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

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

In this homework, all roots of unity are meant over the complex numbers $\mathbb{C}$.

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 multiplicative group $(\mathbb{Z}/n\mathbb{Z})^\times$;
   - the number of generators of $(\mathbb{Z}/n\mathbb{Z}, +)$;
   - the number of primitive nth roots of unity;
   - the degree of the nth cyclotomic polynomial $\Phi_n(x)$;
   - $[\mathbb{Q}(\zeta_n) \colon \mathbb{Q}]$, where $\zeta_n = e^{\frac{2\pi i}{n}}$ 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 ζ_n be a primitive nth root of unity. Prove that $[\mathbb{Q}(\zeta_n + \zeta_n^{-1}) : \mathbb{Q}] = \varphi(n)/2$.
   Hint: It suffices to show $[\mathbb{Q}(\zeta_n) : \mathbb{Q}(\zeta_n + \zeta_n^{-1})] = 2$ (why?). To show $[\mathbb{Q}(\zeta_n) : \mathbb{Q}(\zeta_n + \zeta_n^{-1})] \leq 2$, find a degree two polynomial $f(x) \in \mathbb{Q}(\zeta_n + \zeta_n^{-1})[x]$ which has ζ_n as a root. To show that $\mathbb{Q}(\zeta_n + \zeta_n^{-1}) \neq \mathbb{Q}(\zeta_n)$, 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 $f(x) = x^3 + px + q \in \mathbb{Q}[x]$. Show that one root of $f(x)$ has the form $x = \sqrt[3]{A} + \sqrt[3]{B}$ where
   $$A = \frac{-q}{2} + \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}, \quad B = \frac{-q}{2} - \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}.$$
   (This solution to the cubic equation is often called *Cardano's formula*.)
   Hint: First notice (and explain why!) that with $x = \sqrt[3]{A} + \sqrt[3]{B}$ we get
   $$x^3 + px + q = A + B + (3\sqrt[3]{AB} + p)(\sqrt[3]{A} + \sqrt[3]{B}) + q.$$
   Then what can you say about the term $(3\sqrt[3]{AB} + p)$?
   (c) Continue to let $f(x) = x^3 + px + q \in \mathbb{Q}[x]$. Show that the other two roots of $f(x)$ are $x = \omega\sqrt[3]{A} + \omega^2\sqrt[3]{B}$ and $x = \omega^2\sqrt[3]{A} + \omega\sqrt[3]{B}$, where A and B are as above, and $\omega = e^{2\pi i/3}$ is a primitive third root of unity.