143/168

①

# Dev : Théorème de Kronecker.

Rombaldi : AGG p406
X-ENS T1 AG p 213
Caldero p35

Soit $P$ un polynôme unitaire de $\mathbb{Z}[X]$ dont les racines complexes sont toutes de module $\leq 1$. On suppose que $P(0) \neq 0$ !

Mq toutes les racines de $P$ sont racines de l'unité.

<u>Idée</u> : 1) on définit $E_n = \{ P \in \mathbb{Z}[X] \mid P$ unitaire de deg $n$ et $|z_i| \leq 1$ tq $P(z_i) = 0 \}$

$E_n$ est fini.

2) Soit $k \in \mathbb{Z}$ $P_k = \prod_{j=1}^{n} (X - \alpha_j^k) \in E_n$

3) Non injectivité entre deux ensembles.

<u>Preuve</u> : 1) Un polynôme de $E_n$ est donc de la forme $P(X) = \sum_{k=0}^{n} a_k X^k = \prod_{i=1}^{n} (X - z_i)$

où les $a_k \in \mathbb{Z}$ avec $a_0 = 1$ et $z_i$ sont les racines de $P$ tq $|z_i| \leq 1$.

On utilise les relations coefficients-racines.

(préciser la déf de $\sigma_{n-k}$) Gourdon p75 algèbre

$$P(X) = \sum_{k=0}^{n-1} (-1)^{n-k} \sigma_{n-k} X^k + X^n = \sum_{j=0}^{n} a_j X^j \quad \text{et } \underline{a_n = 1}$$

d'où
$$|a_j| = |\sigma_{n-j}| = \left| \sum_{1 \leq i_1 \leq \dots \leq i_j \leq n} z_{i_1} \cdots z_{i_j} \right|$$
$$\leq \sum_{1 \leq i_1 \leq \dots \leq i_j \leq n} |z_{i_1} \cdots z_{i_j}|$$
$$\leq \sum_{1 \leq i_1 \leq \dots \leq i_j \leq n} 1 = \binom{n}{n-j} = \binom{n}{j}$$

or $a_j \in \mathbb{Z}$, donc l'ensemble des coefficients possibles est fini, $E_n$ est fini.

↑ et nombre fini de coeff pour $n$ fixé !

2) Soit $P \in E_n$ et $C_P$ sa matrice compagnon.

On va montrer que le polynôme caractéristique $\chi_{C_P^m}$ de la puissance m-ième de $C_P$ est encore dans $E_n$. $\forall m \in \mathbb{N}$

$C_P$ s'écrit $\begin{pmatrix} 0 & & -a_0 \\ 1 & \ddots & \vdots \\ & 1 & -a_{n-1} \end{pmatrix}$ $\quad P = X^n + a_{n-1} X^{n-1} + \dots + a_0$

On a $\chi_{C_P} = P$

<u>preuve</u> : il faut calculer $\det(C_P - X I_n)$, donc le déterminant de la matrice

$$(C_P - X I_n) = \begin{pmatrix} -X & & & -a_0 \\ 1 & \ddots & & \vdots \\ & \ddots & \ddots & -a_{n-2} \\ 0 & & 1 & -X-a_{n-1} \end{pmatrix}$$

$L_1 \leftarrow L_1 + X L_2 + \dots + X^{n-1} L_n$ où $L_i$ désigne la ième ligne.

on obtient

$$\begin{pmatrix} 0 & 0 & \cdots & 0 & -P \\ 1 & -X & & \vdots & -a_1 \\ & \ddots & \ddots & 0 & \vdots \\ & & & & -a_{n-2} \\ 0 & & 1 & -X & -X-a_{n-1} \end{pmatrix}$$

Développant par rapport à la première ligne.

$$\det(C_P - X I_P) = (-1)^n P.$$

Au signe près, le polynôme caractéristique de la matrice est le polynôme donné

Donc sur $\mathbb{C}$, $\exists P \in GL_n(\mathbb{C})$ tel que $C_P = P^{-1} \begin{pmatrix} z_1 & & * \\ & \ddots & \\ 0 & & z_n \end{pmatrix} P$

d'où $C_P^m = P^{-1} \begin{pmatrix} z_1^m & & * \\ & \ddots & \\ 0 & & z_n^m \end{pmatrix} P$

d'où $\chi_{C_P^m} = \prod_{i=1}^{n} (X - z_i^m)$ unitaire, de degré $n$

et $\forall i \in [\![1, n]\!]$ $|z_i^m| \leq 1$

$\chi_{C_P^m} \in E_n$.

3) On $R_n = \{$ racines des polynômes $P \in E_n$, $z_i \in \mathbb{C} \}$

Comme l'ensemble $E_n$ est fini, alors $R_n$ est fini.

Soit $z \in R_n$, on définit $\varphi_z : \mathbb{N}^* \to R_n$, $m \mapsto z^m$

Elle ne peut pas être injective car $\mathbb{N}^*$ est infini et $R_n$ est fini

donc $\exists\, m$ et $m'$ tq $z^m = z^{m'}$ avec $m \neq m'$

si $z = 0$, c'est fini.

sinon $z^{m-m'} = 1$ donc $z \in$ racines de l'unité.

<u>Contre-exemple.</u> Polynôme n'est pas unitaire $P(X) = 2X + 1$

<u>Rq</u> : le th montre qu'avec ses hypothèses, toutes les racines non nulles sont des racines de l'unité.

Par contre, on peut voir que les racines non nulles sont forcément sur le cercle unité.

En effet, quitte à diviser par $X$ (pour enlever la racine 0), on se ramène au cas où le polynôme n'a pas de racines nulles.

Le produit des racines $\pi = \prod_{k=1}^{n} z_i$ est égal au signe près à $a_0$, il est donc entier.

et $|\pi| \leq 1$ et $\pi \in \mathbb{N}^*$ donc $|\pi| = 1$. Il en résulte que toutes les racines sont de module 1

Dénombrement de polynômes de Kronecker :

polynôme de $\mathbb{Z}[X]$ tq $\forall i \in [\![1, n]\!]$ $z_i \neq 0$ et $|z_i| \leq 1$

Combien y-a-t-il de polynômes selon le degré $n$ ?

deg 1 : $(z-1)$ et $(z+1)$

deg 2 : $|a_{n-k}| \leq \binom{n}{k}$ et $X^2 + aX + b$ avec $|a| \leq 2$ $|b| \leq 1$, $b \neq 0$

6 polynômes au total

Cas général : si un polynôme irréductible divise P de Kronecker,

c'est un polynôme minimal sur $\mathbb{Q}$ d'une racine de l'unité

donc 1 polynôme cyclotomique. . 1

$\mathbb{Z}[X]$ est factoriel, on a unicité de la décomp de P en produit de polynômes cyclotomiques.

↳ $P_i$ sont irréductibles dans $\mathbb{Z}[X]$ donc dans $\mathbb{Q}[X]$ !

Il faut donc faire un dénombrement de famille de poly. cyclotomiques avec répétition. tq $\sum \deg = n$

On utilise l'indicatrice d'Euler $\varphi(n)$ qui fournit le degré du polynôme cyclotomique $\Phi_n$.

Soit $Kr(n)$ le nombre cherché pour le degré $n$.

$$\sum_{n \geq 0} Kr(n) z^n = \prod_{n \geq 1} \frac{1}{1 - z^{\varphi(n)}}$$ (série génératrice)...