KRONECKER ET LANDAU-MIGNOTTE

Les deux parties de ce devoir sont indépendantes.

On note $\mathbb{Z}[X]$ l'ensemble des polynômes à une indéterminée X à coefficients dans $\mathbb{Z}$.

Pour tous $n \in \mathbb{N}^*$, $k \in [\![1,n]\!]$ et $z_1,\dots,z_n \in \mathbb{C}$, on pose : $\sigma_k(z_1,\dots,z_n) = \sum_{i_1<\dots<i_k} z_{i_1}\dots z_{i_k}$, mais cette quantité sera aussi notée $\sigma_k(P)$ pour tout polynôme $P = a(X-z_1)\dots(X-z_n)$ avec $a \in \mathbb{C}^*$.

Trois niveaux de difficulté/longueur :

— Piste verte : questions **1)** à **4)** du premier problème.

— Piste bleue : questions **1)** à **4)** du premier problème et tout le deuxième problème.

— Piste rouge : tout le devoir.

1 THÉORÈME DE KRONECKER ET POLYNÔMES CYCLOTOMIQUES

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 de module inférieur ou égal à 1. Leur ensemble est alors inclus dans $\{0\} \cup \mathbb{U}_r$ pour un certain $r \in \mathbb{N}^*$.

Pour tout $n \in \mathbb{N}^*$, on note $\mathscr{K}_n$ 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 $\mathscr{R}_n$ l'ensemble des racines des polynômes éléments de $\mathscr{K}_n$.

1) a) Montrer que les racines de P dans $\mathbb{C}$ sont de module 1 pour tout $P \in \mathscr{K}_2$.

b) Déterminer $\mathscr{K}_2$, puis montrer que $\mathscr{R}_2 = \mathbb{U}_4 \cup \mathbb{U}_6$.

Dans les questions **2)**, **3)** et **4)**, l'entier $n \in \mathbb{N}^*$ est fixé.

2) a) Majorer pour tous $P \in \mathscr{K}_n$ et $k \in [\![1,n]\!]$ le réel $\left|\sigma_k(P)\right|$ en fonction de n et k, mais indépendamment de P.

b) Combien existe-t-il, pour tout $N \in \mathbb{N}$, de polynômes de $\mathbb{Z}[X]$ unitaires de degré n à coefficients dans $[\![-N,N]\!]$?

c) En déduire que l'ensemble $\mathscr{R}_n$ est fini.

3) Soit $P \in \mathbb{Z}[X]$ non constant de degré n.

a) Montrer qu'il existe un et un seul polynôme $\widehat{P} \in \mathbb{Z}[X]$ — à coefficients entiers, donc — de degré n pour lequel $P(X)P(-X) = (-1)^n \widehat{P}\left(X^2\right)$.

b) Décrire la forme scindée sur $\mathbb{C}$ de $\widehat{P}$ en fonction de celle de P.

c) Montrer que si $P \in \mathscr{K}_n$, alors $\widehat{P} \in \mathscr{K}_n$.

d) En déduire que l'ensemble $\mathscr{R}_n$ est stable par la fonction $z \longmapsto z^2$.

4) a) Montrer que $\mathscr{R}_n$ est inclus dans $\mathbb{U}_r$ pour un certain $r \in \mathbb{N}^*$.

b) En déduire le *théorème de Kronecker*.

On s'intéresse finalement 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 $\mathbb{P}_n = \left\{k \in [\![0,n-1]\!] \mid \quad k \wedge n = 1\right\}$ et on note Φ_n le $n^{ème}$ *polynôme cyclotomique*, i.e. le polynôme $\prod_{k\in\mathbb{P}_n}\left(X - \mathrm{e}^{\frac{2ik\pi}{n}}\right)$ 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 $A = BC$. Montrer que $C \in \mathbb{Z}[X]$ en adaptant la preuve du théorème de la division euclidienne.

Pour tout $n \in \mathbb{N}^*$, on note à présent $\mathrm{div}^+(n)$ l'ensemble des diviseurs positifs de n.

