1. The goal of this problem is to produce a (particular) proof that the cyclotomic polynomials for a prime p are irreducible. Let p be a prime. The p-th cyclotomic polynomial is $\Phi_p(x) = x^{p-1} + x^{p-2} + \cdots + x^2 + x + 1$. Let $u = e^{2\pi i/p}$. Let $m(x)$ be the minimal monic polynomial for u in $\mathbb{Q}(u)$. Do not assume $m(x) = \Phi_p(x)$.

   (a) A *primitive* p-th root of unity is a complex number ζ such that $\zeta^p = 1$ and $\zeta^k \neq 1$ for any $k < p$. Prove that u is a primitive p-th root of unity.

   Proof. Let $u = e^{i\frac{2\pi}{p}}$, then $u^p = e^{ip\frac{2\pi}{p}} = e^{2\pi i} = 1$
   Recall that the n-th roots of unity form a group G under complex multiplication, with $|G| = n$. Now suppose $u^d = 1$. Then $d|p$ since the order of the element divides the order of the group, and either $d = 1$ (in this case $u = 1$), or $d = p$. So then u must have order p, and u is a primitive p-th root of unity. In fact, any non-identity element in G is a primitive root.

   (b) Verify that each u^k for $k = 1, \ldots, p-1$ is a root of $\Phi_p(x)$

   Solution: Let k be as above, and observe:

   $$\Phi_p(x)(x-1) = (x-1)(x^{p-1} + \ldots + x + 1) = x^p - x^{p-1} + x^{p-1} - x^{p-2} + \ldots - x + x + 1 = x^p - 1.$$

   And since $(u^k)^p - 1 = e^{\frac{2kp\pi i}{p}} - 1 = e^{2ik\pi} - 1 = 1 - 1 = 0$, and u^k is a root of this product of polynomials. But since the linear polynomial $x - 1$ is irreducible and $u^k \neq 1$ for any of the given k, u^k cannot be a root of $x - 1$ and it must instead be a root of the pth cyclotomic polynomial.

   (c) Prove that for any prime $q \neq p$, $m(u^q) = 0$.
   Skipped as per the news item on D2L

   (d) Conclude that $m(x) = \Phi_p(x)$ and that therefore $\Phi_p(x)$ is irreducible.

   Solution: Since Φ_p has a root u, the minimal polynomial $m(x)$ must divide Φ_p. And $m(x)$ by assumption is irreducible and monic, and since it has u^q as a root it must be the minimal polynomial for u^q as well as u. Then take u^k for some $k = 1, \ldots, p-1$. This has a prime factorization $k = q_1 q_2 \ldots q_m$ and by repeating (c) on u with each prime, we can see that $m(u^k) = 0$ and m is minimal for u^k. But since every root of Φ_p is a root of m, $\Phi_p | m$. Since the two polynomials divide each other, they must differ by at most a constant multiple. And since they are both monic and minimal, we must have $m(x) = \Phi_p(x)$.

2. Exercise 6.4.13 If E is an extension of $\mathbb{Z}_p$ and $u \in E$ is a root of $f(x) \in \mathbb{Z}_p[x]$, show that u^p is also a root.

   Solution: Let u be a root of $f(x) \in \mathbb{Z}_p[x]$. Let f have degree n, and write it as $f(x) = a_0 + a_1 x + \ldots + a_n x^n$, with $a_i \in \mathbb{Z}_p$.

   Then let $\sigma : E \to E$ be the automorphism that fixes $\mathbb{Z}_p$ and has $\sigma(u) = u^p$. We know this automorphism to commute with polynomial functions;

$$\begin{aligned} f(\sigma(u)) &= a_0 + a_1\sigma(u) + \ldots + a_n\sigma(u)^n \\ &= \sigma(a_0) + \sigma(a_1)\sigma(u) + \ldots + \sigma(a_n)\sigma(u)^n \\ &= \sigma(a_0) + \sigma(a_1 u) + \ldots + \sigma(a_n u^n) \\ &= \sigma(a_0 + a_1 u + \ldots + a_n u^n) \\ &= \sigma(f(u)) \\ &= \sigma(0) \\ &= 0. \end{aligned}$$

   So $f(\sigma(u)) = \sigma(f(u)) = \sigma(0) = 0$.

3. Exercise 10.1.8: If $E = \mathbb{Q}(\sqrt{2}, \sqrt{3})$, show that $Gal(E : \mathbb{Q}) \cong C_2 \times C_2$.

   Solution: First find the minimal monic polynomials. $x^2 - 2$ for $\sqrt{2}$ is irreducible over $\mathbb{Q}$ by the quadratic equation (Its roots $\pm\sqrt{2}$ are real). For the same reason $x^2 - 3$ is minimal for $\sqrt{3}$, it has roots $\pm\sqrt{3}$. So we have four roots to permute, which tells us that our group must be either $C_2 \times C_2$ or C_4 thanks to our classification of finite groups.

   Let $\sigma \in Gal(E : \mathbb{Q})$ such that $\sigma(\sqrt{2}) = \sqrt{3}$ and $\sigma(\sqrt{3}) = \sqrt{2}$. Then $\sigma^2(\sqrt{2}) = \sigma(\sqrt{3}) = \sqrt{2}$ and $\sigma^2(\sqrt{3}) = \sigma(\sqrt{2}) = \sqrt{3}$. So $\sigma \cdot \sigma = \varepsilon$, and the order of σ is 2.

   Then pick τ so that $\tau(\sqrt{2}) = -\sqrt{2}$ and $\tau(\sqrt{3}) = \sqrt{3}$. Note that we can say that τ is distinct from σ since they are uniquely determined by their action on $\sqrt{2}, \sqrt{3}$. Then $\tau^2(\sqrt{2}) = \tau(-\sqrt{2}) = -\tau(\sqrt{2}) = \sqrt{2}$, and $\tau^2(\sqrt{3}) = \tau(\sqrt{3}) = \sqrt{3}$. So the order of τ is 2, which tells us the Galois group must be $C_2 \times C_2$ since it has two distinct elements of order 2, which C_4 does not.