# Homework #13

Due **TUESDAY, May 5** in Gradescope by **11:59 pm ET**

**READ** Sections 9.1, 11.1, 11.2 in Cox

**WATCH** 1. Video 35: Cardano, Ferrari, Radical, Solvable (9:30)
2. Video 36: A Cyclotomic Galois Group (7:07)
3. Video 37: Cyclic Multiplicative Group (12:34)

**WRITE AND SUBMIT** solutions to the following problems.

---

**Problem 1.** (5 points, not from Cox):
Let $R, S$ be rings with unity. Prove that $(R \times S)^\times = R^\times \times S^\times$.

**Problem 2.** (5 points) 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 $\alpha$ 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.]

**Problem 3.** (12 points) 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 $\Phi_n$ 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.]

**Problem 4.** (12 points) 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 $\mu$-sum formula above and Proposition 9.1.5.]

(continued next page)

**Problem 5.** (10 points) 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.]

**Problem 6.** (10 points) 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 $\mathbb{F}_{p^n}$.

---

**Optional Challenges (do NOT hand in)**: Cox Problems 9.1 #14; 11.1 #4,8,9

---

**Questions?** You can ask in:

**Class**: MWF 9:00am – 9:50am, SCCE C101

**My office hours**: in my office (SMUD 406):
Mon 2:00–3:30pm
Tue 1:30–3:15pm
Fri 1:00–2:00pm

Also, you may email me any time at `rlbenedetto@amherst.edu`