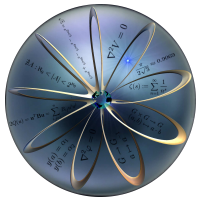

planetmath.org

Math for the people, by the people.

proof that the cyclotomic polynomial is irreducible

Canonical name	ProofThatTheCyclotomicPolynomialIsIrreducible
Date of creation	2013-03-22 12:38:04
Last modified on	2013-03-22 12:38:04
Owner	djao (24)
Last modified by	djao (24)
Numerical id	9
Author	djao (24)
Entry type	Proof
Classification	msc 12E05
Classification	msc 11R60
Classification	msc 11R18
Classification	msc 11C08

We first prove that $\Phi_n(x) \in \mathbb{Z}[x]$. The field extension $\mathbb{Q}(\zeta_n)$ of $\mathbb{Q}$ is the splitting field of the polynomial $x^n - 1 \in \mathbb{Q}[x]$, since it splits this polynomial and is generated as an algebra by a single root of the polynomial. Since splitting fields are normal, the extension $\mathbb{Q}(\zeta_n)/\mathbb{Q}$ is a Galois extension. Any element of the Galois group, being a field automorphism, must map ζ_n to another root of unity of exact order n. Therefore, since the Galois group of $\mathbb{Q}(\zeta_n)/\mathbb{Q}$ permutes the roots of $\Phi_n(x)$, it must fix the coefficients of $\Phi_n(x)$, so by Galois theory these coefficients are in $\mathbb{Q}$. Moreover, since the coefficients are algebraic integers, they must be in $\mathbb{Z}$ as well.

Let $f(x)$ be the minimal polynomial of ζ_n in $\mathbb{Q}[x]$. Then $f(x)$ has integer coefficients as well, since ζ_n is an algebraic integer. We will prove $f(x) = \Phi_n(x)$ by showing that every root of $\Phi_n(x)$ is a root of $f(x)$. We do so via the following claim:

Claim: For any prime p not dividing n, and any primitive n^{th} root of unity $\zeta \in \mathbb{C}$, if $f(\zeta) = 0$ then $f(\zeta^p) = 0$.

This claim does the job, since we know $f(\zeta_n) = 0$, and any other primitive n^{th} root of unity can be obtained from ζ_n by successively raising ζ_n by prime powers p not dividing n a finite number of times[1].

To prove this claim, consider the factorization $x^n - 1 = f(x)g(x)$ for some polynomial $g(x) \in \mathbb{Z}[x]$. Writing $\mathcal{O}$ for the ring of integers of $\mathbb{Q}(\zeta_n)$, we treat the factorization as taking place in $\mathcal{O}[x]$ and proceed to mod out both sides of the factorization by any prime ideal $\mathfrak{p}$ of $\mathcal{O}$ lying over (p). Note that the polynomial $x^n - 1$ has no repeated roots mod $\mathfrak{p}$, since its derivative nx^{n-1} is relatively prime to $x^n - 1 \bmod \mathfrak{p}$. Therefore, if $f(\zeta) = 0 \bmod \mathfrak{p}$, then $g(\zeta) \neq 0 \bmod \mathfrak{p}$, and applying the p^{th} power Frobenius map to both sides yields $g(\zeta^p) \neq 0 \bmod \mathfrak{p}$. This means that $g(\zeta^p)$ cannot be 0 in $\mathbb{C}$, because it doesn't even equal 0 mod $\mathfrak{p}$. However, ζ^p is a root of $x^n - 1$, so if it is not a root of g, it must be a root of f, and so we have $f(\zeta^p) = 0$, as desired.

[1] Actually, if one applies Dirichlet's theorem on primes in arithmetic progressions here, it turns out that one prime is enough, but we do not need such a sharp result here.