7) Soit $n \in \mathbb{N}^*$ fixé. Pour tout $d \in \mathrm{div}^+(n)$, on pose $E_d = \left\{k \in [\![0, n-1]\!] \mid \quad k \wedge n = d\right\}$.

a) Montrer que la fonction $r \longmapsto dr$ est bijective de $\mathbb{P}_{\frac{n}{d}}$ sur E_d pour tout $d \in \mathrm{div}^+(n)$.

b) Montrer que pour tout $d \in \mathrm{div}^+(n)$: $\quad \Phi_{\frac{n}{d}} = \prod_{k \in E_d} \left(X - \mathrm{e}^{\frac{2\mathrm{i}k\pi}{n}}\right)$.

c) En déduire que $X^n - 1 = \prod_{d \in \mathrm{div}^+(n)} \Phi_d$.

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

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 $X^4\Phi_3\Phi_8^5$.

2 Inégalité de Landau et borne de Mignotte

Pour tout $P = \sum_{k=0}^{+\infty} a_k X^k \in \mathbb{C}[X]$, on pose : $\quad \|P\|_1 = \sum_{k=0}^{+\infty} |a_k|$ $\quad$ et $\quad \|P\|_2 = \sqrt{\sum_{k=0}^{+\infty} |a_k|^2}$, $\quad$ et si P est non constant de degré n et de racines $z_1, \dots, z_n$ dans $\mathbb{C}$ comptées avec multiplicité, on pose également : $\quad M(P) = |a_n| \prod_{i=1}^{n} \max\left\{1, |z_i|\right\}$.

1) Montrer que pour tous $P, Q \in \mathbb{C}[X]$ non constants : $\quad M(PQ) = M(P)M(Q)$.

2) **a)** Montrer que pour tous $P = \sum_{k=0}^{+\infty} a_k X^k \in \mathbb{C}[X]$ et $\lambda, \mu \in \mathbb{C}$:

$$\left\|(\lambda X + \mu)P\right\|_2^2 = \left(|\lambda|^2 + |\mu|^2\right)\|P\|_2^2 + 2\sum_{k=0}^{+\infty} \mathrm{Re}\left(\overline{\lambda}\mu\,\overline{a_k}\,a_{k+1}\right).$$

b) En déduire que pour tous $P \in \mathbb{C}[X]$ et $z \in \mathbb{C}$: $\quad \left\|(X - z)P\right\|_2 = \left\|\left(\overline{z}X - 1\right)P\right\|_2$.

3) Soit $P \in \mathbb{C}[X]$ non constant de degré n, de coefficient dominant a_n et de racines $z_1, \dots, z_n$ dans $\mathbb{C}$ comptées avec multiplicité. Quitte à réordonner $z_1, \dots, z_n$, on peut supposer sans perte de généralité que $|z_i| \leqslant 1$ pour tout $i \in [\![1, r]\!]$ et $|z_i| > 1$ pour tout $i \in [\![r+1, n]\!]$.

On pose $\widetilde{P} = a_n \prod_{i=1}^{r} (X - z_i) \prod_{j=r+1}^{n} \left(\overline{z_j}X - 1\right)$.

a) Montrer que $\left\|\widetilde{P}\right\|_2 = \|P\|_2$.

b) En déduire l'*inégalité de Landau* : $\quad M(P) \leqslant \|P\|_2$. $\quad$ On pourra s'intéresser au coefficient dominant de $\widetilde{P}$.

4) **a)** Montrer que pour tous $x_1, \dots, x_n \geqslant 0$: $\quad 1 + \sum_{k=1}^{n} \sigma_k(x_1, \dots, x_n) = \prod_{i=1}^{n}(1 + x_i) \leqslant 2^n \prod_{i=1}^{n} \max\left\{1, x_i\right\}$.

b) En déduire que pour tout $P \in \mathbb{C}[X]$ non constant de degré n : $\quad \|P\|_1 \leqslant 2^n M(P)$.

5) Soient $P \in \mathbb{Z}[X]$ non constant de degré n et $D \in \mathbb{Z}[X]$ un diviseur de P dans $\mathbb{Z}[X]$ — en d'autres termes $P = DQ$ pour un certain $Q \in \mathbb{Z}[X]$.

a) Montrer que $\|D\|_1\|Q\|_1 \leqslant 2^n M(P)$.

b) En déduire la *borne de Mignotte* : $\quad \|D\|_2 \leqslant 2^n \|P\|_2$.

Associée à des outils qu'il n'est pas possible de détailler ici, la borne de Mignotte est utilisée pour factoriser les polynômes de $\mathbb{Z}[X]$ en produit de polynômes de $\mathbb{Z}[X]$ de degrés inférieurs.