Student: Yu Cheng (Jade)

Math 612

Final Presentation Draft

April 27, 2011

Problem: Show that $\Phi_n(x)$ is irreducible over $\mathbb{Q}$.

Proof: First we want to show that $\Phi_n(x) \in \mathbb{Z}[x]$. This is proved in class by induction.

The root of unity ζ_n is an algebraic integer since there exists a monic polynomial, $x^n - 1$, such that ζ is a root. Equivalently, the minimal polynomial $m_{\zeta_n}(x) \in \mathbb{Q}[x]$ is in $\mathbb{Z}[x]$. We claim that $\Phi_n(x) = m_{\zeta_n}(x)$. By definition, $m_{\zeta_n}(x)$ is monic and irreducible over $\mathbb{Q}$, so $\Phi_n(n)$ is irreducible over $\mathbb{Q}$.

We can express $m_{\zeta_n}(x)$ as the following, where $a_1, \cdots, a_r \in \mathbb{Q}$ are the roots.

$$m_{\zeta_n}(x) = (x - a_1) \cdot (x - a_2) \cdot \cdots \cdot (x - a_r).$$

According to its definition $\Phi_n(x)$ can be expressed as the following, where $b_1, \cdots, b_s \in \mathbb{Q}$ are the roots and $s = \varphi(x)$. φ is the Euler's totient function, the number of positive integers less than or equal to n that are co-prime to n.

$$\begin{aligned}\Phi_n(x) &= \prod_{\substack{gcd(a,n)=1 \\ 1 \leq a < n}} (x - \zeta_n^a) \\ &= (x - b_1) \cdot (x - b_2) \cdot \cdots \cdot (x - b_s).\end{aligned}$$

To prove the claim, $\Phi_n(x) = m_{\zeta_n}(x) \in \mathbb{Q}$, we want to show that all roots of $m_{\zeta_n}(x)$ are also the roots for $\Phi_n(x)$, and vice versa. Since $m_{\zeta_n}(x)$ is irreducible over $\mathbb{Q}$, we just need to show all roots for $\Phi_n(x)$ are also roots for $m_{\zeta_n}(x)$. Because if there are other roots in $m_{\zeta_n}(x)$ that are not in $\Phi_n(x)$, it indicates $\Phi_n(x) \in \mathbb{Q}$ is a factor of $m_{\zeta_n}(x)$. This is a conflict.

All roots for $\Phi_n(x)$ are in the form ζ_n^p where p is a positive integer co-prime with n.

$$\begin{aligned}\Phi_n(x) &= \prod_{\substack{gcd(a,n)=1 \\ 1 \leq a < n}} (x - \zeta_n^a) \\ &= (x - \zeta_n^{p_1}) \cdot (x - \zeta_n^{p_2}) \cdot \cdots \cdot (x - \zeta_n^{p_s}).\end{aligned}$$

So the problem is converted to proving an arbitrary ζ_n^p is a root for $m_{\zeta_n}(x)$. We will prove this by contradiction. Let's assume that ζ_n^p is not a root for $m_{\zeta_n}(x)$. Since ζ_n^p is a root in $x^n - 1$ we have the following relation.

$$\begin{aligned}
&x^n - 1 = m_{\zeta_n}(x) \cdot g(x) \\
&\Rightarrow g(\zeta_n^p) = 0.
\end{aligned}$$

We can consider ζ_n as a root for polynomial $g(x^p)$. Since $m_{\zeta_n}(x)$ is the minimal polynomial of ζ_n, $m_{\zeta_n}(x)$ has to be a factor in $g(x^p)$.

$$g(x^p) = m_{\zeta_n}(x) \cdot h(x).$$

Let's take the polynomials on both sides and mod p.

$$\begin{aligned}
&g'(x^p) = m'_{\zeta_n}(x) \cdot h'(x) \\
&g'(x^p),\ m'_{\zeta_n}(x),\ h'(x) \in \mathbb{Q}_p[x].
\end{aligned}$$

According to proposition 35 in Dummit & Foote, if a field F has a characteristic p, then for any $a, b \in F$ we have the following.

$$\begin{aligned}
a^p + b^p &= (a+b)^p \\
a^p b^p &= (ab)^p.
\end{aligned}$$

Hence, we derive that $g'(x^p) = [g'(x)]^p$.

$$\begin{aligned}
g'(x^p) &= c_0 + c_1 x^p + c_2 (x^p)^2 + c_3 (x^p)^3 + \cdots \\
&= c_0 + c_1 x^p + c_2 \left(x^2\right)^p + c_3 \left(x^3\right)^p + \cdots \\
&= \left(c_0 + c_1 x + c_2 x^2 + c_3 x^3 \cdots\right)^p \\
&= [g'(x)]^p.
\end{aligned}$$

Plug this in the earlier equation.

$$[g'(x)]^p = m'_{\zeta_n}(x) \cdot h'(x).$$

Since $\mathbb{Q}_p$ is a UFD, there is only one way to factorize a polynomial in $\mathbb{Q}_p$. Therefore,$m'_{\zeta_n}(x)$ and $g'(x)$ have to share at least one common factor $I(x) \in \mathbb{Q}_p[x]$. Recall that we have $x^n - 1 = m_{\zeta_n}(x) \cdot g(x)$. We can mod p on both sides of this equation as well.

$$\begin{aligned}
(x^n - 1) \mathit{mod}\, p &= m'_{\zeta_n}(x) \cdot g'(x) \\
&= [I(x)]^2 \cdot J(x) \\
I(x),\ J(x) &\in \mathbb{Q}_p[x].
\end{aligned}$$

This indicates that $(x^n - 1) \, mod \, p$ has duplicate roots in $\mathbb{Q}_p$. Furthermore, $x^n - 1$ has duplicate roots in $\mathbb{Q}_p$ since $(x^n - 1) \, mod \, p$ is a factor in $x^n - 1$. Now, let's evaluate the derivative polynomial of $x^n - 1$.

$$D_x (x^n - 1) \quad = \quad nx^{n-1}$$

According to proposition 33 in Dummit & Foote, a polynomial $f(x)$ has a multiple root α if and only if α is also a root of $D_x f(x)$. But $x^n - 1$ does not share any common factor with nx^{n-1} for p being relatively prime to n.

So, we've derived a contradiction. Namely, $x^n - 1$ cannot have duplicated roots in $\mathbb{Q}_p$. Therefore, ζ_n^p has to be a root in $m_{\zeta_n}(x)$ rather than a root in $g(x)$, for $x^n - 1 = m_{\zeta_n}(x) \cdot g(x)$.

At this point, we've shown all roots in $\Phi_n(x)$ are also roots in $m_{\zeta_n}(x)$, and hence $\Phi_n(x) = m_{\zeta_n}(x)$. Since $m_{\zeta_n}(x)$ is irreducible over $\mathbb{Q}$, $\Phi_n(x)$ is irreducible over $\mathbb{Q}$.