \geq k$. Then since $a \neq 0$ and hence $\gamma \neq 0$, it follows that $\zeta^{n-k} = 1$. But $0 \leq n-k \leq m-1$, and ζ is a *primitive* m-th root of unity, and hence $n - k = 0$. That is, $k = n$, as desired. QED (a)

(b): To see that φ is a homomorphism, given $\sigma, \tau \in \mathrm{Gal}(K/F)$, let $n = \varphi(\sigma)$ and $k = \varphi(\tau)$ (both viewed as integers mod m).
Then since $\zeta \in F$, we have $\sigma\tau(\gamma) = \sigma\big(\tau(\gamma)\big) = \sigma\big(\zeta^k \gamma\big) = \zeta^k \sigma(\gamma) = \zeta^k \zeta^n \gamma = \zeta^{k+n}\gamma$, and therefore $\varphi(\sigma\tau) \equiv k + n \pmod{n}$. That is, $\varphi(\sigma\tau) = \varphi(\sigma) + \varphi(\tau)$.
To see that φ is injective, given $\sigma, \tau \in \mathrm{Gal}(K/F)$ such that $\varphi(\sigma) = \varphi(\tau)$, represent this common value in $\mathbb{Z}/m\mathbb{Z}$ by $n \in \mathbb{Z}$. Then $\sigma(\gamma) = \zeta^n \gamma = \tau(\gamma)$, so that σ and τ agree on F and at γ, and hence on $K = F(\gamma)$. That is, $\sigma = \tau$. QED (b)

(c): Let $H = \varphi(\mathrm{Gal}(K/F)) \subseteq \mathbb{Z}/m\mathbb{Z}$ be the image of φ. Then H is a subgroup of the cyclic group $\mathbb{Z}/m\mathbb{Z}$, and hence H is also cyclic. Since φ is an injective homomorphism with image H, we have that $\varphi : \mathrm{Gal}(K/F) \to H$ is an isomorphism. That is, $\mathrm{Gal}(K/F)$ is isomorphic to a cyclic group and hence is cyclic. QED (c)

Problem 2. Cox, Section 8.3, Exercise 5, slightly rephrased:
Let $M/L/K/F$ be finite extensions such that M/F and L/K are both Galois. Prove that $|\mathrm{Gal}(L/K)|$ divides $|\mathrm{Gal}(M/F)|$.

Proof. Because they are Galois extensions, we have $|\mathrm{Gal}(L/K)| = [L:K]$ and $|\mathrm{Gal}(M/F)| = [M:F]$. By the Tower Theorem, we have $[M:F] = [M:L][L:K][K:F]$, and hence $[L:K] \,|\, [M:F]$. That is, $|\mathrm{Gal}(L/K)|$ divides $|\mathrm{Gal}(M/F)|$. QED

Problem 3. Cox, Section 8.4, Exercise 1:
Let G be a nontrivial finite abelian group. Prove that G is simple if and only if $G \cong \mathbb{Z}/p\mathbb{Z}$ for some prime number p.

Proof. ($\Rightarrow$): Since G is nontrivial, there exists $a \in G \smallsetminus \{e\}$. Let $H = \langle a \rangle$, which is a nontrivial subgroup of G. Since G is abelian, we have $H \lhd G$. Because of our assumption that G is simple, it follows that $H = G$.
Thus, $G = H = \langle a \rangle$ is cyclic of order $n = o(a) \geq 2$. If n is not prime, then there exist integers $k, m \geq 2$ with $n = km$. Then $H' = \langle a^m \rangle$ is subgroup of G of order k. Again because G is abelian, we have

$H' \lhd G$. Because $1 < k = |H'| < n = |G|$, then, H' is a nontrivial proper normal subgroup of G, a contradiction.
Thus, $n = p$ is prime. That is, G is cyclic of order p, and hence $G \cong \mathbb{Z}/p\mathbb{Z}$. QED ($\Rightarrow$)

($\Leftarrow$): Since $G \cong \mathbb{Z}/p\mathbb{Z}$, we have $|G| = p$. For any normal subgroup $H \lhd G$, we have $|H| \,\big|\, |G| = p$ by Lagrange's Theorem, and hence $|H| = 1$ or $|H| = p$.
If $|H| = 1$, then H is trivial; and if $|H| = p$, then $H = G$ is improper. Thus, G has no improper nontrivial normal subgroups, i.e., G is simple. QED ($\Leftarrow$) QED

Problem 4. Cox, Section 8.4, Exercise 6, slightly rephrased:
Let G be a finite group of order $n \geq 1$.

