IRREDUCIBILITY OF THE CYCLOTOMIC POLYNOMIAL

JUNNOSUKE KOIZUMI

Abstract. In this note, we present a geometric proof of the irreducibility of the cyclotomic polynomial using the language of schemes.

We fix a positive integer n.

Definition 0.1. We set $\zeta_n = e^{2\pi i/n}$ and define $\Phi_n \in \overline{\mathbb{Q}}[T]$ by $\Phi_n = \prod_{k\in(\mathbb{Z}/n\mathbb{Z})^\times}(T-\zeta_n^k)$.

Lemma 0.2. $\Phi_n \in \mathbb{Z}[T]$.

Proof. The set $S = \{\zeta^k \mid k \in (\mathbb{Z}/n\mathbb{Z})^\times\}$ can be written as $S = \{a \in \overline{\mathbb{Q}} \mid a^n = 1,\ a^d \neq 1\ (0 < d < n)\}$. Therefore for any $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, we have $\sigma(S) = S$ and hence $\sigma(\Phi_n) = \Phi_n$. This shows that $\Phi_n \in \mathbb{Q}[T]$. Since $\Phi_n \mid T^n - 1$, we get $\Phi_n \in \mathbb{Z}[T]$ by Gauss's lemma. □

Lemma 0.3. *For any positive integer m which is coprime to n, we have $\Phi_n(T) \mid \Phi_n(T^m)$.*

Proof. For any $k \in (\mathbb{Z}/n\mathbb{Z})^\times$, we have $\Phi_n((\zeta_n^k)^m) = \Phi_n(\zeta_n^{km}) = 0$. This proves the claim. □

Definition 0.4. We define a ring A_n by $A_n = \mathbb{Z}[1/n][T]/(\Phi_n)$, and we set $X_n = \operatorname{Spec} A_n$.

Lemma 0.5. *The canonical morphism $\pi\colon X_n \to \operatorname{Spec}\mathbb{Z}[1/n]$ is finite étale.*

Proof. It is obvious that π is finite locally free and hence flat. We have

$$\Omega_{A_n/\mathbb{Z}[1/n]} \simeq \mathbb{Z}[1/n][T]/(\Phi_n, \Phi_n'),$$

so it suffices to show that the right hand side is zero. If we write $T^n - 1 = \Phi_n\Psi_n$, then we get

$$nT^{n-1} = \Phi_n'\Psi_n + \Phi_n\Psi_n' \in (\Phi_n, \Phi_n')$$

and hence $T^{n-1} \in (\Phi_n, \Phi_n')$ in $\mathbb{Z}[1/n][T]$. This shows that $(\Phi_n, \Phi_n') = \mathbb{Z}[1/n][T]$. □

Theorem 0.6. *X_n is integral. In other words, Φ_n is irreducible in $\mathbb{Z}[1/n][T]$.*

Proof. By Lemma 0.5, the scheme X_n is a noetherian normal scheme. Therefore X_n can be written as a disjoint union of integral schemes. Each connected component of X_n is also finite étale over $\operatorname{Spec}\mathbb{Z}[1/n]$ and hence surjective over $\operatorname{Spec}\mathbb{Z}[1/n]$. Let $\pi_0(X_n)$ denote the set of connected components of X_n. It suffies to show that $\pi_0(X_n)$ has only one element.

By Lemma 0.3, we can define a ring homomorphism

$$\varphi_m\colon A_n \to A_n; \quad T \mapsto T^m$$

for any positive integer m which is coprime to n. Let F_m denote the induced morphism of schemes $X_n \to X_n$. We can define an action of $(\mathbb{Z}/n\mathbb{Z})^\times$ on X_n by letting $[m]$ act by F_m. We prove that the action of $(\mathbb{Z}/n\mathbb{Z})^\times$ on $\pi_0(X_n)$ is both trivial and transitive.

Let p be any prime number not dividing n. Then $F_p \otimes \mathrm{id}\colon X_n \otimes_{\mathbb{Z}[1/n]} \mathbb{F}_p \to X_n \otimes_{\mathbb{Z}[1/n]} \mathbb{F}_p$ coincides with the absolute Frobenius morphism, so the action of $[p] \in (\mathbb{Z}/n\mathbb{Z})^\times$ on the fiber of

$(p) \in \operatorname{Spec} \mathbb{Z}[1/n]$ is set-theoretically trivial. Since every connected component of X_n intersects with this fiber, the action of $[p] \in (\mathbb{Z}/n\mathbb{Z})^\times$ on $\pi_0(X_n)$ is trivial. Moreover, since the images of prime numbers generate the group $(\mathbb{Z}/n\mathbb{Z})^\times$, we can conclude that the action of $(\mathbb{Z}/n\mathbb{Z})^\times$ on $\pi_0(X_n)$ is trivial.

On the other hand, the set $X_n(\overline{\mathbb{Q}})$ of $\overline{\mathbb{Q}}$-valued points can be identified with $S = \{\zeta_n^k \mid k \in (\mathbb{Z}/n\mathbb{Z})^\times\}$. The action of $[m] \in (\mathbb{Z}/n\mathbb{Z})^\times$ on $X_n(\overline{\mathbb{Q}})$ is identified with $\zeta_n^k \mapsto \zeta_n^{km}$, so the action of $(\mathbb{Z}/n\mathbb{Z})^\times$ on $X_n(\overline{\mathbb{Q}})$ is transitive. Any point of X_n lying over $(0) \in \operatorname{Spec} \mathbb{Z}[1/n]$ is the image of some $\overline{\mathbb{Q}}$-valued point, so the action of $(\mathbb{Z}/n\mathbb{Z})^\times$ on the fiber of $(0) \in \operatorname{Spec} \mathbb{Z}[1/n]$ is transitive. Since every connected component of X_n intersects with this fiber, this shows that the action of $(\mathbb{Z}/n\mathbb{Z})^\times$ on $\pi_0(X_n)$ is transitive. □

Corollary 0.7. *Φ_n is irreducible in $\mathbb{Q}[T]$.*

Proof. This follows from Theorem 0.6 and Gauss's lemma. □