IRREDUCIBILITY OF CYCLOTONIC POLYNOMIALS

Let $\Phi_n(X) \in \mathbb{Q}[X]$ denote the $n$th cyclotomic polynomial for $n > 1$. This writeup will show that $\Phi_n$ is irreducible. The argument, making use of Dirichlet’s theorem on primes in an arithmetic progression and of localization, was explained to me by Paul Garrett, and the details are based on a treatment by Keith Conrad.

Let $p$ be an odd prime and let $n = p^e$. The group $(\mathbb{Z}/p^e\mathbb{Z})^\times$ is cyclic, $(\mathbb{Z}/p^e\mathbb{Z})^\times = \langle g \mod p^e \rangle$.

By Dirichlet’s theorem, there exists a prime $\ell = g \mod p^e$. In the diagram

\[ \xymatrix{ & \mathbb{Q}(\zeta_{p^e}) \ar[d]^{d_{\ell}} \ar[rd] & \\
\mathbb{Q}(\zeta_{p^e}) \ar[d]^{d} & & \mathbb{Q}_\ell \\
\mathbb{Q} \ar[rr] & & \mathbb{Q}_\ell }
\]

we know that $d_{\ell} | d$ (by Galois theory) and that $d \leq \phi(p^e)$ (since $\zeta_{p^e}$ satisfies $\Phi_{p^e}$, whose degree is $\phi(p^e)$), and we want to show that $d = \phi(p^e)$. But the extension $\mathbb{Q}_\ell(\zeta_{p^e})/\mathbb{Q}_\ell$ is unramified, and its degree $d_{\ell}$ is the order of $\ell$ modulo $p^e$. Thus, by our choice of $\ell$, $d_{\ell} = \phi(p^e)$. It follows that $d = \phi(p^e)$ as desired. This argument also works if $n = 2$ or $n = 4 = 2^2$.

(Also, this argument really doesn’t require any localization. A variant argument is that the extension $\mathbb{Q}(\zeta_{p^e})/\mathbb{Q}$ has degree at least the inertial degree $f(\ell)$ for any prime $\ell$ and degree at most $\phi(p^e)$. As above, Dirichlet’s theorem supplies a prime $\ell = g \mod p^e$, so that $f(\ell)$, being the order of $\ell$ modulo $p^e$, is $\phi(p^e)$. However, the argument used localization to introduce some ideas that will be necessary to prove the irreducibility of $\Phi_n$ for general $n$.)

If $n = 2^e$ with $e \geq 3$ then the argument is slightly more complicated because $(\mathbb{Z}/2^e\mathbb{Z})^\times$ is not cyclic. Retaining the notation and diagram from the previous paragraph but with $p = 2$, take $\ell = 5$, so that $(\mathbb{Z}/2^e\mathbb{Z})^\times = (\ell) \times \{\pm 1\}$.

In the diagram we now have $d_5 = \phi(2^e)/2$, so that $d \in \{\phi(2^e)/2, \phi(2^e)\}$. More specifically, the upper Galois group

\[ \text{Gal}(\mathbb{Q}_\ell(\zeta_{2^e})/\mathbb{Q}_\ell) \cong \{\zeta_{2^e} \mapsto \zeta_{2^e}^k : k \equiv 1 \mod 4\} \]

embeds in the lower Galois group $\text{Gal}(\mathbb{Q}(\zeta_{2^e})/\mathbb{Q})$. However, the lower Galois group also contains complex conjugation,

\[ \zeta_{2^e} \mapsto \zeta_{2^e}^{2^e-1}, \]

1.
and $2^e - 1 = 3 \mod 4$. Thus $d = \phi(2^e)$ as desired.

For the general case $n = \prod p^e$, proceed by induction in the number of distinct prime factors of $n$. We have covered the base case of one distinct prime factor. For more than one distinct prime factor, let $p$ be the largest such, and write

$$n = mp^e, \quad (m,p) = 1.$$ 

For any prime $\ell$, consider the diagram

\[
\begin{array}{c}
\mathbb{Q}(\zeta_n) = \mathbb{Q}(\zeta_m, \zeta_{p^e}) \\
\mathbb{Q}(\zeta_m) \\
\mathbb{Q}(\zeta_{p^e})
\end{array}
\]

Again we know that $d_\ell \mid d \leq \phi(p^e)$ and we want to show that $d = \phi(p^e)$. Since $p > 2$, again let $(\mathbb{Z}/p^e\mathbb{Z})^\times = (g \mod p^e)$.

By Dirichlet’s theorem and the Sun-Ze theorem, there exist primes $\ell$ that satisfy the conditions

$$\ell = 1 \mod m \quad \text{and} \quad \ell = g \mod p^e.$$ 

Since $\ell = 1 \mod m$, the right side of the diagram simplifies (and we drop the lowest part of the left side),

\[
\begin{array}{c}
\mathbb{Q}(\zeta_{p^e}) \\
\mathbb{Q}(\zeta_m, \zeta_{p^e}) \\
\mathbb{Q}(\zeta_m)
\end{array}
\]

As before, since $\ell = g \mod p^e$, we now get $d = \phi(p^e)$. This completes the argument.