(a) Consider the set S of all proper normal subgroups of G. (I.e., $S = \{N \lhd G \,|\, N \neq G\}$.)
If $n \geq 2$, prove that there exists $H \in S$ of maximal order, i.e.,
such that $|N| \leq |H|$ for all $N \in S$.

(b) For the normal subgroup H of part (a), prove that G/H is simple.

(c) Use strong induction on n to prove that every finite group has a composition series.

[**Suggestion**: For part (b), the Correspondence Theorem (between subgroups of G/H and subgroups of G that contain H) may come in handy.]

Proof. (a): We have $\{e\} \lhd G$, and since $|G| = n \geq 1$, we also have $\{e\} \neq G$.
Thus, $\{e\} \in S$, and hence $S \neq \varnothing$.

Define $T = \{n - |N| \,|\, N \in S\}$, which is a nonempty set of positive integers. (Clearly $T \subseteq \mathbb{Z}$, and $n - |N| > 0$ for all $N \in S$, since $N \subseteq G$. And T is nonempty since S is nonempty.)

Thus, T contains a least element k. Hence, there exists $H \in S$ with $n - |H| = k$.

Given any $N \in S$, then, we have $n - |N| \in T$ and hence $n - |N| \geq k = n - |H|$. Therefore, $|N| \leq |H|$.
QED (a)

(b): Given an arbitrary normal subgroup M of G/H, then by the Correspondence Theorem, there is a normal subgroup N of G that contains H such that $M = N/H$. We consider two cases.

Case 1. If $N \in S$, then by the maximality of H, we must have $|N| \leq |H|$; but because $N \supseteq H$, we also have $|N| \geq |H|$, and hence $|N| = |H|$. Because G is finite, it follows that $N = H$, and hence $M = N/H = H/H = \{He\}$ is the trivial subgroup of G/H.

Case 2. Otherwise, we have $N \notin S$, and hence $N = G$ Then $M = N/H = G/H$ is the improper subgroup of G/H.

Thus, G/H has no proper, nontrivial normal subgroups. QED (b)

(c): Our inductive claim, for each $n \geq 1$, is that every group G of order n has a composition series.

If $n = 1$, then any group G with $|G| = n$ is a trivial group $G = \{e\}$, which has composition series $\{e\} = G_0 = G$ of length zero. [It vacuously satisfies the normality and quotient conditions, because there are no subgroup relationships in the composition series to check.]

For the inductive step $n \geq 2$, suppose we already know the claim for each m with $1 \leq m \leq n - 1$.
Let H be a maximal normal subgroup of G, from part (a). Then $|H| < |G|$, so by the inductive hypothesis, H has a composition series

$$\{e\} = G_0 \lhd G_1 \lhd \cdots \lhd G_k = H$$

with each quotient G_i/G_{i-1} simple, for $1 \leq i \leq k$. Let $G_{k+1} = G$. Then we have

$$\{e\} = G_0 \lhd G_1 \lhd \cdots \lhd G_k = H \lhd G_{k+1} = G$$

with G_i/G_{i-1} simple for $1 \leq i \leq k$. We also have $G_{k+1}/G_k = G/H$ simple, by part (b). Thus, G_i/G_{i-1} is simple for $1 \leq i \leq k + 1$, so that the sequence above is a composition series for G. QED (c)

Problem 5. Cox, Section 8.4, Exercise 8:

Prove that $\mathbb{Z}/4\mathbb{Z}$ and $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ are nonisomorphic groups whose composition series consist of the same list of simple groups (up to isomorphism).

