Solutions to Homework 13

Problem 1.(not from Cox):
Let R, S be rings with unity. Prove that $(R \times S)^\times = R^\times \times S^\times$.

Proof. ($\subseteq$): Given $(x, y) \in (R \times S)^\times$, then by definition there exists $(a, b) \in (R \times S)$ such that $(x, y)(a, b) = (1_R, 1_S) = (a, b)(x, y)$.
That is, $xa = 1_R = ax$ and $yb = 1_S = by$, and hence x is a unit in R (with inverse $a \in R$), while y is a unit in S (with inverse $b \in S$). Hence, $x \in R^\times$ and $y \in S^\times$, and therefore $(x, y) \in R^\times \times S^\times$. QED ($\subseteq$)

($\supseteq$): Given $(x, y) \in R^\times \times S^\times$, then x has multiplicative inverse $x^{-1} \in R$, and y has multiplicative inverse $y^{-1} \in S$. Therefore, $(x^{-1}, y^{-1}) \in R \times S$, and

$$(x, y)(x^{-1}, y^{-1}) = (xx^{-1}, yy^{-1}) = (1_R, 1_S) = (x^{-1}x, y^{-1}y) = (x^{-1}, y^{-1})(x, y).$$

Thus, $(x^{-1}, y^{-1}) \in R \times S$ is a multiplicative inverse of (x, y), so $(x, y) \in (R \times S)^\times$. QED

Problem 2. Cox, Section 9.1, Exercise 2:
Let $m, n \geq 1$ be positive integers with $\gcd(m, n) = 1$. By Lemma A.5.2, the function
$\alpha : \mathbb{Z}/mn\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$ given by $\alpha([j]_{mn}) = ([j]_n, [j]_m)$ is a ring isomorphism.
Prove that α induces a group isomorphism $(\mathbb{Z}/mn\mathbb{Z})^\times \cong (\mathbb{Z}/n\mathbb{Z})^\times \times (\mathbb{Z}/m\mathbb{Z})^\times$.

[**Suggestion**: Use Problem 1 above.]

Proof. For any $x \in \mathbb{Z}/mn\mathbb{Z}$, we have $\alpha(x)$ is a unit in $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$ if and only if x is a unit in $\mathbb{Z}/mn\mathbb{Z}$, since α is a ring isomorphism. Thus, restricting α to the group of units $(\mathbb{Z}/mn\mathbb{Z})^\times$ yields a group isomorphism $(\mathbb{Z}/mn\mathbb{Z})^\times \cong \big((\mathbb{Z}/n\mathbb{Z}) \times (\mathbb{Z}/m\mathbb{Z})\big)^\times$.
By the previous problem, we have $\big((\mathbb{Z}/n\mathbb{Z}) \times (\mathbb{Z}/m\mathbb{Z})\big)^\times = (\mathbb{Z}/n\mathbb{Z})^\times \times (\mathbb{Z}/m\mathbb{Z})^\times$, so we are done. QED

Problem 3. Cox, Section 9.1, Exercise 16:
Let $m, n \geq 1$ be integers with $\gcd(m, n) = 1$.

(a) Prove that $\mathbb{Q}(\zeta_m, \zeta_n) = \mathbb{Q}(\zeta_{mn})$

(b) Prove that Φ_n is irreducible over $\mathbb{Q}(\zeta_m)$.

[**Note/Suggestion**: For part (b), Problem 2 above may be useful, along with various other results from Section 9.1.]

Proof. **(a)**: We have $\zeta_m = \zeta_{mn}^n \in \mathbb{Q}(\zeta_{mn})$ and $\zeta_n = \zeta_{mn}^m \in \mathbb{Q}(\zeta_{mn})$. Therefore $\mathbb{Q}(\zeta_m, \zeta_n) \subseteq \mathbb{Q}(\zeta_{mn})$.
Conversely, since $\gcd(m, n) = 1$, there exist integers $a, b \in \mathbb{Z}$ such that $am + bn = 1$. It follows that $\zeta_{mn} = \zeta_{mn}^{am+bn} = \big(\zeta_{mn}^n\big)^b \big(\zeta_{mn}^m\big)^a = \zeta_m^b \zeta_n^a \in \mathbb{Q}(\zeta_m, \zeta_n)$. Hence, $\mathbb{Q}(\zeta_m, \zeta_n) \supseteq \mathbb{Q}(\zeta_{mn})$. QED (a)

