Math 211 (Modern Algebra II), HW# 4,

Spring 2025; Instructor: Sam Hopkins; Due: Wednesday, March 19th

1. Let $1 \leq k \leq n$ be integers. Prove that k is a unit in the ring $\mathbb{Z}/n\mathbb{Z}$ if and only if $\gcd(k, n) = 1$. Conclude that the following quantities are all equal to Euler's totient function $\varphi(n)$:

   - the order of the group of units $(\mathbb{Z}/n\mathbb{Z})^{\times}$;
   - the number of generators of $(\mathbb{Z}/n\mathbb{Z}, +)$;
   - the degree of the nth cyclotomic polynomial $\Phi_x(n)$;
   - $[\mathbb{Q}(\omega) \colon \mathbb{Q}]$, where ω is a primitive nth root of unity.

2. Let $\Phi_n(x)$ denote the nth cyclotomic polynomial. Prove the following about these $\Phi_n(x)$:

   (a) If $n = p$ is prime, then $\Phi_p(x) = 1 + x + x^2 + \cdots + x^{p-1}$.

   (b) If $n = 2p$ is twice an odd prime p, then $\Phi_{2p}(x) = \Phi_p(-x)$.

   (c) If $n = p^k$ is a power of the prime p, then $\Phi_{p^k}(x) = \Phi_p(x^{p^{k-1}})$.

3. Let $n > 2$, and let ω be a primitive nth root of unity. Prove that $[\mathbb{Q}(\omega + \omega^{-1}) : \mathbb{Q}] = \varphi(n)/2$. **Hint:** It suffices to show $[\mathbb{Q}(\omega) : \mathbb{Q}(\omega + \omega^{-1})] = 2$ (why?). To show $[\mathbb{Q}(\omega) : \mathbb{Q}(\omega + \omega^{-1})] \leq 2$, find a degree two polynomial $f(x) \in \mathbb{Q}(\omega + \omega^{-1})[x]$ which has ω as a root. To show that $\mathbb{Q}(\omega + \omega^{-1}) \neq \mathbb{Q}(\omega)$, think about which of these are subfields of $\mathbb{R}$ versus $\mathbb{C}$.

4. (a) Let $f(x) = ax^3 + bx^2 + cx + d \in \mathbb{Q}[x]$ be a cubic polynomial (so $a \neq 0$). Show that the polynomial $\frac{1}{a} \cdot f(x - \frac{b}{3a})$ has the form $x^3 + px + q$ for $p, q \in \mathbb{Q}$.

   (b) Let $f(x) = x^3 + px + q \in \mathbb{Q}[x]$ with $p \neq 0$ and $q \neq 0$. Show that a root of $f(x)$ has the form $C - \frac{p}{3C}$ where

   $$C = \sqrt[3]{\frac{-q}{2} + \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}}.$$

   (This solution to the cubic equation is often called *Cardano's formula.*)

   (c) Conclude that if $f(x) \in \mathbb{Q}[x]$ is any cubic polynomial, then the splitting field of $f(x)$ is a radical extension of $\mathbb{Q}$.