Proof. $G = \mathbb{Z}/4\mathbb{Z}$ is cyclic of order 4, but each of the four elements of $H = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ has order 1 or 2. Thus, H is not cyclic, so $G \ncong H$.

Writing $G = \{0, 1, 2, 3\}$ (with addition modulo 4), let $G_0 = \{0\}$, let $G_1 = \langle 2 \rangle = \{0, 2\}$, and let $G_2 = G$. Then because G is abelian, we have $G_0 \lhd G_1 \lhd G_2$. Moreover, $|G_1/G_0| = |G_1|/|G_0| = 2/1 = 2$, so that $G_1/G_0 \cong \mathbb{Z}/2\mathbb{Z}$, and $|G_2/G_1| = |G_2|/|G_1| = 4/2 = 2$, so that $G_2/G_1 \cong \mathbb{Z}/2\mathbb{Z}$.

Since 2 is prime, these are both simple groups, so $G_0 \lhd G_1 \lhd G_2$ is the composition series of G, with simple quotients $\mathbb{Z}/2\mathbb{Z}$ and $\mathbb{Z}/2\mathbb{Z}$.

Writing $H = \{(0,0), (1,0), (0,1), (1,1)\}$ (with addition modulo 2 in each coordinate), let $H_0 = \{(0,0)\}$, let $H_1 = \langle (1,0) \rangle = \{(0,0), (1,0)\}$, and let $H_2 = H$. Then because H is abelian, we have $H_0 \lhd H_1 \lhd H_2$. Moreover, $|H_1/H_0| = |H_1|/|H_0| = 2/1 = 2$, so that $H_1/H_0 \cong \mathbb{Z}/2\mathbb{Z}$, and $|H_2/H_1| = |H_2|/|H_1| = 4/2 = 2$, so that $H_2/H_1 \cong \mathbb{Z}/2\mathbb{Z}$.

Since 2 is prime, these are both simple groups, so $H_0 \lhd H_1 \lhd H_2$ is the composition series of H, and just as for G, the corresponding simple quotients are $\mathbb{Z}/2\mathbb{Z}$ and $\mathbb{Z}/2\mathbb{Z}$. QED

Problem 6. (14 points) Cox, Section 9.1, Exercise 12a:
Let $n \geq 1$ be an integer, and define $m = \prod_{p|n} p$ be the product of all primes dividing n, each only to the first power.
Prove that $\Phi_n(x) = \Phi_m(x^{n/m})$.

[**Note**: This reduces the computation of Φ_n to the case that n is squarefree.]

Proof. Let ζ_n be a primitive n-th root of unity, so that $\Phi_n(x) = \prod_{i \in T}(x - \zeta_n^i)$, where

$$T = \{i \in \mathbb{Z} \,|\, 0 \leq i < n \text{ and } \gcd(i, n) = 1\}.$$

Let $\ell = n/m \in \mathbb{Z}_{\geq 1}$, and note (by HW 11 Problem 6) that $\zeta_n^\ell = \zeta_m$ is a primitive m-th root of unity. Thus, $\Phi_m(x) = \prod_{j \in U}(x - \zeta_m^j) = \prod_{j \in U}(x - \zeta_n^{j\ell})$, where

$$U = \{j \in \mathbb{Z} \,|\, 0 \leq j < m \text{ and } \gcd(j, m) = 1\}.$$

By the division algorithm, every $i \in \mathbb{Z}$ with $0 \leq i < n$ can be written uniquely as $mq + j$, where $j, q \in \mathbb{Z}$ with $0 \leq q < \ell$ and $0 \leq j \leq m - 1$. (And conversely, for any such j, q, we have $0 \leq mq + j < n$.) Thus,

$$T = \{mq + j \,|\, j, q \in \mathbb{Z},\, 0 \leq q < \ell,\, 0 \leq j < m, \text{ and } \gcd(mq + j, n) = 1\}.$$