(b): By Problem 2, we have

$$\phi(mn) = \big|(\mathbb{Z}/mn\mathbb{Z})^\times\big| = \big|(\mathbb{Z}/n\mathbb{Z})^\times \times (\mathbb{Z}/m\mathbb{Z})^\times\big| = \big|(\mathbb{Z}/n\mathbb{Z})^\times\big| \cdot \big|(\mathbb{Z}/m\mathbb{Z})^\times\big| = \phi(m)\phi(n).$$

Therefore,

$$[\mathbb{Q}(\zeta_m, \zeta_n) : \mathbb{Q}] = [\mathbb{Q}(\zeta_{mn}) : \mathbb{Q}] = \phi(mn) = \phi(m)\phi(n) = \phi(m) \cdot \deg(\Phi_n),$$

where the first equality is by part (a), the second is by Corollary 9.1.10, and the fourth is because $\phi(n) = \deg(\Phi_n)$, as was noted with the definition of Φ_n on page 231.

Let $f \in \mathbb{Q}(\zeta_m)[x]$ be the minimal polynomial of ζ_n over $\mathbb{Q}(\zeta_m)$. Since $\Phi_n(\zeta_n) = 0$, we have $f | \Phi_n$. On the other hand, by the above computation, the Tower Theorem, and Corollary 9.1.10 again, we have

$$\phi(m) \cdot \deg(\Phi_n) = [\mathbb{Q}(\zeta_m, \zeta_n) : \mathbb{Q}] = [\mathbb{Q}(\zeta_m, \zeta_n) : \mathbb{Q}(\zeta_m)] \cdot [\mathbb{Q}(\zeta_m) : \mathbb{Q}] = (\deg f)\phi(m).$$

Dividing both sides by $\phi(m) > 0$, we have $\deg f = \deg \Phi_n$. Since $f | \Phi_n$ with both polynomials monic, it follows that $\Phi_n = f$ is irreducible over $\mathbb{Q}(\zeta_m)$. QED

Problem 4. Cox, Section 9.1, Exercise 15:
Let $\mu : \mathbb{Z}_{\geq 1} \to \mathbb{Z}$ be the Möbius function, defined by

$$\mu(n) = \begin{cases} 1 & \text{if } n = 1, \\ (-1)^s & \text{if } n = p_1 \cdots p_s \text{ for distinct primes } p_1, \ldots, p_s, \\ 0 & \text{otherwise.} \end{cases}$$

Prove that $\Phi_n(x) = \prod_{d|n} (x^d - 1)^{\mu(n/d)}$ for all integers $n \geq 1$.

You may use, without proof, the fact that for any positive integer $n \geq 1$, we have

$$\sum_{d|n} \mu(d) = \begin{cases} 1 & \text{if } n = 1, \\ 0 & \text{if } n \geq 2. \end{cases}$$

Here, in both the product formula you are asked to prove and the sum formula you are allowed to assume, the product (respectively, sum) is over all *positive* integers $d \in \mathbb{Z}_{\geq 1}$ such that $d|n$.

[**Note**: You may be tempted to use some kind of induction, or to use special facts from other courses. Resist these temptations. Instead, use the μ-sum formula above and Proposition 9.1.5.]

