UN THÉORÈME DE KRONECKER ET SES ALENTOURS

On note $\mathbb{Z}[X]$ l'ensemble des polynômes à une indéterminée X à coefficients dans $\mathbb{Z}$. On souhaite établir le résultat suivant :

Théorème (Théorème de Kronecker) Soit $P \in \mathbb{Z}[X]$ unitaire non constant. On suppose que les racines de P dans $\mathbb{C}$ sont non nulles et de module inférieur ou égal à 1. Leur ensemble est alors inclus dans $\mathbb{U}_r$ pour un certain $r \in \mathbb{N}^*$.

Pour tout $n \in \mathbb{N}^*$, on note $\mathcal{K}_n$ l'ensemble des polynômes de $\mathbb{Z}[X]$ unitaires de degré n dont les racines dans $\mathbb{C}$ sont toutes non nulles et de module inférieur ou égal à 1, ainsi que $\mathcal{R}_n$ l'ensemble des racines des polynômes éléments de $\mathcal{K}_n$.

Pour tout $P \in \mathbb{C}[X]$ non constant de degré n, on note $\sigma_1(P), \ldots, \sigma_n(P)$ les fonctions symétriques élémentaires de P.

1) **a)** Soit $P \in \mathcal{K}_2$. Montrer que les racines de P dans $\mathbb{C}$ sont de module 1.
b) Déterminer l'ensemble $\mathcal{K}_2$ et montrer que : $\mathcal{R}_2 = \mathbb{U}_4 \cup \mathbb{U}_6$. Prouver enfin le théorème de Kronecker pour $n = 2$.

2) **a)** Montrer que pour tous $n \in \mathbb{N}^*$ et $k \in [\![1, n]\!]$: $\sigma_k\big((X-1)^n\big) \leqslant 2^n$.
b) En déduire que pour tous $n \in \mathbb{N}^*$, $P \in \mathcal{K}_n$ et $k \in [\![1, n]\!]$: $\big|\sigma_k(P)\big| \leqslant 2^n$.
c) En déduire que les ensembles $\mathcal{K}_n$ et $\mathcal{R}_n$ sont finis.

3) Soit $P \in \mathbb{Z}[X]$ non constant de degré n.
a) Justifier l'existence d'un polynôme $\widehat{P} \in \mathbb{Z}[X]$ de degré n pour lequel : $P(X)\, P(-X) = (-1)^n \widehat{P}\big(X^2\big)$.
b) Décrire la forme scindée sur $\mathbb{C}$ de $\widehat{P}$ en fonction de celle de P.
c) Montrer que si : $P \in \mathcal{K}_n$, alors : $\widehat{P} \in \mathcal{K}_n$.
d) En déduire que l'ensemble $\mathcal{R}_n$ est stable par la fonction $z \longmapsto z^2$ pour tout $n \in \mathbb{N}^*$.

4) Démontrer enfin le théorème de Kronecker.

On va maintenant s'intéresser à une famille importante de polynômes unitaires à coefficients entiers dont les racines sont non nulles et de module 1.

Définition (Polynômes cyclotomiques) Pour tout $n \in \mathbb{N}^*$, on pose : $\mathbb{P}_n = \big\{k \in [\![0, n-1]\!] / \quad k \wedge n = 1\big\}$ et on note Φ_n le $n^{\text{ème}}$ *polynôme cyclotomique*, i.e. le polynôme : $\displaystyle\prod_{k \in \mathbb{P}_n} \left(X - e^{\frac{2ik\pi}{n}}\right)$ dont les coefficients sont a priori complexes.

5) Calculer Φ_n pour tout $n \in [\![1, 4]\!]$ et Φ_p pour tout $p \in \mathbb{P}$.

6) Soient $A, B \in \mathbb{Z}[X]$. On suppose que B est unitaire et qu'il existe un polynôme $C \in \mathbb{C}[X]$ pour lequel : $A = BC$.
a) Justifier l'existence d'un polynôme R de degré minimal r, éventuellement $-\infty$, dans l'ensemble $\big\{A - BZ\big\}_{Z \in \mathbb{Z}[X]}$.
b) Montrer que : $r < \deg(B)$.
c) En déduire que : $C \in \mathbb{Z}[X]$.

7) Soit $n \in \mathbb{N}^*$. On note $\operatorname{div}(n)$ l'ensemble des diviseurs **POSITIFS** de n et f la fonction $k \longmapsto k \wedge n$ définie sur $[\![0, n-1]\!]$.
a) Montrer que la fonction $r \longmapsto dr$ est bijective de $\mathbb{P}_{\frac{n}{d}}$ sur $f^{-1}\big(\{d\}\big)$ pour tout $d \in \operatorname{div}(d)$.
b) Montrer que pour tout $d \in \operatorname{div}(n)$: $\displaystyle\Phi_{\frac{n}{d}} = \prod_{k \in f^{-1}(\{d\})} \left(X - e^{\frac{2ik\pi}{n}}\right)$.
c) En déduire que : $\displaystyle X^n - 1 = \prod_{d \in \operatorname{div}(n)} \Phi_d$.

8) Montrer que pour tout $n \in \mathbb{N}^*$: $\Phi_n \in \mathbb{Z}[X]$.

On peut montrer en travaillant davantage que Φ_n est *irréductible sur* $\mathbb{Z}$ pour tout $n \in \mathbb{N}^*$, i.e. que pour tous $A, B \in \mathbb{Z}[X]$: $\Phi_n = AB \implies A = \pm 1$ ou $B = \pm 1$. Une caractérisation explicite des polynômes du théorème de Kronecker en découle. Les polynômes unitaires à coefficients entiers dont les racines dans $\mathbb{C}$ sont de module inférieur ou égal à 1 sont exactement les produits qu'on peut faire à partir du polynôme X et des polynômes cyclotomiques — par exemple $X^4 \Phi_3 \Phi_8^5$.