However, the condition $\gcd(i, n) = 1$ is equivalent to $\gcd(i, m) = 1$, since m and n have precisely the same prime factors. Therefore, $\gcd(mq + j, n) = 1 \Leftrightarrow \gcd(mq + j, m) = 1 \Leftrightarrow \gcd(j, m) = 1$, and hence

$$T = \{mq + j \,|\, j \in U,\, q \in \mathbb{Z}, \text{ and } 0 \leq q < \ell\}.$$

Therefore,

$$\Phi_n(x) = \prod_{i \in T} \left(x - \zeta_n^i\right) = \prod_{j \in U} \prod_{q=0}^{\ell-1} \left(x - \zeta_n^{j+mq}\right) = \prod_{j \in U} \prod_{q=0}^{\ell-1} \left(x - \zeta_\ell^q \zeta_n^j\right),$$

where $\zeta_\ell = \zeta_n^m$ is a primitive ℓ-th root of unity, again by Homework 11, Problem 6. However, we also have

$$\prod_{q=0}^{\ell-1} \left(x - \zeta_\ell^q \zeta_n^j\right) = x^\ell - \left(\zeta_n^j\right)^\ell = x^\ell - \zeta_n^{j\ell}.$$

Combining the two above computations yields

$$\Phi_n(x) = \prod_{j \in U} \left(x^\ell - \zeta_n^{j\ell}\right) = \Phi_m\left(x^\ell\right) = \Phi_m\left(x^{n/m}\right).$$

by our computation of Φ_m earlier. QED

Problem 7. (12 points) Cox, Section 9.1, Exercise 12b:
If $n \geq 3$ is odd, prove that $\Phi_{2n}(x) = \Phi_n(-x)$.

[**Note**: Together with the previous problem, this reduces the computation of Φ_n to the case that n is odd and squarefree.]

Proof. Let ζ_{2n} be a primitive $2n$-th root of unity. By Homework 11, Problem 6, note that $\zeta_{2n}^2 = \zeta_n$ is a primitive n-th root of unity, and that $\zeta_{2n}^n = -1$. We have $\Phi_n(x) = \prod_{i\in T}(x - \zeta_n^i)$, where

$$T = \{i \in \mathbb{Z} \,|\, 0 \le i < n \text{ and } \gcd(i,n) = 1\}.$$

Since $n \ge 3$ is odd, there is an odd prime p with $p|n$. Thus, $|T| = |(\mathbb{Z}/n\mathbb{Z})^\times| = \phi(n)$ is divisible by $(p-1)$, and hence $|T|$ is even.

Write $n = 2m+1$, with $m \in \mathbb{Z}_{\ge 1}$, and write $T = T_0 \cup T_1$, where

$$T_0 = \{i \in T \,|\, 0 \le i \le m\} \text{ and } T_1 = \{i \in T \,|\, m < i \le n-1\}.$$

Also define

$$U_0 = \{j \in \mathbb{Z} \,|\, 0 \le j < n \text{ and } \gcd(j,2n) = 1\} \text{ and } U_1 = \{j \in \mathbb{Z} \,|\, n \le j < 2n \text{ and } \gcd(j,2n) = 1\}.$$

We claim that $U_1 = \{2i + n \,|\, i \in T_0\}$. Indeed, for any $i \in T_0$, we have $n \le 2i + n \le 2n - 1$, and $\gcd(2i+n, n) = \gcd(2i, n) = 1$. In addition, $2i+n$ is odd, so $2 \nmid (2i+n)$, and hence $\gcd(2i+n, 2n) = 1$, proving that $2i + n \in U_1$. Conversely, for any $j \in U_1$, we have $0 \le j - n \le n - 1$ with $j - n$ even, so $i = (j-n)/2 \in \mathbb{Z}$ with $0 \le i \le m$. Since $\gcd(j, 2n) = 1$, we have $\gcd(j, n) = 1$ and hence $\gcd(j-n) = 1$ as well. Therefore $\gcd(i, n) = 1$, so that $j = 2i + n$ with $i \in T_0$, proving the claim.

