Quelques propriétés des polynômes cyclotomiques et des entiers algébriques

6 décembre 2018

1 Généralités

Notations : Si m est un entier naturel, on note U_m le groupe des racines m-ièmes de l'unité dans $\mathbf{C}$ et P_m l'ensemble de ses générateurs.

1.1

On note pour m entier, $m \geq 1$,

$$\Phi_m(X) = \prod_{1 \leq k \leq m, k \wedge m = 1} (X - e^{\frac{2ik\pi}{m}})$$

le m-ième polynôme cyclotomique.
a) Déterminer Φ_n lorsque n est un nombre premier.
b) Montrer que, pour tout entier $n \geq 1$,

$$X^n - 1 = \prod_{d|n} \Phi_d(X)$$

c) Prouver que, pour tout m, $\Phi_m(X) \in \mathbf{Z}[X]$.

1.2

On suppose les entiers naturels m et n premiers entre eux. Comparer $\Phi_{mn}(X)$ et $\Phi_m(X)\Phi_n(X)$.

2 Une version simple du théorème de Dirichlet

2.1

Soit $P \in \mathbf{Z}[X]$ non constant.
a) Soit $(k, n) \in \mathbf{N}^* \times \mathbf{N}^*$. Montrer qu'il existe un entier m tel que $P(n + kP(n)) = P(n)(1 + kP(n)m)$.

b) Montrer que l'ensemble des nombres premiers p tels que

$$\exists n \in \mathbf{N}^*, P(n) \text{ non nul et } p \,|\, P(n)$$

est infini. On pourra raisonner par l'absurde, noter π le produit des facteurs premiers distincts intervenant dans les entiers $P(n)$, et envisager pour l et n grands le nombre $P(n + l\pi P(n))$

2.2

On fixe un entier $m \geq 2$. Soient p un nombre premier ne divisant pas m et a un entier naturel tels que $\Phi_m(a) \equiv 0[p]$. On note $\overline{x}$ la classe d'un entier x dans $\mathbf{Z}/p\mathbf{Z}$.
a) Montrer que $a^m \equiv 1[p]$.
b) Soit d l'ordre de $\overline{a}$ dans $\mathbf{Z}/p\mathbf{Z}^*$. Montrer que d divise m et que $\Phi_\delta(a) = 0$ pour l'un des diviseurs δ de d.
c) Si $d < m$ monter que $\overline{a}$ annule la dérivée de $X^m - 1$ dans $\mathbf{Z}/p\mathbf{Z}$. En déduire que $p \equiv 1[m]$.
d) En déduire que l'ensemble des nombres premiers de la forme $1+km$ est infini.

3

Soient p un nombre premier ≥ 3, et P un polynôme non nul de $\mathbf{Z}[X]$. On dit que P vérifie (S) lorsque le polynôme de $\mathbf{Z}/p\mathbf{Z}[X]$ obtenu par réduction de P modulo p est scindé à racines simples dans $\mathbf{Z}/p\mathbf{Z}$.

3.1

a) Soit $m \in \mathbf{N}^*$, $\zeta \in U_m$ d'ordre m et $\eta \in U_p$. Etudier l'ordre de $\zeta\eta$.

b) On note $n = mp$. Montrer que $\Phi_n(X) = \frac{\Phi_m(X^p)}{\Phi_m(X)}$ si p ne divise pas m, et $\Phi_n(X) = \Phi_m(X^p)$ sinon. En déduire que Φ_n ne vérifie pas (S).

b) Soit $n \in \mathbf{N}^*$. On suppose que p divise $n-1$. Montrer que Φ_n vérifie (S).

c) Etablir la réciproque du résultat précédent.