Proof. Given $n \geq 1$, applying Proposition 9.1.5 to $x^d - 1$ yields

$$\prod_{d|n} (x^d - 1)^{\mu(n/d)} = \prod_{d|n} \Big(\prod_{k|d} \Phi_k(x) \Big)^{\mu(n/d)} = \prod_{k|n} \Big(\prod_{\substack{d|n \\ \text{s.t. } k|d}} \big(\Phi_k(x)\big)^{\mu(n/d)} \Big) = \prod_{k|n} \prod_{j|(n/k)} \big(\Phi_k(x)\big)^{\mu((n/k)/j)}$$

where we have written $d = kj$. Thus, we have $\prod_{d|n} (x^d - 1)^{\mu(n/d)} = \prod_{k|n} \big(\Phi_k(x)\big)^{E(n,n/k)}$, where

$$E(n, m) = \sum_{j|m} \mu\Big(\frac{m}{j}\Big) = \sum_{i|m} \mu(i) = \begin{cases} 1 & \text{if } m = 1, \\ 0 & \text{if } m \geq 2. \end{cases}$$

Hence, $E(n, n/k)$ is 1 if $k = n$, and 0 otherwise. That is, $\prod_{d|n} (x^d - 1)^{\mu(n/d)} = \Phi_n(x)$. QED

Problem 5. Cox, Section 11.1, Exercise 1:
Let $L/\mathbb{F}_p$ such that $f = x^q - x \in \mathbb{F}_p[x]$ splits completely over L, where $q = p^n$, for some integer $n \geq 1$. Let $F \subseteq L$ be the set of roots of f in L. Prove that F is a subfield of L.

[**Note**: This fact was used in the proof of Proposition 11.1.5, so obviously you cannot quote that result or any results that follow from it. Instead, simply prove that F is a nonempty subset of L that is closed under the four arithmetic operations.]

Proof. We have $0^q = 0$ and $1^p = 1$, so $0, 1 \in F$. If q is odd, then clearly we also have $(-1)^q = -1$. And if q is even, then we must have $p = 2$, and hence $(-1)^q = 1 = -1$. Thus, in all cases, we have $0, 1, -1 \in F$.
Given $\alpha, \beta \in F$, we have $(\alpha\beta)^q = \alpha^q \beta^q = \alpha\beta$, and hence $\alpha\beta \in F$. Since $-1 \in F$, then, we also have $-\alpha \in F$.
If $\alpha \neq 0$, then we have $(\alpha^{-1})^q = \alpha^{-q} = (\alpha^q)^{-1} = \alpha^{-1}$, and hence $\alpha^{-1} \in F$.
Since $q = p^n$ and $(\alpha + \beta)^p = \alpha^p + \beta^p$ (as $\operatorname{char} L = \operatorname{char} \mathbb{F}_p = p$), a quick induction on n shows that $(\alpha + \beta)^q = \alpha^q + \beta^q$. Thus, $(\alpha + \beta)^q = \alpha^q + \beta^q = \alpha + \beta$, and hence $\alpha + \beta \in F$.
Because F is a nonempty subset of L that is closed under addition, negatives, multiplication, and multiplicative inverses, it follows that F is a subfield of L. QED

Problem 6. Cox, Section 11.1, Exercise 11:
Let $f \in \mathbb{F}_p[x]$ be an irreducible polynomial of degree $n \geq 1$. Prove that f splits completely in $\mathbb{F}_{p^n}$.

Proof. Without loss, assume f is monic. Define $q = p^n$.

Let $L = \mathbb{F}_p(\alpha)$, where α is a root of f. [Note: recall, from way back when, that officially the way to do this is to define $L = \mathbb{F}_p[x]/\langle f \rangle$, with α defined to be $x + \langle f \rangle$. But never mind.]

Then $[L : \mathbb{F}_p] = \deg f = n$. Since L is a vector space over $\mathbb{F}_p$ of dimension n, it follows that $|L| = q$. By Corollary 11.1.3, we have $L \cong \mathbb{F}_q$. Thus, $\mathbb{F}_q$ contains a root of f. Call this root $\beta \in \mathbb{F}_q$.
By Theorem 11.1.2(a), β is a root of $x^q - x$, and therefore $f(x)|(x^q - x)$ in $\mathbb{F}_p[x]$, since f is the minimal polynomial of β over $\mathbb{F}_p$. But by Theorem 11.1.2(c), $x^q - x$ splits completely over $\mathbb{F}_q$, and therefore its factor f also splits completely over $\mathbb{F}_q$. QED