Similarly, we also have $U_0 = \{2i - n \,|\, i \in T_1\}$. Thus,

$$\Phi_n(-x) = \prod_{i\in T}\big(-x - \zeta_n^i\big) = (-1)^{|T|}\prod_{i\in T}\big(x + \zeta_n^i\big) = \prod_{i\in T}\big(x + \zeta_{2n}^{2i}\big) = \left(\prod_{i\in T_0}\big(x + \zeta_{2n}^{2i}\big)\right)\cdot\left(\prod_{i\in T_1}\big(x + \zeta_{2n}^{2i}\big)\right)$$

$$= \left(\prod_{i\in T_0}\big(x - \zeta_{2n}^{2i+n}\big)\right)\left(\prod_{i\in T_1}\big(x - \zeta_{2n}^{2i-n}\big)\right) = \left(\prod_{j\in U_1}\big(x - \zeta_{2n}^{j}\big)\right)\left(\prod_{j\in U_0}\big(x - \zeta_{2n}^{j}\big)\right) = \Phi_{2n}(x) \qquad \text{QED}$$

Problem 8. (12 points) Cox, Section 9.1, Exercise 12c:
If $n \ge 1$ and p is a prime *not* dividing n, prove that $\Phi_{pn}(x) = \Phi_n(x^p)/\Phi_n(x)$.

[**Note**: This gives a strategy for computing Φ_n for n odd and squarefree, although the computations can get quite messy in practice because of the quotient.]

Proof. Define $W = \{i \in \mathbb{Z} \,|\, 0 \le i < pn \text{ and } \gcd(i,n) = 1\}$. Let ζ_{pn} be a primitive pn-th root of unity. By HW 11 Problem 6, $\zeta_n = \zeta_{pn}^p$ is a primitive n-th root of unity, and $\zeta_p = \zeta_{pn}^n$ is also a primitive p-th root of unity. We have

$$\Phi_{pn}(x) = \prod_{i\in T}(x - \zeta_{pn}^i) \quad \text{and} \quad \Phi_n(x) = \prod_{j\in U}(x - \zeta_n^j) = \prod_{j\in U}(x - \zeta_{pn}^{pj}),$$

where

$$T = \{i \in W \,|\, p \nmid i\} \quad \text{and} \quad U = \{j \in W \,|\, 0 \le j < n\}.$$

Further define $V = W \smallsetminus T = \{i \in W \,|\, p|i\} = \{pj \,|\, j \in U\}$.

By the division algorithm, every $i \in \mathbb{Z}$ with $0 \le i < pn$ can be written uniquely as $i = qn + j$, where $j, q \in \mathbb{Z}$ with $0 \le j < n$ and $0 \le q \le p-1$. (And conversely, for any such j, q, we have $0 \le qn + j < pn$.) In addition, the condition $\gcd(qn + j, n) = 1$ is equivalent to $\gcd(j, n) = 1$. Thus,

$$W = \{qn + j \,|\, j, q \in \mathbb{Z},\ 0 \le j < n,\ 0 \le q < p, \text{ and } \gcd(j,n) = 1\}.$$

That is, $W = \{qn + j \,|\, j \in U,\ q \in \mathbb{Z}, \text{ and } 0 \le q < p-1\}$. Therefore,

$$\Phi_n(x^p) = \prod_{j\in U}\big(x^p - \zeta_{pn}^{pj}\big) = \prod_{j\in U}\prod_{q=0}^{p-1}\big(x - \zeta_p^q\zeta_{pn}^j\big) = \prod_{j\in U}\prod_{q=0}^{p-1}\big(x - \zeta_{pn}^{j+nq}\big) = \prod_{i\in W}\big(x - \zeta_{pn}^i\big)$$

$$= \left(\prod_{i\in T}\big(x - \zeta_{pn}^i\big)\right)\cdot\left(\prod_{i\in V}\big(x - \zeta_{pn}^i\big)\right) = \Phi_{pn}(x)\cdot\prod_{j\in U}\big(x - \zeta_{pn}^{pj}\big) = \Phi_{pn}(x)\cdot\prod_{j\in U}\big(x - \zeta_n^j\big) = \Phi_n(x)\cdot\Phi_{pn}(x).$$

The desired result then follows by dividing by $\Phi_n(x)$. QED